Algebraic Number Theory

PROCEEDINGS OF AN INSTRUCTIONAL CONFERENCE
ORGANIZED BY THE LONDON MATHEMATICAL SOCIETY

Edited by

J. W. S. CASSELS
Trinity College, University of Cambridge, U.K.

and

A. FRÖHLICH
King's College, University of London, U.K.

1967
ACADEMIC PRESS
London and New York

Алгебраическая теория чисел

ПОД РЕДАКЦИЕЙ
ДЖ. КАССЕЛСА и А. ФРЁЛИХА

Перевод с английского
А. А. БЕЛЬСКОГО, А. Ю. ГЕРОНИМУСА,
М. Е. НОВОДВОРСКОГО и В. М. ФИШМАНА

Под редакцией
И. И. ПЯТЕЦКОГО-ШАПИРО

ИЗДАТЕЛЬСТВО «МИР» ● МОСКВА 1969

УДК 511.6

Книга содержит лекции виднейших специалистов в области алгебраической теории чисел, охватывающие широкий круг вопросов этой теории — от ее классических разделов до самых последних достижений. Особенно подробно рассматриваются локальная и глобальная теории полей классов; излагается как история вопроса, так и его современное состояние.

Книга представляет большой интерес в первую очередь для специалистов в области алгебраической теории чисел. Однако она будет полезна и для математиков, интересующихся смежными областями, такими, например, как алгебраическая геометрия, теория чисел, теория автоморфных функций, теория алгебраических групп. Книга доступна для аспирантов и студентов старших курсов университетов и педагогических институтов.

Редакция литературы по математическим наукам

Инд. 2-2-3
1-69

ПРЕДИСЛОВИЕ РЕДАКТОРА ПЕРЕВОДА

Настоящая книга представляет собой сборник лекций по теории алгебраических чисел, прочитанных рядом крупнейших специалистов в этой области. Центральное место в ней занимают лекции Серра по локальной теории полей классов и лекции Тэйта по глобальной теории полей классов.

Теория полей классов (сам этот термин был введен Гильбертом) — это по существу изучение алгебраических расширений с коммутативной группой Галуа. В отличие от теории алгебраических расширений с некоммутативными группами Галуа теория полей классов представляется в настоящее время теорией, которая в основном закончена. В то же время она имеет многочисленные применения. Знакомство с ней необходимо не только для специалистов в данной области, но и для математиков, работающих в смежных областях, например в алгебраической геометрии, в теории автоморфных функций, теории алгебраических групп и т. д. Истории возникновения и развития теории полей классов посвящена лекция Хассе. Эта лекция охватывает лишь период до второй мировой войны. О современном же состоянии теории читатель может судить по другим лекциям, помещенным в книге.

Лекция IX и большая часть лекции XIV содержат изложение последних достижений советской школы по теории алгебраических чисел.

Несколько особняком в книге стоит лекция М. Кнезера по теории полупростых алгебраических групп. В отличие от других лекций, в которых, как правило, проводятся почти все доказательства, здесь доказательств очень мало. Однако предмет лекции по своему духу близок к основному содержанию сборника; поэтому помещение ее в книге вполне целесообразно.

В русском переводе мы сочли возможным опустить гл. XV. Причина состоит в том, что эта глава представляет собой диссертацию Тэйта (1950 г.), которая полностью содержится в недавно переведенной книге Ленга «Алгебраические числа».

И. И. Пятецкий-Шапиро

ПРЕДИСЛОВИЕ

Эта книга является результатом работы конференции по алгебраической теории чисел, проходившей с 1 по 17 сентября 1965 года в Сассексском университете в Брайтоне. Она была организована Лондонским математическим обществом под покровительством и при щедрой финансовой поддержке Международного математического объединения и Фонда научных исследований при НАТО. Организаторы конференции весьма обязаны постоянному содействию, которое им оказывали ведущие работники принявшего их университета.

Здесь собраны все лекции, прочитанные на конференции, за исключением нескольких сообщений информационного характера [1]); кроме того, в книгу включены упражнения, составленные Серром и Тэйтом. Тексты лекций для публикации либо предоставлялись самими авторами, либо были подготовлены участниками конференции в сотрудничестве с лекторами. Мы пользуемся случаем выразить нашу глубокую признательность лекторам как за удовольствие от встречи с ними, так и за возникшую в результате этого возможность опубликовать эту книгу. Мы также благодарны за сотрудничество тем, кто записал лекции и наряду с лекторами принимал участие в отшлифовке доказательств.

[1]) В русском переводе опущена гл. XV (диссертация Тэйта) по причине, указанной в предисловии редактора перевода.— *Прим. ред.*

Редакторы должны подчеркнуть, однако, что ни лекторы, ни лица, которые вели записи, не могут поручиться, что не осталось никаких неточностей.

Мы глубоко благодарны за содействие, которое оказали нам издатели.

Январь 1967 г.

Дж. У. С. Касселс
А. Фрёлих

Введение

Все главы этой книги являются публикациями лекций и лекционных курсов, читавшихся на конференции в Брайтоне. Темы и общая программа курсов были выбраны в соответствии с основной целью конференции, а именно: дать неспециалисту-математику (т. е. математику, специализирующемуся в какой-либо иной области) введение в алгебраическую теорию чисел, начиная с более элементарных аспектов и кончая теорией полей классов, а также ознакомить его с некоторыми из недавних успехов в этой области. Индивидуальные замыслы, таким образом, подчинены общему плану.

Первые три главы дают подробное введение в теорию полей алгебраических чисел; они содержат, в частности, все более элементарные сведения, необходимые в дальнейшем. Темы, излагающиеся в гл. I и II, тесно связаны между собой; соответствующие заглавия выбраны так, чтобы провести (не слишком точно) демаркационную линию между теориями локальных и глобальных полей. Можно было бы выбрать иные заглавия: «Алгебраическая теория дедекиндовых областей» для гл. I и «Топологическая арифметика» для гл. II.

Главы IV и V чисто утилитарны: в них приводятся конструкции, необходимые в теории полей классов.

Костяк книги состоит из двух глав — Серра и Тэйта — о локальной и глобальной теориях полей классов соответственно, причем вторая из названных глав зависит от первой. В главе Серра особенно интересным представляется впервые включенное как собственная часть локальной теории полей классов описание максимального абелева расширения в терминах формальных групп, принадлежащее Любину и Тэйту. Это дает новый подход к теореме суще-

ствования и к уточнению локального закона взаимности, связанному с вопросом о фильтрациях группы Галуа и группы единиц.

В то время как первые семь глав можно рассматривать как единое целое, остальные касаются различных частных вопросов теории и их применений. Эти последние главы совершенно независимы одна от другой, однако в них предполагается знание части материала первых семи глав. Упражнения, помещенные в конце книги,— они были составлены Серром и Тэйтом — имеют целью осветить некоторые вопросы, для которых не хватило времени на конференции.

Невозможно было (даже если бы это и было желательно) ввести вполне унифицированную систему обозначений во всех главах. Однако, помимо обозначений, являющихся слишком «классическими», чтобы упоминать о них, всюду выдерживались следующие: $\mathbf{Q}$, $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{C}$ — соответственно поле рациональных чисел, кольцо целых рациональных чисел, поле вещественных чисел и поле комплексных чисел; $\mathbf{F}$ (если не оговорено ничего другого) — конечное поле.

Специальная стрелка $\longmapsto$ обозначает результат отображения на типичном элементе множества. Так, отображение $\mathbf{R} \to \mathbf{R}$, состоящее в возведении всех чисел в квадрат, может быть записано следующим образом: $r \longmapsto r^2$ $(r \in R)$.

Литература к каждой главе помещена в конце этой главы.

ГЛАВА I

Локальные поля

А. Фрёлих

§ 1. ДИСКРЕТНО НОРМИРОВАННЫЕ КОЛЬЦА

Предварительные сведения о дробных идеалах. Пусть R — некоторая область целостности (т. е. коммутативное кольцо с единицей $1 \neq 0$ и без делителей нуля) и K — ее поле частных. Для R-подмодулей I_1, I_2 поля K можно естественным образом определить следующие операции:

$I_1 + I_2$ (сложение подмодулей);

$I_1 \cap I_2$

$I_1 I_2$ (этот подмодуль порожден произведениями вида ab, где $a \in I_1$, $b \in I_2$).

В дальнейшем будут рассматриваться еще два R-подмодуля поля K, которые сопоставляются каждому R-подмодулю I

$$I^{-1} = \{x \in K \mid xI \subset R\};$$
$$R(I) = \{x \in K \mid xI \subset I\}.$$

Лемма 1.1. (i) *Операции сложения, умножения и пересечения коммутативны и ассоциативны*;

(ii) $I(I_1 + I_2) = II_1 + II_2$;

(iii) $R(I) \supset R \supset II^{-1}$;

(iv) *если* $I \subset R$, *то* $I^{-1} \supset R$.

Назовем *дробным идеалом* кольца R всякий R-подмодуль I поля K, если он отличен от нуля и существует такой ненулевой элемент $a \in K$, что $aI \subset R$. В этой ситуации элемент a всегда может быть выбран из кольца R [1]).

[1]) Важно обратить внимание на то, что aI — идеал кольца R. Несмотря на отсутствие явных указаний, этот факт часто используется в дальнейшем.— *Прим. перев.*

Лемма 1.2. *Если подмодули I, I_1, I_2 являются дробными идеалами, то дробными идеалами будут также и подмодули $I_1 + I_2$, $I_1 \cap I_2$, $I_1 I_2$, I^{-1}, $R(I)$.*

Доказательство. Для первых трех операций утверждение леммы очевидно. Что касается последних двух, то мы докажем более общее утверждение: если I_1, I_2 — дробные идеалы, то модуль

$$J = \{x \in K \mid xI_2 \subset I_1\}$$

также представляет собой дробный идеал.

Пусть a, b — два ненулевых элемента, для которых справедливы включения $aI_2 \subset R$, $b \in I_1 \cap R$. Тогда произведение ab является ненулевым элементом модуля J. Если теперь c, d — ненулевые элементы, удовлетворяющие включениям $cI_1 \subset R$, $d \in I_2$, то $cdJ \subset R$.

Лемма 1.3. *Если кольцо R — нётерово, то ненулевой R-подмодуль I поля K является дробным идеалом в том и только том случае, когда он конечно порожден.*

Доказательство. Необходимость следует из того, что $I \cong aI \subset R$. Для доказательства достаточности нужно только воспользоваться домножением на произведение знаменателей образующих.

Пусть K^* — мультипликативная группа поля K и $\mathbf{Z}$ — группа целых чисел относительно сложения. Отображение

$$v: K \to \mathbf{Z} \cup \infty$$

называется *дискретным нормированием* поля K, если:

(i) отображение v задает сюръективный гомоморфизм групп

$$K^* \to \mathbf{Z}$$

(также обозначаемый через v);

(ii) $v(0) = \infty$;

(iii) $v(x+y) \geqslant \inf\{v(x), v(y)\}$

(на символ ∞ здесь накладываются обычные условия)[1]).

[1]) Ниже такое нормирование часто называется «нормализованным». Это делается для того, чтобы подчеркнуть, что отображение $K^* \to \mathbf{Z}$ является эпиморфизмом.— *Прим. перев.*

Сейчас мы дадим перевод этого определения на язык «мультипликативных» нормирований (см. гл. II). Если v — дискретное нормирование поля K и ρ — вещественное число, такое, что $0 < \rho < 1$, то функция $|x|_v = \rho^{v(x)}$ является дискретным (неархимедовым) мультипликативным нормированием в уточняемом позднее смысле. Такой вид имеет каждое дискретное мультипликативное нормирование, а эквивалентные мультипликативные нормирования соответствуют одному и тому же нормированию v и отличаются только выбором вещественного числа ρ. Таким образом, мы можем сделать и обратный переход — перевести результаты главы II на язык дискретных нормирований. В частности:

(а) если $v(x) \neq v(y)$, то $v(x+y) = \inf\{v(x), v(y)\}$;

(б) множество $R_v = \{x \in K \mid v(x) \geqslant 0\}$ представляет собой область целостности с полем частных K; это кольцо называют *кольцом нормирования* v, а множество $\mathfrak{p}_v = \{x \in K \mid v(x) > 0\}$, являющееся максимальным идеалом в этом кольце, называют *идеалом нормирования* v.

Подробно о топологии, определяемой нормированием, и о пополнениях говорится в следующей главе.

Предложение 1.1. *Каждое дискретное нормирование v поля K может быть единственным образом продолжено до дискретного нормирования пополнения $\bar{K}$ поля K относительно топологии, определенной данным нормированием.*

Доказательство. См. гл. II, § 10. Дискретное мультипликативное нормирование единственным образом продолжается на пополнение, и притом с тем же множеством значений.

Пример. Пусть F — поле и K — *поле формальных степенных рядов* вида

$$\sum_{n \gg -\infty}^{\infty} a_n t^n,$$

где $a_n \in F$ для всех $n \in \mathbf{Z}$, причем обозначение $n \gg -\infty$ указывает на то, что существует такое $m \in \mathbf{Z}$, что $a_n = 0$ при всех $n \leqslant m$. «Стандартное» дискретное нормирование

v поля K задается следующим образом:

$$v\Big(\sum_{n\gg-\infty}^{\infty} a_n t^n\Big) = \inf_{a_n\neq 0} n.$$

Поле K полно относительно топологии этого нормирования [1]).

Приступим к описанию в терминах теории колец пары K, v, где v — дискретное нормирование поля K. Элементы u, для которых $v(u) = 0$, образуют подгруппу $U = U_v$ группы K^*, называемую *группой единиц* (обратимых элементов) кольца R_v нормирования v. Выберем элемент π, для которого $v(\pi) = 1$. Тогда каждый элемент $a \in K^*$ единственным образом представляется в виде

$$a = \pi^n u, \quad n \in \mathbf{Z}, \quad u \in U,$$

где $n = v(a)$.

Определим для дробных идеалов I кольца R_v число

$$v(I) = \inf_{x\in I} v(x).$$

Априори $v(I) \subset \mathbf{Z} \cup \infty \cup -\infty$. Однако при некотором ненулевом идеале J кольца R_v и некотором элементе $a \in K^*$ справедливо равенство $I = aJ$. Следовательно, $v(I) = v(J) + v(a) \in \mathbf{Z}$. Зафиксируем элемент $b \in I$, для которого $v(b) = v(I)$. Тогда

$$\pi^{v(b)} R_v = bR_v \subset I.$$

С другой стороны, имеет место включение

$$I \subset \{x \in K \mid v(x) \geqslant v(I)\}.$$

Если $v(x) \geqslant v(I)$, то $x = \pi^{v(I)} y$, причем $y \in R_v$. Итак,

$$I \subset \pi^{v(I)} R_v = \pi^{v(b)} R_v;$$

следовательно,

$$I = (\pi R_v)^{v(I)}.$$

[1]) Не вдаваясь в подробности общих определений, укажем здесь на то, что последовательность $\{T_n\}$ рядов $T_n \in K$ называется фундаментальной (соответственно сходящейся к ряду $T \in K$), если для любого натурального M существует такое натуральное N, что при всех $n_1, n_2 > N$ (соответственно при всех $n > N$) справедливо неравенство $v(T_{n_1} - T_{n_2}) > M$ (соответственно неравенство $v(T_n - T) > M$). — *Прим. перев.*

В частности,

$$\mathfrak{p}_v = \pi R_v$$

и, таким образом,

$$I = \mathfrak{p}_v^{v(I)}.$$

Последнее равенство показывает, что кольцо R_v обладает одним и только одним ненулевым простым идеалом, а именно идеалом $\mathfrak{p}_v$; предыдущее же равенство показывает, что R_v является областью главных идеалов. Дадим теперь определение: *дискретно нормированным кольцом* называется область главных идеалов R, обладающая одним и только одним ненулевым простым идеалом. Таким образом, мы доказали первую половину следующего утверждения.

Предложение 1.2. *Кольцо R_v дискретного нормирования v является дискретно нормированным кольцом.*

Обратно, каждое дискретно нормированное кольцо R является кольцом R_v некоторого однозначно определенного дискретного нормирования v поля частных K кольца R.

Доказательство второй части предложения 1.2. Пусть $\mathfrak{p} = \pi R$ — ненулевой простой идеал кольца R. Поскольку кольцо R является областью с однозначным разложением на множители, каждый ненулевой элемент $x \in R$ имеет единственное разложение вида $x = \pi^n \cdot u$, где u — единица и $n \geqslant 0$. Заставляя n пробегать всю группу $\mathbf{Z}$, мы получим аналогичное утверждение для каждого $x \in K^*$. Но тогда отображение

$$v(x) = n$$

определяет дискретное нормирование v поля K, для которого $R = R_v$. Единственность нормирования очевидна.

Предложение 1.3. *Область целостности R является дискретно нормированным кольцом тогда и только тогда, когда она нётерова, целозамкнута и обладает ровно одним ненулевым простым идеалом.*

(Элемент x из некоторого кольца, в котором содержится кольцо R, называется *целым* над R, если он является корнем многочлена с коэффициентами из R, старший коэффициент

которого равен единице [1]), т. е. если кольцо $R[x]$ есть конечно порожденный R-модуль. Кольцо R называется *целозамкнутым*, если каждый элемент поля частных кольца R, целый над R, принадлежит R.)

Доказательство (достаточность). Пусть I — любой дробный идеал области R. Рассмотрим идеал $R(I)$ как кольцо (см. определение перед леммой 1.1). Тогда для каждого $x \in R(I)$ кольцо $R[x]$ является подмодулем кольца $R(I)$. Согласно леммам 1.2 и 1.3, модуль $R(I)$ конечно порожден над R, а следовательно, то же имеет место и для модуля $R[x]$. Поэтому x является целым над кольцом R, т. е. $x \in R$. Таким образом,

$$R(I) = R. \tag{1}$$

Пусть $\mathfrak{p}$ — тот единственный ненулевой простой идеал кольца R, о котором говорится в формулировке предложения. Мы покажем, что

$$\mathfrak{p}^{-1} \neq R. \tag{2}$$

Кольцо R обладает такими ненулевыми идеалами I, что $I^{-1} \neq R$; таковыми, например, являются все главные идеалы aR, где $a \in \mathfrak{p}$, $a \neq 0$. Пусть J — ненулевой идеал, являющийся максимальным среди идеалов с указанным свойством. Мы должны показать, что идеал J простой.

Пусть $x, y \in R$, $x \notin J$, $xy \in J$, $z \notin R$, $z \in J^{-1}$. Тогда $zy(xR + J) \subset R$, следовательно, $zy \in R$, и потому $z(yR + J) \subset R$. Отсюда следует, что $(yR + J)^{-1} \neq R$, однако $yR + J \supset J$; поэтому $y \in J$. Соотношение (2) теперь доказано.

В силу леммы 1.1 (пункты (iii), (iv)) мы имеем, что

$$R \supset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{p}R = \mathfrak{p}.$$

Однако равенство $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ означало бы, что $\mathfrak{p}^{-1} \subset R$ ($\mathfrak{p}$), а это противоречит соотношениям (1) и (2). Следовательно,

$$R = \mathfrak{p}\mathfrak{p}^{-1}. \tag{3}$$

Ясно, что $\mathfrak{p}^{-1} \subset R$ ($\cap \mathfrak{p}^n$). В силу соотношений (1), (2) мы получаем, что

$$\cap\, \mathfrak{p}^n = 0. \tag{4}$$

[1]) Многочлен со старшим коэффициентом 1 в дальнейшем часто называется унитарным.— *Прим. перев.*

По этой причине можно выбрать некоторый элемент $a \in \mathfrak{p}$, такой, что $aR \not\subset \mathfrak{p}^2$. Тогда $a\mathfrak{p}^{-1} \subset R$, но в силу соотношения (3) $a\mathfrak{p}^{-1} \not\subset \mathfrak{p}$. Значит, $a\mathfrak{p}^{-1}$ является идеалом кольца R, не содержащимся ни в каком максимальном идеале, т. е. $a\mathfrak{p}^{-1} = R$ [1]), и потому

$$\mathfrak{p} = aR.$$

В силу соотношения (4) каждый ненулевой элемент кольца R однозначно представляется в виде $a^n u$, где $n \geqslant 0$ и u — единица в кольце R. Таким образом, кольцо R является дискретно нормированным.

В заключение мы дадим описание некоторых групп, связанных с заданным дискретным нормированием v поля K, в терминах поля вычетов $k = R/\mathfrak{p}$, где R — кольцо дискретного нормирования v, а $\mathfrak{p}$ — идеал этого нормирования.

Аддитивная группа поля K является объединением открытых (и, следовательно, замкнутых [2])) подгрупп $\mathfrak{p}^n$, $n \in \mathbf{Z}$, пересечение которых равно нулю. Факторгруппы $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ обладают структурой k-модуля, и потому имеет место

Лемма 1.4. *Существует некоторый изоморфизм k-модулей*

$$k \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}.$$

Доказательство. Если $\mathfrak{p} = R\pi$, то умножение на π^n индуцирует такой изоморфизм.

Обращаясь к мультипликативной группе K^* ненулевых элементов поля K, мы прежде всего заметим, что нормиро-

[1]) Здесь неявно используется теорема коммутативной алгебры о том, что каждый отличный от всего кольца идеал содержится в некотором максимальном идеале.— *Прим. перев.*

[2]) В этой книге часто используется следующий простой факт из теории топологических групп: каждая открытая подгруппа топологической группы замкнута. Это следует из того, что дополнение к открытой подгруппе, являясь объединением смежных классов по ней, также открыто.— *Прим. перев.*

вание v приводит к точной последовательности [1])

$$0 \to U \to K^* \xrightarrow{v} \mathbf{Z} \to 0, \tag{5}$$

где U — группа единиц кольца R. Для каждого $n \geqslant 1$ множество

$$U_n = 1 + \mathfrak{p}^n \tag{6}$$

является открытой подгруппой в группе U, и $\bigcap\limits_n U_n = 1$. Следовательно, топология на группе U, определенная этими подгруппами, совпадает с топологией, индуцированной на группе U как на подмножестве поля K, топологией нормирования. Факторгруппы могут быть вновь описаны в терминах поля вычетов.

Предложение 1.4. (i) *Отображение $R \to k$, задаваемое переходом к классам вычетов, индуцирует изоморфизм*

$$U/U_1 \cong k^*,$$

где k^* — мультипликативная группа поля k.

(ii) *Для каждого $n \geqslant 1$ отображение $u \mapsto u - 1$ индуцирует изоморфизм*

$$U_n/U_{n+1} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}.$$

Доказательство проводится очевидным образом. Нужно лишь заметить, что для $u_1, u_2 \in U_n$ имеет место

$$(u_1u_2 - 1) - (u_1 - 1) - (u_2 - 1) = (u_1 - 1)(u_2 - 1) \in \mathfrak{p}^{2n}.$$

Следствие. *Для $n \geqslant 1$ имеет место изоморфизм*

$$U_n/U_{n+1} \cong k^+,$$

где через k^+ обозначена аддитивная группа поля k.

Предложение 1.5. (i) *Если поле k имеет простую характеристику p, то для $n \geqslant 1$ имеет место*

$$U_n^p \subset U_{n+1}.$$

(ii) *Если поле K полно, а натуральное число m не делится на характеристику поля вычетов, то для каждого $n \geqslant 1$ отображение $u \mapsto u^m$ является автоморфизмом группы U_n.*

[1]) Эта последовательность не является канонической, поскольку она существенно зависит от выбора элемента $\pi \in K$, для которого $v(\pi) = 1$. — *Прим. перев.*

Доказательство. Пункт (i) вытекает из предыдущего следствия. Для доказательства пункта (ii) мы прежде всего заметим, что, согласно тому же самому следствию, эндоморфизм группы U_q/U_{q+1}, индуцированный эндоморфизмом $f : u \mapsto u^m$ группы U_n, биективен для каждого $q \geqslant n$. Следовательно, гомоморфизм f уже по крайней мере инъективен. Далее, для каждого элемента $u \in U_n$ мы можем найти такие элементы $v_0 \in U_n$, $w_1 \in U_{n+1}$, что $u = v_0^m w_1$. Затем можно отыскать такие элементы $v_1 \in U_{n+1}$, $w_2 \in U_{n+2}$, что $w_1 = v_1^m w_2$, т. е. $u = (v_0 v_1)^m w_2$. Этот процесс можно продолжать неограниченно. Последовательность $w_1, w_2, \ldots$ будет сходиться к 1, а так как группа U_n полна, то бесконечное произведение $v_0 v_1 \ldots$ будет сходиться к некоторому элементу v из группы U_n. Но тогда $u = v^m \in U_n^m$. Таким образом, мы показали, что отображение f сюръективно, а потому и биективно.

§ 2. ДЕДЕКИНДОВЫ ОБЛАСТИ

На протяжении этого параграфа через R обозначается некоторая область целостности, а через K — ее поле частных. Для любого простого идеала $\mathfrak{p}$ кольца R определим локальное кольцо частных $R_\mathfrak{p}$ следующим образом:

$$R_\mathfrak{p} = \{x \cdot y^{-1} \in K \mid x,\ y \in R,\ y \notin \mathfrak{p}\}.$$

Идеал $\mathfrak{p}R_\mathfrak{p}$ является единственным максимальным идеалом кольца $R_\mathfrak{p}$. Очевидно, что $\mathfrak{p} \subset \mathfrak{p}R_\mathfrak{p} \cap R$. Если же $x \in R$, $x \notin \mathfrak{p}$, то $x^{-1} \in R_\mathfrak{p}$, а потому $x \notin \mathfrak{p}R_\mathfrak{p}$. Итак, имеет место

Лемма 2.1. $\mathfrak{p} = \mathfrak{p}R_\mathfrak{p} \cap R$.

Теперь докажем следующее утверждение.

Лемма 2.2. *Если J — некоторый идеал в кольце $R_\mathfrak{p}$, то*

$$J = (J \cap R) R_\mathfrak{p}.$$

Доказательство. Пусть $x, y \in R$, $y \notin \mathfrak{p}$ и $xy^{-1} \in J$. Тогда $x \in J \cap R$, откуда $xy^{-1} \in (J \cap R) R_\mathfrak{p}$. Следовательно, $(J \cap R) R_\mathfrak{p} \supset J$. Обратное включение устанавливается еще проще.

Предложение 2.1. *Каждое из следующих условий, наложенных на область целостности R, влечет за собой остальные*:

(i) *кольцо R нётерово, целозамкнуто и его ненулевые простые идеалы максимальны*;

(ii) *кольцо R нётерово и для каждого простого ненулевого идеала $\mathfrak{p}$ кольцо $R_{\mathfrak{p}}$ дискретно нормировано*;

(iii) *все дробные идеалы кольца R обратимы.*

(Дробный идеал I называется *обратимым*, если $II^{-1}=R$.)

Область R, удовлетворяющая условиям этого предложения, называется *дедекиндовой областью*. Например, любая область главных идеалов — дедекиндова.

Доказательство. (а) *Из* (i) *следует* (ii).

Воспользуемся предложением 1.3. В силу леммы 2.2 каждый идеал кольца $R_{\mathfrak{p}}$ имеет вид $IR_{\mathfrak{p}}$, где I — некоторый идеал из R. Конечное множество образующих модуля I над кольцом R является также конечным множеством образующих $R_{\mathfrak{p}}$-модуля $IR_{\mathfrak{p}}$. Таким образом, кольцо $R_{\mathfrak{p}}$ нётерово.

Если x — целый элемент над кольцом $R_{\mathfrak{p}}$, т. е.

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

где $b,\ a_i \in R,\ b \notin \mathfrak{p}$, то элемент bx является целым над кольцом R. Следовательно, если элемент x лежит в поле частных K кольца R, то $bx \in R$, откуда $x \in R_{\mathfrak{p}}$.

Пусть J — ненулевой простой идеал кольца $R_{\mathfrak{p}}$. Пересечение $J \cap K$ является, конечно, простым идеалом кольца R и притом, согласно лемме 2.2, ненулевым. В силу включения $J \subset \mathfrak{p}R_{\mathfrak{p}}$, справедливого потому, что $\mathfrak{p}R_{\mathfrak{p}}$ — единственный максимальный идеал в кольце $R_{\mathfrak{p}}$, пересечение $J \cap R$ принадлежит идеалу $\mathfrak{p}$ (лемма 2.1). Следовательно, $J \cap R = \mathfrak{p}$ и, согласно лемме 2.2, $J = \mathfrak{p}R_{\mathfrak{p}}$.

(б) *Из* (ii) *следует* (iii).

Пусть I — дробный идеал кольца R с образующими $a_1, \ldots, a_n$. Тогда при некотором i имеет место $v_{\mathfrak{p}}(a_i) = \inf_{x \in I} v_{\mathfrak{p}}(x)$, где $v_{\mathfrak{p}}$ — нормирование с кольцом нормирования $R_{\mathfrak{p}}$. Пусть для определенности $i = 1$. Тогда $IR_{\mathfrak{p}} = a_1 R_{\mathfrak{p}}$.

Следовательно,

$$a_1^{-1}a_i = x_i y_i^{-1},$$

где $x_i,\ y_i \in R,\ y_i \notin \mathfrak{p}\ (i = 1, \ldots, n)$. Пусть $y = \prod_i y_i$. Тогда $ya_1^{-1}a_i \in R$; поэтому $ya_1^{-1} \in I^{-1}$ и $y \in II^{-1}$. Однако, так как $y \notin \mathfrak{p}$, произведение II^{-1} не принадлежит $\mathfrak{p}$. Это верно для всех максимальных идеалов $\mathfrak{p}$ кольца R. Следовательно, $II^{-1} = R$.

(в) *Из* (iii) *следует* (i).

Пусть I — дробный идеал кольца R. Тогда существуют такие элементы $a_1, \ldots, a_n \in I,\ b_1, \ldots, b \in I^{-1}$, что $\sum a_i b_i = 1$. Если $x \in I$, то $x = \sum a_i (b_i x)$, причем $b_i x \in R$. Следовательно, элементы $a_1, \ldots, a_n$ порождают идеал I. Это означает, что кольцо R нётерово.

Пусть $x \in K$ — целый элемент над R. В силу леммы 1.3 множество $S = R[x]$ является дробным идеалом. Кроме того, оно является кольцом, т. е. $S^2 = S$. Следовательно,

$$S = SR = SSS^{-1} = SS^{-1} = R.$$

Это означает, что кольцо R целозамкнуто.

Пусть I — ненулевой простой идеал, а $\mathfrak{p}$ — максимальный идеал, его содержащий. Тогда $I\mathfrak{p}^{-1}$ — идеал кольца R и $(I\mathfrak{p}^{-1})\mathfrak{p} = I$. Поэтому или $I\mathfrak{p}^{-1} \subset I$, или $\mathfrak{p} \subset I$, т. е. $\mathfrak{p} = I$. Но первое соотношение означает, что

$$\mathfrak{p}^{-1} \subset I^{-1}I\mathfrak{p}^{-1} \subset I^{-1}I = R,$$

т. е. $\mathfrak{p}^{-1} = R$ и, таким образом, $\mathfrak{p} = R$, что невозможно.

Предложение 2.1 доказано.

Если $\mathfrak{p}$ — ненулевой простой идеал дедекиндовой области R, то через $v_{\mathfrak{p}}$ мы будем обозначать нормирование ее поля частных K с кольцом нормирования $R_{\mathfrak{p}}$.

Следствие 1. *Пусть $|x|$ — нетривиальное мультипликативное нормирование поля K, для которого $|R| \leqslant 1$. Тогда $|x| = \rho^{v_{\mathfrak{p}}(x)}$ при некотором ρ, $0 < \rho < 1$, и некотором ненулевом простом идеале $\mathfrak{p}$ кольца R.*

Доказательство. Неравенство $|x| < 1$ определяет некоторый ненулевой простой идеал $\mathfrak{p} \subset R$. Следо-

вательно, локальное кольцо $R_\mathfrak{p}$ характеризуется в поле K неравенством $|x| \leqslant 1$. Из этого и вытекает наше утверждение.

Для каждого непустого подмножества I поля K положим

$$v_\mathfrak{p}(I) = \inf_{x \in I} v_\mathfrak{p}(x)$$

(может случиться, что $v_\mathfrak{p}(I) = -\infty$).

Предложение 2.2. *Дробные идеалы дедекиндовой области R образуют абелеву группу $\mathscr{F}(R)$ относительно умножения. Эта группа свободно порождается простыми идеалами $\mathfrak{p}$. Представление любого дробного идеала I через эти образующие задается равенством*

$$I = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(I)}.$$

Кроме того,

$$IR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^{v_\mathfrak{p}(I)}.$$

Доказательство. Первое утверждение следует из леммы 1.1 и из предложения 2.1.

Для того чтобы показать, что простые идеалы $\mathfrak{p}$ порождают группу $\mathscr{F}(R)$, достаточно проверить, что каждый целый идеал I (т. е. такой, что $I \subset R$), отличный от R, является произведением простых идеалов. Всякий такой идеал I содержится в некотором максимальном идеале $\mathfrak{p}$. Следовательно, $I = \mathfrak{p}(I\mathfrak{p}^{-1})$ при $I \subset I\mathfrak{p}^{-1} \subset R$. Требуемый результат получается теперь из условия обрыва возрастающих цепей.

Благодаря тому, что в силу леммы 1.1 $(IR_\mathfrak{p})(JR_\mathfrak{p}) = (IJ)R_\mathfrak{p}$, мы получаем сюръективный гомоморфизм

$$f_\mathfrak{p} : \mathscr{F}(R) \to \mathscr{F}(R_\mathfrak{p}), \qquad (1)$$

который инъективен на подгруппе, порожденной идеалом $\mathfrak{p}$. Если $\mathfrak{p}_1 \neq \mathfrak{p}$, то $\mathfrak{p}_1 R_\mathfrak{p} = R_\mathfrak{p}$. Для $a \in \mathfrak{p}_1$, $a \notin \mathfrak{p}$ в таком случае справедливо равенство $aR_\mathfrak{p} = R_\mathfrak{p}$. Поэтому каждый простой идеал $\mathfrak{p}_1$, отличный от $\mathfrak{p}$, лежит в $\ker f_\mathfrak{p}$. В качестве первого следствия отсюда получается, что ненулевые простые идеалы составляют множество свободных образующих группы $\mathscr{F}(R)$. Во-вторых, мы видим, что если

$$I = \prod \mathfrak{p}^{r_\mathfrak{p}},$$

то

$$IR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^{r_\mathfrak{p}}.$$

Следовательно,

$$r_\mathfrak{p} = v_\mathfrak{p}(IR_\mathfrak{p}) = v_\mathfrak{p}(I) + v_\mathfrak{p}(R_\mathfrak{p}) = v_\mathfrak{p}(I).$$

Следствие 1. *Если $a \in K^*$, то для почти всех простых идеалов $\mathfrak{p}$ имеет место $v_\mathfrak{p}(a) = 0$.*

Следствие 2.

$$v_\mathfrak{p}(I_1 I_2) = v_\mathfrak{p}(I_1) + v_\mathfrak{p}(I_2),$$
$$v_\mathfrak{p}(I^{-1}) = -v_\mathfrak{p}(I),$$
$$v_\mathfrak{p}(I_1 + I_2) = \inf\{v_\mathfrak{p}(I_1),\ v_\mathfrak{p}(I_2)\},$$
$$v_\mathfrak{p}(I_1 \cap I_2) = \sup\{v_\mathfrak{p}(I_1),\ v_\mathfrak{p}(I_2)\}.$$

Следствие 3. *Отображение $f_\mathfrak{p}$ индуцирует некоторый изоморфизм*

$$\mathscr{F}(R) \cong \prod_\mathfrak{p} \mathscr{F}(R_\mathfrak{p}).$$

(Символ $\prod$ употребляется для ограниченных прямых произведений или прямых сумм групп.)

Пусть $\bar{R}_\mathfrak{p}$ — кольцо нормирования пополнения поля K относительно $v_\mathfrak{p}$. Согласно предложению 1.1,

$$\mathscr{F}(R_\mathfrak{p}) \cong \mathscr{F}(\bar{R}_\mathfrak{p}) \qquad (\cong \mathbf{Z}!).$$

Следовательно, имеет место

$$\mathscr{F}(R) \cong \prod_\mathfrak{p} \mathscr{F}(\bar{R}_\mathfrak{p}).$$

§ 3. МОДУЛИ И БИЛИНЕЙНЫЕ ФОРМЫ

В этом параграфе мы вводим ряд понятий, которые впоследствии используются при рассмотрении норм идеалов, дифферент и дискриминантов расширений дедекиндовых

областей. Мы обозначаем здесь через R некоторую дедекиндову область, через K — ее поле частных, через U — некоторое конечномерное векторное пространство над полем K размерности $n > 0$. Символом T всегда обозначается R-подмодуль пространства U, а символы L, M, N употребляются для конечно порожденных R-подмодулей, порождающих пространство U, т. е. содержащих его базис. Если $\mathfrak{p}$ — ненулевой простой идеал кольца R, то $T_\mathfrak{p} = TR_\mathfrak{p}$ обозначает $R_\mathfrak{p}$-модуль, порожденный модулем T.

Лемма 3.1. $\bigcap_\mathfrak{p} T_\mathfrak{p} = T$.

Доказательство. Если $\mathfrak{p}$ пробегает множество простых идеалов, содержащее все максимальные, то этот факт будет верным не только для дедекиндовой, но и для любой области целостности R.

Ясно, что $T \subset \bigcap_\mathfrak{p} T_\mathfrak{p}$. Для доказательства обратного включения рассмотрим элемент u из $\bigcap_\mathfrak{p} T_\mathfrak{p}$ и покажем, что идеал

$$J_u = \{x \in R \mid xu \in T\}$$

совпадает со всем кольцом R, т. е. не содержится ни в одном максимальном идеале $\mathfrak{p}$. Действительно, $u = x^{-1}w$, где $w \in T$, $x \in R$, $x \notin \mathfrak{p}$. Так как $x \in J_u$, то, очевидно, $J_u \not\subset \mathfrak{p}$.

Лемма 3.2. *Для любых двух модулей M и N существует такой ненулевой элемент $a \in K$, что $aM \subset N$.*

Доказательство. Пусть $\{u_i\}$ — базис пространства U, содержащийся в модуле N. Тогда в качестве элемента a можно взять «общий знаменатель» коэффициентов тех линейных комбинаций, которыми представляются элементы некоторого заданного множества образующих $\{w_i\}$ модуля M через базис $\{u_i\}$.

Лемма 3.3. *Для почти всех $\mathfrak{p}$ имеет место равенство*

$$M_\mathfrak{p} = N_\mathfrak{p}.$$

Доказательство. Согласно предыдущей лемме, мы можем выбрать такие ненулевые элементы a, $b \in K$, что $aM \subset N \subset bM$. Поэтому $M_\mathfrak{p} = N_\mathfrak{p}$, если только

$v_\mathfrak{p}(a) = v_\mathfrak{p}(b) = 0$. В силу следствия 1 из предложения 2.2 последние равенства имеют место для почти всех идеалов $\mathfrak{p}$.

Будем временно считать, что M и N — свободные R-модули. Поскольку ранг каждого из них равен n, они изоморфны. Поэтому существует такое неособое линейное преобразование ℓ пространства U, что $M\ell = N$. Определитель $\det(\ell)$ отличен от нуля и с точностью до обратимого элемента кольца R зависит только от модулей M и N. Следовательно, только от M и N зависит и дробный идеал

$$R \det(\ell) = (M : N). \tag{1}$$

Пусть теперь условие, что модули M и N свободны, не выполняется. Тогда для каждого простого идеала $\mathfrak{p}$ кольца R рассмотрим дробный идеал $(M_\mathfrak{p} : N_\mathfrak{p})$ кольца $R_\mathfrak{p}$. Из равенства $M_\mathfrak{p} = N_\mathfrak{p}$ следует, что $(M_\mathfrak{p} : N_\mathfrak{p}) = R_\mathfrak{p}$. В силу леммы 3.3 и следствия 3 из предложения 2.2 существует такой однозначно определенный дробный идеал

$$(M : N) = (M : N)_R$$

кольца R, называемый *индексом модулей*, что при всех $\mathfrak{p}$

$$(M : N) R_\mathfrak{p} = (M_\mathfrak{p} : N_\mathfrak{p}). \tag{2}$$

Легко проверяется, что определения (1) и (2) согласуются между собой, когда модули M и N свободны. Нетрудно видеть также, что если $R = \mathbf{Z}$ и $M \supset N$, то $(M : N)$ — индекс в обычном групповом смысле, рассматриваемый как $\mathbf{Z}$-идеал.

Предложение 3.1.

(i) $(M : N)(N : L) = (M : L)$;
$(M : M) = R$;

(ii) *предположим, что $M \supset N$. Тогда индекс $(M : N)$ является целым идеалом и из равенства $(M : N) = R$ следует равенство $M = N$.*

Доказательство. В локальном случае (т. е. для каждого кольца $R_\mathfrak{p}$) предложение очевидно. В глобальном же случае надо применить лемму 3.1 и воспользоваться предложением 2.2.

Предложение 3.2. *Если t — неособое линейное преобразование векторного пространства U, то*

$$(Mt : Nt) = (M : N).$$

Доказательство получается сразу сведением к локальному случаю и применением определения (1).

Можно, кроме того, показать, что изоморфизм $M \cong N$ имеет место в том и только том случае, когда индекс $(M : N)$ является главным дробным идеалом.

Пусть теперь $B(u, v)$ — невырожденная симметричная K-билинейная форма на векторном пространстве U. Если $\{u_i\}$ — базис пространства U, то *двойственный базис* $\{v_j\}$ определяется равенствами

$$B(u_i, v_j) = \delta_{ij},$$

где δ_{ij} — символ Кронекера.

Двойственный модуль $D(T)$ для модуля T определяется следующим образом:

$$D(T) = D_R(T) = \{u \in U \mid B(u, T) \subset R\}. \qquad (3)$$

Лемма 3.4. *Если M — свободный R-модуль с базисом $\{u_i\}$, то модуль $D(M)$ является свободным R-модулем, порожденным базисом $\{v_j\}$, и имеет место равенство*

$$D(D(M)) = M.$$

Доказательство очевидно.

В последующем символ D обозначает переход к двойственному модулю относительно кольца R, а вместо $D_{R\mathfrak{p}}$ мы будем писать $D_{\mathfrak{p}}$.

Предложение 3.3.

(i) *Модуль $D(M)$ является конечно порожденным R-модулем, порождающим пространство U;*

(ii) $D(M)_{\mathfrak{p}} = D_{\mathfrak{p}}(M_{\mathfrak{p}})$;

(iii) $D(M) = \bigcap_{\mathfrak{p}} D_{\mathfrak{p}}(M_{\mathfrak{p}})$;

(iv) $D(D(M)) = M$;

(v) $(D(M) : D(N)) = (N : M)$.

Доказательство. (i) Модуль M содержит свободный R-модуль N и, согласно лемме 3.2, содержится в некотором свободном R-модуле $L = bN$, причем как L, так и N порождают пространство U. Следовательно,

$$D(N) \supset D(M) \supset D(L).$$

В силу леммы 3.4 модули $D(L)$ и $(D(N)$ свободны и порождают пространство U. Из этого вытекает (i).

(ii) Пусть $\{w_i\}$ — конечное множество образующих модуля M. Предположим, что $v \in D_{\mathfrak{p}}(M_{\mathfrak{p}})$. Тогда при всех i выполняется равенство $B(v, w_i) = b^{-1}a_i$, где a_i, $b \in R$, $b \notin \mathfrak{p}$. Итак, $v \in D(M)\, b^{-1} \subset D(M)_{\mathfrak{p}}$. Мы показали, что

$$D_{\mathfrak{p}}(M)_{\mathfrak{p}} \subset D_R(M)_{\mathfrak{p}}.$$

Чтобы получить обратное включение, заметим, что

$$B(D_R(M_{\mathfrak{p}}), M_{\mathfrak{p}}) \subset B(D_R(M), M)\, R_{\mathfrak{p}} \subset R_{\mathfrak{p}}.$$

Утверждение (iii) следует из (ii) и леммы 3.1, а утверждение (iv) — из (ii) и леммы 3.4. Доказательство утверждения (v) на основании (ii) сводится к случаю, когда модули M и N свободны. Напомним лишь, что если $\{u_i\}$ и $\{v_j\}$ — двойственные базисы и базисы $\{u_i \ell\}$ и $\{v_j \ell^*\}$ также двойственны, то

$$\det(\ell) \det(\ell^*) = 1.$$

Предложение 3.3 доказано.

Определим теперь *дискриминант* $\mathfrak{d}(M)$ модуля M равенством

$$\mathfrak{d}(M) = \mathfrak{d}(M/R) = (D_R(M) : M)_R. \qquad (4)$$

Предложение 3.4.

(i) $\mathfrak{d}(N) = \mathfrak{d}(M)(M : N)^2$;

(ii) $\mathfrak{d}(M_{\mathfrak{p}}/R_{\mathfrak{p}}) = \mathfrak{d}(M/R)\, R_{\mathfrak{p}}$;

(iii) *если M — свободный R-модуль, натянутый на множество $\{u_i\}$, то дискриминант $\mathfrak{d}(M)$ является дробным идеалом, порожденным определителем*

$$\det B(u_i, u_j).$$

Доказательство. (i) В силу предложения 3.1, (i) имеет место равенство

$$(D(N):N) = (D(N):D(M))\,(D(M):M)\,(M:N),$$

а его правая часть равна $(D(M):M)\,(M:N)^2$ в силу предложения 3.3, (v).

Утверждение (ii) следует из предложения 3.3, (ii).

Для доказательства утверждения (iii) рассмотрим базис $\{v_j\}$, двойственный к базису $\{u_i\}$, и положим $u_i = v_i \ell$. Согласно лемме 3.4,

$$(D(M):M) = R \det(\ell).$$

С другой стороны,

$$\det B(u_i, v_j\ell) = \det(\ell) \det B(u_i, v_j) = \det(\ell).$$

Следствие 1. *Пусть $M \supset N$. Тогда дискриминант $\mathfrak{d}(M)$ делит дискриминант $\mathfrak{d}(N)$, и равенство $\mathfrak{d}(M) = \mathfrak{d}(N)$ влечет за собой равенство $M = N$.*

Последнее предложение показывает, что в случае $R = \mathbf{Z}$ введенный нами дискриминант совпадает с точностью до знака с классическим дискриминантом над кольцом $\mathbf{Z}$.

Пусть теперь $U = U_1 + U_2$ — прямая сумма векторных пространств. Предположим, что модули M_i и N_i порождают пространство U_i, и введем следующие обозначения: $M = M_1 + M_2$, $N = N_1 + N_2$. Для утверждений (ii) и (iii) в следующем предложении предположим также, что $B(U_1, U_2) = 0$, так что B задает невырожденную билинейную форму на каждом из пространств U_1 и U_2.

Предложение 3.5.

(i) $(M:N) = (M_1:N_1)\,(M_2:N_2)$;

(ii) $D(M) = D(M_1) + D(M_2)$;

(iii) $\mathfrak{d}(M) = \mathfrak{d}(M_1)\cdot\mathfrak{d}(M_2)$.

Доказательство очевидно.

Для простоты будем в дальнейшем считать, что M и N — свободные R-модули, хотя утверждения будут оставаться справедливыми и в общем случае. Пусть $\overline{R}$ — дедекиндова область, содержащая кольцо R и имеющая полем частных поле $\overline{K}$. Пространство U будет рассматриваться как подпространство векторного пространства $\overline{U} = U \otimes_K \overline{K}$ над полем $\overline{K}$. Билинейная форма B может быть единственным образом продолжена до некоторой $\overline{K}$-билинейной формы $\overline{B}$, которая также симметрична и невырождена. Наконец, $\overline{R}$-модуль $M\overline{R}$, порожденный модулем M, свободен и порождает пространство $\overline{U}$.

Предложение 3.6.

(i) $(M\overline{R} : N\overline{R})_{\overline{R}} = (M:N)_R\overline{R}$;

(ii) $D_{\overline{R}}(M\overline{R}) = D_R(M)\overline{R}$;

(iii) $\mathfrak{d}(M\overline{R}/\overline{R}) = \mathfrak{d}(M/R)\,\overline{R}$.

Доказательство очевидно.

§ 4. РАСШИРЕНИЯ

В этом параграфе через R обозначается некоторая дедекиндова область, через K — ее поле частных и через L — некоторое конечное сепарабельное алгебраическое расширение поля K. Условие о сепарабельности не является обязательным для части предложения 4.1, а также для предложения 4.2 (см. [1], гл. V, теорема 19, и [3], гл. II, предложение 3). Однако здесь несепарабельный случай мы рассматривать не будем.

Элементы поля L, являющиеся целыми над кольцом R, образуют кольцо S, которое называется *целым замыканием* кольца R в поле L; кольцо S целозамкнуто в поле L (см. [1], гл. V, § 1).

Лемма 4.1. *Если $\mathfrak{p}$ — простой идеал кольца R, то кольцо $SR_{\mathfrak{p}}$ является целым замыканием кольца $R_{\mathfrak{p}}$ в поле L.*

Доказательство. Очевидно, что элементы кольца $SR_{\mathfrak{p}}$ являются целыми над $R_{\mathfrak{p}}$. Обратно, для каждого целого над $R_{\mathfrak{p}}$ элемента x, т. е. такого элемента, что

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

где $a_i \in R$, $b \in R$, $b \notin \mathfrak{p}$, имеет место $bx \in S$. Следовательно, $x \in SR_{\mathfrak{p}}$.

Мы говорим, что *простой идеал* $\mathfrak{P}$ *кольца* S *лежит над простым идеалом* $\mathfrak{p}$ *кольца* R, если

$$\mathfrak{P} \cap R = \mathfrak{p}.$$

В этом случае мы будем писать $\mathfrak{P} | \mathfrak{p}$.

Предложение 4.1. *Кольцо* S *как* R*-модуль является конечно порожденным; оно порождает векторное пространство* L *над полем* K *и представляет собой дедекиндову область.*

Каждый ненулевой простой идеал $\mathfrak{P}$ *кольца* S *лежит над некоторым простым ненулевым идеалом кольца* R; *обратно, над каждым ненулевым простым идеалом* $\mathfrak{p}$ *кольца* R *лежит некоторый простой идеал кольца* S.

Доказательство. Применяя лемму 4.1 для $\mathfrak{p} = (0)$, мы получаем, что модуль S порождает пространство L/K.

След $\mathrm{tr}_{L/K} : L \to K$ определяет некоторую невырожденную K-билинейную форму

$$B(u, v) = tr_{L/K}(uv)$$

на пространстве L [1]). Так как $SK = L$, то модуль S содержит свободный R-подмодуль N, порождающий пространство L. Но тогда мы можем утверждать (используя обозначения § 3), что $D(N)$ — свободный модуль, порождающий пространство L. Кроме того,

$$D(N) \supset D(S).$$

Следы целых элементов лежат в кольце R, и потому

$$D(S) \supset S,$$

т. е.

$$D(N) \supset S.$$

Итак, S — конечно порожденный R-модуль. Отсюда следует, что он нётеров и, как уже отмечалось, кольцо S целозамкнуто.

[1]) Здесь используется сепарабельность расширения L/K. — *Прим. перев.*

Пусть $\mathfrak{P}$ — простой ненулевой идеал кольца S, и пусть

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

есть минимальное уравнение для ненулевого элемента b из идеала $\mathfrak{P}$. Тогда $a_i \in R$ при всех i и, следовательно, $a_0 \in \mathfrak{p} = \mathfrak{P} \cap R$. Таким образом, идеал $\mathfrak{p}$ — ненулевой. Кроме того, $\mathfrak{P} \supset \mathfrak{p}S$, т. е. $\mathfrak{P}/\mathfrak{p}S$ является простым идеалом [коммутативной алгебры $S/\mathfrak{p}S$ над полем $R/\mathfrak{p}$. Поскольку модуль S конечно порожден над кольцом R, кольцо $S/\mathfrak{p}S$ является конечномерной алгеброй и то же самое верно для $(S/\mathfrak{p}S)/(\mathfrak{P}/\mathfrak{p}S) = S/\mathfrak{P}$. Отсюда следует, что $S/\mathfrak{P}$ — поле, т. е. $\mathfrak{P}$ — максимальный идеал. Мы показали, что кольцо S — дедекиндова область.

Пусть $\mathfrak{p}$ — ненулевой простой идеал кольца R. Из равенства $\mathfrak{p}S = S$ получалось бы, что $\mathfrak{p}^{-1}S = \mathfrak{p}^{-1}(\mathfrak{p}S) = S$, т. е. $\mathfrak{p}^{-1} \subset S \cap K = R$, что неверно. Если же простой идеал $\mathfrak{P}$ кольца S является делителем идеала $\mathfrak{p}S$, то $\mathfrak{P} \cap R \supset \mathfrak{p}$, т. е. $\mathfrak{P} \cap R = \mathfrak{p}$.

Следствие 1. (Используется в гл. II.) *Каждое дискретное (мультипликативное) нормирование поля* K *может быть продолжено на конечное сепарабельное расширение* L *поля* K.

Доказательство. Пусть R — кольцо нормирования поля K. Утверждению следствия 1 удовлетворяет подходящим образом нормализованное нормирование поля L вида $\rho^{v_{\mathfrak{P}}(x)}$.

Следствие 2. *Отображение* $I \mapsto IS$ *является инъективным гомоморфизмом групп* $\mathcal{F}(R) \to \mathcal{F}(S)$.

Доказательство получается из предложения 4.1 с помощью того соображения, что если I_1, I_2 — два целых идеала кольца R, таких, что $I_1 + I_2 = R$, то $I_1S + I_2S = S$.

Комбинируя предложение 4.1 с теоремами из гл. II о единственности продолжения нормирований полных полей (см. § 10), мы получаем

Предложение 4.2. *Если кольцо* R *— дискретно нормировано, а поле* K *полно, то и кольцо* S *дискретно нормировано, а поле* L *полно.*

В оставшейся части этого параграфа и первой части следующего мы будем изучать понятия, связанные с вложением кольца R в кольцо S. Всякий раз нашей целью будет получение редукции к полному локальному случаю.

Дробный идеал J кольца S конечно порожден над кольцом S, а потому и над кольцом R. Кроме того, если $0 \neq a \in J$, то $J \supset aS$; следовательно, модуль J порождает векторное пространство L над K. Мы можем теперь определить *норму идеала* $N_{L/K}(J)$ равенством

$$N_{L/K}(J) = (S : J)_R. \tag{1}$$

Связь этого понятия с понятием нормы элемента устанавливает

Предложение 4.3. *Если* $a \in L^*$, *то*

$$N_{L/K}(aS) = N_{L/K}(a)\, R.$$

Доказательство. Элемент $N_{L/K}(a)$ является определителем линейного преобразования $x \mapsto ax$ векторного пространства L.

Заметим, что если $R = \mathbf{Z}$ и J — некоторый идеал кольца S, то норма $N_{L/K}(J)$ в точности равна числу классов вычетов кольца S, рассматриваемому как $\mathbf{Z}$-идеал по модулю J. Это следует из нашего замечания (см. § 3) об интерпретации индекса модуля как группового индекса в случае $R = \mathbf{Z}$.

Норма идеала коммутирует в уточняемом ниже смысле с изоморфизмом, который установлен в следствии 4 из предложения 2.2. Сформулируем сначала теорему, доказываемую в гл. II (см. § 10).

Пусть R — дискретно нормированное кольцо, $\mathfrak{p}$ — его максимальный идеал и $\overline{K}$ — пополнение поля K относительно нормирования $v_{\mathfrak{p}}$. Пусть $\mathfrak{P}_i$ пробегает множество ненулевых простых идеалов кольца S; обозначим через $\overline{L}_i$ соответствующие пополнения. Тогда имеет место равенство (понимаемое как равенство алгебр над полем $\overline{K}$ и топологических пространств)

$$L \otimes_K \overline{K} = \sum \overline{L}_i \tag{2}$$

(в правой части взята прямая сумма полей). Рассмотрим L, $\overline{L}_i$, $\overline{K}$ как подалгебры этой суммы. Обозначим через $\overline{R}$ кольцо нормирования поля $\overline{K}$, через $\overline{S}_i$ — кольцо нормирования поля $\overline{L}_i$. Тогда справедлива следующая

Лемма 4.2. $\overline{R}S = \sum \overline{S}_i$.

Доказательство. Алгебра $\sum \overline{S}_i$ является целым замыканием кольца $\overline{R}$ в алгебре $\sum \overline{L}_i$. Следовательно, $\overline{R}S \subset \sum \overline{S}_i$. Кольцо $\overline{R}S$ полно, а потому замкнуто. Таким образом, достаточно показать, что кольцо S всюду плотно в кольце $\sum \overline{S}_i$. Так как мы не формулировали и не доказывали основную аппроксимационную теорему, из которой легко следует этот результат, то мы дадим несколько искусственное доказательство.

Известно (см. гл. II), что поле L всюду плотно в алгебре $\sum \overline{L}_i$, так что $\sum \overline{S}_i$ является замыканием модуля $(\sum \overline{S}_i) \cap L$. Мы покажем, что этот модуль содержится в кольце S. Минимальный многочлен любого элемента $x \in (\sum \overline{S}_i) \cap L$ над полем $\overline{K}$ имеет коэффициенты в кольце $\overline{R}$. Но поскольку он совпадает с минимальным многочленом над полем K, его коэффициенты лежат в $K \cap \overline{R} = R$. Таким образом, $x \in S$.

Вернемся теперь к случаю произвольной дедекиндовой области R. Если $\mathfrak{p}$ — ненулевой простой идеал кольца R, то через $K_{\mathfrak{p}}$ будем обозначать соответствующее пополнение поля K и через $\overline{R}_{\mathfrak{p}}$ — кольцо его нормирования. Для каждого ненулевого простого идеала $\mathfrak{P}$ кольца S соответствующие объекты обозначаются через $L_{\mathfrak{P}}$ и $\overline{S}_{\mathfrak{P}}$.

Предложение 4.4. *Если* J — *дробный идеал кольца* S, *то*

$$N_{L/K}(J)\, \overline{R}_{\mathfrak{p}} = \prod_{\mathfrak{P} \mid \mathfrak{p}} N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(J \overline{S}_{\mathfrak{P}}).$$

Доказательство. Принимая во внимание определение индекса модуля и лемму 4.1, мы можем предположить, что $R = R_{\mathfrak{p}}$ является дискретно нормированным кольцом. Тогда предложение следует из леммы 4.2 и предложений 3.5 и 3.6.

Следствие 1. *Норма $N_{L/K}$ задает гомоморфизм групп $\mathcal{J}(S) \to \mathcal{J}(R)$.*

Доказательство. На основании следствия 4 из предложения 2.2 и только что доказанного предложения 4.4 доказательство сводится к случаю, когда R — дискретно нормированное кольцо и K — полное поле. Но в этом случае каждый дробный идеал кольца S является главным, и утверждение вытекает из предложения 4.3 и мультипликативности норменного отображения на множестве элементов поля.

Аналогичными рассуждениями устанавливаются еще два следствия.

Следствие 2. *Для всех $I \in \mathcal{J}(R)$ имеет место равенство*

$$N_{L/K}(IS) = I^n,$$

где $n = [L : K]$ — степень расширения.

Следствие 3. *Если $L \supset F \supset K$, то*

$$N_{L/K}(J) = N_{F/K}(N_{L/F}(J)).$$

Мы можем теперь вернуться к билинейной форме, которая задается следом. Модуль $D_R(S)$, двойственный к модулю S, является, очевидно, S-модулем. Согласно предложениям 4.1 и 3.3, он конечно порожден над кольцом R, а потому и над кольцом S. Так как $D_R(S) \supset S$, то

$$D_R(S) = \mathfrak{D}^{-1}, \tag{3}$$

где $\mathfrak{D} = \mathfrak{D}(S/R)$ — некоторый целый идеал кольца S, называемый *дифферентой*.

Дискриминант, определенный в § 3 равенством (4), мы будем записывать так:

$$\mathfrak{d} = \mathfrak{d}(S/R).$$

Так как $D_R(S) \supset S$, то $\mathfrak{d}$ является целым идеалом кольца R. Более того,

$$\mathfrak{d} = N_{L/K}(\mathfrak{D}). \tag{4}$$

Действительно,

$$\mathfrak{d} = (D_R(S) : S) = (S : D_R(S))^{-1} =$$
$$= N_{L/K}(\mathfrak{D}^{-1})^{-1} = N_{L/K}(\mathfrak{D}).$$

Предложение 4.5. *В обозначениях предложения 4.4 имеет место*

(i) $\mathfrak{D}(S/R)\,\bar{S}_{\mathfrak{P}} = \mathfrak{D}(\bar{S}_{\mathfrak{P}}/\bar{R}_{\mathfrak{p}})$;

(ii) $\mathfrak{d}(S/R)\,\bar{R}_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{d}(\bar{S}_{\mathfrak{P}}/\bar{R}_{\mathfrak{p}})$.

Доказательство получается применением леммы 4.2 и предложений 3.4, 3.5, 3.6.

Следующее предложение устанавливает связь между дискриминантом $\mathfrak{d}(S/R)$ и дискриминантами целых элементов, порождающих расширение L. Эта связь устанавливается обычно с помощью теории «нётерова кондуктора» кольца; однако понятие индекса модуля позволит нам обойтись без нее.

Пусть x — некоторый элемент кольца S, такой, что $L = K[x]$; пусть $g(X)$ — минимальный многочлен элемента x над полем K. Кольцо $R[x]$ порождает тогда пространство L и является свободным R-модулем, натянутым, как на образующие, на $1, x, \ldots, x^{n-1}$. В следующем предложении через $g'(X)$ обозначается производная многочлена $g(X)$.

Предложение 4.6.

(i) $D(R[x]) = \frac{1}{g'(x)} R[x]$;

(ii) $\mathfrak{d}(R[x]) = (N_{L/K} g'(x))\,R$;

(iii) *равенство $R[x] = S$ имеет место тогда и только тогда, когда $\mathfrak{D}(S/R) = g'(x)\,S$.*

Доказательство. Согласно формуле Эйлера, мы имеем, что

$$\mathrm{tr}_{L/K}(x^i/g'(x)) \in R \qquad \text{при} \qquad i = 0, \ldots, n-1.$$

Следовательно,

$$D(R[x]) \supset \frac{1}{g'(x)} R[x]. \tag{5}$$

В силу предложения 3.4

$$\mathfrak{d}(R[x]) = \det \mathrm{tr}_{L/K}(x^{i+j})\,R.$$

Однако (см. любой учебник по алгебре)

$$\det \mathrm{tr}_{L/K}(x^{i+j}) = \pm N_{L/K}(g'(x)),$$

и, таким образом,

$$(D(R[x]) : R[x]) = N_{L/K}(g'(x))\, R = \left(\frac{1}{g'(x)} R[x] : R[x]\right).$$

Следовательно, согласно (5),

$$D(R[x]) = \frac{1}{g'(x)} R[x].$$

Мы установили справедливость утверждений (i) и (ii). Необходимость в утверждении (iii) тривиальна, и остается только доказать достаточность.

Предположим, что $\mathfrak{D}(S/R) = g'(x)\, S$; тогда

$$D(R[x]) \supset D(S) = \frac{1}{g'(x)} S \supset \frac{1}{g'(x)} R[x] = D(R[x]).$$

Теперь вновь рассмотрим двойственные модули и, применяя предложение 3.3, получим равенство $S = R[x]$.

Докажем, наконец, «*формулу башен*».

Предложение 4.7. *Если $L \supset F \supset K$ и T — целое замыкание кольца R в поле F, то*

(i) $\mathfrak{D}(S/R) = \mathfrak{D}(S/T) \cdot \mathfrak{D}(T/R)$;

(ii) $\mathfrak{d}(S/R) = \mathfrak{d}(T/R)^m \cdot (N_{F/K}\mathfrak{d}(S/T))$,

где $m = [L : F]$.

Доказательство. Покажем, что

$$\mathfrak{D}(S/R)^{-1} = \mathfrak{D}(S/T)^{-1} \cdot \mathfrak{D}(T/R)^{-1}.$$

Тогда (ii) будет вытекать из формулы (4) и следствий из предложения 4.4.

Благодаря транзитивности следа мы имеем, что

$$\mathrm{tr}_{L/K}(Sx) = \mathrm{tr}_{F/K}[\mathrm{tr}_{L/F}(Sx)\, T].$$

Следовательно, полагая $\mathfrak{D}_0 = \mathfrak{D}(T/R)$, мы получаем

$$\begin{aligned} \mathrm{tr}_{L/K}(Sx) \subset R &\Leftrightarrow \mathrm{tr}_{L/F}(Sx) \subset \mathfrak{D}_0^{-1} \Leftrightarrow \\ &\Leftrightarrow \mathrm{tr}_{L/K}(Sx\mathfrak{D}_0) \subset T \Leftrightarrow \\ &\Leftrightarrow x\mathfrak{D}_0 \subset \mathfrak{D}(S/T)^{-1} \Leftrightarrow \\ &\Leftrightarrow x \in \mathfrak{D}_0^{-1}\mathfrak{D}(S/T)^{-1}. \end{aligned}$$

§ 5. ВЕТВЛЕНИЕ

Рассмотрим сначала две дедекиндовы области R_1 и R_2, связанные включением $R_1 \subset R_2$, с полями частных K_1 и K_2. Пусть $\mathfrak{p}_2$ — ненулевой простой идеал кольца R_2, и пусть простой идеал

$$\mathfrak{p}_1 = \mathfrak{p}_2 \cap R_1$$

также ненулевой. В этом случае поле классов вычетов $k_1 = R_1/\mathfrak{p}_1$ естественным образом вкладывается в поле классов вычетов $k_2 = R_2/\mathfrak{p}_2$. Степень

$$(k_2 : k_1) = f(\mathfrak{p}_2/\mathfrak{p}_1) \tag{1}$$

называется *степенью классов вычетов* (может случиться, что $f = \infty$). *Индекс ветвления* $e(\mathfrak{p}_2/\mathfrak{p}_1)$ определяется равенством

$$v_{\mathfrak{p}_2}(\mathfrak{p}_1 R_2) = e(\mathfrak{p}_2/\mathfrak{p}_1), \tag{2}$$

т. е.

$$\begin{aligned} &\text{ограничение нормирования } v_{\mathfrak{p}_2} \\ &\text{на группу } K^* \text{ равно } e(\mathfrak{p}_2/\mathfrak{p}_1)\, v_{\mathfrak{p}_1}. \end{aligned} \tag{3}$$

Имеет место

Предложение 5.1.

$$f(\mathfrak{p}_3/\mathfrak{p}_2) \cdot f(\mathfrak{p}_2/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_1);$$
$$e(\mathfrak{p}_3/\mathfrak{p}_2) \cdot e(\mathfrak{p}_2/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_1).$$

Доказательство очевидно.

Предложение 5.2. *Пусть $\overline{\mathfrak{p}}$ — идеал нормирования в пополнении поля $K = K_i$ относительно нормирования $v_{\mathfrak{p}} = v_{\mathfrak{p}_i}$. Тогда*

$$f(\overline{\mathfrak{p}}/\mathfrak{p}) = e(\overline{\mathfrak{p}}/\mathfrak{p}) = 1.$$

Доказательство. Пусть $R_{\mathfrak{p}}$ — кольцо нормирования $v_{\mathfrak{p}}$ в поле K. Согласно предложению 2.2, имеет место $e(\mathfrak{p}R_{\mathfrak{p}}/\mathfrak{p}) = 1$, а в силу предложения 1.1 можно заключить, что $e(\overline{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}) = 1$. Из предложения 5.1 тогда следует, что $e(\overline{\mathfrak{p}}/\mathfrak{p}) = 1$.

Каждый элемент из факторкольца $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ имеет вид xy^{-1}, где $x,\ y \in R/\mathfrak{p}$. Следовательно, поля $R_\mathfrak{p}$ и $\mathfrak{p}R_\mathfrak{p}$ совпадают, т. е. $f(\mathfrak{p}R_\mathfrak{p}/\overline{\mathfrak{p}}) = 1$. Кроме того, кольцо $R_\mathfrak{p}$ плотно в кольце нормирования $\overline{R}_\mathfrak{p}$ соответствующего пополнения. Следовательно, образ поля $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ плотен в дискретной группе $\overline{R}_\mathfrak{p}/\overline{\mathfrak{p}}$, т. е. $f(\overline{\mathfrak{p}}/\mathfrak{p}R_\mathfrak{p}) = 1$. Отсюда $f(\overline{\mathfrak{p}}/\mathfrak{p}) = 1$.

Следствие.

$$f(\mathfrak{p}_2/\mathfrak{p}_1) = f(\overline{\mathfrak{p}}_2/\overline{\mathfrak{p}}_1);$$
$$e(\mathfrak{p}_2/\mathfrak{p}_1) = e(\overline{\mathfrak{p}}_2/\overline{\mathfrak{p}}_1).$$

Результаты § 4 вместе с последним следствием показывают, что дифференты, дискриминанты, степени классов вычетов, индексы ветвления и нормы идеалов расширения L/K могут быть описаны локально в терминах пополнений. Начиная с этого места и до конца § 10, мы будем предполагать, что кольцо R является дискретно нормированным, а поле K — полным относительно топологии нормирования. Эта ситуация сохраняется при переходе к конечным сепарабельным расширениям (см. предложение 4.2). Видоизменение результатов применительно к глобальному случаю будет чаще всего оставляться читателю.

Мы сейчас несколько изменим обозначения, которые были введены в § 4, и для «относительных» объектов будем использовать символы $\mathfrak{D}(L/K)$, $\mathfrak{d}(L/K)$, $f(L/K)$, $e(L/K)$. Через v_L будет обозначаться нормирование поля L, а через k_L — поле вычетов. Вместо k_K мы будем просто писать k. Через $\mathfrak{p}$ в дальнейшем обозначается максимальный идеал кольца R, а через $\mathfrak{P}$ — максимальный идеал целого замыкания S кольца R в поле L.

Все наши результаты, за исключением § 9, будут установлены без предположения о том, что расширения полей вычетов сепарабельны.

Предложение 5.3.

$$e(L/K)\, f(L/K) = [L : K].$$

Доказательство. Векторное пространство $S/\mathfrak{p}S$ над полем k имеет следующий ряд факторпространств:

$$S/\mathfrak{P},\quad \mathfrak{P}/\mathfrak{P}^2,\ \ldots,\ \mathfrak{P}^{e-1}/\mathfrak{P}^e \quad (\mathfrak{P}^e = \mathfrak{p}S);$$

все они, согласно лемме 1.4, изоморфны. Так как размерность пространства $S/\mathfrak{P}$ над полем k равна $f = f(L/K)$, размерность $S/\mathfrak{p}S$ равна ef. С другой стороны, так как S является свободным R-модулем ранга $[L : K]$, размерность пространства $S/\mathfrak{p}S$ равна $[L : K]$.

Пусть U_K и U_L — группы единиц колец R и S соответственно. Мы уже знаем, что вложение $j\colon K^* \to L^*$ задает коммутативную диаграмму (с точными строками, см. § 1, (5))

$$\begin{array}{ccccccccc} 0 & \to & U_K & \to & K^* & \xrightarrow{v_K} & \mathbf{Z} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow e & & \\ 0 & \to & U_L & \to & L^* & \xrightarrow{v_L} & \mathbf{Z} & \to & 0. \end{array}$$

Теперь в дополнение к этому мы получаем

Следствие. *Норменное отображение на элементах определяет коммутативную диаграмму*

$$\begin{array}{ccccccccc} 0 & \to & U_L & \to & L^* & \to & \mathbf{Z} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow f & & \\ 0 & \to & U_K & \to & K^* & \to & \mathbf{Z} & \to & 0, \end{array}$$

т. е.

$$f v_L(x) = v_K(N_{L/K}(x))$$

и

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f.$$

Доказательство. Имеет место

$$N_{L/K}(U_L) \subset U_K \quad \text{и} \quad N_{L/K} \cdot j = [L : K].$$

Несколько фактов об операторе следа. Пусть A — конечномерная коммутативная алгебра над полем k со следующими свойствами: (i) если N — радикал этой алгебры, то $A/N = B$ — поле; (ii) $N^e = 0$, $N^{e-1} \neq 0$ и при $i < e$ имеет место изоморфизм B-модулей: $B \cong N^i/N^{i+1}$. Обозначим через $\tilde{a}$ образ элемента $a \in A$ в поле B. Тогда выполняется следующая

Лемма 5.1. $\mathrm{tr}_{A/k}(a) = e\,\mathrm{tr}_{B/k}(\bar{a})$.

Доказательство (мы даем лишь набросок). Элемент $\mathrm{tr}_{A/k}(a)$ является следом линейного преобразования $x \mapsto xa$ пространства A над полем k. Пусть $B = B_0 = A/N, \ldots, B_i = N^i/N^{i+1}, \ldots$ — ряд фактормодулей A-модуля A, и пусть a_i — линейное преобразование модуля B_i, индуцированное элементом a. Тогда

$$\mathrm{tr}_{A/k}(a) = \sum_i \text{след}\ (a_i).$$

Но вследствие изоморфизма A-модулей B_i

$$\text{след}\,(a_i) = \text{след}\,(a_0) = \mathrm{tr}_{B/k}(\bar{a}).$$

Отсюда вытекает утверждение леммы.

Будем теперь обозначать отображение классов вычетов $S \to S/\mathfrak{P}$ через $a \mapsto \bar{a}$.

Лемма 5.2. $\overline{\mathrm{tr}_{L/K}(a)} = e\,\mathrm{tr}_{k_L/k}(\bar{a})$.

Доказательство. Лемма следует из леммы 5.1 при $A = S/\mathfrak{p}S$, $N = \mathfrak{P}/\mathfrak{p}S$.

Замечание. Аналогичным способом можно показать, что

$$\overline{N_{L/K}(a)} = N_{k_L/k}(\bar{a})^e. \tag{4}$$

Предложение 5.4. $v_L(\mathfrak{D}) \geqslant e - 1$.

Доказательство. Пусть по-прежнему $A = S/\mathfrak{p}S$, $N = \mathfrak{P}/\mathfrak{p}S$, и пусть $\tilde{x}$ — образ в модуле A элемента $x \in S$. Выберем такой k-базис $\{a_i\}$ алгебры A, что при $1 \leqslant i < (e-1)f$ элементы a_i образуют k-базис в N. Мы можем поднять $\{a_i\}$ до некоторого R-базиса $\{x_i\}$ алгебры S так, что $\tilde{x}_i = a_i$. Для $1 \leqslant i \leqslant (e-1)f$ и всех j элементы $\tilde{x}_i\,\tilde{x}_j$ будут лежать в модуле N, т. е. $\overline{x_i x_j} = 0$, откуда в силу леммы 5.2

$$\mathrm{tr}_{L/K}(x_i x_j) \in \mathfrak{p}.$$

Следовательно, каждая из $(e-1)f$ первых строк матрицы

$$(\mathrm{tr}_{L/K}(x_i x_j))$$

лежит в идеале $\mathfrak{p}$, и потому в силу предложения 3.4

$$v_K(\mathfrak{d}) \geqslant (e-1)f,$$

т. е.

$$v_L(\mathfrak{D}) = \frac{1}{f} v_K(N_{L/K}(\mathfrak{D})) = \frac{1}{f} v_K(\mathfrak{d}) \geqslant e - 1.$$

Будем называть расширение L *неразветвленным* над полем K, если

(i) $e(L/K) = 1$;

(ii) расширение k_L сепарабельно над k.

Теорема 5.1. *Расширение L является неразветвленным над K тогда и только тогда, когда $\mathfrak{d}(L/K) = R$.*

Доказательство. В силу предложения 5.4 равенство $\mathfrak{d} = R$ или, что равносильно, равенство $\mathfrak{D} = S$ влечет за собой равенство $e = 1$. Предположим теперь, что $e = 1$. Пусть $\{x_i\}$ — множество свободных образующих модуля S над кольцом R, и пусть

$$d = \det[\mathrm{tr}_{L/K}(x_i x_j)].$$

Согласно предложению 3.4, равенство $\mathfrak{d} = R$ имеет место тогда и только тогда, когда класс вычетов $\bar{d}$ отличен от нулевого. По лемме 5.2 элемент

$$\bar{d} = \det[\mathrm{tr}_{k_L/k}(\bar{x}_i \bar{x}_j)]$$

является дискриминантом базиса $\{\bar{x}_i\}$ расширения k_L над полем k, а последний отличен от нуля в том и только том случае, если расширение k_L сепарабельно над k.

Пусть в дальнейшем χ означает характеристику поля k. Расширение L называется *слабо разветвленным* над полем K, если

(i) $\chi \nmid e(L/K)$;

(ii) расширение k_L сепарабельно над k.

В частности, если $\chi = 0$, расширение L/K всегда слабо разветвлено.

Теорема 5.2. *Следующие условия эквивалентны:*

(i) *расширение L слабо разветвлено над K;*

(ii) $\mathrm{tr}_{L/K}(S) = R$;

(iii) $v_L(\mathfrak{D}) = e - 1$.

Замечание. Множество $\mathrm{tr}_{L\,K}(S)$ всегда является ненулевым идеалом в кольце R.

Доказательство. Эквивалентность условий (i) и (ii) немедленно следует из леммы 5.2.

Для доказательства эквивалентности условий (ii) и (iii) заметим сначала, что если $a \in K$, то

$$\mathrm{tr}_{L/K}(Sa) = \mathrm{tr}_{L/K}(S)\cdot a.$$

Следовательно,

$$\mathrm{tr}_{L/K}(S)^{-1} = \mathfrak{D}^{-1} \cap K,$$

или, полагая $v = v_L(\mathfrak{D})$, $r = v_K(\mathrm{tr}_{L/K}(S))$,

$$r \leqslant \frac{v}{e} < r+1.$$

Таким образом, если $v = e - 1$, то $r = 0$. Если $r = 0$, то $v < e$ и в силу предложения 5.4 $v = e - 1$.

Замечание. Если расширение L нормально над K, то из условия (ii) только что доказанной теоремы можно вывести еще один критерий. Для этой цели обозначим через $R(\Gamma)$ групповое кольцо над кольцом R группы Галуа Γ. Тогда имеет место следующее утверждение.

Теорема о нормальном базисе. *Модуль S над кольцом R [Γ] изоморфен модулю R [Γ] тогда и только тогда, когда расширение L слабо разветвлено над K* (см. [2]).

Доказательство оставляется читателю в качестве упражнения. Укажем, впрочем, на следующее обстоятельство: результат следует из интерпретации существования элемента со следом, равным 1, в терминах кольца эндоморфизмов, поскольку отсюда получается, что расширение L/K слабо разветвлено в том и только том случае, когда модуль S проективен; после этого надо воспользоваться теоремой Суона (см. [4], следствие 6.4).

Приложение к глобальному случаю.

Сформулируем в явном виде теорему 5.1 в терминах произвольной дедекиндовой области. Пусть (временно) R — произвольная дедекиндова область, не обязательно дискретно нормированная, K — ее поле частных, S — целое замыкание кольца R в конечном сепарабельном расширении L/K. Ненулевой простой идеал $\mathfrak{P}$ кольца S считается неразветвленным над полем K, если его индекс ветвления над идеалом $\mathfrak{P} \cap R$ равен 1 и $S/\mathfrak{P}$ сепарабельно над $R/\mathfrak{P} \cap R$. Ненулевой простой идеал $\mathfrak{p}$ кольца R считается неразветвленным в расширении L, если все простые идеалы $\mathfrak{P}$ кольца S, лежащие над $\mathfrak{p}$, не разветвлены над K.

Следствие 1 из теоремы 5.1. *Идеал $\mathfrak{p}$ является неразветвленным в расширении L в том и только том случае, когда он не делит дискриминант $\mathfrak{d}$ расширения S/R.*

Доказательство. С одной стороны, мы знаем (см. предложение 5.2), что как индекс ветвления, так и расширение поля вычетов не меняются при переходе к пополнениям. Таким образом, идеал $\mathfrak{p}$ не разветвлен в L тогда и только тогда, когда пополнения $L_{\mathfrak{P}}$ по всем $\mathfrak{P}$, лежащим над $\mathfrak{p}$, являются неразветвленными над пополнением $K_{\mathfrak{p}}$ поля K.

С другой стороны, из предложения 4.5 и следствия 4 из предложения 2.2 вытекает, что идеал $\mathfrak{p}$ не делит дискриминант $\mathfrak{d}$ тогда и только тогда, когда произведение локальных дискриминантов тривиально. Ввиду того что каждый сомножитель является целым идеалом, сказанное эквивалентно тривиальности каждого из локальных дискриминантов.

Теперь применим теорему 5.1.

(Заменяя дискриминант на дифференту, можно получить более сильный критерий, относящийся к неразветвленности отдельно взятого идеала $\mathfrak{P}$.)

Следствие 2 из теоремы 5.1. *Почти все ненулевые простые идеалы кольца R являются неразветвленными в расширении S.*

Доказательство. Не разветвлены все те идеалы, которые не делят дискриминант.

§ 6. ВПОЛНЕ РАЗВЕТВЛЕННЫЕ РАСШИРЕНИЯ

Обозначения этого параграфа, а также § 7—9 такие же, как в § 5. Кольцо R всегда считается дискретно нормированным, K обозначает поле частных кольца R, а L — конечное сепарабельное расширение поля K.

Многочлен $g(X) \in K[X]$ называется *сепарабельным*, если $(g(X), g'(X)) = 1$. *Многочленом Эйзенштейна* называется такой сепарабельный многочлен

$$E(X) = X^m + b_{m-1}X^{m-1} + \ldots + b_1X + b_0 \qquad (1)$$

из $K[X]$, что

$$v_K(b_i) \geqslant 1 \quad \text{при} \quad i = 1, \ldots, m-1 \text{ и } v_K(b_0) = 1. \qquad (2)$$

(Условия о сепарабельности как расширения L, так и многочлена $E(X)$ не являются необходимыми для дальнейших теорем. Но ввиду того что рассматриваются лишь сепарабельные расширения полей, мы должны наложить соответствующее ограничение и на многочлен $E(X)$.)

Расширение L называется *вполне разветвленным* над полем K, если $e(L/K) = [L : K]$, т. е. $f(L/K) = 1$.

Теорема 6.1. (i) *Многочлен Эйзенштейна неприводим. Если* Π *— корень многочлена Эйзенштейна* $E(X)$, *то расширение* $L = K[\Pi]$ *вполне разветвлено и* $v_L(\Pi) = 1$;

(ii) *если расширение* L/K *вполне разветвлено и* $v_L(\Pi) = 1$, *то минимальный многочлен элемента* Π *над полем* K *является многочленом Эйзенштейна и*

$$S = R(\Pi), \quad L = K[\Pi].$$

Для доказательства нам понадобится предложение о представлении элементов полного поля сходящимися рядами. Если при всех $n \in \mathbf{Z}$ имеет место $v(\Pi_n) = n$, $v(a_n) \geqslant \rho$ (ρ — константа), то ряд

$$\sum_{n \gg -\infty}^{\infty} a_n \Pi_n$$

($n \gg -\infty$ означает, что $a_n = 0$ для всех n, достаточно близких к $-\infty$) сходится и, таким образом, имеет сумму в поле K. Предположим теперь, что нам заданы отображения $\Pi\colon \mathbf{Z} \to K^*$, $r : k \to R$, такие, что $r(0) = 0$, и отображения

$$\mathbf{Z} \xrightarrow{\Pi} K^* \xrightarrow{v} \mathbf{Z},$$

$$k \xrightarrow{r} R \xrightarrow{\text{переход к классам вычетов}} k$$

являются тождественными отображениями. Обозначим через Π_n образ числа n при отображении Π и положим $\mathfrak{R} = \operatorname{Im} r$. Тогда имеет место

Предложение 6.1. *Каждый элемент поля* K *однозначно представляется в виде*

$$a = \sum_{n \gg -\infty}^{\infty} a_n \Pi_n, \quad a_n \in \mathfrak{R}.$$

Значение нормирования на элементе a *определяется равенством*

$$v(a) = \inf_{a_n \neq 0} n.$$

Доказательство проводится стандартным образом.

Доказательство теоремы 6.1. Сначала предположим, что многочлен $E(X)$ в равенстве (1) является многочленом Эйзенштейна и что $L = K[\Pi]$, где $E(\Pi) = 0$. Положим $n = (L : K)$, $e = e(L/K)$.

Ясно, что $v_L(\Pi) \geqslant 0$; поэтому

$$v_L(\Pi^m) = v_L(b_{m-1}\Pi^{m-1} + \ldots + b_0) \geqslant 1,$$

т. е. $v_L(\Pi) \geqslant 1$ Пусть s — такое целое число, что

$$s \geqslant \frac{e}{v_L(\Pi)} > s - 1.$$

Тогда

$$m \geqslant n \geqslant e \geqslant s. \qquad (3)$$

Если $m > s$, то $v_L(\Pi^m) > e$. Кроме того,

$$v_L(b_i)\, e v_K(b_i) \geqslant e,$$

и, таким образом,

$$v_L(b_{m-1}\Pi^{m-1} + \ldots + b_1\Pi) > e.$$

Отсюда $v_L(b_0) > e$, т. е. $v_K(b_0) > 1$, что противоречит (2). Мы показали, что $m \leqslant s$, а значит, в силу (3)

$$m = n = e = s.$$

Поэтому

$$v_L(\Pi) = 1.$$

Все утверждения из (i) теперь установлены.

Для доказательства (ii) применим предложение 6.1 к расширению L. Поскольку $f(L/K) = 1$, мы можем сделать так, чтобы $\mathfrak{R}$ принадлежало полю K. Выбрав такой элемент $c \in K$, что $v_K(c) = 1$, положим

$$\Pi_{qe+r} = c^q \Pi^r \qquad (q \in \mathbf{Z},\ 0 \leqslant r < e).$$

Перестановка слагаемых в сумме $\sum a_n \Pi_n$ показывает, что на самом деле $L = K[\Pi]$ и $S = R[\Pi]$.

Пусть теперь многочлен $E(X)$ в равенстве (1) является минимальным многочленом элемента Π над полем K. Тогда он будет и характеристическим многочленом. Поэтому, во-первых, $b_0 = \pm N_{L/K}(\Pi)$, и в силу следствия 1 из предложения 5.3

$$v_K(b_0) = v_L(\Pi) = 1.$$

Во-вторых, многочлен $E(X)$, редуцированный по mod $\mathfrak{p}$, является характеристическим многочленом нильпотентного элемента $\Pi \bmod \mathfrak{p}S$ алгебры $S/\mathfrak{p}S$ над полем k. Следовательно, $E \equiv X^m \pmod{\mathfrak{p}}$, т. е. $v_K(b_i) > 0$ при всех i.

Следствие. *Поле K обладает вполне разветвленным расширением любой степени e.*

Доказательство. Если $v_K(c) = 1$, то можно положить

$$E(X) = X^e - cX - c.$$

Целесообразно указать на некоторые результаты, которые вытекают из предложения 6.1, но не будут доказаны в этом курсе (см. [3], гл. II).

Если K — поле формальных степенных рядов $\sum_{n \gg -\infty} a_n t^n$ над полем F (см. пример из § 1), то можно, очевидно, считать, что $\Pi_n = t^n$ и $\mathfrak{R} = F$ (т. е. $F \cong k$). В этом случае характеристики полей k и K совпадают. Обратно, если имеет место указанная ситуация, то поле K является (с точностью до изоморфизма) полем формальных степенных рядов над полем k.

Остается случай, когда $\chi = p \neq 0$, но характеристика поля K равна нулю (типичный пример — поле рациональных p-адических чисел $\mathbf{Q}_p$). Если к тому же предположить, что поле k совершенно (например, конечно), то можно

выбрать $\mathfrak{R}$ мультипликативно замкнутым и притом только одним способом. Можно показать, что если k совершенно и имеет характеристику $p \neq 0$, то существует одно и (с точностью до изоморфизма) только одно дискретно нормированное полное поле K характеристики 0, которое имеет поле k своим полем вычетов и для которого $v_K(p) = 1$.

§ 7. НЕРАЗВЕТВЛЕННЫЕ РАСШИРЕНИЯ

Сепарабельное расширение L поля K индуцирует некоторое алгебраическое расширение поля вычетов k. Если L не разветвлено над K, то соответствующее расширение поля классов вычетов сепарабельно. Одна из целей этого параграфа — показать, что справедливо и обратное: каждое сепарабельное расширение поля k может быть единственным образом поднято (в функториальном смысле) до неразветвленного расширения поля K.

Мы установим сначала факт, аналогичный теореме последней главы, который позволит описывать неразветвленные расширения как расширения корнями некоторых многочленов. Обозначения: $\bar{a}$ — образ элемента $a \in S$ в поле k_L; $\bar{g}(X)$ — образ многочлена $g(X) \in S[X]$ в кольце $k_L[X]$.

Предложение 7.1. (i) *Пусть L — неразветвленное расширение поля K. Существует такой элемент $x \in S$, что $k_L = k[\bar{x}]$. Если $g(X)$ — минимальный многочлен над полем K такого элемента x, то $S = R[x]$, $L = K[x]$ и $\bar{g}(X)$ неприводим в кольце $k[X]$ и сепарабелен.*

(ii) *Пусть $g(X)$ — такой унитарный многочлен из $R[X]$, что $\bar{g}(X)$ неприводим в кольце $k[X]$ и сепарабелен. Тогда если x — корень многочлена $g(X)$, то расширение $L = K[x]$ является неразветвленным над полем K и $k_L = k[\bar{x}]$.*

Доказательство. (i) Поскольку расширение k_L сепарабельно над k, оно имеет вид $k[\bar{x}]$ при некотором $x \in S$. Для каждого такого x минимальный многочлен $G(X)$ образа $\bar{x}$ сепарабелен над полем k. Кроме того,

$$[L : K] \geqslant \deg g(X) \geqslant \deg G(X) = [k_L : k] = [L : K].$$

Следовательно, на самом деле $G(X) = \bar{g}(X)$, т. е. $\bar{g}(X)$ неприводим, и $L = K[x]$. Равенство $S = R[x]$ может быть теперь выведено или из предложения 6.1, примененного к расширению L, или из предложения 4.6.

(ii) Мы имеем

$$[L : K] = \deg g(X) = [k[\bar{x}] : k] \leqslant [k_L : k] \leqslant [L : K].$$

Следовательно, во-первых, $[L : K] = f(L/K)$, т. е. $e(L/K) = 1$, и, во-вторых, $k_L = k[\bar{x}]$, т. е. k_L сепарабельно над k.

Рассмотрим некоторый класс алгебраических расширений E, E_1, ... заданного поля F. Под *гомоморфизмом* $\sigma: E \to E_1$ *над полем* F подразумевается такой гомоморфизм полей, который оставляет неподвижным каждый элемент из поля F. Пример такого гомоморфизма — тождественное отображение $E \to E$. Если $\sigma: E \to E_1$ и $\tau: E_1 \to E_2$ — гомоморфизмы над полем F, то таковой же будет и их композиция $\sigma \circ \tau: E \to E_2$. Другими словами, мы имеем «категорию» (в грубом смысле этого слова). Обозначим через $\mathrm{Hom}^F(E, E_1)$ множество гомоморфизмов $E \to E_1$ над полем F. Если расширение E нормально над F, то $\mathrm{Hom}^F(E, E)$ — не что иное, как группа Галуа расширения E/F.

Пусть E^s — сепарабельное замыкание поля F в расширении E, т. е. максимальное подполе поля E, сепарабельное над F. Тогда получаются отображения

$$\mathrm{Hom}^F(E, E_1) \to \mathrm{Hom}^F(E^s, E_1^s), \qquad (1)$$

которые сохраняют композицию $\sigma \circ \tau$ и тождественные отображения полей E; иными словами, мы определили функтор. Отображения (1) инъективны, а если $E = E^s$, то и биективны.

Применим теперь этот аппарат к классу конечных сепарабельных алгебраических расширений L поля K. Для различных L мы будем обозначать соответствующие кольца нормирований через R_L, а идеалы нормирований — через $\mathfrak{p}_L$.

Предложение 7.2. *Пусть* $\sigma: L \to L'$ *— некоторый гомоморфизм над полем* K. *Тогда для всех* $x \in L$ *имеет место*

$$v_{L'}(x\sigma) = e(L'/L\sigma)\, v_L(x).$$

Доказательство. Функция v на множестве L, определенная равенством

$$e(L'/L\sigma)\, v(x) = v_{L'}(x\sigma),$$

является дискретным нормированием поля L, которое на поле K совпадает с нормированием v_L. В силу единственности (см. гл. II) $v = v_L$.

Следствие 1. *Применение предложения* 7.2 *к нормальным расширениям* L *и их группам Галуа.*

Следствие 2. *Ограничивая гомоморфизм* $\sigma: L \to L'$ *над полем* K *на кольца нормирований и редуцируя его по модулю идеалов нормирований, мы получаем гомоморфизм* $\bar{\sigma}$: $k_L \to k_{L'}$ *над полем* k. *Полученные таким образом отображения*

$$\mathrm{Hom}^K(L, L') \to \mathrm{Hom}^k(k_L, k_{L'})$$

сохраняют тождественные отображения полей и композиции отображений.

Итак, поле вычетов k_L определяет некоторый функтор; то же можно сказать и о сепарабельном замыкании k_L^s поля k в расширении k_L. Наша следующая теорема, говоря на языке теории категорий, утверждает, что для функтора k_L^s существует присоединенный функтор. В частности устанавливается изоморфизм категории сепарабельных расширений поля k и категории неразветвленных расширений поля K.

Теорема 7.1. *Пусть* $\bar{k}$ *— конечное сепарабельное алгебраическое расширение поля* k. *Тогда существует такое конечное сепарабельное алгебраическое расширение* $L = L(\bar{k})$ *поля* K, *что*

(i) $\bar{k} \cong k_L$ (*над* k);

(ii) *расширение* L *является неразветвленным над* K;

(iii) *отображения*

$$\mathrm{Hom}^K(L, L') \to \mathrm{Hom}^k(k_L, k_{L'})$$

биективны для всех L'.

Свойства (i), (ii) *или* (i), (iii) *определяют расширение* L/K *однозначно с точностью до изоморфизма над полем* K.

Замечание. В (iii) можно было бы заменить расширения k_L и $k_{L'}$ соответственно на k_L^s и $k_{L'}^s$.

Для доказательства нам нужна следующая

Лемма 7.1. *Пусть $g(X)$ — унитарный многочлен в кольце $R[X]$, такой, что многочлен $\bar{g}(X)$ сепарабелен; предположим, что элемент $\alpha \in k$ является корнем многочлена $\bar{g}(X)$. Тогда в кольце R существует один и только один элемент x, такой, что*

$$g(x)=0 \quad и \quad \bar{x}=\alpha.$$

Доказательство см. в гл. II, добавление B.

Доказательство теоремы 7.1. Мы знаем, что $\bar{k}=k[\alpha]$, где минимальный многочлен $G(X)$ элемента α над полем k сепарабелен. Выберем произвольный унитарный многочлен $g(X) \in R[X]$, для которого $\bar{g}(X)=G(X)$, и пусть $L=K[x]$, где x — корень многочлена $g(X)$. В силу предложения 7.1 расширение L обладает свойствами (i) и (ii).

Чтобы показать, что расширение L обладает и свойством (iii), рассмотрим произвольный гомоморфизм w: $k_L \to k_{L'}$ над k.

Согласно лемме 7.1, расширение L' содержит однозначно определенный элемент y, для которого $g(y)=0$ и $\bar{y}=\bar{x}w$. Но тогда существует и однозначно определенный гомоморфизм σ: $L \to L'$ над полем K, для которого $x\sigma=y$. Ясно, что $\bar{\sigma}=w$; если, кроме того, $\bar{\tau}=w$, то $x\tau=y$ и, следовательно, $\tau=\sigma$.

Предположим теперь, что L' не разветвлено над K и w — некоторый изоморфизм $k_L \cong k_{L'}$ над k. Тогда $[L':K]=[L:K]$, в силу чего поднятый изоморфизм σ: $L \to L'$ над полем K должен быть изоморфизмом. Таким образом, мы показали, что свойства (i) и (ii) определяют расширение L однозначно с точностью до изоморфизма над полем K. Результат о единственности расширения L, обладающего свойствами (i) и (iii), общеизвестен.

Следствие. *Расширение $L(\bar{k})$ нормально над K тогда и только тогда, когда расширение $\bar{k}$ нормально над k; в этом случае их группы Галуа изоморфны.*

В дальнейшем, говоря о «подполе» конечного алгебраического сепарабельного расширения L поля K, мы всегда будем подразумевать подполе, содержащее поле K.

Теорема 7.2. *Расширение L содержит такое подполе L_0, что каждое неразветвленное расширение L' поля K, содержащееся в L, является подполем поля L_0, и обратно. Кроме того, $k_{L_0}=k_L^s$.*

Если L — нормальное расширение поля K с группой Галуа Γ, то расширение L_0 нормально над K и является неподвижным полем группы

$$\Gamma_0=\{\gamma \in \Gamma \mid v_L(x\gamma-x)>0 \quad при\ всех \quad x \in R_L\}.$$

Группа Γ_0 называется *группой инерции* расширения L/K.

Доказательство. Существование подполя L_0, неразветвленного над полем K и такого, что $k_{L_0}=k_L^s$, следует из теоремы 7.1. В таком случае все подполя расширения L_0 не разветвлены над K. Действительно, из определения понятия «неразветвленности» мы видим, что для любой башни полей $E \supset F \supset K$ расширение E/K не разветвлено тогда и только тогда, когда не разветвлены E/F и F/K.

Обратно, пусть L' — подполе поля L, неразветвленное над K. Тогда $k_{L'} \subset k_L^s = k_{L_0}$. В силу теоремы 7.1, примененной к случаю $\bar{k}=k_{L'}$, мы получаем некоторый гомоморфизм σ: $L' \to L_0$ над полем K, для которого $\bar{\sigma}$ — включение. Пусть теперь $k_{L'}=k[\bar{x}]$, где $x \in L'$. Тогда x и $x\sigma$ являются элементами поля L и имеют один и тот же класс вычетов; по лемме 7.1 отсюда следует, что $x=x\sigma$. Однако, согласно предложению 7.1, $L'=K[x]$, так что $L' \subset L_0$.

Предположим теперь, что расширение L нормально. Поскольку все сопряженные с L_0 поля в расширении L являются неразветвленными над K, они совпадают с L_0, благодаря чему L_0 нормально. Группа инерции Γ_0 по определению является ядром гомоморфизма

$$\Gamma \to \mathrm{Hom}^h(k_L, k_L).$$

В силу инъективности отображения (1) группа Γ_0 является также и ядром гомоморфизма из группы Γ в группу Галуа

$\mathrm{Hom}^h(k_L^s, k_L^s)$ расширения k_{L_0}. Если Ω — группа Галуа расширения L_0/K, то из теоремы 7.1 следует, что

$$\Gamma_0 = \ker(\Gamma \to \Omega),$$

откуда и вытекает доказываемое утверждение.

Следствие 1. *Композит неразветвленных расширений L и L' в заданном сепарабельном замыкании поля K является неразветвленным.*

Объединение K_{nr} всех неразветвленных расширений L поля K в данном сепарабельном замыкании поля K называется *максимальным неразветвленным расширением поля K.*

Следствие 2. *Каждое конечное расширение поля K, лежащее в K_{nr}, является неразветвленным над K. Группа Галуа $\Gamma(K_{\mathrm{nr}}/K)$ изоморфна (как топологическая группа) группе Галуа $\Gamma(\bar{k}^s/k)$ сепарабельного замыкания $\bar{k}^s$ поля k.*

Приложения (см. гл. III и V). Предположим, что k — конечное поле характеристики p, состоящее из $q = p^m$ элементов. Обозначим через $\overline{\mathbf{Z}}$ пополнение группы $\mathbf{Z}$ относительно топологии, определяемой подгруппами $n\mathbf{Z}$ $(n > 0)$. Тогда отображение

$$\nu \longmapsto w_q^\nu,$$

где $\alpha w_q = \alpha^q$, устанавливает изоморфизм групп $\Gamma(\bar{k}^s/k)$ и $\overline{\mathbf{Z}}$. Поэтому справедливо такое утверждение.

I. *Существует единственный элемент $\sigma_q \in \Gamma(K_{\mathrm{nr}}/K)$ со следующим свойством: если поле L является подполем поля K_{nr}/K, то для всех $a \in R_L$ имеет место*

$$a\sigma_q = a^q \pmod{\mathfrak{p}_L}.$$

Отображение $\nu \longmapsto \sigma_q^\nu$ устанавливает изоморфизм $\overline{\mathbf{Z}} \cong \Gamma(K_{\mathrm{nr}}/K)$ топологических групп.

(Элемент σ_q называется *подстановкой Фробениуса.*)

Из этого результата следует тот факт, что для каждого целого числа $n > 0$ поле K имеет одно и (с точностью до изоморфизма над K) только одно неразветвленное расширение L степени n. Это расширение L нормально над K и его группа Галуа циклична.

Из теории конечных полей при помощи предложения 7.1 мы получаем следующее утверждение.

II. *Расширение K_{nr} является объединением расширений корнями m-й степени из единицы (в данном сепарабельном замыкании поля K) для всех m, взаимно простых с p.*

В заключение мы рассмотрим действие норменного отображения на группах единиц (см. следствие из предложения 5.3). Подгруппы, определенные в § 1 формулой (6) для полей K и L, будут обозначаться через $U_{K,n}$ и $U_{L,n}$.

Предложение 7.3. *Если расширение L не разветвлено над K, то для всех $n \geqslant 1$ имеет место*

$$N_{L/K}(U_{L,n}) = U_{K,n}.$$

Доказательство. Выберем такой элемент $\Pi \in K$, что $v_K(\Pi) = 1$, т. е. $v_L(\Pi) = 1$. Тогда $U_{L,n}$ состоит из элементов

$$u = 1 - \Pi^n x, \qquad x \in R_L.$$

Если $m = [L:K]$, то характеристический многочлен $h(X)$ элемента Π_x^n над полем K имеет вид

$$h(X) = X^m - \Pi^n \mathrm{tr}_{L/K}(x) X^{m-1} + \Pi^{n+1} h_1(X),$$

где $h_1(X) \in R[X]$. Поэтому

$$N_{L/K}(u) = h(1) \equiv 1 + \Pi^n \mathrm{tr}_{L/K}(x) \pmod{\mathfrak{p}^{n+1}}.$$

Из этого вытекает, прежде всего, что

$$N_{L/K}(U_{L,n}) \subset U_{K,n}.$$

В силу теоремы 5.2 $\mathrm{tr}_{L/K}(R_L) = R$ и, следовательно,

$$N_{L/K}(U_{L,n}) U_{K,n+1} = U_{K,n}.$$

Теперь, чтобы закончить доказательство, нужно только воспользоваться полнотой, подобно тому как это делалось в предложении 1.5.

Следствие. *Пусть L не разветвлено над K. Тогда единица из группы U_K принадлежит образу норменного отображения группы U_L в том и только том случае, когда*

класс вычетов этой единицы по mod $\mathfrak{p}$ *является нормой элемента из* k_L. *В частности, если поле* k *конечно, то*

$$N_{L/K}(U_L) = U_K.$$

Доказательство. Утверждение следует из формулы (4) § 5.

§ 8. СЛАБО РАЗВЕТВЛЕННЫЕ РАСШИРЕНИЯ

Обозначения здесь будут теми же, что и в § 7; через χ будет обозначаться характеристика поля k. Термин «подполе» употребляется в том же смысле, что и в теореме 7.2. Через Γ_0 всегда обозначается группа инерции, которую мы там ввели.

Теорема 8.1. (i) *Расширение* L *обладает таким подполем* L_1, *что каждое разветвленное над* K *подполе* L' *поля* L *является подполем поля* L_1 *и обратно. Если* $\chi = p \neq 0$, *то* $[L : L_1]$ *является степенью числа* p.

(ii) *Пусть* L — *нормальное расширение поля* K *с группой Галуа* Γ. *Тогда расширение* L_1 *нормально над* K *и является полем неподвижных элементов группы*

$$\Gamma_1 = \{\gamma \in \Gamma \mid v_L(x\gamma - x) \geqslant v_L(x) + 1 \text{ для всех } x \in R_L\}.$$

Если $v_L(\Pi) = 1$, *то отображение*

$$\gamma \longmapsto \overline{\Pi\gamma/\Pi}$$

определяет гомоморфизм θ_0 *группы* Γ_0 *в группу* $k_{L_0}^*$, *который не зависит от выбора элемента* Π *и ядро которого равно группе* Γ_1. *Группа* Γ_0/Γ_1 *циклична. Если* $\chi = p \neq 0$, *то группа* Γ_1 *является (однозначно определенной)* p*-силовской подгруппой группы* Γ_0.

Замечание. Если $\chi = 0$, то расширение L слабо разветвлено в любом случае. Тогда эта теорема утверждает лишь существование гомоморфизма θ_0 и цикличность группы Γ_0.

Доказательство. Начнем с нормального случая и опишем свойства гомоморфизма θ_0. Очевидно, группа Γ_1 содержится в группе Γ_0 и является нормальным делителем в группе Γ.

Если $\gamma \in \Gamma_0$ и u — единица кольца R_L, то $u\gamma/u \equiv 1 \pmod{\mathfrak{p}_L}$. Следовательно, класс вычетов $\theta_0(\gamma) = \overline{\Pi\gamma/\Pi}$ в группе k_L^* не зависит от выбора элемента Π (при условии, что $v_L(\Pi) = 1$). Так как группа Γ_0 действует на группе k_L^* тривиально, то $\theta_0(\gamma_1\gamma_2) = \theta_0(\gamma_1)\theta_0(\gamma_2)$. Поскольку группа Γ_0 конечна, элементы $\theta_0(\gamma)$ являются корнями из единицы и, следовательно, лежат в группе $(k_L^s)^* = k_{L_0}^*$. Кроме того, можно показать, что группа $\Gamma_0/\ker\theta_0 \cong \operatorname{Im}\theta_0$ циклична и что ее порядок не делится на χ. Наконец, так как $\overline{u\gamma/u} = 1$ для всех единиц u, то для $a \in L^*$ имеет место $\overline{a\gamma/a} = \theta_0(\gamma)^{v_L(a)}$. Таким образом, на самом деле $\Gamma_1 = \ker\theta_0$.

Пусть теперь L_1 — неподвижное поле группы Γ_1. Мы уже видели, что если $\chi = p \neq 0$, то степень $[L_1 : L_0]$ взаимно проста с числом p. Так как $k_L \supset k_{L_1} \supset k_{L_0}$ и $[k_L : k_{L_0}]$ — степень числа p, то $f(L_1/L_0) = 1$. Кроме того, $e(L_1/L_0)$ не делится на p. Таким образом, расширение L_1 слабо разветвлено над L_0.

В заключение воспользуемся тем фактом, что для любой башни полей $E \supset F \supset K$ расширение E/K слабо разветвлено тогда и только тогда, когда слабо разветвлены расширения E/F и F/K. Это следует из определения слабого ветвления. В качестве первого следствия отметим, что L_1 и его подполя слабо разветвлены над K.

Пусть L' — подполе поля L, слабо разветвленное над K. Покажем; что $L' \subset L_1$. Пусть $L'L_0 = E$, $L' \cap L_0 = F$. Тогда расширение L'/F слабо разветвлено и, следовательно, по теореме 5.2 существует такой элемент $a \in R_{L'}$, что $\operatorname{tr}_{L'/F}(a) = 1$. Так как группа Γ_0 является нормальным делителем, то мы, кроме того, имеем, что $\operatorname{tr}_{E/L_0}(a) = 1$, откуда вновь в силу теоремы 5.2 расширение E/L_0 слабо разветвлено; по этой причине расширение E слабо разветвлено и над K. Следовательно, $k_E \subset k_L^s$, т. е. $k_E = k_{L_0}$, и, таким образом, расширение E вполне разветвлено над L_0.

Пусть $v_E(c) = 1$ и $g(X)$ — минимальный многочлен элемента c над полем L_0. В силу теоремы 6.1 и предложения 4.6 мы имеем

$$\mathfrak{D}(E/L_0) = R_E g'(c);$$

следовательно, по теореме 5.2,

$$v_E(g'(c)) = e-1, \qquad e = e(E/L_0),$$

т. е.

$$v_L(g'(c)) = (e-1)\, v_L(c). \tag{1}$$

Пусть теперь E — неподвижное поле подгруппы $\Delta \subset \Gamma_0$. Выберем в каждом правом смежном классе $\Gamma_0 \bmod \Delta$, отличном от Δ, некоторый элемент γ. Тогда

$$g'(c) = \prod_{\gamma} (c - c\gamma).$$

Для каждого из $e-1$ сомножителей, содержащихся в этом произведении, имеем

$$v_L(c - c\gamma) \geqslant v_L(c),$$

и в силу (1)

$$v_L(c - c\gamma) = v_L(c).$$

Следовательно, $\gamma \notin \Gamma_1$. А из этого вытекает, что $\Delta \supset \Gamma_1$, т. е. $E \subset L_1$, и, таким образом, $L' \subset L_1$.

Предположим теперь, что $\chi = p \neq 0$ и что L'' — собственное расширение поля L_1 в поле L. Тогда L'' не является слабо разветвленным над L_1, т. е. или $p \mid e(L''/L_1)$, или $p \mid f(L''/L_1)$; в любом случае $p \mid [L'' : L_1]$. Следовательно, группа Γ_1 совпадает со своей силовской p-группой.

Выводы для расширения L, не являющегося нормальным, получаются с помощью вложения L в некоторое нормальное расширение поля K. Детальное доказательство оставляется читателю.

Следствие 1. *Группа инерции Γ_0 всегда разрешима. Точнее: если $\chi = 0$, то Γ_0 циклична, а если $\chi = p \neq 0$, то Γ_0 является расширением некоторой p-группы циклической группой.*

Если поле k конечно, то группа Галуа любого нормального расширения разрешима.

Следствие 2. *Композит слабо разветвленных расширений L и L' в сепарабельном замыкании поля K является слабо разветвленным.*

Максимальным слабо разветвленным расширением K_{tr} поля K называется объединение всех слабо разветвленных расширений в сепарабельном замыкании поля K.

Следствие 3. *Все конечные расширения поля K в K_{tr} слабо разветвлены. Расширение K_{tr} содержит расширение K_{nr}. Если $\chi = 0$, то $\Gamma(K_{\mathrm{tr}}/K_{\mathrm{nr}}) \cong \overline{\mathbf{Z}}$; если $\chi = p \neq 0$, то $\Gamma(K_{\mathrm{tr}}/K_{\mathrm{nr}}) \cong \prod_{q \neq p} \overline{\mathbf{Z}}_q$.*

Замечание. Группа Γ_1 допускает интересное описание в терминах теории модулей. Кольцо R_L обладает структурой некоторого модуля над групповым кольцом $R(\Gamma)$. Для подгруппы Δ группы Галуа Γ можно показать, что модуль R_L слабо проективен относительно кольца $R(\Delta)$ тогда и только тогда, когда $\Delta \supset \Gamma_1$.

Из теоремы 8.1 видно, что для того, чтобы «добраться» до слабо разветвленного расширения, надо проделать два шага. На первом из них строится неразветвленное расширение (о котором шла речь в § 7), а на втором — вполне и слабо разветвленное нормальное расширение. Последний этап может быть также описан явно.

Напомним несколько фактов из теории Куммера (см. гл. III). Предположим, что поле K содержит первообразный корень e-й степени из единицы и что элемент $c \in K^*$ имеет в точности порядок e по модулю K^{*e}. Тогда поле $K(\Pi)$, где $\Pi^e = c$, нормально над K и имеет степень e; равенства

$$\psi_c(\gamma) = \Pi\gamma/\Pi$$

определяют некоторый инъективный гомоморфизм ψ_c группы Галуа в группу K^*. Будем писать

$$\overline{\psi}_c(\gamma) = \overline{\psi_c(\gamma)}.$$

Предложение 8.1. (i) *Пусть L — нормальное, вполне и слабо разветвленное расширение степени e. Тогда поле K содержит первообразный корень e-й степени из единицы и существует элемент $c \in K^*$, для которого $v_K(c) = 1$ и $L = K(c^{1/e})$.*

Более того, $\overline{\psi}_c$ совпадает с гомоморфизмом θ_0, определенным в теореме 8.1.

Кроме того, $L = K(b^{1/e})$ при $v_K(b) = 1$ тогда и только тогда, когда

$$\overline{bc^{-1}} \in k^{*e}.$$

(ii) *Если $\chi \nmid e$ и поле K содержит первообразный корень e-й степени из единицы, и если $v_K(c) = 1$, то поле $L = K(c^{1/e})$ нормально, вполне и слабо разветвлено над K и имеет степень e.*

Доказательство. (i) В силу теоремы 8.1 $\operatorname{Im}\theta_0$ — это в точности группа корней e-й степени из единицы в группе k^*. Так как многочлен $X^e - 1$ сепарабелен над k, то из леммы 7.1 следует, что K содержит первообразный корень e-й степени из единицы и что все такие корни взаимно однозначно отображаются в k^*. Из того, что группа Галуа Γ расширения L/K — циклическая порядка e, следует по теории Куммера, что $L = K(c^{1/e})$, где e равно порядку элемента c по $\bmod K^{*e}$. Более того, и $\bar{\psi}_c$, и θ_0 — инъективные гомоморфизмы группы Γ в k^*, имеющие один и тот же образ. Поэтому

$$\bar{\psi}_c = \theta_0^r, \quad (r, e) = 1. \tag{2}$$

Но, как было видно из доказательства теоремы 8.1,

$$r = v_L(c^{1/e}) = v_K(c). \tag{3}$$

Таким образом, $(v_K(c), e) = 1$. Мы можем теперь заменить элемент c на $c^s a^e$, где $(s, e) = 1$ и $a \in K^*$, и быть уверенными в том, что $v_K(c) = 1$; следовательно, в силу (2), (3) имеет место $\bar{\psi}_c = \theta_0$.

Если теперь, кроме этого, $L = K(b^{1/e})$, то, согласно теории Куммера, $b = c^r a^e$, где $a \in K^*$, $(r, e) = 1$ и $0 < r < e$. Если $v_K(b) = 1$, то $r = 1$ и, следовательно, элемент a является единицей. Окончательное доказательство нашего критерия получается с помощью предложения 1.5.

Утверждение (ii) следует из теории Куммера и теоремы 6.1.

Следствие 1. *Пусть $v_K(c) = 1$. Тогда расширение K_{tr} представляет собой объединение полей $K_{\mathrm{nr}}(c^{1/e})$, где e пробегает множество всех натуральных чисел, которые не делятся на χ.*

Наконец, мы вновь обращаемся к нормам единиц. В обозначениях предложения 7.3 имеет место

Предложение 8.2. *Если расширение L слабо разветвлено над K, то*

$$N_{L/K}(U_{L,1}) = U_{K,1}.$$

Доказательство. В силу формулы (4) § 5 всегда имеет место включение $N_{L/K}(U_{L,1}) \subset U_{K,1}$. На основании предложения 7.3 и в силу транзитивности норм мы можем считать, что расширение L вполне разветвлено над K; пусть оно имеет степень e. Тогда на основании предложения 1.5

$$U_{K,1} = U_{K,1}^e \subset N_{L/K}(U_{L,1}).$$

§ 9. ГРУППЫ ВЕТВЛЕНИЯ

Как и всюду, на протяжении этой главы расширение L считается нормальным, а его группа Галуа обозначается через $\Gamma = \Gamma(L/K)$. Ряды подгрупп, начинающиеся с групп Γ_0, Γ_1 (см. § 7, 8), могут быть продолжены. Оставив в стороне описание общего случая, мы предположим в этом параграфе раз и навсегда, что расширение k_L/k сепарабельно, т. е. $k_L = k_{L_0}$. Так будет всегда, когда k — конечное поле. При этом предположении, независимо от того, нормально расширение L или нет, имеет место

Предложение 9.1. $R_L = R[a]$.

Доказательство. В силу предложения 7.1 существует такой элемент $b \in L_0$ (мы используем обозначения теоремы 7.2), что $k_L = k[\bar{b}]$, и потому редуцированный многочлен $\bar{g}(X)$ минимального многочлена $g(X)$ элемента b над полем K сепарабелен. Следовательно, $\bar{g}'(\bar{b}) \neq 0$.

Пусть теперь $a = b + h$, где $v_L(h) = 1$. Тогда из тейлоровского разложения многочлена $g(X)$ мы получаем равенство

$$g(a) = hg'(b) + O(h^2).$$

Следовательно,

$$v_L(g(a)) = 1.$$

Применим предложение 6.1 к расширению L. Так как $k_L = k[\bar{a}]$, то можно выбрать некоторое множество $\mathfrak{N}$,

состоящее из «многочленов» от a с коэффициентами из R. Для $n = me + r$, где $e = e(L/K)$, $0 \leqslant r < e$, $m \in \mathbf{Z}$, положим $\Pi_n = g(a)^r c^m$, где $c \in K$, $v_K(c) = 1$. Переставляя члены ряда для элемента из R_L, мы получаем $R_L = R[a]$.

Определим теперь с помощью элемента a, фигурирующего в формулировке предложения, следующую функцию $i = i_{L/K}$: $\Gamma \to \mathbf{Z} \cup \infty$:

$$i_{L/K}(\gamma) = i(\gamma) = v_L(a\gamma - a). \tag{1}$$

Кроме того, положим (для $i \geqslant -1$)

$$\Gamma_i = [\gamma \in \Gamma \mid v_L(x\gamma - x) \geqslant i+1 \text{ для всех } x \in R_L]. \tag{2}$$

Таким образом, $\Gamma_{-1} = \Gamma$. Для $i = 0$ мы, очевидно, получаем группу инерции из § 7. Для $i = 1$, как мы впоследствии увидим, введенное определение согласуется с определением из § 8.

Следующее предложение связывает группу Γ_i с функцией $i_{L/K}$ и показывает, в частности, что эта функция не зависит от выбора образующей a.

Предложение 9.2.

(i) $\gamma \in \Gamma_i \Leftrightarrow i(\gamma) \geqslant i+1$;
(ii) $i(\gamma\delta) \geqslant \inf(i(\gamma), i(\delta))$;
(iii) $i(\delta\gamma\delta^{-1}) = i(\gamma)$.

Доказательство очевидно.

Следствие 1. *Группы Γ_i являются нормальными делителями группы Γ, причем $\Gamma_{i+1} \subset \Gamma_i$ и при достаточно больших m имеет место $\Gamma_m = 1$.*

Действительно, последнее условие выполняется для чисел m, удовлетворяющих неравенству

$$m \geqslant \sup_{\gamma \neq 1} i(\gamma).$$

Следствие 2. *Если $i(\gamma) \neq i(\delta)$, то*

$$i(\gamma\delta) = \inf\{i(\gamma), i(\delta)\}.$$

Группы Γ_i называются *группами ветвления* (Гильберт).

Если Δ — подгруппа группы Γ, то она является группой Галуа расширения поля L над неподвижным полем группы Δ. Очевидно, имеет место следующее

Предложение 9.3. $\Delta_i = \Gamma_i \cap \Delta$.

В дальнейшем через U обозначается группа единиц кольца R_L и через U_i — подгруппы, определенные формулой (6) § 1 (если считать, что K заменено на L).

Теорема 9.1. *Пусть $i \geqslant 1$. Тогда $\gamma \in \Gamma_i$ в том и только том случае, если при всех $x \in L^*$ элемент $x\gamma/x$ лежит в группе U_i.*

Зафиксируем некоторый элемент $\Pi \in L$, для которого $v_L(\Pi) = 1$. Тогда отображение

$$\gamma \longmapsto \Pi\gamma/\Pi \bmod U_{i+1}$$

является гомоморфизмом

$$\theta_i : \Gamma_i \to U_i/U_{i+1},$$

который не зависит от выбора элемента Π и ядро которого равно Γ_{i+1}.

Замечание. Теперь мы уже знаем, что Γ_1 (§ 8) $=$ $= \Gamma_1$ (§ 9).

Доказательство. Если $x\gamma/x \in U_i$ при всех $x \in L^*$, то оператор γ действует на поле k_L тривиально; следовательно, $\gamma \in \Gamma_0$. Так как $k_L = k_{L_0}$, то элементы кольца R_L имеют вид $y + z$, где $y \in \mathfrak{p}_L$, $z \in R_{L_0}$. Но тогда

$$v_L((y+z)\gamma - (y+z)) = v_L(y\gamma - y) =$$
$$= v_L\left(\frac{y\gamma}{y} - 1\right) + v_L(y) \geqslant i+1.$$

Таким образом, $\gamma \in \Gamma_i$.

Обратно, предположим, что $\gamma \in \Gamma_i$. Если $y \in U$, то

$$v_L(y\gamma/y - 1) = v_L(y\gamma - y) \geqslant i+1.$$

Следовательно,

$$y\gamma/y \in U_{i+1}. \tag{3}$$

Пусть теперь $v_L(\Pi) = 1$. Тогда

$$v_L(\Pi\gamma/\Pi - 1) = v_L(\Pi\gamma - \Pi) = 1 \geqslant i,$$

т. е. $\Pi\gamma/\Pi \in U_i$. Положим

$$\theta_i(\gamma) \equiv \Pi\gamma/\Pi \bmod U_{i+1}.$$

В силу формулы (3) мы, во-первых, видим, что $\theta_i(\gamma)$ не зависит от выбора элемента Π и, во-вторых, что если $x \in L^*$, то

$$\theta_i(\gamma)^{v_L(x)} \equiv x\gamma/x \bmod U_{i+1}.$$

Поэтому, с одной стороны,

$$x\gamma/x \in U_i,$$

а с другой стороны, учитывая уже доказанное, мы получаем, что

$\theta_i(\gamma) = 1$ тогда и только тогда, когда $\gamma \in \Gamma_{i+1}$.

Наконец, для элементов γ, $\delta \in \Gamma_i$ мы имеем

$$\Pi\gamma\delta/\Pi = (\Pi\gamma/\Pi)\,\delta\,(\Pi\delta/\Pi).$$

Так как $\Pi\gamma/\Pi \in U$, то из формулы (3) следует, что

$$(\Pi\gamma/\Pi)\,\delta \equiv \Pi\gamma/\Pi \pmod{U_{i+1}}$$

и, таким образом,

$$\theta_i(\gamma\delta) = \theta_i(\gamma)\,\theta_i(\delta).$$

Предложение 9.3 доказано.

Мы знаем, что если $\chi = 0$, то уже $\Gamma_1 = 1$. В то же время если $\chi = p \neq 0$, то, согласно предложению 1.5, имеет место включение $U_1^p \subset U_{i+1}$. Поэтому мы имеем такое

Следствие. *Если $\chi = p \neq 0$, то при $i \geqslant 1$ группа Γ_i/Γ_{i+1} является элементарной абелевой p-группой.*

О коммутационных свойствах групп ветвления см. [3], гл. IV.

Замечание. Если расширение k_L не сепарабельно над k, то приходится определять два ряда подгрупп. Один из них задается соотношением (2) (при $i \geqslant 0$); будем временно обозначать его члены символами Γ_{i*}. С другой стороны, критерий теоремы 9.1 — *$x\gamma/x \in U_i$ для всех $x \in L^*$* — задает второй ряд подгрупп Γ_i^* ($i \geqslant 1$). Следствие 1 из предложения 9.2 и предложение 9.3 остаются справедливыми для каждого из этих двух рядов и то же можно сказать о следствии из теоремы 9.1. Другими словами, при $i \geqslant 1$ факторгруппы $\Gamma_{i*}/\Gamma_{i+1*}$ и $\Gamma_i^*/\Gamma_{i+1}^*$ являются элементарными

абелевыми p-группами. Оба ряда подгрупп тесно связаны друг с другом, так как $\Gamma_{i*} \supset \Gamma_{i+1}^* \supset \Gamma_{i+1*}$ при $i \geqslant 0$. Если расширение k_L сепарабельно над k, то по теореме 9.1 $\Gamma_{i+1}^* = \Gamma_{i+1*}$. С другой стороны, если $e(L/L_1) = 1$, то $\Gamma_{i*} = \Gamma_{i+1}^*$ (для $i \geqslant 1$).

Теперь мы вновь будем предполагать, что расширение k_L/k сепарабельно. Группы ветвления дают одно из явных определений дифференты, которое обобщает формулу (см. теорему 5.2), выполняющуюся в слабо разветвленном случае. Введем обозначение:

$$g_i = \text{порядок группы } \Gamma_i. \tag{4}$$

Отметим, что теперь расширение L/L_0 вполне разветвлено, т. е.

$$g_0 = e(L/L_0) = e(L/K).$$

Предложение 9.4.

$$v_L(\mathfrak{D}) = \sum_{\gamma \neq 1} i(\gamma) = \sum_{i=0}^{\infty} (g_i - 1).$$

Доказательство. Пусть $R_L = R[a]$, и пусть $g(X)$ — минимальный многочлен элемента a над полем K. Согласно предложению 4.6,

$$\mathfrak{D} = g'(a)\,R_L$$

и, следовательно,

$$v_L(\mathfrak{D}) = v_L(g'(a)) = v_L\Big(\prod_{\gamma \neq 1} (a - a\gamma)\Big) =$$

$$= \sum_{\gamma \neq 1} i(\gamma) = \sum_{i=0}^{\infty} i((g_{i-1} - 1) - (g_i - 1)) = \sum_{i=0}^{\infty} (g_i - 1).$$

Следствие. *Пусть Δ — подгруппа группы Γ и F — ее неподвижное поле. Тогда*

$$e(L/F)\,v_F(\mathfrak{D}(F/K)) = \sum_{\gamma \notin \Delta} i_{L/K}(\gamma).$$

Доказательство. В силу формулы башен (см. предложение 4.7) мы имеем, что

$$e(L/F)\,v_F(\mathfrak{D}(F/K)) = v_L(\mathfrak{D}(L/K)) - v_L(\mathfrak{D}(L/F)).$$

Остается применить предложение 9.4 для преобразования выражения в правой части, учитывая, что в силу предложения 9.3 для $\delta \in \Delta$ имеет место $i_{L/K}(\delta) = i_{L/F}(\delta)$.

С этого места мы будем рассматривать случай, когда Δ — нормальный делитель группы Γ с неподвижным полем F. Поле F является нормальным расширением поля K с группой Галуа Γ/Δ. Наша ближайшая цель — определить функцию $i_{F/K}$.

Предложение 9.5. *Для* $\omega \in \Gamma/\Delta$ *имеет место*

$$e(L/F)\, i_{F/K}(\omega) = \sum_{\gamma \to \omega} i_{L/K}(\gamma).$$

Доказательство. Для $\omega = 1$ выражения в обеих частях равенства бесконечны. Предположим теперь, что $\omega \neq 1$. Пусть $R_L = R[a]$, и пусть $g(X)$ — минимальный многочлен элемента a над полем F. Действуя оператором ω на многочлен $g(X)$ покоэффициентно, мы получаем многочлен $(g\omega)(X)$. Тогда

$$\mathfrak{p}_F^{i_{F/K}(\omega)} = \mathfrak{p}_L^{e(L/F) i_{F/K}(\omega)}$$

делит коэффициенты многочлена $(g\omega)(X) - g(X)$, а потому делит и выражение

$$(g\omega)(a) - g(a) = (g\omega)(a) = \prod_{\gamma \to \omega} (a - a\gamma).$$

Другими словами,

$$e(L/F)\, i_{F/K}(\omega) \leqslant \sum_{\gamma \to \omega} i_{L/K}(\gamma). \tag{5}$$

Вычислим $e(L/F)\, v_F(\mathfrak{D}(F/K))$ сначала с помощью предложения 9.4 (заменяя L на F), а потом с помощью следствия из этого предложения. Сравнивая результаты, мы получим равенство

$$\sum_{\omega \neq 1} e(L/F)\, i_{F/K}(\omega) = \sum_{\omega \neq 1} \sum_{\gamma \to \omega} i_{L/K}(\gamma).$$

Но это означает, что в формуле (5) на самом деле имеет место равенство.

Обратимся теперь к группам ветвления группы Γ/Δ. Из результата § 7 и § 8 следует, что $(\Gamma/\Delta)_i = \Gamma_i\Delta/\Delta$ для

$i = 0, 1$. Но, вообще говоря, это неверно при x. Для того чтобы получить аналог предложения 9.3 применительно к факторгруппам, нужно, следуя Эрбрану, ввести новую нумерацию групп ветвления.

Пусть x обозначает вещественную переменную, которая $\geqslant -1$. Положим

$$\Gamma_x = \Gamma_i, \text{ где } i \text{ — наименьшее целое число, которое} \geqslant x. \tag{6}$$

Определим далее функцию $\phi = \phi_{L/K}$ следующим образом:

$$\phi(x) = \begin{cases} x, \text{ если } -1 \leqslant x \leqslant 0; \\ \frac{1}{g_0}[g_1 + \ldots + g_m + (x - m)\, g_{m+1}], \\ \text{если } x \geqslant 0 \text{ и } m \text{ — целая часть числа } x. \end{cases} \tag{7}$$

Функция $\phi(x)$ непрерывна, строго возрастает и потому обладает обратной функцией $\psi(y)$, которая также непрерывна и строго возрастает $(-1 \leqslant y)$. Новая, «верхняя» нумерация групп ветвления задается теперь так:

$$\Gamma^y = \Gamma_x, \quad \text{если } x = \psi(y), \quad \text{т. е. } y = \phi(x). \tag{8}$$

Нам потребуются некоторые формальные свойства функции ϕ.

Лемма 9.1. *Функция* ϕ *однозначно определяется следующими свойствами:*

(i) $\phi(0) = 0$;
(ii) $\phi(x)$ *непрерывна*;
(iii) *если* m *— целое число* $\geqslant -1$, *то* $\phi(x)$ *линейна в замкнутом интервале* $[m, m+1]$ *и имеет производную*

$$\phi'(x) = (\text{порядок группы } \Gamma_x)/e(L/K)$$

в открытом интервале $(m, m+1)$.

Доказательство очевидно.

Лемма 9.2. *Если* $\phi(x)$ *— целое число, то и число* x *целое.*

Доказательство. Для $x \in [-1, 0]$ утверждение очевидно. Если же $x \in [m, m+1]$, где $m \geqslant 0$, и $y = \phi(x)$, то

$$x = \frac{1}{g_{m+1}} [g_0 y + m g_{m+1} - (g_1 + \ldots + g_m)].$$

Лемма следует теперь из того, что g_{m+1} делит $g_0, \ldots, g_m$.

Лемма 9.3.

$$\phi(x) + 1 = \frac{1}{g_0} \sum_{\gamma \in \Gamma} \inf(i(\gamma), x+1).$$

Доказательство мы проведем лишь для $x > 0$. Пусть m—такое целое число, что $m < x \leqslant m+1$. Тогда

$$x + 1 = \inf(i(\gamma), x+1) \Leftrightarrow \gamma \in \Gamma_{m+1}.$$

Поэтому

$$\frac{1}{g_0} \sum_{\gamma \in \Gamma} \inf(i(\gamma), x+1) = \frac{1}{g_0} \Big(\sum_{\gamma \notin \Gamma_{m+1}} i(\gamma) + (x+1) g_{m+1} \Big) =$$

$$= \frac{1}{g_0} \Big(\sum_{i=0}^{m+1} (g_{i-1} - g_i) i + (x+1) g_{m+1} \Big) =$$

$$= \frac{1}{g_0} \Big(\sum_{i=0}^{m} g_i - (m+1) g_{m+1} + (x+1) g_{m+1} \Big) = \phi(x) + 1.$$

Теперь мы докажем следующее утверждение.

Теорема 9.2.

(i) $\phi_{L/K}(x) = \phi_{F/K}(\phi_{L/F}(x))$;
(ii) *для всех* $y \geqslant -1$ *имеет место*

$$(\Gamma/\Delta)^y = \Gamma^y \Delta/\Delta.$$

Доказательство. Для $\omega \in \Gamma/\Delta$ положим

$$j(\omega) = \sup_{\gamma \to \omega} i_{L/K}(\gamma). \tag{9}$$

Первый шаг состоит в доказательстве того, что

$$i_{F/K}(\omega) - 1 = \phi_{L/F}(j(\omega) - 1). \tag{10}$$

Выберем такой элемент $\gamma_0 \in \Gamma$, что $\gamma_0 \to \omega$ и что $i_{L/K}(\gamma_0) = j(\omega)$. Тогда равенство в предложении 9.5 может быть переписано в виде

$$e(L/F)\, i_{F/K}(\omega) = \sum_{\delta \in \Delta} i_{L/K}(\gamma_0 \delta). \tag{11}$$

Если $i_{L/K}(\delta) < j(\omega)$, то в силу следствия 2 из предложения 9.2 имеет место $i_{L/K}(\gamma_0 \delta) = i_{L/K}(\delta)$. Если $i_{L/K}(\delta) \geqslant j(\omega)$, то, согласно предложению 9.2,

$$j(\omega) \geqslant i_{L/K}(\gamma_0 \delta) = \inf(i_{L/K}(\delta),\ j(\omega)) = j(\omega),$$

т. е.

$$i_{L/K}(\gamma_0 \delta) = j(\omega).$$

Таким образом, во всех случаях имеет место равенство

$$i_{L/K}(\gamma_0 \delta) = \inf(i_{L/F}(\delta),\ j(\omega)) \tag{12}$$

(нужно только помнить, что в силу предложения 9.3 справедливо равенство $i_{L/F}(\delta) = i_{L/K}(\delta)$). Подставив теперь (12) в (11) и воспользовавшись леммой 9.3 (для случая L/F), мы получим равенство (10), и на основании него будем иметь, что

$$\omega \in \Gamma_x \Delta/\Delta \Leftrightarrow x \leqslant j(\omega) - 1 \Leftrightarrow \phi_{L/F}(x) \leqslant \phi_{L/F}(j(\omega) - 1) \Leftrightarrow$$
$$\Leftrightarrow \phi_{L/F}(x) \leqslant i_{F/K}(\omega) - 1 \Leftrightarrow \omega \in (\Gamma/\Delta)_y,$$

где $y = \phi_{L/F}(x)$. Другими словами, мы показали, что

$$\Gamma_x \Delta/\Delta = (\Gamma/\Delta)_y, \text{ где } y = \phi_{L/F}(x). \tag{13}$$

Докажем теперь утверждение (i) теоремы 9.2. Положим $\theta(x) = \phi_{F/K}(\phi_{L/F}(x))$. Покажем, что $\theta(x)$ обладает всеми свойствами, характеризующими, согласно лемме 9.1, функцию $\phi_{L/K}(x)$. Очевидно, $\theta(x)$ обладает свойствами (i) и (ii) из леммы 9.1. Далее, если x меняется в открытом интервале $(m, m+1)$, то интервал $(\phi_{L/F}(m), \phi_{L/F}(m+1))$ по лемме 9.2 не содержит целых чисел. Следовательно, функция $\phi_{F/K}(y)$ будет линейной в замкнутом интервале $[\phi_{L/F}(m), \phi_{L/F}(m+1)]$, а потому функция $\theta(x)$ будет линейной в замкнутом интервале $[m, m+1]$.

Остается сравнить производные для не целых значений x. Мы имеем

$$\theta'(x) = \phi'_{F/K}(y)\, \phi'_{L/F}(x), \text{ где } y = \phi_{L/F}(x). \tag{14}$$

По лемме 9.1 (для случая F/K)

$$\phi'_{F/K}(y) = (\text{порядок группы } (\Gamma/\Delta)_y)/e(F/K)$$

и потому, согласно (13),

$$\phi'_{F/K}(y) = [\Gamma_x\Delta : \Delta]/e(F/K). \tag{15}$$

В силу леммы 9.1 (для случая L/F) и предложения 9.3

$$\phi'_{L/F}(x) = (\text{порядок группы } (\Gamma_x \cap \Delta))/e(L/F).$$

Значит, согласно формулам (14), (15) и лемме 9.1 (для случая L/K),

$$\theta'(x) = \phi'_{L/K}(x),$$

и потому

$$\phi_{L/K}(x) = \phi_{F/K}(\phi_{L/F}(x)).$$

Последнее равенство вместе с равенством (13) дает нам, что

$$\Gamma^z\Delta/\Delta = (\Gamma/\Delta)^z$$

(где $z = \phi_{F/K}(y) = \phi_{L/K}(x)$). Теорема, таким образом, доказана.

О других свойствах функции Эрбрана см. [3], гл. IV и V.

§ 10. РАЗЛОЖЕНИЕ

Вернемся теперь к глобальному случаю. Через R обозначается произвольная дедекиндова область, через K — ее поле частных, через S — целое замыкание кольца R в конечном сепарабельном расширении L поля K. Символ $\mathfrak{p}$ означает ненулевой простой идеал кольца R, а символ $\mathfrak{P}$ — ненулевой простой идеал кольца S. Соответствующие пополнения будут обозначаться через $K_\mathfrak{p}$ и $L_\mathfrak{P}$. Индекс ветвления идеала $\mathfrak{P}$ над $\mathfrak{P} \cap R$ обозначается через $e_\mathfrak{P}$, а степень классов вычетов — через $f_\mathfrak{P}$. Таким образом,

$$\mathfrak{p}S = \prod_{\mathfrak{P}\mid\mathfrak{p}} \mathfrak{P}^{e}\mathfrak{p}, \tag{1}$$

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f}\mathfrak{P} \qquad (\mathfrak{p} = \mathfrak{P} \cap R). \tag{2}$$

Предложение 10.1. $[L : K] = \sum_{\mathfrak{P}\mid\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P}$.

Доказательство. В силу формулы (2) § 4

$$[L : K] = \sum_{\mathfrak{P}\mid\mathfrak{p}} [L_\mathfrak{P} : K_\mathfrak{p}]$$

и, согласно предложению 5.3,

$$[L_\mathfrak{P} : K_\mathfrak{p}] = e_\mathfrak{P} f_\mathfrak{P}.$$

С этого момента будем считать, что расширение L нормально над K и Γ — его группа Галуа. Так как $S\gamma = S$, то идеалы $\mathfrak{P}\gamma$ ($\gamma \in \Gamma$), сопряженные с простым идеалом $\mathfrak{P}$, будут простыми идеалами кольца S, и если $\mathfrak{P} \mid \mathfrak{p}$, то, очевидно, $\mathfrak{P}\gamma \mid \mathfrak{p}$. Обратно, справедливо

Предложение 10.2. *Все простые идеалы кольца S, лежащие над идеалом $\mathfrak{p} = \mathfrak{P} \cap R$, являются идеалами $\mathfrak{P}\gamma$, сопряженными с простым идеалом $\mathfrak{P}$.*

Доказательство содержит в себе по сути дела частный случай «китайской теоремы об остатках», которую раньше мы не формулировали. Пусть I — произведение простых идеалов кольца S, лежащих над простым идеалом $\mathfrak{p}$ и отличных от $\mathfrak{P}$. Тогда $\mathfrak{P} + I = S$. Поэтому существуют элементы $a \in \mathfrak{P}$, $b \in I$, для которых $a + b = 1$. Пусть $\mathfrak{P}_1 \mid \mathfrak{p}$ и $\mathfrak{P}_1 \neq \mathfrak{P}$. Тогда

$$a \in \mathfrak{P}, \quad a \notin \mathfrak{P}_1.$$

Предположим, что $\mathfrak{P}_1 \neq \mathfrak{P}\gamma$ для всех γ. Тогда

$$a\gamma \in \mathfrak{P}\gamma, \quad a\gamma \notin \mathfrak{P}_1.$$

Беря произведение по всем $\gamma \in \Gamma$, мы получаем, что

$$\prod(a\gamma) \notin \mathfrak{P}_1.$$

Но

$$\prod(a\gamma) = N_{L/K}(a) \in \mathfrak{P} \cap R = \mathfrak{p}.$$

Таким образом, в действительности из $\mathfrak{P}_1 \mid \mathfrak{p}$ вытекает, что $\mathfrak{P}_1 = \mathfrak{P}\gamma$ при некотором γ.

Следствие. *Числа* $e_{\mathfrak{P}}=e$ *и* $f_{\mathfrak{P}}=f$ *зависят только от идеала* $\mathfrak{p}=\mathfrak{P}\cap R$. *Если* g *— число простых идеалов кольца* S, *лежащих над* $\mathfrak{p}$, *то*

$$efg=[L:K]. \tag{3}$$

Операторы $\gamma\in\Gamma$, для которых $\mathfrak{P}\gamma=\mathfrak{P}$, образуют подгруппу $\Gamma_{\mathfrak{P}}\subset\Gamma$, называемую *группой разложения*. Ее элементы характеризуются равенством

$$v_{\mathfrak{P}}(x\gamma)=v_{\mathfrak{P}}(x)$$

для всех $x\in L$ (или для всех $x\in S$). Если $\gamma\in\Gamma$, то очевидно, что

$$\Gamma_{\mathfrak{P}\gamma}=\gamma^{-1}\Gamma_{\mathfrak{P}}\gamma. \tag{4}$$

Предложение 10.3. *Пусть идеал* $\mathfrak{P}$ *лежит над идеалом* $\mathfrak{p}$. *Тогда расширение* $L_{\mathfrak{P}}$ *нормально над* $K_{\mathfrak{p}}$. *Обозначим через* $\Sigma_{\mathfrak{P}}$ *его группу Галуа. Тогда ограничение на множество* L *автоморфизмов* $\sigma\in\Sigma_{\mathfrak{P}}$ *задает изоморфизм*

$$\Sigma_{\mathfrak{P}}\cong\Gamma_{\mathfrak{P}}.$$

Доказательство. Рассмотрим группу $\Sigma_{\mathfrak{P}}$ как группу автоморфизмов расширения $L_{\mathfrak{P}}$, оставляющих неподвижными элементы поля $K_{\mathfrak{p}}$. Элемент $\sigma\in\Sigma_{\mathfrak{P}}$ отображает расширение L в расширение $L_{\mathfrak{P}}$ поля K и оставляет неподвижными элементы из K. Так как L нормально, то $L\sigma=L$. Другими словами, существует единственный элемент $\hat{\sigma}\in\Gamma$, действие которого на L совпадает с действием элемента σ. Более того, в силу предложения 7.2 $v_{\mathfrak{P}}(x\hat{\sigma})=v_{\mathfrak{P}}(x)$ при всех $x\in L$, т. е. $\hat{\sigma}\in\Gamma_{\mathfrak{P}}$. Таким образом, мы получаем гомоморфизм

$$h\colon\ \Sigma_{\mathfrak{P}}\to\Gamma_{\mathfrak{P}},\quad h(\sigma)=\hat{\sigma}. \tag{5}$$

Пусть $\gamma\in\Gamma_{\mathfrak{P}}$. Элемент γ действует на L непрерывно относительно $v_{\mathfrak{P}}$-топологии. Далее, из универсального свойства погружения пополнений следует, что существует элемент $\gamma'=t(\gamma)$ из группы $\Sigma_{\mathfrak{P}}$, определяющий коммутативную диаграмму

$$\begin{array}{ccc} L & \xrightarrow{\gamma} & L \\ \downarrow & & \downarrow \\ L_{\mathfrak{P}} & \xrightarrow{\gamma'} & L_{\mathfrak{P}} \end{array}$$

Таким образом, мы получаем гомоморфизм

$$t:\Gamma_{\mathfrak{P}}\to\Sigma_{\mathfrak{P}},\quad t(\gamma)=\gamma',$$

для которого отображения $h\circ t$ и $t\circ h$ являются тождественными. Следовательно, в действительности h — изоморфизм.

Теперь мы должны лишь показать, что порядок группы $\Sigma_{\mathfrak{P}}$, совпадающий с порядком группы $\Gamma_{\mathfrak{P}}$, равен степени $[L_{\mathfrak{P}}:K_{\mathfrak{p}}]=e_{\mathfrak{P}}f_{\mathfrak{P}}=ef=[L:K]/g$ (см. следствие из предложения 10.2), т. е. индекс $[\Gamma:\Gamma_{\mathfrak{P}}]$ равен g. Но это следует из определения группы $\Gamma_{\mathfrak{P}}$ и предложения 10.2.

Теперь мы можем дать определение *групп ветвления* расширения L/K. Отождествим группу $\Gamma_{\mathfrak{P}}$ с группой Галуа расширения $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ и определим $\Gamma_{\mathfrak{P},i}$ сначала локально, как в § 9. Так как множество S плотно в каждом пополнении, то

$$\Gamma_{\mathfrak{P},i}=\{\gamma\in\Gamma_{\mathfrak{P}}\mid v_{\mathfrak{P}}(x\gamma-x)\geqslant i+1 \text{ при всех } x\in S\}.$$

Для $i\geqslant 0$ можно сверх того показать, что

$$\Gamma_{\mathfrak{P},i}=\{\gamma\in\Gamma\mid v_{\mathfrak{P}}(x\gamma-x)\geqslant i+1 \text{ при всех } x\in S\}.$$

ЛИТЕРАТУРА

Зарисский, Самюэль (Zarisski O., Samuel P.)
[1] Commutative algebra, London — New York, 1958. (Русский перевод: Зарисский О., Самюэль П., Коммутативная алгебра, ИЛ, М., 1963.)

Нётер (Noether E.)
[2] Normalbasis bei Körpern ohne höhere Verzweigung, *J. reine und angew. Math.*, **167** (1932), 147—152.

Серр (Serre J.-P.)
[3] Corps locaux, Paris, Hermann, 1962.

Суон (Swan R. S.)
[4] Induced representations and projective modules, *Ann. Math.*, **71** (1960), 552—578. (Русский перевод: *Математика*, 8:1 (1964), 3—29.)

ГЛАВА II

Глобальные поля

Дж. Касселс

§ 1. НОРМИРОВАНИЯ

Мы ограничимся только нормированиями ранга 1, так что термин «нормирование» всегда будет означать «нормирование ранга 1».

Определение. *Нормированием* $|\ |$ *поля* k *называется функция, определенная на* k, *принимающая неотрицательные вещественные значения и удовлетворяющая следующим аксиомам*:

1. $|\alpha| = 0$ *тогда и только тогда, когда* $\alpha = 0$,
2. $|\alpha\beta| = |\alpha|\,|\beta|$,
3. *существует константа* C, *такая, что* $|1 + \alpha| \leqslant C$ *при* $|\alpha| \leqslant 1$.

Определение. *Тривиальным нормированием поля* k *называется такое нормирование, что* $|\alpha| = 1$ *для всех* $\alpha \neq 0$.

Замечание. Тривиальное нормирование часто будет исключаться из рассмотрения.

Из аксиомы 2 следует равенство

$$|1| = |1|\,|1|,$$

так что $|1| = 1$ в силу аксиомы 1. Если некоторая степень элемента $\omega \in k$ равна 1, например, $\omega^n = 1$, то $|\omega| = 1$ в силу аксиомы 2. В частности, единственным нормированием конечного поля является тривиальное.

Аналогично показывается, что $|-1| = 1$ и, следовательно,

$$|-\alpha| = |\alpha| \text{ для всех } \alpha \in k.$$

Определение. *Два нормирования* $|\ |_1$, $|\ |_2$ *поля* k *называются эквивалентными, если существует* $c > 0$, *такое, что для всех* $\alpha \in k$

$$|\alpha|_2 = |\alpha|_1^c. \tag{1}$$

Замечание. Если $|\alpha|_1$ — нормирование, то $|\alpha|_2$, определенное по формуле (1),— тоже нормирование. Определенная нами эквивалентность нормирований является, очевидно, отношением эквивалентности.

Легко видеть, что всякое нормирование эквивалентно нормированию с константой $C = 2$. Для такого нормирования можно доказать [1]) «неравенство треугольника»:

$3'$. $|\beta + \gamma| \leqslant |\beta| + |\gamma|$,

[1]) В действительности мы ограничимся нормированиями, удовлетворяющими аксиоме 3 при $C = 1$, для которых условие $3'$ тривиально (см. следующий параграф), или нормированиями, эквивалентными обычной абсолютной величине вещественных или комплексных чисел — для них справедливость условия $3'$ хорошо известна. Мы (следуя Артину) используем аксиому 3 вместо $3'$ лишь по той технической причине, что хотим называть нормированием также квадрат модуля комплексного числа. Однако для полноты изложения мы приведем вывод условия $3'$ из аксиомы 3 при $C = 2$. Во-первых, $|\alpha_1 + \alpha_2| \leqslant 2 \max\{|\alpha_1|, |\alpha_2|\}$ (достаточно положить $\alpha_2 = \alpha\alpha_1$, если, скажем, $|\alpha_1| \geqslant |\alpha_2|$). Далее, по индукции

$$\Big|\sum_{j=1}^{2^r} \alpha_j\Big| \leqslant 2^r \max|\alpha_j|,$$

так что для любого $n > 0$ мы получаем, что

$$\Big|\sum_{j=1}^{n} \alpha_j\Big| \leqslant 2^r \cdot \max|\alpha_j| \leqslant 2n \cdot \max|\alpha_j|,$$

если $2^{r-1} < n \leqslant 2^r$ (мы добавили $2^r - n$ нулевых слагаемых). В частности,

$$|n| \leqslant 2n\,|1| = 2n \ (n > 0),$$

но тогда

$$|\beta+\gamma|^n = \Big|\sum_{j=1}^{n} \binom{n}{j} \beta^j \gamma^{n-j}\Big| \leqslant 2(n+1) \max \binom{n}{j} |\beta|^j |\gamma|^{n-j} <$$

$$< 4\,(n+1) \max \binom{n}{j} \cdot |\beta|^j |\gamma|^{n-j} \leqslant 4(n+1)(|\beta|^n + |\gamma|^n).$$

Извлекая из обеих частей неравенства корень n-й степени и совершая предельный переход при $n \to \infty$, мы получаем неравенство $3'$.

Обратно, условия 1, 2 и 3′ тривиальным образом влекут за собой условие 3, причем можно положить $C = 2$. Вначале мы будем рассматривать почти исключительно свойства нормирований, не зависящие от замены нормирования на эквивалентное, так что часто будем использовать аксиому 3′ вместо 3.

Для дальнейшего нам понадобится формальное следствие неравенства 3′:

$$|| \beta | - | \gamma || \leqslant | \beta - \gamma |$$

(здесь внешние вертикальные черточки в левой части обозначают обычную абсолютную величину). Для доказательства достаточно применить неравенство треугольника к тождествам

$$\beta = \gamma + (\beta - \gamma), \quad \gamma = \beta + (\gamma - \beta).$$

§ 2. ТИПЫ НОРМИРОВАНИЙ

Определим два важных понятия, относящихся к нормированиям; оба они инвариантны относительно перехода к эквивалентным нормированиям.

Определение. *Нормирование* $| \ |$ *называется дискретным, если найдется* $\delta > 0$, *такое, что условие* $1 - \delta < | \alpha | < 1 + \delta$ *влечет за собой равенство* $| \alpha | = 1$.

Иначе говоря, требуется, чтобы множество значений $\log \alpha$, где $a \in k$, $a \neq 0$, было дискретной подгруппой группы вещественных чисел по сложению. Такая подгруппа обязательно будет свободной подгруппой с одной образующей, т. е. найдется число $c < 1$, такое, что $| \alpha |$, где $\alpha \neq 0$, пробегает в точности множество $\{c^m;\ m \in \mathbf{Z}\}$. Если $| \alpha | = c^m$, мы назовем число $m = m(\alpha)$ *порядком* элемента α ($\mathrm{ord}(\alpha)$). Из аксиомы 2 вытекает равенство

$$\mathrm{ord}(\alpha\beta) = \mathrm{ord}(\alpha) + \mathrm{ord}(\beta).$$

Определение. *Нормирование* $| \ |$ *называется неархимедовым, если в аксиоме* 3 *можно положить* $C = 1$, *т. е. если*

$$| \beta + \gamma | \leqslant \max \{| \beta |, | \gamma |\}. \qquad (1)$$

В противном случае нормирование называется архимедовым.

Отметим сразу следствие условия (1):

$$| \beta + \gamma | = | \beta |, \quad \text{если} \quad | \gamma | < | \beta |.$$

Действительно, из (1) мы получаем

$$| \beta | = | (\beta + \gamma) - \gamma | \leqslant \max \{| \beta + \gamma |, | \gamma |\}.$$

В случае неархимедовых нормирований множество тех α, для которых $| \alpha | \leqslant 1$, является, очевидно, кольцом; его называют *кольцом целых элементов* и обозначают символом $\mathfrak{o}$. Два неархимедовых нормирования поля k эквивалентны тогда и только тогда, когда им соответствует одно и то же кольцо целых элементов; действительно, $| \beta | < | \gamma |$ имеет место тогда и только тогда, когда $\beta\gamma^{-1} \in \mathfrak{o}$, $\beta^{-1}\gamma \notin \mathfrak{o}$ (ср. § 4).

Множество элементов α таких, что $| \alpha | < 1$, образует идеал $\mathfrak{p}$ в кольце $\mathfrak{o}$, причем, очевидно, максимальный. Он состоит в точности из тех $\alpha \in \mathfrak{o}$, для которых $\alpha^{-1} \notin \mathfrak{o}$.

Обозначения $\mathfrak{o}$ и $\mathfrak{p}$ будут употребляться все время. Читатель легко докажет следующую лемму.

Лемма 2.1. *Пусть нормирование* $| \ |$ *неархимедово. Тогда оно дискретно в том и только том случае, когда идеал* $\mathfrak{p}$ *— главный.*

В дальнейшем нам понадобится еще одна лемма.

Лемма 2.2. *Для того чтобы нормирование* $| \ |$ *было неархимедовым, необходимо и достаточно условие:* $| n | \leqslant 1$ *для всех элементов* n *из кольца, порожденного в поле* k *его единичным элементом.*

Замечание. Это кольцо нельзя отождествить с $\mathbf{Z}$, если k имеет ненулевую характеристику.

Доказательство. Необходимость очевидна. Чтобы доказать достаточность, положим $| \alpha | \leqslant 1$; тогда в силу неравенства треугольника

$$| 1 + \alpha |^n = | (1 + \alpha)^n | \leqslant \sum_{j=0}^{n} \binom{n}{j} | \alpha | \leqslant 1 + 1 + \ldots + 1 = n,$$

откуда предельным переходом при $n \to \infty$ убеждаемся, что $| 1 + \alpha | \leqslant 1$.

Следствие. *Если* $\operatorname{char} k = p \neq 0$, *то любое нормирование поля* k *неархимедово.*

В самом деле, кольцо, порожденное в k единичным элементом, есть поле $\mathbf{F}$, состоящее из p элементов. Если $b \in \mathbf{F}$, то $b^{p-1} = 1$, так что $|b| = 1$.

§ 3. ПРИМЕРЫ НОРМИРОВАНИЙ

Характернейшим примером архимедова нормирования является нормирование поля $\mathbf{C}$ комплексных чисел с помощью абсолютной величины. Оно замечательно следующим:

Теорема 3.1 (Гельфанд — Торнхейм). *Любое поле* k *с архимедовым нормированием изоморфно вкладывается в* $\mathbf{C}$ *так, что нормирование поля* k *оказывается эквивалентным нормированию, индуцированному абсолютной величиной в* $\mathbf{C}$.

Мы не доказываем этого факта, так как он нам не понадобится. См., например, [2], стр. 45 и 67.

Примеров неархимедовых нормирований можно привести очень много. В поле рациональных чисел $\mathbf{Q}$ для каждого простого числа p можно определить *p-адическое нормирование*:

$$|p^a u/v|_p = p^{-a},$$

где $a, u, v \in \mathbf{Z}$, $p \nmid u$, $p \nmid v$. При этом имеет место следующая

Теорема 3.2 (Островский). *Любое нетривиальное нормирование поля* $\mathbf{Q}$ *эквивалентно одному из p-адических нормирований* $|\ |_p$ *или обычной абсолютной величине* $|\ |_\infty$.

Доказательство. Пусть $|\ |$ — нетривиальное нормирование поля $\mathbf{Q}$, удовлетворяющее (что можно предположить без ограничения общности) неравенству треугольника.

Пусть $a \in \mathbf{Z}$ и $a > 1$. Всякое $b \in \mathbf{Z}$ может быть представлено в виде

$$b = b_m a^m + b_{m-1} a^{m-1} + \ldots + b_0,$$

где

$$0 \leqslant b_j < a \qquad (0 \leqslant j \leqslant m)$$

и

$$m \leqslant \log b / \log a.$$

В силу неравенства треугольника

$$|b| \leqslant \mathscr{M}\,[(\log b/\log a) + 1] \max\{1, |a|^{\log b/\log a}\},$$

где

$$\mathscr{M} = \max_{1 \leqslant d \leqslant 0} |d|.$$

Полагая $b = c^n$ и устремляя $n \to \infty$, мы получаем

$$|c| \leqslant \max\{1, |a|^{\log c/\log a}\}. \tag{1}$$

Первый случай. В поле $\mathbf{Z}$ найдется $c > 1$, такое, что $|c| > 1$. Тогда $|a| > 1$ для каждого $a > 1$ из $\mathbf{Z}$ и условие (1) дает

$$|c|^{1/\log c} = |a|^{1/\log a}.$$

Следовательно, нормирование $|\ |$ эквивалентно обычной абсолютной величине.

Второй случай. $|c| \leqslant 1$ для всех $c \in \mathbf{Z}$; тогда по предыдущей лемме нормирование $|\ |$ неархимедово. Но так как оно нетривиально, то множество $\mathfrak{a}$ тех элементов $a \in \mathbf{Z}$, для которых $|a| < 1$, не пусто и является, очевидно, $\mathbf{Z}$-идеалом. Так как $|bc| = |b|\,|c|$, то идеал $\mathfrak{a}$ — простой; пусть он порожден числом $p > 0$. Тогда нормирование $|\ |$ эквивалентно, очевидно, нормированию $|\ |_p$.

Пусть теперь k_0 — любое поле, и пусть $k = k_0(t)$, где t трансцендентно. Если $p = p(t)$ — неприводимый многочлен в кольце $k[t]$, то мы определим нормирование поля k формулой

$$|p(t)^a u(t)/v(t)|_p = c^{-a}, \tag{2}$$

где $c < 1$ фиксировано, $a \in \mathbf{Z}$ и $u(t), v(t) \in k_0[t]$, $p(t) \nmid u(t)$, $p(t) \nmid v(t)$.

Кроме этого, существует неархимедово нормирование $|\ |_\infty$, определяемое формулой

$$|u(t)/v(t)|_\infty = c^{\deg v - \deg u}. \tag{3}$$

Отметим аналогию между $k_0(t)$ и $\mathbf{Q}$, которая, однако, не является полной. Если положить $s = t^{-1}$, так что $k_0(t) = k_0(s)$, то нормирование $|\ |_\infty$ принимает вид (2) с многочленом $p(s) = s$.

Читатель легко докажет следующую лемму.

Лемма 3.1. *Любое нетривиальное нормирование поля $k_0(t)$, которое тривиально на k_0, эквивалентно одному из нормирований вида* (2) *или* (3).

Следствие. *Если* $\mathbf{F}$ *— конечное поле, то все нетривиальные нормирования поля* $\mathbf{F}(t)$ *исчерпываются с точностью до эквивалентности нормированиями вида* (2) *или* (3).

§ 4. ТОПОЛОГИЯ

Нормирование $|\ |$ поля k индуцирует топологию, в которой базой окрестностей $\alpha \in k$ являются «открытые сферы»

$$S_d(\alpha) = \{\xi \mid |\xi - \alpha| < d\}$$

для всех $d > 0$. Эквивалентные нормирования индуцируют одну и ту же топологию. Нормирование, удовлетворяющее неравенству треугольника, задает метрику для этой топологии, если определить расстояние от α до β как $|\alpha - \beta|$.

Лемма 4.1. *Поле с топологией, индуцированной некоторым нормированием, является топологическим полем, т. е. операции сложения, умножения и взятия обратного элемента в этом поле непрерывны.*

Доказательство. Рассмотрим, например, операцию умножения; из неравенства треугольника следует, что

$$|(\alpha + \theta)(\beta + \phi) - \alpha\beta| \leqslant$$
$$\leqslant |\theta|\,|\phi| + |\alpha|\cdot|\phi| + |\beta|\cdot|\theta|,$$

и потому левая часть мала, коль скоро малы $|\theta|$ и $|\phi|$ (α и β фиксированы).

Лемма 4.2. *Если два нормирования $|\ |_1$, $|\ |_2$ одного и того же поля индуцируют одну и ту же топологию, то они эквивалентны в смысле данного выше определения.*

Доказательство. Условие $|\alpha| < 1$ выполняется тогда и только тогда, когда $\alpha^n \to 0$ $(n \to \infty)$ в смысле индуцированной нормированием $|\ |$ топологии, так что неравенство $|\alpha|_1 < 1$ равносильно неравенству $|\alpha|_2 < 1$. Переходя к обратным элементам, мы получаем, что неравенство $|\alpha|_1 > 1$ равносильно неравенству $|\alpha|_2 = 1$; следовательно, наконец, равенство $|\alpha|_1 = 1$ равносильно равенству $|\alpha|_2 = 1$.

Пусть теперь $\beta, \gamma \in k$ и $\beta \neq 0$, $\gamma \neq 0$. Применяя предыдущее рассуждение к элементу

$$\alpha = \beta^m \cdot \gamma^n \qquad (m, n \in \mathbf{Z}),$$

мы видим, что

$$m \log|\beta|_1 + n \log|\gamma|_1 \geqslant 0$$

имеет место тогда и только тогда, когда

$$m \log|\beta|_2 + n \log|\gamma|_2 \geqslant 0,$$

так что

$$\log|\beta|_1/\log|\beta|_2 = \log|\gamma|_1/\log|\gamma|_2.$$

§ 5. ПОЛНОТА

Поле k называется *полным* по отношению к нормированию $|\ |$, если оно полно как метрическое пространство по отношению к метрике $|\alpha - \beta|$, где $\alpha, \beta \in k$, т. е. если для каждой последовательности α_n $(n = 1, 2, \ldots)$, такой, что

$$|\alpha_m - \alpha_n| \to 0 \qquad (m, n \to \infty, \infty)$$

(фундаментальная последовательность), существует $\alpha^* \in k$, такое, что

$$\alpha_n \to \alpha^* \text{ в смысле нормирования } |\ |$$

(т. е. $|\alpha_n - \alpha^*| \to 0$).

Теорема 5.1. *Всякое поле k с нормированием $|\ |$ может быть погружено в полное поле $\bar{k}$ с нормированием $|\ |$, продолжающим исходное таким образом, что $\bar{k}$ является замыканием поля k по отношению к нормированию $|\ |$. Более того, поле $\bar{k}$ для данного k единственно (с точностью до изоморфизма).*

Доказательство (мы даем лишь набросок). Определим $\bar{k}$ (как метрическое пространство) как пополнение k (как метрического пространства) по отношению к нормированию $|\ |$. Так как операции сложения, умножения и взятия обратного элемента непрерывны в поле k, то они корректно определены в $\bar{k}$. Отсюда и вытекает теорема.

Следствие 1. *Нормирование* $|\ |$ *неархимедово в поле* $\bar{k}$ *тогда и только тогда, когда оно неархимедово в поле* k. *Если это имеет место, то множества значений, принимаемых нормированием* $|\ |$ *на элементах полей* k *и* $\bar{k}$, *совпадают.*

Доказательство. Используем лемму 2.2. Предположим, что нормирование $|\ |$ поля k неархимедово, тогда неравенство

$$|\beta+\gamma| \leqslant \max\{|\beta|, |\gamma|\}$$

выполняется по непрерывности также и для любых элементов из k. Далее, если $\beta \in \bar{k}$, $\beta \neq 0$, то найдется $\gamma \in k$, такое, что $|\beta-\gamma| \leqslant |\beta|$ и, значит, $|\beta| = |\gamma|$. Обратное утверждение тривиально.

Следствие 2. *Любое сохраняющее нормирование погружение поля* k *в полное поле* K *может быть единственным образом продолжено до погружения поля* $\bar{k}$.

§ 6. НЕЗАВИСИМОСТЬ

Следующая лемма показывает, что неэквивалентные нормирования в действительности почти совершенно независимы. Для наших целей, впрочем, будет нужен более сильный результат из § 15.

Лемма 6.1. («Слабая аппроксимационная теорема».) Пусть $|\ |_n$ $(1 \leqslant n \leqslant N)$ — *неэквивалентные нетривиальные нормирования поля* k. *Для каждого* n *обозначим через* k_n *топологическое пространство, состоящее из множества элементов поля* k, *с топологией, индуцированной нормированием* $|\ |_n$. *Пусть* Δ — *образ поля* k *в топологическом произведении* $\Pi = \prod\limits_{1 \leqslant n \leqslant N} k_n$ (*с топологией прямого произведения*). *Тогда* Δ *всюду плотно в пространстве* Π.

Утверждение леммы может быть выражено в менее топологических терминах: пусть заданы какие-нибудь элементы $\alpha_n \in k$ $(1 \leqslant n \leqslant N)$ и вещественное число $\varepsilon > 0$; тогда найдется элемент $\xi \in k$, такой, что одновременно для всех $n = 1, \ldots, N$ имеет место

$$|\alpha_n - \xi|_n < \varepsilon.$$

Замечание. Если $k = \mathbf{Q}$ и нормирования $|\ |_n$ являются p-адическими нормированиями, то это утверждение превращается в «китайскую теорему об остатках»; однако настоящим обобщением последней является сильная аппроксимационная теорема (§ 15).

Доказательство. Заметим вначале, что достаточно будет найти $\theta_n \in k$, такие, что

$$|\theta_n|_n > 1, \quad |\theta_n|_m < 1 \quad (m \neq n), \tag{1}$$

где $1 \leqslant n \leqslant N$, $1 \leqslant m \leqslant N$. В самом деле, тогда при $r \to \infty$ мы будем иметь

$$\frac{\theta_n^r}{1+\theta_n^r} = \frac{1}{1+\theta_n^{-r}} \to \begin{cases} 1 \text{ в смысле нормирования } |\ |_n, \\ 0 \text{ в смысле нормирования } |\ |_m,\ m \neq n, \end{cases}$$

и, следовательно, для достаточно большого r

$$\xi = \sum_{n=1}^{N} (\theta_n^r/(1+\theta_n^r))\,\alpha_n.$$

В силу симметричности достаточно показать существование такого $\theta = \theta_1$, что

$$|\theta|_1 > 1, \quad |\theta|_n < 1 \qquad (2 \leqslant n \leqslant N).$$

Применим индукцию по N.

Пусть $N = 2$. Так как нормирования $|\ |_1$ и $|\ |_2$ неэквивалентны, то найдется α, такое, что

$$|\alpha|_1 < 1, \quad |\alpha|_2 \geqslant 1,$$

и аналогично β, такое, что

$$|\beta|_1 \geqslant 1, \quad |\beta|_2 < 1,$$

и, значит, можно положить $\theta = \beta\alpha^{-1}$.

Пусть $N \geqslant 3$. По предположению индукции найдется $\phi \in k$, такое, что

$$|\phi|_1 > 1, \quad |\phi|_n < 1 \qquad (2 \leqslant n \leqslant N-1),$$

а согласно случаю $N=2$, найдется $\psi \in k$, такое, что $|\psi|_1 > 1$, $|\psi|_N < 1$.

Тогда положим

$$\theta = \begin{cases} \phi, & \text{если } |\phi|_N < 1; \\ \phi^r\psi, & \text{если } |\phi|_N = 1; \\ \phi^r\psi/(1+\phi^r), & \text{если } |\phi|_N > 1, \end{cases}$$

где $r \in \mathbf{Z}$ — достаточно большое число.

§ 7. СЛУЧАЙ КОНЕЧНОГО ПОЛЯ ВЫЧЕТОВ

Пусть k — поле с неархимедовым нормированием $|\ |$. Тогда множество элементов $\alpha \in k$, таких, что $|\alpha| \leqslant 1$, образует кольцо $\mathfrak{o}$, которое мы назвали кольцом целых элементов нормирования $|\ |$. Множество элементов $\varepsilon \in k$, таких, что $|\varepsilon| = 1$, является группой по умножению, называемой группой единиц. Наконец, множество элементов $\alpha \in k$, для которых $|\alpha| < 1$, является максимальным идеалом $\mathfrak{p}$, так что факторкольцо $\mathfrak{o}/\mathfrak{p}$ — поле. Мы рассмотрим случай, когда поле $\mathfrak{o}/\mathfrak{p}$ имеет конечное число P элементов.

Предположим далее, что нормирование $|\ |$ дискретно. Тогда $\mathfrak{p}$ является главным идеалом. Если $\mathfrak{p} = (\pi)$, то всякий элемент $\alpha \in k$ имеет вид $\alpha = \pi^v\varepsilon$, где ε — единица кольца $\mathfrak{o}$. Мы назовем число v *порядком* элемента α. Если одновременно $\mathfrak{p} = (\pi')$, то π/π' есть единица, и обратно; таким образом, порядок элемента α не зависит от выбора π.

Пусть $\bar{\mathfrak{o}}$, $\bar{\mathfrak{p}}$ аналогично определены для пополнения $\bar{k}$ поля k. Тогда, очевидно, $\bar{\mathfrak{o}}/\bar{\mathfrak{p}} = \mathfrak{o}/\mathfrak{p}$ и $\bar{\mathfrak{p}} = (\pi)$ (в смысле равенства $\bar{\mathfrak{o}}$-идеалов).

Лемма 7.1. *Пусть поле k полно относительно нормирования $|\ |$; тогда $\mathfrak{o}$ состоит из тех и только тех элементов α, которые могут быть записаны в виде*

$$\alpha = \sum_{j=0}^{\infty} a_j\pi^j, \qquad (1)$$

где a_j пробегают независимо друг от друга некоторое множество Σ представителей факторкольца $\mathfrak{o}/\mathfrak{p}$ в кольце $\mathfrak{o}$.

Формула (1) понимается, конечно, в смысле предела фундаментальной последовательности $\sum_{j=0}^{J} a_j\pi^j$ при $J \to \infty$.

В самом деле, существует единственным образом определенный элемент $a_0 \in \Sigma$, такой, что $|\alpha - a_0| < 1$.

Тогда $\alpha_1 = \pi^{-1}(\alpha - a_0) \in \mathfrak{o}$. Определим теперь $a_1 \in \Sigma$ так, чтобы имело место $|\alpha_1 - a_1| < 1$. Этот процесс можно продолжить неограниченно.

Теорема 7.1. *При условиях леммы 7.1 кольцо $\mathfrak{o}$ компактно в $|\ |$-топологии.*

Доказательство. Пусть $\{O_\lambda\}_{\lambda\in\Lambda}$ — некоторое семейство открытых множеств, покрывающих кольцо $\mathfrak{o}$. Мы должны показать, что найдется конечное подпокрытие. Предположим противное. Пусть Σ — множество представителей факторкольца $\mathfrak{o}/\mathfrak{p}$; тогда $\mathfrak{o}$ является объединением конечного числа множеств вида $a + \pi\mathfrak{o}$ ($a \in \Sigma$). Таким образом, по крайней мере для одного $a_0 \in \Sigma$ множество $a_0 + \pi\mathfrak{o}$ не покрывается конечным подсемейством из $\{O_\lambda\}$. Аналогично найдется $a_1 \in \Sigma$, такое, что $a_0 + a_1\pi + \pi^2\mathfrak{o}$ не допускает конечного покрытия. И так далее. Пусть $\alpha = a_0 + \pi a_1 + \dots$. Тогда $\alpha \in O_{\lambda_0}$ для некоторого $\lambda_0 \in \Lambda$. Так как множество O_{λ_0} открыто, то при некотором J имеет место $\alpha + \pi^J\mathfrak{o} \subset O_{\lambda_0}$. Мы получили противоречие.

Следствие. *Поле k локально компактно.*

(Обратное также верно. Если поле k локально компактно в топологии, индуцированной неархимедовым нормированием $|\ |$, то
1) k полно,
2) поле вычетов конечно,
3) нормирование $|\ |$ дискретно.
В самом деле, найдется компактная окрестность c нуля. Тогда $\pi^v\mathfrak{o} \subset c$ для достаточно большого v, так что множество $\pi^v\mathfrak{o}$ компактно, так как оно замкнуто. Значит, $\mathfrak{o}$ компактно. Так как нормирование $|\ |$ — метрика, то $\mathfrak{o}$ является секвенциальным компактом, т. е. любая фундаментальная последовательность в $\mathfrak{o}$ имеет предел, из чего вытекает 1). Пусть a_λ ($\lambda \in \Lambda$) будет множеством представителей факторкольца $\mathfrak{o}/\mathfrak{p}$ в $\mathfrak{o}$. Тогда $O_\lambda = \{|\xi - a_\lambda| < 1\}$ — открытое покрытие кольца $\mathfrak{o}$. Следовательно, 2) выполняется, поскольку $\mathfrak{o}$ компактно. Наконец, $\mathfrak{p}$ компактно как замкнутое подмножество

компактного множества $\mathfrak{o}$. Пусть S_n будет множеством всех $\alpha \in k$, для которых $|\alpha| < 1 - 1/n$. Тогда $\{S_n: 1 \leqslant n < \infty\}$ будет открытым покрытием идеала $\mathfrak{p}$, так что для некоторого n имеет место $\mathfrak{p} = S_n$, т. е. верно 3).

Если мы предположим нормирование $|\ |$ архимедовым, то единственными возможностями для поля k остаются $k = \mathbf{R}$ или $k = \mathbf{C}$, причем нормирование $|\ |$ эквивалентно абсолютной величине.)

Обозначим через k^+ коммутативную топологическую группу, точками которой являются элементы поля k, композицией является сложение в поле, а топология индуцируется нормированием $|\ |$. Из общей теории следует, что существует инвариантная мера (мера Хаара), определенная на k^+, и что эта мера единственна с точностью до мультипликативной константы. Мы можем легко узнать, что представляет собой эта мера μ.

Так как мера μ инвариантна, то

$$\mu(\alpha + \pi^v\mathfrak{o}) = \mu_v$$

не зависит от α. Далее,

$$\alpha + \pi^v\mathfrak{o} = \bigcup_{1 \leqslant j \leqslant P} (\alpha + \pi^v a_j + \pi^{v+1}\mathfrak{o}),$$

где $a_j (1 \leqslant j \leqslant P)$ — множество представителей фактор-кольца $\mathfrak{o}/\mathfrak{p}$. Поэтому

$$\mu_v = P \cdot \mu_{v+1}.$$

Если мы нормализуем меру μ, положив

$$\mu(\mathfrak{o}) = 1, \tag{2}$$

то получим, что

$$\mu_v = P^{-v}.$$

Обратно, не прибегая к теории меры Хаара, легко видеть, что существует единственная инвариантная мера на группе k^+, удовлетворяющая условию (2).

Все, о чем говорилось до этого, относилось по сути дела не к отдельным нормированиям, а к классам эквивалентных нормирований. Однако в свете предыдущих рассмотрений представляется целесообразным выделить в каждом классе одно особенно важное нормирование.

Определение. *Пусть k — поле с дискретным нормированием $|\ |$ и полем классов вычетов, состоящим из $P < \infty$ элементов. Мы будем говорить, что нормирование $|\ |$ нормализовано, если*

$$|\pi| = P^{-1},$$

где $\mathfrak{p} = (\pi)$.

Теорема 7.2. *Пусть поле k полно относительно нормализованного нормирования $|\ |$. Тогда*

$$\mu(\alpha + \beta\mathfrak{o}) = |\beta|,$$

где μ — мера Хаара на k^+, нормализованная условием $\mu(\mathfrak{o}) = 1$.

Суть этой теоремы может быть выражена более подробно. Пусть $\beta \in k$, $\beta \neq 0$, и пусть μ будет мерой Хаара на k^+ (не обязательно нормализованной, как в условиях теоремы). Тогда на группе k^+ можно определить новую меру Хаара μ_β, положив $\mu_\beta(E) = \mu(\beta E)$ $(E \subset k^+)$. Но мера Хаара единственна с точностью до мультипликативной константы и, следовательно, $\mu_\beta(E) = \mu(\beta E) = f\mu(E)$ для всех измеримых множеств E, где множитель f зависит только от β. Теорема утверждает, что f равно $|\beta|$ в нормализованном нормировании.

(В теории локально компактных топологических групп вводится в рассмотрение двойственная к группе k^+ группа (группа характеров). Оказывается, что она изоморфна группе k^+. Для теории полей классов нам этот факт не нужен, так что мы его здесь не доказываем. Доказательство и приложения см. [10]; обобщения см. [6] и [8]. Определение группы характеров для k^* составляет предмет локальной теории полей классов.)

Множество ненулевых элементов поля k образует группу k^* относительно умножения. Очевидно, что операции умножения и взятия обратного элемента непрерывны в топологии, индуцированной в k^* как в подмножестве поля k, так что k^* есть топологическая группа в этой топологии [1]). При этом

$$k^* \supset E \supset E_1,$$

где E — группа единиц поля k, а E_1 — группа главных единиц, т. е. таких элементов $\varepsilon \in k$, что $|1 - \varepsilon| < 1$. Ясно, что подгруппы E и E_1 обе открыты и замкнуты в k^*.

[1]) Позже мы будем рассматривать случай топологического кольца R, где в R^* задана топология, вообще говоря, отличная от топологии подмножества.

Очевидно, что группа k^*/E изоморфна аддитивной группе $\mathbf{Z}^+$ натуральных чисел в дискретной топологии; изоморфизм задается отображением

$$\pi^v E \to v \quad (v \in \mathbf{Z}).$$

Далее, группа E/E_1 изоморфна мультипликативной группе ненулевых элементов поля вычетов, которая рассматривается в дискретной топологии [1]). Далее, так как E компактна, то группа k^* локально компактна. Ясно, что аддитивная мера Хаара инвариантна также относительно умножения на элементы из E_1, так что она индуцирует меру Хаара на E_1; тем самым мы получаем меру Хаара на k^*.

Наконец, отметим следующую лемму.

Лемма 7.2. *Группы k^+ и k^* вполне несвязны (единственными связными подмножествами в них являются точки).*

Доказательство очевидно.

(Быть может, стоит заметить, что k^+ и k^* локально изоморфны, если поле k имеет характеристику 0. Действительно, экспоненциальное отображение

$$\alpha \to \exp \alpha = \sum \frac{\alpha^n}{n!}$$

определено для всех достаточно малых α, а обратное отображение

$$\log \alpha = \sum \frac{(-1)^{n-1} \cdot (\alpha - 1)^n}{n}$$

определено для всех α, достаточно близких к 1.)

[1]) k^* — циклическая группа порядка $P - 1$. Можно показать, что k всегда содержит первообразный корень ρ степени $P - 1$ из единицы и что элементы из k^* однозначно представляются в виде $\pi^v \cdot \rho^u \cdot \varepsilon$, $\varepsilon \in E_1$, т. е. группа k^* есть прямое произведение групп $\mathbf{Z}$, $\mathbf{Z}/(P-1)\mathbf{Z}$ и E_1.

Действительно, пусть $f(X) = X^{P-1} - 1$, и пусть элемент $\alpha \in \mathfrak{o}$ таков, что $\alpha \bmod \mathfrak{p}$ порождает мультипликативную группу ненулевых элементов поля вычетов. Тогда $|f(\alpha)| < 1$, $|f'(\alpha)| = 1$. Значит, по лемме Гензеля (см. добавление B) найдется элемент $\rho \in k$, такой, что $f(\rho) = 0$, $\rho \equiv \alpha \bmod \mathfrak{p}$.

§ 8. НОРМИРОВАННЫЕ ПРОСТРАНСТВА

Определение. *Пусть k — поле с нормированием $|\ |$, и пусть V — векторное пространство над k. Вещественнозначная функция $\|\ \|$ на V называется нормой, если:*

1) $\|\mathfrak{a}\| > 0$ *для* $\mathfrak{a} \in V$, $\mathfrak{a} \neq 0$,
2) $\|\mathfrak{a} + \mathfrak{b}\| \leqslant \|\mathfrak{a}\| + \|\mathfrak{b}\|$,
3) $\|\alpha\mathfrak{a}\| = |\alpha| \cdot \|\mathfrak{a}\|$ $(\alpha \in k, \mathfrak{a} \in V)$.

Определение. *Две нормы $\|\ \|_1$, $\|\ \|_2$ на одном пространстве называются эквивалентными, если существуют константы c_1, c_2, такие, что*

$$\|\mathfrak{a}\|_1 \leqslant c_1 \|\mathfrak{a}\|_2, \quad \|\mathfrak{a}\|_2 \leqslant c_2 \|\mathfrak{a}\|_1.$$

Очевидно, что это действительно есть отношение эквивалентности.

Лемма 8.1. *Предположим, что поле k полно относительно нормирования $|\ |$ и что пространство V конечномерно. Тогда любые две нормы на V эквивалентны.*

Замечание. Как будет видно далее, требование полноты существенно.

Доказательство. Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_N$ — какой-нибудь базис в V. Зададим норму $\|\ \|_0$ формулой

$$\Big\| \sum \xi_n \mathfrak{a}_n \Big\|_0 = \max_n |\xi_n|.$$

Достаточно показать, что любая норма $\|\ \|$ эквивалентна норме $\|\ \|_0$. Очевидно, что

$$\Big\| \sum \xi_n \mathfrak{a}_n \Big\| \leqslant \sum |\xi_n| \cdot \|\mathfrak{a}_n\| \leqslant c_1 \Big\| \sum \xi_n \mathfrak{a}_n \Big\|_0,$$

где

$$c_1 = \sum \|\mathfrak{a}_n\|.$$

Предположим, что не существует числа c_2, такого, что [1])

$$\|\mathfrak{a}\|_0 \leqslant c_2 \|\mathfrak{a}\|.$$

[1]) Если k не только полно относительно нормирования $|\ |$, но и локально компактно — этот случай представляет особый интерес, — то можно упростить рассуждение следующим образом. Как уже было показано, функция $\|\mathfrak{a}\|$ непрерывна в смысле $\|\ \|_0$-топологии и, следовательно, достигает своей нижней границы δ на множестве $\|\mathfrak{a}\|_0 = 1$. Вследствие условия $1\ \delta > 0$, а тогда в силу однородности $\|\mathfrak{a}\|_0 \leqslant \delta^{-1} \|\mathfrak{a}\|$ для всех $\mathfrak{a} \in V$.

Тогда для любого $\varepsilon > 0$ существуют $\xi_1, \ldots, \xi_n$, такие, что

$$0 < \| \sum \xi_n a_n \| \leqslant \varepsilon \max |\xi_n|.$$

Ввиду симметричности мы можем предположить, что

$$\max |\xi_n| = |\xi_N|,$$

и, значит, в силу однородности

$$\xi_N = 1.$$

При $m = 1, 2, \ldots$ мы теперь имеем элементы $\xi_{n,m}$ $(1 \leqslant n \leqslant N-1)$, такие, что

$$\| \sum_{n=1}^{N-1} \xi_{n,m} a_n + a_N \| \to 0 \qquad (m \to \infty),$$

так что

$$\| \sum_{n=1}^{N-1} (\xi_{n,l} - \xi_{n,m}) a_n \| \to 0 \quad (l, m \to \infty, \infty).$$

Лемма тривиальна для $N = 1$; предположим по индукции, что она верна для $(N-1)$-мерного пространства, порожденного векторами $a_1, \ldots, a_{N-1}$, и, следовательно,

$$|\xi_{n,l} - \xi_{n,m}| \to 0 \qquad (l, m \to \infty, \infty)$$

для $1 \leqslant n \leqslant N-1$. Так как k полно, то найдутся $\xi_n^* \in k$, такие, что

$$|\xi_{n,m} - \xi_n^*| \to 0 \qquad (m \to \infty).$$

Тогда

$$\| \sum^{N-1} \xi_n^* a_n + a_N \| \leqslant \| \sum^{N-1} \xi_{n,m} a_n + a_n \| +$$
$$+ \sum^{N-1} |\xi_n^* - \xi_{n,m}| \, \| a_n \| \to 0 \qquad (m \to \infty),$$

что противоречит условию 1.

§ 9. ТЕНЗОРНОЕ УМНОЖЕНИЕ

Нам нужен только один частный случай. Пусть A и B будут коммутативными кольцами, содержащими поле k; предположим, кроме того, что B имеет конечную размерность N над k. Пусть

$$1 = \omega_1, \omega_2, \ldots, \omega_N$$

— базис B над k. Кольцо B определено с точностью до изоморфизма таблицей умножения

$$\omega_l \omega_m = \sum c_{lmn} \omega_n, \quad c_{lmn} \in k.$$

Мы можем определить новое кольцо C, содержащее k, элементами которого являются выражения вида

$$\sum a_m \bar{\omega}_m, \quad a_m \in A,$$

где $\bar{\omega}_m$ имеют тот же закон умножения

$$\bar{\omega}_l \bar{\omega}_m = \sum c_{lmn} \bar{\omega}_n,$$

что и ω_m. Существуют изоморфизмы колец A и B на кольцо C:

$$i\colon a \to a\bar{\omega}_1,$$

$$j\colon \sum \lambda_m \omega_m \to \sum \lambda_m \bar{\omega}_m.$$

Ясно, что C определено с точностью до изоморфизма кольцами A и B и не зависит от конкретного выбора базиса $\{\omega_m\}$. Мы будем писать

$$C = A \otimes_k B,$$

так как это в действительности частный случай тензорного умножения колец.

(Читатель без труда проверит, что кольцо C вместе с отображениями i, j удовлетворяет свойству универсального отображения.)

Предположим далее, что A — топологическое кольцо, т. е. имеет топологию, в которой сложение и умножение непрерывны. Отображение

$$\sum a_m \bar{\omega}_m \to (a_1, \ldots, a_N)$$

является взаимно однозначным соответствием между кольцом C и N экземплярами кольца A (рассматриваемыми как множества). Мы введем в C топологию произведения. Легко проверить, что

(i) эта топология не зависит от выбора базиса $\omega_1, \ldots, \omega_n$;

(ii) умножение и сложение в C непрерывны в этой топологии; таким образом C теперь топологическое кольцо.

Мы назовем эту топологию в C топологией тензорного произведения. Теперь отбросим наше предположение о том, что в A есть топология, но предположим, что A и B являются не просто кольцами, но полями.

Лемма 9.1. *Пусть A и B — поля, содержащие поле k; предположим еще, что B — сепарабельное расширение поля k степени $[B : k] = N < \infty$. Тогда $C = A \otimes_k B$ есть прямая сумма конечного числа полей K_j, каждое из которых содержит изоморфный образ поля A и изоморфный образ поля B.*

Доказательство. По известной теореме (см. добавление Б) $B = k(\beta)$, где $f(\beta) = 0$ для некоторого сепарабельного многочлена $f(X) \in k[X]$ степени N, неприводимого в $k[X]$. Тогда элементы $1, \beta, \ldots, \beta^{N-1}$ образуют базис расширения B/k, и, таким образом, $A \otimes_k B = A[\bar{\beta}]$, где $1, \bar{\beta}, \ldots, \bar{\beta}^{N-1}$ линейно независимы над A и $f(\bar{\beta}) = 0$.

Хотя многочлен $f(X)$ неприводим в $k[X]$, он необязательно будет неприводимым в $A[X]$; пусть

$$f(X) = \prod_{1 \leqslant j \leqslant J} g_i(X),$$

где многочлены $g_i(X) \in A[X]$ неприводимы. Все $g_i(X)$ различны, поскольку $f(X)$ сепарабелен. Пусть $K_j = A(\beta_j)$, где $g_j(\beta_j) = 0$. Ясно, что отображение

$$A \otimes_k B \xrightarrow{\mu_j} K_j,$$

заданное формулой

$$h(\bar{\beta}) \xrightarrow{\mu_j} h(\beta), \quad h(X) \in A[X],$$

является гомоморфизмом колец.

Мы, таким образом, получили кольцевой гомоморфизм

$$A \otimes_k B \xrightarrow{\mu_1 \oplus \ldots \oplus \mu_j} \bigoplus_{1 \leqslant j \leqslant J} K_j. \qquad (1)$$

Пусть $h(\bar{\beta})$, где $h(X) \in A[X]$, лежит в его ядре. Тогда многочлен $h(X)$ делится на каждый многочлен $g_i(X)$ и, следовательно, также и на $f(X)$, т. е. $h(\bar{\beta}) = 0$. Тем самым (1) — вложение. Так как оба кольца в формуле (1) имеют одинаковую размерность как векторные пространства над A, то отображение (1) является изоморфизмом, что и требовалось доказать.

Осталось показать, что гомоморфизмы колец

$$\lambda_j \colon B \longrightarrow A \otimes_k B \xrightarrow{\mu_j} K_j$$

— вложения. Если $\lambda_j(\beta) \neq 0$ для некоторого $\beta \in B$, то $\lambda_j(\beta_1) \neq 0$ для всех $\beta_1 \neq 0$, так как $\lambda_j(\beta) = \lambda_j(\beta_1)\lambda_j(\beta\beta^{-1})$. Значит, все, что нам осталось показать,— это то, что λ_j не отображают все поле B в 0; но это тривиально.

Следствие 1. *Пусть $\alpha \in B$, и пусть $F(X) \in k[X]$, $G_j(X) \in A[X]$ $(1 \leqslant j \leqslant J)$ будут характеристическими многочленами элемента α над k и образов элемента α при отображениях*

$$B \longrightarrow A \otimes_k B \longrightarrow K_j$$

над A соответственно. Тогда

$$F(X) = \prod_{1 \leqslant j \leqslant J} G_j(X). \qquad (2)$$

Доказательство. Мы покажем, что обе части формулы (2) равны характеристическому многочлену $T(X)$ образа элемента α в $A \otimes_k B$ над A. То, что $F(X) = T(X)$, следует сразу из выражения для характеристического многочлена через базис $\bar{\omega}_1, \ldots, \bar{\omega}_N$, где $\omega_1, \ldots, \omega_n$ — базис расширения B над k. Равенство $T(X) = \prod G_j(X)$ получается аналогично использованием базиса кольца $A \otimes_k B = \bigoplus K_j$, составленного из базисов отдельных колец K_j над A.

Следствие 2. *Для $\alpha \in B$ имеют место равенства*

$$\mathrm{Norm}_{B/k}\,\alpha = \prod_{1 \leqslant j \leqslant J} \mathrm{Norm}_{K_j/A}\,\alpha;$$

$$\mathrm{trace}_{B/k}\,\alpha = \sum_{1 \leqslant j \leqslant J} \mathrm{trace}_{K_j/A}\,\alpha.$$

Доказательство. Норма и след равны соответственно второму и последнему коэффициенту характеристического уравнения.

§ 10. ПРОДОЛЖЕНИЕ НОРМИРОВАНИЙ

Пусть k и K — поля, $|\ |$ и $\|\ \|$ — нормирования полей k и K соответственно, и пусть $k \subset K$. Мы скажем, что нормирование $\|\ \|$ продолжает нормирование $|\ |$, если $|b| = \|b\|$ для всех $b \in k$.

Теорема 10.1. *Пусть поле k полно относительно нормирования $|\ |$, и пусть K — расширение поля k степени $[K : k] = N < \infty$. Тогда существует единственное продолжение нормирования $|\ |$ на поле K, а именно*

$$\|\alpha\| = |\operatorname{Norm}_{K/k}\alpha|^{1/N}. \qquad (1)$$

Доказательство. *Единственность.* Поле K можно рассматривать как векторное пространство над полем k; тогда нормирование $\|\ \|$ будет нормой в смысле вышеприведенного определения. Следовательно, два продолжения $\|\ \|_1$ и $\|\ \|_2$ нормирования $|\ |$ эквивалентны как нормы и, значит, индуцируют одинаковую топологию в пространстве K. Но мы видели, что два нормирования, индуцирующие одинаковую топологию в K, являются эквивалентными нормированиями, т. е. $\|\ \|_1 = \|\ \|_2^c$ для некоторого $c \neq 0$. Наконец, $c = 1$, потому что $\|b\|_1 = \|b\|_2$ для всех $b \in k$.

Существование. Доказательство существования в общем случае см. в [2]; для случая сепарабельного поля K и неархимедовых дискретных нормирований см. гл. I, следствие 1 из предложения 4.1. Здесь мы дадим доказательство (предложенное Гейером на конференции), проходящее для случая локально компактного поля k, который единственно нам и интересен. В любом случае легко видеть, что функция, заданная формулой (1), удовлетворяет условиям 1 и 2 из определения нормирования (см. § 1): 1) $\|\alpha\| \geqslant 0$, причем равенство имеет место только при $\alpha = 0$, 2) $\|\alpha\beta\| = \|\alpha\|\,\|\beta\|$. Трудность состоит в том, чтобы показать существование константы C, такой, что из условия $\|\alpha\| \leqslant 1$ следует $\|1 + \alpha\| \leqslant C$. Пусть $\|\ \|_0$ будет любая норма в поле K, рассматриваемом как векторное пространство над полем k. Тогда величина $\|a\|$, определенная формулой (1), является непрерывной ненулевой функцией на компакте $\{\|\alpha\|_0 = 1\}$, так что $\Delta \geqslant \|\alpha\| \geqslant \delta > 0$ для некоторых постоянных Δ и δ. Значит, в силу однородности имеет место

$$\Delta \geqslant \frac{\|\alpha\|}{\|\alpha\|_0} \geqslant \delta > 0 \qquad (\text{для всех } \alpha \neq 0).$$

Предположим теперь, что $\|\alpha\| \leqslant 1$. Тогда $\|\alpha\|_0 \leqslant \delta^{-1}$ и, значит,

$$\|1+\alpha\| \leqslant \Delta\|1+\alpha\|_0 \leqslant \Delta(\|1\|_0 + \|\alpha\|_0) \leqslant \Delta(\|1\|_0 + \delta^{-1}).$$

Постоянную величину $\Delta(\|1\|_0 + \delta^{-1})$ и можно взять в качестве константы C.

Формула. Доказательство существования Гейера содержит также и доказательство формулы (1). Но интересно отметить, что в любом случае формула (1) получается как следствие существования и единственности следующим образом. Пусть $L \supset K$ будет конечным нормальным расширением поля k. Тогда, как показано выше, найдется единственное продолжение нормирования $|\ |$ на поле L, которое мы обозначим также через $\|\ \|$. Если σ — автоморфизм поля L над K, то

$$\|\alpha\|_\sigma = \|\sigma\alpha\|$$

тоже будет продолжением нормирования $|\ |$ на L, так что $\|\ \|_\sigma = \|\ \|$, т. е.

$$\|\sigma\alpha\| = \|\alpha\| \qquad (\text{для всех } \alpha \in L).$$

Но тогда для $\alpha \in K$ имеет место равенство

$$\operatorname{Norm}_{K/k}\alpha = \sigma_1\alpha \cdot \sigma_2\alpha \ldots \sigma_N\alpha,$$

где $\sigma_1, \ldots, \sigma_N$ — автоморфизмы поля L над k. Значит,

$$|\operatorname{Norm}_{K/k}\alpha| = \|\operatorname{Norm}_{K/k}\alpha\| = \prod_{1 \leqslant n \leqslant N} \|\sigma_n\alpha\| = \|\alpha\|^N,$$

что и требовалось доказать.

Следствие 1. *Пусть $\omega_1, \ldots, \omega_N$ — базис поля K над полем k. Тогда найдутся константы c_1 и c_2, такие, что*

$$c_1 \leqslant |\textstyle\sum b_n\omega_n| / \max|b_n| \leqslant c_2,$$

где $b_1, \ldots, b_N$ — любые элементы из k, не все равные нулю.

Доказательство. $|\sum b_n\omega_n|$ и $\max|b_n|$ — две нормы в поле K, рассматриваемом как векторное пространство над полем k.

Следствие 2. *Конечное расширение полного нормированного поля k полно относительно продолжения нормирования.*

Доказательство. Согласно предыдущему следствию, указанное расширение имеет топологию конечномерного пространства над k.

Когда поле k неполно относительно нормирования $|\ |$, положение усложняется.

Теорема 10.2. *Пусть K — сепарабельное расширение поля k степени $[K:k]=N<\infty$. Тогда существует не более чем N продолжений нормирования $|\ |$ на K. Если обозначить их через $\|\ \|_j$ $(1\leqslant j\leqslant J)$, то пусть $\bar{k}$, K_j будут пополнениями поля k, соответственно поля K, относительно нормирования $|\ |$, соответственно $\|\ \|_j$. Тогда имеет место равенство*

$$\bar{k}\otimes_k K=\bigoplus_{1\leqslant j\leqslant J}K_j, \tag{2}$$

справедливое как в алгебраическом, так и в топологическом смысле, если в правой части ввести топологию произведения.

Доказательство. Мы уже знаем, что $\bar{k}\otimes_k K$ имеет вид (2), причем K_j — конечные расширения поля $\bar{k}$. Значит, существует единственное продолжение $|\ |_j^*$ нормирования $|\ |$ на поле K_j, и K_j полно относительно продолженного нормирования. Далее, согласно доказанному ранее, гомоморфизмы колец

$$\lambda_j: K\longrightarrow\bar{k}\otimes_k K\longrightarrow K_j$$

являются вложениями. Поэтому мы получаем продолжение $\|\ \|_j$ нормирования $|\ |$ на поле K, полагая

$$\|\beta\|_j=|\lambda_j(\beta)|_j^*.$$

Далее, $K\cong\lambda_j(K)$ плотно в поле K_j относительно нормирования $\|\ \|_j$, потому что $K=k\otimes_k K$ плотно в $\bar{k}\otimes_k K$. Значит, поле K_j является в точности пополнением поля K.

Осталось показать, что нормирования $\|\ \|_j$ различны и что они являются единственными продолжениями нормирования $|\ |$ на поле K.

Пусть $\|\ \|$ будет нормированием поля K, продолжающим нормирование $|\ |$. Тогда $\|\ \|$ продолжается по непрерывности до вещественнозначной функции на $\bar{k}\otimes_k K$, которую мы также обозначим через $\|\ \|$. В силу непрерывности

$$\left.\begin{aligned}\|\alpha+\beta\|&\leqslant\max\{\|\alpha\|,\ \|\beta\|\}\\ \|\alpha\cdot\beta\|&=\|\alpha\|\ \|\beta\|\end{aligned}\right\}\quad\alpha,\beta\in\bar{k}\otimes K.$$

Мы рассмотрим ограничение нормирования $\|\ \|$ на одно из полей K_j. Если $\|\alpha\|\neq 0$ для некоторого $\alpha\in K_j$, то $\|\alpha\|=\|\beta\|\,\|\alpha\beta^{-1}\|$ для каждого $\beta\neq 0$ из K_j, так что $\|\beta\|\neq 0$. Тогда функция $\|\ \|$ либо тождественно равна 0 на K_j, либо индуцирует нормирование поля K_j.

Далее, функция $\|\ \|$ не может индуцировать нормирования на *двух* полях K_j, потому что

$$(\alpha_1\oplus 0\oplus\ldots\oplus 0)\cdot(0\oplus\alpha_2\oplus 0\ldots\oplus 0)=(0\oplus 0\oplus\ldots\oplus 0)$$

и, таким образом,

$$\|\alpha_1\|\,\|\alpha_2\|=0,\ \text{где}\ a_1\in K_1,\quad\alpha_2\in K_2.$$

Следовательно, функция $\|\ \|$ индуцирует нормирование в точности на одном из полей K_j, причем это индуцированное нормирование, очевидно, продолжает данное нормирование $|\ |$ поля $\bar{k}$. Значит, $\|\ \|=\|\ \|_j$ в точности для одного j.

Осталось показать только, что формулу (2) можно понимать также как топологический гомоморфизм. Для $(\beta_1,\ldots,\beta_J)\in K_1\oplus\ldots\oplus K_J$ положим

$$\|(\beta_1,\ldots,\beta_J)\|_0=\max_{1\leqslant j\leqslant J}\|\beta_j\|_j.$$

Ясно, что $\|\ \|_0$ есть норма на правой части равенства (2), рассматриваемой как векторное пространство над полем $\bar{k}$, и что эта норма индуцирует топологию произведения. С другой стороны, так как поле $\bar{k}$ полно, любые две нормы эквивалентны, и потому $\|\ \|_0$ индуцирует топологию тензорного произведения и на левой части равенства (2).

Следствие. *Пусть* $K = k(\beta)$, *и пусть* $f(X) \in k[X]$ — *неприводимый многочлен для* β. *Предположим, что в кольце* $\bar{k}[X]$ *имеет место разложение*

$$f(X) = \prod_{1 \leqslant j \leqslant J} g_j(X),$$

причем многочлены $g_i(X)$ *неприводимы. Тогда* $K_j = \bar{k}(\beta_j)$, *где* $g_j(\beta_j) = 0$.

§ 11. ПРОДОЛЖЕНИЕ НОРМАЛИЗОВАННЫХ НОРМИРОВАНИЙ

Пусть k — поле с нормированием $|\ |$. Мы рассмотрим три случая.

1. Нормирование $|\ |$ — дискретное неархимедово, а поле вычетов конечно.

2i. Пополнение поля k относительно нормирования $|\ |$ совпадает с $\mathbf{R}$.

2ii. Пополнение поля k относительно нормирования $|\ |$ совпадает с $\mathbf{C}$.

(В силу замечания из § 7 эти случаи могут быть объединены следующим условием: пополнение $\bar{k}$ поля k локально компактно.)

В случае 1 мы уже определили понятие нормализованного нормирования (§ 7). В случае 2i мы будем говорить, что нормирование $|\ |$ нормализовано, если оно является обычной абсолютной величиной, а в случае 2ii — если оно есть квадрат абсолютной величины. Тогда в любом случае отображение

$$\alpha : \xi \longrightarrow \alpha\xi \quad (\xi \in \bar{k}^+,\ \alpha \in \bar{k})$$

аддитивной группы $\bar{k}^+$ пополнения поля k умножает меру Хаара на группе $\bar{k}^+$ на число $|\alpha|$; это характеризует нормализованное нормирование среди эквивалентных ему нормирований.

Лемма 11.1. *Пусть поле* k *полно относительно нормализованного нормирования* $|\ |$, *и пусть* K — *расширение поля* k *степени* $[K : k] = N < \infty$. *Тогда нормализованное нормирование* $\|\ \|$ *поля* K, *эквивалентное единственному продолжению нормирования* $|\ |$ *на поле* K, *задается формулой*

$$\|\alpha\| = |\operatorname{Norm}_{K/k}\alpha| \qquad (\alpha \in K).$$

Доказательство. Согласно изложенному в предыдущем параграфе,

$$\|\alpha\| = |\operatorname{Norm}_{K/k}\alpha|^c \qquad (\alpha \in K) \tag{1}$$

для некоторого вещественного $c > 0$, и все, что нам осталось — это доказать, что $c = 1$. Это тривиально в случаях 2i, 2ii и следует из структурных теорем гл. I в случае 1. Можно рассуждать следующим образом. Пусть $\omega_1, \ldots, \omega_N$ — базис в поле K над полем k. Тогда отображение

$$\Xi = \sum \xi_n \omega_n \longleftrightarrow (\xi_1, \ldots, \xi_N) \qquad (\xi_1, \ldots, \xi_N \in k)$$

дает изоморфизм между аддитивной группой K^+ и прямой суммой $\bigoplus^N k^+$ (N экземпляров группы k^+), и это отображение будет гомеоморфизмом, если в правой части равенства ввести топологию прямого произведения. В частности, меры Хаара на группах K^+ и $\bigoplus^N k^+$ совпадают с точностью до мультипликативной константы. Пусть $b \in k$. Тогда отображение

$$b : \Xi \longrightarrow b\Xi$$

группы K^+ — это то же самое, что и отображение

$$(\xi_1, \ldots, \xi_N) \longrightarrow (b\xi_1, \ldots, b\xi_N)$$

группы $\bigoplus^N k^+$; следовательно, отображение b умножает меру Хаара на число $|b|^N$, поскольку нормирование $|\ |$ нормализовано. Значит,

$$\|b\| = |b|^N.$$

Но $\operatorname{Norm}_{K/k} b = b^N$, и потому в равенстве (1) имеет место $c = 1$.

Без предположения полноты справедлива

Теорема 11.1. *Пусть* $|\ |$ — *нормализованное нормирование поля* k, *и пусть* K — *конечное расширение поля* k. *Тогда*

$$\prod_{1 \leqslant i \leqslant J} \|\alpha\|_j = |\operatorname{Norm}_{K/k}\alpha|,$$

где $\| \|_j$ *— нормализованные нормирования, эквивалентные продолжениям нормирования* $| |$ *на поле* K.

Доказательство. Пусть

$$\bar{k} \otimes_k K = \bigoplus_{1 \leqslant j \leqslant J} K_j,$$

где $\bar{k}$ — пополнение поля k. Тогда (следствие 2 из леммы 9.1)

$$\mathrm{Norm}_{K/k} \alpha = \prod_{1 \leqslant j \leqslant J} \mathrm{Norm}_{K_j/\bar{k}} \alpha.$$

Теорема теперь следует из предыдущей леммы и результатов § 10.

§ 12. ГЛОБАЛЬНЫЕ ПОЛЯ

Под глобальным полем k мы будем понимать либо конечное расширение поля $\mathbf{Q}$ рациональных чисел, либо конечное сепарабельное [1]) расширение поля $\mathbf{F}(t)$, где $\mathbf{F}$ — конечное поле и t трансцендентно над $\mathbf{F}$. В нашем изложении мы сконцентрируем внимание на расширениях поля $\mathbf{Q}$ (случай поля алгебраических чисел), оставляя случай расширений поля $\mathbf{F}(t)$ (случай поля функций) читателю.

Лемма 12.1. *Пусть* $\alpha \neq 0$ *— элемент глобального поля* k. *Тогда найдется не более конечного числа неэквивалентных нормирований* $| |$ *поля* k, *таких, что*

$$|\alpha| > 1.$$

Доказательство. Мы уже знаем этот факт для полей $\mathbf{Q}$ и $\mathbf{F}(t)$. Пусть k будет конечным расширением поля $\mathbf{Q}$; тогда

$$a^n + a_1 a^{n-1} + \ldots + a_n = 0$$

для некоторого n и некоторых $a_1, \ldots a_n$. Если нормирование $| |$ поля k неархимедово, то

$$|\alpha|^n = |-a_1\alpha^{n-1} - \ldots - a_n| \leqslant$$
$$\leqslant \max\{1, |a|^{n-1}\} \cdot \max\{|a_1|, \ldots, |a_n|\}$$

[1]) Это условие в действительности не является необходимым. Если k — любое конечное расширение поля $\mathbf{F}(t)$, то найдется «сепарирующий элемент» $s \in k$, т. е. такой, что k является конечным сепарабельным расширением поля $\mathbf{F}(s)$.

и, таким образом,

$$|\alpha| \leqslant \max\{1, |a_1|, \ldots, |a_n|\}.$$

Так как всякое нормирование поля $\mathbf{Q}$ имеет лишь конечное число продолжений на k и так как существует лишь конечное число архимедовых нормирований, то справедливость леммы для поля k следует из справедливости ее для поля $\mathbf{Q}$.

Все нормирования глобального поля k имеют вид, описанный в § 11, так как это верно для полей $\mathbf{Q}$ и $\mathbf{F}(t)$. Значит, можно говорить и о нормализованных нормированиях.

Теорема 12.1. *Пусть* $\alpha \in k$, *где* k *— глобальное поле, и* $\alpha \neq 0$. *Пусть* $|\ |_v$ *пробегает все нормализованные нормирования поля* k. *Тогда* $|\alpha|_v = 1$ *для всех* v, *за исключением конечного числа, и*

$$\prod_v |\alpha|_v = 1.$$

Замечание. Позже мы дадим другое, менее выкладочное доказательство этого факта.

Доказательство. Согласно лемме, $|a|_v \leqslant 1$ для почти всех v (т. е. для всех, кроме конечного числа). Аналогично $|a^{-1}|_v \leqslant 1$ для почти всех v, так что $|a|_v = 1$ для почти всех v.

Пусть V пробегает все нормализованные нормирования поля $\mathbf{Q}$ (или $\mathbf{F}(t)$); мы будем писать $v \mid V$, если ограничение нормирования v на $\mathbf{Q}$ эквивалентно нормированию V. Тогда

$$\prod_v |\alpha|_v = \prod_V \Big(\prod_{v \mid V} |\alpha|_v\Big) = \prod_V |\mathrm{Norm}_{k/\mathbf{Q}} \alpha|_V,$$

согласно предыдущему параграфу. Это сводит теорему к случаю $k = \mathbf{Q}$. Но если

$$b = \pm \prod_p p^{\beta_p} \in \mathbf{Q},$$

где p пробегает все простые числа, а $\beta_p \in \mathbf{Z}$, то

$$|b|_p = p^{-\beta_p}$$

для p-адического нормирования $|\ |_p$ и

$$|b|_\infty = \prod_p p^{\beta_p}$$

для абсолютной величины $|\ |_\infty$. Это и требовалось доказать.

Пусть K будет конечным сепарабельным расширением глобального поля k. Тогда для всякого нормирования v поля k имеет место изоморфизм

$$k_v \otimes_k K = K_1 \oplus \ldots \oplus K_J,$$

где k_v обозначает пополнение поля k относительно нормирования v, а $K_1, \ldots, K_J$ — пополнения поля K относительно продолжений $V_1, \ldots, V_J$ этого нормирования на поле K (§ 10); число $J = J(v)$ зависит от v. Впоследствии нам нужна будет следующая лемма.

Лемма 12.2. *Пусть $\omega_1, \ldots, \omega_N$ — базис расширения K над полем k. Тогда для почти всех нормализованных нормирований v имеет место равенство*

$$\omega_1\mathfrak{o} \oplus \omega_2\mathfrak{o} \oplus \ldots \oplus \omega_N\mathfrak{o} = \mathfrak{O}_1 \oplus \ldots \oplus \mathfrak{O}_J, \qquad (1)$$

где $N = [K : k]$, через $\mathfrak{o} = \mathfrak{o}_v$ обозначено кольцо целых элементов поля k с нормированием $|\ |_v$ и через $\mathfrak{O}_j \subset K_j$ — кольцо целых элементов для нормирований $|\ |_{V_j} (1 \leqslant j \leqslant J)$. Здесь мы отождествили элемент $\alpha \in K$ с его каноническим образом в $k_v \otimes K$.

Доказательство. Левая часть равенства (1) содержится в правой части, если только $|\omega_n|_{V_j} \leqslant 1$ $(1 \leqslant n \leqslant N, 1 \leqslant j \leqslant J)$. Так как $|\alpha|_V = 1$ для почти всех V, то левая часть содержится в правой части для почти всех V.

Чтобы получить включение в другую сторону, мы используем дискриминант

$$D(\gamma_1, \ldots, \gamma_N) = \det_{m,n}(\mathrm{trace}_{K/k}\, \gamma_m\gamma_n),$$

где $\gamma_1, \ldots, \gamma_N \in k_v \otimes_k K$. Если γ_n $(1 \leqslant n \leqslant N)$ принадлежат правой части равенства (1), то (§ 9)

$$\mathrm{trace}_{K/k}\, \gamma_m\gamma_n = \sum_{1 \leqslant j \leqslant J} \mathrm{trace}_{K_j/k}\, \gamma_m\gamma_n \in \mathfrak{o} = \mathfrak{o}_v,$$

и, таким образом,

$$D(\gamma_1, \ldots, \gamma_N) \in \mathfrak{o}_v.$$

Предположим теперь, что элемент α принадлежит правой части равенства (1) и что

$$\beta = \sum_1^N b_n\omega_n \in \mathfrak{O}_1 \oplus \ldots \oplus \mathfrak{O}_J \quad (b_n \in k_v). \qquad (2)$$

Тогда для любого m, $1 \leqslant m \leqslant N$, имеем

$$D(\omega_1, \ldots, \omega_{m-1}, \beta, \omega_{m+1}, \ldots, \omega_N) = b_m^2 D(\omega_1, \ldots, \omega_N),$$

и, таким образом,

$$ab_m^2 \in \mathfrak{o}_v \qquad (1 \leqslant m \leqslant N),$$

где

$$d = D(\omega_1, \ldots, \omega_N) \in k.$$

Но (см. добавление Б) $d \neq 0$, и потому $|d|_v = 1$ для почти всех v. Тем самым для почти всех v из условия (2) вытекает, что

$$b_m \in \mathfrak{o}_m \qquad (1 \leqslant m \leqslant N),$$

т. е. правая часть содержится в левой части. Это доказывает лемму.

(Следствие. *Почти все v являются неразветвленными в расширении K поля k.*

Действительно, согласно результатам гл. I, необходимым и достаточным условием того, чтобы v было неразветвленным, является существование таких $\gamma_1, \ldots, \gamma_N$ в правой части равенства (1), что $|D(\gamma_1, \ldots, \gamma_N)|_v = 1$. А для почти всех v можно положить $\gamma_n = a^{n-1}$.)

§ 13. ОГРАНИЧЕННОЕ ТОПОЛОГИЧЕСКОЕ ПРОИЗВЕДЕНИЕ

Мы опишем сейчас топологический механизм, который нам понадобится позже.

Определение. *Пусть Ω_λ $(\lambda \in \Lambda)$ будет семейством топологических пространств, и пусть $\Theta_\lambda \subset \Omega_\lambda$ будет открытым подмножеством в Ω_λ для почти всех λ. Рассмотрим пространство Ω, точками которого являются множества $\boldsymbol{\alpha} = \{\alpha_\lambda\}_{\lambda \in \Lambda}$, где $\alpha_\lambda \in \Omega_\lambda$ для каждого λ и $\alpha_\lambda \in \Theta_\lambda$ для почти всех λ. Мы введем в Ω топологию, взяв за базис открытых множеств множества*

$$\prod \Gamma_\lambda,$$

где $\Gamma_\lambda \subset \Omega_\lambda$ открыто для всех λ и $\Gamma_\lambda \subset \Theta_\lambda$ открыто для почти всех λ. Пространство Ω с так введенной топологией мы назовем ограниченным топологическим произведением пространств Ω_λ по отношению к Θ_λ.

Следствие. *Пусть S — конечное подмножество в Λ, и пусть Ω_s — множество элементов $\boldsymbol{\alpha} \in \Omega$, таких, что*

$\alpha_\lambda \in \Theta_\lambda$ $(\lambda \notin S)$, *т. е.*

$$\Omega_S = \prod_{\lambda \in S} \Omega_\lambda \prod_{\lambda \notin S} \Theta_\lambda. \qquad (1)$$

Тогда Ω_S открыто в пространстве Ω, и топология, индуцированная в Ω_S как в подмножестве пространства Ω, совпадает с топологией прямого произведения.

Доказательство очевидно.

Ограниченное топологическое произведение зависит от совокупности всех Θ_λ в целом, но не от индивидуальных Θ_λ.

Лемма 13.1. *Пусть $\Theta'_\lambda \subset \Omega_\lambda$ — открытые множества, определенные для почти всех λ; предположим, что $\Theta'_\lambda = \Theta_\lambda$ для почти всех $\lambda \in \Lambda$. Тогда ограниченное произведение пространств Ω_λ по отношению к Θ'_λ совпадает с* [1] *ограниченным произведением по отношению к Θ_λ.*

Доказательство очевидно.

Лемма 13.2. *Предположим, что пространства Ω_λ локально компактны и что все Θ_λ компактны. Тогда пространство Ω локально компактно.*

Доказательство. Пространства Ω_S локально компактны в силу равенства (1), так как множество S конечно. А так как $\Omega = \bigcup \Omega_S$ и подмножество Ω_S открыто в Ω то отсюда и вытекает нужный результат.

Определение. *Предположим, что на пространствах Ω_λ определены меры μ_λ и что $\mu_\lambda(\Theta_\lambda) = 1$, когда Θ_λ определено. Меру произведения μ на Ω мы определим как меру, для которой базисом измеримых множеств будет*

$$\prod_\lambda M_\lambda,$$

где $M_\lambda \subset \Omega_\lambda$ имеет конечную μ_λ-меру и $M_\lambda = \Theta_\lambda$ для почти всех $\lambda \in \Lambda$, причем

$$\mu\left(\prod_\lambda M_\lambda\right) = \prod_\lambda \mu_\lambda(M_\lambda).$$

Следствие. *Ограничение меры μ на Ω_S представляет собой в точности обычное произведение мер.*

[1] Пурист сказал бы: «канонически изоморфно».

§ 14. КОЛЬЦО АДЕЛЕЙ (ИЛИ КОЛЬЦО ВЕКТОРОВ НОРМИРОВАНИЙ)

Пусть k — глобальное поле. Для каждого нормализованного нормирования $|\ |_v$ поля k обозначим через k_v пополнение поля k. Если нормирование $|\ |_v$ неархимедово, то обозначим через $\mathfrak{o}_v$ кольцо целых элементов поля k_v. *Кольцом V_k аделей* поля k называется топологическое кольцо, топологическим пространством которого является ограниченное произведение колец k_v относительно $\mathfrak{o}_v$, а сложение и умножение определяются покомпонентно, т. е.

$$(\alpha\beta)_v = \alpha_v\beta_v, \quad (\alpha+\beta)_v = \alpha_v + \beta_v, \quad \alpha, \beta \in V_k. \qquad (1)$$

Легко проверить, что, во-первых, это определение корректно, т. е. если $\alpha, \beta \in V_k$, то элементы $\alpha\beta$ и $\alpha + \beta$, компоненты которых заданы формулами (1), также принадлежат V_k, и, во-вторых, что сложение и умножение непрерывны в V_k-топологии, так что V_k действительно является топологическим кольцом.

Кольцо V_k локально компактно, потому что все k_v локально компактны, а все $\mathfrak{o}_v$ компактны (§ 7).

Существует естественное отображение поля k в кольцо V_k, отображающее элемент $\alpha \in k$ в адель, все компоненты которого равны α (это действительно адель, потому что $\alpha \in \mathfrak{o}_v$ для почти всех v). Данное отображение — вложение, потому что отображение поля k в любое пополнение k_v является вложением. Образ поля k при этом вложении называется *кольцом главных аделей*. Отождествление поля k с этим кольцом не может привести к недоразумениям, поэтому мы будем говорить о k как о подкольце кольца V_k.

Лемма 14.1. *Пусть K — конечное сепарабельное расширение глобального поля k. Тогда имеет место изоморфизм*

$$V_k \otimes_k K = V_K \qquad (2)$$

в алгебраическом и топологическом смыслах. При этом $k \otimes_k K = K \subset V_k \otimes_k K$, где $k \subset V_k$, отображается тождественно на $K \subset V_K$.

Доказательство. Вначале мы докажем изоморфность обеих частей формулы (2) как топологических про-

странств. Пусть $\omega_1, \ldots, \omega_N$ — базис расширения K над полем k, и пусть v пробегает все нормализованные нормирования поля k. Легко видеть, что левая часть равенства (2) с топологией тензорного произведения есть в точности ограниченное произведение пространств

$$k_v \otimes {}_kK = k_v\omega_1 \oplus \ldots \oplus k_v\omega_N \tag{3}$$

по отношению к

$$\mathfrak{o}_v\omega_1 \oplus \ldots \oplus \mathfrak{o}_v\omega_N. \tag{4}$$

Но (см. § 10) пространство (3) в точности совпадает с пространством

$$K_{V_1} \oplus \ldots \oplus K_{V_J}, \quad (V_1 | v, \ldots, V_J | v), \tag{5}$$

где $V_1, \ldots, V_J$, $J = J(v)$ — нормализованные продолжения нормирования v на поле K. Далее (§ 12), отождествление пространства (3) с пространством (5) приводит к отождествлению пространства (4) с пространством

$$\mathfrak{O}_{V_1} \oplus \ldots \oplus \mathfrak{O}_{V_J} \tag{6}$$

для почти всех [1]) v. Значит, левая часть равенства (2) является ограниченным произведением пространств (3) по отношению к (4), которое, очевидно, есть то же самое, что и ограниченное произведение колец K_V по отношению к $\mathfrak{o}_V$, если V пробегает все нормализованные нормирования поля K. Но это есть как раз правая часть равенства (2). Тем самым мы доказали изоморфность обеих частей равенства (2) как топологических пространств. Алгебраический изоморфизм устанавливается просто.

Следствие. *Пусть V_k^+ обозначает топологическую группу, полученную из V_k отбрасыванием мультипликативной структуры. Тогда*

$$V_K^+ = \underbrace{V_k^+ \oplus \ldots \oplus V_k^+}_{N\text{-слагаемых}} \qquad (N = [K : k]).$$

При этом изоморфизме аддитивная группа $K^+ \subset V_K^+$ главных аделей отображается в группу $k^+ \oplus \ldots \oplus k^+$ (обозначения естественные).

[1]) Это было доказано только для случая $\omega_n = \alpha^{n-1}$, где $K = k(\alpha)$. Поэтому мы выберем ω_n именно таким образом.

Доказательство. Группа $\omega V_k^+ \subset V_K^+$ для ненулевого $\omega \in K$, очевидно, изоморфна группе V_k^+ (в топологическом смысле). Значит, имеют место изоморфизмы

$$V_K^+ = V_k^+ \otimes {}_kK = \omega_1 V_k^+ \oplus \ldots \oplus \omega_N V_k^+ = V_k^+ \oplus \ldots \oplus V_k^+.$$

Теорема 14.1. *Кольцо k дискретно* [1]) *в V_k, и факторгруппа V_k^+/k^+ компактна в фактортопологии.*

Доказательство. Предыдущее следствие (с k вместо K и $\mathbf{Q}$ или $\mathbf{F}(t)$ вместо k) показывает, что достаточно проверить теорему для полей $\mathbf{Q}$ или $\mathbf{F}(t)$; мы сделаем это для поля $\mathbf{Q}$.

Чтобы показать, что группа $\mathbf{Q}^+$ дискретна в $V_{\mathbf{Q}}^+$, достаточно (потому что это группа) найти окрестность U нуля, не содержащую никаких других элементов группы k^+. Мы возьмем в качестве U множество всех $\boldsymbol{\alpha} = \{\alpha_v\} \in V_{\mathbf{Q}}^+$, таких, что

$$|\alpha_\infty|_\infty < 1, \quad |\alpha_p|_p \leqslant 1 \quad (\text{при всех } p),$$

где $|\ |_p$, $|\ |_\infty$ обозначают соответственно p-адические нормирования и абсолютную величину в $\mathbf{Q}$.

Если $b \in \mathbf{Q} \cap U$, то первая компонента аделя b — целое число (так как $|b|_p \leqslant 1$ для всех p) и потому, учитывая, что $|b| < 1$, мы получаем $b = 0$.

Пусть теперь $W \subset V_{\mathbf{Q}}^+$ состоит из всех тех $\boldsymbol{\alpha} = \{\alpha_v\}$, для которых

$$|\alpha_\infty|_\infty \leqslant \frac{1}{2}, \quad |\alpha_p|_p \leqslant 1 \quad (\text{при всех } p).$$

Мы покажем, что всякий адель $\boldsymbol{\beta}$ имеет вид

$$\boldsymbol{\beta} = b + \boldsymbol{\alpha}, \quad \text{где } b \in \mathbf{Q}, \ \boldsymbol{\alpha} \in W. \tag{7}$$

Для всякого p можно найти число

$$r_p = z_p/p^{x_p} \quad (z_p \in \mathbf{Z}, \ x_p \in \mathbf{Z}, \ x_p \geqslant 0),$$

такое, что

$$|\beta_p - r_p|_p \leqslant 1,$$

[1]) Нельзя представить себе иной индивидуально определенной топологии в k. Эта метаматематическая причина более по существу, чем аргументы, приводимые далее в тексте.

и так как α — адель, то можно положить

$$r_p = 0 \text{ для почти всех } p.$$

Значит, число $r = \sum_p r_p$ определено корректно и

$$|\beta_p - r|_p \leqslant 1 \text{ при всех } p.$$

Теперь выберем число $s \in \mathbf{Z}$ так, чтобы выполнялось неравенство

$$|\beta_\infty - r - s|_\infty \leqslant \frac{1}{2}.$$

Тогда $b = r + s$, $\beta = \alpha - b$, что и требовалось.

Таким образом, непрерывное отображение $W \to V_{\mathbf{Q}}^+/\mathbf{Q}^+$, индуцированное факторотображением $V_{\mathbf{Q}}^+ \to V_{\mathbf{Q}}^+/\mathbf{Q}^+$, сюръективно. Но W — компакт (как топологическое произведение компактов $\left\{|\alpha_\infty|_\infty \leqslant \frac{1}{2}\right\}$ и $\mathfrak{o}_p$), и, следовательно, компактна также и группа $V_{\mathbf{Q}}^+/\mathbf{Q}^+$.

Как уже отмечалось, V_k^+ — локально компактная группа и потому обладает инвариантной мерой (Хаара). Легко видеть, что в действительности эта мера Хаара есть произведение мер Хаара на группах k_v в смысле, описанном выше.

Следствие 1. *Существует подмножество W кольца V_k, определенное неравенствами вида $|\xi_v|_v \leqslant \delta_v$, где $\delta_v = 1$ для почти всех v, такое, что всякий элемент $\varphi \in V_k$ может быть представлен в виде*

$$\varphi = \theta + \gamma, \quad \theta \in W, \quad \gamma \in k.$$

Доказательство. Множество W, построенное в доказательстве теоремы 14.1, очевидно, включается в одно из подмножеств искомого типа.

Следствие 2. *Группа V_k^+/k^+ имеет конечную меру в фактормере, индуцированной мерой Хаара группы V_k^+.*

Замечание. Это утверждение, конечно, не зависит от частного выбора мультипликативной константы в мере Хаара на группе V_k^+. Мы здесь не обсуждаем вопроса нахождения меры группы V_k^+/k^+ в терминах явно заданной меры Хаара на V_k^+.

Доказательство. Как и раньше, это утверждение может быть сведено к случаям полей $\mathbf{Q}$ или $\mathbf{F}(t)$, в которых получается почти немедленно; действительно, подмножество W, определенное выше, имеет меру 1 в нашей мере Хаара.

Обратно, конечность меры следует из компактности: покроем группу V_k^+/k^+ сдвигами множества F, где F — открытое множество конечной меры; тогда существование конечного подпокрытия влечет конечность меры.

(Дадим теперь другое доказательство формулы $\prod |\xi|_v = 1$ для $\xi \in k$, $\xi \neq 0$. Мы видели, что если $\beta_v \in k_v$, то умножение на β_v изменяет меру Хаара в группе k_v^+ на множитель $|\beta_v|_v$. Значит, если $\beta = \{\beta_v\} \in V_k$, то умножение на β изменяет меру Хаара в группе V_k на множитель $\prod |\beta_v|_v$. В частности, умножение на главный адель ξ изменяет меру Хаара на $\prod |\xi|_v$. Но умножение на ξ переводит группу $k^+ \subset V_k^+$ в k^+, так что дает корректно определенное взаимно однозначное отображение группы V_k^+/k^+ на V_k^+/k^+, которое изменяет меру на множитель $\prod |\xi|_v$. Значит, $\prod |\xi|_v = 1$, согласно следствию 2.)

В следующем параграфе нам будет нужна

Лемма 14.2. *Существует константа $C > 0$, зависящая только от глобального поля k, со следующим свойством: пусть элемент $\alpha = \{\alpha_v\} \in V_k$ таков, что*

$$\prod_v |\alpha_v|_v > C. \tag{8}$$

Тогда найдется такой главный адель $\beta \in k \subset V_k$, $\beta \neq 0$, что

$$|\beta|_v \leqslant |\alpha_v|_v \quad (\textit{для всех } v).$$

Доказательство мы проведем аналогично доказательству Блихфельдта теоремы Минковского, касающейся геометрии чисел.

Заметим, что условие (8) влечет за собой равенство $|\alpha_v|_v = 1$ для почти всех v, потому что $|\alpha_v|_v \leqslant 1$ для почти всех v.

Пусть число c_0 будет равно мере Хаара группы V_k^+/k^+, а число c_1 — мере Хаара множества тех элементов $\gamma =$

$= \{\gamma_v\} \in V_k^+$, для которых

$|\gamma_v|_v \leqslant \frac{1}{10}$, если нормирование v архимедово,

$|\gamma_v|_v \leqslant 1$, если нормирование v неархимедово.

Тогда $0 < c_0 < \infty$ и $0 < c_1 < \infty$, потому что число архимедовых нормирований конечно. Мы покажем, что число

$$C = c_0/c_1$$

обладает требуемым в лемме свойством.

Множество T элементов $\tau = \{\tau_v\} \in V_k^+$, таких, что

$|\tau_v|_v \leqslant \frac{1}{10}|\alpha_v|_v$, если v архимедово,

$|\tau_v|_v \leqslant |\alpha_v|_v$, если v неархимедово,

имеет меру

$$c_1 \prod_v |\alpha_v|_v > c_1 \quad C = 0.$$

Значит, при факторотображении $V_k^+ \to V_k^+/k^+$ хотя бы одна пара различных точек из T должна иметь один и тот же образ. Пусть это будут точки

$$\tau' = \{\tau_v'\} \in T, \quad \tau'' = \{\tau_v''\} \in T,$$

и пусть

$$\tau' - \tau'' = \beta \in k^+.$$

Тогда

$$|\beta|_v = |\tau_v' - \tau_v''|_v \leqslant |\alpha_v|_v$$

для всех v, что и требовалось установить.

Следствие. *Пусть v_0 — нормализованное нормирование, и пусть числа $\delta_v > 0$ заданы для каждого нормирования $v \neq v_0$, причем $\delta_v = 1$ для почти всех нормирований v. Тогда найдется элемент $\beta \in k$, $\beta \neq 0$, такой, что*

$$|\beta|_v \leqslant \delta_v \ (\textit{при всех } v \neq v_0).$$

Доказательство. Это утверждение — просто вырожденный случай леммы 14.2. Выберем $\alpha_v \in k_v$ так, чтобы выполнялись неравенства $0 < |\alpha_v|_v \leqslant \delta_v$ и чтобы имело место $|\alpha_v|_v = 1$, если $\delta_v = 1$. Тогда можно так выбрать $\alpha_{v_0} \in k_{v_0}$, что $\prod\limits_{v \neq v_0} |\alpha_v|_v > C$. Теперь утверждение сразу следует из леммы 14.2.

(Группа характеров локально компактной группы V_k^+ изоморфна группе V_k^+, причем здесь группа k^+ играет особую роль, см. [10], [6], [8]. Эта роль тесно связана с функциональным уравнением для ζ- и для L-функций. Ивасава показал [9], что кольцо аделей характеризуется некоторыми свойствами, формулируемыми в общих тополого-алгебраических терминах.)

§ 15. СИЛЬНАЯ АППРОКСИМАЦИОННАЯ ТЕОРЕМА

Результаты, полученные выше, в частности дискретность группы k в V_k, основаны на том, что в определении группы аделей V_k используются *все* нормализованные расширения.

Теорема 15.1. (Сильная аппроксимационная теорема.) *Пусть v_0 — некоторое нормирование глобального поля k. Определим $\mathscr{V}$ как ограниченное топологическое произведение групп k_v по отношению к $\mathfrak{o}_v$, где v пробегает все нормализованные нормирования $v \neq v_0$. Тогда k всюду плотно в $\mathscr{V}$.*

Доказательство[1]). Легко видеть, что эта теорема эквивалентна следующему утверждению. Предположим, что даны: (i) конечное множество S нормирований $v \neq v_0$; (ii) элементы $\alpha_v \in k_v$ для каждого $v \in S$; (iii) число $\varepsilon > 0$. Тогда найдется $\beta \in k$, такое, что $|\beta - \alpha_v|_v < \varepsilon$ для всех $v \in S$ и $|\beta|_v \leqslant 1$ для всех $v \notin S$, $v \neq v_0$.

По следствию 1 из теоремы 14.1 найдется подмножество $W \subset V_k$, определенное неравенствами вида $|\xi_v|_v \leqslant \delta_v$ ($\delta_v = 1$ для почти всех v), такое, что всякое $\varphi \in V_k$ имеет вид

$$\varphi = \theta + \gamma, \quad \theta \in W, \quad \gamma \in k. \tag{1}$$

По следствию из леммы 14.2 найдется $\lambda \in k$, $\alpha \neq 0$, такое, что

$$\begin{aligned} &|\lambda|_v < \delta_v^{-1}\varepsilon \quad (v \in S), \\ &|\lambda|_v \leqslant \delta_v^{-1} \quad (v \notin S,\ v \neq v_0). \end{aligned} \tag{2}$$

[1]) Предложено профессором Кнезером на конференции.

Полагая $\varphi = \lambda^{-1}\alpha$ в (1) и умножая на λ, мы видим, что всякое $\alpha \in V_k$ имеет вид

$$\alpha = \psi + \beta, \quad \psi \in \lambda W, \quad \beta \in k, \tag{3}$$

где λW есть множество элементов вида $\lambda\xi$, $\xi \in W$. Если теперь мы возьмем элемент α, имеющий компоненты α_v для всех v из S и, например, 0 в остальных местах, то легко видеть, что соответствующий элемент β обладает требуемыми свойствами.

(Доказательство, очевидно, дает количественную форму теоремы (т. е. с ограничением на $|\beta|_{v_0}$). Иное доказательство см. в [11].)

§ 16. ГРУППА ИДЕЛЕЙ

Множество обратимых элементов любого коммутативного топологического кольца R образует группу R^* по умножению. Вообще говоря, R^* не является топологической группой, если в нее ввести топологию подмножества, потому что взятие обратного элемента не обязательно непрерывно. Поэтому обычно в R^* вводится следующая топология. Рассмотрим вложение

$$x \longrightarrow (x,\ x^{-1}) \tag{1}$$

группы R^* в топологическое произведение $R \times R$ и зададим в R^* индуцированную этим вложением топологию подмножества. Ясно, что R^* в этой топологии является топологической группой и вложение $R^* \to R$ непрерывно.

Определение. *Группой иделей J_k поля k называется V_k^*, т. е. группа обратимых элементов кольца аделей V_k с топологией, которая только что была определена.*

Мы будем обычно говорить о J_k как подмножестве кольца V_k и будем различать J_k- и V_k-топологии [1]).

Мы видели, что поле k естественно вкладывается в кольцо V_k, так что группа k^* естественно погружена в группу J_k.

[1]) Пусть $\alpha^{(q)}$ для простого рационального числа q будет элементом группы $J_{\mathbf{Q}}$ с компонентами $\alpha_q^{(q)} = q$, $\alpha_v^{(q)} = 1$ $(v \neq q)$. Тогда $\alpha^{(q)} \to 1$ $(q \to \infty)$ в $V_{\mathbf{Q}}^q$-топологии, но не в $J_{\mathbf{Q}}$-топологии.

Группу k^*, рассматриваемую как подгруппу в J_k, мы будем называть группой *главных* иделей.

Лемма 16.1. *k^* — дискретная подгруппа группы J_k.*

Доказательство. k дискретно в V_k, и потому k^* вкладывается в $V_k \times V_k$ при отображении (1) как дискретное подмножество.

Лемма 16.2. *Группа J_k представляет собой в точности ограниченное топологическое произведение групп k_v^* по отношению к единицам $U_v \subset k_v$ (с топологией ограниченного произведения).*

Доказательство очевидно.

Определение. *Для $\alpha = \{\alpha_v\} \in J_k$ определим число $c(\alpha) = \prod_v |\alpha_v|_v$ и назовем это число содержанием элемента α.*

Лемма 16.3. *Отображение $\alpha \to c(\alpha)$ является непрерывным гомоморфизмом топологической группы J_k в мультипликативную группу (строго) положительных вещественных чисел.*

Доказательство очевидно.

(Лемма 16.4. *Пусть $\alpha \in J_k$. Тогда отображение $\xi \to \alpha\xi$ группы V_k^+ на себя умножает меру Хаара группы V_k^+ на множитель $c(\alpha)$.* Доказательство очевидно.

Заметим также, что J_k-топология совпадает с обычной топологией группы операторов на группе V_n^+: базисом открытых множеств являются множества $S(C, O)$, где $C,\ O \in V_k^+$ — соответственно V_k-компакт и V_k-открытое множество, а $S(C, O)$ состоит из всех $\alpha \in J_k$, таких, что $(1 - \alpha)C \subset O$ и $(1 - \alpha^{-1})C \subset O$.)

Пусть J_k^1 будет ядром отображения $\alpha \to c(\alpha)$ с топологией подмножества из J_k. Нам нужна будет следующая лемма.

Лемма 16.5. *Группа J_k^1, рассматриваемая как подмножество в J_k, замкнута, и V_k-топология на J_k^1 совпадает с J_k-топологией.*

Доказательство. Пусть $\alpha \in V_k$ и $\alpha \notin J_k^1$. Мы должны найти V_k-окрестность W элемента α, которая не пересекается с J_k^1.

Первый случай. $\prod_v |\alpha_v|_v < 1$ (возможно равенство нулю). Тогда найдется конечное множество S нормирований, такое, что:

(i) S содержит все нормирования v, для которых $|\alpha_v|_v > 1$;

(ii) $\prod_{v \in S} |\alpha_v|_v < 1$. Поэтому множество W можно определить неравенствами

$$\begin{aligned} |\xi_v - \alpha_v|_v &< \varepsilon, & v &\in S, \\ |\xi_v|_v &\leqslant 1, & v &\notin S, \end{aligned}$$

для достаточно малого ε.

Второй случай. $\prod_v |\alpha_v|_v > 1$. Пусть $\prod_v |\alpha_v|_v = C$. Тогда найдется конечное множество S нормирований v, такое, что

(i) S содержит все v, такие, что $|\alpha_v|_v > 1$;

(ii) если $v \notin S$, то неравенство $|\xi_v|_v < 1$ влечет за собой[1]) неравенство $|\xi_v|_v < \frac{1}{2} C$. Мы можем выбрать ε настолько малым, чтобы условие $|\xi_v - \alpha_v|_v < \varepsilon$ $(v \in S)$ влекло за собой неравенство $1 < \prod_{v \in S} |\xi_v| < 2C$. Тогда W можно определить неравенствами

$$\begin{aligned} |\xi_v - \alpha_v|_v &< \varepsilon & (v &\in S), \\ |\xi_v| &\leqslant 1 & (v &\notin S). \end{aligned}$$

Мы должны теперь показать, что J_k- и V_k-топологии на J_k^1 совпадают. Если $\mathbf{\alpha} \in J_k^1$, то нужно показать, что всякая J_k-окрестность элемента $\mathbf{\alpha}$ содержит V_k-окрестность и обратно.

[1]) Если $k \supset \mathbf{Q}$ и v — нормализованное продолжение p-адического нормирования на k, то группа значений v состоит из (некоторых) степеней числа p. Значит, для справедливости условия (ii) достаточно включить в S все архимедовы нормирования v и все продолжения p-адических нормирований при $p \leqslant 2C$. Аналогично обстоит дело, если $k \supset \mathbf{F}(t)$.

Пусть[1]) $W \subset J_k^1$ будет V_k-окрестностью элемента $\mathbf{\alpha}$. Тогда она содержит V_k-окрестность вида

$$\left.\begin{aligned} |\xi_v - \alpha_v|_v &< \varepsilon & (v &\in S), \\ |\xi_v|_v &\leqslant 1 & (v &\notin S), \end{aligned}\right\} \tag{2}$$

где S — конечное множество нормирований, а эта окрестность содержит J_k-окрестность, в которой знак $\leqslant$ в формуле (2) заменен знаком $=$.

Теперь пусть $H \subset J_k^1$ будет J_k-окрестностью. Тогда она содержит J_k-окрестность вида

$$\left.\begin{aligned} |\xi_v - \alpha_v|_v &< \varepsilon & (v &\in S), \\ |\xi_v|_v &= 1 & (v &\notin S), \end{aligned}\right\} \tag{3}$$

где конечное множество S содержит по крайней мере все архимедовы нормирования и все нормирования v, для которых $|\alpha_v|_v \neq 1$. Так как $\prod |\alpha_v|_v = 1$, то мы можем также предположить ε настолько малым, чтобы условие (3) влекло за собой неравенство

$$\prod_v |\xi_v|_v < 2.$$

Тогда пересечение множества (3) с J_k^1 есть в точности то же самое[2]), что и пересечение множества (2) с группой J_k^1, т. е. условия (3) определяют V_k-окрестность.

По формуле произведения мы имеем, что $k^* \subset J_k^1$. Следующий результат очень важен для теории полей классов.

Теорема 16.1. *Группа J_k^1/k^* компактна в фактортопологии.*

Доказательство. По лемме 5 достаточно найти V_k-компактное множество $W \subset V_k$, такое, что отображение

$$W \cap J_k^1 \longrightarrow J_k^1/k^*$$

эпиморфно.

[1]) Эта половина доказательства совпадения топологий не использует специальных свойств иделей. Она есть лишь выражение факта, замеченного выше: включение $R^* \to R$ непрерывно для любого топологического кольца R.

[2]) См. предыдущую сноску.

Мы возьмем в качестве W множество элементов $\xi=\{\xi_v\}$, таких, что

$$|\xi_v|_v \leqslant |\alpha_v|_v,$$

где $\alpha=\{\alpha_v\}$ — идель с содержанием, большим чем число C из леммы 14.2.

Пусть $\beta=\{\beta_v\}\in J_k^1$. Тогда по только что упомянутой лемме найдется элемент $\eta\in k^*$, такой, что

$$|\eta|_v \leqslant |\beta_v^{-1}\alpha_v|_v \quad \text{(при всех } v\text{)}.$$

Следовательно, $\eta\beta\in W$, что и требовалось.

(J_k/k^* вполне несвязно в случае поля функций. О структуре его связной компоненты в числовом случае см. работы [3] и [7] или [5]. Определение группы характеров для J_k/k^* составляет глобальную теорию полей классов.)

§ 17. ИДЕАЛЫ И ДИВИЗОРЫ

Предположим, что k — конечное расширение поля $\mathbf{Q}$. Мы определим группу идеалов I_k поля k как свободную абелеву группу, множество образующих которой находится во взаимно однозначном соответствии с *неархимедовыми* нормированиями v поля k, т. е. как группу формальных сумм вида

$$\sum_{v \text{ неарх.}} n_v v, \tag{1}$$

где $n_v\in\mathbf{Z}$ и $n_v=0$ для почти всех v; сложение покомпонентное. Мы назовем сумму вида (1) идеалом и назовем его целым, если $n_v\geqslant 0$ для всех v. Эта терминология оправдана существованием взаимно однозначного соответствия между целыми идеалами и идеалами в обычном смысле в дедекиндовом кольце

$$\mathfrak{o}=\bigcap_{v \text{ неарх.}} \mathfrak{o}_v;$$

ср. гл. I, предложение 2.2.

Существует естественное непрерывное отображение

$$J_k \to I_k$$

группы иделей на группу идеалов [1]), определяемое формулой

$$\alpha=\{\alpha_v\}\to\sum(\mathrm{ord}_v\,\alpha)\,v.$$

Образ группы $k^*\subset J_k$ в I_k называется группой главных идеалов.

Теорема 17.1. *Группа классов идеалов, т. е. факторгруппа группы I_k по модулю главных идеалов, конечна.*

Доказательство. Отображение $J_k^1\to I_k$ сюръективно, так что группа классов идеалов есть непрерывный образ компактной группы J_k^1/k^*, и потому она компактна. Но компактная дискретная группа конечна.

Когда k — конечное сепарабельное расширение поля $\mathbf{F}(t)$, мы определим группу дивизоров D_k поля k как свободную группу, порожденную всеми нормированиями v. Для каждого v число элементов поля вычетов есть некоторая степень q^{d_v} числа q элементов поля $\mathbf{F}$. Мы назовем d_v степенью дивизора (нормирования) v и аналогично определим $\Sigma\, n_v d_v$ как степень дивизора $\Sigma\, n_v v$. Дивизоры степени нуль образуют группу D_k^0. Можно определить главные дивизоры аналогично главным идеалам, и тогда верна следующая теорема.

Теорема 17.2. *Факторгруппа группы D_k^0 по модулю главных дивизоров конечна.*

Доказательство. Факторгруппа есть непрерывный образ компактной группы J_k^1/k^*.

§ 18. ЕДИНИЦЫ

В этом параграфе мы выведем из наших результатов о классах иделей структурную теорему для единиц.

Пусть S — конечное непустое множество нормализованных нормирований; предположим еще, что S содержит все архимедовы нормирования. Множество элементов $\eta\in k$, таких, что

$$|\eta|_v=1 \qquad (v\notin S), \tag{1}$$

[1]) В группе I_k вводится дискретная топология.

образует группу по умножению, называемую группой S-единиц и обозначаемую через H_S. Если $k \supset \mathbf{Q}$ и S — в точности множество всех архимедовых нормирований, то H_S — группа единиц кольца целых элементов.

Лемма 18.1. *Пусть $0 < c < C < \infty$. Тогда множество S-единиц η, таких, что*

$$c \leqslant |\eta|_v \leqslant C \qquad (v \in S), \tag{2}$$

конечно.

Доказательство. Множество W иделей $\alpha = \{\alpha_v\}$, таких, что

$$|\alpha_v|_v = 1 \quad (v \notin S), \quad c \leqslant |\alpha_v|_v \leqslant C \quad (v \in S), \tag{3}$$

— компакт (как произведение компактных множеств с топологией произведения). Искомое множество единиц есть в точности пересечение множества W с дискретным подмножеством k группы J_k и, следовательно, одновременно компактно и дискретно, т. е. конечно.

Лемма 18.2. *Существует лишь конечное множество элементов $\varepsilon \in k$, таких, что $|\varepsilon|_v = 1$ для всех v, а именно это корни из единицы поля k и только они.*

Доказательство. Если $\varepsilon \in k$ — корень из единицы, то ясно, что $|\varepsilon|_v = 1$ для всех v. Обратно, по лемме 18.1 (с любым S и $C = c = 1$) найдется лишь конечное множество элементов $\varepsilon \in k$, таких, что $|\varepsilon|_v = 1$ для всех v. Они образуют группу по умножению и, следовательно, все являются корнями из единицы.

Теорема 18.1 (теорема о единицах). *H_S является прямой суммой конечной циклической группы и свободной абелевой группы ранга $s - 1$.*

Доказательство. Чтобы обойти незначительные трудности в обозначениях, мы рассмотрим только случай, когда $\mathbf{Q} \subset k$ и S — множество архимедовых нормирований.

Пусть J_S состоит из иделей $\alpha = \{\alpha_v\}$, таких, что $|\alpha_v|_v = 1$ $(v \notin S)$; положим

$$J_S^1 = J_S \cap J_k^1.$$

Ясно, что подгруппа J_S^1 открыта в группе J_k^1 и, значит, подгруппа

$$J_S^1/H_S = J_S^1/(J_S^1 \cap k^*) \tag{4}$$

открыта в J_k^1/k^*. Как подгруппа, она также и замкнута и, следовательно, компактна (§ 16).

Рассмотрим отображение

$$\lambda : J_S \to \underbrace{\mathbf{R}^+ \oplus \mathbf{R}^+ \oplus \ldots \oplus \mathbf{R}^+}_{s \text{ раз}}$$

(где $\mathbf{R}^+$ — аддитивная группа вещественных чисел), задаваемое формулой

$$\alpha \to \{\log|\alpha_1|_1, \log|\alpha_2|_2, \ldots, \log|\alpha_s|_s\},$$

где s — число нормирований в S. Ясно, что отображение λ непрерывно и сюръективно.

Ядро отображения λ, ограниченного на группу H_S, состоит в точности из тех ε, для которых $|\varepsilon|_v = 1$ при любых v, и потому это ядро является конечной циклической группой по лемме 18.2. По лемме 18.1 найдется лишь конечное число элементов $\eta \in H_S$, таких, что

$$\frac{1}{2} \leqslant |\eta|_v \leqslant 2, \qquad v \in S. \tag{5}$$

Значит, группа $\lambda(H_S)$ (обозначим ее через Λ) дискретна.

Далее, $T = \lambda(J_S^1)$ — это в точности множество тех $(x_1, \ldots, x_s)$, для которых $x_1 + x_2 + \ldots + x_s = 0$, т. е. $(s-1)$-мерное вещественное векторное пространство. Наконец, группа T/Λ компактна как непрерывный образ компактного множества (4). Значит, Λ — свободная группа с $s - 1$ образующими, как и утверждалось.

Конечно, эта структурная теорема (Дирихле) и конечность числа классов идеалов (Минковский) были известны задолго до введения понятия иделей. Более общепринятым является вывод компактности группы J_k^1/k^* из этих теорем, а не обратно.

§ 19. ВКЛЮЧЕНИЕ И ОТОБРАЖЕНИЯ НОРМ ДЛЯ АДЕЛЕЙ, ИДЕЛЕЙ И ИДЕАЛОВ

Пусть K — конечное расширение глобального поля k. Мы уже видели (лемма 14.1), что существует естественный изоморфизм

$$V_k \otimes_k K = V_K \tag{1}$$

в алгебраическом и топологическом смыслах; значит, $V_k = V_k \otimes_k k$ может быть естественным образом рассматриваемо как подкольцо кольца V_K, которое замкнуто в топологии V_K. Это вложение V_k в V_K называется отображением вложения, или конорменным отображением, и обозначается

$$\mathrm{con} : \boldsymbol{\alpha} \longrightarrow \mathrm{con}\,\boldsymbol{\alpha} = \mathrm{con}_{K/k}\boldsymbol{\alpha} \in V_K \quad (\boldsymbol{\alpha} \in V_K).$$

Точнее, если $\mathbf{A} = \mathrm{con}\,\boldsymbol{\alpha}$, то компоненты удовлетворяют равенству

$$A_V = \alpha_v \subset k_v \subset K_V, \tag{2}$$

где V пробегает все нормализованные нормирования поля K и v — нормализованное нормирование поля k, продолжением которого является V. Если $k \subset L \subset K$, то

$$\mathrm{con}_{K/k}\,\boldsymbol{\alpha} = \mathrm{con}_{L/k}\,(\mathrm{con}_{K/L}\,\boldsymbol{\alpha}). \tag{3}$$

Наконец, на главных аделях конорменное отображение совпадает в точности с обычным вложением поля k в K.

Принято отождествлять $\mathrm{con}_{K/k}\,\boldsymbol{\alpha}$ с $\boldsymbol{\alpha}$; обычно это не ведет к недоразумениям.

Можно также определить отображения нормы и следа из V_K в V_k, повторяя обычную процедуру (ср. добавление А). Пусть $\omega_1, \ldots, \omega_n$ — базис поля K над k. Тогда ввиду изоморфизма (1) всякий элемент $\mathbf{A} \in V_K$ единственным образом представляется в виде

$$\mathbf{A} = \sum \boldsymbol{\alpha}_j \omega_j, \quad \boldsymbol{\alpha}_j \in V_K, \tag{4}$$

и отображение $\mathbf{A} \to \boldsymbol{\alpha}_j$ кольца V_K в V_k непрерывно по самому определению топологии тензорного произведения (§ 9). Значит, если мы определим элементы

$$\boldsymbol{\alpha}_{ij} = \alpha_{ij}\,(\mathbf{A}) \in V_k,$$

так что

$$\mathbf{A}\omega_i = \sum_j \boldsymbol{\alpha}_{ij}\omega_j, \tag{5}$$

то матрицы (α_{ij}) порядка $n \times n$ дадут непрерывное представление кольца V_K над V_k. В частности,

$$S_{K/k}\mathbf{A} = \sum \boldsymbol{\alpha}_{ii} \tag{6}$$

и

$$N_{K/k}\mathbf{A} = \det\,(\alpha_{ij}) \tag{7}$$

будут непрерывными функциями от $\mathbf{A}$, обладающими обычными формальными свойствами

$$S_{K/k}\,(\mathbf{A}_1 + \mathbf{A}_2) = S_{K/k}\mathbf{A}_1 + S_{K/k}\mathbf{A}_2, \tag{8}$$

$$S_{K/k}\,\mathrm{con}\,\boldsymbol{\alpha} = n\boldsymbol{\alpha}, \tag{9}$$

$$N_{K/k}\,(\mathbf{A}_1\mathbf{A}_2) = N_{K/k}\mathbf{A}_1 \cdot N_{K/k}\mathbf{A}_2, \tag{10}$$

$$N_{K/k}\,\mathrm{con}\,\boldsymbol{\alpha} = \boldsymbol{\alpha}^n. \tag{11}$$

Далее, нормы и следы операторов согласованы с погружениями k и K соответственно в V_k и V_K, т. е. при $\mathbf{A} \in K \subset V_K$ мы получим одинаковый результат, если будем вычислять $N_{K/k}\mathbf{A}$ и $S_{K/k}\mathbf{A}$ в K или в V_K, так что в наших обозначениях нет неопределенности.

Наконец, если $K \supset L \supset k$, то $V_k \subset V_L \subset V_K$ (рассматриваем конорму как отождествление), и, значит, имеют место обычные соотношения (ср. добавление А)

$$S_{L/k}\,(S_{K/L}\mathbf{A}) = S_{K/k}\mathbf{A} \tag{12}$$

и

$$N_{L/k}\,(N_{K/L}\mathbf{A}) = N_{K/k}\mathbf{A}. \tag{13}$$

Мы можем при желании расписать отображения (6) и (7) покомпонентно. Пусть $V_1, \ldots, V_J$ будут продолжениями какого-либо заданного нормирования поля k на расширение K. Обозначим $\bigoplus\limits_{1 \leqslant j \leqslant J} K_j$ через K_v. Тогда (§ 9)

$$K_v = k_v \otimes_k K = \bigoplus_{1 \leqslant i \leqslant n} k_v\omega_i, \tag{14}$$

где k_v и K_j — пополнения полей k и K по отношению к нормированиям v и V_j соответственно. Любой элемент $\mathbf{A} \in V_K$ можно рассматривать как элемент с компонентами

$$A_{V_1} \oplus \ldots \oplus A_{V_J} = A_v \tag{15}$$

в K_v, и тогда компоненты матриц представления (5) для $\mathbf{A}$ будут в точности представлениями для A_v. В частности,

$$S_{K/k}\,\mathbf{A} = \{S_{K_v/k_v} A_v\} \tag{16}$$

и

$$N_{K/k}\mathbf{A} = \{N_{K_v/k_v} A_v\}. \tag{17}$$

Наконец, используя последние замечания § 9, мы получаем равенства

$$S_{K/k}\mathbf{A} = \{\sum_{V|v} S_{K_V/k_v}(A_V)\}_v \tag{18}$$

и

$$N_{K/k}\mathbf{A} = \{\prod_{V|v} N_{KV/k_v} A_V\}_v, \tag{19}$$

где запись $V \mid v$ означает, что V есть продолжение нормирования v.

Рассмотрим теперь следствия для иделей. Если $\boldsymbol{\alpha}$ — идель, то из определения (2) ясно, что $\mathrm{con}_{K/k}\boldsymbol{\alpha}$ — тоже идель, так что мы имеем вложение

$$\mathrm{con}_{K/k} : J_k \longrightarrow J_K,$$

которое, очевидно, является гомеоморфизмом группы J_k на замкнутое подмножество группы J_K. Далее, если $\mathbf{A} \in \in J_K \subset V_K$, так что элемент $\mathbf{A}$ обратим, то из формулы (9) следует, что $N_{K/k}\mathbf{A}$ тоже обратим, т. е. является элементом из группы J_k. Значит, получено отображение

$$N_{K/k} : J_K \longrightarrow J_k,$$

непрерывное по определению топологии в иделях (§ 16) и удовлетворяющее условиям (10), (11), (13) и (19).

Наконец, рассмотрим конормненное и норменное отображения для идеалов, когда k — конечное расширение поля $\mathbf{Q}$. Ядро отображения (§ 17)

$$J_k \longrightarrow I_k$$

группы иделей в группу идеалов — это в точности группа иделей $\boldsymbol{\alpha} = \{\alpha_v\}$, для которых $|\alpha_v|_v = 1$ во всех неархимедовых нормированиях v. Обозначим ее через U_k. Если K — конечное расширение поля k, то ясно, что

$$\mathrm{con}_{K/k} U_k \subset U_K$$

и из леммы 11.1 и равенства (17) следует включение

$$N_{K/k} U_K \subset U_k.$$

Значит, переходя от группы J_k к фактору, мы получим индуцированные отображения

$$\mathrm{con}_{K/k} : I_k \longrightarrow I_K,$$
$$N_{K/k} : I_K \longrightarrow I_k$$

с обычными свойствами (10), (11) и (13); эти отображения согласованы с нормой и конормой элементов из K и k, если рассматривать главные идеалы. По определению (2) мы получаем соотношение

$$\mathrm{con}_{K/k}\, v = \sum_{V|v} e_V V, \tag{20}$$

в котором положительные целые числа e_V определены равенствами

$$|\pi_v|_V = |\Pi_V|_V^{e_V}, \tag{21}$$

где π_v и Π_V — простые элементы полей k_v и K_V соответственно. Аналогично из (19) следует равенство

$$N_{K/k} V = f_V v, \tag{22}$$

где f_V — степень поля вычетов нормирования V над полем вычетов нормирования v. Мы заметим, кстати, что условия (11), (20) и (22) влекут за собой равенство

$$\sum_{V|v} e_V f_V = n,$$

как и должно быть, поскольку

$$e_V f_V = [K_V : k_v].$$

Аналогично, когда k — конечное расширение поля $\mathbf{F}(t)$, определяются конорма и норма дивизора с соответствующими свойствами.

Добавление А

НОРМЫ И СЛЕДЫ

Пусть R — коммутативное кольцо с единицей. Под векторным пространством V над R размерности n мы будем понимать свободный R-модуль с n образующими $\omega_1, \ldots, \omega_n$, совокупность которых называется *базисом*. Если $\omega'_1, \ldots, \omega'_n$ — другой базис, то найдутся $u_{ij}, v_{ij} \in R$, такие, что

$$\omega_i = \sum_j u_{ij}\omega'_j, \quad \omega'_j = \sum v_{ij}\omega_i \tag{1}$$

и

$$\sum_j u_{ij}v_{jl} = \sum v_{ij}u_{jl} = \delta_{il} \ (\delta_{il} — \text{символ Кронекера}). \qquad (2)$$

Множество всех R-линейных эндоморфизмов пространства V есть кольцо, которое мы обозначим через $\mathrm{End}_R V$. Кольцо R погружается в $\mathrm{End}_R V$, если отождествить элемент $b \in R$ с умножением на него в V, как мы и сделаем. Кольцо $\mathrm{End}_R V$ изоморфно, но не канонически, кольцу всех матриц порядка $n \times n$ с элементами из R. Изоморфизм становится каноническим, если в V фиксирован какой-либо базис. Действительно, если $\beta \in \mathrm{End}_R V$ и

$$\beta\omega_i = \sum_j b_{ij}\omega_j \qquad (b_{ij} \in R), \qquad (3)$$

то взаимно однозначное соответствие между β и транспонированной матрицей (b_{ji}) есть изоморфизм колец.

Для $\beta \in \mathrm{End}_R V$ мы обозначим через

$$F_\beta(x) = \det(x\delta_{ij} — b_{ij}) \qquad (4)$$

характеристический многочлен в R. Используя равенство (2), легко увидеть, что многочлен $F_\beta(x)$ не зависит от выбора базиса в пространстве V. Теорема Гамильтона — Кэли утверждает, что

$$F_\beta(\beta) = 0\ ^1). \qquad (5)$$

Мы определим *след*

$$S_{V/R}(\beta) = S(\beta) = \sum_i b_{ii} =$$

$$= — \text{коэффициент при } x^{n-1} \text{ в } F_\beta(x) \qquad (6)$$

и *норму*

$$N_{V/R}(\beta) = N = \det(b_{ij}) =$$

$$= (-1)^n \text{ свободный член в } F_\beta(x), \qquad (7)$$

[1]) Доказательство. Перепишем (3) в виде $\sum_j (\delta_{ij}\beta - b_{ij})\,\omega_j = 0$. Действуя в коммутативном кольце $R[\beta]$, умножим это уравнение на алгебраические дополнения к ω_1 и сложим. Тогда $\omega_2, \ldots, \omega_n$ исчезнут, и мы получим равенство $F_\beta(\beta)\,\omega_1 = 0$. Аналогично $F_\beta(\beta)\,\omega_j = 0$ $(2 \leqslant j \leqslant n)$, откуда $F_\beta(\beta) = 0$.

которые не зависят от выбора базиса, поскольку это верно для $F_\beta(x)$. Ясно, что

$$S(\beta_1 + \beta_2) = S(\beta_1) + S(\beta_2), \qquad (8)$$

$$S(b) = nb \ (b \in R), \qquad (9)$$

$$N(\beta_1\beta_2) = N(\beta_1)\,N(\beta_2), \qquad (10)$$

$$N(b) = b^n \ (b \in R), \qquad (11)$$

потому что соответствие (3) между $\beta \in \mathrm{End}_R V$ и матрицей (b_{ji}) является изоморфизмом колец.

Лемма А.1. *Пусть t трансцендентно над кольцом R. Тогда*

$$N(t — \beta) = F_\beta(t). \qquad (12)$$

Здесь, конечно, подразумевается, что мы рассматриваем векторное пространство V с базисом $\omega_1, \ldots, \omega_n$, определенное над $R[t]$, и β, заданное при помощи соотношения (3).

Доказательство. Мы имеем

$$(t — \beta)\,\omega_i = \sum_j (t\delta_{ij} — b_{ij})\,\omega_j$$

и, значит, в силу определений (4) и (7)

$$N(t — \beta) = \det(t\delta_{ij} — b_{ij}) = F_\beta(t).$$

Следствие. *Равенство* (12) *верно для любого $t \in R$.*

Лемма А.2. *Пусть $\beta_1, \ldots, \beta_l \in \mathrm{End}_R V$, и пусть t трансцендентно над R. Тогда*

$$N(t^l + \beta_1 t^{l-1} + \ldots + \beta_l) = t^{nl} + g_1 t^{nl-1} + \ldots + g_{nl}, \qquad (13)$$

где $g_1, \ldots, g_{nl} \in R$ и, в частности,

$$g_1 = S(\beta_1), \quad g_{nl} = N(\beta_l). \qquad (14)$$

Доказательство аналогично доказательству леммы А.1 и оставляется читателю.

Пусть теперь R и $P \subset R$ — коммутативные кольца с единицей, и предположим, что кольцо R, рассматриваемое как P-модуль, свободно и имеет конечное число образующих, скажем, $\Omega_1, \ldots, \Omega_m$ (т. е. R является m-мерным P-векторным пространством). Пусть V будет n-мерным R-векторным

пространством с базисом $\omega_1, \ldots, \omega_n$. Тогда R можно также рассматривать как mn-мерное P-векторное пространство с базисом

$$\Omega_i\omega_j \quad (1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n),$$

и, очевидно, существует естественное вложение кольца $\mathrm{End}_R V$ в $\mathrm{End}_P V$. Теперь мы можем доказать следующее утверждение.

Теорема А.1. *Пусть*

$$\beta \in \mathrm{End}_R V \subset \mathrm{End}_P V. \tag{15}$$

Тогда

$$S_{V/P}(\beta) = S_{R/P}(S_{V/R}(\beta)), \tag{16}$$

$$N_{V/P}(\beta) = N_{R/P}(N_{V/R}(\beta)). \tag{17}$$

Кроме того,

$$\Phi(x) = N_{R/P}F(x), \tag{18}$$

где $\Phi(x) \in P[x]$, $F(x) \in R[x]$ — *характеристические многочлены элемента* β *соответственно в кольцах* $\mathrm{End}_P V$ *и* $\mathrm{End}_R V$.

Доказательство. Пусть элемент β задан при помощи формулы (3); зададим $\gamma \in \mathrm{End}_R V$ формулами

$$\begin{aligned} \gamma\omega_1 &= \omega_1 - \sum_{j>1} b_{ij}\omega_j, \\ \gamma\omega_i &= b_{11}\omega_i \quad (i > 1). \end{aligned} \tag{19}$$

Тогда для $\alpha = \gamma\beta$ получаем

$$\begin{aligned} \alpha\omega_1 &= b_{11}\omega_1, \\ \alpha\omega_i &= b_{i1}\omega_1 + \sum_{j>1}(b_{11}b_{ij} - b_{i1}b_{1j})\,\omega_j = \\ &= b_{i1}\omega_1 + \sum_{j>1}\alpha_{ij}\omega_j, \end{aligned} \tag{20}$$

где $a_{ij} = b_{i1}b_{1j} - b_{i1}b_{1j}$. Значит,

$$N_{V/R}\alpha = b_{11}N_{W/R}\alpha^*, \tag{21}$$

где W является $(n-1)$-мерным R-векторным пространством, натянутым на $\omega_2, \ldots, \omega_n$, а α^* есть R-линейное ото-

бражение

$$\omega_i \longrightarrow \sum_{j>1}\alpha_{ij}\omega_j \quad (i > 1).$$

Следовательно,

$$N_{R/P}(N_{V/R}\alpha) = N_{R/P}b_{11} \cdot N_{R/P}(N_{W/R}\alpha^*). \tag{22}$$

Теперь используем индукцию по размерности n, принимая во внимание, что теорема тривиальна при $n = 1$. Так как W имеет размерность $n - 1$, то из индуктивного предположения мы имеем

$$N_{R/P}(N_{W/P}\alpha^*) = N_{W/P}\alpha^*. \tag{23}$$

С другой стороны, непосредственно из (20) следует равенство

$$N_{V/P}\alpha = N_{R/P}b_{11} \cdot N_{W/P}\alpha^*,$$

так что

$$N_{V/P}\alpha = N_{R/P}N_{V/P}\alpha. \tag{24}$$

Далее, ясно, что

$$N_{V/P}\gamma = N_{R/P}N_{V/P}\gamma = (N_{R/P}b_{11})^{n-1}.$$

Так как $\alpha = \beta\gamma$ и обе функции $N_{V/P}$ и $N_{R/P}N_{V/P}$ мультипликативны (по формуле (10)), то из (24) следует равенство

$$(N_{R/P}b_{11})^{n-1}N_{V/P}\beta = (N_{R/P}b_{11})^{n-1}N_{R/P}(N_{V/P}\beta). \tag{25}$$

Если элемент $N_{R/P}b_{11}$ обратим, то равенство (17) получается немедленно. В общем случае, однако, это не так, и мы должны использовать несложный искусственный прием.

Пусть t трансцендентно над кольцом R, и пусть β_t будет преобразованием, полученным из β заменой b_{11} на $b_{11} + t$ (все остальные коэффициенты b_{ij} остаются неизменными). Тогда условие (25), примененное к β_t, дает равенство

$$(N_{R/P}(b_{11}+t))^{n-1}N_{V/P}\beta_t = N_{R/V}(b_{11}+t)^{n-1}N_{R/P}(N_{V/R}\beta_t). \tag{26}$$

Все нормы, входящие в (26), являются многочленами от t. Сравнивая коэффициенты при степенях t в (26), начиная со старших, получаем, что

$$N_{V/P}\beta_t = N_{R/P}(N_{V/P}\beta_t), \tag{27}$$

потому что коэффициент при наивысшей степени t в $N_{R/P}(b_{11}+t)$ равен единице. Тогда мы получаем равенство (17), полагая $t=0$.

Теперь мы докажем равенство (18). По лемме А.1 имеют место равенства

$$\Phi(x)=N_{V/P}(x-\beta), \quad F(x)=N_{V/R}(x-\beta),$$

так что равенство (18) получается из (17) заменой β на $x-\beta$.

Наконец, равенство (16) следует из (18) при помощи определения (6) и первого из равенств (14).

Когда R является полем, то все несколько упрощается, так как всякий конечно порожденный модуль V над полем свободен, т. е. является векторным пространством. Далее, всякий элемент $\beta \in \mathrm{End}_R V$ в этом случае имеет минимальный многочлен, т. е. многочлен $f(x)$ наинизшей степени со старшим коэффициентом 1, такой, что $f(\beta)=0$.

Для многочлена $g(x) \in k[x]$ равенство $g(\beta)=0$ имеет место тогда и только тогда, когда $g(x)$ делится на $f(x)$ в кольце $k[x]$. В частности, теорема Гамильтона — Кэли (5) теперь утверждает, что $f(x)$ делит характеристический многочлен $F_\beta(x)$.

Наконец, справедлива следующая

Теорема А.2. *Пусть K — поле конечной степени n над полем k, и пусть $\beta \in K$. Тогда степень m минимального многочлена $f(x)$ для β над полем k делит n и*

$$F(x)=(f(x))^{n/m},$$

где $F(x)$ — характеристический многочлен элемента β. В частности,

$$S_{K/k}(\beta)=\frac{n}{m}(\beta_1+\ldots+\beta_m),$$

$$N_{K/k}(\beta)=(\beta_1, \beta_2, \ldots, \beta_m)^{n/m},$$

где $\beta_1, \ldots, \beta_m$ — корни многочлена $f(x)$ в каком-либо поле разложения.

Доказательство. Предположим вначале, что $K=k(\beta)$. Тогда минимальный многочлен $f(x)$ и характеристический многочлен $F(x)$ для β имеют одинаковые степени и одинаковые старшие коэффициенты, так что $F(x)=f(x)$, согласно замечанию, предшествующему формулировке теоремы.

Общий случай теперь следует из теоремы А.1 при $V=K$, $R=k(\beta)$, $P=k$ с помощью равенства (11).

Добавление Б

СЕПАРАБЕЛЬНОСТЬ

В этой книге нас в основном интересуют сепарабельные алгебраические расширения. Здесь мы отметим их наиболее важные элементарные свойства.

Лемма Б.1. *Пусть K, M — расширения конечной степени поля k. Тогда найдется самое большее $[K:k]$ вложений поля K в поле M, которые оставляют каждый из элементов поля k на месте.*

Доказательство тривиально, когда $K=k(\alpha)$ для некоторого α (нужно рассмотреть минимальный многочлен для α). В общем случае строится башня

$$k=K_0 \subset K_1 \subset \ldots \subset K_J=K, \tag{1}$$

где $K_j=K_{j-1}(\alpha_{j-1})$, и используется индукция по J.

Определение. *Конечное расширение K поля k называется сепарабельным, если найдется некоторое конечное расширение M поля k, такое, что существует $[K:k]$ различных вложений поля K в M, оставляющих каждый из элементов поля k на месте. В противном случае K называется несепарабельным.*

Следствие 1. *Пусть $K \supset L \supset k$. Если K сепарабельно над k, то также сепарабельны K над L и L над k.*

Доказательство. По лемме 1 найдется самое большее $[L:k]$ различных вложений поля L в M и, снова по лемме 1, каждое из них может быть продолжено не более чем $[K:L]$ способами до вложения поля K в M. По определению имеется

$$[K:k]=[K:L][L:k]$$

вложений поля K в M, так что в обоих случаях имеет место равенство.

Следствие 2. *Пусть $\alpha \in K$, где K сепарабельно над k, и пусть $\alpha_1, \ldots, \alpha_m$ будут корнями в поле M неприводимого многочлена $f(x)$ для α над полем k. Тогда элементы $\sigma_i \alpha$ $(1 \leqslant i \leqslant n = [K : k])$, где $\sigma_1, \ldots, \sigma_n$ — вложения поля K в M, в точности совпадают с элементами $\alpha_1, \ldots, \alpha_m$ (каждый берется n/m раз).*

Доказательство. Достаточно в предыдущих рассуждениях положить $L = k(\alpha)$.

Следствие 3.

$$S_{K/k}(\alpha) = \sum_i \sigma_i \alpha.$$

Доказательство получается из теоремы А.2 и предыдущего следствия.

Лемма Б.2. *Пусть K — конечное расширение поля k, и пусть σ — вложение поля k в некоторое поле M. Тогда найдутся конечное расширение M_1 поля M и вложение σ_1 поля K в M_1, которое совпадает с σ на поле k.*

Доказательство тривиально, если $K = k(\alpha)$, а в общем случае получается с помощью башни (1).

Теорема Б.1. *Пусть K и L — сепарабельные расширения полей L и k соответственно. Тогда K — сепарабельное расширение поля k.*

Доказательство. Пусть U — конечное расширение поля L и

$$\tau_i\colon K \to U \quad (1 \leqslant i \leqslant [K : L])$$

— вложения, продолжающие тождественное отображение поля L в себя; аналогично пусть V — конечное расширение поля k и вложения

$$\sigma_j\colon L \to V \quad (1 \leqslant j \leqslant [L : K])$$

продолжают тождественное отображение поля k. Повторно применяя лемму Б.2, построим конечное расширение M поля V и $[L : k]$ вложений

$$\sigma'_j\colon U \to M \quad (1 \leqslant j \leqslant [L : k]),$$

продолжающих σ_j. Тогда всевозможные $\sigma'_j\tau_i$ дают

$$[K : L]\,[L : k] = [K : k]$$

различных вложений поля K в M, продолжающих тождественное отображение поля k.

Следствие. *Всякое конечное расширение поля характеристики нуль сепарабельно.*

Доказательство очевидно для простого расширения $k(\alpha)$ поля k; в общем случае нужно применить теорему 1 к башне простых расширений.

Теорема Б.2. *Всякое сепарабельное расширение K поля k является простым, т. е. $K = k(\gamma)$ для некоторого γ.*

Замечание. Обратное, конечно, неверно.

Доказательство. Если k — конечное поле, то и поле K конечно, и, значит, согласно структурной теории конечных полей, $K = \Pi(\alpha)$ для некоторого $\alpha \in K$ (здесь Π — простое поле). Поэтому мы должны рассмотреть только случай бесконечного поля k. Предположим вначале, что $K = k(\alpha, \beta)$, и пусть $\sigma_1, \ldots, \sigma_n$, где $n = [K : k]$, будут различными вложениями поля K в некоторое поле M. Если $i \neq j$, то из различности вложений следует, что имеет место хотя бы одно из неравенств

$$\sigma_i\alpha \neq \sigma_j\alpha \quad \text{или} \quad \sigma_i\beta \neq \sigma_j\beta.$$

Значит, мы можем найти элементы $a, b \in k$, удовлетворяющие конечному множеству неравенств

$$a(\sigma_i\alpha - \sigma_j\alpha) + b(\sigma_i\beta - \sigma_j\beta) \neq 0 \quad (i \neq j).$$

Положим

$$\gamma = a\alpha + b\beta,$$

так что

$$\sigma_i\gamma \neq \sigma_j\gamma \quad (i \neq j).$$

Элементы $\sigma_i\gamma$ являются корнями неприводимого уравнения для γ над полем k; поэтому

$$[k(\gamma) : k] \geqslant n.$$

Но $k(\gamma) \subset K$ и, значит, $K = k(\gamma)$.

В общем случае, когда $K = k(\alpha_1, \alpha_2, \ldots, \alpha_J)$, где $J > 2$, можно использовать индукцию по J. Мы получаем, что $k(\alpha_2, \ldots, \alpha_J) = k(\beta)$ для некоторого β и, значит, $k(\alpha_1, \beta) = k(\gamma)$.

Теорема Б.3. *Пусть K — сепарабельное расширение поля k. Тогда*

$$S(\alpha, \beta) = S_{K/k}(\alpha\beta)$$

— невырожденная симметрическая билинейная форма на K, рассматриваемом как векторное пространство над полем k.

Доказательство. Доказывать нужно только невырожденность. Пусть $\omega_1, \ldots, \omega_n$ — базис в K над полем k, и пусть

$$D = \det (S_{K/k}(\omega_i\omega_j))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}.$$

Утверждение теоремы эквивалентно тому, что $D \neq 0$. Обозначим через $\sigma_1, \ldots, \sigma_n$ различные вложения поля K в некоторое поле M. По следствию 3 из леммы Б.1 мы имеем, что

$$D = \Delta^2,$$

где

$$\Delta = \det (\sigma_i\omega_j)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}.$$

По теореме Б.2 $K = k(\gamma)$ и, значит, можно положить $\omega_j = \gamma^{j-1}$. Тогда

$$\Delta = \prod_{i<j} (\sigma_j\gamma - \sigma_i\gamma) \neq 0,$$

что и требовалось доказать [1]).

Теперь выясним, при каких условиях простое расширение $k(\alpha)$ поля k сепарабельно. Пусть $f(x)$ — неприводимый многочлен в кольце $k[x]$, и пусть $f'(x)$ — его производная.

Если $f'(x) \neq 0$, то многочлен $f'(x)$ взаимно прост с $f(x)$, так как имеет меньшую степень, и потому найдутся

[1]) Вместо того факта, что $K = k(\gamma)$, мы могли бы использовать теорему Артина о том, что любые вложения одного поля в другое линейно независимы (см. [4] или [1]).

многочлены $a(x)$, $b(x) \in k[x]$, такие, что

$$a(x) f(x) + b(x) f'(x) = 1.$$

Значит, если $f(\beta) = 0$ в каком-либо расширении поля k, то $f'(\beta) \neq 0$, так что β — простой корень. Поэтому число корней многочлена $f(x)$ в поле разложения равно его степени.

С другой стороны, если $f'(x) \equiv 0$, то всякий корень многочлена $f(x)$ — кратный, так что общее количество корней меньше, чем степень. В первом случае мы назовем многочлен $f(x)$ сепарабельным, во втором — несепарабельным. Второй случай имеет место тогда и только тогда, когда $f(x) = g(x^p)$ для некоторого $g(x) \in k[x]$, где p — характеристика поля k.

Лемма Б.3. *Необходимым и достаточным условием того, что поле $k(\alpha)$ сепарабельно над k, является сепарабельность неприводимого многочлена $f(x) \in k[x]$ для α.*

Доказательство очевидно.

Следствие 1. *Пусть $K \supset k$, и пусть поле $k(a)$ сепарабельно над k. Тогда $K(\alpha)$ сепарабельно над K.*

Доказательство. Неприводимый над K многочлен $F(x) \in K[x]$ делит $f(x)$.

Следствие 2. *Необходимым и достаточным условием сепарабельности поля K над полем k является сепарабельность над k каждого элемента из K.*

Доказательство. Предположим, что всякий элемент из K сепарабелен и что поле K задано башней

$$k = K_0 \subset K_1 \subset \ldots \subset K_J = K,$$

где $K_j = K_{j-1}(\alpha_{j-1})$. Тогда поле K_j сепарабельно над K_{j-1} в силу предыдущего следствия, и потому поле K сепарабельно над k по теореме Б.1.

Обратное утверждение вытекает из следствия 1 из леммы 1.

Для несепарабельного случая положение полностью противоположно, как показывает

Теорема Б.4. *Пусть поле K несепарабельно над k. Тогда след $S_{K/k}(\beta)$ равен нулю для всех $\beta \in K$.*

Доказательство. Предположим вначале, что $K=k(\alpha)$, где $\alpha^p\in k$, $\alpha\notin k$ и p — характеристика. Тогда элементы

$$\omega_1=1,\quad \omega_2=\alpha,\ \ldots,\ \alpha_p=\alpha^{p-1}$$

образуют базис в K над полем k. Если $\beta=b_1+b_2\alpha+\ldots+b_p\alpha^{p-1}$ и $b_j\in k$, то

$$\beta\omega_i=\sum b_{ij}\omega_j,\ b_{ij}\in k,$$

где, очевидно,

$$b_{ii}=b_1\quad (1\leqslant i\leqslant p).$$

Значит,

$$S_{K/k}\beta=\sum_i b_{ii}=pb_1=0.$$

Теперь пусть K — любое несепарабельное расширение поля k. Согласно следствию 2 из леммы Б.3, найдется несепарабельный элемент $\alpha\in K$. Положим $L=k(\alpha)$, $M=k(\alpha^p)$, так что L — расширение поля M только что рассмотренного вида. Утверждение теоремы следует теперь из транзитивности следа:

$$S_{K/k}\beta=S_{M/k}(S_{L/M}(S_{K/L}\beta)).$$

Добавление В

ЛЕММА ГЕНЗЕЛЯ

Под этим названием в литературе фигурирует целый ряд результатов, суть которых состоит в утверждении о том, что существование приближенного решения уравнения или системы уравнений в полном нормированном поле влечет за собой существование точного решения, к которому данное является приближением, при условии, что приближенное решение «достаточно хорошее». Эти результаты являются, собственно говоря, примерами процесса нахождения решений методом последовательной аппроксимации, который восходит по крайней мере к Ньютону. В этом приложении мы дадим один типичный образец.

Лемма В.1. *Пусть k — поле, полное относительно неархимедова нормирования $|\ |$, и пусть*

$$f(X)\in\mathfrak{o}[X], \tag{1}$$

где $\mathfrak{o}\subset k$ — кольцо целых элементов относительно этого нормирования. Пусть, далее, $\alpha_0\in\mathfrak{o}$ таково, что

$$|f(\alpha_0)|<|f'(\alpha_0)|^2, \tag{2}$$

где $f'(X)$ — (формальная) производная многочлена $f(X)$. Тогда существует решение $X=\alpha$ уравнения $f(X)=0$, такое, что

$$|\alpha-\alpha_0|\leqslant|f(\alpha)|/|f'(\alpha)|. \tag{3}$$

Доказательство (набросок). Пусть многочлены $f_i(X)\in\mathfrak{o}(X)$ определены тождеством

$$f_1(X+Y)=f_1(X)+f_1(X)\cdot Y+\ldots+f_j(X)\cdot Y^j+\ldots, \tag{4}$$

где X, Y — независимые переменные, так что $f_1(X)=f'(X)$. Определим β_0 из равенства

$$f(\alpha_0)+\beta_0 f_1(\alpha_0)=0. \tag{5}$$

Тогда ввиду (4) и в силу того, что $f_i(\alpha_0)\in\mathfrak{o}$, мы получаем неравенства

$$|f(\alpha_0+\beta_0)|\leqslant\max_{j\geqslant 2}|f_j(\alpha_0)\beta_0^j|\leqslant$$

$$\leqslant\max_{j\geqslant 2}|\beta_0|\ \leqslant|f(\alpha_0)|^2/|f_1(\alpha_0)|^2<|f(\alpha_0)|. \tag{6}$$

Используя аналог тождества (4) для многочлена $f_1(X)$, легко проверить, что

$$|f_1(\alpha_0+\beta_0)-f_1(\alpha_0)|<|f_1(\alpha_0)|.$$

Итак, полагая $\alpha_1=\alpha_0+\beta_0$, получаем

$$|f(\alpha_1)|\leqslant|f(\alpha_0)|^2/|f_1(\alpha_0)|^2,$$

$$|f_1(\alpha_1)|=|f_1(\alpha_0)$$

и

$$|\alpha_1-\alpha_0|\leqslant|f(\alpha_0)|/|f(\alpha_1)|.$$

Повторяя эту процедуру с α_1 и так далее, получаем последовательность α_0, α_1, α_2, ..., которая, как легко видеть,

фундаментальна. Ввиду полноты поля k она имеет предел $\lim_{n\to\infty} \alpha_n = \alpha \in k$, который, очевидно, и будет искомым решением.

В действительности решение (3) не только существует, но и единственно, потому что если $\alpha + \beta$, $\beta \neq 0$,— другое решение, то легко получить противоречие, полагая в тождестве (4) $X = \alpha$, $Y = \beta$.

ЛИТЕРАТУРА

Адамсон (Adamson)
[1] Introduction to field theory, Oliver and Boyd.

Артин (Artin E.)
[2] Theory of algebraic numbers, Striker, Göttingen, 1956.
[3] Representatives of the connected component of the idele class group, Proc. Int. Simp. Algebraic Number Theory, Tokio — Nikko, 1955.
[4] Galois theory, Notre Dame, Paris, 1946. (Украинский перевод: Артин, Теория Галуа, «Радяньска школа», Киев, 1963.)

Артин, Тэйт (Artin E., Tate J.)
[5] Class fied theory, Harvard, 1951.

Вейль (Weil)
[6] Adeles and algebraic groups, Inst. Adv. Studies, Prinston, 1961. (Русский перевод: *Математика*, 8 : 4 (1964), 3—74.)
[7] On a certain type of the idele class group of an algebraic number field, Proc. Int. Simp. Algebraic Number Theory, Tokio — Nikko, 1955, 9—22.

Годман (Godement R.)
[8] Bourbaki seminars, exp. 171, 176.

Ивасава (Iwasawa K.)
[9] On the rings of valuation vectors, *Ann. Math.*, 57 (1953), 331—356.

Ленг (Lang S.)
[10] Algebraic numbers, Addison Wesley, 1964. (Русский перевод: Ленг С., Алгебраические числа, «Мир», М., 1966.)

Малер (Mahler K.)
[11] Inequalities for ideal bases, *J. Austr. Math. Soc.*, 4 (1964), 425—448.

ГЛАВА III

Круговые поля и расширения Куммера

Б. Дж. Бёрч

§ 1. КРУГОВЫЕ ПОЛЯ

Пусть K — любое поле характеристики нуль и $m > 1$ — целое число. Тогда существует минимальное расширение L поля K, такое, что многочлен $x^m - 1$ полностью распадается в L. Нули многочлена $x^m - 1$ образуют подгруппу мультипликативной группы поля L; это циклическая подгруппа (ибо такова любая конечная подгруппа мультипликативной группы поля). Образующие этой подгруппы называются первообразными корнями m-й степени из единицы. Если ζ — первообразный корень m-й степени из единицы, то любой нуль многочлена $x^m - 1$ является степенью этого корня, так что $L = K(\zeta)$. Ясно, что L — нормальное расширение поля K; мы будем писать $L = K(\sqrt[m]{1})$.

Если σ — элемент группы Галуа $G(L/K)$, то элемент $\sigma\zeta$ тоже должен быть первообразным корнем m-й степени из единицы, так что $\sigma\zeta = \zeta^k$ при некотором целом k, таком, что $(k, m) = 1$. Если ζ^a — другой первообразный корень, то $\sigma\zeta^a = \zeta^{ik}$; согласно этому, $\sigma \mapsto k$ является каноническим отображением группы $G(L/K)$ в мультипликативную группу $G(m)$ классов вычетов по модулю m, взаимно простых с m. В частности, $[L : K] \leqslant \phi(m)$.

Если $m = rs$, где $(r, s) = 1$, то существуют целые числа a, b, такие, что $ar + bs = 1$; тогда $\zeta = (\zeta^r)^a(\zeta^s)^b$, так что $K(\zeta) = K(\zeta^r, \zeta^s)$, т. е. расширение $K(\zeta)$ можно получить композицией расширений $K(\zeta^r)$ и $K(\zeta^s)$. Таким образом, вместо произвольных расширений достаточно рассматривать расширения $K(\sqrt[m]{1})$, где m — степень простого числа. Если простое число p нечетно, то группа $G(p^n)$ циклична; другими словами, если $m = p^n$, $L = K(\sqrt[m]{1})$, то

группа $G(L/K)$ — циклическая; с другой стороны, группа $G(2^n)$ порождается числами -1 и 5, так что если мы положим $\eta = \zeta + \zeta^{-1}$, где $\zeta^{2^n} = 1$, то $K(\zeta) = K(i, \eta)$, и группа $G[K(\eta)/K]$ — циклическая.

Нас особенно будут интересовать расширения $\mathbf{Q}(\sqrt[m]{1})$ и $\mathbf{Q}_p(\sqrt[m]{1})$; согласно гл. I (§ 4 и начало § 5), изучать разложение простого числа p в расширении $\mathbf{Q}(\sqrt[m]{1})$ поля $\mathbf{Q}$ — это то же самое, что изучать расширение $\mathbf{Q}_p(\sqrt[m]{1})$ поля $\mathbf{Q}_p$. Для того чтобы сделать абстрактные теоремы более прозрачными, мы будем иногда приводить несколько различных доказательств одного и того же утверждения. Хороший обзор круговых расширений дан в книгах Вейля [2] и Вайса [1], гл. 7.

Лемма 1.1. $\mathbf{Q}(\sqrt[m]{1})$ — *нормальное расширение поля* $\mathbf{Q}$ *степени* $\phi(m)$. *Его группа Галуа изоморфна группе* $G(m)$.

Доказательство (по Ван дер Вардену). Пусть ζ — первообразный корень m-й степени из единицы; согласно только что сказанному, достаточно показать, что уравнение минимальной степени для ζ над полем $\mathbf{Q}$ имеет степень $\phi(m)$. Другими словами, нужно доказать, что если $f(x) \in \mathbf{Z}[x]$ и $f(\zeta) = 0$, то $f(\zeta^a) = 0$, коль скоро $(a, m) = 1$. Ясно, что достаточно рассмотреть случай $a = p$, где p — простое число, не делящее m.

Рассмотрим поле k_p из p элементов; пусть $f(x)$ — многочлен, содержащийся в $\mathbf{Z}[x]$; обозначим его естественный образ в кольце $k_p[x]$ через $f^*(x)$. Пусть L^* — конечное расширение поля k_p, являющееся полем разложения многочлена $(x^m - 1)$; этот многочлен взаимно прост со своей производной mx^{m-1}, так что все его корни простые.

Предположим, что многочлен $x^m - 1$ распадается в кольце $\mathbf{Z}[x]$ на множители: $x^m - 1 = f_1(x) f_2(x) \dots f_r(x)$, где многочлены $f_i(x)$ неприводимы. Тогда в кольце $k_p[x]$ имеет место $(x^m - 1) = \prod_i f_i^*(x)$, и в поле L^* все нули всех многочленов $f_i^*(x)$, будучи корнями многочлена $x^m - 1$, различны. Выберем нумерацию для $\{f_i(x)\}$ так, чтобы ζ был корнем многочлена $f_1(x)$, и предположим, что ζ^p — корень многочлена $f_j(x)$. Тогда $f_1(x)$ делит $f_j(x^p)$, так что $f_1^*(x)$ делит $f_j^*(x^p)$. Пусть ζ^* — корень многочлена $f_1^*(x)$; тогда $f_j^*(\zeta^{*p}) = 0$ и, с другой стороны, $f_1^*(\zeta^{*p}) = [f_1^*(\zeta^*)]^p = 0$. Значит, f_j совпадает с f_1.

Лемма 1.2. *Если* $p \nmid m$, *то найдется единственный элемент* σ_p *группы Галуа* $G[\mathbf{Q}(\sqrt[m]{1})/\mathbf{Q}]$, *такой, что* $\sigma_p \alpha \equiv \alpha^p (p)$ *для всех целых* $\alpha \in \mathbf{Q}(\sqrt[m]{1})$. *Если* ζ — *первообразный корень* m-*й степени из единицы, то* σ_p *задается формулой* $\sigma_p(\sum a_i \zeta^i) = \sum a_i \zeta^{pi}$, *где* $a_i \in \mathbf{Q}$ (*элемент* σ_p *принято называть автоморфизмом Фробениуса*).

Доказательство. Базис поля $1, \zeta, \dots, \zeta^{\phi(m)-1}$ имеет дискриминант, взаимно простой с p. Следовательно, согласно гл. I, § 3, любое целое число поля может быть представлено в виде $\sum a_i \zeta^i / b$, где $a_1, \dots, a_{p-2}$, $b \in \mathbf{Z}$ и $(b, p) = 1$; таким образом, автоморфизм σ_p, определенный выше, дает как раз то, что нужно. Осталось показать, что он единствен. Действие элемента σ группы Галуа, очевидно, определяется его действием на ζ; ясно также, что всякий элемент σ переводит ζ в другой первообразный корень ζ^a, где $(a, m) = 1$. Нужно показать, что сравнение $\zeta^a \equiv \zeta^b (p)$ выполняется только в том случае, если $\zeta^a = \zeta^b$; другими словами, что сравнение $1 - \zeta^b \equiv 0 (p)$ имеет место только тогда, когда $\zeta^b = 1$.

Первый способ. Предположим, что $\zeta^b \neq 1$. Мы знаем, что

$$x^m - 1 = \prod_{i=1}^{m} (x - \zeta^i),$$

так что

$$mx^{(m-1)} = \sum_j \prod_{i \neq j} (x - \zeta^i)$$

и

$$m = \prod_{i=1}^{m-1} (1 - \zeta^i).$$

Поэтому $(1 - \zeta^b)$ делит m и, значит, p не делит $(1 - \zeta^b)$.

Второй способ. Рассмотрим пополнение $\mathbf{Q}_p$ поля $\mathbf{Q}$ и образуем расширение $\mathbf{Q}_p(\sqrt[m]{1})$. Пусть L^* — поле выче-

тов для поля $\mathbf{Q}_p(\sqrt[m]{1})$; тогда L^* представляет собой конечное расширение поля k_p и является полем разложения многочлена x^m-1. Имеет место включение $\mathbf{Q}(\sqrt[m]{1}) \subset \subset \mathbf{Q}_p(\sqrt[m]{1})$, так что естественное отображение ставит в соответствие каждому корню многочлена x^m-1 в поле L^* корень того же многочлена в поле $\mathbf{Q}(\sqrt[m]{1})$. Обратно, корни x^m-1 в поле L^* различны, и каждый из них по лемме Гензеля есть вычет элемента из $\mathbf{Q}_p(\sqrt[m]{1})$ (см. гл. I, лемма 7.1, или гл. II, добавление B). Таким образом, получено взаимно однозначное соответствие между корнями m-й степени из единицы в полях L^* и $\mathbf{Q}(\sqrt[m]{1})$, откуда все и следует.

Лемма 1.3. *Если $q=p^f$ — степень простого числа и ζ — первообразный корень q-й степени из единицы, то простое число p вполне разветвлено, а именно $(p)=(1-\zeta)^{\phi(q)}$.*

Первое доказательство. Положим $\lambda=1-\zeta$. Тогда $\zeta^q=1$, но $\zeta^{q/p}\neq 1$, так что λ является корнем многочлена $F(x)=[(1+x)^q-1]/[(1+x)^{q/p}-1]$. Многочлен F имеет старший коэффициент, равный 1, и свободный член p; легко проверить, что все остальные коэффициенты делятся на p. Таким образом, $F(x)=0$ — уравнение Эйзенштейна, а потому, согласно теореме 6.1 гл. I, $\mathbf{Q}_p(\sqrt[q]{1})$ — вполне разветвленное расширение поля $\mathbf{Q}_p$ степени $\phi(q)$ и $(p)=(\lambda)^{\phi(q)}$. Возвращаясь к $\mathbf{Q}\sqrt[q]{1}$, мы видим, что это поле представляет собой расширение поля $\mathbf{Q}$ степени $\phi(q)$ (тем самым мы получили в этом случае новое доказательство леммы 1) и число p вполне разветвлено в этом расширении.

Второе доказательство (более непосредственное). Если $(a, p)=(b, p)=1$, то сравнение $a\equiv bs\,(q)$ разрешимо, так что число

$$(1-\zeta^a)/(1-\zeta^b)=(1-\zeta^{bs})/(1-\zeta^b)=1+\zeta^b+\ldots+\zeta^{b(s-1)}$$

целое и аналогично число $(1-\zeta^b)/(1-\zeta^a)$ тоже целое; таким образом, $(1-\zeta^a)/(1-\zeta^b)$ — единица, коль скоро $(a, p)=(b, p)=1$. Кроме того,

$$p=\lim_{x\to 1}\frac{x^q-1}{x^{q/p}-1}=\lim_{x\to 1}\prod_{\substack{(a,\,p)=1\\ 0<a<q}}(x-\zeta^a)=(1-\zeta)^{\phi(q)}\prod\frac{1-\zeta^a}{1-\zeta},$$

так что идеал (p) является просто $\phi(q)$-й степенью идеала $(\lambda)=(1-\zeta)$.

Лемма 1.4. *Пусть ζ — первообразный корень m-й степени из единицы. Если число p — простое, не делящее число m, то p неразветвлено в поле $\mathbf{Q}(\sqrt[m]{1})$, и степень классов вычетов f_p (см. гл. I, § 5) равна наименьшему целому числу $f\geqslant 1$, такому, что $p^f\equiv 1\,(m)$.*

Доказательство (по Серру [3]). Рассмотрим расширение $\mathbf{Q}_p(\zeta)$ поля $\mathbf{Q}_p$; поле вычетов k_p состоит из p элементов. Многочлен x^m-1 разлагается в поле k_{p^f} на линейные множители тогда и только тогда, когда $m\mid(p^f-1)$. Возьмем наименьшее f, такое, что $p^f\equiv 1\,(m)$, и построим неразветвленное расширение L поля $\mathbf{Q}_p$ с полем вычетов k_{p^f} (см. гл. I, теорема 7.1). Как и во втором доказательстве леммы 1.2, строится мультипликативный гомоморфизм групп $k_{p^f}^*\to L^*$; таким образом, x^m-1 разлагается в L на линейные множители; и, очевидно, L — минимальное поле, обладающее этим свойством. Следовательно, $L=\mathbf{Q}_p(\zeta)$.

Возвращаясь к $\mathbf{Q}(\zeta)$, мы видим, что число p неразветвлено в этом поле, а степень классов вычетов равна f_p, что и требовалось доказать.

(В действительности лемма является непосредственным следствием свойств автоморфизма Фробениуса, описанного в лемме 1.2.)

Следствие. *Если $p\nmid m$, то p полностью распадается тогда и только тогда, когда $p\equiv 1\,(m)$.*

Лемма 1.5. *Если $q=p^f$ — степень простого числа и ζ — первообразный корень q-й степени из единицы, то дискриминант расширения $\mathbf{Q}(\zeta)$ поля $\mathbf{Q}$ равен $q^{\phi(q)}/p^{q/p}$;*

элементы $1, \zeta, \zeta^2, \ldots, \zeta^{\phi(q)-1}$ *составляют базис для* **Z***-модуля целых чисел в* $\mathbf{Q}(\zeta)$.

Доказательство. Рассмотрим вначале случай $t = 1$. Согласно леммам 1.3 и 1.4, единственным простым числом, разветвляющимся в поле $\mathbf{Q}(\zeta)$, является p, и ветвление числа p слабое, причем $e = p - 1$. Значит, согласно теореме 5.2 гл. I, дискриминант равен $p^{p^{n}-2}$. Поэтому в силу предложения 4.6 гл. I $1, \zeta, \zeta^2, \ldots, \zeta^{p^n-2}$ образуют базис, что и требовалось доказать.

В случае $t \geqslant 2$ ветвление дикое, так что из результатов гл. I следует только то, что дискриминант является степенью числа p, причем по меньшей мере равен $p^{\phi(q)}$. Мы дадим прямое доказательство того, что степени числа ζ образуют базис целых чисел; это доказательство проходит при любых t. Рассмотрим **Z**-модуль $\mathbf{Z}(\zeta)$. Согласно предложению 4.6 гл. I, дискриминант модуля $\mathbf{Z}(\zeta)$ равен $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}[g'(\zeta)]$, где

$$g(x) = \prod_{(k,\, p)=1} (x - \zeta^k);$$

после довольно длинных вычислений это выражение превращается в $q^{\phi(q)}/p^{q/p}$.

Мы хотим показать, что $\mathbf{Z}(\zeta)$ является кольцом всех целых чисел поля $\mathbf{Q}(\zeta)$. В силу предложения 3.4 гл. I нужно проверить только, что

$$\sum_{0 \leqslant i \leqslant \phi(q)-1} a_i \zeta^i,$$

где $a_i \in \mathbf{Z}$, делится на p тогда и только тогда, когда все a_i делятся на p; другими словами,

$$\sum_{0 \leqslant i \leqslant \phi(q)-1} b_i (1-\zeta)^i$$

делится на p тогда и только тогда, когда на p делятся все b_i. Чтобы убедиться в этом, предположим, что $p \mid \sum b_i (1-\zeta)^i$, вспомним, что $(p) = (1-\zeta)^{\phi(q)}$, и допустим, что $p \mid b_i$ для $i = 0, \ldots, s-1$. Тогда

$$(1-\zeta)^{\phi(q)} \mid b_s (1-\zeta)^s + b_{s+1} (1-\zeta)^{s+1} + \ldots,$$

так что $(1-\zeta) \mid b_s$, т. е. $p \mid b_s$, и по индукции мы получаем, что все b_i делятся на p. Отсюда следует утверждение леммы.

Лемма 1.6. *Если* ζ *— первообразный корень* m*-й степени из единицы, то* $\mathbf{Q}(\zeta)$ *— расширение поля* $\mathbf{Q}$ *степени* $\phi(m)$; *дискриминант* $\mathbf{Q}(\zeta)$ *над* $\mathbf{Q}$ *равен*

$$m^{\phi(m)} / \prod_{p \mid m} p^{\phi(m)/(p-1)};$$

базисом для **Z***-модуля целых чисел поля* $\mathbf{Q}(\zeta)$ *являются числа* $1, \zeta, \zeta^2, \ldots, \zeta^{\phi(m)-1}$; *число* p *разветвляется тогда и только тогда, когда* $p \mid m$.

Большинство из этих фактов было уже доказано (леммы 1.1 и 1.3, 1.4); утверждения о дискриминанте и базисе целых элементов эквивалентны друг другу и могут быть доказаны непосредственно (см. [1], гл. 7, § 5). Можно также проверить утверждение о поле $\mathbf{Q}(\sqrt[m]{1})$, объединив расширения $\mathbf{Q}(\sqrt[q]{1})$, где q пробегает все степени простых чисел, делящие m.

Во-первых, заметим, что если q и q' — степени различных простых чисел, то

$$\mathbf{Q}(\sqrt[q]{1}) \cap \mathbf{Q}(\sqrt[q']{1}) = \mathbf{Q}.$$

Теперь рассмотрим дискриминант. Предположим, что $p^h \mid m$. По лемме 1.5 дискриминант поля $\mathbf{Q}_p(\sqrt[p^h]{1})$ над $\mathbf{Q}_p$ равен $p^{hp^h-(h+1)p^{h-1}}$. Идеал (p) дальше в поле $\mathbf{Q}_p(\sqrt[m]{1})$ не разветвляется, так что, согласно предложению 4.7 гл. I, дискриминант поля $\mathbf{Q}_p(\sqrt[m]{1})$ над $\mathbf{Q}_p$ равен $p^{h\phi(m)-\phi(m)/(p-1)}$. Согласно предложению 4.6 гл. I, дискриминант поля $\mathbf{Q}(\zeta)$ над $\mathbf{Q}$ равен

$$m^{\phi(m)} / \prod_{p\ m} p^{\phi(m)/(p-1)}.$$

Из способа вычисления видно, что это число равно дискриминанту кольца $\mathbf{Z}(\zeta)$, так что, согласно предложению 3.4 гл. I, $1, \zeta, \zeta^2, \ldots, \zeta^{\phi(m)-1}$ образуют базис для **Z**-модуля всех целых чисел.

Замечание. Все утверждения о разложении простых чисел в поле $\mathbf{Q}(\sqrt[m]{1})$ могут быть получены из леммы 1.6 с использованием теоремы Куммера (см. добавление). Если $\mathbf{Z}(\zeta)$ — кольцо всех целых чисел поля $\mathbf{Q}(\zeta)$, а $g(x) = 0$ — характеристическое уравнение элемента ζ над полем $\mathbf{Q}$, то простое число p разлагается в поле $\mathbf{Q}(\zeta)$ таким же образом, как многочлен $g(x)$ разлагается по модулю p; точнее, если $g(x) \equiv \Pi g_i(x) \pmod p$, то $(p) = \Pi [p, g_i(\zeta)]$.

Конечно, вполне возможно вычислить в этом случае группу ветвления в явном виде, но мы отсылаем читателя к книге [3].

Заключение. Мы показали, что всякое круговое расширение, а значит, и всякое подполе кругового расширения поля $\mathbf{Q}$ обладает абелевой группой Галуа. Верно и обратное: всякое абелево расширение поля $\mathbf{Q}$ является подполем кругового расширения (теорема Кронекера); однако это уже относится к теории полей классов (гл. VII, § 5, 7).

§ 2. РАСШИРЕНИЯ КУММЕРА

В этом параграфе K будет обозначать поле характеристики, взаимно простой с n, в котором многочлен $x^n - 1$ разлагается на линейные множители; ζ — первообразный корень n-й степени из единицы. Будет показано, что циклические расширения поля K степени, делящей n,— это так называемые куммеровы расширения $K(\sqrt[n]{a})$.

Пусть a — ненулевой элемент поля K. Если L — расширение поля K, такое, что у многочлена $x^n - a$ есть корень α, лежащий в L, то все корни $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ уравнения $x^n = \alpha$ лежат в L и любой автоморфизм поля L над K переставляет их. Мы обозначим минимальное поле разложения многочлена $x^n - a$ через $K(\sqrt[n]{a})$. Пусть σ — элемент группы Галуа $G[K(\sqrt[n]{a})/K]$. Если выбран корень α уравнения $x^n = a$, то автоморфизм σ вполне определен, если известен образ элемента α при этом автоморфизме: $\sigma\alpha = \zeta^b \cdot \alpha$. В частности, если a — элемент порядка n в мультипликативной группе $K^*/(K^*)^n$, то a^r является n-й степенью только в том случае, если $n \mid r$, так что многочлен

$x^n - a$ неприводим; в этом случае отображение $\sigma \mapsto \zeta^b$ дает изоморфизм группы Галуа на циклическую группу порядка n. Сформулируем все это в виде леммы.

Лемма 2.1. *Если в поле K выбран ненулевой элемент a, то найдется однозначно определенное нормальное расширение $K(\sqrt[n]{a})$, которое является полем разложения многочлена $x^n - a$. Если α — корень уравнения $x^n = a$, то существует отображение группы $G[K(\sqrt[n]{a})/K]$ в группу K^*, задаваемое формулой $\sigma \mapsto \sigma\alpha/\alpha$; в частности, если α — элемент порядка n в факторгруппе $K^*/(K^*)^n$, то группа Галуа циклична и порождается элементом σ, удовлетворяющим условию $\sigma\alpha = \zeta\alpha$.*

Лемма 2.2. *Если L — циклическое расширение поля K (т. е. группа $G(L/K)$ циклическая), то $L = K(\sqrt[n]{b})$ для некоторого $b \in K$ (b должно порождать факторгруппу $K^*/(K^*)^n$).*

Доказательство дается прямым построением, которое, очевидно, возможно. Пусть σ — образующий элемент группы $G(L/K)$; тогда $L = K(\gamma)$ для некоторого γ, так как все сепарабельные расширения простые, и мы можем выбрать γ так, чтобы элементы $\gamma, \sigma\gamma, \ldots, \sigma^{n-1}\gamma$ были базисом в L над полем K. Образуем сумму

$$\beta = \sum_{s=0}^{n-1} \zeta^s \sigma^s \gamma.$$

Тогда $\sigma\beta = \zeta^{-1}\beta$ и $\beta \neq 0$, так как элементы $\gamma, \ldots, \sigma^{n-1}\gamma$ линейно независимы над K; следовательно, $\beta^n \in K$ и $\beta^r \notin K$ при $0 < r < n$. Таким образом, $\beta^n = b$ является элементом порядка n в факторгруппе $K^*/(K^*)^n$; по лемме 2.1 поле $K(\sqrt[n]{b})$ является циклическим расширением степени n, содержащимся в L, так что $L = K(\sqrt[n]{b})$.

Лемма 2.3. *Два циклических расширения $K(\sqrt[n]{a})$ и $K(\sqrt[n]{b})$ поля K одинаковой степени совпадают тогда и только тогда, когда $a = b^r c^n$ для некоторых $c \in K$ и $r \in \mathbf{Z}$, где $(r, n) = 1$.*

Действительно, достаточность очевидна. Мы должны доказать только необходимость. Это легко сделать с помощью элементарной теории Галуа. Предположим, что $K(\alpha) = K(\beta)$ и $\alpha^n = a$, $\beta^n = b$. Пусть σ — образующая группы Галуа и $\sigma\alpha = \zeta\alpha$; тогда $\sigma\beta = \zeta^i\beta$ для некоторого i. Положим

$$\beta = \sum_{j=0}^{n-1} c_j\alpha^j;$$

тогда

$$\sigma\beta = \sum_{j=0}^{n-1} c_j\zeta^j\alpha^j,$$

так что обязательно

$$\beta = c_i\alpha^i.$$

Следствие. *Пусть L — конечное расширение поля K с абелевой группой Галуа G степени, делящей n. Тогда группа G есть прямое произведение циклических подгрупп $G_1, \ldots, G_r$. Пусть для каждого i через L_i обозначено подполе, неподвижное для подгруппы $G_1 \times \ldots \times G_{i+1} \times \ldots \times G_r$; тогда $G(L_i/K) = G_i$, $L_i = K(\alpha_i)$, где $\alpha_i^n = a_i \in K$ и $L = K(\alpha_1, \ldots, \alpha_r)$.*

Последние две леммы можно рассмотреть с точки зрения теории когомологий Галуа (см. [3]). Мы дадим обобщение леммы 2.2.

Лемма 2.4. *Если L — нормальное алгебраическое расширение поля K с группой Галуа G, то*

$$H^1(G, L^*) = 0.$$

(1-коцикл — это «непрерывное» отображение $G \to L^*$, при котором $\sigma \to \alpha_\sigma$, где $\sigma(\alpha_\tau) = \alpha_\sigma^{-1}\alpha_{\sigma\tau}$; «непрерывность» понимается в том смысле, что отображение может быть пропущено через конечную факторгруппу G' группы G. Образуем сумму $\beta = \sum_{\sigma\in G'} \alpha_\sigma\sigma(\gamma)$; в силу линейной независимости автоморфизмов (см. гл. V, § 2, п. 7) мы можем выбрать γ так, чтобы имело место $\beta \neq 0$; тогда $\alpha_\sigma = \beta/\sigma\beta$.)

Применим лемму 2.4, беря в качестве L (сепарабельное) алгебраическое замыкание поля K. Тогда имеет место точная последовательность $0 \to E_n \to L^* \xrightarrow{\nu} L^* \to 0$, где ν — отображение $x \mapsto x^n$, а E_n — совокупность корней n-й степени из единицы. Переходя к когомологиям, получаем точную последовательность

$$H^0(G, E_n) \to H^0(G, L^*) \xrightarrow{\nu} H^0(G, L^*) \to H^1(G, E_n) \to$$
$$\to H^1(G, L^*) \to \ldots$$

Так как G действует на E_n тривиально, то группа $H^1(G, E_n)$ совпадает с группой $\mathrm{Hom}(G, E_n)$, и, очевидно, $H^0(G, L^*)$ является частью группы L^*, неподвижной относительно действия G; таким образом, получена последовательность

$$E_n \to K^* \xrightarrow{\nu} K^* \to \mathrm{Hom}(G, E_n) \to 0,$$

т. е.

$$K^*/(K^*)^n \cong \mathrm{Hom}(G, E_n).$$

Этот изоморфизм можно задать явно. Вспомним, что если точна тройка $0 \to A \to B \to C \to 0$, то элемент $c \in C^G$ задает отображение $G \to A$, если только фиксирован такой элемент $b \in B$, что $b \to c$; тогда $\sigma \mapsto b/\sigma b$ — отображение $G \to A$. В нашем случае начнем с элемента $c \in K^*$; выберем γ так, чтобы $\gamma^n = c$; тогда $\sigma \mapsto \gamma/\sigma\gamma$ будет отображением $G \to E_n$. Обратно, если $\phi \in \mathrm{Hom}(G, E_n)$, то обозначим через G' ядро отображения ϕ. Тогда факторгруппа G/G' будет группой Галуа циклического расширения K' поля K степени, делящей n; если элемент $\sigma \in G$ таков, что $\phi(\sigma) = \zeta$, то найдется элемент $\gamma \in K'$, такой, что $\sigma\gamma = \zeta\gamma$; тогда $\gamma^n \in K^*$, так что γ^n определяет класс в факторгруппе $K^*/(K^*)^n$.

Те элементы группы G, порядки которых делят n, сохраняются в группе $\mathrm{Hom}(G, E_n)$. Обозначим через K_n объединение всех абелевых расширений поля K, группы Галуа которых имеют порядки, делящие число n; тогда $\mathrm{Hom}[G(K_n/K), E_n)] \cong K^*/(K^*)^n$. В частности, конечные абелевы расширения группы G, порядки которых делят n, соответствуют конечным подгруппам факторгруппы $K^*/(K^*)^n$.

Наконец, мы хотим коснуться разложения простого идеала $\mathfrak{p}$ поля K в расширении $K(\sqrt[n]{a})$; согласно гл. I, этот вопрос сводится к изучению расширения $K_\mathfrak{p}(\sqrt[n]{a})$ локального поля $K_\mathfrak{p}$.

Лемма 2.5. *Дискриминант поля* $K(\sqrt[n]{a})$ *над* K *делит* $n^n a^{n-1}$; *идеал* $\mathfrak{p}$ *неразветвлен, если* $\mathfrak{p} \nmid na$. *Если* a^f *— наименьшая степень, такая, что сравнение* $a^f \equiv x^n (\mathfrak{p})$ *разрешимо, то* f *равно степени классов вычетов.*

Положим $\alpha^n = a$; тогда, если $\mathfrak{o}$ — кольцо целых элементов поля K, то кольцо $\mathfrak{o}[\alpha]$ является подмодулем кольца целых элементов поля $K(\alpha)$, и, согласно предложению 4.6 гл. I, его дискриминант равен $(n\alpha^{n-1})^n = n^n a^{n-1}$; итак, дискриминант поля $K(\alpha)$ над K делит $n^n a^{n-1}$. В частности, согласно § 5 гл. I, идеал $\mathfrak{p}$ неразветвлен, если $\mathfrak{p} \nmid na$; согласно теореме Куммера (или в силу леммы Гензеля и результатов § 16 гл. II), разложение идеала $\mathfrak{p}$ копирует тогда разложение многочлена $x^n - a$ по модулю $\mathfrak{p}$. Значит, если a^f — такая наименьшая степень элемента a, что сравнение $x^n \equiv a^f (\mathfrak{p})$ разрешимо, то $\mathfrak{p}$ разлагается в произведение n/f простых идеалов в поле $K(\alpha)$, а его степень классов вычетов равна f. Это последнее утверждение можно доказать от противного так же, как лемму 1.4, образовав неразветвленное расширение поля $K_\mathfrak{p}$, в котором многочлен $x^n - a$ разлагается на линейные множители.

Лемма 2.6. *Если* $\mathfrak{p} \mid a$, $\mathfrak{p} \nmid n$ *и* $\mathfrak{p}^n \nmid a$, *то идеал* $\mathfrak{p}$ *слабо разветвлен в поле* $K(\sqrt[n]{a})$; *если* $\mathfrak{p} \mid a$ *и* $\mathfrak{p}^2 \nmid a$, *то идеал* $\mathfrak{p}$ *вполне разветвлен в поле* $K(\sqrt[n]{a})$.

Пусть α — корень уравнения $x^n = a$. Вторая часть леммы доказывается легко; именно, если $\mathfrak{p} \mid a$, но $\mathfrak{p}^2 \nmid a$, то $\mathfrak{p} = (\mathfrak{p}\alpha)^n$. Этот результат также может быть получен с помощью теоремы 6.1 гл. I, так как в этом случае многочлен $x^n - a$ является многочленом Эйзенштейна.

Если $\mathfrak{p} \nmid n$, т. е. идеал $\mathfrak{p}$ не делит степени расширения, ветвление, конечно, может быть только слабым (см. гл. I, § 5). С другой стороны, если $\mathfrak{p} \mid a$, но $\mathfrak{p}^n \nmid a$, то идеал $\mathfrak{p}$, очевидно, разветвлен, потому что $(\mathfrak{p}, \alpha) \mid \mathfrak{p} \mid (\mathfrak{p}, \alpha)^n$, но $\alpha \notin \mathfrak{p}$.

Остается случай, когда $\mathfrak{p}^r \mid a$, $\mathfrak{p}^{r+1} \nmid a$, $\mathfrak{p} \nmid n$, где $2 \leqslant r \leqslant n-1$. Если $(r, n) = 1$, то найдутся такие числа k, m, что $rk + nm = 1$; выберем элемент $q \in K$ так, чтобы $\mathfrak{p} \mid q$, но $\mathfrak{p}^2 \nmid q$. Тогда $K(\sqrt[n]{a^k q^{-nm}}) = K(\sqrt[n]{a})$, и мы вернулись к случаю $r = 1$. Если $(r, n) = s > 1$, то ветвление больше не будет полным, и идеал может разлагаться как полностью, так и не полностью. Индекс ветвления равен n/s; идеал $\mathfrak{p}$ неразветвлен в расширении $K\sqrt[s]{a}$ поля K, в то время как делители его вполне разветвлены в расширении $K\sqrt[n]{a}$ поля $K\sqrt[s]{a}$.

Добавление

ТЕОРЕМА КУММЕРА

В этом добавлении K будет обозначать поле алгебраических чисел, $\mathfrak{o}$ — кольцо его целых элементов, $L = K(\theta)$ — расширение степени n; мы предположим, что θ — целое и что многочлен $f(x) \in \mathfrak{o}[x]$ является характеристическим для θ. Обозначим через $\mathfrak{p}$ простой идеал кольца $\mathfrak{o}$, через v — ассоциированное с ним нормирование, через $K_\mathfrak{p}$ — пополнение поля K по этому нормированию, через $\mathfrak{o}_\mathfrak{p}$ — кольцо целых элементов поля $K_\mathfrak{p}$ и через $K_\mathfrak{p}^*$ — поле вычетов. Разложение простого идеала $\mathfrak{p}$ в поле L запишем в виде $\mathfrak{p} = \prod \mathfrak{q}_j^{e_j}$; соответствующие нормирования, пополнения, кольца целых элементов и поля вычетов обозначим через V_j, L_j $\mathfrak{o}_j$, L_j^*. Если f, g — многочлены из колец $\mathfrak{o}[x]$, $\mathfrak{o}_\mathfrak{p}[x]$, то их образы при отображении в поле вычетов обозначим через f^*, g^*.

В § 10 гл. II было показано, что если

$$f(x) = \prod_{1 \leqslant j \leqslant J} g_j(x)$$

представляет собой разложение многочлена $f(x)$ из $\mathfrak{o}[x]$ на неприводимые сомножители, то $L_j = K_\mathfrak{p}(\theta_j)$, где $g_j(\theta_j) = 0$. Имеют место вложения полей μ_j: $L \to L_j$, где $\mu_j(\theta) = \theta_j$, и отображения в поля вычетов ψ_j: $\mathfrak{o}_j \to L_j^*$.

Мы хотим связать разложение идеала $\mathfrak{p}$ в поле L с разложением многочлена $f_j^*(x)$ в кольце $K_\mathfrak{p}^*[x]$. Нам нужна следующая лемма.

Лемма. *В обозначениях, принятых выше, многочлены* $g_j^*(x)$ *являются степенями неприводимых много-*

членов в кольце $K_{\mathfrak{p}}^*(x)$; *если, скажем,* $g_j^*(x) = [G_j^*(x)]^{e_j}$, *то* $\psi_j(\theta_j)$ — *корни многочленов* $G_j^*(x)$.

Утверждение станет достаточно очевидным, если мы покажем, что редукция по модулю идеала $\mathfrak{p}$ каждого неприводимого многочлена из кольца $\mathfrak{o}_{\mathfrak{p}}[x]$ является степенью неприводимого многочлена в кольце $K_{\mathfrak{p}}^*[x]$. Предполагая противное, т. е. что для $h(x) \in \mathfrak{o}_{\mathfrak{p}}[x]$ имеет место

$$h^*(x) = h_1^*(x)\, h_2^*(x), \quad (h_1^*(x),\ h_2^*(x)) = 1,$$

можно будет найти многочлены $h_1(x)$, $h_2(x)$ из кольца $\mathfrak{o}_{\mathfrak{p}}[x]$, такие, что $h(x) = h_1(x)\, h_2(x)$. Это представляет собой просто вариант леммы Гензеля (см. гл. II, добавление B, или [1], гл. II, § 2).

Теорема Куммера. *Предположим, что идеал* $\mathfrak{p}$ *и элемент* θ *обладают тем свойством, что элемент*

$$\sum_0^{n-1} a_i \theta^i \in K[\theta]$$

является целым только в том случае, если $v(a_i) \geqslant 0$ *при* $i = 0, \ldots, n-1$. *Предположим далее, что разложение многочлена* $f^*(x)$ *на неприводимые сомножители в кольце* $K_{\mathfrak{p}}^*[x]$ *таково:* $f^*(x) = \prod [G_j^*(x)]^{e_j}$. *Для любого* j *обозначим через* $G_j(x) \in \mathfrak{o}[x]$ *унитарные многочлены, образы которых при отображении в классы вычетов равны* $G_j^*(x)$. *Тогда разложение идеала* $\mathfrak{p}$ *на простые идеалы таково:* $\mathfrak{p} = \prod \mathfrak{q}_j^{e_j}$, *где* $\mathfrak{q}_j = (\mathfrak{p},\ G_j(\theta))$.

(Ср. гл. II, формула (20), § 19; утверждение о наличии равенства $\gamma = \prod \mathfrak{q}_j^{e_j}$ эквивалентно утверждению о том, что нормированиями поля L, продолжающими v, являются V_j, $j = 1, \ldots, J$, соответствующие индексы ветвления равны e_j, а множества целых элементов поля L, таких, что $V_j(\alpha) > 0$ — это множества $\mathfrak{q}_j$. В наших обозначениях последнее условие выглядит так: $V_j(\alpha) > 0$, если $\psi_j \alpha = 0$.)

Мы должны проверить, что индексы ветвления действительно таковы, как указано в теореме, что $\mathfrak{q}_j = (\mathfrak{p},\ G_j(\theta))$, а также, что различные многочлены G_j^* получаются из различных многочленов g_j.

Нам уже известно, что $L_j \cong K_{\mathfrak{p}}[x]/(G_j(x))$. По условиям теоремы каждый целый элемент поля L имеет вид $\sum a_i \theta^i$, где $v(a_i) \geqslant 0$, так что всякий элемент из L_j^* представим в виде $\sum a_i^* (\psi_j \theta)^i$; поэтому $L_j^* \cong K_{\mathfrak{p}}^*[x]/G_j^*(x)$ и индексы ветвления равны $e_j = [L_j:\ K_{\mathfrak{p}}]/[L_j^*:\ K_{\mathfrak{p}}^*]$.

Если $\alpha \in (\mathfrak{p},\ G_j(\theta))$, то, очевидно, $\psi_j \alpha = 0$, так что $\alpha \in \mathfrak{q}_j$. Обратно, предположим, что $\alpha \in \mathfrak{q}_j$; тогда

$$\alpha = \sum_0^{n-1} a_i \theta^i,$$

и по условиям теоремы $v(a_i) \geqslant 0$ при $i = 0, \ldots, n-1$. Положим $h(x) = \sum a_i x^i$, так что $h(x) \in \mathfrak{o}_{\mathfrak{p}}[x]$. Так как $\alpha \in \mathfrak{q}_j$, $\psi_j a = 0$, то $h^*(\psi_j \theta) = 0$. Мы можем представить многочлен $h(x)$ в виде $h(x) = G_j(x)\, q_j(x) + r_j(x)$, где q_j, $r_j \in \mathfrak{o}_{\mathfrak{p}}[x]$ и $\deg(r_j) < \deg(G_j)$; тогда $r_j^*(\psi_j \theta) = 0$, так что многочлен $r_j^*(x)$ тождественно равен 0, и $h(\theta) \in (\mathfrak{p},\ G_j(\theta))$. Значит, $\mathfrak{q}_j = (\mathfrak{p},\ G_j(\theta))$, как и утверждалось.

Наконец, если $G_i^* = G_j^*$ при $i \neq j$, то $\mathfrak{q}_i = \mathfrak{q}_j$, так что многочлен $g_i(x)$ совпадает с $g_j(x)$, что противоречит условию.

ЛИТЕРАТУРА

Вайс (Weiss E.)
[1] Algebraic number theory, McGraw Hill, New York, 1963.

Вейль Г. (Weyl H.)
[2] Algebraic theory of numbers, Annals of Math. Studies, Princeton, 1940. (Русский перевод: Вейль Г., Алгебраическая теория чисел, ИЛ, М., 1947.)

Серр (Serre J.-P.)
[3] Corps locaux, Hermann, Paris, 1962.

ГЛАВА IV

Когомологии групп

М. Атья, К. Уолл [1])

§ 1. ОПРЕДЕЛЕНИЕ КОГОМОЛОГИЙ

Пусть G — группа, а $\Lambda = \mathbf{Z}[G]$ — ее целочисленное групповое кольцо. Термин *G-модуль* (*левый*) будет означать то же, что и *Λ-модуль* (*левый*). В дальнейшем под G-модулем всегда будет пониматься левый G-модуль. Сразу же заметим, что на левом G-модуле можно определить структуру правого G-модуля, положив $a \cdot g = g^{-1} \cdot a$.

Рассмотрим два G-модуля: A и B. Группу гомоморфизмов $A \to B$ в смысле гомоморфизма абелевых групп обозначим через $\mathrm{Hom}(A, B)$, а группу гомоморфизмов $A \to B$ в смысле гомоморфизма G-модулей — через $\mathrm{Hom}_G(A, B)$. Группу $\mathrm{Hom}(A, B)$ можно снабдить естественной структурой G-модуля: если $\varphi \in \mathrm{Hom}(A, B)$, то $g\varphi$: $A \to B$ определяется как отображение $a \mapsto g \cdot \varphi(g^{-1}a)$ $(a \in A)$.

Для каждого G-модуля A подмножество элементов, неподвижных при действии группы G, обозначается через A^G. Это подмножество — абелева группа, функториально зависящая от A, а именно наибольший подмодуль модуля A, на котором группа G действует тривиально.

Пусть A и B — два G-модуля; легко показать, что

$$\mathrm{Hom}_G(A, B) = (\mathrm{Hom}(A, B))^G; \tag{1}$$

в частности,

$$\mathrm{Hom}_G(\mathbf{Z}, A) = (\mathrm{Hom}(\mathbf{Z}, A))^G \cong A^G.$$

Здесь $\mathbf{Z}$ рассматривается как G-модуль с тривиальным действием группы G. Функтор Hom является точным слева.

[1]) Подготовлено для печати Макдональдом на основе рукописи Атья.

Отсюда следует, что A^G — точный слева ковариантный функтор от A. Это значит, что для любой точной последовательности G-модулей

$$0 \to A \to B \to C \to 0 \tag{2}$$

точна последовательность абелевых групп

$$0 \to A^G \to B^G \to C^G.$$

Если X — произвольная абелева группа, мы можем образовать G-модуль $\mathrm{Hom}(\Lambda, X)$. Полученный таким образом G-модуль мы будем называть *коиндуцированным*.

Под *когомологическим расширением* функтора A^G мы будем понимать последовательность функторов $H^q(G, A)$ $(q = 0, 1, \ldots)$, где $H^0(G, A) = A^G$, вместе со *связывающими* (или *граничными*) гомоморфизмами

$$\delta : H^q(G, C) \to H^{q+1}(G, A),$$

определенными функториально для каждой точной последовательности (2), если при этом:

(i) последовательность

$$\ldots \to H^q(G, A) \to H^q(G, B) \to H^q(G, C) \xrightarrow{\delta} \xrightarrow{\delta} H^{q+1}(G, A) \to \ldots \tag{3}$$

точна;

(ii) $H^q(G, A) = 0$ при всех $q \geqslant 1$, если A коиндуцирован.

Теорема 1.1. *Когомологическое расширение функтора A^G существует. Оно единственно с точностью до канонической эквивалентности.*

Однозначно определенные, согласно теореме 1.1, группы $H^q(G, A)$ называются *группами когомологий* G-модуля A.

Существование в теореме 1.1 устанавливается следующим образом. Выберем для G-модуля $\mathbf{Z}$ резольвенту P (G действуют тривиально на $\mathbf{Z}$) из свободных G-модулей:

$$\ldots \to P_1 \to P_0 \to \mathbf{Z} \to 0$$

и образуем комплекс $K = \mathrm{Hom}_G(P, A)$, т. е.

$$0 \to \mathrm{Hom}_G(P_0, A) \to \mathrm{Hom}_G(P_1, A) \to \ldots .$$

Пусть $H^q(K)$ $(q \geqslant 0)$ обозначает q-мерную группу когомологий этого комплекса. Тогда группы $H^q(G, A) = H^1(K)$ обладают свойствами когомологического расширения функтора A^G.

Действительно, по основной теореме гомологической алгебры группы $H^q(G, A)$, определенные таким образом, удовлетворяют условию точности (3); кроме того, $H^0(G, A) = H^0(K) = \mathrm{Hom}_G(\mathbf{Z}, A) = A^G$; наконец, если A коиндуцирован, т. е. $A = \mathrm{Hom}(\Lambda, X)$, где X — некоторая абелева группа, то для каждого G-модуля B мы имеем

$$\mathrm{Hom}_G(B, A) \cong \mathrm{Hom}(B, X)$$

(изоморфизм строится так: каждому G-гомоморфизму $\varphi\colon B \to A$ сопоставим отображение $B \to X$, определенное формулой $b \mapsto \varphi(b)(1)$, где 1 — единица группы G). Тогда комплекс K принимает вид

$$0 \to \mathrm{Hom}(P_0, X) \to \mathrm{Hom}(P_1, X) \to \dots .$$

Эта последовательность точна в каждом члене, начиная со второго, так как P_i свободны как абелевы группы. Следовательно, $H^q(G, A) = 0$ для всех $q \geqslant 1$.

Для доказательства единственности групп когомологий рассмотрим вместе с каждым G-модулем A также G-модуль $A^* = \mathrm{Hom}(\Lambda, A)$. Существует естественное вложение $A \to A^*$, которое отображает элемент $a \in A$ в φ_a, где φ_a определяется так: $\varphi_a(g) = ga$. Следовательно, мы получаем точную последовательность G-модулей

$$0 \to A \to A^* \to A' \to 0, \tag{4}$$

где $A' = A^*/A$. Из условия (i) и коиндуцированности A^* следует, что отображение

$$\delta\colon H^q(G, A') \to H^{q+1}(G, A) \tag{5}$$

является изоморфизмом для всех $q \geqslant 1$, и потому

$$H^1(G, A) \cong \mathrm{coker}\,(H^0(G, A^*) \to H^0(G, A')). \tag{6}$$

Таким образом, $H^q(G, A)$ можно последовательно построить из H^0, и потому эти группы единственны с точностью до канонической эквивалентности. Эту конструкцию можно использовать для индуктивного определения групп H^q.

Замечание. Из единственности следует, что группы $H^1(G, A)$ не зависят от выбора резольвенты P для $\mathbf{Z}$, которая необходима для их построения. Мы можем построить P любым удобным для нас способом.

§ 2. СТАНДАРТНЫЙ КОМПЛЕКС

Резольвенту P для $\mathbf{Z}$ можно выбрать, в частности, положив $P_i = \mathbf{Z}[G^{i+1}]$; тогда P_i будет свободным $\mathbf{Z}$-модулем с базисом $G \times \dots \times G$ ($(i+1)$ раз). G действует на каждый базисный элемент так:

$$s(g_0, g_1, \dots, g_i) = (sg_0, sg_1, \dots, sg_i).$$

Гомоморфизм $d\colon P_i \to P_{i-1}$ задается хорошо известной формулой

$$d(g_0, \dots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \dots, g_{j-1}, g_{j+1}, \dots, g_i), \tag{1}$$

а гомоморфизм $\varepsilon\colon P_0 \to \mathbf{Z}$ переводит каждую образующую (g_0) в $1 \in \mathbf{Z}$. (Чтобы показать, что последовательность

$$\dots \xrightarrow{d} P_1 \xrightarrow{d} P_0 \xrightarrow{\varepsilon} \mathbf{Z} \to 0 \tag{2}$$

точна, выберем элемент $s \in G$ и зададим отображение $h\colon P_i \to P_{i+1}$ формулой $h(g_0, \dots, g_i) = (s, g_0, g_1, \dots, g_i)$. Немедленно проверяется, что $dh + hd = 1$ и что $dd = 0$, откуда и вытекает точность последовательности.)

Каждый элемент из $K^i = \mathrm{Hom}_G(P_i, A)$ является тогда функцией $f\colon G^{i+1} \to A$, такой, что

$$f(sg_0, sg_1, \dots, sg_i) = s \cdot f(g_0, g_1, \dots, g_i).$$

Такая функция определяется своими значениями на элементах из G^{i+1} вида $(1, g_1, g_1g_2, \dots, g_1g_2 \dots g_i)$: если положить

$$\varphi(g_1, \dots, g_i) = f(1, g_1, g_1g_2, \dots, g_1 \dots, g_i),$$

то граничный оператор задается формулой

$$\begin{aligned}(d\varphi)(g_1, \dots, g_{i+1}) &= g_1 \cdot \varphi(g_2, \dots, g_{i+1}) + \\ &+ \sum_{j=1}^{i} (-1)^j \varphi(g_1, \dots, g_jg_{j+1}, \dots, g_{i+1}) + \\ &+ (-1)^{i+1} \varphi(g_1, \dots, g_i).\end{aligned} \tag{3}$$

Это показывает, что 1-коцикл — это *скрещенный гомоморфизм*, т. е. отображение $\varphi\colon G \to A$, удовлетворяющее соотношению

$$\varphi(gg') = g\cdot\varphi(g') + \varphi(g),$$

и φ является кограницей, если существует $a \in A$, такое, что $\varphi(g) = ga - a$. В частности, если G тривиально действует на A, то

$$H^1(G, A) = \mathrm{Hom}(G, A). \tag{4}$$

Из формулы (3) следует также, что 2-коцикл — это функция $\varphi\colon G \times G \to A$, такая, что

$$g_1\cdot\varphi(g_2, g_3) - \varphi(g_1g_2, g_3) + \varphi(g_1, g_2g_3) - \varphi(g_1, g_2) = 0.$$

Такие функции (они называются системами факторов) встречаются в теории расширений групп, причем $H^2(G, A)$ описывает все возможные расширения E группы G с помощью A, т. е. точные последовательности $1 \to A \to E \to G \to 1$, в которых A является абелевым нормальным делителем в E и G действует на A посредством внутренних автоморфизмов. Для такого расширения E выберем сечение $\sigma\colon G \to E$ (систему представителей из классов смежности). Тогда мы получим, что

$$\sigma(g_1)\cdot\sigma(g_2) = \varphi(g_1, g_2)\,\sigma(g_1g_2)$$

для некоторого $\varphi(g_1, g_2) \in A$. Функция φ является 2-коциклом на G со значением в A. Если мы заменим сечение σ, то φ изменится на кограницу, значит, класс φ из $H^2(G, A)$ зависит только от расширения. Следовательно, каждый элемент из $H^2(G, A)$ получается этим способом из расширения G с помощью A.

Дальше нам понадобится явное описание связывающего гомоморфизма $\delta\colon H^0(G, C) \to H^1(G, A)$ в точной последовательности (3). Пусть $c \in H^0(G, C) = C^G$. Рассмотрим представитель $b \in B$ элемента c. Тогда db будет функцией $s \mapsto sb - b$. Класс элемента $sb - b$ в C равен нулю, следовательно, $sb - b \in A$, и потому db — это 1-коцикл группы G со значением в A. Если заменить b на элемент из A, то db изменится на кограницу; следовательно, класс db в $H^1(G, A)$ зависит только от c. Этот класс и является образом элемента c при отображении δ.

§ 3. ГОМОЛОГИИ

Пусть A и B — два G-модуля. Обозначим через $A \otimes B$ и $A \otimes_G B$ их тензорные произведения соответственно над $\mathbf{Z}$ и Λ. Произведение $A \otimes B$ имеет естественную структуру G-модуля, которая определяется следующим образом: $g(a \otimes b) = (ga) \otimes (gb)$.

Пусть I_G — ядро гомоморфизма $\Lambda \to \mathbf{Z}$, который отображает каждый элемент $s \in G$ в $1 \in \mathbf{Z}$. Это ядро представляет собой идеал в Λ, порожденный элементами вида $s - 1$ ($s \in G$). Из точности последовательности

$$0 \to I_G \to \Lambda \to \mathbf{Z} \to 0 \tag{1}$$

и точности справа функтора $\otimes$ следует, что для всякого G-модуля A

$$\mathbf{Z} \otimes_G A \cong A/I_GA.$$

Обозначим G-модуль A/I_GA через A_G. Это наибольший фактормодуль модуля A, на котором группа G действует тривиально. Очевидно, что A_G является точным справа функтором от A. Для любых двух G-модулей A и B имеем

$$A \otimes_G B \cong (A \otimes B)_G. \tag{2}$$

G-модуль вида $\Lambda \otimes X$, где X — любая абелева группа, называется *индуцированным*. Определение *гомологического расширения функтора* A_G получится «обращением стрелок» и заменой термина «коиндуцированный модуль» на термин «индуцированный модуль» в определении когомологического расширения функтора A^G.

Теорема 3.1. *Существует, и притом единственное, гомологическое расширение функтора* A_G.

Группы гомологий $H_q(G, A)$ в теореме 3.1. могут быть получены с помощью стандартного комплекса P из § 2. Достаточно положить

$$H_q(G, A) = H_q(P \otimes_G A).$$

Единственность можно доказать с помощью точной последовательности

$$0 \to A' \to A_* \to A \to 0, \tag{3}$$

где $A_* = \Lambda \otimes A$. Все доказательство совершенно аналогично доказательству теоремы 1.1.

Связывающий гомоморфизм δ: $H_1(G, C) \to H_0(G, A)$ можно описать явно. 1-цикл на G со значениями в C — это такая функция f: $G \to C$, что $f(s) = 0$ для почти всех $s \in G$ и $df = \sum_{s \in G} (s^{-1} - 1) f(s) = 0$. Для каждого $s \in G$ рассмотрим $\bar{f}(s) \in B$ — представитель элемента $f(s)$ (если $f(s) = 0$, то положим $\bar{f}(s) = 0$). Образ элемента $d\bar{f}$ в C равен 0, следовательно, $d\bar{f} \in A$. Класс элемента $d\bar{f}$ в $H_0(G, A)$ и будет образом класса f при гомоморфизме δ.

Предложение 3.1. *Имеет место изоморфизм* $H_1(G, \mathbf{Z}) \cong G/G'$, *где* G' — *коммутатор группы* G.

Доказательство. Из точности последовательности (1) и свойства индуцированности Λ следует, что связывающий гомоморфизм

$$\delta : H_1(G, \mathbf{Z}) \to H_0(G, I_G) = I_G/I_G^2$$

является изоморфизмом. С другой стороны, отображение $s \mapsto s - 1$ индуцирует изоморфизм G/G' на I_G/I_G^2.

§ 4. ЗАМЕНА ГРУПП

Пусть G' — подгруппа группы G. Если задан G'-модуль A', мы можем рассмотреть и G-модуль $A = \mathrm{Hom}_{G'}(\Lambda, A')$. Правда, A имеет структуру правого G-модуля, но мы можем превратить A в левый G-модуль способом, описанным в § 1 (пусть $\varphi \in A$, тогда $g \cdot \varphi$ — гомоморфизм $g' \mapsto \varphi(g'g^{-1})$). Имеет место

Предложение 4.1. (Лемма Шапиро.)

$$H^q(G, A) = H^q(G', A') \text{ для всех } q \geqslant 0.$$

Доказательство. Свободная Λ-резольвента P для $\mathbf{Z}$ является одновременно свободной Λ'-резольвентой и, кроме того,

$$\mathrm{Hom}_G(P, A) \cong \mathrm{Hom}_{G'}(P, A').$$

Аналогичный результат имеет место для гомологий. В рассуждениях нужно только заменить Hom на $\otimes$. Заметим, что предложение 4.1 можно рассматривать как обобщение свойства (ii) для групп когомологий (§ 1). Действительно, если $G' = (1)$, то $\Lambda' = \mathbf{Z}$, модуль A коиндуцирован и $H^q(G', A')$ тривиальны при $q \geqslant 1$.

Если f: $G' \to G$ — гомоморфизм групп, то он индуцирует гомоморфизм $P' \to P$ их стандартных комплексов, а значит, и гомоморфизм

$$f^*: H^q(G, A) \to H^q(G', A)$$

для любого G-модуля A (гомоморфизм f позволяет рассматривать A и как G'-модуль). В частности, если в качестве G' взять подгруппу H группы G и рассмотреть вложение f: $H \to G$, то полученные в этом случае гомоморфизмы называются гомоморфизмами *ограничения* и обозначаются так:

$$\mathrm{Res}: H^q(G, A) \to H^q(H, A).$$

Пусть H — нормальный делитель в G. Рассмотрим каноническое отображение f: $G \to G/H$. Каждому G-модулю A соответствует G/H-модуль A^H и, следовательно, гомоморфизм $H^q(G/H, A^H) \to H^q(G, A^H)$. Взяв его композицию с гомоморфизмом, индуцированным вложением $A^H \to A$, получим гомоморфизм *инфляции*

$$\mathrm{Inf}: H^q(G/H, A^H) \to H^q(G, A).$$

Аналогичные рассуждения можно провести для гомологий. Гомоморфизм f: $G' \to G$ индуцирует гомоморфизм

$$f_*: H_q(G', A) \to H_q(G, A).$$

В частности, если $G' = H$ — подгруппа в G, а $f : H \to G$ — вложение, то мы получим гомоморфизмы *кограничения*

$$\mathrm{Cor}: H_q(H, A) \to H_q(G, A).$$

Рассмотрим теперь внутренний автоморфизм $s \mapsto tst^{-1}$ группы G. Он создает на A другую структуру G-модуля. Обозначим через A^t этот новый G-модуль. Автоморфизм $s \mapsto tst^{-1}$ индуцирует также гомоморфизм

$$H^q(G, A) \to H^q(G, A^t). \tag{1}$$

Отображение $a \mapsto t^{-1}a$ определяет изоморфизм $A^t \to A$ и, следовательно, индуцирует гомоморфизм

$$H^q(G, A) \to H^q(G, {}^tA). \tag{2}$$

Предложение 4.2. *Композиция гомоморфизмов* (1) *и* (2) *является тождественным отображением группы* $H^q(G, A)$.

В доказательстве применяется стандартная техника сдвига размерности: мы проверяем результат для $q = 0$, а затем, индуктивным рассуждением по q, используя изоморфизм (5), § 1, сдвигаем размерность вниз.

Пусть $q = 0$. Тогда $H^0(G, A^t) = (A^t)^G = tA^G$ и гомоморфизм (1) состоит как раз в умножении на t. Так как гомоморфизм (2) представляет собой умножение на t^{-1}, их композиция является тождественным отображением.

Предположим теперь, что $q > 0$ и предложение верно для $q - 1$. Имеет место точная последовательность

$$0 \to A^t \to (A^*)^t \to (A')^t \to 0,$$

соответствующая последовательности (4) § 1. Так как G-модуль $(A^*)^t$ изоморфен A^*, то $(A^*)^t$ коиндуцирован. Значит, имеют место функториальные изоморфизмы

$$H^q(G, A^t) \cong H^{q-1}(G, (A')^t) \quad (q \geqslant 2)$$

и, в частности,

$$H^1(G, A^t) = \operatorname{coker}(H^0(G, (A^*)^t) \to H^0(G, (A')^t).$$

Теперь остается применить индуктивное предположение.

§ 5. ПОСЛЕДОВАТЕЛЬНОСТЬ, СВЯЗЫВАЮЩАЯ ОГРАНИЧЕНИЕ И ИНФЛЯЦИЮ

Предложение 5.1. *Пусть H — нормальный делитель в G, и пусть A — некоторый G-модуль. Тогда последовательность*

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A)$$

точна.

Доказательство получается непосредственной проверкой.

(а) *Точность в члене* $H^1(G/H, A^H)$. Пусть f: $G/H \to A^H$ является 1-коциклом. Отображение f индуцирует $\bar{f}$: $G \to G/H \to A^H \to A$, также являющееся 1-коциклом, причем его класс есть инфляция класса f. Пусть $\bar{f}$ — кограница; в этом случае существует такой элемент $a \in A$, что $\bar{f}(s) = sa - a$ ($s \in G$). Но функция $\bar{f}$ постоянна на классах смежности H в G; следовательно, $sa - a = sta - a$ для всех $t \in H$, т. е. $ta = a$ для всех $t \in H$. Это значит, что $a \in A^H$; следовательно, f также является кограницей.

(б) $\text{Res} \circ \text{Inf} = 0$. Если φ: $G \to A$ является 1-коциклом, то класс ограничения $\varphi | H : H \to A$ и есть ограничение класса φ. С другой стороны, если $\varphi = \bar{f}$, то ясно, что $\bar{f} | H = \text{const} = f(1) = 0$.

(в) *Точность в члене* $H^1(G, A)$. Пусть φ: $G \to A$ является 1-коциклом, ограничение которого на H есть кограница. В этом случае существует такое $a \in A$, что $\varphi(t) = ta - a$ для всех $t \in H$. Вычтем из φ кограницу $s \mapsto sa - a$; тем самым все сведется к случаю, когда $\varphi | H = 0$. Формула

$$\varphi(st) = \varphi(s) + s \cdot \varphi(t)$$

показывает (если взять $t \in H$), что φ постоянно на классах смежности G по H. А теперь положим в этой же формуле $s \in H$, $t \in G$ и убедимся, что образ φ содержится в A^H. Таким образом, φ является инфляцией некоторого 1-коцикла $G/H \to A^H$. Это завершает доказательство предложения 5.1.

Предложение 5.2. *Пусть $q \geqslant 1$ и $H^i(H, A) = 0$ при $1 \leqslant i \leqslant q - 1$; тогда последовательность*

$$0 \to H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A)$$

точна.

Здесь мы имеем другой пример сдвига размерности: мы произведем редукцию к случаю $q = 1$; тогда предложение превратится в предложение 5.1. Предположим, что $q > 1$ и утверждение верно для $q - 1$. В точной последовательности (4) § 1 G-модуль A^* коиндуцирован *как H-модуль* (действительно, $\Lambda = \mathbf{Z}[G]$ — свободный $\mathbf{Z}[H]$-модуль); следовательно,

$$H^i(H, A') \cong H^{i+1}(H, A) = 0 \quad \text{при} \quad 1 \leqslant i \leqslant q-2.$$

В частности, так как $H^1(H, A) = 0$, последовательность

$$0 \to A^H \to (A^*)^H \to (A')^H \to 0$$

точна и $(A^*)^H$ является коиндуцированным G/H-модулем (действительно, $(A^*)^H \cong \text{Hom}(\mathbf{Z}[G/H], A)$). Следовательно,

в диаграмме

$$\begin{array}{ccccccc} 0 \to & H^{q-1}(G/H, (A')^H) & \to & H^{q-1}(G, A') & \to & H^{q-1}(H, A') \\ & \downarrow \delta & & \downarrow \delta & & \downarrow \delta \\ 0 \to & H^q(G/H, A^H) & \to & H^q(G, A) & \to & H^q(H, A) \end{array}$$

вертикальные стрелки — изоморфизмы. Диаграмма коммутативна. По индуктивному предположению, примененному к A', верхняя последовательность точна, значит, точна и нижняя.

Следствие. *Если выполняются условия предложения* 5.2, *то*

$$H^i(G/H, A^H) \cong H^i(G, A) \quad (1 \leqslant i \leqslant q-1).$$

§ 6. ГРУППЫ ТЭЙТА

Начиная отсюда, мы будем считать, что группа G конечна. Обозначим через N элемент $\sum\limits_{s \in G} s$ кольца Λ. Для любого G-модуля A умножение на N определяет его эндоморфизм $N: A \to A$. Очевидно, что

$$I_G A \subseteq \ker(N), \quad \operatorname{Im}(N) \subseteq A^G.$$

Отсюда следует, что N индуцирует гомоморфизм

$$N^*: H_0(G, A) \to H^0(G, A).$$

С помощью этого гомоморфизма определим группы

$$\hat{H}_0(G, A) = \ker(N^*), \ \hat{H}^0(G, A) = \operatorname{coker}(N^*) = A^G/N(A).$$

Группа G конечна и потому мы можем определить отображение $\operatorname{Hom}(\Lambda, X) \to \Lambda \otimes X$ (для любой абелевой группы X) по правилу

$$\varphi \mapsto \sum_{s \in G} s \otimes \varphi(s).$$

Легко проверить, что это изоморфизм G-модулей. Отсюда следует, что для конечной группы понятия индуцированного и коиндуцированного модуля совпадают.

Предложение 6.1. *Если A — индуцированный G-модуль, то*

$$\hat{H}_0(G, A) = \hat{H}^0(G, A) = 0.$$

Доказательство. Пусть $A = \Lambda \otimes X$, где X — некоторая абелева группа. Модуль Λ является $\mathbf{Z}$-свободным, поэтому каждый элемент из A можно однозначно представить в виде $\sum\limits_{s \in G} s \otimes x_s$. Если этот элемент G-инвариантен, то $\sum\limits_s gs \otimes x_s = \sum\limits_s s \otimes x_s$ для всех $g \in G$. Отсюда следует, что все x_s равны между собой. Это означает, что такой элемент можно представить в виде $N \cdot (1 \otimes x)$; следовательно, он лежит в $N(A)$. Поэтому $\hat{H}^0(G, A) = 0$.

Аналогично если $N \cdot \sum\limits_s s \otimes x_s = 0$, то $\sum x_s = 0$.

Отсюда следует, что $\sum s \otimes x_s = \sum (s-1)(1 \otimes x_s) \in I_G A$. Значит, $\hat{H}_0(G, A) = 0$.

Определим теперь группы когомологий Тэйта $\hat{H}^q(G, A)$ для всех целых q следующим образом:

$$\hat{H}^q(G, A) = H^q(G, A), \text{ если } q \geqslant 1;$$

$$\hat{H}^{-1}(G, A) = \hat{H}_0(G, A);$$

$$\hat{H}^{-q}(G, A) = H_{q-1}(G, A), \text{ если } q \geqslant 2.$$

Теорема 6.1. *Для каждой точной последовательности G-модулей*

$$0 \to A \to B \to C \to 0$$

имеет место точная последовательность

$$\ldots \to \hat{H}^q(G, A) \to \hat{H}^q(G, B) \to \hat{H}^q(G, C) \xrightarrow{\delta} \hat{H}^{q+1}(G, A) \to \ldots.$$

Доказательство. Мы срастим вместе точные последовательности для гомологий и когомологий. Рассмотрим диаграмму

$$\begin{array}{ccccccccc} \ldots \to & H_1(G, C) & \xrightarrow{\delta} & H_0(G, A) & \to & H_0(G, B) & \to & H_0(G, C) & \to 0 \\ & \downarrow & & \downarrow N_A^* & & \downarrow N_B^* & & \downarrow N_C^* & \downarrow \\ 0 \to & & & H^0(G, A) & \to & H^0(G, B) & \to & H^0(G, C) & \xrightarrow{\delta} H^1(G, A) \end{array}$$

где N_A^*, N_B^*, N_C^* означают гомоморфизмы N^* для соответствующих модулей. Очевидно, что два внутренних квадрата диаграммы коммутативны. Коммутативность двух внешних квадратов сразу следует из явного описания связывающего гомоморфизма δ, данного в § 2 и 3.

Определим $\hat{\delta}\colon \hat{H}_0(G, C) \to \hat{H}^0(G, A)$ следующим образом. Пусть $c \in \hat{H}^0(G, C) = \ker(N_C^*)$. Рассмотрим представитель c — элемент $b \in H_0(G, B)$. Образ элемента $N_B^*(b) \in H^0(G, B)$ в группе $H^0(G, C)$ равен нулю. Следовательно, элемент b получается из элемента $a \in H^0(G, A)$, образ которого в $\hat{H}^0(G, A)$ не зависит от выбора b. Этот элемент a из $\hat{H}^0(G, A)$ мы и положим равным $\hat{\delta}(c)$. Определения других отображений в последовательности

$$H_1(G, C) \to \hat{H}_0(G, A) \to \hat{H}_0(G, B) \to \hat{H}_0(G, C)$$
$$\xrightarrow{\delta} \hat{H}^0(G, A) \to \hat{H}^0(G, B) \to \hat{H}^0(G, C) \to H^1(G, A)$$

очевидны. Точность всей последовательности проверяется непосредственно из диаграммы.

Группы Тэйта можно рассматривать как группы когомологий комплекса, сконструированного из *полной резольвенты* G. Обозначим G-резольвенту кольца $\mathbf{Z}$, состоящую из конечно порожденных свободных G-модулей (например, стандартную резольвенту § 2), через P. Положим, далее, $P^* = \mathrm{Hom}(P, \mathbf{Z})$. Это — последовательность, двойственная к P. Мы имеем точные последовательности

$$\ldots \to P_1 \to P_0 \xrightarrow{\varepsilon} \mathbf{Z} \to 0$$
$$0 \to \mathbf{Z} \xrightarrow{\varepsilon^*} P_0^* \to P_1^* \to \ldots .$$

Двойственная последовательность точна, потому что каждый P_i — свободный $\mathbf{Z}$-модуль. Положив $P_{-n} = P_{n-1}^*$ и срастив вместе обе последовательности, получим бесконечную в обе стороны точную последовательность

$$\ldots \to P_1 \to P_0 \to P_{-1} \to P_{-2} \to \ldots . \qquad (\mathrm{L})$$

Группы Тэйта совпадают с группами когомологий $H^q(\mathrm{Hom}_G(L, A))$ для любого G-модуля A. Это утверждение очевидно, если $q \geqslant 1$. Для его доказательства при $q \leqslant -2$

используем следующий факт. Пусть C — конечно порожденный G-модуль, а $C^* = \mathrm{Hom}(C, \mathbf{Z})$ — двойственный к нему; тогда отображение $\sigma\colon C \otimes A \to \mathrm{Hom}(C^*, A)$, такое, что

$$\sigma(c \otimes a) \text{ отображает } f \in C^* \text{ в } f(c) \cdot a,$$

является изоморфизмом G-модулей. Следовательно, композиция

$$\tau\colon C \otimes {}_GA = (C \otimes A)_G \xrightarrow{N^*} (C \otimes A)^G \xrightarrow{\sigma} (\mathrm{Hom}(C^*, A))^G =$$
$$= \mathrm{Hom}_G(C^*, A)$$

является изоморфизмом (N^* — изоморфизм, потому что G-модуль $C \otimes A$ индуцированный). Отсюда вытекает, что $\mathrm{Hom}_G(P_{-n}, A) \cong P_{n-1} \otimes {}_GA$ и потому $H^{-q}(\mathrm{Hom}_G(L, A)) = H_{q-1}(G, A)$ при $q \geqslant 2$.

Осталось рассмотреть случаи $q = 0, -1$. Отображение

$$\mathrm{Hom}_G(P_{-1}, A) \to \mathrm{Hom}_G(P_0, A) \qquad (1)$$

индуцировано композицией $P_0 \xrightarrow{\varepsilon} \mathbf{Z} \xrightarrow{\varepsilon^*} P_{-1}$. Отождествим с помощью изоморфизма τ модули $\mathrm{Hom}_G(P_1, A)$ и $P_0 \otimes {}_GA$. Отображение (1) превратится тогда в отображение модуля $P_0 \otimes {}_GA$ в модуль $\mathrm{Hom}_G(P_0, A)$. Из определения τ сразу следует, что это отображение разлагается в композицию

$$P_0 \otimes {}_GA \to A_G \xrightarrow{N^*} A^G \to \mathrm{Hom}_G(P_0, A), \qquad (2)$$

где крайние стрелки — отображения, индуцированные ε. Отсюда следует, что $H^q(\mathrm{Hom}_G(L, A)) = \hat{H}^q(G, A)$ при $q = 0, -1$.

Замечание. Так как каждый G-модуль можно представить или как подмодуль, или как фактормодуль индуцированного модуля, то из предложения 6.1 и теоремы 6.1 вытекает, что группы Тэйта можно «сдвигать» вверх и вниз.

Пусть H — подгруппа группы G. Гомоморфизмы ограничения

$$\mathrm{Res}\colon H^q(G, A) \to H^q(H, A)$$

были определены для всех $q \geqslant 0$. Значит, они определены и для групп Тэйта $\hat{H}^1$ при $q \geqslant 1$. Эти гомоморфизмы коммутируют со связывающим гомоморфизмом δ. Из соображе-

ний сдвига размерности следует тогда, что их можно расширить на все $\hat{H}^q$ (нужно использовать точную последовательность (3) § 3 и то обстоятельство, что A_* индуцирован как H-модуль). Аналогично коограничение, которое первоначально определялось для H_q (т. е. для $\hat{H}^{-q-1}$ при $q \geqslant 1$), можно с помощью сдвига размерности распространить на все $\hat{H}^q$ (используя последовательность (4) § 1).

Предложение 6.2. *Пусть H — подгруппа группы G и A — некоторый G-модуль. Тогда*

(i) $\mathrm{Res}: \hat{H}_0(G, A) \longrightarrow \hat{H}_0(H, A)$ *индуцируется отображением* $N'_{G/H}: A_G \longrightarrow A_H$, *где*

$$N'_{G/H}(a) = \sum_i s_i^{-1} a,$$

и (s_i) — система представителей из классов смежности в G/H;

(ii) $\mathrm{Cor}\ \hat{H}^0(H, A) \longrightarrow \hat{H}^0(G, A)$ *индуцируется отображением* $N_{G/H}: A^H \longrightarrow A^G$, *где*

$$N_{G/H}(a) = \sum_i s_i a.$$

Мы докажем утверждение (i), а (ii) оставим читателю. Прежде всего вспомним, что $\hat{\delta}: \hat{H}^0(G, A) \longrightarrow \hat{H}^1(G, A')$ индуцируется отображением $\delta: H^0(G, A) \to H^1(G, A')$. Отображение $\mathrm{Res}: H^0(G, A) \longrightarrow H^0(H, A)$ — это погружение $A^G \longrightarrow A^H$, которое коммутирует с δ. Отсюда следует, что $\mathrm{Res}: \hat{H}^0(G, A) \longrightarrow \hat{H}^0(H, A)$ индуцируется погружением $A^G \longrightarrow A^H$. Пусть теперь $\nu: \hat{H}_0(G, A) \longrightarrow \hat{H}_0(H, A)$ — отображение, индуцированное $N'_{G/H}$. Нам осталось проверить, что диаграмма

$$\begin{array}{ccc} \hat{H}_0(G, A) & \xrightarrow{\delta} & \hat{H}^0(G, A') \\ {\scriptstyle\nu}\downarrow & & \downarrow{\scriptstyle\mathrm{Res}} \\ \hat{H}_0(H, A) & \xrightarrow{\delta} & \hat{H}^0(H, A') \end{array}$$

коммутативна.

Пусть $a \in A$ — представитель элемента $\bar{a} \in \hat{H}_0(G, A)$; тогда $N_G(a) = 0$. Рассмотрим представитель b элемента a в A_*. Образ элемента $N_G(b)$ в A равен 0, кроме того, этот элемент G-инвариантен; значит, $N_G(b)$ содержится в модуле $(A')^G \subseteq (A')^H$. Класс элемента $N_G(b) \pmod{N_H(A')}$ равен $\mathrm{Res} \circ \hat{\delta}(\bar{a})$. С другой стороны, $\nu(\bar{a})$ — это класс по $\mathrm{mod}\, I_H A$ элемента $N'_{G/H}(a)$, представителем которого в A' является элемент $N'_{G/H}(b)$; следовательно, элемент $\hat{\delta} \circ \nu(\bar{a})$ представляется элементом $N_H \circ N'_{G/H}(b) = N_G(b)$.

Замечание. Пусть $q = -2$, $A = \mathbf{Z}$. Тогда $\hat{H}^{-2}(G, \mathbf{Z}) = H_1(G, \mathbf{Z}) \cong G/G'$. Отображение $\mathrm{Res}: G/G' \longrightarrow H/H'$ в классической терминологии называется перенесением; его можно определить следующим образом. Группа G/G' двойственна группе $\mathrm{Hom}(G, \mathbf{C}^*)$, поэтому перенесение должно быть двойственно гомоморфизму

$$\mathrm{Hom}(H, \mathbf{C}^*) \longrightarrow \mathrm{Hom}(G, \mathbf{C}^*).$$

Этот гомоморфизм задается так:

$$\rho \longmapsto \det(i_*\rho)/\det(i_* 1),$$

где $i_*\rho$ — представление G, индуцированное одномерным представлением ρ, а det означает соответствующее одномерное представление, которое получается с помощью рассмотрения определителя. Группа $\mathrm{Hom}(G, \mathbf{C}^*)$ рассматривается здесь в мультипликативной записи.

Предложение 6.3. *Пусть $(G : H) = n$; тогда*

$$\mathrm{Cor} \circ \mathrm{Res} = n.$$

Доказательство. Справедливость предложения для группы $\hat{H}^0$ следует из предложения 6.2, (ii). Отображение Res индуцируется погружением $A^H \longrightarrow A^G$, а отображение Cor индуцируется отображением $N_{G/H}: A^G \longrightarrow A^H$. Кроме того, очевидно, что $N_{G/H}(a) = na$ для всех $a \in A^G$. Общий случай следует отсюда с помощью сдвига размерности.

Следствие 1. *Если G имеет порядок n, то все группы $\hat{H}^q(G, A)$ аннулируются умножением на n.*

Доказательство. В предложении 6.3 положим $H=(1)$ и используем тривиальность в этом случае группы $\hat{H}^q(H, A)$ для всех q.

Следствие 2. *Если A — конечно порожденный G-модуль, все группы $\hat{H}^q(G, A)$ конечны.*

Доказательство. Вычисления групп $\hat{H}^q(G, A)$ из стандартной полной резольвенты L показывают, что эти группы имеют конечное число образующих. По следствию 1 число $n=\mathrm{Card}(G)$ аннулирует каждую из них; значит, эти группы конечны.

Следствие 3. *Пусть S — силовская p-подгруппа группы G; тогда отображение*

$$\mathrm{Res}\colon \hat{H}^q(G, A) \longrightarrow \hat{H}^q(S, A)$$

является мономорфизмом на p-примарной компоненте группы $\hat{H}^q(G, A)$.

Доказательство. Пусть $\mathrm{Card}(G)=p^\alpha m$, где m взаимно просто с p. Пусть еще x содержится в p-примарной компоненте группы $\hat{H}^q(G, A)$ и $\mathrm{Res}(x)=0$; тогда

$$mx=\mathrm{Cor}\circ\mathrm{Res}(x)=0$$

в силу предложения 6.3, потому что $m=(G:S)$. С другой стороны, $p^\alpha x=0$ по следствию 1, а так как $(p^\alpha, m)=1$, то $x=0$.

Следствие 4. *Если ограничение элемента x из $\hat{H}^q(G, A)$ в группе $\hat{H}^q(S, A)$ равно нулю для всех силовских подгрупп S группы G, то $x=0$.*

§ 7. $\cup$-ПРОИЗВЕДЕНИЯ

Теорема 7.1. *Пусть G — конечная группа. Существует, и притом единственное, семейство таких гомоморфизмов*

$$\hat{H}^p(G, A)\otimes\hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, A\otimes B)$$

(соответствующее обозначение: $(a\otimes b)\longrightarrow a\cdot b$; элемент $a\cdot b$ называется $\cup$-произведением элементов a и b), определенных для всех целых чисел p, q и всех G-модулей A и B, что:

(i) *эти гомоморфизмы функториально зависят от A и B;*

(ii) *для $p=q=0$ соответствующие гомоморфизмы индуцируются естественным отображением*

$$A^G\otimes B^G \longrightarrow (A\otimes B)^G;$$

(iii) *если $0\longrightarrow A\longrightarrow A'\longrightarrow A''\longrightarrow 0$ — точная последовательность G-модулей и последовательность $0\longrightarrow A\otimes B\longrightarrow A'\otimes B\longrightarrow A''\otimes B\longrightarrow 0$ также точна, то для всех $a''\in\hat{H}^p(G, A'')$ и $b\in\hat{H}^q(G, B)$ справедливо равенство*

$$(\delta a'')\cdot b=\delta(a''\cdot b)\quad(\in\hat{H}^{p+q+1}(G, A\otimes B));$$

(iv) *если $0\longrightarrow B\longrightarrow B'\longrightarrow B''\longrightarrow 0$ — точная последовательность G-модулей и последовательность $0\longrightarrow A\otimes B\longrightarrow A\otimes B'\longrightarrow A\otimes B''\longrightarrow 0$ также точна, то для всех $a\in\hat{H}^p(G, A)$ и $b''\in\hat{H}^q(G, B'')$ справедливо равенство*

$$a\cdot(\delta b'')=(-1)^p\delta(a\cdot b'')\quad(\in\hat{H}^{p+q+1}(G, A\otimes B)).$$

Пусть $(P_n)_{n\in\mathbf{Z}}$ — полная резольвента для G в смысле § 6. Доказательство существования опирается на конструкцию для всех целых чисел p и q гомоморфизмов G-модулей

$$\varphi_{p,q}\colon P_{p+q}\longrightarrow P_p\otimes P_q,$$

которые обладают следующими свойствами:

$$\varphi_{p,q}\circ d=(d\otimes 1)\circ\varphi_{p+1,q}+(-1)^p(1\otimes d)\circ\varphi_{p,q+1}; \quad (1)$$

$$(\varepsilon\otimes\varepsilon)\circ\varphi_{0,0}=\varepsilon, \quad (2)$$

где $\varepsilon\colon P_0\longrightarrow\mathbf{Z}$ определяется так: $\varepsilon(g)=1$ для любого $g\in G$.

Предположим пока, что $\varphi_{p,q}$ уже построены, и проведем доказательство дальше следующим образом. Пусть $f\in\mathrm{Hom}_G(P_p, A)$, $g\in\mathrm{Hom}_G(P_q, B)$ — коцепи. Определим произведение коцепей $f\circ g\in\mathrm{Hom}_G(P_{p+q}, A\otimes B)$ так:

$$f\cdot g=(f\otimes g)\circ\varphi_{p,q}.$$

Тогда из равенства (1) сразу следует, что

$$d(f\cdot g)=(df)\cdot g+(-1)^p f\cdot dg. \quad (3)$$

Отсюда получаем, что $f \cdot g$ — коцикл, если f и g — коциклы и что класс когомологий $f \cdot g$ зависит только от классов когомологий f и g. Иными словами, существует гомоморфизм

$$\hat{H}^p(G, A) \otimes \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, A \otimes B).$$

Очевидно, что он обладает свойством (i); свойство (ii) сразу следует из равенства (2). Докажем свойство (iii). Рассмотрим точную последовательность

$$0 \longrightarrow \mathrm{Hom}_G(P_p, A) \longrightarrow \mathrm{Hom}_G(P_p, A') \longrightarrow \mathrm{Hom}_G(P_p, A'') \longrightarrow 0.$$

Пусть $\alpha'' \in \mathrm{Hom}_G(P_p, A'')$ — коцикл, являющийся представителем класса a''. Рассмотрим $\alpha' \in \mathrm{Hom}_G(P, A')$ — прообраз α''. Образ $d\alpha'$ в $\mathrm{Hom}_G(P_{p+1}, A'')$ равен 0; следовательно, $d\alpha'$ лежит в модуле $\mathrm{Hom}_G(P_{p+1}, A)$. Классом элемента $d\alpha'$ в $\hat{H}^{p+1}(G, A)$ является $\delta(a'')$. Следовательно, если $\beta \in \mathrm{Hom}_G(P_q, B)$ — коцикл, представляющий элемент $b \in \hat{H}^q(G, B)$, то $\alpha'' \cdot \beta$ представляет класс $a'' \cdot b$; $d(\alpha' \cdot \beta)$ представляет класс $\delta(a'' \cdot b)$ и $(d\alpha') \cdot \beta$ представляет класс $(\delta a'') \cdot \beta$. Кроме того, $d(\alpha' \cdot \beta) = (d\alpha') \cdot \beta$ (это вытекает из равенства (3) и из того, что $d\beta = 0$). Следовательно, $\delta(a'' \cdot b) = (\delta a'') \cdot b$. Доказательство свойства (iv) проводится аналогично.

Осталось построить гомоморфизмы $\varphi_{p,q}$. Построим их для стандартной полной резольвенты ($P_q = \mathbf{Z}[G^{q+1}]$, если $q \geqslant 0$; модуль P_{-q} двойствен к P_{q-1}, если $q \geqslant 1$). Пусть $q \geqslant 1$; тогда $P_{-q} = P_{q-1}^*$ имеет (как $\mathbf{Z}$-модуль) базис, состоящий из всех $(g_1^*, \ldots, g_q^*)$, где $(g_1^*, \ldots, g_q^*)$ отображает $(g_1, \ldots, g_q) \in P_{q-1}$ в $1 \in \mathbf{Z}$, а любой другой базисный элемент модуля P_{q-1} в 0. В терминах этого базиса отображение $d: P_{-q} \longrightarrow P_{-q-1}$ задается формулой

$$d(g_1^*, \ldots, g_q^*) = \sum_{s \in G} \sum_{i=0}^{q} (-1)^i (g_1^*, \ldots, g_i^*, s^*, g_{i+1}^*, \ldots, g_q^*),$$

а отображение $d: P_0 \longrightarrow P_{-1}$ — формулой $d(g_0) = \sum_{s \in G} (s^*)$.

Определим $\varphi_{p,q}: P_{p+q} \longrightarrow P_p \otimes P_q$ следующим образом:

(а) если $p \geqslant 0$, $q \geqslant 0$, то

$$\varphi_{p,q}(g_0, \ldots, g_{p+q}) = (g_0, \ldots, g_p) \otimes (g_p, \ldots, g_{p+q});$$

(б) если $p \geqslant 1$, $q \geqslant 1$, то

$$\varphi_{-p,-q}(g_1^*, \ldots, g_{p+q}^*) = (g_1^*, \ldots, g_p^*) \otimes (g_{p+1}^*, \ldots, g_{p+q}^*);$$

(в) если $p \geqslant 0$, $q \geqslant 1$, то

$$\varphi_{p,-p-q}(g_1^*, \ldots, g_q^*) = \sum (g_1, s_1, \ldots, s_p) \otimes (s_p^*, \ldots, s_1^*, g_1^*, \ldots, g_q^*);$$

$$\varphi_{-p-q,p}(g_1^*, \ldots, g_q^*) = \sum (g_1^*, \ldots, g_q^*, s_1^*, \ldots, s_p^*) \otimes (s_p^*, \ldots, s_1^*, g_q);$$

$$\varphi_{p+q,-q}(g_0, \ldots, g_p) = \sum (g_0, \ldots, g_p, s_1, \ldots, s_q) \otimes (s_q^*, \ldots, s_1^*);$$

$$\varphi_{-q,p+q}(g_0, \ldots, g_p) = \sum (s_1^*, \ldots, s_q^*) \otimes (s_q, \ldots, s_1, g_0, \ldots, g_p).$$

(В суммах правых частей s_i независимо пробегают элементы группы G.) То, что $\varphi_{p,q}$ обладает свойством (1), проверяется непосредственно, хотя выкладки весьма громоздки.

Это завершает доказательство существования в теореме 7.1. Единственность доказывается исходя из условия (ii). Используется сдвиг размерности с помощью условий (iii) и (iv); центральный пункт доказательства состоит в следующем: точная последовательность (3) § 3, а именно

$$0 \longrightarrow A' \longrightarrow A_* \longrightarrow A \longrightarrow 0,$$

распадается над $\mathbf{Z}$, из чего следует наличие $\mathbf{Z}$-гомоморфизма $A \to A_* = \Lambda \otimes A$, определенного формулой $a \longmapsto 1 \otimes a$. Отсюда вытекает, что результат тензорного умножения последовательности (3) § 3 на любой G-модуль B — снова точная последовательность, и, кроме того, $A_* \otimes B = \Lambda \otimes A \otimes B = (A \otimes B)_*$. Аналогично обстоит дело и с точной последовательностью (4) § 1.

Отметим следующие свойства ∪-произведения, которые легко доказываются с помощью сдвига размерности.

Предложение 7.1.
(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(при этом отождествляются* $(A \otimes B) \otimes C$ *и* $A \otimes (B \otimes C)$*);*

(ii) $a \cdot b = (-1)^{\dim a \dim b} b \cdot a$ (*отождествляются* $A \otimes B$ *и* $B \otimes A$);

(iii) $\mathrm{Res}\,(a \cdot b) = \mathrm{Res}\,(a) \cdot \mathrm{Res}\,(b)$;

(iv) $\mathrm{Cor}\,(a \cdot \mathrm{Res}\,(b)) = \mathrm{Cor}\,(a) \cdot b$.

Докажем, например, (iv). Рассмотрим подгруппу H группы G; пусть $a \in \hat{H}^p(H, A)$ и $b \in \hat{H}^q(G, B)$. Тогда обе части равенства (iv) являются элементами из $\hat{H}^{p+q}(G, A \otimes B)$. Пусть сначала $p = q = 0$. Элемент a можно представить элементом $\alpha \in A^H$; в силу предложения 6.2, (ii) $\mathrm{Cor}\,(a)$ представляется элементом $N_{G/H}(\alpha) = \sum_i s_i \alpha \in A^G$; элемент b представляется элементом $\beta \in B^G$, следовательно, $\mathrm{Cor}\,(a) \cdot b$ представляется элементом

$$N_{G/H}(\alpha) \otimes \beta = \left(\sum s_i \alpha\right) \otimes \beta = \sum s_i (\alpha \otimes \beta) = N_{G/H}(\alpha \otimes \beta).$$

С другой стороны, $a \cdot \mathrm{Res}\,(b)$ представляется элементом $\alpha \otimes \beta \in (A \otimes B)^H$, следовательно, $\mathrm{Cor}\,(a \cdot \mathrm{Res}\,(b))$ представляется элементом $N_{G/H}(\alpha \otimes \beta)$. Это доказывает равенство (iv) для $p = q = 0$. Теперь используем сдвиг размерности, как в доказательстве единственности $\cup$-произведения. Нужно только принять во внимание, что Cor и Res коммутируют со связывающими гомоморфизмами, относящимися соответственно к точным последовательностям (3) § 3 и (4) § 1.

В дальнейшем нам придется рассматривать произведения несколько более общего вида. Пусть A, B, C — некоторые G-модули, а φ: $A \otimes B \to C$ есть G-гомоморфизм. Если сделать композицию $\cup$-произведения с гомоморфизмом когомологий φ^*, индуцированным φ, то получается отображение

$$\hat{H}^p(G, A) \otimes \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, C);$$

в явном виде оно выглядит так: $a \otimes b \mapsto \varphi^*(a \cdot b)$. Элемент $\varphi^*(a \cdot b)$ называется *$\cup$-произведением относительно* φ.

§ 8. ЦИКЛИЧЕСКИЕ ГРУППЫ; ИНДЕКС ЭРБРАНА

Пусть G — циклическая группа порядка n с образующей s. Можно построить простую полную резольвенту K для G. Каждое K_i в ней изоморфно Λ, а d: $K_{i+1} \to K_i$ — это умножение на $T = s - 1$ в случае четного i и на N в случае нечетного i. Ядром T является $\Lambda^G = N \cdot \Lambda$, т. е. образ N; образ T равен I_G т. е. ядру N. Следовательно, для каждого G-модуля A комплекс $\mathrm{Hom}_G(K, A)$ имеет вид

$$\ldots \leftarrow A \xleftarrow{N} A \xleftarrow{T} A \xleftarrow{N} A \xleftarrow{T} \ldots;$$

поэтому

$$\hat{H}^{2q}(G, A) = \hat{H}^0(G, A) = A^G/NA,$$

$$\hat{H}^{2q+1}(G, A) = \hat{H}_0(G, A) = {}_NA/I_GA,$$

где ${}_NA$ обозначает ядро отображения N: $A \to A$.

В частности, $H^2(G, \mathbf{Z}) = \mathbf{Z}^G/N\mathbf{Z} = \mathbf{Z}/n\mathbf{Z}$ — циклическая группа порядка n.

Теорема 8.1. *$\cup$-произведение на образующую группы* $H^2(G, \mathbf{Z})$ *индуцирует изоморфизм*

$$\hat{H}^q(G, A) \longrightarrow \hat{H}^{q+2}(G, A)$$

для всех целых q *и всех* G*-модулей* A.

Доказательство. Из точных последовательностей

$$0 \longrightarrow I_G \longrightarrow \Lambda \longrightarrow \mathbf{Z} \longrightarrow 0, \tag{1}$$

$$0 \longrightarrow \mathbf{Z} \xrightarrow{N} \Lambda \xrightarrow{T} I_G \longrightarrow 0 \tag{2}$$

получаются изоморфизмы

$$\hat{H}^0(G, \mathbf{Z}) \xrightarrow{\delta} H^1(G, I_G) \xrightarrow{\delta} H^2(G, \mathbf{Z}).$$

Обе последовательности (1) и (2) распадаются на $\mathbf{Z}$, поэтому они останутся точными, если каждый их член умножить тензорно на A. Следовательно, нам достаточно показать, что $\cup$-умножение на образующую группы $\hat{H}^0(G, \mathbf{Z})$ индуцирует автоморфизм группы $\hat{H}^q(G, A)$. Используя снова сдвиг размерности, сведем вопрос к случаю $q = 0$. Так как $\hat{H}^0(G, \mathbf{Z}) = \mathbf{Z}/n\mathbf{Z}$; мы можем представить образующую $b \in \hat{H}^0(G, \mathbf{Z})$ каким-нибудь целым числом β, взаимно простым с n, а $\cup$-умножение на b — это просто умножение на β. Так как β взаимно просто с n, существует такое целое

число γ, что $\beta\gamma \equiv 1 \pmod{n}$. Группа $\hat{H}^0(G, A)$ аннулируется умножением на число n, следовательно, умножение на β является ее автоморфизмом.

Обозначим через $h_q(A)$ порядок группы $\hat{H}^q(G, A)$ $(q = 0,1)$ в том случае, если эта группа конечна. Если конечны обе группы, определим *индекс Эрбрана* $h(A)$ равенством

$$h(A) = h_0(A)/h_1(A).$$

Предложение 8.1. *Пусть* $0 \to A \to B \to C \to 0$— *точная последовательность G-модулей (G—циклическая группа). Если определены два из трех индексов Эрбрана* $h(A)$, $h(B)$, $h(C)$, *то определен и третий, причем*

$$h(B) = h(A) \cdot h(C).$$

Доказательство. Ввиду периодичности $\hat{H}^q$ точная последовательность когомологий имеет вид точного шестиугольника

$$\begin{array}{ccccc} & & H^0(A) & \to & H^0(B) \\ & \nearrow & & & \searrow \\ H^1(C) & & & & H^0(C) \\ & \nwarrow & & & \swarrow \\ & & H^1(B) & \leftarrow & H^1(A) \end{array}$$

В диаграмме и дальнейших рассуждениях обозначение $H^0(A)$ равносильно $\hat{H}^0(G, A)$, то же относится и к остальным сокращениям. Предположим, например, что группы $H^0(A)$, $H^1(A)$, $H^0(B)$, $H^1(B)$ конечны. Обозначим через M_1 образ группы $H^0(A)$ в $H^0(B)$, через M_i — образы при последующих отображениях в шестиугольнике в порядке их следования по часовой стрелке. Последовательность $0 \to M_2 \to H^0(C) \to M_3 \to 0$ точна, кроме того, группы M_2, M_3 конечны (M_2 конечна, потому что это гомоморфный образ $H^0(B)$; M_3 — потому что это подгруппа группы $H^1(A)$), следовательно, $H^0(C)$ также конечна. Аналогичными рассуждениями показывается конечность $H^1(C)$. Порядки групп $H^0(A)$, . . ., $H^1(C)$ соответственно равны m_6m_1, m_1m_2, . . ., m_5m_6 (m_i — порядок группы M_i), следовательно, $h(B) = h(A) \cdot h(C)$.

Предложение 8.2. *Если G-модуль A конечен, то* $h(A) = 1$.

Доказательство. Рассмотрим точные последовательности

$$0 \to A^G \to A \xrightarrow{T} A \to A_G \to 0,$$

$$0 \to H^1(A) \to A_G \xrightarrow{N^*} A^G \to H^0(A) \to 0.$$

Первая из них показывает, что равны порядки групп A^G и A_G, а из второй тогда вытекает, что равны порядки групп $H^0(A)$ и $H^1(A)$.

Следствие. *Пусть A, B — два G-модуля,* $f: A \to B$— *гомоморфизм с конечными ядром и коядром. Если определено одно из чисел* $h(A)$, $h(B)$, *то определено и другое, и при этом они равны между собой.*

Доказательство. Предположим, например, что определен индекс $h(A)$. Из точных последовательностей

$$0 \to \ker(f) \to A \to f(A) \to 0,$$

$$0 \to f(A) \to B \to \operatorname{coker}(f) \to 0$$

вытекает (если использовать предложения 8.1 и 8.2), что $h(f(A))$ определено и равно $h(A)$ и что $h(B)$ определено и равно $h(f(A))$.

Предложение 8.3. *Пусть E — конечномерное вещественное линейное пространство, в котором задано представление группы G. Пусть L и L′ — две решетки, каждая из которых порождает E и на которых группа G действует инвариантно. Если один из индексов* $h(L)$, $h(L')$ *определен, то определен и другой, причем они равны.*

Доказательству теоремы предпошлем следующую лемму.

Лемма 8.1. *Пусть G — конечная группа, M, M′ — два конечномерных* $\mathbf{Q}[G]$*-модуля, таких, что* $M_{\mathbf{R}} = M \otimes_{\mathbf{Q}} \mathbf{R}$ *и* $M'_{\mathbf{R}} = M' \otimes_{\mathbf{Q}} \mathbf{R}$ *изоморфны как* $\mathbf{R}[G]$*-модули; тогда M и M′ изоморфны как* $\mathbf{Q}[G]$*-модули.*

Доказательство. Пусть K — произвольное поле, L — его расширение, A — некоторая K-алгебра. Если V — некоторое K-векторное пространство, то L-векторное

пространство $V \otimes {}_K L$ обозначим через V_L. Пусть A-модули M и M' конечномерны как векторные пространства над K. Каждый A-гомоморфизм φ: $M \to M'$ индуцирует A_L-гомоморфизм $\varphi \otimes 1$: $M_L \to M'_L$, и отображение $\varphi \mapsto \varphi \otimes 1$ задает изоморфизм векторных пространств над L:

$$(\mathrm{Hom}_A(M, M'))_L \cong \mathrm{Hom}_{A_L}(M_L, M'_L). \qquad (3)$$

Рассмотрим теперь случай $K = \mathbf{Q}$, $L = \mathbf{R}$, $A = \mathbf{Q}[G]$; тогда $A_L = \mathbf{R}[G]$. Из условий леммы вытекает, в частности, что M и M' имеют одинаковую размерность над $\mathbf{Q}$, а следовательно, выбрав базисы в M и M', мы можем говорить про *определитель* элемента из $\mathrm{Hom}_{\mathbf{Q}[G]}(M, M')$ или элемента из $\mathrm{Hom}_{\mathbf{R}[G]}(M_{\mathbf{R}}, M'_{\mathbf{R}})$. (Конечно, определитель зависит от выбора базиса.)

Из (3) следует, что если элементы ξ_i образуют $\mathbf{Q}$-базис в $\mathrm{Hom}_{\mathbf{Q}[G]}(M, M')$, то они также образуют $\mathbf{R}$-базис в $\mathrm{Hom}_{\mathbf{R}[G]}(M_{\mathbf{R}}, M'_{\mathbf{R}})$. Так как $M_{\mathbf{R}}$ $\mathbf{R}[G]$-изоморфно $M'_{\mathbf{R}}$, то существуют такие $a_i \in \mathbf{R}$, что $\det(\sum a_i \xi_i) \neq 0$. Отсюда следует, что многочлен

$$F(t) = \det\left(\sum t_i \xi_i\right) \in \mathbf{Q}[t_1, \ldots, t_m],$$

где t_i — независимые переменные над $\mathbf{Q}$, не равен тождественно 0 (действительно, $F(a) \neq 0$). Так как поле $\mathbf{Q}$ бесконечно, существует $b \in \mathbf{Q}$, такое, что $F(b) \neq 0$, а тогда $\sum b_i \xi_i$ является $\mathbf{Q}[G]$-изоморфизмом M на M'.

Для доказательства предложения 8.3 положим $M = L \otimes \mathbf{Q}$, $M' = L' \otimes \mathbf{Q}$. Тогда $M_{\mathbf{R}}$ и $M'_{\mathbf{R}}$ оба $\mathbf{R}[G]$-изоморфны E. По лемме 8.1 существует $\mathbf{Q}[G]$-изоморфизм φ: $L \otimes \mathbf{Q} \to L' \otimes \mathbf{Q}$, осуществляющий вложение L в решетку, содержащуюся в решетке $(1/N)L'$ для некоторого натурального числа N. Следовательно, $f = N \cdot \varphi$ вкладывает решетку L в L'. Так как L и L' — абелевы группы одинакового конечного ранга, то коядро этого отображения конечно. Таким образом, результат получается из следствия из предложения 8.2.

§ 9. КОГОМОЛОГИЧЕСКАЯ ТРИВИАЛЬНОСТЬ

G-модуль A называется *когомологически тривиальным*, если для всякой подгруппы H группы G имеет место $\hat{H}^q(H, A) = 0$ при всех целых q. Например, индуцированный модуль когомологически тривиален.

Лемма 9.1. *Пусть p — простое число; G — p-группа и A — такой G-модуль, что $pA = 0$. Тогда эквивалентны следующие три утверждения:*

(i) $A = 0$;

(ii) $H^0(G, A) = 0$;

(iii) $H_0(G, A) = 0$.

Доказательство. Очевидно, что из (i) вытекает (ii) и (iii).

(ii) $\Rightarrow$ (i). Пусть $A \neq 0$ и x — ненулевой элемент в A. Подмодуль B, порожденный элементом x, конечен, и его порядок есть степень числа p.

Рассмотрим G-орбиты элементов из B. Все они имеют порядки, равные степеням числа p (так как порядок группы G равен степени p), кроме того, в B есть неподвижная точка, а именно 0. Значит, таких точек по меньшей мере p, и потому $H^0(G, A) = A^G \neq 0$.

(iii) $\Rightarrow$ (i). Пусть $A' = \mathrm{Hom}(A, \mathbf{F}_p)$ — двойственный к A модуль, рассматриваемый как векторное пространство над полем $\mathbf{F}_p$ из p элементов. Тогда группа

$$H^0(G, A') = (A')^G = \mathrm{Hom}_G(A, \mathbf{F}_p)$$

двойственна к $H_0(G, A)$. Следовательно, $H^0(G, A') = 0$, так что $A' = 0$, а значит, и $A = 0$.

Лемма 9.2. *Пусть выполнены условия леммы* 1 *и, кроме того, $H_1(G, A) = 0$. Тогда A — свободный модуль над кольцом $\mathbf{F}_p[G] = \Lambda/p\Lambda$.*

Доказательство. $pA = 0$, а потому и $p \cdot H_0(G, A) = 0$; следовательно, $H_0(G, A)$ можно рассматривать как векторное пространство над $\mathbf{F}_p$. Зафиксируем базис e_λ этого пространства и рассмотрим для каждого e_λ его представитель $a_\lambda \in A$. Пусть A' — подмодуль в A, порожденный элементами a_λ, и пусть $A'' = A/A'$. Тогда мы имеем точную последовательность

$$H_0(G, A') \xrightarrow{\alpha} H_0(G, A) \to H_0(G, A'') \to 0.$$

Из построения модуля A' следует, что α — изоморфизм. Следовательно, $H_0(G, A'') = 0$ и по лемме 9.1 $A'' = 0$.

Отсюда вытекает, что элементы a_λ порождают A как G-модуль. Этим определяется G-эпиморфизм φ: $L \to A$, в котором L является свободным $\mathbf{F}_p[G]$-модулем. По построению φ индуцирует изоморфизм

$$\beta\colon H_0(G, L) \to H_0(G, A).$$

Пусть $R = \ker \varphi$. Ввиду того что $H_1(G, A) = 0$, мы получаем точную последовательность

$$0 \to H_0(G, R) \to H_0(G, L) \xrightarrow{\beta} H_0(G, A) \to 0.$$

Так как β — изоморфизм, $H_0(G, R) = 0$, а значит, и $R = 0$ по лемме 9.1. Следовательно, φ — изоморфизм.

Теорема 9.1. *Пусть G — p-группа, A — такой G-модуль, что $pA = 0$, тогда следующие утверждения равносильны:*

(i) *A — свободный $\mathbf{F}_p[G]$-модуль;*
(ii) *A — индуцированный модуль;*
(iii) *A когомологически тривиален;*
(iv) *$\hat{H}^q(G, A) = 0$ для некоторого целого числа q.*

Доказательство. Ясно, что (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv).
(iv) $\Rightarrow$ (i). С помощью сдвига размерности сконструируем такой G-модуль B, что $pB = 0$ и $\hat{H}^{q+r}(G, A) = \hat{H}^{r-2}(G, B)$ для всех r. Тогда $H_1(G, B) = 0$, и потому B свободен над $\mathbf{F}_p[G]$ (лемма 9.2); значит,

$$\hat{H}^{-2}(G, A) = \hat{H}^{-q-4}(G, B) = 0.$$

Отсюда следует (снова по лемме 9.2), что A — свободный модуль над $\mathbf{F}_p[G]$.

Теорема 9.2. *Пусть G — p-группа и A — G-модуль без p-кручения; тогда следующие утверждения равносильны:*
(i) *A когомологически тривиален;*
(ii) *$\hat{H}^q(G, A) = \hat{H}^{q+1}(G, A) = 0$ для некоторого целого числа q;*
(iii) *A/pA — свободный $\mathbf{F}_p[G]$-модуль.*

Доказательство. То, что (i) $\Rightarrow$ (ii), очевидно.
(ii) $\Rightarrow$ (iii). Из точной последовательности

$$0 \to A \xrightarrow{p} A \to A/pA \to 0$$

мы получаем точную последовательность $\hat{H}^q(G, A) \to \hat{H}^q(G, A/pA) \to \hat{H}^{q+1}(G, A)$. Поэтому $\hat{H}^q(G, A/pA) = 0$, а значит, по теореме 1 модуль A/pA свободен над $\mathbf{F}_p[G]$.
(iii) $\Rightarrow$ (i). Из этой же точной последовательности мы получаем, что

$$\hat{H}^q(H, A) \xrightarrow{p} \hat{H}^q(H, A)$$

является изоморфизмом для всех целых чисел q и всех подгрупп H группы G. Но группа $\hat{H}^q(H, A)$ является p-группой (следствие 1 из предложения 6.3), поэтому $\hat{H}^q(H, A) = 0$.

Следствие. *Пусть A — G-модуль, свободный над $\mathbf{Z}$ и удовлетворяющий одному из эквивалентных условий теоремы 9.2. Тогда для каждого G-модуля B без кручения G-модуль $N = \mathrm{Hom}(A, B)$ когомологически тривиален.*

Доказательство. Так как A свободен над $\mathbf{Z}$, точная последовательность $0 \to B \xrightarrow{p} B \to B/pB \to 0$ дает точную последовательность

$$0 \to N \xrightarrow{p} N \to \mathrm{Hom}(A, B/pB) \to 0,$$

так что модуль N не имеет p-кручения и

$$N/pN \cong \mathrm{Hom}(A/pA, B/pB).$$

Так как A/pA — свободный $\mathbf{F}_p[G]$-модуль, то он индуцированный и потому является прямой суммой подмодулей вида $s \cdot A'$ ($s \in G$), где A' — подгруппа группы A/pA. Следовательно, N/pN — прямая сумма подгрупп $s \cdot \mathrm{Hom}(A', B/pB)$ и потому N/pN индуцирован. Следовательно, по теоремам 9.1 и 9.2 N когомологически тривиален.

G-модуль A называется *проективным*, если функтор $\mathrm{Hom}_G(A, \cdot)$ точный или, что то же самое, если A является прямым слагаемым свободного G-модуля. Проективный G-модуль когомологически тривиален.

Теорема 9.3. *Пусть G — конечная группа, A — $\mathbf{Z}$-свободный G-модуль и G_p — силовская p-подгруппа группы G. Тогда следующие утверждения эквивалентны:*

(i) *для каждого простого числа p модуль A, рассматриваемый как G_p-модуль, обладает одним из равносильных свойств теоремы* 9.2;

(ii) *A — проективный G-модуль.*

Доказательство. Импликация (ii) $\Rightarrow$ (i) очевидна.

(i) $\Rightarrow$ (ii): выберем такую точную последовательность $0 \to Q \to F \to A \to 0$, что ее член F является свободным G-модулем. Так как A свободен над $\mathbf{Z}$, то последовательность

$$0 \longrightarrow \mathrm{Hom}(A, Q) \longrightarrow \mathrm{Hom}(A, F) \longrightarrow \mathrm{Hom}(A, A) \longrightarrow 0$$

точна. По следствию из теоремы 9.2 модуль $\mathrm{Hom}(A, Q)$ когомологически тривиален как G_p-модуль для всех p и потому по следствию 4 из предложения 6.3 $H^1(G, \mathrm{Hom}(A, Q)) = 0$. Принимая во внимание, что $H^0(G, \mathrm{Hom}(A, Q)) = (\mathrm{Hom}(A, Q))^G = \mathrm{Hom}_G(A, Q)$ и т. д., мы получаем, что отображение $\mathrm{Hom}_G(A, F) \to \mathrm{Hom}_G(A, A)$ сюръективно. В частности, тождественное отображение A в A продолжается до G-гомоморфизма A в F. Отсюда следует, что модуль A является прямым слагаемым в F и, следовательно, проективен.

Теорема 9.4. *Пусть A — произвольный G-модуль. Тогда следующие утверждения равносильны:*

(i) *для каждого простого числа p равенство $\hat{H}^q(G_p, A) = 0$ имеет место для некоторых двух последовательных значений q (вообще говоря, зависящих от p);*

(ii) *A когомологически тривиален;*

(iii) *существует точная последовательность $0 \to B_1 \to B_0 \to A \to 0$, в которой модули B_0 и B_1 проективны.*

Доказательство. Импликация (ii) $\Rightarrow$ (i) очевидна; импликация (iii) $\Rightarrow$ (ii) также вытекает сразу, если принять во внимание когомологическую тривиальность G-модуля.

(i) $\Rightarrow$ (iii). Выберем точную последовательность G-модулей

$$0 \longrightarrow B_1 \longrightarrow B_0 \longrightarrow A \longrightarrow 0,$$

такую, что B_0 — свободный G-модуль. Тогда $\hat{H}^q(G_p, B_1) \cong \hat{H}^{q-1}(G_p, A)$ для всех p и q, и потому $\hat{H}^q(G_p, B_1) = 0$ для двух последовательных значений q. Таким образом, модуль B_1 свободен над $\mathbf{Z}$ (потому что таков B_0), а значит, по теореме 9.3 он проективен.

§ 10. ТЕОРЕМА ТЭЙТА

Теорема 10.1. *Пусть G — конечная группа, B и C — два G-модуля и $f\colon B \to C$ — G-гомоморфизм. Для любого простого числа p обозначим через G_p силовскую p-подгруппу группы G. Предположим, что для любого p существует такое целое число n_p, что отображение*

$$f_q^*\colon \hat{H}^q(G_p, B) \longrightarrow \hat{H}^q(G_p, C)$$

сюръективно при $q = n_p$, биективно при $q = n_p + 1$ и инъективно при $q = n_p + 2$. Тогда для любой подгруппы H группы G и любого целого числа q отображение

$$f_q^*\colon \hat{H}^q(H, B) \longrightarrow \hat{H}^q(H, C)$$

является изоморфизмом.

Доказательство. Пусть $B^* = \mathrm{Hom}(\Lambda, B)$ и отображение $i\colon B \to B^*$ — естественное вложение (определенное формулой $i(b)(g) = g \cdot b$). Отображение $(f, i)\colon B \to C \oplus B^*$ будет тогда инъективным, и потому существует точная последовательность

$$0 \longrightarrow B \longrightarrow C \oplus B^* \longrightarrow D \longrightarrow 0.$$

Когомологии у $C \oplus B^*$ такие же, как и у модуля C, так как модуль B^* когомологически тривиален. Точная последовательность когомологий и условия теоремы дают тогда равенство $\hat{H}^q(G_p, D) = 0$ при $q = n_p$ и $q = n_p + 1$. Из теоремы 9.4 следует, что модуль D тривиален, а отсюда вытекает справедливость доказываемой теоремы.

Теорема 10.2. *Пусть A, B, C — три G-модуля, $\varphi\colon A \otimes B \to C$ — G-гомоморфизм. Зафиксируем целое число q и элемент a из $\hat{H}^q(G, A)$. Предположим, что для каждого простого числа p существует такое целое число n_p, что отображение $\hat{H}^n(G_p, B) \to \hat{H}^{n+q}(G_p, C)$, индуцированное $\cup$-умножением на $\mathrm{Res}_{G/G_p}(a)$ (относительно φ), сюръектив-*

но для $n = n_p$, биективно для $n = n_p + 1$ и инъективно для $n = n_p + 2$. Тогда для всех подгрупп H из G и всех целых n $\cup$-умножение на $\mathrm{Res}_{G/H}(a)$ индуцирует изоморфизм

$$\hat{H}^n(H, B) \longrightarrow \hat{H}^{n+q}(H, C)$$

(в явном виде задаваемый формулой $b \mapsto \varphi^*_{n+q}(\mathrm{Res}_{G/H}(a) \cdot b)$.)

Доказательство. Случай $q = 0$ — это по существу теорема 10.1. У нас есть элемент $a \in \hat{H}^0(G, A)$. Выберем его представитель $\alpha \in A^G$ (заметим, что α представляет также все элементы $\mathrm{Res}_{G/H}(a)$ для любой подгруппы H). Зададим отображение $f: B \longrightarrow C$ формулой $f(\beta) = \varphi(\alpha \otimes \beta)$; отображение f является G-гомоморфизмом в силу G-инвариантности α. Мы покажем, что для всякого $b \in \hat{H}^n(H, B)$

$$\varphi^*(\mathrm{Res}_{G/H}(a) \cdot b) = f^*(b). \tag{1}$$

Из определения f следует, что равенство (1) верно при $n = 0$. Общий случай после этого получается сдвигом размерности. Чтобы сдвинуть ее, например, вниз, предположим, что равенство (1) верно для $n + 1$, и рассмотрим коммутативную диаграмму

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B' & \longrightarrow & B_* & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle 1\otimes f} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & C' & \longrightarrow & C_* & \longrightarrow & C & \longrightarrow & 0, \end{array} \tag{2}$$

где $B_* = \Lambda \otimes B$, $C_* = \Lambda \otimes C$ и строки точны. Модули B_* и C_* индуцированы и, следовательно, когомологически тривиальны; связывающие гомоморфизмы δ являются изоморфизмами, и диаграмма

$$\begin{array}{ccc} \hat{H}^n(H, B) & \xrightarrow{\delta} & \hat{H}^{n+1}(H, B') \\ \downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle f'^*} \\ \hat{H}^n(H, C) & \xrightarrow{\delta} & \hat{H}^{n+1}(H, C') \end{array}$$

коммутативна. Более того, строки в диаграмме (2) расщепляются над $\mathbf{Z}$ и, следовательно, остаются точными (а вся диаграмма коммутативной), если ее тензорно умножить

на A (над $\mathbf{Z}$). Пусть $\varphi'': A \otimes B' \longrightarrow C'$ — гомоморфизм, индуцированный гомоморфизмом φ: $A \otimes B \longrightarrow C$. Используя индуктивное предположение и перестановочность $\cup$-произведений со связывающими гомоморфизмами, получаем, что

$$\hat{\delta} \circ f^*(b) = f'^* \circ \hat{\delta}(b) = \varphi''^*(\mathrm{Res}_{G/H}(a) \cdot \hat{\delta}(b)) =$$
$$= \varphi''^* \circ \hat{\delta}(\mathrm{Res}_{G/H}(a) \cdot b) = \hat{\delta} \circ \varphi^*(\mathrm{Res}_{G/H}(a) \cdot b).$$

Так как $\hat{\delta}$ — изоморфизм, равенство (1) доказано.

Мы доказали тем самым, что f удовлетворяет условию теоремы 10.1; следовательно, f^*_n — изоморфизм. Этим устанавливается справедливость теоремы 10.2 в случае $q = 0$.

Общий случай получается с помощью другого использования сдвига размерности. Чтобы сдвинуть ее вниз с $q + 1$ до q, рассмотрим точную последовательность

$$0 \longrightarrow A' \longrightarrow A_* \longrightarrow A \longrightarrow 0,$$

где $A_* = \Lambda \otimes A$. Она дает изоморфизмы $\hat{\delta}: \hat{H}^q(H, A) \longrightarrow \hat{H}^{q+1}(H, A')$. Пусть $u = \mathrm{Res}_{G/H}(a) \subset \hat{H}^q(H, A)$, тогда $u' = \hat{\delta}(u) = \mathrm{Res}_{G/H}(\hat{\delta}(a))$. Кроме того, $\varphi: A \otimes B \longrightarrow C$ индуцирует $\varphi': A' \otimes B \longrightarrow C'$. Рассмотрим диаграмму

$$\begin{array}{ccccc} \hat{H}^n(H, B) & \xrightarrow{u} & \hat{H}^{n+q}(H, A \otimes B) & \xrightarrow{\varphi^*} & \hat{H}^{n+q}(H, C) \\ \| & & & & \downarrow{\scriptstyle \delta} \\ \hat{H}^n(H, B) & \xrightarrow{u'} & \hat{H}^{n+q+1}(H, A' \otimes B) & \xrightarrow{\varphi'^*} & \hat{H}^{n+q+1}(H, C') \end{array}$$

Эта диаграмма коммутативна, потому что

$$\hat{\delta} \circ \varphi^*(u \cdot b) = \varphi'^* \circ \hat{\delta}(u \cdot b) = \varphi'^*(\hat{\delta}(u) \cdot b) = \varphi'^*(u' \cdot b).$$

По предположению индукции нижняя строка — изоморфизм и δ — изоморфизм; следовательно, верхняя строка — также изоморфизм.

Теорема 10.3. (Тэйт.) *Пусть A — некоторый G-модуль и $a \in H^2(G, A)$. Для каждого простого числа p обозначим через G_p силовскую p-подгруппу группы G и предположим, что*

(i) $H^1(G_p, A) = 0$;

(ii) $H^2(G_p, A)$ *— циклическая группа с образующей* $\mathrm{Res}_{G/G_p}(a)$ *и порядком, равным порядку G_p. Тогда для всех*

подгрупп H группы G и всех целых n $\cup$-умножение на $\mathrm{Res}_{G/H}(a)$ *индуцирует изоморфизм*

$$\hat{H}^n(H, \mathbf{Z}) \longrightarrow \hat{H}^{n+2}(H, A).$$

Доказательство. Положим в теореме 10.2 $B = \mathbf{Z}$, $C = A$, $q = 2$, $n_p = -1$. Для $n = -1$ сюръективность следует из (i). Для $n = 0$ группа $\hat{H}^0(G_p, \mathbf{Z})$ циклическая, причем порядок ее равен порядку G_p, поэтому и биективность следует из (iii). При $n = 1$ инъективность вытекает из того, что $H^1(G_p, \mathbf{Z}) = \mathrm{Hom}(G_p, \mathbf{Z}) = 0$. Таким образом, полностью выполнены условия теоремы 10.2.

ГЛАВА V

Проконечные группы

К. Грюнберг

§ 1. ГРУППЫ

1.1. Введение

Проконечной группой называется проективный предел конечных групп. Мы начнем с разъяснения некоторых деталей этого определения (все основные факты, касающиеся проективных пределов, а также индуктивных пределов, которые понадобятся нам позже, содержатся в [5], гл. VIII).

Все наши топологические группы предполагаются хаусдорфовыми пространствами. Морфизмами топологических групп будут называться непрерывные гомоморфизмы.

1.2. Проективные системы

Пусть I — направленное множество с отношением $\leqslant$. Это значит, что отношение $\leqslant$ рефлексивно, транзитивно и что для любых i_1, i_2 из I найдется $i \in I$, такое, что $i \geqslant i_1$ и $i \geqslant i_2$.

Проективной системой топологических групп над I называется объект $(I; G_i; \pi_i^j)$, где каждому i из I сопоставлена топологическая группа G_i и каждой паре $i \leqslant j$ из I сопоставлен морфизм $\pi_i^j\colon G_j \to G_i$. Далее, π_i^i — тождественный морфизм группы G_i; и если $i \leqslant j \leqslant k$, то $\pi_i^j \cdot \pi_j^k = \pi_i^k$ (отображения читаются справа налево). Проективную систему мы будем часто обозначать просто через (G_i).

Предположим, что $(G'_{i'})$ (над I') — вторая проективная система. Пусть $\phi\colon I' \to I$ — отображение, сохраняющее порядок, и для каждого $i' \in I'$ задан морфизм $\phi_{i'}\colon G_{\phi(i')} \to G'_{i'}$,

такой, что, коль скоро $i' \leqslant j'$ в I', диаграмма

$$\begin{array}{ccc} G_{\Phi(i')} & \xrightarrow{\phi_{i'}} & G'_{i'} \\ \uparrow{\scriptstyle \pi^{\Phi(j')}_{\Phi(i')}} & & \uparrow{\scriptstyle \pi'^{j'}_{i'}} \\ G_{\Phi(j')} & \xrightarrow{\phi_{j'}} & G'_{j'} \end{array}$$

коммутативна. Тогда мы скажем, что $(\phi;\ \phi_{i'},\ i' \in I') = \Phi$ есть морфизм (G_i) в $(G'_{i'})$.

1.3. Проективные пределы

Конечные группы будут теперь рассматриваться как топологические с дискретной топологией. Пусть (G_i) — проективная система *конечных* групп; образуем $\prod G_i$ — прямое произведение всех групп G_i, $i \in I$, и введем в него топологию обычным образом, объявив базой окрестности единицы ядра проекций $\prod G_i \to G_i$. Обозначим через L подмножество всех точек (x_i) из $\prod G_i$ со следующим свойством: $\pi^j_i(x_j) = x_i$, если $i \leqslant j$. Тогда L — подгруппа в $\prod G_i$, и мы можем ввести в нее индуцированную топологию. Назовем L *проективным (обратным) пределом* системы (G_i) (или, менее точно, групп G_i, $i \in I$). Если все группы G_i — конечные p-группы, то L называется *про-p-группой*. Мы будем писать $L = \varprojlim G_i$.

Очевидно, что L замкнуто в $\prod G_i$; действительно, если $x \notin L$, то существуют $i \leqslant j$, такие, что $\pi^j_i(x_j) \neq x_i$, а множество всех элементов в $\prod G_i$ с i-й координатой x_i и j-й координатой x_j открыто и содержит x, но не содержит элементов из L.

Если Φ: $(G_i) \to (G'_{i'})$ — морфизм проективных систем, то можно определить отображение ψ: $\prod G_i \to \prod G'_{i'}$ следующим образом: для данного x из $\prod G_i$ и любого i' из I' образ $\psi(x)$ есть тот элемент в $\prod G'_{i'}$, i'-я координата которого равна $\phi_{i'}(x_{\phi(i')})$. Очевидно, что ψ будет гомоморфизмом групп, причем непрерывным, поскольку для каждого i' ядро отображения $\prod G_i \to G'_{i'}$ открыто. Ограничением на L получаем непрерывный гомоморфизм $\varprojlim G_i$ в $\varprojlim G'_{i'}$.

1.4. Топологическая характеристика проконечных групп

Основной результат этого пункта нам в дальнейшем не будет нужен. Читатель может принять его на веру; будут нужны только следствия. Мы приведем тем не менее доказательство во всех подробностях, поскольку его не так легко извлечь из существующей литературы.

Теорема 1.1. *Топологическая группа является проконечной тогда и только тогда, когда она компактна и вполне несвязна.*

Отметим два факта, за доказательствами которых мы отошлем читателя к книге [2].

(i) Утверждение о том, что компактная группа вполне несвязна, эквивалентно следующему: единица совпадает с пересечением всех открытых компактных окрестностей единицы ([2], стр. 38).

(ii) В компактной вполне несвязной группе всякая окрестность единицы содержит открытый нормальный делитель (и, значит, единица есть пересечение всех открытых нормальных делителей; [2], стр. 56).

Доказательство. Пусть (G_i) — проективная система конечных групп; введем обозначения $L = \varprojlim G_i$, $C = \prod G_i$. Тогда C — компакт (теорема Тихонова) и, следовательно, L — также компакт, потому что L замкнуто в C.

Далее мы должны показать, что L вполне несвязно. Рассмотрим вначале C. Если $x \neq 1$ в C, то $x_i \neq 1$ для какого-нибудь $i \in I$. Положим $U_i = 1_i$, $U_j = G_j$ при $j \neq i$ и $U = \prod U_k$. Тогда группа U компактна, открыта и содержит 1, но не содержит x. Значит, C вполне несвязно (утверждение (i), см. выше). В компактной группе подмножество компактно тогда и только тогда, когда оно замкнуто. Так как в C единица есть пересечение всех открыто-замкнутых подмножеств, содержащих ее, то, следовательно, то же верно и для L (в индуцированной топологии); значит, L вполне несвязно.

Теперь допустим обратное, а именно что G — компактная вполне несвязная группа. Пусть (H_i) — семейство всех открытых нормальных делителей группы G. Тогда

семейство факторгрупп (G/H_i) образует проективную систему (положим $i \leqslant j$, если $H_i \supseteq H_j$, и воспользуемся естественным эпиморфизмом $G/H_j \to G/H_i$). Пусть $L = \varprojlim G/H_i$. Так как каждая группа G/H_i конечна, то группа L проконечна. Отображение θ: $g \to (gH_i)$ является, очевидно, непрерывным гомоморфизмом группы G в L. Поскольку $1 = \bigcap H_i$ (утверждение (ii), см. выше), отображение θ взаимно однозначно. С другой стороны, если $a = (a_i H_i) \in L$ и $S = \bigcap a_i H_i$, то S непусто (в силу компактности) и, таким образом, $\theta(g) = a$ для $g \in S$, так что отображение θ сюръективно. Значит, θ^{-1} также является отображением, и притом непрерывным. Отсюда мы заключаем, что θ — изоморфизм, и, следовательно, G — проконечная группа.

Последняя часть нашего доказательства дает также возможность получить

Следствие 1. *Для любой проконечной группы G имеет место*

$$G \cong \varprojlim G/U,$$

где U пробегает семейство всех открытых нормальных делителей группы G.

Следствие 2. *Если H — замкнутая подгруппа группы G, то*

$$H \cong \varprojlim H/(H \cap U).$$

Доказательство. Если V — открытый нормальный делитель группы H, то $V = O \cap H$ для некоторой окрестности O единицы в G. Значит, O содержит некоторый нормальный делитель U группы G (утверждение (ii), см. выше), так что $U \cap H \subseteq V$. Итак, семейство $(U \cap H)$ для произвольных U конфинально семейству всех открытых нормальных делителей группы H. Наше утверждение получается теперь из следствия 1 и из [5], следствие 3.16.

Следствие 3. *Если H — замкнутый нормальный делитель группы G, то*

$$G/H \cong \varprojlim G/UH.$$

Доказательство. Мы только что показали, что группа G/H проконечна. Ясно, что G/H компактна. Осталось проверить, что G/H вполне несвязна. Возьмем любое $x \notin H$. Для каждого h из H можно выбрать открытую и компактную окрестность O_h, не содержащую x (потому что группа G вполне несвязна). Тогда $H \subseteq \bigcup O_h$, и, таким образом, в силу компактности H можно утверждать, что $H \subseteq O_{h_1} \cup O_{h_2} \cup \ldots \cup O_{h_r}$. Таким образом, $O_{h_1} \cup O_{h_2} \cup \ldots O_{h_r}$ открыто, компактно и содержит H, но не содержит x.

1.5. Построение проконечных групп из абстрактных группп

Пусть G — абстрактная группа, и пусть $(H_i;\ i \in I)$ — такое семейство ее нормальных делителей, что для любых H_{i_1}, H_{i_2} найдется $H_i \subseteq H_{i_1} \cap H_{i_2}$. Если I частично упорядочить, положив $i \leqslant j$, коль скоро $H_i \supseteq H_j$, то I станет направленным множеством, и (G/H_i) будет проективной системой групп (роль π_i^j играют естественные гомоморфизмы $G/H_j \to G/H_i$). Отображение θ: $g \to (gH_i)$ есть гомоморфизм группы G на $L = \varprojlim G/H_i$.

Если $G_0 = \bigcap H_i$, то факторгруппа G/G_0 становится топологической группой, если за базу открытых множеств, содержащих единицу, мы возьмем группы H_i/G_0 (см. [2], стр. 25). Гомоморфизм θ индуцирует непрерывный гомоморфизм $G/G_0 \to L$, и группа L будет *пополнением* группы G/G_0 по отношению к H_i/G_0.

Отметим два важных случая.

(i) (H_i) совпадает с семейством всех нормальных делителей конечного индекса группы G. Обозначим проконечную группу $\varprojlim G/H_i$ через $\hat{G}$. Например, $\hat{\mathbf{Z}}$ есть проективный предел всех конечных циклических групп.

(ii) (H_i) совпадает с семейством всех нормальных делителей, индекс которых есть степень заданного простого числа p. Тогда $\varprojlim G/H_i = \hat{G}_p$ является про-p-группой. Например, $\hat{\mathbf{Z}}_p$ (обычно пишут $\mathbf{Z}_p$) есть проективный предел всех конечных циклических p-групп. Это группа целых p-адических чисел.

Упражнение. Доказать, что $\hat{\mathbf{Z}} = \prod \mathbf{Z}_p$.

1.6. Проконечные группы в теории полей

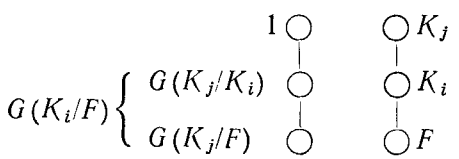
Пусть E — расширение Галуа поля F. Это значит, что E алгебраично над F и группа $G = G(E/F)$ всех F-автоморфизмов поля E не имеет неподвижных точек вне F. (Простейшие факты теории полей, включая конечную теорию Галуа, см. в [1], гл. V.)

Пусть $\{K_i;\ i \in I\}$ — семейство всех конечных расширений Галуа поля F, содержащихся в E. Тогда $E = \bigcup K_i$ (см. [1], 10.1).

Далее:

(i) если $K_i \subseteq K_j$, то существует естественный гомоморфизм π_i^j: $G(K_j/F) \to G(K_i/F)$;

(ii) F-композит полей K_{i_1} и K_{i_2} есть одно из полей K_j.



Таким образом, группы Галуа $G(K_i/F)$ образуют проективную систему, и можно построить ее проективный предел; обозначим его через L.

Предложение 1.1. $G(E/F) \cong L$.

Доказательство. Для каждого $i \in I$ мы имеем гомоморфизм $G(E/F) \to G(K_i/F)$. Все эти гомоморфизмы, вместе взятые, дают гомоморфизм θ: $G(E/F) \to \prod G(K_i/F)$. Образ отображения θ, очевидно, содержится в группе L. Мы утверждаем, что θ есть изоморфизм на группу L.

Если $g \neq 1$ в группе G, то найдется элемент x в E, такой, что $g(x) \neq x$, и найдется поле K_i, содержащее x. Далее, образ элемента g в группе $G(K_i/F)$ отображает элемент x в $g(x)$ и, следовательно, не является тождественным отображением. Значит, отображение θ взаимно однозначно.

Возьмем в группе L элемент (g_i). Если $x \in E$ и если мы положим $g(x) = g_i(x)$, где $x \in K_i$, то получим однозначное определение отображения g поля E в себя. Легко проверить, что g действительно является F-автоморфизмом поля E. Так как $\theta(g) = (g_i)$, то группа L совпадает с образом отображения θ.

Используя изоморфизм θ, можно перенести топологию с группы L на G. *Таким образом, $G = G(E/F)$ теперь — проконечная группа*, и если положить $U_i = G(E/K_i)$, то семейство (U_i) определяет в ней систему окрестностей единицы (см. [2], стр. 25—26).

Пример. Если E — алгебраическое замыкание поля $\mathbf{F}_p$ из p элементов, то $G(E/\mathbf{F}_p) \cong \hat{\mathbf{Z}}$ (см. п. 1.5).

Теорема 1.2 (основная теорема теории Галуа). *Пусть E — расширение Галуа поля F с группой G; $\mathcal{S}$ — множество всех замкнутых подгрупп группы G; $\mathcal{F}$ — множество всех полей, заключенных между E и F. Тогда $K \to G(E/K)$ является взаимно однозначным отображением $\mathcal{F}$ на $\mathcal{S}$. Обратным к нему будет отображение $S \to E^S$, где E^S обозначает поле неподвижных точек для замкнутой подгруппы S.*

Доказательство. *Первый шаг.* Покажем, что если $K \in \mathcal{F}$, то $G(E/K) \in \mathcal{S}$.

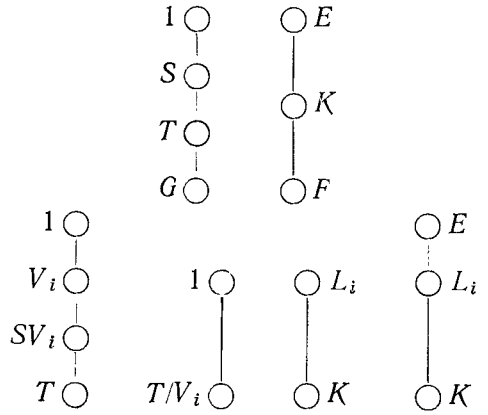
Пусть $\{L_j;\ j \in J\}$ — семейство всех конечных расширений поля F, содержащихся в K. Тогда $K = \bigcup L_j$, и потому $G(E/K) = \bigcap G(E/L_j)$.

Каждое поле L_j содержится в некотором конечном расширении Галуа K_i; следовательно, $G(E/L_j) \supseteq G(E/K_i)$. Согласно предложению 1.1, группа $G(E/K_i)$ открыта, и потому группа $G(E/L_j)$ также открыта в $G(E/F)$. Значит, группа $G(E/L_j)$ замкнута, и, следовательно, группа $\bigcap G(E/L_j) = G(E/K)$ также замкнута.

Второй шаг. Если $K \in \mathcal{F}$, то $K = E^{G(E/K)}$ (см. [1], 10.2).

Третий шаг. Пусть S — замкнутая подгруппа группы G, и пусть $K = E^S$ и $T = G(E/K)$. Ясно, что $S \subseteq T$. Но в силу результата второго шага $E^S = E^T$. Значит, для каждого открытого нормального делителя V_i группы T имеет место

$L_i^{T/V_i} = K = L_i^{SV_i/V_i}$, если только $L_i = E^{V_i}$.



Согласно конечной теории Галуа, мы заключаем, что $T/V_i = SV_i/V_i$, т. е. $T = SV_i$. Следовательно, подгруппа S плотна в группе T. Но S замкнута (см. первый шаг), поэтому $S = T$.

§ 2. ТЕОРИЯ КОГОМОЛОГИЙ

2.1. Введение

Для того чтобы развить теорию когомологий проконечных групп, мы воспользуемся двумя соображениями: (i) понятие проконечной группы вводится через понятие конечной группы; (ii) известно, как строится теория когомологий конечных групп.

2.2. Индуктивные системы и индуктивные пределы

Мы ограничимся здесь только категорией всех дискретных абелевых групп (записываемых аддитивно).

Рассмотрим семейство (A_i) абелевых групп, занумерованных направленным множеством индексов I. Предположим, что для любых $i \leqslant j$ из I задан гомоморфизм $\tau_i^j\colon A_i \to A_j$, причем: (i) τ_i^i — тождественный морфизм $A_i \to A_i$; (ii) если $i \leqslant j \leqslant k$, то $\tau_j^k \cdot \tau_i^j = \tau_i^k$. Назовем объект $(I;\ A_i;\ \tau_i^j)$ *индуктивной системой* абелевых групп над I. Иногда мы будем писать просто (A_i).

Пусть $(A'_{i'})$ (над I') — вторая индуктивная система, а $\psi\colon I \to I'$ — сохраняющее порядок отображение; пусть также для каждого $i \in I$ задан гомоморфизм $\psi_i\colon A_i \to A'_{\psi(i)}$; если из того, что $i \leqslant j$, следует коммутативность диаграммы

$$\begin{array}{ccc} A_i & \xrightarrow{\psi_i} & A'_{\psi(i)} \\ {\scriptstyle \tau_i^j}\downarrow & & \downarrow{\scriptstyle \tau'^{\psi(j)}_{\psi(i)}} \\ A_j & \xrightarrow{\psi_j} & A'_{\psi(j)} \end{array}$$

то мы назовем $\Psi = (\psi;\ \psi_i)$ морфизмом индуктивных систем $(A_i) \to (A'_{i'})$.

Для данной системы (A_i) обозначим через S дизъюнктное объединение групп A_i, $i \in I$. Если $x \in A_i$, $y \in A_j$, то запись $x \sim y$ будет означать, что найдется такое k, что $k \geqslant i$, $k \geqslant j$ и $\tau_i^k(x) = \tau_j^k(y)$. Тогда $\sim$ будет отношением эквивалентности во множестве S. Множество классов эквивалентности обозначим через $\varinjlim A_i$, а класс, содержащий элемент x,— через $\tilde{x}$.

Превратим теперь $A = \varinjlim A_i$ в абелеву группу (индуктивный предел групп A_i, $i \in I$) следующим образом. Если $\tilde{x}$, $\tilde{y} \in A$, где $x \in A_i$, $y \in A_j$, то найдем такое k, что $k \geqslant i$ и $k \geqslant j$, и определим $\tilde{x} + \tilde{y}$ как класс, содержащий $\tau_i^k(x) + \tau_j^k(y)$; аналогично класс $-\tilde{x}$ определим как $\widetilde{-x}$. Ясно, что A при этом становится абелевой группой.

Если $\Psi\colon (A_i) \to (A'_{i'})$ — морфизм индуктивных систем, то мы получаем гомоморфизм $\varinjlim A_i$ в $\varinjlim A'_{i'}$, определяя образ класса $\tilde{x}$, где $x \in A_i$, как класс элемента $\psi_i(x)$.

2.3. Дискретные модули

Пусть G — проконечная группа и A — (левый) G-модуль. Если U — открытая подгруппа группы G, то мы, как обычно, обозначим через A^U множество всех элементов из A, неподвижных при действии U. Мы будем рас-

сматривать только G-модули A, удовлетворяющие условию

$$A = \bigcup A^U;$$

здесь объединение берется по всем нормальным делителям группы G. Такие модули называются *дискретными G-модулями*.

Нетрудно видеть, что следующие три условия, наложенные на G-модуль A, эквивалентны:

(i) A — дискретный G-модуль;

(ii) стабилизатор в G любого элемента из модуля является открытой подгруппой в G;

(iii) спаривание $G \times A \to A$ непрерывно, если модуль A рассматривается как дискретное топологическое пространство, а группа G — в ее обычной топологии проконечной группы.

2.4. Когомологии проконечных групп

Пусть A — дискретный G-модуль, и пусть $\{U_i;\ i \in I\}$ — семейство всех открытых нормальных делителей группы G. Тогда $G \cong \varprojlim G/U_i$ (следствие 1 из теоремы 1.1) и $A \cong \varinjlim A^{U_i}$ (так как $A = \bigcup A^{U_i}$, а $\bigcup A^{U_i}$ естественно изоморфно $\varinjlim A^{U_i}$).

Пусть q — фиксированное неотрицательное целое число. Для любых $i \leqslant j$ построим гомоморфизм (инфляцию)

$$\lambda_i^j\colon H^q(G/U_i, A^{U_i}) \to H^q(G/U_j, A^{U_j})$$

стандартным способом (см. гл. IV, § 4). Ясно, что тем самым мы получаем индуктивную систему абелевых групп

$$(I;\ H^q(G/U_i, A^{U_i});\ \lambda_i^j).$$

Определение. *Группа* $\varinjlim H^q(G/U_i, A^{U_i})$ *называется q-й группой когомологий группы G с коэффициентами в G-модуле A и обозначается через* $H^q(G, A)$.

Существует другой способ определения этих групп когомологий. Рассмотрим аддитивную группу $C^n = C^n(G, A)$ всех *непрерывных* отображений группы G^n в G-модуль A и определим кограницу d: $C^n \to C^{n+1}$ стандартной формулой:

$$(df)(g_1, \ldots, g_{n+1}) = g_1 \cdot f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n).$$

Тем самым мы получаем комплекс $C(G, A)$, и его группы когомологий как раз и будут группами $H^q(G, A)$.

Конечно, это нужно доказать. Рассуждение несложно, но (если излагать его полностью) длинно и скучно. Основной момент состоит в следующем. Отображение ϕ проконечной группы H в дискретное пространство S непрерывно тогда и только тогда, когда существуют открытый нормальный делитель K группы H и такое отображение ψ конечной группы H/K в S, что ϕ есть композиция естественной проекции $H \to H/K$ и ψ. Отсюда следует, что если $f \in C^n(G, A)$, то найдется открытый нормальный делитель U_1 группы G, такой, что f совпадает с отображением

$$G^n \to (G/U_1)^n \to A.$$

Так как функция f конечнозначна, то образ ее лежит в A^{U_2} для некоторого открытого нормального делителя U_2. Если $U = U_1 \cap U_2$, то функция f совпадает с отображением

$$G^n \to (G/U)^n \to A^U \to A$$

и отображение f': $(G/U)^n \to A^U$ является элементом из $C^n(G/U, A^U)$. Теперь уже нетрудно получить равенство $C^n(G, A) = \varinjlim C^n(G/U, A^U)$.

2.5. Пример: образующие про-p-групп

Пусть G — про-p-группа, а $\mathbf{F}_p$ — поле из p элементов, рассматриваемое как дискретный G-модуль с тривиальным действием. Из формулы, приведенной выше для df, немедленно следует равенство

$$H^1(G, \mathbf{F}_p) = \mathrm{Hom}(G, \mathbf{F}_p).$$

Если $G^* = G^{(p)}[G, G]$, то правая часть этого равенства совпадает с группой $\mathrm{Hom}(G/G^*, \mathbf{F}_p)$.

Предположим, что G как топологическая группа является конечно порожденной. Тогда факторгруппа G/G^* конечна, и ее размерность d как векторного пространства над $\mathbf{F}_p$ совпадает с размерностью группы $H^1(G, \mathbf{F}_p)$. Пусть $x_1G^*, \ldots, x_dG^*$ — базис факторгруппы G/G^*. Если U — какой-нибудь открытый нормальный делитель группы G, содержащийся в G^*, то $x_1, \ldots, x_d$ порождают G по модулю U (по теореме Бернсайда о базисе для конечных p-групп), и потому $x_1, \ldots, x_d$ порождают G топологически. Следовательно, $\dim_{\mathbf{F}_p} H^1(G, \mathbf{F}_p)$ *равна минимальному числу образующих группы* G.

2.6. Когомологии Галуа. I. Аддитивная теория

Мы предполагаем известными сведения из элементарной теории комологий Галуа в объеме [4], гл. X.

Пусть E, как и в п. 1.6, обозначает расширение Галуа поля F с группой $G = G(E/F)$. Обозначим через $\{K_i;\ i \in I\}$ семейство всех конечных расширений Галуа поля F, содержащихся в E, и положим $U_i = G(E/K_i)$. Тогда $G = \varprojlim G/U_i$.

Действие группы G на E превращает аддитивную группу поля E в G-модуль. При этом $E^{U_i} = K_i$ и $E = \bigcup K_i$, так что E — дискретный G-модуль. Далее, K_i является $G(K_i/F)$-модулем и $G(K_i/F) \cong G/U_i$. Итак, мы получаем, что

$$H^q(G, E) \cong \varinjlim H^q(G(K_i/F), K_i). \tag{1}$$

Предложение 2.1. $H^q(G, E) = 0$ *для всех* $q \geqslant 1$.

В силу соотношения (1) справедливость этого предложения немедленно вытекает из следующей леммы.

Лемма 2.1. *Пусть E — конечное расширение Галуа поля F и $G = G(E/F)$. Тогда $H^q(G, E) = 0$ для всех $q \geqslant 1$.*

Доказательство. Теорема о нормальном базисе утверждает, что E является свободным FG-модулем с одной образующей (см. [1], 10.8), т. е. FG-модуль E изоморфен индуцированному с F модулю. Отсюда и получается наше утверждение (см. гл. IV, § 6).

Заметим, что из этого рассуждения вытекает следующий более сильный результат.

Следствие. *Если E — конечное расширение Галуа поля F, то группы когомологий Тэйта $\hat{H}^q(G(E/F), E)$ нулевые для всех целых q.*

(Вспомним, что $\hat{H}^q = H^q$ для всех $q \geqslant 1$.)

2.7. Когомологии Галуа. II. «Теорема Гильберта 90»

Обозначения сохраняются те же, что и в п. 2.6. Мы видели, что E как G-модуль с когомологической точки зрения неинтересен. Совсем по-иному обстоит дело, когда мы рассматриваем как G-модуль группу E^* (мультипликативную группу поля E).

Так как $(E^*)^{U_i} = K_i^*$ и $E^* = \bigcup K_i^*$, то группа E^* также является дискретным G-модулем, причем

$$H^q(G, E^*) \cong \varinjlim H^q(G(K_i/F), K_i^*). \tag{2}$$

Предложение 2.2. $H^1(G, E^*) = 0$.

Доказательство. Ввиду изоморфизма (2) достаточно доказать это предложение только для конечных расширений E.

Пусть f будет 1-коциклом группы G с коэффициентами в E^*. По теореме о независимости автоморфизмов (см. [1], 7.5) найдется число c, такое, что

$$b = \sum_{x \in G} f(x) \cdot x(c) \neq 0.$$

Применяя к этому равенству действие элемента y из G и учитывая, что $f(yx) = f(y) \cdot yf(x)$, мы получаем

$$y(b) = \sum_{x \in G} [yf(x)]\,[yx(c)] = \sum_{x \in G} f^{-1}(y) f(yx) \cdot yx(c) =$$
$$= f^{-1}(y) \sum_{z \in G} f(z) \cdot z(c) = f^{-1}(y)\, b.$$

Итак, $f(y) = b \cdot y(b)^{-1}$, т. е. f является кограницей.

Следствие («теорема Гильберта 90»). *Если $G = G(E/F)$ — конечная циклическая группа с образу-*

ющим элементом g и элемент $a \in E^*$ таков, что $N_{E/F}(a) = 1$, то существует $b \in E^*$, такой, что $a = b/g(b)$.

Доказательство. Так как группа G циклическая, то $H^1(G, A) = {}_N A/(1-g)A$ (см. гл. IV, § 8). Здесь $A = E^*$ и потому (в мультипликативных обозначениях) $(1-g)A$ совпадает с $\{b/g(b),\ b \in E^*\}$. Так как $H^1(G, E^*) = 0$, отсюда получается требуемый результат.

2.8. Когомологии Галуа. III. Группы Брауэра

Пусть E_1 и E_2 — два расширения Галуа поля F, и пусть $G_i = G(E_i/F)$ $(i = 1, 2)$.

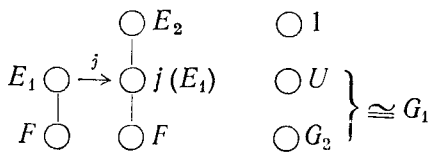
Обозначим через j некоторый F-гомоморфизм $E_1 \to E_2$. Тогда $j(E_1)$ будет расширением Галуа поля F, и потому ограничение $g \to g \mid j(E_1)$ дает морфизм $\bar{j}$: $G_2 \to G_1$. Пусть $U = G(E_2/j(E_1))$. Тогда

$$H^q(G_1, E_1^*) \xrightarrow{\sim} H^q(G_2/U, E_2^{*U}) \xrightarrow{\inf} H^q(G_2, E_2^*);$$

мы обозначим через j^* композицию этих двух гомоморфизмов:

$$j^*\colon H^l(G_1, E_1^*) \to H^q(G_2, E_2^*).$$

Мы утверждаем, что j^* и j независимы.



Пусть j' — другой F-гомоморфизм $E_1 \to E_2$, дающий морфизм $\bar{j}'$: $G_2 \to G_1$. Так как $j'(E_1) = j(E_1)$ (см. [1], 6.3), то $j' = jg$ для некоторого g из G_1. Следовательно, $(j')^* = j^*g^*$.

Автоморфизм g: $E_1 \to E_1$ приводит при помощи описанного процесса к морфизму $\bar{g}$: $G_1 \to G_1$. Ясно, что $\bar{g}$ будет внутренним автоморфизмом $x \to g^{-1}xg$ группы G_1. Поэтому g^* тождествен на группе $H^q(G_1, E_1^*)$ (см. гл. IV, предложение 4.2).

Итак, $(j')^* = j^*$ и, значит, j^* и j действительно независимы.

Предположим теперь, что E_1 и E_2 — два сепарабельных замыкания поля F. Тогда всегда существует F-изоморфизм $E_1 \to E_2$, и поэтому E_1 и E_2 дают *один и тот же* изоморфизм $H^l(G_1, E_1^*) \to H^q(G_2, E_2^*)$. Поэтому с когомологической точки зрения несущественно, какое из сепарабельных замыканий используется, и мы будем обозначать группу $H^q(G(E/F), E^*)$, где E — какое-либо заданное сепарабельное замыкание поля F, просто через $H^l(F)$. Группы $H^q(F)$ зависят от поля F функториально.

Определение. *Группой Брауэра поля F называется группа $H^2(F)$.*

Теорема 2.1. *Если E — расширение Галуа поля F, содержащее расширение Галуа K поля F, то имеет место точная последовательность*

$$0 \to H^2(G(K/F), K^*) \to H^2(G(E/F), E^*) \to H^2(G(E/K), E^*).$$

Следствие 1. *Если K — расширение Галуа поля F, то последовательность*

$$0 \to H^2(G(K/F), K^*) \to H^2(F) \to H^2(K)$$

точна.

Доказательство. Нужно взять какое-либо сепарабельное замыкание E поля F, содержащее поле K, и применить теорему 2.1.

Из следствия 1 непосредственно вытекает

Следствие 2. *Если (K_i) — семейство всех конечных расширений Галуа поля F в его сепарабельном замыкании, то*

$$H^2(F) = \bigcup H^2(G(K_i/F), K_i^*).$$

Чтобы доказать теорему 2.1, мы сначала переформулируем ее в терминах абстрактных проконечных групп.

Пусть $G = G(E/F)$, $H = G(E/K)$ и $A = E^*$. Тогда, согласно теории Галуа, $G/H \cong G(K/F)$ и $A^H \cong K^*$. Отображение $H^2(G, A) \to H^2(H, A)$ является ограничением, а отображение $H^2(G/H, A^H) \to H^2(G, A)$ — инфляцией. (Ограничение и инфляция для проконечных групп определяются точно так же, как и для абстрактных групп.) Теорема 2.1, а также предложение 2.2 вытекают теперь из следующего результата.

Предложение 2.3. *Пусть H — замкнутый нормальный делитель проконечной группы G и A — дискретный G-модуль, такой, что $H^1(H, A) = 0$. Тогда точна следующая последовательность*:

$$0 \to H^2(G/H, A^H) \xrightarrow{\inf} H^2(G, A) \xrightarrow{\mathrm{Res}} H^2(H, \ ).$$

Набросок доказательства. Условие $H^1(H, A) = 0$ эквивалентно тому, что для всех открытых нормальных делителей U_i группы G имеет место

$$H^1(HU_i/U_i, A^{U_i}) = 0.$$

Значит, для каждого U_i последовательность

$$0 \to H^2(G/HU_i, A^{HU_i}) \to H^2(G/U_i, A^{U_i}) \to H^2(HU_i/U_i, A^{U_i})$$

точна (гл. IV, предложение 5.2 при $q = 1$). Если $i \leqslant j$, то возьмем точные последовательности для i и для j и отображение инфляции, связывающее их между собой и дающее коммутативную диаграмму. Совокупность всех таких диаграмм образует «точную последовательность индуктивных систем». Требуемый результат получается теперь взятием индуктивного предела, если воспользоваться следующим:

(i) $\varinjlim$ является точным функтором на категории индуктивных систем над фиксированным множеством индексов (см. [5]);

(ii) $\varprojlim H/H \cap U_i \cong H$ и $\varprojlim G/HU_i \cong G/H$ (см. следствия 2 и 3 из теоремы 1.1).

Предложение 2.3 можно также доказать непосредственно методом, почти идентичным с тем, который используется в абстрактном случае.

ЛИТЕРАТУРА

Бурбаки (Bourbaki N.)
[1] Algèbre, Hermann, Paris, 1950. (Русский перевод: Бурбаки Н., Алгебра, Физматгиз, М., 1962, 1965, 1966.)

Монтгомери, Циппин (Montgomery D., Zippin L.)
[2] Topological transformation groups, Interscience, New York — London, 1955.

Серр (Serre J.-P.)
[3] Cohomologie Galoisienne, Springer-Verlag, Berlin, 1965. (Русский перевод: Серр Ж.-П., Когомологии Галуа, изд-во «Мир», М., 1968.)
[4] Corps locaux, Hermann, Paris, 1962.

Стинрод, Эйленберг (Steenrod N., Eilenberg S.)
[5] Foundations of algebraic topology, Princeton Univ. Press., Princeton, 1952. (Русский перевод: Стинрод Н., Эйленберг С., Основания алгебраической топологии, Физматгиз, М., 1958.)

ГЛАВА VI

Локальная теория полей классов

Ж.-П. Серр[1])

ВВЕДЕНИЕ

Мы называем поле K *локальным*, если оно полно в топологии дискретного нормирования v и если его поле вычетов k конечно. Через q обозначается число $p^f = \mathrm{Card}\,(k)$ элементов поля k, и все время предполагается, что нормирование v нормализовано, т. е. гомоморфизм $v\colon K^* \to \mathbf{Z}$ сюръективен. Структура таких полей нам известна.

1. Если поле K имеет характеристику 0, то оно является конечным расширением p-адического поля $\mathbf{Q}_p$, которое представляет собой пополнение поля рациональных чисел $\mathbf{Q}$ относительно p-адического нормирования. Если $[K : \mathbf{Q}_p] = n$, то $n = ef$, где f — степень классов вычетов (т. е. $f = [k : \mathbf{F}_p]$) и e — индекс ветвления, равный $v(p)$.

2. Если же поле K имеет характеристику p («случай равных характеристик»), то оно изоморфно полю $k((T))$ формальных степенных рядов, где T — униформизирующий параметр.

Первый случай — это именно та ситуация, которая возникает в процессе пополнения числового поля относительно простого числа p.

Мы будем изучать группы Галуа расширений поля K. Конечно, желательно было бы описать структуру группы Галуа $G(K_s/K)$ сепарабельного замыкания K_s поля K, так как она содержит информацию обо всех таких расширениях. (В случае характеристики 0 имеет место совпадение: $K_s = \bar{K}$.) Однако изложение ограничивается следующим.

1. Описание когомологических свойств всех расширений Галуа, как абелевых, так и не абелевых.

[1]) Подготовлено для печати Амитэйджем и Нигерсом.

2. Определение абелевых расширений поля K, т. е. определение группы G по модулю ее производной группы G'.

На протяжении этой главы мы будем придерживаться следующих обозначений. Кольцо целых элементов поля K мы обозначаем через O_K, мультипликативную группу поля K — через K^* и, наконец, группу единиц — через U_K. Аналогичные обозначения используются для расширений L/K; если расширение L/K является расширением Галуа, то его группу Галуа мы обозначаем или через $G(L/K)$, или через $G_{L/K}$, или просто через G. Если $s \in G$ и $\alpha \in L$, то результат действия s на α обозначается через ${}^s\alpha$ или $s(\alpha)$.

Изложение всех опущенных деталей читатель может найти в предыдущих главах, а также в книге [8].

§ 1. ГРУППА БРАУЭРА ЛОКАЛЬНОГО ПОЛЯ

1.1. Формулировки теорем

В этом пункте мы сформулируем главные результаты; доказательства будут даны в п. 1.2—1.6.

Начнем с определения группы Брауэра $\mathrm{Br}(K)$ поля K (см. также гл. V, п. 2.8). Пусть L — конечное расширение Галуа поля K с группой $G(L/K)$. Условимся обозначать группу $H^2(G_{L/K}, L^*)$ через $H^2(L/K)$. Если $(L_i)_{i\in I}$ — множество всевозможных конечных расширений Галуа поля K, то индуктивный (прямой) предел $\varinjlim H^2(L_i/K)$ и называется группой Брауэра $\mathrm{Br}(K)$ поля K.

Из определения следует, что $\mathrm{Br}(K) = H^2(K_s/K)$. Для вычисления группы $\mathrm{Br}(K)$ мы обратимся сначала к промежуточному полю K_{nr}, $K \subset K_{\mathrm{nr}} \subset K_s$, которое является максимальным неразветвленным расширением данного поля K. Со свойствами расширения K_{nr} читатель может познакомиться в гл. I, § 7. Мы лишь напомним, что поле вычетов расширения K_{nr} равно алгебраическому замыканию $\bar{k}$ поля k и что $G(K_{\mathrm{nr}}/K) = G(\bar{k}/k)$. Через F обозначается элемент Фробениуса группы $G(K_{\mathrm{nr}}/K)$; его действие на поле вычетов $\bar{k}$ задается правилом: $\lambda \mapsto \lambda^q$. Отображение $v \mapsto F^v$ представляет собой изоморфизм $\hat{\mathbf{Z}} \to G(K_{\mathrm{nr}}/K)$ топологических групп. Из гл. V, п. 2.5, мы знаем, что

группа $\hat{\mathbf{Z}}$ равна проективному (обратному) пределу $\varprojlim \mathbf{Z}/n\mathbf{Z}$ циклических групп $\mathbf{Z}/n\mathbf{Z}$.

Так как расширение K_{nr} содержится в замыкании K_s, группа $H^2(K_{\mathrm{nr}}/K)$ содержится в группе $\mathrm{Br}(K) = H^2(K_s/K)$. В действительности же имеют место следующие теоремы.

Теорема 1.1. $H^2(K_{\mathrm{nr}}/K) = \mathrm{Br}(K)$.

Выше мы уже отметили, что $H^2(K_{\mathrm{nr}}/K) = H^2(\hat{\mathbf{Z}}, K_{\mathrm{nr}}^*)$.

Теорема 1.2. *Нормирование* v: $K_{\mathrm{nr}}^* \to \mathbf{Z}$ *определяет изоморфизм* $H^2(K_{\mathrm{nr}}/K) \to H^2(\hat{\mathbf{Z}}, \mathbf{Z})$.

Вычислим группу $H^2(\hat{\mathbf{Z}}, \mathbf{Z})$. Пусть вообще G — некоторая проконечная группа; рассмотрим точную последовательность G-модулей

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

при тривиальном действии операторов из группы G. Модуль $\mathbf{Q}$ имеет тривиальные когомологии, так как он однозначно делим (т. е. $\mathbf{Z}$-инъективен); поэтому кограница δ: $H^1(\mathbf{Q}/\mathbf{Z}) \to H^2(\mathbf{Z})$ устанавливает некоторый изоморфизм $H^1(\mathbf{Q}/\mathbf{Z}) \to H^2(G, \mathbf{Z})$. Теперь мы имеем: $H^1(\mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ и, следовательно, $\mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) \cong H^2(G, \mathbf{Z})$.

Обратимся к группе $\mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z})$. Определим отображение γ: $\mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) \to \mathbf{Q}/\mathbf{Z}$ посредством $\phi \mapsto \phi(1) \in \mathbf{Q}/\mathbf{Z}$, где $\phi \in \mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z})$ [1]. Из теоремы 1.2 следует, что имеют место изоморфизмы

$$H^2(K_{\mathrm{nr}}/K) \xrightarrow{v} H^2(\hat{\mathbf{Z}}, \mathbf{Z}) \xrightarrow{\delta^{-1}} \mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\gamma} \mathbf{Q}/\mathbf{Z}.$$

В итоге определено отображение inv_K: $H^2(K_{\mathrm{nr}}/K) \to \mathbf{Q}/\mathbf{Z}$:

$$\mathrm{inv}_K = \gamma \circ \delta^{-1} \circ v.$$

Для удобства дальнейших ссылок суммируем наши выводы в виде следствия.

Следствие. *Отображение* $\mathrm{inv}_K = \gamma \circ \delta^{-1} \circ v$ *определяет изоморфизм групп* $H^2(K_{\mathrm{nr}}/K)$ *и* $\mathbf{Q}/\mathbf{Z}$.

[1] $1 \in \hat{\mathbf{Z}}$ — каноническая образующая, составленная из образов $1 \in \mathbf{Z}$ в группах $\mathbf{Z}/n\mathbf{Z}$. — *Прим. перев.*

Так как в силу теоремы 1.1 имеет место равенство $H^2(K_{\mathrm{nr}}/K) = \mathrm{Br}(K)$, то этим *установлен изоморфизм* inv_K: $\mathrm{Br}(K) \to \mathbf{Q}/\mathbf{Z}$.

Если L — конечное расширение поля K, то соответствующее отображение будет обозначаться через inv_L.

Теорема 1.3. *Пусть* L/K *— конечное расширение степени* n. *Тогда*

$$\mathrm{inv}_L \circ \mathrm{Res}_{K/L} = n \cdot \mathrm{inv}_K.$$

Другими словами, коммутативна следующая диаграмма:

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{\mathrm{Res}_{K/L}} & \mathrm{Br}(L) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbf{Q}/\mathbf{Z} & \xrightarrow{n} & \mathbf{Q}/\mathbf{Z} \end{array}$$

(Определение гомоморфизма $\mathrm{Res}_{K/L}$ читатель может найти в гл. IV, § 4 и в гл. V, п. 2.7.)

Следствие 1. *Элемент* $\alpha \in \mathrm{Br}(K)$ *переходит в нуль из группы* $\mathrm{Br}(L)$ *тогда и только тогда, когда* $n\alpha = 0$.

Следствие 2. *Пусть* L/K *— расширение степени* n. *Тогда группа* $H^2(L/K)$ *циклична и имеет порядок* n. *Точнее группа* $H^2(L/K)$ *порождается элементом* $u_{L/K} \in \mathrm{Br}(K)$, *инвариант* [1] *которого равен* $1/n \in \mathbf{Q}/\mathbf{Z}$.

Доказательство. Это следует из того, что группа $H^2(L/K)$ равна ядру гомоморфизма Res.

1.2. Вычисление группы $H^2(K_{\mathrm{nr}}/K)$

В этом пункте мы докажем теорему 1.2. Итак, нужно доказать, что гомоморфизм $H^2(K_{\mathrm{nr}}/K) \to H^2(\hat{\mathbf{Z}}, \mathbf{Z})$ является изоморфизмом.

Предложение 1.1. *Пусть* K_n *— неразветвленное расширение степени* n *поля* K *и* $G = G(K_n/K)$. *Тогда для всех* $q \in \mathbf{Z}$:

[1] То есть образ относительно отображения inv_K. — *Прим. перев.*

(1) $H^q(G, U_n) = 0$, *где* $U_n = U_{Kn}$;

(2) *отображение* v: $H^q(G, K_n^*) \to H^q(G, \mathbf{Z})$ *есть изоморфизм.*

(Теорема 1.2 представляет собой очевидное следствие утверждения (2) предложения 1.1, так как $H^2(K_{\text{nr}}/K) = H^2(\hat{\mathbf{Z}}, K_{\text{nr}}^*)$.)

Доказательство. Тот факт, что (1) влечет за собой (2), вытекает из последовательности когомологий:

$$H^q(G, U_n) \to H^q(G, K_n^*) \to H^q(G, \mathbf{Z}) \to H^{q+1}(G, U_n).$$

Остается доказать утверждение (1). Рассмотрим убывающую последовательность открытых подгрупп $U_n \supset U_n^1 \supset \supset U_n^2 \supset \ldots$, определенных следующим образом: $x \in U_n^i$ тогда и только тогда, когда $v(x-1) \geqslant i$. Пусть $\pi \in K$ — униформизирующий элемент; тогда $U_n^i = 1 + \pi^i O_n$, где $O_n = O_{K_n}$. В таком случае $U_n = \varprojlim U_n/U_n^i$. Доказательство теперь строится на следующих трех леммах.

Лемма 1.1. *Пусть* k_n *— поле вычетов расширения* K_n *Тогда существуют изоморфизмы, согласованные с группой Галуа:* $U_n/U_n^1 \cong k_n^*$ *и (при* $i \geqslant 1$) $U_n^i/U_n^{i+1} \cong k_n^+$.

(Изоморфизмы, согласованные с действием группы Галуа, будем называть *изоморфизмами Галуа.*)

Доказательство. Отобразим $\alpha \in U_n$ в элемент $\bar{\alpha}$, являющийся редукцией данного α в поле k_n. Согласно определению, $U_n^1 = 1 + \pi O_n$; поэтому если $\alpha \in U_n^1$, то $\bar{\alpha} = 1$, и первая часть леммы доказана.

Чтобы доказать вторую часть, возьмем элемент $\alpha \in U_n^i$ и запишем его в виде $\alpha = 1 + \pi^i\beta$, где $\beta \in O_n$. Отобразим $\alpha \mapsto \bar{\beta}$. Мы должны показать, что при таком отображении произведению $\alpha\alpha'$ соответствует сумма $\bar{\beta} + \bar{\beta}'$. По определению $\alpha\alpha' = 1 + \pi^i(\beta + \beta') + \ldots$, следовательно, $\alpha\alpha' \mapsto \bar{\beta} + \bar{\beta}'$.

Наконец, эти изоморфизмы являются изоморфизмами Галуа, так как ${}^s\alpha = 1 + \pi^i \cdot {}^s\beta$.

Лемма 1.2. *Для всех целых чисел* q *и всех целых чисел* $i \geqslant 0$ *имеет место равенство* $H^q(G, U_n^i/U_n^{i+1}) = 0$.

Доказательство. Для $i = 0$ мы имеем $U_n^0 = U_n$, и первая часть леммы 1.1 дает

$$H^q(G, U_n/U_n^1) = H^q(G, k_n^*) = H^q(G_{k_n/k}, k_n^*).$$

Далее, при $q = 1$ в силу «теоремы Гильберта 90» (см. гл. V, п. 2.7) $H^1(G_{k_n}/_k, k_n^*) = 0$. В случае $q = 2$ вспомним, что группа G циклична; поскольку группа k_n^* конечна, индекс Эрбрана $h(k_n^*)$ равен 1 гл. IV, предложение 8.2). Отсюда получаем требуемое для $q = 2$. Для остальных q результат следует из периодичности.

Для $i \geqslant 1$ доказываемая лемма следует из леммы 1.1 и того факта, что группа k_n^+ имеет тривиальные когомологии.

Доказательство теоремы 1.2 будет завершено, если мы сможем перейти от групп U_n^i/U_n^{i+1} к самой группе U_n, и сделать это нам поможет следующая

Лемма 1.3. *Пусть* G *— конечная группа и* M *— некоторый* G*-модуль. Пусть* M^i $(i \geqslant 0, M^0 = M)$ *— убывающая последовательность* G*-подмодулей, и пусть* $\bar{M} = \varprojlim M/M^i$ *(точнее, предположим, что отображение из* M *в предел биективно). Тогда если при некотором* $q \in \mathbf{Z}$ *при всех* i *имеет место* $H^q(G, M^i/M^{i+1}) = 0$, *то справедливо равенство* $H^q(G, \bar{M}) = 0$.

Доказательство. Пусть f — какой-то q-коцикл со значениями в $\bar{M}$. Так как $H^q(G, \bar{M}/M^1) = 0$, то существует $(q-1)$-коцепь ψ_1 на группе G со значениями в модуле $\bar{M}$, такая, что $f = \delta\psi_1 + f_1$ при некотором q-коцикле f_1 со значениями в M^1. Аналогично существует такая коцепь ψ_2, что $f_1 = \delta\psi_2 + f_2$ при некотором коцикле f_2 со значениями в M^2 и т. д. Построим таким способом последовательность пар (ψ_n, f_n), где ψ_n — некоторая $(q-1)$-коцепь со значениями в модуле M^{n-1} и f_n — некоторый q-коцикл со значениями в модуле M^n, причем $f_n = \delta \cdot \psi_{n+1} + f_{n+1}$. Положим $\psi = \psi_1 + \psi_2 + \ldots$. В силу сделанных предположений о модуле $\bar{M}$ этот ряд сходится и определяет некоторую $(q-1)$-коцепь на группе G со значениями в модуле $\bar{M}$. Суммируя равенства $f_n = \delta\psi_{n+1} + f_{n+1}$, мы получаем, что $f = \delta\psi$, а это доказывает лемму.

Вернемся теперь к доказательству предложения 1.1. Возьмем в качестве модуля M из леммы 1.3 группу U_n. Из лемм 1.3 и 1.2 следует, что когомологии группы U_n тривиальны, что и доказывает предложение 1.1 и теорему 1.2.

1.3. Некоторые диаграммы

Предложение 1.2. *Пусть L/K — конечное расширение степени n, и пусть L_{nr} (соответственно K_{nr}) — максимальное неразветвленное расширение поля L (соответственно поля K); таким образом, $K_{\mathrm{nr}} \subset L_{\mathrm{nr}}$. Тогда коммутативна следующая диаграмма:*

$$\begin{array}{ccc} H^2(K_{\mathrm{nr}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L_{\mathrm{nr}}/L) \\ {\scriptstyle \mathrm{inv}_K}\downarrow & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbf{Q}/\mathbf{Z} & \xrightarrow{n} & \mathbf{Q}/\mathbf{Z} \end{array}$$

Доказательство. Пусть $\Gamma_K = G(K_{\mathrm{nr}}/K)$, и пусть F_K — элемент Фробениуса из группы Γ_K; аналогичным образом определим Γ_L и F_L. Имеем: $F_L = (F_K)^f$, где $f = [l : k]$ — степень классов вычетов расширения L/K.

Обозначим через e индекс ветвления расширения L/K и рассмотрим следующую диаграмму:

$$\begin{array}{ccccccc} H^2(\Gamma_K, K_{\mathrm{nr}}^*) & \xrightarrow{v_K} & H^2(\Gamma_K, \mathbf{Z}) & \xrightarrow{\delta^{-1}} & \mathrm{Hom}(\Gamma_K, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\gamma_K} & \mathbf{Q}/\mathbf{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & (1) & {\scriptstyle e\cdot\mathrm{Res}}\downarrow & (2) & {\scriptstyle e\cdot\mathrm{Res}}\downarrow & (3) & {\scriptstyle n}\downarrow \\ H^2(\Gamma_L, L_{\mathrm{nr}}^*) & \xrightarrow{v_L} & H^2(\Gamma_L, \mathbf{Z}) & \xrightarrow{\delta^{-1}} & \mathrm{Hom}(\Gamma_L, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\gamma_L} & \mathbf{Q}/\mathbf{Z} \end{array}$$

в которой гомоморфизм Res индуцируется включением $\Gamma_L \to \Gamma_K$, а гомоморфизм γ_K (соответственно γ_L) задается посредством $\varphi \mapsto \varphi(F_K)$ (соответственно $\varphi \mapsto \varphi(F_L)$). Три квадрата (1), (2) и (3), выделенные в этой диаграмме, *коммутативны*; для квадрата (1) это следует из того, что гомоморфизм v_L на группе K_{nr}^* равен произведению $e \cdot v_K$; для квадрата (3) коммутативность следует из того, что $F_L = F_K^f$ и $n = ef$; коммутативность квадрата (2) очевидна.

С другой стороны, определение гомоморфизма inv_K: $H^2(\Gamma_K, K_{\mathrm{nr}}^*) \to \mathbf{Q}/\mathbf{Z}$ эквивалентно заданию композиции

$$\mathrm{inv}_K = \gamma_K \circ \delta^{-1} \circ v_K$$

и аналогично

$$\mathrm{inv}_L = \gamma_L \circ \delta^{-1} \circ v_L.$$

Предложение 1.2 теперь доказано.

Следствие 1. *Пусть $H^2(L/K)_{\mathrm{nr}}$ — подгруппа в группе $H^2(K_{\mathrm{nr}}/K)$, состоящая из тех элементов $\alpha \in H^2(K_{\mathrm{nr}}/K)$, которые «распадаются над полем L» (т. е. равны нулю в группе $\mathrm{Br}(L)$). Тогда группа $H^2(L/K)_{\mathrm{nr}}$ циклична, имеет порядок n и порождается элементом $u_{L/K}$ из группы $H^2(K_{\mathrm{nr}}/K)$, для которого $\mathrm{inv}_K(u_{L/K}) = 1/n$.*

Доказательство. Заметим, что более просто группа $H^2(L/K)_{\mathrm{nr}}$ может быть определена следующим образом: $H^2(L/K)_{\mathrm{nr}} = H^2(L/K) \cap H^2(K_{\mathrm{nr}}/K)$.

Рассмотрим точную последовательность

$$0 \to H^2(L/K)_{\mathrm{nr}} \to H^2(K_{\mathrm{nr}}/K) \xrightarrow{\mathrm{Res}} H^2(L_{\mathrm{nr}}/L).$$

Ядром отображения $H^2(K_{\mathrm{nr}}/K) \to H^2(L_{\mathrm{nr}}/L)$ является группа $H^2(L/K)_{\mathrm{nr}}$, которая отображается в нуль при inv_L: $H^2(L_{\mathrm{nr}}/L) \to \mathbf{Q}/\mathbf{Z}$. С другой стороны, из предложения 1.2 следует, что $\mathrm{inv}_L \circ \mathrm{Res} = n \cdot \mathrm{inv}_K$. Ядро последнего отображения есть $(1/n)\mathbf{Z}/\mathbf{Z}$, и потому группа $H^2(L/K)_{\mathrm{nr}}$ циклична, имеет порядок n и порождается элементом $u_{L/K} \in H^2(K_{\mathrm{nr}}/K)$, для которого $\mathrm{inv}_K(u_{L/K}) = 1/n$.

Следствие 2. *Порядок группы $H^2(L/K)$ кратен числу n.*

Доказательство. Группа $H^2(L/K)$, согласно следствию 1, содержит циклическую подгруппу порядка n.

1.4. Построение подгруппы с тривиальными когомологиями

Пусть L/K — конечное расширение Галуа с группой Галуа G, где L и K — локальные поля. Согласно рассуждениям, которые проводились в связи с доказательством пред-

ложения 1.1, G-модуль U_L имеет тривиальные когомологии, когда расширение L не разветвлено.

Предложение 1.3. *В группе U_L существует открытая подгруппа V, когомологии которой тривиальны, т. е. $H^q(G, V) = 0$ при всех q.*

Доказательство. Мы дадим два доказательства: первое проходит лишь в случае характеристики 0; второе носит совершенно общий характер.

Способ 1. Идея заключается в сравнении аддитивной и мультипликативной групп поля L. Мы знаем, что L^+ представляет собой свободный модуль над алгеброй $K[G]$. Это означает, что существует элемент $\alpha \in L$, для которого $[{}^s\alpha]_{s\in G}$ является базисом векторного пространства L над полем K.

Возьмем теперь кольцо O_K целых элементов поля K и положим $A = \sum_{s\in G} O_K \cdot {}^s\alpha$. Этот модуль свободен над группой G и имеет тривиальные когомологии. Более того, умножая α на достаточно высокую степень локальной униформизирующей π_K, мы можем взять модуль A такого типа в любой заданной окрестности нуля.

Все сказанное есть следствие теории Ли, согласно которой аддитивная группа поля L локально изоморфна его мультипликативной группе. Точнее степенной ряд $e^x = \sum_{n=0}^{\infty} x^n/n!$ сходится при $v(x) > v(p)/(p-1)$, и, таким образом, в окрестности $v(x) > v(p)/(p-1)$ нуля группа L^+ локально изоморфна группе L^* относительно отображения $x \mapsto e^x$. (Отметим, что в этой окрестности обратное отображение задается так: $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$.)

Пусть $V = e^A$; ясно, что когомологии модуля V тривиальны.

Вышеприведенные аргументы не проходят в случае характеристики p, а именно в том месте, где речь идет о локальном изоморфизме групп L^+ и L^*.

Способ 2. Начнем с модуля A, построенного выше: $A = \sum_{s\in G} O_K \cdot {}^s\alpha$. Можно считать, что $A \subset O_L$. Так как множество A открыто в O_L, то при некотором N $\pi_K^N O_L \subset A$. Положим $M = \pi_K^i A$. Тогда $M \cdot M \subset \pi_K M$ при $i \geqslant N+1$. Так как $M \cdot M = \pi_K^{2i} A \cdot A \subset \pi_K^{2i} O_L$, то при $i \geqslant N+1$

$$\pi_K^{2i} O_L \subset \pi_K \cdot \pi_K^i A \subset \pi_K M.$$

Пусть теперь $V = 1 + M$. Тогда V является открытой подгруппой в группе U_L. Остается доказать, что когомологии модуля V тривиальны. Определим фильтрацию модуля V с помощью подгрупп $V^i = 1 + \pi_K^i M$, $i \geqslant 0$. (Отметим, что V^i является подгруппой, так как $(1+\pi_K^i x)(1+\pi_K^i y) = 1 + \pi_K^i (x + y + \pi_K^i xy)$ и т. д.) Получается убывающая фильтрация $V = V^0 \supset V^1 \supset V^2 \supset \dots$. Подобно тому как в лемме 1.2, мы подошли теперь к тому, чтобы доказать, что $H^q(G, V^i/V^{i+1}) = 0$ для всех q. Возьмем $x = 1 + \pi_K^i \beta$, $\beta \in M$, и сопоставим этому элементу его образ $\overline{\beta} \in M/\pi_K M$. Такое сопоставление определяет изоморфизм групп V^i/V^{i+1} и $M/\pi_K M$, а мы знаем, что последняя имеет тривиальные когомологии, так как является свободной над группой G.

Это завершает доказательство предложения 1.3.

Напомним определение индекса Эрбрана $h(M)$. Именно, $h(M) = \mathrm{Card}(\hat{H}^0(M))/\mathrm{Card}(H^1(M))$ при условии, что выражения в обеих частях конечны (см. гл. IV, § 8).

Следствие 1. *Пусть L/K — циклическое расширение степени n. Тогда $h(U_L) = 1$ и $h(L^*) = n$.*

Доказательство. Пусть V — открытая подгруппа группы U_L с тривиальными когомологиями (см. предложение 1.3). Так как функция h мультипликативна, то $h(U_L) = h(V) \cdot h(U_L/V) = 1$.

Аналогично $L^*/U_L \cong \mathbf{Z}$. Таким образом, $h(L^*) = h(\mathbf{Z}) \cdot h(U_L)$. Однако $h(U_L) = 1$ и $h(\mathbf{Z}) = n$, поскольку $\hat{H}^0(G, \mathbf{Z}) = n$ и $H^1(G, \mathbf{Z})$ — тривиальная группа. Следовательно, $h(L^*) = n$.

Следствие 2. *Пусть L/K — циклическое расширение степени n. Тогда группа $H^2(L/K)$ имеет порядок $n = [L : K]$.*

Доказательство. Имеем:

$$h(L^*) = \frac{\mathrm{Card}\,(H^2(G, L^*))}{\mathrm{Card}\,(H^1(G, L^*))}.$$

Следствие 1 показывает, что $h(L^*) = n$. Более того, $H^1(G, L^*) = 0$ («теорема Гильберта 90»). Следовательно, $\mathrm{Card}\,(H^2(G, L^*)) = n$. Но $H^2(G, L^*)$ и $H^2(L/K)$ — одна и та же группа. Отсюда следует результат.

1.5. Одна неприятная лемма

Лемма 1.4. *Пусть G — конечная группа и M — некоторый G-модуль. Предположим, что $\rho \geqslant 0$, $q \geqslant 0$ — целые числа. Пусть, далее,*

(а) *$H^i(H, M)$ для любых $0 < i < q$ и любых подгрупп $H \subset G$;*

(б) *если $H \subset K \subset G$ и H — нормальный делитель в K, для которого группа K/H циклична и имеет порядок, равный простому числу, то порядок группы $H^q(H, M)$ (соответственно группы $\hat{H}^0(H, M)$ при $q = 0$) делит $[K : H]^\rho$.*

Тогда группа $H^q(G, M)$ (соответственно группа $\hat{H}^0(G, M)$) имеет порядок, делящий число $[G : 1]^\rho$.

Доказательство. Так как отображение ограничения $\mathrm{Res}\colon \hat{H}^1(G, M) \to \hat{H}^1(G_p, M)$ инъективно на p-примарных компонентах групп $\hat{H}^1(G, M)$, где G_p — силовская p-подгруппа группы G, то мы можем сосредоточить внимание на случае, когда группа G является p-группой. В этом случае мы проведем доказательство леммы индукцией по порядку группы G.

Предположим, что группа G имеет порядок, больший чем 1. Зафиксируем некоторую подгруппу $H \subset G$, которая является нормальным делителем индекса p, и применим индуктивное предположение к группе G/H. Мы знаем из (б), что при $q > 0$ порядок группы $H^q(G/H, M^H)$ делит $[G : H]^\rho = p^\rho$, а по индуктивному предположению порядок группы $H^q(H, M)$ делит $[H : 1]^\rho$. Из (а) теперь следует, что имеет место точная последовательность (см. гл. IV, § 5)

$$0 \to H^q(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^q(G, M) \xrightarrow{\mathrm{Res}} H^q(H, M).$$

Таким образом, группа $H^q(G, M)$ имеет порядок, делящий $p^\rho \cdot [H : 1]^\rho = [G : 1]^\rho$.

Для $q = 0$ напомним (гл. IV, § 6), что

$$\hat{H}^0(G, M) = M^G/N_G M.$$

Кроме того, мы имеем точную последовательность

$$M^H/N_H M \xrightarrow{N_{G/H}} M^G/N_G M \to (M^H)^{G/H}/N_{G/H} M^H,$$

где $N_{G/H}$ обозначает норменное отображение, а второе отображение индуцировано тождественным. Оставшаяся часть доказательства проводится подобно предыдущей.

1.6. Окончание доказательств

Предложение 1.4. *Пусть L/K — конечное расширение Галуа с группой Галуа G порядка $n = [L : K]$. Тогда $H^2(L/K)$ — циклическая группа порядка n, имеющая такую образующую $u_{L/K} \in H^2(K_{\mathrm{nr}}/K)$, что $\mathrm{inv}_K(u_{L/K}) = 1/n$.*

Доказательство. В лемме 1.4 положим $M = L^*$, $\rho = 1$ и $q = 2$. Условие (а) выполняется в силу «теоремы Гильберта 90», а условие (б) — в силу следствия 2 из предложения 1.3. Следовательно, группа $H^2(G, L^*)$ имеет порядок, делящий $[G : 1] = n$. Но в силу следствия 1 из предложения 1.2 группа $H^2(L/K)$ содержит некоторую циклическую подгруппу порядка n, порожденную элементом $u_{L/K} \in H^2(K_{\mathrm{nr}}/K)$ и такую, что $\mathrm{inv}_K(u_{L/K}) = 1/n$. Отсюда вытекает справедливость предложения 1.4.

Из этого предложения следует, что группа $H^2(L/K)$ содержится в группе $H^2(K_{\mathrm{nr}}/K)$.

Вернемся теперь к доказательству теоремы 1.1. Она утверждает, что включение $\mathrm{Br}(K) \supset H^2(K_{\mathrm{nr}}/K)$ является в действительности равенством. Отметим, что по определению $\mathrm{Br}(K) = \bigcup H^2(L/K)$, где L пробегает множество конечных расширений Галуа поля K. Но, как было замечено выше, $H^2(L/K) \subset H^2(K_{\mathrm{nr}}/K)$ и потому $\mathrm{Br}(K) \subset H^2(K_{\mathrm{nr}}/K)$, что и требовалось доказать.

Очевидно, что теорема 1.3 следует из теоремы 1.1 и предложения 1.2.

1.7. Один вспомогательный результат

Мы уже доказали все утверждения из п. 1.1 и эту главу закончим результатом, который найдет приложение к глобальным полям.

Пусть A — абелева группа и n — целое число $\geqslant 1$. Рассмотрим циклическую группу $\mathbf{Z}/n\mathbf{Z}$, тривиально действующую на модуль A. Обозначая соответствующий индекс Эрбрана через $h_n(A)$, если только он определен, имеем

$$h_n(A) = \frac{\text{порядок } (A/nA)}{\text{порядок } ({}_nA)},$$

где ${}_nA$ — множество таких $\alpha \in A$, что $n\alpha = 0$. В противном случае мы могли бы начать с отображения $A \xrightarrow{n} A$ и взять $h_n(A)$ равным

$$\text{порядок (coker } (n))/\text{порядок (ker } (n)).$$

Пусть теперь K — локальное поле. Тогда для $\alpha \in K$ существует нормализованное нормирование $|\alpha|_K$ (см. гл. II, § 11). Если $\alpha \in O_K$, то $|\alpha|_K = 1/\mathrm{Card}\,(O_K/\alpha O_K)$.

Предложение 1.5. *Пусть K — локальное поле и $n \geqslant 1$ — целое число, взаимно простое с характеристикой поля K. Тогда $h_n(K^*) = n/|n|_K$.*

Доказательство. Предположим, что поле K имеет характеристику 0. Имеем: $h_n(K^*) = h_n(\mathbf{Z}) \cdot h_n(U_K)$; кроме того, $h_n(\mathbf{Z}) = n$. Мы должны вычислить $h_n(U_K)$. Как и в предложении 1.3, мы рассмотрим подгруппу $V \subset U$, являющуюся открытой и изоморфной аддитивной группе кольца O_K. Имеем: $h_n(U_K) = h_n(V) \cdot h_n(U_K/V)$ и, так как U_K/V — конечная группа, $h_n(U_K/V) = 1$. Далее,

$$h_n(V) = h_n(O_K)$$

и

$$h_n(O_K) = \mathrm{Card}\,(O_K/nO_K) = 1/|n|_K.$$

Отсюда

$$h_n(K^*) = n \cdot (1/|n|_K) = n/|n|_K.$$

Предположим теперь, что поле K имеет характеристику p. Проделаем те же шаги, что и выше. Прежде всего,

$h_n(K^*) = n \cdot h_n(U_K)$. Рассмотрим точную последовательность

$$0 \to U_K^1 \to U_K \to k^* \to 0,$$

где U_K^1 — про-p-группа (см. лемму 1.1). Так как n не делится на p, то $h_n(U_K^1) = 1$ и $h_n(k^*) = 1$. Таким образом, $n \cdot h_n(U_K) = n$. Отсюда следует требуемый результат.

Отметим, что утверждение этого предложения выполняется также и в полях $\mathbf{R}$ *и* $\mathbf{C}$. В этих случаях мы имеем: $|n|_{\mathbf{R}} = |n|$, $|n|_{\mathbf{C}} = |n|^2$ и можно непосредственно проверить, что для $\mathbf{R}$

$$h_n(\mathbf{R}^*) = n/|n| = 1$$

и для $\mathbf{C}$

$$h_n(\mathbf{C}^*) = n/|n|_{\mathbf{C}} = 1/n.$$

Добавление. Алгебры с делением над локальным полем

Известно, что элементы группы Брауэра находятся в некоторой связи с телами (см., например, [4]); мы собираемся воспользоваться этой связью для описания тел и их инвариантов. Большинство результатов будет дано без доказательств.

Пусть K — локальное поле, D — алгебра с делением над K с центром, равным K, и $[D : K] = n^2$. Нормирование v поля K единственным способом продолжается с поля K на алгебру D (например, с помощью продолжения v сначала на $K(\alpha)$, $\alpha \in D$, а затем — согласования всех таких продолжений). Область D полна относительно этого нормирования, и в очевидных обозначениях кольцо O_D имеет степень n^2 над O_K. Пусть d — поле вычетов алгебры D; тогда $n^2 = ef$, где e — индекс ветвления и $f = [d : k]$.

Отметим теперь, что $e \leqslant n$, так как существует такой элемент $\alpha \in D$, что $v_D(\alpha) = e^{-1}$, и α принадлежит некоторому коммутативному подтелу, имеющему над K степень не большую, чем n. Тело вычетов d коммутативно, поскольку k — конечное поле и $d = k(\bar{\alpha})$ при некотором $\alpha \in D$. Следовательно, $f \leqslant n$. Учитывая то, что $n^2 = ef$, мы получаем, что неравенства $e \leqslant n$ и $f \leqslant n$ должны давать $e = n$ и $f = n$.

Так как $[d : k] = n$, то можно найти такое $\bar{\alpha} \in d$, что $k(\bar{\alpha}) = d$. Выберем теперь соответствующее $\alpha \in O_D$, и пусть

$L = K(\alpha)$. Очевидно, что $[L : K] \leqslant n$, так как тело L — коммутативное подтело алгебры D. С другой стороны, элемент $\bar{\alpha}$ принадлежит полю вычетов l поля L, и $l = d$; следовательно, $[l : k] = n$. Отсюда получается, что $[L : K] = n$ и расширение L — неразветвленное. Этот последний вывод мы сформулируем так: *алгебра D содержит максимальное коммутативное подтело L, неразветвленное над центром K.*

Элемент $\delta \in \mathrm{Br}(K)$, соответствующий алгебре D, распадается над полем L, т. е. $\delta \in H^2(L/K)$. Таким образом, любой элемент из группы $\mathrm{Br}(K)$ распадается над некоторым неразветвленным расширением, и мы получили новое доказательство теоремы 1.1.

Описание инварианта

Расширение L поля K, построенное выше, не единственно; однако теорема Сколема — Нётер (см. [2], гл. VIII, § 10) показывает, что все такие расширения сопряжены. Эта же теорема утверждает, что любой автоморфизм расширения L индуцируется некоторым внутренним автоморфизмом алгебры D. Следовательно, существует такой элемент $\gamma \in D$, что $\gamma L \gamma^{-1} = L$, и внутренний автоморфизм $x \mapsto \gamma x \gamma^{-1}$, ограниченный на поле L, является автоморфизмом Фробениуса F. Более того, элемент γ определен однозначно с точностью до множителя из группы L^*.

Пусть v_L: $L^* \to \mathbf{Z}$ — нормирование поля L; таким образом, $v_D : D^* \to (1/n)\,\mathbf{Z}$ продолжает v_L на тело D. Образ $i(D$ элемента $v_D(\gamma)$ в группе $(1/n)\,\mathbf{Z}/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$ не зависит от выбора элемента γ. Можно доказать, что $i(D) = \mathrm{inv}_K(\delta)$, где $\delta \in \mathrm{Br}(K)$ — элемент, ассоциированный с D.

Мы можем сформулировать определение элемента $i(D)$ несколько иначе. Отображение $x \mapsto \gamma^n x \gamma^{-n}$ равно F^n на поле L и, таким образом, тождественно. Следовательно, γ^n коммутирует с элементами из поля L и $\gamma^n = c \in L^*$. Теперь имеем:

$$v_D(\gamma) = \frac{1}{n} v_D(\gamma^n) = \frac{1}{n} v_D(c) = \frac{1}{n} v_L(c).$$

Следовательно, $v_D(\gamma) = (1/n)\, v_L(c) = i/n$, где $c = \pi_L^i u$.

Приложение

Предположим, что расширение K'/K имеет степень n. В силу следствия 2 из теоремы 1.3 некоторый элемент $\delta \in \mathrm{Br}(K)$ распадается над полем K'. Следовательно, *любое расширение K'/K степени n может быть вложено в D в качестве максимального коммутативного подтела.* Это может быть сформулировано более эффективным образом: любое неприводимое уравнение степени n над полем K может быть решено в D.

Упражнение

Рассмотрим 2-адическое поле $\mathbf{Q}_2$; пусть H — тело кватернионов над полем $\mathbf{Q}_2$. Доказать, что кольцо целых элементов тела H состоит из кватернионов вида $a + bi + cj + dk$, где $a, b, c, d \in \mathbf{Z}_2$ или $a, b, c, d \equiv \frac{1}{2} (\mathrm{mod}\ \mathbf{Z}_2)$. Перечислить семь (с точностью до сопряженности) квадратичных подтел тела H.

§ 2. АБЕЛЕВЫ РАСШИРЕНИЯ ЛОКАЛЬНЫХ ПОЛЕЙ

2.1. Когомологические свойства

Пусть L/K — конечное расширение Галуа локальных полей с группой Галуа $G = G(L/K)$ порядка n. Мы уже видели (следствие 2 из теоремы 1.3), что группа $H^2(L/K) = H^2(G, L^*)$ циклична, имеет порядок n и имеет такую образующую $u_{L/K}$, что $\mathrm{inv}_K(u_{L/K}) = \frac{1}{n} \in \mathbf{Q}/\mathbf{Z}$. С другой стороны, мы знаем, что $H^1(G, L^*) = 0$.

Пусть теперь H — некоторая подгруппа порядка m в группе G. Так как H является группой Галуа расширения L/K' при некотором $K' \supset K$, то, кроме того, мы имеем: $H^1(H, L^*) = 0$ и $H^2(H, L^*)$ — циклическая группа порядка m, порожденная элементом $u_{L/K'}$.

Для дальнейшего нам необходимо выяснить некоторые свойства образующей $u_{L/K'}$. Мы имеем отображение ограничения $\mathrm{Res}: \mathrm{Br}(K) \to \mathrm{Br}(K')$ и при этом $u_{L/K'} = \mathrm{Res}(u_{L/K})$. Чтобы в этом убедиться, проведем легкое вычисление

с инвариантами:

$$\mathrm{inv}_{K'}(\mathrm{Res}\, u_{L/K}) = [K' : K]\,\mathrm{inv}_K(u_{L/K}) = [K' : K]\cdot\frac{1}{n} = \frac{1}{m} = \mathrm{inv}_{K'}(u_{L/K'}).$$

Воспользовавшись теперь теоремой Тэйта (гл. IV, § 10), мы получаем следующий результат.

Теорема 2.1. *Для всех $q \in \mathbf{Z}$ отображение $\alpha \longmapsto \alpha \cdot u_{L/K}$, заданное $\cup$-умножением, является изоморфизмом группы $\hat{H}^q(G, \mathbf{Z})$ на группу $\hat{H}^{q+2}(G, L^*)$.*

Аналогичное утверждение может быть сформулировано для подгруппы H группы G, соответствующей некоторому расширению L/K'. Отображения Res и Cor связывают эти два изоморфизма, и мы получаем более явную формулировку в терминах диаграмм.

Утверждение. *Диаграммы*

$$\begin{array}{ccc} \hat{H}^q(G, \mathbf{Z}) & \xrightarrow{u_{L/K}} & \hat{H}^{q+2}(G, L^*) \\ \mathrm{Res}\downarrow & & \mathrm{Res}\downarrow \\ \hat{H}^q(H, \mathbf{Z}) & \xrightarrow{u_{L/K'}} & \hat{H}^{q+2}(H, L^*) \end{array} \qquad \text{и} \qquad \begin{array}{ccc} \hat{H}^q(G, \mathbf{Z}) & \xrightarrow{u_{L/K}} & \hat{H}^{q+2}(G, L^*) \\ \mathrm{Cor}\uparrow & & \mathrm{Cor}\uparrow \\ \hat{H}^q(H, \mathbf{Z}) & \xrightarrow{u_{L/K'}} & \hat{H}^{q+2}(H, L^*) \end{array}$$

коммутативны.

Доказательство. Как и выше, $u_{L/K'} = \mathrm{Res}(u_{L/K})$. Надо показать, что

$$\mathrm{Res}_{K/K'}(u_{L/K}\cdot\alpha) = u_{L/K'}\cdot\mathrm{Res}_{K/K'}(\alpha).$$

Левая часть равенства равна $\mathrm{Res}_{K/K'}(u_{L/K})\,\mathrm{Res}_{K/K'}(\alpha)$ (см. [5], гл. XII, стр. 311), и, таким образом, коммутативность диаграммы с отображением Res установлена.

Что касается второй диаграммы, то там надо показать, что $\mathrm{Cor}(u_{L/K'}\cdot\beta) = u_{L/K}\cdot\mathrm{Cor}(\beta)$. Имеем: $\mathrm{Cor}(u_{L/K'}\cdot\beta) = \mathrm{Cor}(\mathrm{Res}(u_{L/K})\cdot\beta) = u_{L/K}\cdot\mathrm{Cor}(\beta)$ ([5], гл. XII, стр. 311), а это и доказывает коммутативность второй диаграммы.

2.2. Отображение взаимности

Случай, который мы будем рассматривать, получается из рассмотренного выше при $q = -2$. По определению группа $\hat{H}^{-2}(G, \mathbf{Z})$ равна группе $H_1(G, \mathbf{Z})$, и мы знаем, что $H_1(G, \mathbf{Z}) = G/G' = G^{\mathrm{ab}}$. С другой стороны, $\hat{H}^0(L/K) = K^*/N_{L/K}L^*$, где $N_{L/K}$ — норменное отображение. В этом случае теорема 2.1 звучит так:

Теорема 2.2. *$\cup$-умножение на $u_{L/K}$ определяет некоторый изоморфизм группы $G^{\mathrm{ab}}(L/K)$ на группу $K^*/N_{L/K}L^*$.*

Мы дадим определенное название только что построенному изоморфизму, а точнее — изоморфизму, обратному к нему. Определим $\theta = \theta_{L/K}$ как изоморфизм группы $K^*/N_{L/K}L^*$ на группу G^{ab}, который является обращением $\cup$-умножения на $u_{L/K}$. Отображение θ называется *локальным отображением взаимности*, или *символом норменного вычета*.

Если $\alpha \in K^*$ соответствует элементу $\bar{\alpha} \in K^*/N_{L/K}L^*$, то будем писать $\theta_{L/K}(\bar{\alpha}) = (\alpha, L/K)$. Название «символ норменного вычета» связано с тем обстоятельством, что этот символ показывает, является ли элемент $\alpha \in K^*$ нормой из L^* или нет. Именно $(\alpha, L/K) = 0$ (напоминаем, что 0 означает 1!) тогда и только тогда, когда α является нормой из L^*.

Отметим, что если L/K — абелево расширение, то $G^{\mathrm{ab}} = G$ и мы имеем изоморфизм θ: $K^*/N_{L/K}L^* \to G$.

2.3. Описание символа $(\alpha, L/K)$ с помощью характеров

Пусть L/K — расширение Галуа с группой G. Начнем с элемента $\alpha \in K^*$ и охарактеризуем символ $(\alpha, L/K) \in G^{\mathrm{ab}}$. Для простоты записи положим $s_\alpha = (\alpha, L/K)$. Пусть $\chi \in \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) \cong H^2(G, \mathbf{Z})$ — некоторый характер степени 1 группы G, и пусть $\delta\chi \in H^2(G, \mathbf{Z})$ — образ характера χ относительно когранничного отображения δ: $H^1(G, \mathbf{Q}/\mathbf{Z}) \to H^2(G, \mathbf{Z})$ (см. п. 1.1). Пусть

$$\bar{\alpha} \in K^*/N_{L/K}(L^*) = \hat{H}^0(G, L^*)$$

— образ элемента α. Тогда $\cup$-произведение $\bar{\alpha}\cdot\delta\chi$ является элементом группы $H^2(G, L^*) \subset \mathrm{Br}(K)$.

Предложение 2.1. *В вышеприведенных обозначениях имеет место следующая формула:*

$$\chi(s_\alpha) = \mathrm{inv}_K(\bar{\alpha}\cdot\delta\chi).$$

Доказательство. По определению $s_\alpha \cdot u_{L/K} = \bar{\alpha} \in \hat{H}^0(G, L^*)$, где s_α отождествляется с некоторым элементом из группы $H^{-2}(G, \mathbf{Z})$. Используя ассоциативность $\cup$-умножения, получаем $\bar{\alpha}\cdot\delta\chi = u_{L/K}\cdot s_\alpha\cdot\delta\chi = u_{L/K}(s_\alpha\cdot\delta\chi) = u_{L/K}\cdot\delta(s_\alpha\cdot\chi)$, где $s_\alpha\cdot\chi \in \hat{H}^{-1}(G, \mathbf{Q}/\mathbf{Z})$. Далее, $\hat{H}^{-1}(G, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\delta} \hat{H}^0(G, \mathbf{Z}) = \mathbf{Z}/n\mathbf{Z}$, и мы отождествим группу $\hat{H}^{-1}(G, \mathbf{Q}/\mathbf{Z})$ с группой $\mathbf{Z}/n\mathbf{Z}$. Более того, отождествление групп $H^{-2}(G, \mathbf{Z})$ и G^{ab} осуществляется таким образом, что гарантировано равенство $s_\alpha\cdot\chi = \chi(s_\alpha)$ (см. [8], гл. XI, стр. 184—186). Положим $s_\alpha\cdot\chi = r/n$, $r \in \mathbf{Z}$. Тогда $\delta(r/n) \in \hat{H}^0(G, \mathbf{Z})$ и $\delta(r/n) = r$. Следовательно, $u_{L/K}\cdot(s\cdot\delta\chi) = r\cdot u_{L/K}$, и инвариант этого класса когомологий как раз равен $r/n = \chi(s_\alpha)$. Предложение 2.1 доказано.

В качестве приложения остановимся на следующем вопросе. Рассмотрим башню расширений Галуа $K \subset L' \subset L$, где $G = G(L/K)$ и $H = G(L/L')$. Пусть χ' — характер группы $(G/H)^{\mathrm{ab}}$ и χ — соответствующий характер группы G^{ab}; тогда если $\alpha \in K^*$ индуцирует элемент $s_\alpha \in G^{\mathrm{ab}}$ и элемент $s'_\alpha \in (G/H)^{\mathrm{ab}}$ относительно отображения $s_\alpha \longmapsto s'_\alpha$, то $\chi(s_\alpha) = \chi'(s'_\alpha)$. Это следует из предложения 2.1 и того факта, что отображение инфляции переводит характер χ' (соответственно элемент $\delta\chi'$) в характер χ (соответственно в элемент $\delta\chi$).

Эта согласованность позволяет определить символ s_α для любого абелева расширения; в частности, полагая $L = K^{\mathrm{ab}}$, где K^{ab} — максимальное абелево расширение поля K, мы получаем некоторый гомоморфизм θ_K: $K^* \to G(K^{\mathrm{ab}}/K)$, определенный отображением $\alpha \longmapsto (\alpha, K^{\mathrm{ab}}/K)$.

2.4. Изменение подполей данного поля

Рассмотрев действие на символ $(\alpha, L/K)$ расширений поля L, мы обратимся к расширениям поля K. Пусть

K'/K — какое-то сепарабельное расширение, и пусть K^{ab}, K'^{ab} — максимальные абелевы расширения полей K и K' соответственно.

Рассмотрим сначала диаграммы из «утверждения» в п. 2.1, притом в случае, когда $q = -2$. Беря проективный предел соответствующих групп, мы получаем коммутативную диаграмму

$$\begin{array}{ccc} K^* & \xrightarrow{\theta_K} & G_K^{\mathrm{ab}} \\ {\scriptstyle \mathrm{incl}}\downarrow & & \downarrow{\scriptstyle V} \\ K'^* & \xrightarrow{\theta_{K'}} & G_{K'}^{\mathrm{ab}} \end{array}$$

Здесь символ V обозначает перенесение (см. гл. IV, § 6), $G_{K'}^{\mathrm{ab}}$ обозначает $G(K'^{\mathrm{ab}}/K)$ и G_K^{ab} обозначает группу $G(K^{\mathrm{ab}}/K) = G^{\mathrm{ab}}(K'^{\mathrm{ab}}/K)$.

Аналогично, используя вторую диаграмму упомянутого утверждения, мы получаем следующую коммутативную диаграмму:

$$\begin{array}{ccc} K'^* & \xrightarrow{\theta'_K} & G_{K'}^{\mathrm{ab}} \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle i} \\ K^* & \xrightarrow{\theta_K} & G_K^{\mathrm{ab}} \end{array}$$

где i индуцируется включением группы $G_{K'}$ в группу G_K.

(Заметим, что если K'/K не является сепарабельным расширением, то в первой из этих диаграмм перенесение V должно было бы быть заменено на qV, где q — множитель несепарабельности степени расширения K'/K. Вторая же диаграмма имеет место даже в несепарабельном случае.)

2.5. Неразветвленные расширения

В этом случае оказывается возможным вычислить символ нормменного вычета явно в терминах автоморфизма Фробениуса.

Предложение 2.2. *Пусть L/K — неразветвленное расширение степени n и $F \in G_{L/K}$ — элемент Фробениуса.*

Пусть $\alpha \in K^*$ *и* $v(\alpha) \in \mathbf{Z}$ *— нормализованное нормирование элемента* α. *Тогда* $(\alpha, L/K) = F^{v(\alpha)}$.

Доказательство. Пусть χ — некоторый элемент группы $\mathrm{Hom}(G_{L/K}, \mathbf{Q}/\mathbf{Z})$. Согласно предложению 2.1, имеет место равенство

$$\chi((\alpha, L/K)) = \mathrm{inv}_K(\bar{\alpha} \cdot \delta\chi).$$

Отображение inv_K: $H^2(G_{L/K}, L^*) \to \mathbf{Q}/\mathbf{Z}$ было определено как композиция следующих отображений:

$$H^2(G_{L/K}, L^*) \xrightarrow{v} H^2(G_{L/K}, \mathbf{Z}) \xrightarrow{\delta^{-1}} H^1(G_{L/K}, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\gamma} \mathbf{Q}/\mathbf{Z}.$$

Имеем: $v(\bar{\alpha} \cdot \delta\chi) = v(\alpha) \cdot \delta\chi$, откуда

$$\mathrm{inv}_K(\bar{\alpha} \cdot \delta\chi) = \gamma \circ \delta^{-1} \circ v(\bar{\alpha} \cdot \delta\chi) =$$
$$= v(\alpha) \cdot \gamma(\chi) = v(\alpha) \cdot \chi(F) = \chi(F^{v(\alpha)}).$$

Это показывает, что

$$\chi((\alpha, L/K)) = \chi(F^{v(\alpha)})$$

для произвольного характера χ группы $G_{L/K}$; поэтому $(\alpha, L/K) = F^{v(\alpha)}$.

Следствие. *Пусть* E/K *— некоторое конечное абелево расширение. Символ норменного вычета* $K^* \to G_{E/K}$ *отображает группу* U_K *на подгруппу инерции* $T \subset G_{E/K}$.

Доказательство. Пусть L — промежуточное расширение, соответствующее подгруппе T. В силу предложения 2.2 образ группы U_K в группе $G_{L/K}$ тривиален; это означает, что образ группы U_K в группе $G_{E/K}$ содержится в подгруппе T. Обратно, пусть $t \in T$ и $f = [L : K]$; существует такой элемент $a \in K^*$, что $t = (a, E/K)$. Так как $t \in T$, то предложение 2.2 показывает, что число f делит $v_K(a)$; следовательно, существует такой элемент $b \in E^*$, что $v_K(a) = v_K(Nb)$. Если положить $u = a \cdot Nb^{-1}$, то мы получим, что $u \in U_K$ и $(u, E/K) = (a, E/K) = t$.

2.6. Норменные подгруппы

Определение. *Подгруппа* $M \subset K^*$ *называется норменной, если существует такое конечное абелево расширение* L/K, *что* $M = N_{L/K}L^*$.

Пример. Пусть $m \geqslant 1$ — любое целое число и M_m — множество элементов $a \in K^*$, для которых $v_K(a) \equiv 0 \pmod{m}$; из предложения 2.2 (или из непосредственного вычисления норм) следует, что M_m — норменная подгруппа неразветвленного расширения степени m поля K.

Норменные подгруппы тесно связаны с отображением взаимности

$$\theta_K: K^* \to G_K^{\mathrm{ab}} = G(K^{\mathrm{ab}}/K),$$

определенным в п. 2.3. По построению отображение θ_K получается как проективный предел изоморфизмов $K^*/NL^* \to G_{L/K}$, где L пробегает все конечные абелевы расширения поля K. Если мы положим

$$\widetilde{K} = \varprojlim K^*/NL^*,$$

то увидим, что отображение θ_K может быть разложено в композицию

$$K^* \xrightarrow{i} \widetilde{K} \xrightarrow{\widetilde{\theta}} G_K^{\mathrm{ab}},$$

где i — естественное отображение, а $\widetilde{\theta}$ — некоторый *изоморфизм*. Заметим, что группа $\widetilde{K}$ является *пополнением* группы K^* в топологии, определенной норменными подгруппами.

Это показывает, что норменные подгруппы группы K^* и открытые подгруппы группы G_K^{ab} соответствуют друг другу взаимно однозначным образом: если $U \subset G_K^{\mathrm{ab}}$ — открытая подгруппа с неподвижным полем L, то ей сопоставляется норменная подгруппа $\theta_K^{-1}(U) = N_{L/K}L^*$; если $M \subset K^*$ — норменная подгруппа, то ей сопоставляется замыкание группы $\theta_K(M)$; соответствующее поле L_M является множеством тех элементов из K^{ab}, которые инвариантны относительно $\theta_K(a)$, $a \in M$. Мы, таким образом, получаем «соответствие Галуа» между норменными подгруппами и конечными абелевыми расширениями; сформулируем это в виде отдельного предложения.

Предложение 2.3. (a) *Отображение* $L \mapsto NL^*$ *является биективным отображением множества конечных абелевых расширений поля* K *на множество норменных подгрупп группы* K^*;

(б) *это биективное отображение обращает включения*;

(в) $N(L\cdot L')=NL\cap NL'$ *и* $N(L\cap L')=NL\cdot NL'$;

(г) *любая подгруппа группы* K^*, *содержащая некоторую норменную подгруппу, сама является норменной.*

(Прямое доказательство дано в [8], гл. XI, § 4.)

Неабелевы расширения задают те же норменные подгруппы, что и абелевы, как показывает

Предложение 2.4. *Пусть* E/K *— конечное расширение и* L/K *— наибольшее абелево расширение, содержащееся в поле* E. *Тогда*

$$N_{E/K}E^*=N_{L/K}L^*.$$

Доказательство. Это легко следует из свойств символа норменного вычета, установленных в п. 2.4; более подробное доказательство см. в [1], стр. 228—229, или в [8], стр. 180. (В обеих книгах рассматривается лишь случай сепарабельного расширения E/K; общий случай сводится к этому благодаря тому, что $NL=K$, если L — чисто несепарабельное расширение поля K.)

Следствие («лимитационная теорема»). *Индекс* $[K^*:NE^*]$ *делит степень* $[E:K]$ *и равен ей тогда и только тогда, когда расширение* E/K *абелево.*

Доказательство следует из того факта, что индекс подгруппы NL^* в группе K^* равен $[L:K]$.

2.7. Формулировка теоремы существования

Следующая теорема дает описание норменных подгрупп группы K^*:

Теорема 2.3. *Подгруппа* $M\subset K^*$ *является норменной тогда и только тогда, когда она удовлетворяет следующим двум условиям*:

(1) *индекс* $[K^*:M]$ *конечен*;

(2) *группа* M *открыта в группе* K^*.

(Отметим, что если выполняется условие (1), то условие (2) эквивалентно следующему: «группа M замкнута в группе K^*».)

Доказательство необходимости. Если $M=NL^*$, где L — конечное абелево расширение поля K, то группа K^*/M изоморфна группе Галуа $G_{L/K}$; следовательно, индекс $[K^*:M]$ конечен. Более того, непосредственно проверяется, что отображение $N\colon L^*\to K^*$ непрерывно и *собственно* (т. е. прообраз компакта относительно него есть компакт); следовательно, группа $M=NL^*$ замкнута (см. [3], гл. I, § 10). Как было замечено выше, это показывает то, что группа M открыта. (Это последнее свойство норменных подгрупп может быть также выражено тем, что отображение взаимности

$$\theta_K\colon K^*\to G_K^{ab}$$

непрерывно.)

Доказательство достаточности будет дано в п. 3.8, где оно выводится из теории Любина — Тэйта. Обычное же доказательство дано, например, в [8]; там оно основано на уравнениях Куммера и Артина — Шрейера.

Сейчас мы дадим несколько эквивалентных формулировок этой теоремы.

Рассмотрим отображение взаимности $\theta_K\colon K^*\to G_K^{ab}$. Согласно предложению 2.2, композиция отображений

$$K^*\xrightarrow{\theta_K}G_K^{ab}\to G(K_{nr}/K)=\hat{\mathbf{Z}}$$

равна отображению нормирования $v\colon K^*\to\mathbf{Z}$. Следовательно, мы имеем коммутативную диаграмму

$$\begin{array}{ccccccccc}
0 & \to & U_K & \to & K^* & \to & \mathbf{Z} & \to & 0\\
 & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\mathrm{id}} & & \\
0 & \to & I_K & \to & G_K^{ab} & \to & \hat{\mathbf{Z}} & \to & 0
\end{array}$$

где $I_K=G(K^{ab}/K_{nr})$ — *подгруппа инерции* группы G_K^{ab}, и группа $G(K_{nr}/K)$ отождествляется с группой $\hat{\mathbf{Z}}$.

Отображение $\theta\colon U_K\to I_K$ непрерывно, и его образ плотен в группе I_K (см. следствие из предложения 2.2); так как группа U_K компактна, то это отображение *сюръективно*.

Теперь мы можем сформулировать теорему существования двумя эквивалентными способами.

Теорема 2.3а. *Отображение* θ: $U_K \to I_K$ *является изоморфизмом.*

Теорема 2.3б. *Топология, индуцированная на группе* U_K *нормальными подгруппами, является топологией группы* U_K.

Группа I_K как раз равна $\varprojlim U_K/(M \cap U_K)$, где M пробегает все нормальные подгруппы группы K^*; эквивалентность теорем 2.3а и 2.3б следует отсюда почти сразу. Тот факт, что {теорема 2.3а} $\Rightarrow$ {теорема 2.3б}, очевиден; обратную импликацию легко установить с помощью предложения 2.2.

Следствие. *Точная последовательность* $0 \to U_K \to K^* \to \mathbf{Z} \to 0$ *при пополнении дает точную последовательность*

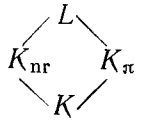
$$0 \to U_K \to \widetilde{K} \to \hat{\mathbf{Z}} \to 0.$$

Коротко говоря, это означает, что группа $\widetilde{K}$ получается из группы K^* «заменой группы $\mathbf{Z}$ на группу $\hat{\mathbf{Z}}$».

2.8. Описание символа $(\alpha, L/K)$

Пусть L — абелево расширение поля K, содержащее поле K_{nr} (максимальное неразветвленное расширение). Мы хотим описать отображение взаимности $\theta: K^* \to G_{L/K}$.

Так как $K_{\mathrm{nr}} \subset L$, то имеет место точная последовательность $0 \to H \to G_{L/K} \to \hat{\mathbf{Z}} \to 0$, где $H = G(L/K_{\mathrm{nr}})$ и $\hat{\mathbf{Z}}$ отождествляется с $G(K_{\mathrm{nr}}/K)$. Выберем какую-нибудь локальную униформизирующую $\pi \in K$ и положим $\sigma_\pi = \theta(\pi) = (\pi, L/K) \in G_{L/K}$. Известно, что элемент σ_π отображается на элемент Фробениуса $F \in G_{K_{\mathrm{nr}}/K}$. Более того, мы можем записать группу $G_{L/K}$ как прямое произведение подгрупп $G_{L/K} = H \cdot I_\pi$, где I_π — подгруппа, порожденная элементом σ_π. В соответствии с этим разложением мы получаем, что $L = K_{\mathrm{nr}} \otimes K_\pi$, где K_π — поле неподвижных элементов оператора $\sigma_\pi = \theta(\pi)$. В терминах диаграмм взаимосвязь между этими полями выражается так:



где расширения K_{nr} и K_π линейно разделены.

Предложение 2.5. *Пусть* f: $K^* \to G$ — *некоторый гомоморфизм; предположим, что*

(1) *композиция отображений* $K^* \xrightarrow{f} G \to G(K_{\mathrm{nr}}/K)$, *где* $G \to G(K_{\mathrm{nr}}/K)$ — *естественное отображение, является нормированием* v: $K^* \to \mathbf{Z}$;

(2) *для каждого униформизирующего элемента* $\pi \in K$ *элемент* $f(\pi)$ *является тождественным преобразованием на соответствующем расширении* K_π.

Тогда отображение f *является отображением взаимности.*

Доказательство. Заметим, что условие (1) может быть переформулировано так: для $\alpha \in K^*$ элемент $f(\alpha)$ индуцирует на расширении K_{nr} степень $F^{v(\alpha)}$ элемента Фробениуса F.

Мы знаем, что элемент $f(\pi)$ равен F на поле K_{nr} и что $\theta(\pi)$ также равен F на K_{nr}. С другой стороны, элемент $f(\pi)$ равен 1 на поле K_π и элемент $\theta(\pi)$ равен 1 на K_π. Следовательно, $f(\pi) = \theta(\pi)$ на L.

Группа K^* порождена униформизирующими элементами πu (элемент $\pi^n u$ записываем как $(\pi u) \cdot \pi^{n-1}$). Следовательно, $f = \theta$.

Предложение 2.6. *Пусть* f: $K^* \to G$ — *некоторый гомоморфизм; предположим, что выполняется условие* (1) *предложения* 2.5, *в то время как условие* (2) *заменено на следующее*:

(2′) *если* K'/K — *конечное подрасширение расширения* L *и* $\alpha \in K^*$ *является нормой из* K'^*, *то автоморфизм* $f(\alpha)$ *тривиален на поле* K'.

Тогда гомоморфизм f *есть отображение взаимности* θ.

Доказательство. Достаточно доказать, что (2′)$\Rightarrow$(2). Другими словами, мы должны доказать, что если π —

униформизирующий элемент, то автоморфизм $f(\pi)$ тривиален на расширении K_π. Пусть K'/K — конечное подрасширение расширения K_π. Мы хотим доказать, что $\pi \in NK'^*$. Но элемент $\theta(\pi)$ тривиально действует на K_π, а потому и на K'. Это означает, что $\pi \in NK'^*$.

2.9. Архимедов случай

Для глобальной теории полей классов необходимо распространить эти результаты на тривиальные случаи, когда поле K есть или $\mathbf{R}$ или $\mathbf{C}$. Пусть $G = G(\mathbf{C}/\mathbf{R})$. В случае $K = \mathbf{C}$ группа Брауэра тривиальна: $\mathrm{Br}(\mathbf{C}) = 0$. С другой стороны, $\mathrm{Br}(\mathbf{R}) = H^2(G, \mathbf{C}^*) = \mathbf{R}^*/\mathbf{R}_+^*$, и, таким образом, группа $\mathrm{Br}(\mathbf{R})$ имеет порядок 2.

Образ отображения $\mathrm{inv}_\mathbf{R} : \mathrm{Br}(\mathbf{R}) \to \mathbf{Q}/\mathbf{Z}$ равен $\{0, 1/2\} \in \mathbf{Q}/\mathbf{Z}$, а образ отображения $\mathrm{inv}_\mathbf{C} : \mathrm{Br}(\mathbf{C}) \to \mathbf{Q}/\mathbf{Z}$ — нулю. Группа $H^2(G, \mathbf{C}^*) = H^2(\mathbf{C}/\mathbf{R})$ циклична, имеет порядок 2 и порождается таким элементом $u \in \mathrm{Br}(\mathbf{R})$, что $\mathrm{inv}_\mathbf{R}(u) = 1/2$.

В силу отображения взаимности (точнее в силу обратного к нему отображения) мы имеем изоморфизм $G = H^{-2}(G, \mathbf{Z}) \to H^0(G, \mathbf{C}^*) = \mathbf{R}^*/\mathbf{R}_+^*$.

§ 3. ФОРМАЛЬНОЕ УМНОЖЕНИЕ В ЛОКАЛЬНЫХ ПОЛЯХ

Результаты этого раздела принадлежат Любину и Тэйту [6].

Главными следствиями из них для нас будут: (1) построение конфинальной системы абелевых расширений заданного локального поля K; (2) формула, дающая выражение символа $(\alpha, L/K)$ в явном виде с помощью этих расширений; (3) теорема существования из п. 2.7.

Для того чтобы проиллюстрировать используемые ниже идеи, начнем со случая $K = \mathbf{Q}_p$. Результаты, которые будут доказаны, в этом случае уже известны; однако они были получены не без труда, в то время как из теории Любина — Тэйта они следуют тривиально.

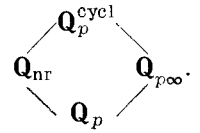
3.1. Случай $K = \mathbf{Q}_p$

Т е о р е м а 3.1. *Пусть* $\mathbf{Q}_p^{\mathrm{cycl}}$ *— поле, порожденное над* $\mathbf{Q}_p$ *всеми корнями из единицы. Тогда* $\mathbf{Q}_p^{\mathrm{cycl}}$ *является максимальным абелевым расширением поля* $\mathbf{Q}_p$.

Для того чтобы определить $(\alpha, L/K)$, удобно разложить расширение $\mathbf{Q}_p^{\mathrm{cycl}}$ на части. Определим $\mathbf{Q}_{\mathrm{nr}}$ как поле, порожденное над $\mathbf{Q}_p$ корнями всех тех степеней из единицы, которые не делятся на p (таким образом, $\mathbf{Q}_{\mathrm{nr}}$ — максимальное неразветвленное расширение поля $\mathbf{Q}_p$), и определим $\mathbf{Q}_{p\infty}$ как поле, порожденное над $\mathbf{Q}_p$ корнями из единицы степеней p^v, $v = 1, 2, \ldots$ (так что $\mathbf{Q}_{p\infty}$ вполне разветвлено). Тогда расширения $\mathbf{Q}_{\mathrm{nr}}$ и $\mathbf{Q}_{p\infty}$ линейно разделены и

$$\mathbf{Q}_p^{\mathrm{cycl}} = \mathbf{Q}_{\mathrm{nr}} \cdot \mathbf{Q}_{p\infty} = \mathbf{Q}_{\mathrm{nr}} \otimes Q_{p\infty}.$$

В итоге мы имеем диаграмму



Далее, $G(\mathbf{Q}_{\mathrm{nr}}/\mathbf{Q}_p) = \hat{\mathbf{Z}}$, и если $\sigma \in G(\mathbf{Q}_{p\infty}/\mathbf{Q}_p)$, то автоморфизм σ определяется своим действием на корни из единицы. Пусть E — группа корней степени p^v из единицы, $v = 1, 2, \ldots$. Как абелева группа, группа E изоморфна $\varinjlim \mathbf{Z}/p^v\mathbf{Z} = \mathbf{Q}_p/\mathbf{Z}_p$. Мы будем рассматривать группу E как $\mathbf{Z}_p$-модуль. Существует каноническое отображение $\mathbf{Z}_p \to \mathrm{End}(E)$, определенное очевидным образом, и это отображение является изоморфизмом. Действие группы Галуа на модуль E определяет гомоморфизм $G(\mathbf{Q}_{p\infty}/\mathbf{Q}_p) \to \mathrm{Aut}(E) = U_p$ и, как известно, он является изоморфизмом (см. гл. III и [8], гл. IX, § 4, и гл. XIV, § 7). Если $u \in U_p$, то мы будем обозначать через $[u]$ соответствующий автоморфизм расширения $\mathbf{Q}_{p\infty}/\mathbf{Q}_p$.

Т е о р е м а 3.2. *Если* $\alpha = p^n u$, *где* $u \in U_p$, *то символ* $(\alpha, \mathbf{Q}_p^{\mathrm{cycl}}/\mathbf{Q}_p) = \sigma_\alpha$ *описывается следующими условиями*:

(1) *на расширении* $\mathbf{Q}_{\mathrm{nr}}$ *элемент* σ_α *индуцирует* n*-ю степень автоморфизма Фробениуса*;

(2) *на расширении* $\mathbf{Q}_{p\infty}$ *элемент* σ_α *индуцирует автоморфизм* $[u^{-1}]$.

В данном случае утверждение (1) тривиально, потому что было доказано еще в предложении 2.2. Утверждение же (2) может быть доказано либо глобальными методами, либо

трудными локальными методами (Дворк), либо, наконец, с помощью теории Любина — Тэйта (см. теорему 3.3).

Замечание. Утверждение (2) теоремы 3.2 эквивалентно следующему: если w — первообразный корень p^n-й степени из единицы и $u \in U_p$, то

$$\sigma_u(w) = w^{u^{-1}} = 1 + \sum_{n=1}^{\infty} \binom{u^{-1}}{n} x^n,$$

где $w = 1 + x$.

3.2. Формальные группы

Главное, что мы здесь исследуем,— это вопросы о замене группового закона умножения $F(X, Y) = X + Y + XY$ и биномиального разложения. Групповой закон будет определен с помощью формального степенного ряда от двух переменных; мы приступаем к изучению таких групповых законов.

Определение. *Пусть A — коммутативное кольцо с единицей, и пусть $F \in A[[X, Y]]$. Мы говорим, что F является коммутативным формальным групповым законом, если:*

(а) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;

(б) $F(0, Y) = Y$ *и* $F(X, 0) = X$;

(в) *существует такой однозначно определенный элемент* $G(X)$, *что* $F(X, G(X)) = 0$;

(г) $F(X, Y) = F(Y, X)$;

(д) $F(X, Y) \equiv X + Y \pmod{\deg 2}$.

(На самом деле, как можно проверить, пункты (в) и (д) следуют из (а), (б) и (г).)

В этом определении подразумевается, что два формальных степенных ряда сравнимы по mod deg n тогда и только тогда, когда они совпадают в членах степени, строго меньшей, чем n.

Положим $A = O_K$; пусть $F(X, Y)$ — коммутативный формальный групповой закон, определенный над кольцом O_K, и пусть $\mathfrak{m}_K$ — максимальный идеал кольца O_K. Если $x, y \in \mathfrak{m}_K$, то ряд $F(x, y)$ сходится и его сумма $x*y$ принадлежит кольцу O_K. Относительно этого группового закона на $\mathfrak{m}_K$ является *группой*, которую мы обозначим через $F(\mathfrak{m}_K)$.

Эти соображения применимы и к расширению L/K и к максимальному идеалу $\mathfrak{m}_L$ кольца O_L. Тогда мы получим группу $F(\mathfrak{m}_L)$, определенную для каждого алгебраического расширения поля K с помощью перехода к индуктивному пределу от конечного случая.

Если $F(X, Y) = X + Y + XY$, то мы получаем мультипликативный групповой закон группы $1 + \mathfrak{m}_K$.

Элементы конечного порядка группы $F(\mathfrak{m}_K)$ образуют группу кручения, и группа $G(K_s/K)$ действует на нее. Вопрос о структуре этого модуля относительно группы Галуа является интересной проблемой, которая на сегодняшний день решена лишь в некоторых специальных случаях.

3.3. Формальные групповые законы Любина—Тэйта

Пусть K — локальное поле, $q = \mathrm{Card}(k)$ и $\pi \in O_K$ — униформизирующий элемент. Пусть $\mathfrak{F}_\pi$ — множество формальных степенных рядов f, для которых:

(1) $f(X) \equiv \pi X \pmod{\deg 2}$;

(2) $f(X) \equiv X^q \pmod{\pi}$.

(Говорят, что два степенных ряда сравнимы по mod π, если каждый коэффициент их разности делится на π. Таким образом, второе условие означает, что если мы перейдем к полю вычетов и обозначим через $\bar{f}(X)$ соответствующий элемент кольца $k[[X]]$, то $\bar{f}(X) = X^q$.)

Примеры.

(а) $f(X) = \pi X + X^q$;

(б) $K = \mathbf{Q}_p$, $\pi = p$, $f(X) = pX + \binom{p}{2} X^2 + \ldots + pX^{p-1} + X^p$.

Следующие четыре предложения будут доказаны ниже как следствия предложения 3.5.

Предложение 3.1. *Пусть $f \in \mathfrak{F}_\pi$. Тогда существует единственный формальный групповой закон F_f с коэффициентами в кольце A, для которого f является эндоморфизмом.*

(Это означает, что $f(F_f(X, Y)) = F_f(f(X), f(Y))$, т. е. $f \circ F_f = F_f \circ (f \times f)$.)

Предложение 3.2. *Пусть $f \in \mathfrak{F}_\pi$ и F_f — соответствующий групповой закон из предложения 3.1. Тогда для любого $a \in A = O_K$ существует единственный элемент $[a]_f \in A[[X]]$, такой, что*

(1) *$[a]_f$ коммутирует с f;*

(2) *$[a]_f \equiv aX \pmod{\deg 2}$.*

Кроме того, элемент $[a]_f$ является тогда эндоморфизмом группового закона F_f.

Из предложения 3.2 мы получаем отображение $A \to \mathrm{End}(F_f)$, определенное формулой $a \mapsto [a]_f$. Рассмотрим, например, случай

$$K = \mathbf{Q}_p, \quad f = pX + \binom{p}{2} X^2 + \ldots + X^p;$$

тогда F_f является мультипликативным законом $X + Y + XY$ и

$$[a]_f = (1+X)^a - 1 = \sum_{i=1}^{\infty} \binom{a}{i} X^i.$$

Предложение 3.3. *Отображение $a \mapsto [a]_f$ является инъективным гомоморфизмом кольца A в кольцо $\mathrm{End}(F_f)$.*

Предложение 3.4. *Пусть f и g — элементы из множества $\mathfrak{F}_\pi$. Тогда соответствующие групповые законы изоморфны.*

3.4. Формулировки

Пусть K — локальное поле и π — униформизирующий элемент. Пусть $f \in \mathfrak{F}_\pi$, и пусть F_f — соответствующий групповой закон (из предложения 3.1). Обозначим через $M_f = F_f(\mathfrak{m}_{K_s})$ группу точек в сепарабельном замыкании, снабженную тем групповым законом, который индуцируется законом F_f. Пусть $a \in A$, $x \in M_f$ и $ax = [a]_f x$. Согласно предложению 3.3, это определяет структуру некоторого A-модуля на множестве M_f. Пусть E_f — подмодуль кручения модуля M_f; он представляет собой множество таких элементов из M_f, которые аннулируются степенью униформизирующей π.

Теорема 3.3. *Справедливы следующие утверждения.*

(а) *Подмодуль кручения E_f изоморфен (как A-модуль) модулю K/A.*

(б) *Пусть $K_\pi = K(E_f)$ — поле, порожденное модулем E_f над K. Тогда поле K_π является абелевым расширением поля K.*

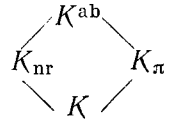
(в) *Пусть u — некоторая единица из группы K^*. Тогда элемент $\sigma_u = (u, K_\pi/K)$ группы $G(K_\pi/K)$ действует на модуль E_f с помощью элемента $[u^{-1}]_f$.*

(г) *Операция, описанная в* п. (в), *определяет некоторый изоморфизм $U_K \to G(K_\pi/K)$.*

(д) *Символ норменного вычета $(\pi, K_\pi/K)$ равен* 1.

(е) *Поля K_{nr} и K_π линейно разделены и $K^{\mathrm{ab}} = K_{\mathrm{nr}} \cdot K_\pi$.*

Результаты теоремы 3.3 могут быть высказаны также следующим образом. Имеет место диаграмма:



В данном случае $G(K_{\mathrm{nr}}/K) = \hat{\mathbf{Z}}$ и $G(K_\pi/K) = U_K$. Более того, каждый элемент $\alpha \in K^*$ может быть записан в виде $\alpha = \pi^n u$, и оператор σ_π дает автоморфизм (Фробениуса) σ на расширении K_{nr}/K, тогда как оператор σ_u определяет автоморфизм $[u^{-1}]$ расширения K_π/K.

Пример. Возьмем $K = \mathbf{Q}_p$, $\pi = p$ и $f = pX + \binom{p}{2} X^2 + \ldots + X^p$. Формальный групповой закон является мультипликативным групповым законом; множество E_f представляет собой множество корней степени p^v из единицы; расширение K_π является полем, которое в п. 3.1 обозначалось через $\mathbf{Q}_{p\infty}$, и мы вновь приходим к теоремам 3.1 и 3.2.

3.5. Построение формального группового закона F_f и эндоморфизма $[a]_f$

В этом параграфе мы построим формальный групповой закон F_f и отображение $a \mapsto [a]_f$.

Предложение 3.5. *Пусть $f, g \in \mathfrak{F}_\pi$, число n — целое, и пусть $\phi_1(X_1, \ldots, X_n)$ — линейная форма от*

$X_1, \ldots, X_n$ с коэффициентами из кольца A. Тогда существует такой однозначно определенный ряд $\phi \in A\,[[X_1, \ldots, X_n]]$, что

(а) $\phi \equiv \phi_1 \pmod{\deg 2}$;
(б) $f \circ \phi = \phi \circ (g \times \ldots \times g)$.

Замечания. (1) Свойство (б) может быть записано так:

$$f(\phi(X_1, \ldots, X_n)) = \phi(g(X_1), \ldots, g(X_n)).$$

(2) В доказательстве не будет использоваться полнота кольца A. Кроме того, из доказательства следует, что ряд ϕ является единственным степенным рядом с коэффициентами в некотором расширении кольца A, которое, как A-модуль, свободно от кручения, удовлетворяющим условиям (а) и (б).

Доказательство. Мы построим ряд ϕ с помощью последовательных приближений. Точнее будет построена такая последовательность $(\phi^{(p)})$, что $\phi^{(p)}$ принадлежит $A\,[[X_1, \ldots, X_n]]$, удовлетворяет условиям (а) и (б) по $\bmod \deg (p+1)$ и единствен по $\bmod \deg (p+1)$. После этого мы положим $\phi = \lim \phi^{(p)}$, и это будет тем самым рядом ϕ, существование которого утверждается.

Положим $\phi^{(1)} = \phi_1$.

Допустим, что приближение $\phi_1 + \ldots + \phi_p = \phi^{(p)}$ уже построено. Таким образом, $f \circ \phi^{(p)} \equiv \phi^{(p)} \circ (g \times \ldots \times g) \pmod{\deg (p+1)}$. Для удобства записи заменим символ $g \times \ldots \times g$ на символ g. Пусть теперь $\phi^{(p+1)} = \phi^{(p)} + \phi_{p+1}$. Тогда мы можем написать:

$$f \circ \phi^{(p)} \equiv \phi^{(p)} \circ g + E_{p+1} \pmod{\deg (p+2)},$$

где E_{p+1} («погрешность») удовлетворяет сравнению $E_{p+1} \equiv 0 \pmod{\deg (p+1)}$. Рассмотрим $\phi^{(p+1)}$; имеем:

$$f \circ \phi^{(p+1)} = f \circ (\phi^{(p)} + \phi_{p+1}) \equiv f \circ \phi^{(p)} + \pi\phi_{p+1} \pmod{\deg (p+2)}$$

(производная ряда f в начале координат равна π) и

$$\phi^{(p)} \circ g + \phi_{p+1} \circ g \equiv \phi^{(p)} \circ g + \pi^{p+1}\phi_{p+1} \pmod{\deg (p+2)}.$$

Таким образом,

$$f \circ \phi^{(p+1)} - \phi^{(p+1)} \circ g \equiv$$
$$\equiv E_{p+1} + (\pi - \pi^{p+1})\,\phi_{p+1} \pmod{\deg (p+2)}.$$

Эти сравнения показывают, что мы должны положить

$$\phi_{p+1} = -E_{p+1}/\pi\,(1 - \pi^p).$$

Единственность теперь очевидна, и остается показать, что ряд ϕ_{p+1} имеет коэффициенты из кольца A. Иными словами, $E_{p+1} \equiv 0 \pmod{\pi}$. Для $\phi \in \mathbf{F}_q[[X]]$ мы имеем $\phi(X^q) = (\phi(X))^q$, и вместе со сравнением $f(X) \equiv X^q \pmod{\pi}$ это дает, что

$$f \circ \phi^{(p)} - \phi^{(p)} \circ f \equiv (\phi^{(p)}(X))^q - \phi^{(p)}(X^q) \equiv 0 \pmod{\pi}.$$

Итак, если задан ряд $\phi^{(p)}$, то мы можем построить единственный ряд $\phi^{(p+1)}$, и доказательство завершается с помощью индукции и перехода к пределу.

Доказательство предложения 3.1. Для каждого $f \in \mathfrak{F}_\pi$ обозначим через $F_f(X, Y)$ единственное решение сравнения $F_f(X, Y) \equiv X + Y \pmod{\deg 2}$, такое, что $f \circ F_f = F_f \circ (f \times f)$; существование F_f гарантирует предложение 3.5.

Для того чтобы F_f был формальным групповым законом, надо проверить выполнение правил (а) — (д), сформулированных выше. Но это — простое упражнение на применение предложения 3.5: в каждом случае мы проверяем, что левая и правая части соответствующего равенства являются решениями задачи, описанной выше, и используем утверждение о единственности замечания (2) к предложению 3.5. Например, для того чтобы доказать ассоциативность, заметим, что оба выражения $F_f(F_f(X, Y), Z)$ и $F_f(X, F_f(Y, Z))$ являются решениями сравнения

$$H(X, Y, Z) \equiv X + Y + Z \pmod{\deg 2}$$

и уравнения

$$H(f(X), f(Y), f(Z)) = f(H(X, Y, Z)).$$

Доказательство предложения 3.2. Для каждого $a \in A$ и $f, g \in \mathfrak{F}_\pi$ обозначим через $[a]_{f,g}(T)$ единственное решение сравнения

$$[a]_{f,g}(T) \equiv aT \pmod{\deg 2}$$

и уравнения

$$f([a]_{f,g}(T)) = [a]_{f,g}(g(T))$$

(т. е. $f \circ [a]_{f,g} = [a]_{f,g} \circ g$). Положим $[a]_f = [a]_{f,f}$.

Теперь мы имеем, что

$$F_f([a]_{f,g}(X),\ [a]_{f,g}(Y)) = [a]_{f,g}(F_g(X,\ Y)).$$

Так как выражения в обеих частях сравнимы с $aX + aY \pmod{\deg 2}$, то, заменив X на $g(X)$ и Y на $g(Y)$ в обеих частях, мы получим тот же результат, как если бы мы подставляли оба эти выражения в ряд f. Таким образом, ряд $[a]_{f,g}$ является формальным гомоморфизмом закона F_g в закон F_f. При $g = f$ это показывает, что элементы $[a]_f$ являются эндоморфизмами закона F_f.

Доказательство предложения 3.3. Тем же способом, который был в общих чертах описан выше, доказывается, что

$$[a+b]_{f,g} = F_f \circ ([a]_{f,g} \times [a]_{f,g})$$

и

$$[ab]_{f,h} = [a]_{f,g} \circ [b]_{g,h}.$$

Это следует из того, что композиция двух гомоморфизмов только что описанного вида отражается на произведении соответствующих элементов кольца A. Полагая $f = g$, мы видим, что отображение $a \longmapsto [a]_f$ является кольцевым гомоморфизмом из A в $\mathrm{End}(E_f)$. Оно инъективно, потому что член степени 1 в ряде $[a]_f$ равен aX.

Доказательство предложения 3.4. Если a — единица кольца A, то ряд $[a]_{f,g}$ обратим (см. доказательство предложения 3.2), так что $F_g \cong F_f$ относительно изоморфизма $[a]_{f,g}$.

Заметим, что $[\pi]_f = f$ и $[1]_f$ — тождественное отображение (доказательство аналогично предыдущим).

Это завершает доказательства предложений 3.1, 3.2, 3.3, 3.4.

3.6. Первые свойства расширения K_π поля K

С этого момента мы сосредоточим внимание на подполях некоторого фиксированного сепарабельного замыкания K_s поля K. Если задан ряд $f \in \mathfrak{F}_\pi$, обозначим через F_f соответствующий формальный групповой закон и через E_f — подмодуль кручения A-модуля $F_f(\mathfrak{m}_{K_s})$. Пусть E_f^n — ядро эндоморфизма $[\pi^n]_f$; тогда $E_f = \bigcup E_f^n$. Пусть $K_\pi^n = K(E_f^n)$ и $K_\pi = \bigcup K_\pi^n$. Если через $G_{\pi,n}$ обозначена группа Галуа поля $K(E_f^n)$ над полем K, то $G(K_\pi/K) = \varprojlim G_{\pi,n}$.

Предложение 3.6. (а) *A-модуль E_f изоморфен модулю K/A;*

(б) *естественный гомоморфизм $G(K_\pi/K) \to \mathrm{Aut}(E_f)$ является изоморфизмом.*

Доказательство. Мы можем выбрать элемент f по нашему усмотрению, так как в силу предложения 3.4 различные выборы дают изоморфные групповые законы. Возьмем $f = \pi X + X^q$. Тогда $\alpha \in E_f^n$ в том и только том случае, если $f^{(n)}(\alpha) = 0$, где $f^{(n)}$ обозначает композицию $f \circ \ldots \circ f$ (n раз); таким образом, $f^{(n)} = [\pi^n]_f$.

Если $\alpha \in \mathfrak{m}_{K_s}$, то уравнение $\pi X + X^q = \alpha$ сепарабельно и, следовательно, разрешимо в поле K_s, причем в действительности решение принадлежит идеалу $\mathfrak{m}_{K_s}$. Это показывает, что модуль M_f делим. Следовательно, делим также и модуль E_f. Это уже означает, что модуль E_f является прямой суммой модулей, изоморфных модулю K/A.

Рассмотрим подмодуль $E_f^1 \subset E_f$, состоящий (см. выше) из тех элементов $\alpha \in M_f$, для которых $[\pi]_f \alpha = 0$. Подмодуль E_f^1 изоморфен модулю $A/\mathfrak{m}_{K_s}$, так как он является A-модулем из q элементов. Этого достаточно для того, чтобы показать, что E_f изоморфен модулю K/A.

Любой автоморфизм $\sigma \in G(K_\pi/K)$ индуцирует некоторый автоморфизм A-модуля E_f. Но, так как $E_f \cong K/A$ и $\mathrm{End}_A(K/A) = A$, то это дает некоторое отображение $G(K_\pi/K) \longrightarrow \mathrm{Aut}(E_f) = U_K$. Оно инъективно по определению поля K_π, и остается показать его сюръективность.

Возьмем $n \geqslant 1$ и определим множества E_f^n и K_π^n указанным выше способом. Мы имеем инъективное отображение $G(K_\pi^n/K) \longrightarrow U_K/U_K^n$, где $U_K^n = 1 + \pi^n A$. Пусть $\alpha \in E_f^n$ — примитивный элемент, т. е. такой элемент из E_f^n, что $[\pi^{n-1}]_f \alpha = 0$, но $[\pi^{n-1}]_f \alpha \neq 0$. Наконец, определим многочлен ϕ следующим образом:

$$\phi = f^{(n)}/f^{(n-1)} = f(f^{(n-1)}/f^{(n-1)}).$$

Но так как $f = X^q + \pi X$, то $f/X = X^{q-1} + \pi$. Следовательно,

$$\frac{f(f^{(n-1)})}{f^{(n-1)}} = (f^{(n-1)}(X))^{q-1} + \pi,$$

и степень этого выражения равна $q^n - q^{n-1}$; построенный многочлен неприводим, так как он — многочлен Эйзенштейна. Все примитивные элементы α являются корнями многочлена ϕ. Таким образом, порядок группы $G(K_\pi^n/K)$ не меньше, чем $(q-1)q^{n-1}$. С другой стороны, это число есть порядок группы U_K/U_K^n. Следовательно, $G(K_\pi^n/K) = U_K/U_K^n$. Отсюда вытекает, что

$$G(K_\pi/K) = \varprojlim G(K_\pi^n/K) = \varprojlim U_K/U_K^n = U_K,$$

чем завершается доказательство предложения 3.6.

Из этого же доказательства можно получить

Следствие. *Элемент π является нормой из поля $K(\alpha) = K_\pi^n$.*

Доказательство. Многочлен ϕ, построенный выше, унитарен, и его свободный член равен π. Следовательно, $N(-\alpha) = \pi$.

3.7. Отображение взаимности

Мы будем изучать композит $L = K_{\mathrm{nr}}K_\pi$ расширений K_{nr} и K_π и символ $(\alpha, L/K)$, $\alpha \in K^*$. Нам нужно сравнить два униформизирующих элемента π и $\omega = \pi u$, $u \in U_K$.

Пусть $\hat{K}_{\mathrm{nr}}$ — пополнение поля K_{nr} (напомним, что поле K_{nr} является возрастающим объединением полных полей, но само полным не является) и $\hat{A}_{\mathrm{nr}}$ — кольцо целых элементов поля $\hat{K}_{\mathrm{nr}}$. По определению поле $\hat{K}_{\mathrm{nr}}$ полно; оно имеет некоторое алгебраически замкнутое поле вычетов, и элемент π является униформизирующим параметром поля $\hat{K}_{\mathrm{nr}}$. Возьмем $f \in \mathfrak{F}_\pi$ и $g \in \mathfrak{F}_\omega$.

Лемма 3.1. *Пусть $\sigma \in G(K_{\mathrm{nr}}/K)$ — эндоморфизм Фробениуса; продолжим его непрерывно на поле $\hat{K}_{\mathrm{nr}}$. Тогда существует некоторый степенной ряд $\phi \in \hat{A}_{\mathrm{nr}}[[X]]$, такой, что $\phi(X) \equiv \varepsilon X \pmod{\deg 2}$, где ε — единица и*

(а) ${}^\sigma\phi = \phi \circ [u]_f$;

(б) $\phi \circ F_f = F_g \circ (\phi \times \phi)$;

(в) $\phi \cdot [a]_f = [a]_g \circ \phi$ *для всех* $a \in A$.

Доказательство. Так как отображение $\sigma - 1$ сюръективно на кольце $\hat{A}_{\mathrm{nr}}$ и на группе $\hat{U}_{\mathrm{nr}}$ (см. [8], стр. 209), то существует такой ряд $\phi \in \hat{A}_{\mathrm{nr}}[[X]]$, что $\phi(X) \equiv \varepsilon X \pmod{\deg 2}$, где ε — некоторая единица и ${}^\sigma\phi = \phi \circ [u]_f$. Это доказывается с помощью последовательных приближений, и мы отсылаем читателя за деталями к работе [6]. Выбранный таким способом ряд ϕ не обязательно удовлетворяет требованиям (б) и (в); однако его можно подправить так, чтобы он им стал удовлетворять. Вычисления даны в [6] (где они фигурируют как (17) и (18) в лемме 2 на стр. 385). Заметим, что оба эти условия вместе выражают тот факт, что ряд ϕ является изоморфизмом A-модулей законов F_f и F_g.

Вычисление норменного отображения взаимности в расширении L/K

Пусть $L_\pi = K_{\mathrm{nr}} \cdot K_\pi$. Так как расширения K_{nr} и K_π линейно разделены над полем K, то группа Галуа $G(L_\pi/K)$ является произведением групп Галуа $G(K_\pi/K)$ и $G(K_{\mathrm{nr}}/K)$. Для каждого униформизирующего элемента $\pi \in A$ мы определим гомоморфизм r_π: $K^* \to G(L_\pi/K)$, такой, что

(а) $r_\pi(\pi)$ равно 1 на K_π и равно автоморфизму Фробениуса σ на поле K_{nr};

(б) для $u \in U_K$ элемент $r_\pi(u)$ равен $[u^{-1}]_f$ на поле K_π и равен 1 на поле K_{nr}.

Мы хотим доказать, что *поле L_π и гомоморфизм r_π не зависят от выбора элемента π*. Пусть $\omega = \pi u$ — другой униформизирующий элемент.

Прежде всего $L_\pi = L_\omega$. По лемме 3.1 законы F_f и F_g изоморфны над полем $\hat{K}_{\mathrm{nr}}$. Следовательно, поля, порожденные их точками деления, совпадают. Значит, $\hat{K}_{\mathrm{nr}} \cdot K_\pi = \hat{K}_{\mathrm{nr}} \cdot K_\omega$. Переходя к пополнению, мы получаем, что $\widehat{K_{\mathrm{nr}} \cdot K_\pi} = \widehat{K_{\mathrm{nr}} \cdot K_\omega}$. Чтобы отсюда получить равенство $K_{\mathrm{nr}} \cdot K_\pi = K_{\mathrm{nr}} \cdot K_\omega$, докажем следующую лемму.

Лемма 3.2. *Пусть E — любое алгебраическое расширение (конечное или бесконечное) локального поля, и пусть $\alpha \in \hat{E}$. Тогда если α алгебраически сепарабелен над E, то $\alpha \in E$.*

Доказательство. Пусть E_s — сепарабельное замыкание поля E, и пусть E' — множество изолированных точек поля E в поле E_s. Мы можем рассматривать α как элемент из E'. Следовательно, достаточно доказать, что $E' = E$.

Пусть $s \in G(E_s/E)$. Так как оператор s непрерывен и является тождественным на поле E, то он будет тождественным и на E'. Следовательно, $G(E_s/E) = G(E_s/E')$ и по теории Галуа $E' = E$.

Из леммы 3.2 следует, что $L_\pi = L_\omega$ и, таким образом, поле $L = L_\pi$ не зависит от π.

Теперь обратимся к гомоморфизму r_π: $K^* \to G(L/K)$. *Мы покажем, что* $r_\pi(\omega) = r_\omega(\omega)$. Отсюда будет следовать, что $r_\pi(\omega)$ не зависит от выбора π и, таким образом, гомоморфизм r_π совпадает на локальных униформизирующих. Так как последние порождают K^*, то лемма тем самым будет доказана.

Рассмотрим сначала $r_\omega(\omega)$. На поле K_{nr} элемент $r_\omega(\omega)$ является автоморфизмом Фробениуса σ. На поле K_ω он равен 1. С другой стороны, элемент $r_\pi(\omega)$ равен σ на K_{nr}; мы должны рассмотреть действие $r_\pi(\omega)$ на K_ω.

Мы имеем, что $K_\omega = K(E_g)$, где $g \in \mathfrak{F}_\omega$. Пусть $\phi \in \hat{A}[[X]]$ выбран в соответствии с леммой 3.1; ряд ϕ определяет некоторый изоморфизм модулей E_f и E_g. Значит, если $\lambda \in E_g$, то можно считать, что $\lambda = \phi(\mu)$, где $\mu \in E_f$. Рассмотрим элемент $r_\pi(\omega)\lambda$; мы хотим показать, что он равен λ. Как уже отмечалось, $r_\pi(\omega)(\lambda) = r_\pi(\omega)\phi(\mu)$. Положим $s = r_\pi(\omega)$. Мы покажем, что ${}^s\lambda = \lambda$, т. е. ${}^s\phi(\mu) = \phi(\mu)$. Имеем: $r_\pi(\omega) = r_\pi(\pi)\cdot r_\pi(u)$, а действия элементов $r_\pi(\pi)$ и $r_\pi(u)$ были описаны выше в пунктах (а) и (б). Так как ряд ϕ имеет коэффициенты из $\hat{K}_{\mathrm{nr}}$, то ${}^s\phi = {}^\sigma\phi = \phi \circ [u]_f$ в силу пункта (а) из леммы 3.1. Но

$$ {}^s(\phi(\mu)) = {}^s\phi({}^s\mu) = {}^s\phi([u^{-1}]_f(\mu)). $$

Следовательно,

$$ {}^s\phi(\mu) = \phi \circ [u]_f \circ [u^{-1}]_f(\mu) = \phi(\mu). $$

Поэтому гомоморфизм r_π является тождественным на K_ω и, значит, r_π не зависит от π.

Таким образом, r: $K^* \to G(L/K)$ является отображением взаимности θ (предложение 2.5).

Утверждение теоремы 3.3 было доказано без использования равенства $L = K^{\mathrm{ab}}$, которое мы лишь теперь собираемся доказывать.

3.8. Теорема существования

Пусть K^{ab} — максимальное абелево расширение поля K; оно содержит поле K_{nr}. Теорема существования эквивалентна следующему утверждению (теорема 2.3а): если $I_K = G(K^{\mathrm{ab}}/K_{\mathrm{nr}})$ — подгруппа инерции группы $G(K^{\mathrm{ab}}/K)$, то *отображение взаимности* θ: $U_K \to I_K$ *является изоморфизмом.*

Пусть L — композит $K_\pi \cdot K_{\mathrm{nr}}$ и $I'_K = G(L/K_{\mathrm{nr}})$ — подгруппа инерции группы $G(L/K)$. Рассмотрим отображения:

$$ U_K \xrightarrow{\theta} I_K \xrightarrow{e} I'_K, $$

где θ — отображение взаимности и e — каноническое отображение $I_K \to I'_K$. Оба отображения θ и e сюръективны.

С другой стороны, композиция $e \circ \theta$: $U_K \to I_K$ уже была вычислена. Если мы отождествим I'_K с U_K, то она состоит в отображении $u \mapsto u^{-1}$. Следовательно, композиция $e \circ \theta$ является изоморфизмом. Отсюда вытекает, что каждое из отображений θ и e является изоморфизмом.

Как мы уже отмечали, первый изоморфизм эквивалентен теореме существования. Второй же означает, что $L = K^{\mathrm{ab}}$, так как оба поля L и K^{ab} содержат K_{nr}.

(Другое доказательство. Докажем непосредственно, что каждая открытая подгруппа $M \subset K^*$ конечного индекса является нормальной подгруппой, соответствующей некоторому конечному подрасширению поля L. Это докажет и теоремы существования (теорема 2.3), и то, что $L = K^{\mathrm{ab}}$.

Так как подгруппа M открыта, то существует такое $n \geqslant 1$, что $U_K^n \subset M$; так как подгруппа M имеет конечный индекс, то существует $m \geqslant 1$, такое, что $\pi^m \in M$; следовательно, подгруппа M содержит подгруппу $V_{n,m}$, порожден-

ную группой U_K^n и элементом π^m. Пусть K_m — неразветвленное расширение поля K степени m; рассмотрим подполе $L_{n,\,m} = K_\pi^n \cdot K_m \subset L$. Если $u \in U_K$ и $a \in \mathbf{Z}$, то мы знаем, что $(u\pi^a, L_{n,\,m}/K)$ равно $[u^{-1}]$ на расширении K_π^n и равно a-й степени элемента Фробениуса на поле K_m; следовательно, элемент $(u\pi^a, L_{n,\,m}/K)$ тривиален тогда и только тогда, когда $u \in U_K^n$ и $a \equiv 0 \pmod m$, т. е. тогда и только тогда, когда $u\pi^a \in V_{n,\,m}$. Это показывает, что $V_{n,\,m} = NL_{n,\,m}$, и так как M содержит $V_{n,\,m}$, группа M является нормой некоторого подрасширения поля $L_{n,\,m}$, что и требовалось доказать.)

§ 4. ГРУППЫ ВЕТВЛЕНИЯ И КОНДУКТОРЫ

4.1. Группы ветвления

Пусть L/K — расширение Галуа локального поля с группой Галуа $G\,(L/K)$. Напомним в нескольких словах определение верхней нумерации групп ветвления (детали см. в гл. I, § 9 или [8], гл. IV).

Пусть функция i_G: $G\,(L/K) \to \{\mathbf{Z} \cup \infty\}$ определена следующим образом. Для $s \in G\,(L/K)$ обозначим через x образующую O_K-алгебры O_L и положим $i_G\,(s) = v_L\,(s\,(x) - x))$. Определим теперь G_u для всех положительных вещественных чисел u таким условием: $s \in Q_u$ тогда и только тогда, когда $i_G\,(s) \geqslant n + 1$. Группы G_u называются группами ветвления группы $G\,(L/K)$ (или расширения L/K). Для того чтобы иметь дело с факторгруппами, необходимо ввести нумерацию групп ветвления, называемую «верхней нумерацией». Эта новая нумерация задается так: $G^v = G_u$, где $v = \phi\,(u)$ и функция ϕ характеризуется следующими свойствами:

(а) $\phi\,(0) = 0$;
(б) функция ϕ непрерывна;
(в) функция ϕ кусочно линейна;
(г) $\phi'\,(u) = 1/(G_0 : G_u)$, если u — нецелое число.

Группы G^v, определенные таким способом, согласованы с переходом к факторгруппам: $(G/H)^v$ является образом группы G^v в группе G/H («теорема Эрбрана»). Это позволяет определить группы G^v даже для бесконечных расширений.

С другой стороны, мы имеем фильтрацию на группе U_K, определенную так: $U_K^n = 1 + \mathfrak{m}_K^n$. Продолжим эту фильтрацию на вещественные индексы с помощью равенства $U_K^v = U_K^n$, если $n - 1 < v \leqslant n$. (Подчеркнем, что символ v в этом контексте изображает вещественное число, а не отображение нормирования!)

Теорема 4.1. *Пусть L/K — абелево расширение с группой Галуа G. Тогда локальное отображение взаимности $\theta : K^* \to G$ отображает группу U_K^v на группу G^v при всех $v \geqslant 0$.*

Доказательство. (1) Случай расширений K_π^n из п. 3.6.

Пусть $u \in U_K^i$ при $i < n$ и $u \notin U_K^{i+1}$. Пусть, далее, $s = \theta\,(u) \in G\,(K_\pi^n/K)$. Имеем: $i\,(s) = v_{K_\pi^n}(s\lambda - \lambda)$, где λ — униформизирующий элемент. Выберем примитивный элемент α для λ; это означает, что α удовлетворяет равенству $[\pi^n]_f\,\alpha = 0$, но $[\pi^{n-1}]_f\,\alpha \neq 0$. Заметим, что $s_u\,(\alpha) = [u^{-1}]_f\,\alpha$ и $u^{-1} = 1 + \pi^i v$ (см. теорему 3.3), где v — единица. Иными словами,

$$s_u\alpha = [1 + \pi^i v]_f\,\alpha = F_f\,(\alpha,\ [\pi^i v]_f\,\alpha).$$

Если положить $\beta = [\pi^i v]_f\,\alpha$, то β — примитивный элемент $(n-i)$-й степени (т. е. $[\pi^{n-i}]_f\,\beta = 0$ и $[\pi^{n-i-1}]_f\,\beta \neq 0$) и

$$F_f\,(\alpha,\ [\pi^i v]_f\,\alpha) = \alpha + \beta + \sum_{i>1,\ j>1} \gamma_{ij}\alpha^i\beta^j$$

при некоторых $\gamma_{ij} \in O_K$. В соответствии с этим

$$s_u\,(\alpha) - \alpha = \beta + \sum \gamma_{ij}\alpha^i\beta^j$$

и

$$v_{K_\pi^n}(s_u\,(\alpha) - \alpha)) = v_{K_\pi^n}(\beta).$$

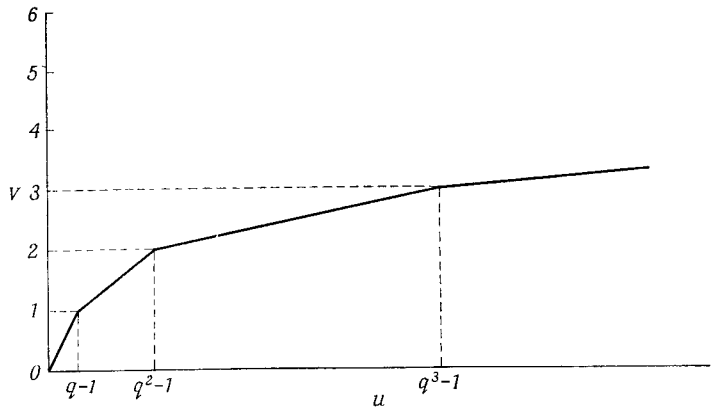
Теперь α является униформизирующим элементом в K_π^n, в то время как β — униформизирующий элемент в поле K_π^{n-i} и расширение K_π^n/K_π^{n-i} вполне разветвлено. Его степень равна q^i. Таким образом, мы определили i как функцию от $\theta\,(u)$; именно, если $u \in U^i$, но $u \notin U^{i+1}$, то $i\,(\theta\,(u)) = q^i$.

Это говорит о том, что если $q^{i-1}-1<u\leqslant q^i-1$, то группа ветвления G_u равна $\theta(U_K^i)$.

Обратимся теперь к верхней нумерации групп G_u. Другими словами, определим функцию $\phi=\phi_{K_\pi^n/K}$, соответствующую расширению K_π^n, которая удовлетворяет перечисленным выше условиям (а)—(г). Именно

$$\phi(u)=\phi_{K_\pi^n/K}(u)=\int_0^u\frac{dt}{(G:G_t)}.$$

Тогда $G^v=G_u$ при $v=\phi(u)$. График функции $\phi(u)$ показан на рисунке.



Общий случай. Доказав теорему 4.1 для полей K_π^n, можно считать ее доказанной и для $K_\pi=\bigcup K_\pi^n$, благодаря возможности перехода к проективным пределам. Следовательно, теорема 4.1 верна и для $K_\pi\cdot K_{\mathrm{nr}}$, потому что оба расширения имеют одну и ту же группу инерции. Так как $K_\pi\cdot K_{\mathrm{nr}}$ — максимальное абелево расширение, то результат верен и в общем случае.

Это завершает доказательство теоремы 4.1.

Следствие. *Скачки в фильтрации $\{G^v\}$ группы G происходят только при целых значениях v.*

Доказательство. Это следует из теоремы 1, так как утверждение тривиально справедливо для фильтраций группы U_K, а теорема 1 позволяет перейти от одной фильтрации к другой.

(Этот результат верен на самом деле для любого поля, полного относительно дискретного нормирования и имеющего совершенное поле вычетов (теорема Хассе — Арфа), см. [8], гл. IV, V.)

4.2. Абелевы кондукторы

Пусть L/K — конечное расширение и $\theta\colon K^*\to G(L/K)$ — соответствующее отображение взаимности. Существует такое наименьшее число n, что $\theta(U_K^n)=0$. Это число n называется *кондуктором* расширения L/K и обозначается через $f(L/K)$.

Предложение 4.1. *Пусть c — такое наибольшее целое число, что группа ветвления G_c не тривиальна. Тогда $f(L/K)=\phi_{L/K}(c)+1$.*

Доказательство. Это предложение является тривиальным следствием теоремы 1 и того факта, что верхняя нумерация получается применением функции ϕ.

Пусть теперь L/K — произвольное расширение Галуа. Обозначим через $\chi: G\to\mathbf{C}^*$ одномерный характер и через L_χ — подполе поля L, соответствующее группе $\ker(\chi)$. Поле L_χ является циклическим расширением поля K, а кондуктор $f(L_\chi/K)$ называется *кондуктором характера* χ и обозначается через $f(\chi)$.

Предложение 4.2. *Пусть $\{G_i\}$ — подгруппы ветвления группы $G=G(L/K)$ и $g_i=\mathrm{Card}(G_i)$. Тогда*

$$(\chi)=\sum_{i=0}^{\infty}\frac{g_i}{g_0}(1-\chi(G_i)),$$

где $\chi(G_i)=g_i^{-1}\sum\limits_{s\in G_i}\chi(s)$ — «среднее значение» характера χ на группе G_i.

Доказательство. Имеем: $\chi(G_i)=1$, если χ тривиален на группе G_i (т. е. везде равен 1), и $\chi(G_i)=$

$= 0$, если χ нетривиален на G_i. Следовательно (мы советуем читателю обратиться за подробностями к [8], гл. IV, VI),

$$\sum_{i=0}^{\infty} \frac{g_i}{g_0}(1-\chi(G_i)) = \sum_{i=0}^{c_\chi} \frac{g_i}{g_0} = \phi_{L/K}(c_\chi)+1,$$

где c_χ — наибольшее число, такое, что ограничение χ на G_{c_χ} не равно 1. Далее, $f(\chi) = f(L_\chi/K) = \phi_{L_\chi/K}(c)+1$, где c определено так же, как в предложении 1 для расширения L_χ/K. Так как функция $\phi_{L/K}$ транзитивна, то достаточно доказать, что $c = \phi_{L/L_\chi}(c_\chi)$, а это следует из теоремы Эрбрана (п. 4.1).

4.3. Кондукторы Артина

Пусть L/K — конечное расширение Галуа с группой Галуа $G = G(L/K)$, и пусть χ — некоторый характер группы G (т. е. некоторая целочисленная комбинация неприводимых характеров). Артин определил *кондуктор* характера χ как число

$$f(\chi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0}(\chi(1)-\chi(G_i)).$$

Если χ является неприводимым характером размерности 1, то число $f(\chi)$ совпадает с предыдущим числом $f(\chi)$. Определим *характер Артина* a_G следующим образом. Для $s \in G$ положим

$$a_G(s) = -f\cdot i_G(s), \quad \text{если } s \neq 1,$$
$$a_G(1) = f\sum_{s\neq 1} i_G(s).$$

Здесь через f обозначена степень классов вычетов $[l:k]$ (не путать с кондуктором!), а через i_G — определенная выше функция.

Предложение 4.3. *Пусть* $g = \mathrm{Card}(G)$. *Тогда*

$$f(\chi) = (a_G, \chi) = \frac{1}{g}\sum_{s\in G}\chi(s)\,a_G(s).$$

Доказательство проводится суммированием последовательных разностей $G_i - G_{i+1}$ и оставляется читателю (см. [8], гл. VI, § 2).

Предложение 4.4. (а) *Пусть* $K \subset L' \subset L$ — *башня расширений Галуа, и пусть* χ' — *характер группы* $G(L'/K)$, *а* χ — *соответствующий характер группы* $G(L/K)$. *Тогда* $f(\chi) = f(\chi')$.

(б) *Пусть* $K \subset K' \subset L$ *и* ψ — *характер группы* $G(L/K')$, *а* ψ^* — *соответствующий индуцированный характер группы* $G(L/K)$. *Тогда*

$$f(\psi^*) = \psi(1)\cdot v_K(\mathfrak{d}_{K'/K}) + f_{K'/K}\cdot f(\psi),$$

где $f_{K'/K}$ — *степень классов вычетов расширения* K'/K *и* $\mathfrak{d}_{K'/K}$ — *дискриминант этого расширения.*

Доказательство опирается на свойства функции i_G и на соотношение между дифферентой и дискриминантом; его можно найти в [8], гл. VI.

Теорема 4.2 (Артин). *Если* χ — *характер представления группы* G, *то* $f(\chi)$ — *положительное целое число.*

Доказательство. Пусть χ — характер рационального представления M группы G. Из теории представлений следует, что

$$\chi(1) = \dim M,$$
$$\chi(G_i) = \dim M^{G_i}.$$

Таким образом, в сумме

$$\sum \frac{g_i}{g_0}(\chi(1)-\chi(G_i))$$

каждый член неотрицателен, причем не все они равны 0. Поэтому $f(\chi) \geqslant 0$.

Остается доказать, что $f(\chi)$ — целое число. Согласно теореме Брауэра, характер χ может быть записан в виде $\chi = \sum m_i\psi_i^*$, где $m_i \in \mathbf{Z}$ и ψ_i^* индуцируется характером ψ_i степени 1 подгруппы $H_i \subset G$.

Следовательно, так как

$$f(\psi_i^*) = \psi_i(1)\,v_K(\mathfrak{d}_{K'/K}) + f_{K'/K}\,f(\psi_i),$$

то $f(\psi_i^*)$ является целым числом при условии, что

целым является и $f(\psi_i)$. Но так как характер ψ_i имеет степень 1, то число $f(\psi_i)$ может быть интерпретировано как абелев кондуктор и, таким образом, очевидно, что оно целое. Это доказывает теорему 4.2.

4.4. Глобальные кондукторы

Пусть L/K — конечное расширение Галуа *числового поля* K, и пусть $G = G(L/K)$ — его группа Галуа. Если χ — характер группы G, то мы определим некоторый идеал $\mathfrak{f}(\chi)$ в поле K — так называемый *кондуктор характера* χ — следующим образом. Пусть $\mathfrak{p}$ — простой идеал в K; выберем простой идеал $\mathfrak{P}$ в L, делящий идеал $\mathfrak{p}$. Обозначим через $G_\mathfrak{p} = G(L_\mathfrak{P}/K_\mathfrak{p})$ соответствующую подгруппу разложения.

Пусть $f(\chi, \mathfrak{p})$ — кондуктор Артина ограничения характера χ на группу $G_\mathfrak{p}$, определенный выше. Если $\mathfrak{p}$ не разветвлен, то $f(\chi, \mathfrak{p}) = 0$. Идеал

$$\mathfrak{f}(\chi) = \prod_\mathfrak{p} \mathfrak{p}^{f(\chi, \mathfrak{p})}$$

называется (глобальным) кондуктором характера χ.

В этих обозначениях предложение 4.4 дает

Предложение 4.5. *Пусть K'/K — подрасширение расширения L/K, ψ — характер группы $H = G(L/K')$ и ψ^* — индуцированный им характер группы $G(L/K)$. Тогда*

$$\mathfrak{f}(\psi^*) = \mathfrak{d}_{K'/K}^{\psi(1)} \cdot N_{K'/K}(\mathfrak{f}(\psi)),$$

где $\mathfrak{d}_{K'/K}$ — дискриминант расширения K'/K.

Применим предложение 5 к случаю $\psi = 1$ и обозначим индуцированный характер ψ^* через $s_{G/H}$ (он соответствует перестановочному представлению группы G/H). Так как $\mathfrak{f}(\psi) = (1)$, то мы получаем

Следствие. *Имеет место равенство $\mathfrak{f}(s_{G/H}, L/K) = \mathfrak{d}_{K'/K}$.*

В случае $H = 1$ справедливо равенство $s_{G/H} = r_G$ (характер регулярного представления группы G) и следствие принимает такой вид:

$$\mathfrak{d}_{L/K} = \prod_\chi \mathfrak{f}(\chi)^{\chi(1)},$$

где χ пробегает множество неприводимых характеров группы G. Это есть «формула произведения главных дискриминантов» («Führerdiskriminantenproduktformel») Артина и Хассе, которая сначала была доказана аналитическими методами (с помощью L-функций). В абелевом случае она выглядит так:

$$\mathfrak{d}_{L/K} = \prod_{\chi: G \to \mathbf{C}^*} \mathfrak{f}(\chi).$$

В квадратичном случае формула выражает тот факт, что дискриминант равен кондуктору.

4.5. Представление Артина

Мы возвращаемся к локальному случаю.

Теорема 4.3. *Пусть L/K — конечное расширение Галуа локальных полей с группой Галуа G, и пусть a_G — характер Артина группы G, определенный выше* (см. п. 4.3). *Тогда a_G является характером комплексного линейного представления группы G, называемого «представлением Артина».*

Доказательство. Характер a_G принимает одинаковые значения на сопряженных элементах и, таким образом, является функцией на классах сопряженных элементов. Следовательно, a_G является комбинацией вида $\sum_\chi m_\chi \chi$, где m_χ — комплексные коэффициенты, а χ — неприводимые характеры. Так как

$$m_\chi = (a_G, \chi) = f(\chi),$$

то, как мы знаем (предложение 4.3 и теорема 4.2), m_χ — положительное целое число. Следовательно, теорема доказана.

Пусть теперь V_χ — неприводимое представление, соответствующее характеру χ. Мы можем определить представление Артина A_G следующим образом:

$$A_G = \sum f(\chi) \cdot V_\chi,$$

где суммирование ведется по всем неприводимым характерам χ.

Замечание. Эта конструкция представления A_G довольно искусственна. Вейль поставил проблему о нахождении «естественного» определения представления A_G.

Теорема 4.4. *Пусть l — простое число, не равное характеристике поля вычетов. Тогда представление Артина может быть реализовано над полем $\mathbf{Q}_l$.*

Доказательство. См. [10] или [9].

Имеются примеры, когда представление Артина не может быть реализовано над полями $\mathbf{Q}$, $\mathbf{R}$ или $\mathbf{Q}_p$, где p — характеристика поля вычетов. Это наводит на мысль о том, что не существует простого определения представления Артина.

Предположим теперь, что расширение L/K вполне разветвлено. Пусть $u_G = r_G - 1$; имеем: $u_G(s) = -1$, если $s \neq 1$, и $u_G(s) = \mathrm{Card}(G) - 1$, если $s = 1$. Поэтому $a_G = u_G + b_G$, где b_G — характер некоторого представления.

Замечание. Равенство $a_G = u_G$ имеет место тогда и только тогда, когда расширение L/K слабо разветвлено. Таким образом, b_G является мерой того, насколько сильно ветвление.

Теорема 4.5. *Пусть l — простое число, не равное характеристике поля вычетов. Тогда существует конечно порожденный проективный $\mathbf{Z}_l[G]$-модуль $B_{G,l}$ с характером b_G и этот модуль единствен с точностью до изоморфизма.*

Доказательство. Это следует из теоремы Суона (см. [11], теорема 5), соединенной с теоремой 4.4, и замечания о том, что $b_G(s) = 0$, если порядок элемента s делится на l (см. также [9]).

О приложениях теоремы 5 к построению инвариантов конечных G-модулей см. [7]. Эти инварианты играют важную роль в функциональном уравнении дзета-функций кривых.

ЛИТЕРАТУРА

Артин, Тэйт (Artin E., Tate J.)
[1] Class field theory, Harvard, 1961.

Бурбаки (Bourbaki N.)
[2] Algèbre, Hermann, Paris, 1950. (Русский перевод: Бурбаки Н., Алгебра, Физматгиз, М., 1965—1966.)

[3] Topologie générale, IIIed., Hermann, Paris. (Русский перевод: Бурбаки Н., Общая топология, Физматгиз, М., 1958—1959.)

Картан (Cartan H.)
[4] Séminaire, exp. 6/7, 1950—1951.

Картан, Эйленберг (Cartan H., Eilenberg S.)
[5] Homological algebra, Princeton, New Jersey, 1956. (Русский перевод: Картан А., Эйленберг С., Гомологическая алгебра, ИЛ, М., 1960.)

Любин, Тэйт (Lubin J., Tate J.)
[6] Formal complex multiplication in local fields, *Ann. Math.*, **81** (1965), 380—387. (Русский перевод: *Математика*, **12** : 1 (1968), 48—54.)

Рэйно (Raynaud M.)
[7] Caracteristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes, Sém. Bourbaki, **17**, № 286, 1964—1965.

Серр (Serre J.-P.)
[8] Corps locaux, Hermann, Paris, 1962.
[9] Introduction à la théore de Brauer, Séminaire IHES, 1965—1966.
[10] Sur la rationalité des representations d'Artin, *Ann. Math.*, **72** (1960), 406—420.

Суон (Swan R.)
[11] The Grothendieck ring of finite group, *Topology*, **2** (1963), 85—110.

ГЛАВА VII

Глобальная теория полей классов

Дж. Тэйт [1])

Всюду в этой главе K обозначает глобальное поле, определенное в гл. II, § 12. Числовые поля мы полностью исследуем, но в функциональном случае наши доказательства имеют один существенный пробел: второе неравенство и ключевая лемма к теореме существования доказаны только для расширений, степень которых взаимно проста с характеристикой. (Читатель может восполнить этот пробел по лекциям Артина и Тэйта [1], стр. 29—38.)

Как и в локальной теории полей классов, рассматриваемый круг вопросов имеет несколько аспектов:

(1) теория когомологий расширений Галуа поля K;

(2) описание абелевых расширений поля K;

(3) L-ряды.

Мы обсудим первые два, оставив, за исключением нескольких замечаний, L-ряды Хейльброну (гл. VIII).

Параграфы 1—6 содержат формулировку и рассмотрение закона взаимности и главной теоремы для абелевых расширений без использования когомологий. Мы надеемся, что это предварительное обсуждение будет служить как ориентиром, так и приманкой для читателей. В § 7—12 содержатся основные доказательства, основанные на вычислении когомологий Галуа классов иделей и группы Брауэра поля K.

Настоящая глава строго ограничивается основными теоремами. В упражнениях в конце книги читатель найдет несколько конкретных примеров и результатов. В тексте

[1]) Подготовлено для печати Бёрчем и Лакстоном.

имеются ссылки на новую литературу, но мы не пытались дать систематическую библиографию. Список используемых обозначений приводится в конце главы.

§ 1. ДЕЙСТВИЕ ГРУППЫ ГАЛУА НА НОРМИРОВАНИЯХ И ПОПОЛНЕНИЯХ

Обозначим через L конечное расширение Галуа поля K с группой Галуа $G = G(L/K)$.

1.1. Прежде всего несколько замечаний о наших обозначениях. Если $a \in L$ и $\sigma \in G$, то действие σ на a обозначается в зависимости от обстоятельств через σa или a^σ. Для $\tau \in G$ мы имеем соотношение $\sigma(\tau a) = (\sigma\tau)a$ или $(a^\tau)^\sigma = a^{(\sigma\tau)}$.

Нормирование есть класс эквивалентных метрик, или нормализованная метрика поля K (гл. II, § 11); мы обычно обозначаем нормирования буквами v и w. Нормирование может быть *архимедовым* или *дискретным*; если v дискретно, то $\mathfrak{O}_v$ обозначает кольцо нормирования, а $\mathfrak{P}_v$ — максимальный идеал в $\mathfrak{O}_v$. Обозначение $\mathfrak{P}$ мы сохраним для простых идеалов.

Пусть w — нормирование поля L; тогда формула $|a|_{\sigma w} = |\sigma^{-1}a|_w$ показывает, что σw — тоже нормирование поля L и $\sigma(\tau w) = (\sigma\tau)w$. Если $\mathfrak{O}_w$ — кольцо показателя w, то $\sigma\mathfrak{O}_w = \mathfrak{O}_{\sigma w}$. Автоморфизмы σ и σ^{-1} переводят друг в друга последовательности Коши для нормирований w и σw; следовательно, по непрерывности σ индуцирует изоморфизм σ_w: $L_w \cong L_{\sigma w}$ пополнений поля L соответственно по нормированиям w и σw. Если w является продолжением нормирования v поля K, то это верно и для σw; отображение σw устанавливает K_v-изоморфизм. Очевидно, что $\sigma_{\tau w} \circ \tau_w = (\sigma\tau)_w$.

Группой разложения G_w называется подгруппа

$$G_w = \{\sigma \in G \mid \sigma w = w\}$$

группы G. Заметим, что

$$G_{\tau w} = \{\sigma \in G \mid \sigma\tau w = \tau w\} = \tau G_w \tau^{-1}; \tag{1}$$

следовательно, группа разложения w с точностью до сопряжения определяется нормированием v. Любой элемент $\sigma \in G_w$ определяет K_v-автоморфизм L_w, и мы тем самым получаем вложение i группы G_w в $G(L_w/K_v)$.

1.2. Предложение. (i) *L_w/K_v есть расширение Галуа, и вложение i: $G_w \to G(L_w/K_v)$ является изоморфизмом.*

(ii) *Если w и w' — продолжения нормирования v поля K, то существует автоморфизм $\sigma \in G$, такой, что $\sigma w = w'$.*

Доказательство. Обозначим через $[X]$ мощность множества X. Имеют место неравенства

$$[G_w] \leqslant [G(L_w/K_v)] \leqslant [L_w : K_v],$$

причем эти неравенства обращаются в равенства тогда и только тогда, когда верно утверждение (i). Положим $r = [G : G_w]$ и обозначим через (σ_i), $1 \leqslant i \leqslant r$, систему представителей смежных классов $\sigma_i G_w$ подгруппы G_w в группе G. Положим $w_i = \sigma_i w$ для $1 \leqslant i \leqslant r$. Все w_i являются нормированиями поля L, лежащими над v; обозначим через w_i для $r+1 \leqslant i \leqslant s$ и все остальные нормирования, лежащие над v, если такие существуют. Тогда

$$[G] = r[G_w] = \sum_{i=1}^{r} [G_{w_i}] \leqslant \sum_{i=1}^{r} [L_{w_i} : K_v] \leqslant$$

$$\leqslant \sum_{i=1}^{s} [L_{w_i} : K_v] = [L : K] = [G];$$

следовательно, мы имеем сквозное равенство. Отсюда мы получаем $r = s$, что влечет за собой (ii) и $[G_w] = [L_w : K_v]$, что доказывает (i). (Тот факт, что сумма локальных степеней равна глобальной степени, следует из биективности отображения $L \otimes_K K_v \to \prod_{i=1}^{s} L_{w_i}$; нужно рассмотреть размерности над K_v (см. гл. II, § 10). Сюръективность этого отображения легко следует из теоремы о слабой аппроксимации.)

Обозначим через $\mathfrak{M}_K$ множество нормирований поля K. Тогда, так как отображение $\mathfrak{M}_L \to \mathfrak{M}_K$ сюръективно (любое нормирование поля K может быть продолжено до нормирования поля L), предложение 1.2 показывает, что $\mathfrak{M}_K \cong \mathfrak{M}_L/G$, т. е. нормирование поля K взаимно однозначно соответствует орбитам G на нормированиях поля L и для каждого нормирования w поля L его стационарная подгруппа G_w изоморфна группе Галуа локального расширения L_w/K_v.

§ 2. АВТОМОРФИЗМ ФРОБЕНИУСА

2.1. Предположим, что w — дискретное неразветвленное нормирование поля L, лежащее над некоторым нормированием v поля K. (Это верно для «почти всех» нормирований v, w, т. е. для всех, кроме конечного числа.) Тогда

$$G \supset G_w \cong G(L_w/K_v) \cong G(k(w)/k(v)), \qquad (1)$$

где $k(v)$ (соответственно $k(w)$) обозначает поле вычетов поля K (соответственно L) относительно v (соответственно w). Так как поля вычетов конечны, то группа Галуа $G(k(w)/k(v))$ — циклическая с канонической образующей

$$F\colon x \mapsto x^{Nv},$$

где $Nv = [k(v)]$ — «абсолютная норма». Следовательно, в силу (1) существует единственный элемент $\sigma_w \in G_w$, характеризуемый свойствами

$$\sigma_w \in G_w \quad \text{и} \quad a^{\sigma_w} \equiv a^{Nv} \pmod{\mathfrak{P}_w}$$

для всех $a \in \mathfrak{O}_w$. Автоморфизм σ_w называется *автоморфизмом Фробениуса*, соответствующим нормированию w. Из определений немедленно следует

2.2. Предложение.

$$\sigma_{\tau w} = \tau^{-1}\sigma_w\tau.$$

Поэтому автоморфизм Фробениуса определен нормированием v *с точностью до сопряжения*, и мы можем положить

$$F_{L/K}(v) = (\text{класс сопряженности } \sigma_w,\ w \mid v) = (\text{множество } \sigma_w \text{ для всех } w \mid v),$$

где $w \mid v$ означает, что w является продолжением v.

Если S — конечное множество нормирований поля K, содержащее все архимедовы и разветвленные в L/K нормирования, то $F_{L/K}$ является отображением $\mathfrak{M}_K - S$ в классы сопряженности группы $G(L/K)$.

2.3. Предложение. *Пусть $\sigma \in F_{L/K}(v)$ имеет порядок f, так что σ порождает подгруппу $\langle\sigma\rangle = \{1, \sigma, \ldots, \sigma^{f-1}\}$. Тогда v распадается в поле L на $[G:\langle\sigma\rangle]$ сомножителей, каждый из которых имеет степень*

$f = [k(w): k(v)]$. *В частности, v полностью распадается тогда и только тогда, когда $F_{L/K}(v) = 1$, где 1 — единичный элемент группы G.*

2.4. Замечание. Предложение утверждает, что знание класса $F_{L/K}$ дает нам закон разложения для неразветвленных нормирований и даже больше, так как оно позволяет выбрать определенные образующие групп разложения.

Так как $F_{L/K}$ является функцией на классах сопряженности группы G, то для определения $F_{L/K}$ достаточно знать $\chi(F_{L/K}(v))$ для всех характеров χ группы G. Поэтому Артин определил свои неабелевы L-ряды, исходя из характеров $\chi(F)$, при помощи которых доказывается фундаментальная *теорема Чеботарева о плотности*:

Пусть $\mathscr{C}$ — класс сопряженности в G; тогда нормирования v, для которых $F(v) = \mathscr{C}$, имеют плотность $[\mathscr{C}]/[G]$. В частности, для каждого класса сопряженности $\mathscr{C}$ существует бесконечное число нормирований v поля K, таких, что $F_{L/K}(v) = \mathscr{C}$.

Для круговых расширений теорема Чеботарева эквивалентна теореме Дирихле о простых числах в арифметических прогрессиях (см. ниже п. 3.4).

Из теоремы Чеботарева почти непосредственно следует, что конечное расширение Галуа L поля K однозначно определяется (с точностью до изоморфизма) множеством $\mathrm{Spl}(L/K)$ нормирований, полностью распадающихся в L (см. упражнение 6). К сожалению, мы не можем непосредственно определить, исходя из арифметики самого поля K, множество T нормирований поля K, входящих в $\mathrm{Spl}(L/K)$, за исключением случая абелевых расширений L/K. Закон разложения в абелевых расширениях вместе с полной классификацией таких расширений дан в приведенной ниже главной теореме (§ 5); но такая теорема неизвестна для неабелевых расширений, т. е. «неабелева теория полей классов» еще не создана. Из абелевой теории можно вывести закон разложения для некоторых разрешимых расширений (см. упражнение 2), но это не то, что мы искали. Недавно Шимура [12] дал явную форму закона разложения для некоторых неразрешимых расширений, полученных присоединением к $\mathbf{Q}$ точек порядка l на некоторой эллиптической кривой. Он связал поведение нормирований в таких расширениях с дзета-функцией кривой и отождествил дзета-функцию с модулярной функцией, коэффициенты q-разложения которой могут быть явно вычислены. Неясно, какова степень общности таких примеров и могут ли они быть отправной точкой общей теории; однако они могут по крайней мере играть роль контрольных проверок для различных гипотез.

§ 3. ЗАКОН ВЗАИМНОСТИ АРТИНА

3.1. Сначала мы введем некоторые обозначения. Через S будет обычно обозначаться *конечное* множество нормирований поля K, включающее все архимедовы нормирования. Если мы рассматриваем, в частности, конечное расширение L/K, то S будет содержать также нормирования, разветвленные в L. Мы будем обозначать через I^S свободную абелеву группу с образующими $\mathfrak{M}_K - S$ (подгруппу группы идеалов, см. гл. II, § 17).

Предположим теперь, что L/K — конечное абелево расширение. Тогда класс сопряженности группы $G = G(L/K)$ содержит один элемент, и поэтому $F_{L/K}$ отображает $\mathfrak{M}_K - S$ в G. По линейности мы можем расширить это отображение до гомоморфизма (тоже обозначаемого через $F_{L/K}$) I^S в G, полагая

$$F_{L/K}\Big(\sum_{v\notin S} n_v v\Big) = \prod_{v\notin S} F_{L/K}(v)^{n_v},$$

где n_v — целые числа и $n_v = 0$ для всех v, кроме конечного числа.

Первое предложение этого параграфа описывает, как меняется отображение $F_{L/K}$ при замене полей. Предположим, что L'/K' и L/K — абелевы расширения с группами Галуа G' и G соответственно, такие, что $L' \supset L$ и $K' \supset K$, и пусть θ — естественное отображение $G' \to G$ (любой автоморфизм L'/K' индуцирует автоморфизм L/K). Пусть S обозначает конечное множество нормирований поля K, включающее все архимедовы и все разветвленные нормирования в L', и пусть S' — такое же множество нормирований поля K'. Тогда имеет место

3.2. Предложение. *Диаграмма*

$$\begin{array}{ccc} I^{S'} & \xrightarrow{F_{L'/K'}} & G' \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle \theta} \\ I^{S} & \xrightarrow{F_{L/K}} & G \end{array}$$

коммутативна. (*N обозначает норменное отображение.*)

Доказательство. В силу линейности, очевидно, достаточно проверить равенство

$$\theta F_{L'/K'}(v') = F_{L/K}(N_{K'/K}v')$$

для произвольного нормирования v' поля K', такого, что $v' \notin S'$. Пусть $N_{K'/K}v' = fv$, где v — нормирование поля K, лежащее под v'; тогда $f = [k(v') : k(v)]$. Положим $\sigma' = F_{L'/K'}(v')$ и $\sigma = F_{L/K}(v)$. Мы должны показать, что $\theta(\sigma') = \sigma^f$. Автоморфизмы σ и σ' определены своим действием на поле вычетов. Пусть w' — нормирование поля L', лежащее над v', и пусть w — нормирование поля L, лежащее под w'. Для $x \in k(w) \subset k(w')$ мы имеем

$$x^{\sigma'} = x^{Nv'} = x^{(Nv)^f} = x^{\sigma^f},$$

что и требовалось.

Если $a \in K^*$ (т. е. если a — ненулевой элемент поля K), то мы положим

$$(a)^S = \sum_{v \notin S} n_v v,$$

где $n_v = v(a)$ для всех $v \notin S$, так что $a^{(S)}$ является элементом из I^S.

Мы можем теперь сформулировать закон взаимности в грубой форме.

3.3. Закон взаимности (грубая форма). *Если L/K — конечное абелево расширение и S — множество нормирований поля K, содержащее все архимедовы нормирования и все нормирования, разветвленные в L, то существует число $\varepsilon > 0$, такое, что если $a \in K^*$ и $|a - 1|_v < \varepsilon$ для всех $v \in S$, то $F((a)^S) = 1$.*

Иначе говоря, если элемент $a \in K^*$ близок к 1 для достаточно большого множества нормирований S, то $F((a)^S) = \prod_{v \notin S} F(v)^{v(a)} = 1$.

В случае числового поля подгруппа $(K_v^*)^n$ открыта в K^* для всех $n > 0$, и мы можем заменить условие $|a - 1|_v < \varepsilon$ на $a \in (K_v^*)^n$ для $v \in S$, где $n = [L : K]$. Действительно, если последнее условие выполнено, то по теореме о слабой аппроксимации существует $b \in K^*$, такое, что $|ab^{-n} - 1|_v < \varepsilon$ для всех $v \in S$, и тогда

$$F((a)^S) = F((b^n ab^{-n})^S) = F((b)^S)^n F((ab^{-n})^S) = 1.$$

Поэтому в случае числовых полей, хотя множество S зависит от L, окрестности 1 для всех нормирований из S зависят только от степени n поля L на K. В частности, для архимедовых нормирований условия вообще не нужны, за исключением случая вещественного v при четном n, где достаточно условия $a > 0$ в K_v.

Используя аппроксимационную теорему в поле L вместо поля K, можно заменить условие «a является локальной $[L : K]$-й степенью в множестве S» на «a является локальной нормой из L в K в множестве S», но для этого придется использовать технику иделей (см. ниже, п. 4.4 и 4.6). Переход от n-х степеней к нормам имеет решающее значение, мы им обязаны Гильберту.

3.4. Пример. *Закон взаимности для круговых расширений.* Закон взаимности может быть проверен непосредственно в случае кругового расширения $k = \mathbf{Q}$, $L = \mathbf{Q}(\zeta)$, где ζ обозначает первообразный корень m-й степени из единицы. Этот частный результат будет позже использован в одном из наших доказательств общего результата (см. ниже, § 10), так что мы приведем некоторые подробности. В случае поля рациональных чисел условимся обозначать простые числа через p, а соответствующие нормирования через v_p. Множество S будет состоять из архимедовых нормирований и p-адических нормирований для всех простых чисел p, делящих m (см. гл. III). Для $v_p \notin S$ и w, лежащего над p, степени ζ имеют *различные* образы в поле классов вычетов $k(w)$; поэтому мы имеем

Предложение.

$$F(v_p)\zeta = \zeta^p \text{ для всех } p \notin S.$$

Отсюда мы выводим

Следствие. *Если* $a \in \mathbf{Z}$, $a > 0$ *и* $(a, m) = 1$, *то* $F((a)^S)\,\zeta = \zeta^a$.

Поэтому если a — положительное рациональное число, причем $|a - 1|_p < |m|_p$ для всех $p \in S$, то a является целым p-адическим числом для всех p, делящих m, и мы можем положить $a = b/c$, причем $(b, m) = (c, m) = 1$ и $b \equiv c \pmod{m}$; значит, $\zeta^b = \zeta^c$, и потому $F((b)^S)\,\zeta = \zeta^b = \zeta^c = F((c)^S)\,\zeta$. По линейности это дает нам $F((a)^S)\,\zeta = \zeta$, так что $F((a)^S) = 1$.

Другие примеры явного описания $F_{L/K}$, а также связь между общим законом взаимности Артина и классическим квадратичным законом взаимности можно найти в упражнении 1.

3.5. Замечание. Случай круговых расширений очень прост, потому что легко выразить действие $F(v)$ для различных v на корнях из единицы. Различные непосредственные доказательства для абелевых расширений комплексных квадратичных полей используют вместо корней из единицы точки конечного порядка и модулярные инварианты эллиптических кривых с комплексным умножением. В общем случае такое доказательство неизвестно (12-я проблема Гильберта), хотя Шимура, Таниями и Вейль получили важные результаты, используя абелевы многообразия вместо эллиптических кривых (см. [3], [14] и более новую работу [13]). Доказательство закона взаимности в общем случае косвенное; фактически показывается, что закон выполняется, «потому что иначе быть не может».

3.6. Замечание. В случае функционального поля, как показал Ленг [5], закон взаимности связан с геометрической теоремой о поле $K = k(C)$ кривой C. Серр выполнил подробно программу, начатую Ленгом. В книге Серра [6] аналог закона взаимности описывается следующим образом. Пусть $f : C \to G$ — рациональное отображение неособой кривой C в коммутативную алгебраическую группу G; обозначим через S конечное множество точек из C, в которых f нерегулярно. Тогда f индуцирует гомоморфизм группы дивизоров I^S в G и имеет место

Теорема. *Если* $\phi \in K$ *принимает значение* 1 *в каждой точке из* S, *то* $f((\phi)) = 1$.

Эта теорема доказана Розенлихтом и независимо от него, но позже Серром. Серр и Ленг применили ее к теории полей классов.

3.7. Определение. Пусть K — глобальное поле, S — конечное множество нормирований поля K, включающее все архимедовы, и G — коммутативная топологическая группа. Гомоморфизм ϕ: $I^S \to G$ называется *допустимым*, если для каждой окрестности N единичного элемента 1 группы G существует число $\varepsilon > 0$, такое, что $\phi((a)^S) \in N$ всякий раз, когда $a \in K^*$ и $|a - 1|_v < \varepsilon$ для всех $v \in S$.

Если G — дискретная группа, мы примем за N просто (1). Тогда справедлива

3.8. Переформулировка закона взаимности: $F_{L/K}$ — *допустимое отображение*.

В нашем контексте конечная группа $G = G(L/K)$ дискретна. Если G — группа вращений окружности, то ϕ допустимо тогда и только тогда, когда оно является характером Гекке (если образ ϕ — конечная подгруппа, то ϕ будет характером Дирихле). Дирихле и Гекке построили из таких характеров L-ряды; Артин был вынужден сначала вывести свой закон взаимности для того, чтобы показать, что в абелевом случае его L-ряды, определенные исходя из характеров группы Галуа, на самом деле совпадают с L-рядами Вебера, иначе говоря, что $\chi(F(v))$ допустимо для каждого линейного характера χ абелевой группы Галуа.

§ 4. ИНТЕРПРЕТАЦИЯ ШЕВАЛЛЕ НА ИДЕЛЯХ

Множество элементов группы иделей J_K (см. гл. II, § 16), которые принимают значение 1 во всех v-компонентах, $v \in S$, обозначим через J_K^S. Если $x \in J_K$, то только конечное число v-компонент иделя x не является единицами; обозначим показатель v-компоненты x_v иделя x через

$n_v \in \mathbf{Z}$ и положим

$$(x)^S = \sum_{v \notin S} n_v v \in I^S.$$

4.1. Предложение. *Пусть K и S обозначают то же, что и выше; пусть, далее, G — полная коммутативная топологическая группа и ϕ — допустимый гомоморфизм I^S в G.*

Тогда существует единственный гомоморфизм ψ: $J_K \to G$, такой, что

(i) *ψ непрерывен;*

(ii) $\psi(K^*) = 1$;

(iii) $\psi(x) = \phi((x)^S)$ *для всех* $x \in J_K^S$.

Обратно, если ψ — непрерывный гомоморфизм $J_K \to G$, такой, что $\psi(K^*) = 1$, он получается из некоторой допустимой пары S, ϕ, как указано выше, если только существует окрестность элемента 1 в G, в которой содержится лишь единичная подгруппа группы G.

Замечание. Ясно, что если такое ψ существует, то оно индуцирует непрерывный гомоморфизм группы классов иделей $C_K \simeq J_K/K^*$ в G. Этот индуцированный гомоморфизм мы тоже будем обозначать через ψ. Более того, если такое ψ существует для данных ϕ и S, то оно не изменится, если S увеличить до большего множества S' и ϕ заменить на его ограничение ϕ' на $I^{S'} \subset I^S$. Точно так же два отображения ϕ множества I^S, совпадающие на $I^{S'}$ для некоторого конечного $S' \supset S$, на самом деле совпадают на I^S (см. упражнение 7).

В приложениях G будет дискретной группой или группой вращения окружности.

Доказательство. Предположим, что у нас есть допустимое отображение ϕ: $I^S \to G$. Если искомое ψ существует, то для любого $a \in K^*$ и $x \in J_K$ мы будем иметь

$$\psi(x) = \psi(ax) = \psi((ax)_1)\,\psi((ax)_2),$$

где $(ax)_1$ обозначает идель с теми же v-компонентами, что и ax, для всех $v \in S$, и с остальными компонентами, равными 1, а $(ax)_2$ — идель с теми же v-компонентами, что и ax, для всех $v \notin S$, и с v-компонентами, равными 1, для $v \in S$ (так что $(ax)_2 \in J_K^S$). По слабой аппроксимационной теореме

(см. гл. II, § 6) мы можем найти последовательность $\{a_n\}$ элементов $a_n \in K^*$, таких, что $a_n \to x^{-1}$ при $n \to \infty$ для всех $v \in S$. Тогда

$$\psi(x) = \lim_{n\to\infty} \psi((a_n x)_1) \cdot \phi((a_n x)^S) = \lim_{n\to\infty} \phi((a_n x)^S).$$

Следовательно, по данному ϕ функция ψ определяется формулой

$$\psi(x) = \lim_{n\to\infty} \phi((a_n x)^S). \tag{1}$$

Если $n, m \to \infty$, то $a_n/a_m \to 1$ для всех $v \in S$ и, следовательно,

$$\frac{\phi((a_n x)^S)}{\phi((a_m x)^S)} = \phi\left(\left(\frac{a_n}{a_m}\right)^S\right) \to 1$$

в G, потому что ϕ допустимо. Такой предел существует, так как G — полная группа, и этот предел не зависит от выбора последовательности $\{a_n\}$, потому что он существует для всех таких последовательностей. При этом отображение ψ непрерывно. Если компоненты иделя x являются единицами при $v \notin S$, то $\psi(x) = \lim \phi((a_n)^S)$; если, кроме того, компоненты иделя x достаточно близки к 1 при $v \in S$, то будут близки к 1 и компоненты главного иделя a_n при больших n, и так как ϕ допустимо, то $\phi((a_n)^S)$ будет близко к единице в G. Последние два условия (ii) и (iii) легко проверить, положив $a_n = x^{-1}$ и 1 для всех n соответственно.

Предположим теперь, что задан непрерывный гомоморфизм ψ: $J_K \to G$, такой, что $\psi(K^*) = 1$. Мы найдем множество S, такое, что: (а) ограничение ψ на J_K^S получается из некоторой функции на I^S; (б) если мы обозначим эту функцию через ϕ, то ϕ — допустимый гомоморфизм.

Для любого конечного множества S нормирований поля K обозначим через U^S множество иделей в J_K с v-компонентами, равными 1 для всех $v \in S$ и единице из K_v для $v \notin S$. Выбирая S достаточно большим, мы можем сделать U^S произвольно малой окрестностью единицы в J_K. Если N — окрестность (1), то мы можем выбрать S достаточно большим, чтобы $\psi(U^S) \subseteq N$, так как ψ непрерывно. Тогда, взяв окрестность достаточно малой, мы видим, что $\psi(U^S) = (1)$ для некоторого множества S в силу предположения об отсутствии «маленьких» подгрупп. Мы выбираем такое множество S. Теперь J_K^S/U^S канонически изоморфно I^S,

и поэтому ψ, ограниченное на J_K^S, индуцирует непрерывный гомоморфизм ϕ из I^S в G.

Осталось проверить, что ϕ допустимо, т. е. что если дана окрестность N, то $\psi((a)^S) \in N$ всякий раз, когда $a \in K^*$ достаточно близко к 1 для всех $v \in S$. Но в этом случае $(a)^S$ близко к a в J_K и, значит, по непрерывности ψ $((a)^S)$ близко к ψ (a), которое равно 1, так как $a \in K^*$.

4.2. Следствие. *Закон взаимности выполняется для конечного абелева расширения L поля K тогда и только тогда, когда существует непрерывный гомоморфизм ψ: $J_K \to G(L/K)$, такой, что*

(i) ψ *непрерывно*;

(ii) $\psi(K^*) = 1$;

(iii) $\psi(x) = F_{L/K}((x)^S)$ *для всех* $x \in J_K^S$, *где* S *состоит из архимедовых и разветвленных в* L *нормирований поля* K.

Такое отображение $\psi = \psi_{L/K}$, существование которого мы постулировали, называется *отображением Артина*, соответствующим расширению L/K. Оно было определено как отображение $J_K \to G(L/K)$; но так как оно тривиально на K^*, то его можно рассматривать как отображение группы классов иделей $C_K = J_K/K^*$ в $G(L/K)$.

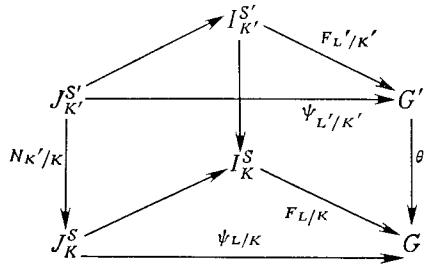
Закон взаимности для конечного абелева расширения будет доказан позже (см. § 10). Однако уже сейчас будут доказаны некоторые утверждения и сделаны некоторые замечания, вытекающие из этого закона. Предположим, что L'/K' и L/K — абелевы расширения с группами Галуа G' и G соответственно и что $L' \supset L$, $K' \supset K$. Пусть θ — естественное отображение $G' \to G$. Тогда в терминах иделей и отображений Артина предложение 3.1 принимает следующий вид:

4.3. Предложение. *Если закон взаимности выполняется для L/K и L'/K', то диаграмма*

$$\begin{array}{ccc} J_{K'} & \xrightarrow{\psi_{L'/K'}} & G' \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle \theta} \\ J_K & \xrightarrow{\psi_{L/K}} & G \end{array}$$

коммутативна.

Доказательство. Пусть S — достаточно большое множество нормирований поля K, а S' — то же для поля K'. Мы имеем коммутативную диаграмму



(2)

Непрямоугольные параллелограммы коммутативны в силу согласованности норм идеалов и иделей и в силу предложения 3.2. Треугольники коммутативны, согласно следствию 4.2, (iii). Таким образом, прямоугольник тоже коммутативен, т. е. ограничения $\psi_{L/K} \circ N_{K'/K}$ и $\theta \circ \psi_{L'/K'}$ на $J_{K'}^{S'}$ совпадают. Но эти два гомоморфизма принимают значение 1 на главных иделях в силу 4.2, (ii), так что они совпадают на множестве $(K')^* J_{K'}^{S'}$, которое является всюду плотным подмножеством $J_{K'}$ по слабой аппроксимационной теореме (гл. II, § 6). Так как оба гомоморфизма непрерывны, они совпадают на всем $J_{K'}$, что мы и хотели доказать.

Для доказательства предложения 6.2, которое необходимо для первого из двух наших доказательств закона взаимности в § 10.4, нам нужен следующий

Вариант. *Предположим, что L/K удовлетворяет закону взаимности и $K \subset M \subset L$. Тогда $\psi_{L/K}(N_{M/K} J_M) \subset G(L/M)$.*

Рассмотрим диаграмму (2) при $L' = L$, $K' = M$, но без верхней горизонтальной стрелки $\psi_{L'/K'} = \psi_{L/M}$. Отсюда видно, что

$$\psi_{L/K}(N_{M/K} J_M^{S'}) \subset G' = G(L/M).$$

Следовательно, то же самое верно при замене $J_M^{S'}$ на $M^* J_M^{S'}$, а так как это множество плотно в J_M, то доказательство закончено.

4.4. Следствие. *Если закон взаимности выполняется для L/K, то*

$$\psi_{L/K}(N_{L/K}J_L) = 1.$$

Отсюда следует, что $\psi_{L/K}(K^*N_{L/K}J_L) = 1$; следующая теорема утверждает, в частности, что $K^*N_{L/K}J_L$ является ядром отображения $\psi_{L/K}$.

§ 5. ФОРМУЛИРОВКА ГЛАВНОЙ ТЕОРЕМЫ ДЛЯ АБЕЛЕВЫХ РАСШИРЕНИЙ

5.1. Главная теорема для абелевых расширений (Такаги — Артин).

(А) *Любое абелево расширение L/K удовлетворяет закону взаимности (т. е. существует отображение Артина $\psi_{L/K}$).*

(Б) *Отображение Артина $\psi_{L/K}$ сюръективно с ядром $K^*N_{L/K}(J_L)$ и, следовательно, оно индуцирует изоморфизм $C_K/N_{L/K}C_L$ на $G(L/K)$.*

(В) *Если $M \supset L \supset K$ — абелевы расширения, то диаграмма*

$$\begin{array}{ccc} C_K/N_{M/K}C_M & \xrightarrow{\psi_{M/K}} & G(M/K) \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle \theta} \\ C_K/N_{L/K}C_L & \xrightarrow{\psi_{L/K}} & G(L/K) \end{array}$$

коммутативна (здесь θ обозначает обычное отображение, а j — естественный эпиморфизм, который существует в силу $N_{M/K}C_M \subset N_{L/K}C_L$).

(Г) (*Теорема существования.*) *Для любой открытой подгруппы N конечного индекса в C_K существует единственное абелево расширение L/K (в фиксированном алгебраическом замыкании K), такое, что $N_{L/K}C_L = N$.*

Подгруппа N в (Г) называется *норменной подгруппой*, а абелево расширение L, такое, что $N_{L/K}C_L = N$, называется *полем классов*, принадлежащим подгруппе N. В случае числового поля любая открытая подгруппа C_K имеет в ней конечный индекс.

5.2. Некоторые утверждения этой теоремы могут быть легко выведены из остальных. Во-первых, если выполняются (А) и (Б), то (В) — частный случай предложения 4.3 (при $K' = K$ и $L' = M$).

5.3. Во-вторых, единственность соответствия, приведенного в (Г), следует из остальных утверждений. Пусть существуют два конечных абелевых расширения L и L' поля K в фиксированном алгебраическом замыкании поля K, и пусть M — их композит (тоже являющийся конечным абелевым расширением поля K). Рассмотрим теперь коммутативную диаграмму, приведенную в пункте (В). Так как горизонтальные стрелки представляют изоморфизмы (по (Б)), то мы видим, что $\ker\theta = G(M/L)$ является изоморфным образом относительно $\psi_{M/K}$ группы $N_{L/K}C_L/N_{M/K}C_M$. Поэтому L, как поле инвариантных элементов группы $\ker\theta$, однозначно определяется по $N_{L/K}C_L$ как подполе поля M. Применяя те же рассуждения к полю L' вместо L, мы видим, что $N_{L'/K}C_{L'} = N_{L/K}C_L$, так что $L = L'$.

О некоторых особых примерах полей классов (гильбертовы поля классов) см. упражнение 3.

О функториальных свойствах отображения Артина при замене основного поля K см. ниже, п. 11.5.

5.4. Коммутативная диаграмма из (В) позволяет нам перейти к проективному пределу (см. гл. III, § 1), когда L пробегает все конечные абелевы расширения поля K. Мы получаем гомоморфизм

$$\psi_K : C_K \to \varprojlim_L G(L/K) \simeq G(K^{ab}/K),$$

где K^{ab} обозначает максимальное абелево расширение поля K, следовательно, согласно (Г),

$$G(K^{ab}/K) \simeq \varprojlim_N (C_K/N),$$

где предел берется по всем открытым подгруппам N конечного индекса в C_K. Таким образом, по группе классов иделей поля K мы можем узнать группы Галуа всех абелевых расширений поля K. Структура гомоморфизма ψ_K: $C_K \to$

$\to G(K^{ab}/K)$ довольно различна в функциональном и числовом случаях. Следующие утверждения не выводятся непосредственно из главной теоремы, однако их доказательство мы опускаем.

5.5. *Случай функционального поля.* Здесь отображение ψ_K является вложением и его образ — всюду плотная подгруппа $G(K^{ab}/K)$, состоящая из тех автоморфизмов, ограничение которых на алгебраическое замыкание $\bar{k}$ поля констант k является просто целой степенью автоморфизма Фробениуса F_k (см. [1], стр. 76).

5.6. *Случай числового поля.* Здесь ψ_K — эпиморфизм и его ядро — связная компонента D_K группы C_K. Тем самым мы имеем канонический изоморфизм $C_K/D_K \cong G(K^{ab}/K)$.

Однако, как подчеркивал Вейль [3], нам нужна интерпретация на языке теории Галуа *всей* группы C_K. Связная компонента D_K может быть очень сложной (см. [1], стр. 82).

5.7. Пример. *Круговые поля.* Рассмотрим $\mathbf{Q}^{mc}/\mathbf{Q}$ — максимальное круговое расширение $\mathbf{Q}$. Пусть $\hat{\mathbf{Z}} = \varprojlim_n \mathbf{Z}/n\mathbf{Z}$; по «китайской теореме об остатках» эта группа изоморфна $\prod_p \mathbf{Z}_p$, где $\mathbf{Z}_p$ — кольцо целых p-адических чисел. $\hat{\mathbf{Z}}$ действует на любой абелевой группе кручения (ибо $\mathbf{Z}/n\mathbf{Z}$ действует на любой абелевой группе, показатель которой делит n) и обратимые элементы в $\hat{\mathbf{Z}}$ совпадают с $\prod_p U_p$, где U_p — множество p-адических единиц в $\mathbf{Z}_p$.

Теперь рассмотрим группу кручения μ, состоящую из всех корней из единицы. Если $\zeta \in \mu$, то мы можем определить ζ^u для всех $u \in \prod_p U_p$; при этом u индуцирует автоморфизм на μ. Группа иделей $J_{\mathbf{Q}}$ изоморфна прямому произведению $\mathbf{Q}^* \times \mathbf{R}_+^* \times \prod_p U_p$. (Действительно, если $x = \{x_\infty, x_2, x_3, \ldots\} \in J_{\mathbf{Q}}$, то $x = a \cdot \{t, u_2, u_3, \ldots\}$, где

$$a = (\operatorname{sign} x_\infty) \prod_p p^{v_p(x_p)} \in \mathbf{Q}^*$$

и где $t > 0$, $u_p \in U_p$ при $p = 2, 3, \ldots$; более того, это разложение единственно, ибо 1 — единственное положительное рациональное число, которое является p-адической единицей для всех простых p.) Значит, $C_{\mathbf{Q}}$ канонически изоморфно $\mathbf{R}_+^* \times \prod_p U_p$, так что существует отображение $C_{\mathbf{Q}}$ на $\prod_p U_p$, которое изоморфно группе Галуа максимального кругового расширения.

Фактически имеет место следующее. Если $x \in C_{\mathbf{Q}}$ и $x \mapsto u$ при этом отображении, то $\zeta^{\psi(x)} = \zeta^{u^{-1}}$ (это легкое упражнение, вытекающее из 3.4 и не зависящее от утверждений (Б) и (Г) главной теоремы). Поэтому ядро ψ совпадает с $\mathbf{R}_+^*$ — связной компонентой $D_{\mathbf{Q}}$ группы $C_{\mathbf{Q}}$. Мы теперь знаем структуру $C_{\mathbf{Q}}/D_{\mathbf{Q}}$; таким образом, если справедливо утверждение (Б) главной теоремы, любое абелево расширение поля $\mathbf{Q}$ является подполем поля $\mathbf{Q}^{mc}$, и утверждение (Г) выполняется для абелевых расширений поля $\mathbf{Q}$.

Связная компонента $\mathbf{R}_+^*$ в $C_{\mathbf{Q}}$ неинтересна; аналогично C_K имеет неинтересную связную компоненту, когда K — комплексное квадратичное поле, так как в этом случае существует только одно архимедово нормирование. Возможно, что именно связная компонента препятствует проведению простого доказательства закона взаимности в общем случае.

§ 6. СООТНОШЕНИЕ МЕЖДУ ГЛОБАЛЬНЫМ И ЛОКАЛЬНЫМ ОТОБРАЖЕНИЯМИ АРТИНА

Мы продолжаем выводить результаты из предположения, что закон взаимности (но не обязательно вся главная теорема из § 5) верен для абелева расширения L/K.

6.1. Для каждого нормирования v поля K обозначим через K_v пополнение поля K относительно v. Если L/K — конечное расширение Галуа, то различные пополнения L_w для $w \mid v$ изоморфны. Условимся обозначать через L^v какое-либо из пополнений L_w для $w \mid v$ и положим, что $G^v = G(L^v/K_v)$ — локальная группа Галуа, которую можно отождествить с подгруппой разложения группы G (см. п. 1.2). В абелевом случае эта подгруппа не зависит от выбора w.

Предположим, что расширение L/K абелево и что существует отображение Артина

$$\psi_{L/K} : J_K \longrightarrow G(L/K) = G.$$

Для каждого нормирования v поля K мы имеем

$$K_v^* \underset{j_v}{\overset{i_v}{\rightleftarrows}} J_K \xrightarrow{\psi_{L/K}} G,$$

где i_v отображает $x \in K_v^*$ в элемент J_K, у которого v-компонента равна x, а остальные компоненты равны 1; j_v обозначает проекцию на v-компоненту. Положим $\psi_v = \psi_{L/K} \circ i_v$, так что $\psi_v : K_v^* \longrightarrow G$. Имеет место следующее

6.2. Предложение. *Если* $K_v \subset \mathscr{M} \subset L^v$, *то* $\psi_v(N_{\mathscr{M}/K_v}\mathscr{M}^*) \subset G(L^v/\mathscr{M})$. *В частности,* $\psi_v(K_v^*) \subset G^v$ *и* $\psi_v(N_{L^v/K_v}(L^v)^*) = 1$.

Доказательство. Пусть $M = L \cap \mathscr{M}$ — поле инвариантных элементов группы $G(L^v/\mathscr{M})$ в L, так что $G(L/M)$ отождествляется с $G(L^v/\mathscr{M})$ при нашем отождествлении группы разложения с локальной группой Галуа. Тогда $\mathscr{M} = M_w$, где $w \mid v$, и диаграмма

$$\begin{array}{ccc} \mathscr{M} = M_w & \xrightarrow{i_w} & J_M \\ {\scriptstyle N_{\mathscr{M}/K_v}}\downarrow & & \downarrow{\scriptstyle N_{M/K}} \\ K_v & \xrightarrow{i_v} & J_K \end{array}$$

коммутативна. В силу «варианта» 4.3 мы заключаем, что

$$\psi_v(N_{\mathscr{M}/K_v}\mathscr{M}^*) \subset \psi_{L/K} N_{M/K} \subset G(L/M) \cong G(L^v/\mathscr{M}).$$

6.3. Мы будем называть ψ_v: $K_v^* \to G^v$ *локальным гомоморфизмом Артина* или его классическим названием: *гомоморфизм норменного вычета*. Если $x = (x_v) \in J_K$, то мы имеем

$$x = \lim_S \left\{ \prod_{v \in S} i_v(x_v) \right\},$$

и, следовательно, по непрерывности

$$\psi_{L/K}(x) = \prod_v \psi_v(x_v)$$

(это произведение на самом деле конечно, так как если x_v является v-единицей и v не разветвлено, то x_v является нормой в L^v/K_v. Таким образом, знание всех локальных отображений Артина ψ_v эквивалентно знанию глобального отображения Артина $\psi_{L/K}$. В классических работах локальные отображения изучались при помощи глобальной теории; в частности, было показано, что они зависят только от локального расширения L^v/K_v и не зависят от глобального расширения L/K, из которого они были выведены. Теперешний образ действия прямо противоположен; сначала дается чисто локальная конструкция (см. гл. VI) отображений $\theta_v : K_v^* \to G_v = G(L^v/K_v)$. Мы рассмотрим эти отображения θ_v и покажем, что $\prod_v \theta_v$ удовлетворяет характеристическим свойствам отображения ψ, в частности, $\prod_v \theta_v(a) = 1$ для всех $a \in K^*$ (см. § 10).

Локальная теория говорит нам, что главная теорема 5.1 верна локально, если заменить C_K на K_v^*, ψ на ψ_v и $G(L/K)$ на $G(L^v/K_v)$. В частности,

$$K_v^*/NL^{v*} \cong G(L^v/K_v),$$

и при этом изоморфизме группы ветвления соответствуют стандартной фильтрации на K_v^*/NL^{v*}. Возвращаясь к глобальной теории, мы получаем полное описание разложения нормирований в терминах классов иделей даже в разветвленном случае.

По вопросу об абелевых и циклических расширениях с рассмотрением локального поведения и теоремы Грюнвальда — Ванга см. [1], гл. X, и [2].

6.4. Мы можем теперь привести более точную, чем в п. 3.3, формулировку закона взаимности.

Закон взаимности (строгая форма). *Пусть* L/K — *абелево расширение, и пусть* S *состоит из всех архимедовых и разветвленных в* L *нормирований поля* K. *Если элемент* $a \in K^*$ *является нормой из* L^v *для всех* $v \in S$, *то* $F_{L/K}((a)^S) = 1$.

Действительно, если $j_v(a)$ является нормой при $v \in S$, то для некоторого $b_v \in L^v$ имеет место $j_v(a) = N_{L^v/K_v}(b_v)$. Тогда из следствия 4.2 вытекает в силу предложения 6.2, что

$$1 = \psi((a)^S) \cdot \prod_{v \in S} \psi_v(j_v(a)) =$$

$$= F_{L/K}((a)^S) \cdot \prod_{v \in S} \psi_v(N_{L^v/K_v}(b_v)) = F_{L/K}((a)^S).$$

О конкретном описании локальных отображений Артина ψ_v при помощи символа норменного вычета $(a, b)_v$ в случае куммеровых расширений и о применении общего закона взаимности n-й степени см. упражнение 2.

§ 7. КОГОМОЛОГИИ ИДЕЛЕЙ

7.1. Пусть L/K — конечное нормальное расширение, не обязательно абелево, с группой Галуа G. Обозначим через A_L кольцо аделей поля L; тогда J_L — группа обратимых элементов $A_L = L \underset{K}{\otimes} A_K$, и G действует на $L \underset{K}{\otimes} A_K$ по формуле $\sigma \mapsto \sigma \otimes 1$; так же G действует на J_L.

Мы хотим, однако, рассмотреть действие G на структуре прямого произведения J_L. Предположим, что $x \in J_L$, тогда $x = (x_w)$, где w пробегает $\mathfrak{M}_L$; автоморфизм $\sigma \in G$ индуцирует $\sigma_w : L_w \to L_{\sigma w}$ (см. п. 1.1) и $(\sigma x)_{\sigma w} = \sigma_w x_w$, так что диаграммы

$$\begin{array}{ccc} L_w^* & \xrightarrow{\sigma_w} & L_{\sigma w}^* \\ {\scriptstyle i_w}\downarrow & & \downarrow{\scriptstyle i_{\sigma w}} \\ J_L & \xrightarrow{\sigma} & J_L \end{array} \qquad \begin{array}{ccc} L_w^* & \xrightarrow{\sigma_w} & L_{\sigma w}^* \\ {\scriptstyle j_w}\downarrow & & \downarrow{\scriptstyle j_{\sigma w}} \\ J_L & \xrightarrow{\sigma} & J_L \end{array}$$

коммутативны. (Заметим, что образ L_w^* в J_L не образует G-инвариантной подгруппы: наименьшей такой подгруппой, содержащей L_w^*, является $\prod_{w|v} L_w^*$.)

7.2. Предложение. *Пусть $v \in \mathfrak{M}_K$ и $w_0 \in \mathfrak{M}_L$, где $w_0 \mid v$. Тогда существуют взаимно обратные изоморфизмы*

$$H^r(G, \prod_{w|v} L_w^*) \underset{j_{w_0} \cdot \mathrm{Res}}{\overset{\mathrm{Cores} \cdot i_{w_0}}{\rightleftarrows}} H^r(G_{w_0}, L_{w_0}^*)$$

и

$$H^r(G, \prod_{w|v} U_w) \underset{j_{w_0} \cdot \mathrm{Res}}{\overset{\mathrm{Cores} \cdot i_{w_0}}{\rightleftarrows}} H^r(G_{w_0}, U_{w_0}),$$

где U_w обозначает подгруппу единиц в L_w.

Утверждение остается верным при замене H^r на $\hat{H}^r$.

Доказательство немедленно следует из леммы Шапиро (см. гл. IV, § 4) в силу предложения 1.2.

Таким образом, группы когомологий $H^r(G_w, L_w^*)$ канонически изоморфны для всех $w \mid v$, поэтому можно использовать обозначение $H^r(G^v, (L^v)^*)$ для любой из них.

7.3. Предложение. (а) $J_K \cong J_L^G$, *где J_L^G — группа аделей поля L, инвариантных относительно всех элементов группы G.*

(б) $$\hat{H}^r(G, J_L) \cong \prod_{v \in \mathfrak{M}_K} \hat{H}^r(G^v, (L^v)^*),$$

где $\prod$ обозначает прямую сумму.

Доказательство. (а) очевидно следует из гл. II, § 19. Для доказательства утверждения(б) мы заметим, что

$$J_L = \varinjlim_S J_{L,S}, \text{ где } J_{L,S} = \prod_{v \in S} \left(\prod_{w|v} L_w^*\right) \prod_{v \notin S} \left(\prod_{w|v} U_w\right), \qquad (1)$$

а S — конечное множество нормирований, содержащее все разветвленные в L и все архимедовы нормирования. Предел берется по возрастающей последовательности S, такой, что $\lim S = \mathfrak{M}_K$. Когомологии конечных групп коммутируют со взятием индуктивного предела, и любые когомологии коммутируют с прямым произведением, так что достаточно рассмотреть когомологии различных частей. В силу предложения 7.2 и п. 1.4 гл. VI $\prod_{v \notin S} \left(\prod_{w|v} U_w\right)$ имеет тривиальные когомологии, если S содержит все разветвленные нормирования. Следовательно, в силу предложения 7.2

$$\hat{H}^r(G, J_{L,S}) \cong \prod_{v \in S} \hat{H}^r(G^v, (L^v)^*).$$

При $S \to \mathfrak{M}_K$ мы находим, что

$$\hat{H}^r(G, J_L) \cong \prod \hat{H}^r(G^v, (L^v)^*).$$

7.4. Следствие.

(а) $H^1(G, J_L) = 0$;

(б) $H^2(G, J_L) \cong \coprod_v \left(\frac{1}{n_v}\mathbf{Z}/\mathbf{Z}\right)$, *где* $n_v = [L^v : K_v]$.

Первое утверждение следует из «теоремы Гильберта 90» для локальных полей (см. гл. V, п. 2.6, и гл. VI, п. 1.4), а второе — из определения группы Брауэра поля K_v в гл. VI, п. 1.6.

§ 8. КОГОМОЛОГИИ КЛАССОВ ИДЕЛЕЙ

I. ПЕРВОЕ НЕРАВЕНСТВО

Рассмотрим точную последовательность $0 \to L^* \to J_L \to C_L \to 0$. Действие группы G на G_L индуцировано ее действием на J_L.

8.1. Предложение. $C_K \cong C_L^G$.

Доказательство. Указанная выше точная последовательность порождает когомологическую последовательность

$$0 \to H^0(G, L^*) \to H^0(G, J_L) \to H^0(G, C_L) \to H^1(G, L^*),$$

т. е.

$$0 \to K^* \to J_K \to C_L^G \to 0.$$

8.2. Замечание. Нашей целью является определение в абелевом случае отображения

$$\psi_{L/K} : C_K/N_{L/K}C_L \to G(L/K) = G.$$

В силу предложения 8.1 $C_K/N_{L/K}C_L = \hat{H}^0(G, C_L)$, с другой стороны, $G = \hat{H}^{-2}(G, \mathbf{Z})$. Сравнение с п. 2.1 гл. VI подсказывает, что глобальная теорема о когомологиях C_L, которую мы хотим доказать, по существу аналогична локальной теореме Серра о когомологиях L^*. Это имеет место на самом деле. Абстрагируя общие свойства, мы приходим к понятию «формации классов» (class formation) (см. [1]).

Вспомним, что если группа G — циклическая и A является G-модулем, то *индекс Эрбрана* определяется так: $h(G, A) = [H^2(G, A)]/[H^1(G, A)]$, если порядки групп $[H^2(G, A)]$ и $[H^1(G, A)]$ конечны (см. гл. IV, § 8).

8.3. Теорема. *Пусть L/K — циклическое расширение степени n. Тогда $h(G, C_L) = n$.*

Доказательство. Выберем конечное множество S нормирований поля K достаточно большим, чтобы можно было считать $J_L = L^* \cdot J_{L,S}$, где

$$J_{L,S} = \coprod_{v \in S} \left(\prod_{w|v} L_w^*\right) \times \coprod_{v \notin S} \left(\prod_{w|v} U_w\right).$$

Более точно, S содержит все архимедовы нормирования поля K, все нормирования, разветвленные в L, и все делители некоторой системы образующих группы классов дивизоров поля L. Обозначим через T множество нормирований поля L, лежащих над нормированиями из S. Тогда

$$C_L \cong J_L/L^* \cong J_{L,S}/(L^* \cap J_{L,S}) = J_{L/S}/L_T,$$

где $L_T = L^* \cap J_{L,S}$ — множество T-единиц в L, т. е. тех элементов поля L, которые являются единицами в L_w для всех $w \notin T$. Отсюда следует, что

$$h(C_L) = h(J_{L,S})/h(L_T),$$

если правая часть определена (заметим, что если S не задано, то приведенное выше равенство использовать невозможно, так как тогда правая часть не определена).

Прежде всего мы определим $h(J_{L,S})$. Так как S содержит все разветвленные нормирования, то группа $\coprod_{v \notin S} \left(\prod_{v|w} U_w\right)$ имеет тривиальные когомологии, как было отмечено в 7.3. Следовательно,

$$h(J_{L,S}) = h\left(\coprod_{v \in S} \left(\prod_{w|v} L_w^*\right)\right) = \coprod_{v \in S} h\left(\prod_{w|v} L_w^*\right),$$

так что в силу предложения 7.2 мы имеем $h(J_{L,S}) = \coprod_{v \in S} n_v$, где n_v — локальная степень (см. гл. VI, п. 1.4). Это завершает «локальную часть» доказательства.

«Глобальная часть» состоит в определении $h(L_T)$; для того чтобы доказать, что $h(C_L) = n$, мы должны показать, что $nh(L_T) = \prod_{v \in S} n_v$. Мы сделаем это, построив вещественное векторное пространство, на котором действует G, с двумя решетками, причем индекс Эрбрана одной из них равен $nh(L_T)$, а другой — $\prod_{v \in S} n_v$.

Пусть V — вещественное векторное пространство отображений $f\colon T \to R$, так что $V \cong \mathbf{R}^t$, где $t = [T]$ ($[T]$ — мощность множества T). Мы заставим G действовать на V по формуле $(\sigma f)(w) = f(\sigma^{-1}w)$ (так что $(\sigma f)(\sigma w) = f(w)$) для всех $f \in V$, $\sigma \in G$ и $w \in T$.

Положим $N = \{f \in V \mid f(w) \in \mathbf{Z}$ для всех $w \in T\}$. Ясно, что N порождает V и что G инвариантно. Мы имеем: $N \cong \prod_{v \in S} (\prod_{w|v} \mathbf{Z}_w)$, где $\mathbf{Z}_w \cong \mathbf{Z}$ для всех w и действие G на N переставляет $\mathbf{Z}_w$ для всех w над данным нормированием $v \in S$. Следовательно,

$$\hat{H}^r(G, N) \cong \prod_{v \in S} \hat{H}^r(G, \prod_{w|v} \mathbf{Z}_w) \cong \prod_{v \in S} \hat{H}^r(G^v, \mathbf{Z}),$$

опять-таки по лемме Шапиро. Следовательно,

$$h(N) = \prod_{v \in S} ([\hat{H}^0(G^v, \mathbf{Z})])/([H^1(G^v, \mathbf{Z})]) = \prod_{v \in S} n_v.$$

Теперь определим другую решетку. Пусть λ — отображение $L_T \to V$, заданное формулой $\lambda(a) = f_a$, где $f_a(w) = \log |a|_w$ для всех $w \in T$. Теорема Дирихле о единицах (или по крайней мере ее доказательство!) говорит нам, что ядро отображения λ конечно и его образ является решеткой M^0 в V, порождающей подпространство $V^0 = \{f \in V \mid \Sigma f(w) = 0\}$.

Так как ядро λ конечно, то $h(L_T) = h(M^0)$ (см. гл. IV, § 8). Далее, $V = V^0 + \mathbf{R}g$, где g определяется из уравнения $g(w) = 1$ для всех $w \in S_L$. Мы определим вторую решетку M как $M^0 + \mathbf{Z}g$. Тогда M порождает V, и как M^0, так и $\mathbf{Z}g$ инвариантны относительно G. Следовательно, $h(M) = h(M^0) \cdot h(\mathbf{Z}) = nh(M^0) = nh(L_T)$.

Так как M, N — решетки, порождающие одно и то же векторное пространство, то $h(N) = h(M)$ в силу гл. IV, § 8. Следовательно, $\Pi n_v = h(N) = h(M) = nh(L_T)$, что и требовалось доказать.

8.4. Следствие. *Если L/K — циклическое расширение степени n, то*

$$[J_K/K^*N_{L/K}J_L] \geqslant n.$$

Это неравенство, которое в прежнее время называлось вторым неравенством, всегда доказывалось неаналитическими методами, берущими свое начало из теории Гаусса родов квадратичных форм. Для нас это — *первое неравенство*, так как другое неравенство выводится с его помощью.

8.5. Следствие. *Если L/K — конечное абелево расширение и D — подгруппа в J_K, такая, что*

(а) $D \subset N_{L/K}J_L$,

(б) K^*D *всюду плотно в* J_K,

то $L = K$.

Доказательство. Мы можем предположить, что L/K — циклическое расширение, так как если $L \supset L' \supset K$ и L'/K — циклическое, то $D \subset N_{L/K}J_L \subset N_{L'/K}J_{L'}$. Серр доказал, что множество локальных норм $N_{L_w/K_v}L_w^*$ является открытым подмножеством в K_v^*, которое содержит U_v для почти всех v, так что множества $N_{L/K}J_L$ (т. е. просто $\prod_w N_{L_w/K_v}L_w^*$) и $K^*N_{L/K}J_L$ открыты, а следовательно, и замкнуты в J_K, причем последнее всюду плотно, так как его подмножество K^*D всюду плотно. Таким образом, оно совпадает с J_K, т. е. $[J_K/K^*N_{L/K}J_L] = 1$, откуда $n = 1$ по предыдущему следствию.

8.6. Замечание. Подчеркнем, что в случае расширения Галуа элемент $x = (x_v) \in J_K$ принадлежит $N_{L/K}J_L$ тогда и только тогда, когда он всюду является локальной нормой, т. е. $x_v \in N_{L^v/K_v}(L^v)^*$ для всех $v \in \mathfrak{M}_K$.

8.7. Следствие. *Если S — конечное подмножество множества $\mathfrak{M}_K$ и L/K — конечное абелево расширение, то $G(L/K)$ порождается элементами $F_{L/K}(v)$ для $v \notin S$ (т. е. отображение $F_{L/K}: I^S \to G(L/K)$ сюръективно*, см. п. 3.3).

Доказательство. Обозначим через G' подгруппу группы $G(L/K)$, порожденную элементами $F_{L/K}(v)$ для $v \notin S$; пусть M — поле инвариантных элементов груп-

пы G'. Для $v \notin S$ все $F_{L/K}(v)$ в силу $G(M/K) \cong G/G'$ тривиальны, так что для всех $v \notin S$ имеет место $M_w = K_v$, если $w \in \mathfrak{M}_M$, $w \mid v$. Очевидно, что любой элемент K_v^* является нормой из такого расширения.

Положим $D = J_K^S$ (идели с компонентами $x_v = 1$ для $v \in S$); любой элемент из D локально является нормой, т. е. $D \subseteq N_{M/K} J_M$. По слабой аппроксимационной теореме (см. гл. II, § 6) $K^* J_K^S$ всюду плотно в J_K, так что в силу 8.5 мы получаем $M = K$ и G' совпадает с G.

8.8. Следствие. *Если L — нетривиальное абелево расширение поля K, то существует бесконечно много нормирований v поля K, которые не вполне распадаются в L (т. е. для которых $F_{L/K}(v) \neq 1$).*

Мы воспользуемся тем, что такие нормирования существуют вне любого конечного множества S.

§ 9. КОГОМОЛОГИИ КЛАССОВ ИДЕЛЕЙ

II. ВТОРОЕ НЕРАВЕНСТВО

Здесь мы выведем то, что в неаналитической трактовке называется *вторым неравенством*. Это неравенство может быть доказано очень быстро и легко с помощью анализа (см. гл. VIII, теорема 2.5) и в классических работах оно называлось первым неравенством. Мы приведем доказательство Шевалле (см. [11]).

9.1. Теорема. *Пусть L/K — расширение Галуа степени n с группой Галуа G. Тогда*

(а) $[\hat{H}^0(G, C_L)]$ *и* $[\hat{H}^2(G, C_L)]$ *делят* n;

(б) $\hat{H}^1(G, C_L) = (0)$.

Доказательство разбивается на несколько этапов.

Этап 1. Предположим, что теорема доказана, когда G — циклическая группа и n — простое число. По «неприятной» лемме (см. гл. VI, п. 1.5) отсюда следует, что $[\hat{H}^0(G, C_L)]$ делит n и $\hat{H}^1(G, C_L) = (0)$. Используя тривиальность $\hat{H}^1$, отсюда получаем (снова по «неприятной» лемме), что $[\hat{H}^2(G, C_L)]$ делит n.

Этап 2. Теперь мы предположим, что G — циклическая группа простого порядка n; в этом случае мы знаем, что $\hat{H}^0 \cong \hat{H}^2$ и (по первому неравенству 8.3) что $[\hat{H}^2] = n[\hat{H}^1]$; таким образом, достаточно будет показать, что $[\hat{H}^0(G, C_L)] = [C_K : N_{L/K} C_L]$ делит n.

Мы будем считать, что в случае функционального поля число n не равно характеристике поля K (противоположный случай исследован в [1], гл. 6).

Этап 3. Теперь мы покажем, что в дальнейшем можно считать, что поле K содержит корни n-й степени из единицы.

Действительно, если мы присоединим первообразный корень n-й степени из единицы ζ к полю K, то мы получим расширение $K' = K(\zeta)$, степень m которого делит $n - 1$, и потому взаимно проста с n. Поэтому

$$\begin{array}{ccc} L' = LK' & \xrightarrow{n} & K' = K(\zeta) \\ \Big\downarrow m & & \Big\downarrow m \\ L & \xrightarrow[n]{} & K \end{array}$$

Степень LK' над K' равна n, а L и K' линейно разделены над K. Поэтому существует коммутативная диаграмма с точными строками (мы опускаем описание, так как оно очевидно):

$$\begin{array}{ccccccc} C_L & \longrightarrow & C_K & \longrightarrow & C_K/NC_L & \longrightarrow & 0 \\ \Big\downarrow \mathrm{Con} & & \Big\downarrow \mathrm{Con} & & \Big\downarrow \mathrm{Con} & & \\ C_{L'} & \longrightarrow & C_{K'} & \longrightarrow & C_{K'}/NC_{L'} & \longrightarrow & 0 \\ \Big\downarrow N & & \Big\downarrow N & & \Big\downarrow N & & \\ C_L & \longrightarrow & C_K & \longrightarrow & C_K/NC_L & \longrightarrow & 0 \end{array}$$

Здесь Con обозначает конорменное отображение; композит отображений $N \cdot \mathrm{Con}$ является просто возведением в m-ю степень (см. гл. II, § 19 и определение конорменного отображения). Группа C_K/NC_L является группой кручения, в которой каждый элемент имеет порядок n; если $a \in C_K$, то a^n является нормой, т. е. $a^n \in NC_L$. Поэтому отображение

$N_{K'/K}\,\mathrm{Con}_{K'/K} : C_K/NC_L \to C_K/NC_L$ сюръективно, так как $(m, n) = 1$. Следовательно, отображение $N_{K'/K} : C_{K'}/NC_{L'} \to C_K/NC_L$ тоже сюръективно; таким образом, если $[C_{K'} : NC_{L'}]$ делит n, то и $[C_K : NC_L]$ тоже делит n.

Этап 4. Итак, мы редуцировали нашу задачу к случаю, когда n — простое число и K содержит корни n-й степени из единицы. Фактически мы непосредственно докажем в этом случае более общий результат:

Пусть K содержит корни n-й степени из единицы, и и L/K — абелево расширение с простым показателем n; пусть, скажем, $G(L/K) = G \cong (\mathbf{Z}/n\mathbf{Z})^r$. Тогда

$$[C_K : N_{L/K}C_L] \text{ делит } [L : K] = n^r. \tag{1}$$

Хотя, как мы уже видели, случай произвольного r следует из случая $r = 1$, тем не менее используемый метод не становится проще, если положить $r = 1$, а некоторые построения доказательства пригодны для больших r (см. п. 9.2 и 9.5).

Из теории Куммера (см. гл. III) мы знаем, что $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$ для некоторых $a_1, a_2, \ldots, a_r \in K$. Выберем S — конечное множество (плохих) нормирований, такое, что:

(i) S содержит все архимедовы нормирования;
(ii) S содержит все нормирования, отвечающие делителям числа n;
(iii) $J_K = K^* J_{K,S}$ (для этого нужно, чтобы S содержало представители некоторой системы образующих групп классов дивизоров); (2)
(iv) S содержит делители числителей и знаменателей всех a_i.

Условие (iv) означает, что все a_i являются S-единицами, т. е. принадлежат $K_S = K \cap J_{K,S}$.

Пусть $M = K(\sqrt[n]{K_S})$ — поле, полученное из K присоединением корней n-й степени из *всех* S-единиц. По теореме Дирихле о единицах группа K_S имеет конечный базис, так что это расширение конечное, и M не разветвлено вне S по условию (ii) на основании теории Куммера. Далее, $M \supset L \supset K$ и

$$K_S = M^{*n} \cap K_S \supset L^{*n} \cap K_S \supset K^{*n} \cap K_S = K_S^n.$$

Согласно теории Куммера, положив $[M : L] = n^t$, $[L : K] = n^r$ (где r дано), $[M : K] = n^s$, мы получаем соответственно

$$[K_S : (L^{*n} \cap K_S)] = n^t,\ [L^{*n} \cap (K_S : K_S^n)] = n^r \text{ и } [K_S : K_S^n] = n^s. \tag{3}$$

Мы утверждаем, что $s = [S]$, где $[S]$ — мощность множества S. По теореме Дирихле в M существует $[S] - 1$ фундаментальных единиц плюс еще корни из единицы, включая корни n-й степени, так что $K_S \cong \mathbf{Z}^{[S]-1} \times$ (циклическая группа порядка, делящегося на n) и

$$[K_S : K_S^n] = n^{[S]} = n^s, \quad \text{где} \quad s = t + r. \tag{4}$$

Мы хотим показать, что $[C_K : N_{L/K}C_L]$ делит n^r, т. е. делит $[(L^{*n} \cap K_S) : K_S^n]$. Другими словами, нам нужно показать, что $N_{L/K}C_L$ достаточно велико.

Если w — нормирование поля L, лежащее над $v \notin S$, то так как M/K не разветвлено вне S, автоморфизм Фробениуса $F_{M/L}(w)$ корректно определен. По следствию 8.7 $F_{M/L}(w)$ порождает $G(M/L)$. Выберем нормирования $w_1, \ldots, w_t$ так, чтобы $F_{M/L}(w_i)$ $(i = 1, \ldots, t)$ образовывали базис $G(M/L)$, и пусть $v_1, \ldots, v_t$ — нормирования поля K, лежащие под ними. Мы утверждаем, что $F_{M/L}(w_i) = F_{M/L}(v_i)$ $(i = 1, \ldots, t)$ (действительно, каждое v не разветвлено, так что $F_{M/L}(v_i)$ определено). Группа разложения $G_v(M/K)$ расширения M/K является циклической подгруппой группы $(\mathbf{Z}/n\mathbf{Z})^s$, так что она либо имеет простой порядок n, либо тривиальна. Мы выбрали w так, чтобы $F_{M/L}(w)$ было нетривиально, поэтому группа разложения $G_w(M/L)$ тоже нетривиальна; следовательно, группа разложения расширения L/K

$$G_v(L/K) \cong G_v(M/K)/G_w(M/L)$$

тривиальна, т. е. v полностью распадается в L. Поэтому $G_{v_i} = G_{w_i}$, и эта группа порождается элементами $F_{M/L}(v_i) = F_{M/K}(w_i)$. Заметим еще, что $L_{w_i} = K_{v_i}$ для всех $i = 1, \ldots, t$.

Введем обозначение $T = \{v_1, \ldots, v_t\}$. Мы утверждаем, что

$$(L^*)^n \cap K_S = \{a \in K_S \mid a \in K_v^n \text{ для всех } v \in T\}. \tag{5}$$

Действительно, так как $L_w = K_v$ для всех $v \in T$ и $w \mid v$, то отсюда тривиально следует, что $L^{*n} \cap K_S$ содержится в правой части. Обратно, если $a \in K_S$, то $\sqrt[n]{a} \in M$. Если, кроме того, $a \in K_v^n$ для всех $v \in T$, то $\sqrt[n]{a} \in K_v$ для всех $v \in T$ и потому он инвариантен относительно всех $F_{M/K}(v) = F_{M/L}(w)$, которые порождают $G(M/L)$; поэтому $\sqrt[n]{a} \in L$. Это доказывает утверждение (5).

Положим

$$E = \prod_{v \in S} K_v^{*n} \times \prod_{v \in T} K_v^* \times \prod_{v \notin S \cup T} U_v, \tag{6}$$

где U_v — множество v-единиц в K_v, так что $E \subset J_{K, S \cup T}$. Кроме того, $E \subset N_{L/K} J_L$ (см. замечание 8.6). Действительно, любой элемент из K_v^{*n} является нормой, так как $K_v^*/NL_w^* \cong G_v$ (см. гл. VI, п. 2.1) и G_v аннулируется умножением на n; далее, мы имеем $K_v^* = L_w^*$ для всех $v \in T$, и потому все элементы таких K_v^* являются нормами, а элементы U_v являются нормами для неразветвленных v (см. гл. VI, предложение 1.1).

Далее,

$$[C_K / N_{L/K} C_L] = [J_K / K^* N_{L/K} J_L]$$

делит $[J_K : K^* E]$, потому что $E \subset N_{L/K} J_L$. Множество S выбрано было так (см. (2), (iii)), что

$$J_K = K^* J_{K, S} = K^* J_{K, S \cup T};$$

следовательно, $[C_K / N_{L/K} C_L]$ делит $[K^* J_{K, S \cup T} : K^* E]$. Общая формула для индексов групп такова:

$$[CA : CB]\,[(C \cap A) : (C \cap B)] = [A : B],$$

так что для доказательства утверждения (1) достаточно показать, что

$$[J_{K, S \cup T} : E] / [K_{S \cup T} : (K \cap E)] = n^r \tag{7}$$

(где $K_{S \cup T} = K^* \cap J_{K, S \cup T}$).

Сначала мы вычислим $[J_{K, S \cap T} : E]$. Имеет место

$$J_{K, S \cup T} = \prod_{v \in S} K_v^* \prod_{v \in T} K_v^* \prod_{v \notin S \cup T} U_v,$$

так что $[J_{K, S \cup T} : E] = \prod_{v \in S} [K_v^* : (K_v^*)^n]$ в силу (5). Из гл. VI, п. 1.7 (см. также [1], стр. XII), мы видим, что индекс Эрбрана $h(K_v^*)$ равен $n / |n|_v$, где $|\ |_v$ обозначает абсолютную величину. Но, кроме того, $h(K_v^*) = [K_v^* : K_v^{*n}]/n$, потому что корни n-й степени из единицы принадлежат K_v^*. Это значит, что $[K_v^* : K_v^{*n}] = n^2 / |n|_v$ и

$$[J_{K, S \cup T} : E] = n^{2s} \prod_{v \in S} |n|_v^{-1} = n^{2s} \tag{8}$$

по формуле произведения, так как $|n|_v = 1$, если $v \notin S$.

Нам еще понадобится формула

$$[U_v : U_v^n] = n / |n|_v, \tag{9}$$

которая следует из того, что $h(U_v) = 1 / |n|_v$ (см. гл. VI, п. 1.7).

Из формулы (8) мы видим, что для доказательства равенства (7) будет достаточно показать, что

$$[K_{S \cup T} : K^* \cap E] = n^{2s - r} = n^{s + t}. \tag{10}$$

Как и в (4), заменяя S на $S \cup T$, мы получаем $[K_{S \cup T} : K_{S \cup T}^n] = n^{s+t}$, так что нужно только показать, что $K^* \cap E = K_{S \cup T}^n$.

Очевидно, что $K^* \cap E \supset K_{S \cup T}^n$, так что осталось доказать, что

$$K^* \cap E \subset K_{S \cup T}^n, \tag{11}$$

а это вытекает из следующей леммы.

9.2. Лемма. *Пусть K содержит корни n-й степени из единицы. Пусть S — подмножество множества $\mathfrak{M}_K$, удовлетворяющее условиям* (i), (ii), (iii) *из* (2) *в приведенном выше доказательстве, и пусть T — множество нормирований, не пересекающееся с S и не зависящее от K_S в том смысле, что отображение $K_S \to \prod_{v \in T} U_v / U_v^n$ сюръективно.*

Предположим, что $b \in K^*$ является n-й степенью в S, единицей вне $S \cup T$, а в T — произвольно. Тогда $b \in K^{*n}$.

Доказательство леммы. Рассмотрим расширение $K' = K(\sqrt[n]{b})$; достаточно показать, что $K' = K$. Положим

$$D = \prod_{v \in S} K_v^* \times \prod_{v \in T} U_v^n \times \prod_{v \notin S \cup T} U_v;$$

по соображениям, аналогичным указанным выше (см. после формулы (6)), $D \subset N_{K'/K}J_{K'}$. Следовательно, согласно следствию 8.5 из первого неравенства, для того чтобы доказать, что $K' = K$, достаточно показать, что $K^*D = J_K$. Но по предположению отображение $K_S \to \prod_{v\in T}(U_v/U_v^n) \cong J_{K,S}/D$ сюръективно. Следовательно, $J_{K,S} = K_S D$ и $J_K = K^*J_{K,S} = K^*D$, что и требовалось доказать.

Чтобы вывести соотношение (11) из леммы, мы должны проверить, что T не зависит от S в том смысле, как говорится в лемме. Пусть H обозначает ядро отображения $K_S \to \prod_{v\in T}(U_v/U_v^n)$. Для доказательства сюръективности этого отображения достаточно показать, что $(K_S : H) = \prod_{v\in T}(U_v : U_v^n)$. Последнее произведение в силу равенства (9) в точности равно n^t, потому что $|n|_v = 1$ для $v \in T$. С другой стороны, из (5) мы получаем $H = K_S \cap (L^*)^n$, и, следовательно, согласно (3), $(K_S : H) = n^+$.

Теперь теорема полностью доказана.

9.3. Замечание. Лемма 9.2 интересна даже в том случае, если T пусто.

Если S удовлетворяет условиям (i), (ii), (iii) *из* (2), *то S-единица, которая локально есть n-я степень для всех нормирований из S, является n-й степенью.*

9.4. Следствие. *Пусть L/K — абелево расширение с группой Галуа G; если существует отображение Артина* ψ: $\hat{H}^0(G, C_L) = C_K/NC_L \to G$, *то ψ должно быть изоморфизмом.*

Действительно, из следствия 8.7 из первого неравенства мы уже знаем, что ψ должно быть эпиморфизмом; если $[\hat{H}^0(G, C_L)] \leqslant [G]$, то ψ может быть только изоморфизмом.

9.5. Следствие (извлеченное из доказательства теоремы 9.1). *Пусть n — простое число и K — поле характеристики, отличной от n, содержащее корни n-й степени из единицы. Пусть S — конечное множество нормирований поля K, удовлетворяющее условиям* (i), (ii) *и* (iii) *из* (2), *и пусть $M = K(\sqrt[n]{K_S})$. Тогда, если закон взаимности*

выполняется для M/K, то мы имеем

$$K^*N_{M/K}J_M = K^*E, \text{ где } E = \prod_{v\in S}(K_v^*)^n \times \prod_{v\notin S} U_v. \quad (12)$$

Рассмотрим в доказательстве теоремы 9.1 случай $L = M$ (т. е. T пусто, $t = 0$ и $s = r$). Тогда $E \subset N_{M/K}J_M$, где E определено формулой (12). Согласно (7), при $L = M$ мы получаем $[J_K : K^*E] = n^s = [M : K]$. С другой стороны, если закон взаимности выполняется, то мы знаем, что

$$[C_K : N_{M/K}C_M] = [J_K : K^*N_{M/K}J_M] = n^s,$$

следовательно, равенство (12) должно выполняться.

Эти результаты пригодятся нам впоследствии; мы воспользуемся ими при доказательстве «теоремы существования» в заключительной части § 12.

9.6. Следствие. Пусть L/K — конечное (не обязательно абелево) расширение Галуа. Так как $H^1(G, C_L) = 0$, то точная последовательность $0 \to L^* \to J_L \to C_L \to 0$ порождает очень короткую точную последовательность $0 \to H^2(G, L^*) \to H^2(G, J_L)$. Далее, в силу предложения 7.3 $H^2(G, J_L) = \coprod_{v\in\mathfrak{M}_K} H^2(G^v, (L^v)^*)$, так что существует вложение

$$0 \to H^2(G, L^*) \to \coprod_{v\in\mathfrak{M}_K} H^2(G^v, (L^v)^*). \quad (13)$$

Позднее мы увидим (например, из того, что стрелка β_1 в диаграмме (9) из § 11 дает изоморфизм), что образ этого вложения состоит из тех элементов прямой суммы, у которых сумма локальных инвариантов равна 0. Таким образом, мы получаем полное описание структуры группы $H^2(G, L^*)$.

В терминах центральных простых алгебр последовательность (13) дает *теорему Брауэра — Хассе — Нётер о том, что центральная простая алгебра над K распадается над K тогда и только тогда, когда она локально распадается всюду*. В частности, если группа G циклическая, то $\hat{H}^2 \cong \hat{H}^0$, и мы получаем *теорему Хассе о нормах*:

Если $a \in K^*$ и L/K — циклическое расширение, то $a \in N_{L/K}L^*$ тогда и только тогда, когда $a \in N_{L^v/K_v}L^{v*}$ для всех $v \in \mathfrak{M}_K$.

Еще более специализируя, возьмем группу G порядка 2, так что $L = K(\sqrt{b})$. Тогда

$$N_{L/K}(x + y\sqrt{b}) = x^2 - by^2,$$

и потому (если характеристика не равна 2) мы получаем, что a представимо в форме $x^2 - by^2$ тогда и только тогда, когда такое представление локально существует всюду. Отсюда следует, что *квадратичная форма $Q(x, y, z)$ над K от трех переменных имеет нетривиальный нуль в K тогда и только тогда, когда она имеет нетривиальный нуль в каждом пополнении поля K*. Переходя к произвольному n, мы можем получить *теорему Минковского — Хассе* о том, что квадратичная форма имеет нуль тогда и только тогда, когда она локально имеет нуль всюду (см. упражнение 4).

Можно рассмотреть общую задачу: если $a \in K^*$ и $a \in NL^{v*}$ для всех v, верно ли, что $a \in NL^*$? К сожалению, ответ не всегда утвердителен (см. п. 11.4).

9.7. Вернемся к последовательности (13). Мы будем писать $H^2(L/K)$ вместо $H^2(G, L^*)$ и $H^2(L^v/K_v)$ вместо $H^2(G^v, L^{v*})$. Тогда (13) записывается так:

$$0 \to H^2(L/K) \to \coprod_v H^2(L^v/K_v). \tag{13'}$$

Серр (гл. VI, следствие 2 из теоремы 3.1) определил $H^2(L^v/K_v)$; это циклическая группа порядка $n_v = [L^v : K_v]$ с канонической образующей. Поэтому

$$H^2(G, J_L) = \coprod_v H^2(L^v/K_v) \cong \coprod_v \left(\frac{1}{n_v}\mathbf{Z}/\mathbf{Z}\right)$$

и

$$0 \to H^2(L/K) \to \coprod_v \left(\frac{1}{n_v}\mathbf{Z}/\mathbf{Z}\right).$$

Если $\alpha \in \coprod_v H^2(L^v/K_v)$, или $\alpha \in H^2(L/K)$, то мы можем найти его локальные инварианты $\mathrm{inv}_v(\alpha)$ (точнее, $\mathrm{inv}_v(j_v(\alpha))$, где j_v — проекция на v-компоненту), которые будут точно определены.

Рассмотрим функториальные свойства отображения inv_v. Пусть $L' \supset L \supset K$ — конечные расширения Галуа с группами

$$G' = G(L'/K)$$

и

$$G = G(L/K) \cong G'/H,$$

где $H = G(L'/L)$. Если $\alpha \in H^2(G, J_L)$, то $\mathrm{infl}(\alpha) \in H^2(G', J_{L'})$ и

$$\mathrm{inv}_v(\mathrm{infl}\,\alpha) = \mathrm{inv}_v(\alpha). \tag{14}$$

Конечно, выбирая нормирование w' поля L' над нормированием v поля L, мы приходим к соответствующему локальному утверждению о башне $L'_{w'} \supset L_w \supset K_v$; см. гл. VI, п. 1.1.

Так как инфляция ничего не меняет, то мы можем перейти инвариантным образом к *группе Брауэра* поля K и получить *локальный инвариант* для $\alpha \in \mathrm{Br}(K) = H^2(\bar{K}/K)$, где $\bar{K}$ — алгебраическое замыкание поля K (см. гл. VI, § 1) и, обобщая, для

$$\alpha \in H^2(G_{\bar{K}/K}, J_{\bar{K}}) = \varinjlim_L H^2(G_{L/K}, J_L),$$

где $J_{\bar{K}} = \varinjlim J_L$ и по определению предел берется по конечным расширениям Галуа L поля K (см. гл. V).

Если теперь $\alpha \in H^2(G', J_{L'})$, то $\mathrm{Res}^{G'}_H \alpha \in H^2(H, J_{L'})$ и

$$\mathrm{inv}_w(\mathrm{Res}^{G'}_H \alpha) = n_{w|v}\,\mathrm{inv}_v(\alpha), \tag{15}$$

где $w \in \mathfrak{M}_L$ лежит над $v \in \mathfrak{M}_K$ и $n_{w|v} = [L_w : K_v]$ (это утверждение снова немедленно сводится к локальному случаю, о котором см. гл. VI, п. 1.1, или [7], стр. 175). При этом L/K не обязано даже быть расширением Галуа.

Отметим еще несколько результатов, хотя мы ими и не воспользуемся. Снова L/K не обязано быть расширением Галуа. Если $\alpha' \in H^2(H, J_{L'})$, то $\mathrm{Cor}^{G'}_H \alpha' \in H^2(G', J_{L'})$ и

$$\mathrm{inv}_v(\mathrm{cor}^{G'}_H \alpha') = \sum_{w|v} \mathrm{inv}_w(\alpha'), \tag{16}$$

где суммирование производится по всем нормированиям $w \in \mathfrak{M}_L$, лежащим над $v \in \mathfrak{M}_K$ (см. [7], стр. 175).

9.8. Следствие. *Пусть* α *принадлежит* $\mathrm{Br}(K)$ *или* $H^2(G(\bar{K}/K), J_{\bar{K}})$, J_K, *где* $\bar{K}$ *— сепарабельное алгебраическое замыкание поля* K. *Пусть* L *— расширение поля* K, *содержащееся в* $\bar{K}$. *Тогда* $\mathrm{Res}_L^K(\alpha) = 0$ *равносильно тому, что* $[L_w : K_v]\,\mathrm{inv}_v(\alpha) = 0$ *для каждого* $w \mid v$ *(это дает только конечное число условий, так как почти все* $\mathrm{inv}_v(\alpha)$ *равны нулю).*

В том случае, когда L/K — расширение Галуа, существует точная последовательность

$$0 \to H^2(L/K) \xrightarrow{\mathrm{infl}} \mathrm{Br}(K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L)$$

и $\alpha \in H^2(L/K)$ тогда и только тогда, когда знаменатель $\mathrm{inv}_v(\alpha)$ делит $[L_w : K_v]$ для всех w, лежащих над v.

§ 10. ДОКАЗАТЕЛЬСТВО ЗАКОНА ВЗАИМНОСТИ

10.1. Пусть теперь L/K — конечное абелево расширение с группой Галуа G. Вспомним наше рассмотрение локальных символов в § 6, где мы отмечали, что если глобальное отображение Артина существует, то мы можем перейти к изучению локальных символов; там же мы заметили, что, и обратно, если локальные отображения Артина определены, то мы можем получить глобальное отображение Артина. Мы предполагаем выполнить здесь эту последнюю программу, используя локальные отображения Артина («норменный вычет»), определенные в гл. VI, п. 2.2.

Локальное отображение Артина мы обозначим через θ_v: $K_v^* \to G^v$; мы определим отображение

$$\theta\colon J_K \to G,$$

положив

$$\theta(x) = \prod_{v \in \mathfrak{M}_K} \theta_v(x_v),\quad x \in J_K.$$

Это определение корректно, так как (в силу гл. VI, п. 2.3) $\theta_v(x_v) = F_{L^v/K_v}(v)^{v(x_v)}$ (где $v(x_v)$ обозначает значения приведенного нормирования на x_v), когда v не разветвлено, и $v(x_v) = 0$, если $x_v \in U_v$; поэтому $\theta_v(x_v) = 1$ для всех v, кроме конечного числа. (В самом деле, даже если L/K — бесконечное расширение, произведение $\theta(x)$ сходится.) Ясно, что θ — непрерывное отображение.

Возьмем в качестве $S_0 \subseteq \mathfrak{M}_K$ множество архимедовых и разветвленных в L/K нормирований; тогда из $x \in J_K^{S_0}$ следует $\theta(x) = F((x)^{S_0})$. Поэтому θ удовлетворяет двум условиям отображения Артина ((i) и (iii) из следствия 4.2); последнее условие ((ii) из 4.2) таково:

$$\theta(\alpha) = \prod_{v \in \mathfrak{M}_K} \theta_v(a) = 1 \text{ для всех } a \in K^*.$$

Так что если мы сможем доказать это равенство, то мы докажем закон взаимности.

10.2. Для доказательства закона взаимности мы сформулируем две связанные между собой теоремы и докажем их обе сразу, последовательно расширяя условия, при которых они верны.

Теорема А. *Любое конечное абелево расширение* L/K *удовлетворяет закону взаимности, и отображение Артина* $\theta\colon J_K \to G(L/K)$ *задается формулой* $\theta = \prod_v \theta_v$.

Теорема Б. *Если* $\alpha \in \mathrm{Br}(K)$, *то* $\sum_{v \in \mathfrak{M}_K} \mathrm{inv}_v(\alpha) = 0$.

Замечания. На основании сказанного выше теорема А сводится к следующему утверждению:

$$\prod_{v \in \mathfrak{M}_K} \theta_v(a) = 1 \text{ для всех } a \in K^*. \qquad (1)$$

Сумма в теореме Б конечна, так как $\mathrm{inv}_v(\alpha) = \mathrm{inv}_v(j_v \cdot \alpha) = 0$ для всех v, кроме конечного числа.

Если $\alpha \in \mathrm{Br}(K)$, то $\alpha \in H^2(L/K)$ для некоторого конечного расширения L/K, т. е. α распадается над конечным расширением поля K.

Логически доказательство содержит четыре главных этапа.

Этап 1. Доказательство теоремы А для произвольного кругового расширения L/K.

Этап 2. Вывод теоремы Б для α, распадающегося над циклическим круговым расширением.

Этап 3. Вывод теоремы Б для произвольного $\alpha \in \mathrm{Br}(K)$.

Этап 4. Вывод теоремы А для всех абелевых расширений.

Практически мы сначала выясним соотношения между теоремами А и Б и выведем (этап 2), что из А вытекает Б для циклических расширений и (этап 4) что из Б вытекает А для произвольного абелева расширения. Затем мы непосредственно доказываем утверждение этапа 1 и, наконец, утверждение этапа 3, показывая, что любой элемент группы $\mathrm{Br}(K)$ имеет циклическое круговое поле разложения.

10.3. *Этапы* 2 *и* 4. *Связь между* А *и* Б. В теореме А речь идет о $\hat{H}^0$, а в теореме Б — о H^2, поэтому нам нужна связывающая их лемма.

Пусть L/K — конечное абелево расширение с группой Галуа G. Пусть, далее, χ — характер группы G, т. е. $\chi \in \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) = H^1(G, \mathbf{Q}/\mathbf{Z})$, где $\mathbf{Q}/\mathbf{Z}$ — тривиальный G-модуль. Для $v \in \mathfrak{M}_K$ обозначим через χ_v ограничение χ на группу разложения G^v. Пусть δ — связывающий гомоморфизм

$$\delta\colon H^1(G, \mathbf{Q}/\mathbf{Z}) \longrightarrow H^2(G, \mathbf{Z}).$$

Если $x = (x_v) \in J_K$, то обозначим через $\bar{x}$ его образ в $J_K/N_{L/K}J_L \cong \hat{H}^0(G, J_L)$. Тогда их $\cup$-произведение (см. гл. IV, § 7) $\bar{x}\cdot\delta\chi$ принадлежит $H^2(G, J_L)$.

Лемма. *Для каждого* v *имеет место*

$$\mathrm{inv}_v(\bar{x}\cdot\delta\chi) = \chi_v(\theta_v(x_v)),$$

и потому

$$\sum_v \mathrm{inv}_v(\bar{x}\cdot\delta\chi) = \chi(\theta(x)).$$

Доказательство. Мы используем результаты гл. VI, п. 2.3. Проекция $j_v\colon J_L \longrightarrow (L^v)^*$ индуцирует отображение

$$j_v\cdot\mathrm{Res}^G_{G_v}\colon H^2(G, J_L) \longrightarrow H^2(G_v, J_L) \longrightarrow H^2(G_v, (L^v)^*),$$

и так как $\cup$-умножение коммутирует с ограничением, то

$$\begin{aligned}\mathrm{inv}_v(\bar{x}\cdot\delta\chi) &= \mathrm{inv}_v(j_v\cdot\mathrm{Res}^G_{G_v}(\bar{x}\cdot\delta\chi)),\\ &= \mathrm{inv}_v((j_v\cdot\bar{x})\cdot\delta\chi_v),\\ &= \mathrm{inv}_v(\bar{x}_v\cdot\delta\chi_v),\\ &= \chi_v(\theta_v(x_v));\end{aligned}$$

последний переход делается на основании гл. VI, п. 2.3.

Отсюда немедленно следует, что

$$\chi(\theta(x)) = \chi\Big(\coprod_v \theta_v(x_v)\Big) = \sum_v \chi_v(\theta_v(x_v)) = \sum_v \mathrm{inv}_v(\bar{x}\cdot\delta\chi).$$

Для проверки этапа 4 применим лемму при $x = a \in K^* \subseteq J_K$. Обозначим через $\tilde{a}$ образ элемента a в $\hat{H}^0(G, L^*)$. Тогда $\tilde{a}\cdot\delta\chi \in \hat{H}^2(G, L^*) \subseteq \mathrm{Br}(K)$, как нам и нужно. Образом $\tilde{a}\cdot\delta\chi$ в $H^2(G, J_L)$ является $\bar{a}\cdot\delta\chi$, где $\bar{a}$ — образ a в $\hat{H}^0(G, J_L)$ и, согласно лемме, $\sum_v \mathrm{inv}_v(\bar{a}\cdot\delta\chi) = \chi(\theta(a))$; таким образом, если теорема Б верна для всех $\alpha \in \mathrm{Br}(K)$, то $\chi(\theta(a)) = 0$, а так как это имеет место для всех χ, то $\theta(a) = 0$. Это и есть теорема А.

Чтобы проверить этап 2, возьмем циклическое расширение L/K. Выберем за χ образующий характер, т. е. вложение G в $\mathbf{Q}/\mathbf{Z}$. Тогда умножение на $\delta\chi$ дает изоморфизм $\hat{H}^0 \cong H^2$, так что любой элемент из $H^2(L/K, L^*)$ представим в виде $\tilde{a}\cdot\delta\chi$. Если теорема А верна, то по лемме

$$\sum_v \mathrm{inv}_v(\bar{a}\cdot\delta\chi) = \chi(\theta(a)) = 0$$

для всех $a \in K^*$, что совпадает с утверждением теоремы Б.

10.4. *Этап* 1 (*случай числового поля*). Мы хотим доказать, что если L/K — круговое расширение, то $\coprod_v \theta_v(a) = 1$ для всех $a \in K^*$.

Пусть L/K — конечное круговое расширение. Тогда для некоторого корня из единицы ζ мы имеем $L \subset K(\zeta)$, и вследствие согласованности локальных символов θ_v

относительно расширений $(K(\zeta))^v/K_v$ и L^v/K_v достаточно будет исследовать случай $L = K(\zeta)$ (см. гл. VI, п. 2.4).

Далее мы сводим задачу к случаю $K = \mathbf{Q}$. Предположим, что $M = K(\zeta)$ с группой Галуа G'; определим $L = \mathbf{Q}(\zeta)$ с группой Галуа G. Тогда $M = LK$, и существуют естественное вложение i: $G' \to G$ и норменное отображение N: $J_K \to J_{\mathbf{Q}}$. Диаграмма

$$\begin{array}{ccc} & & J_K \xrightarrow{\theta'} G' \\ & N_{K/\mathbf{Q}} \downarrow & \downarrow i \\ & J_{\mathbf{Q}} \xrightarrow{\theta} G \end{array}$$

(где $\theta' = \prod_v \theta'_v$ и $\theta = \prod_p \theta_p$) коммутативна, так как

$$(N_{K/\mathbf{Q}}x)_p = \prod_{v \mid p} N_{K_v/\mathbf{Q}_p} x_v$$

(см. гл. II, § 11, последняя формула) и так как диаграммы

$$\begin{array}{ccc} K_v & \longrightarrow & G'_v \\ {\scriptstyle N}\downarrow & & \downarrow i \\ \mathbf{Q}_p & \longrightarrow & G_p \end{array}$$

коммутативны всякий раз, когда v лежит над p (см. гл. VI, п. 2.1). Таким образом, $i \circ \theta'(x) = \theta(N_{K/\mathbf{Q}}(x))$ для всех $x \in J_K$, и потому, в частности, $i \circ \theta'(a) = \theta(N_{K/\mathbf{Q}}(a))$ для всех $a \in K$. Если теорема A верна для $L/\mathbf{Q}$, то $\theta(b) = 1$ для всех $b \in \mathbf{Q}$, так что $\theta'(a) = 1$ для всех $a \in K$, потому что i — вложение.

Первое доказательство для кругового расширения $L/\mathbf{Q}$. Мы знаем на основании вычислений п. 3.4, что закон взаимности в смысле п. 3.8 выполняется для $L/\mathbf{Q}$, т. е. имеется допустимое отображение F: $I^S \to G(L/\mathbf{Q}) = G$ для некоторого S. Используя интерпретацию Шевалле (предложение 4.1), мы получаем отображение Артина ψ: $J_{\mathbf{Q}} \to G$ и индуцированные локальные отображения ψ_p: $\mathbf{Q}_p^* \to G_p$ (см. § 6). В силу предложения 4.3 мы можем перейти к пределу и принять за L максимальное круговое расширение $\mathbf{Q}^{\mathrm{mc}}$ поля $\mathbf{Q}$. Это дает нам локальные отображения ψ_p: $\mathbf{Q}_p^{\mathrm{mc}} \to G(\mathbf{Q}_p^{\mathrm{mc}}/\mathbf{Q}_p)$ для всех простых p. Мы хотим

показать, что эти отображения ψ_p совпадают с отображениями θ_p из гл. VI, п. 2.2; мы сделаем это, используя характеристические свойства, приведенные в гл. VI, предложение 2.6.

Мы должны проверить три утверждения. Во-первых, что $\mathbf{Q}_p^{\mathrm{mc}}$ содержит максимальное неразветвленное расширение $\mathbf{Q}_p^{\mathrm{nr}}$ поля $\mathbf{Q}_p$; это следует из приложения к § 7 гл. I. Во-вторых, что если $\alpha \in \mathbf{Q}_p$, то $\psi_p(\alpha) \mid \mathbf{Q}_p = F^{v_p(\alpha)}$, где $v_p(\alpha)$ — значение приведенного нормирования на элементе α, а F — автоморфизм Фробениуса из $G(\mathbf{Q}_p^{\mathrm{nr}}/\mathbf{Q}_p)$, это очевидно. В-третьих, что если $\mathscr{M}/\mathbf{Q}_p$ — конечное подрасширение в $\mathbf{Q}_p^{\mathrm{mc}}$ и $\alpha \in N_{\mathscr{M}/\mathbf{Q}_p}\mathscr{M}^*$, то $\psi_p(\alpha)$ тривиально действует на $\mathscr{M}$; это следует из предложения 6.2. Значит, $\psi_p = \theta_p$ для всех конечных простых p. Мы должны не забыть проверить, что ψ_∞ совпадает с θ_∞ (см. гл. VI, п. 2.9). В силу предложения 6.2 ψ_∞ — непрерывный гомоморфизм $\mathbf{R}^*$ в $G_\infty = G(\mathbf{C}/\mathbf{R}) \cong \{\pm 1\}$ и $\psi_\infty(N_{\mathbf{C}/\mathbf{R}}\mathbf{C}^*) = 1$. Следовательно, ψ_∞ и θ_∞ индуцируют отображения $\mathbf{R}^*/\mathbf{R}_+^*$ в $G(\mathbf{C}/\mathbf{R})$, причем θ_∞ сюръективно, так что нам осталось только проверить, что ψ_∞ сюръективно, иначе говоря, мы должны проверить, что ψ_∞ — ненулевое отображение.

Так как $\mathbf{C} = \mathbf{R}(i)$, мы рассмотрим действие ψ на $\mathbf{Q}(i) \supset \mathbf{Q}$; в этом расширении разветвлены только 2 и ∞. Следовательно,

$$1 = \psi(-7) = \psi_2(-7)\,\psi_7(-7)\,\psi_\infty(-7) = \psi_7(7)\,\psi_\infty(-1),$$

так как -7 является 2-адической нормой, и потому $\psi_2(-7) = 1$. Далее, $\psi_7(7)$ — это отображение $i \to i^7 = -i$, так что $\psi_\infty(-1)$ есть отображение $i \to -i$, т. е. оно нетривиально.

Второе доказательство для кругового расширения $L/\mathbf{Q}$. Мы можем действовать чисто локально, не пользуясь полученными результатами, но используя явные локальные вычисления символа норменного вычета в круговых расширениях, принадлежащие Дворку.

Пусть ζ — корень из единицы; в силу п. 2.9 гл. VI

$$\zeta^{\theta_\infty(x)} = \zeta^{\mathrm{sign}(x)} \text{ для } x \in \mathbf{R}^*, \qquad (1)$$

а в силу п. 3.1 гл. VI, если $x \in \mathbf{Q}_p^*$, $x = p^\nu u$, причем u — единица в $\mathbf{Q}_p$ и ν — целое число, то

$$\zeta^{\theta_p(p^\nu u)} = \begin{cases} \zeta^{p^\nu}, & \text{если порядок } \zeta \text{ взаимно прост с } p; \\ \zeta^{u^{-1}}, & \text{если порядок } \zeta \text{ равен степени числа } p. \end{cases} \tag{2}$$

Нам нужно проверить, что $\prod\limits_p \theta_p(a) = 1$ для всех $a \in \mathbf{Q}^*$, а для этого достаточно показать, что $\prod\limits_p \theta_p(q) = 1$ для всех простых $q > 0$ и что $\prod\limits_p \theta_p(-1) = 1$. Кроме того, достаточно рассмотреть действие на корне l-й степени из единицы, где l — простое число. Можно явно проверить, что это действие тривиально, используя формулы

$$\zeta^{\theta_p(-1)} = \begin{cases} \zeta^{-1}, & p = \infty; \\ \zeta^{-1}, & p = l; \\ \zeta, & p \neq l, \infty, \end{cases}$$

$$\zeta^{\theta_p(q)} = \begin{cases} \zeta, & p = q = l; \\ \zeta, & p \neq l,\ p \neq q \text{ (включая случай } p = \infty); \\ \zeta^{q^{-1}}, & p = l,\ p \neq q; \\ \zeta^q, & p \neq l,\ p = q. \end{cases}$$

(Так как группа Галуа абелева, то не имеет значения порядок применения автоморфизмов $\theta_p(-1)$, соответственно $\theta_p(q)$.)

10.5. *Этап 3 (случай числового поля).* Достаточно показать, что любой элемент группы $\mathrm{Br}(K)$ имеет циклическое круговое поле разложения. Иначе говоря, для любого $\alpha \in \mathrm{Br}(K)$ существует циклическое круговое расширение L/K, такое, что для любого $v \in \mathfrak{M}_K$ локальная степень $[L^v : K_v]$ кратна знаменателю $\mathrm{inv}_v(\alpha)$ (см. следствие 9.8).

Далее, $\mathrm{inv}_v(\alpha) = 0$ для всех нормирований, кроме конечного числа, и потому нам нужно только доказать следующее.

Лемма. *Пусть даны числовое поле K конечной степени над $\mathbf{Q}$, конечное множество нормирований S поля K и положительное целое число m; тогда существует циклическое круговое расширение L/K, локальные степени которого делятся на m для неархимедовых нормирований v из S и делятся на 2 для вещественных архимедовых нормирований из S (иначе говоря, L — комплексное).*

Доказательство. Достаточно построить L в случае $K = \mathbf{Q}$ (умножив m на степень $[K : \mathbf{Q}]$). Выберем достаточно большое число r и нечетное простое число q. Группа Галуа расширения $L(q) = \mathbf{Q}(\sqrt[q^r]{1})$ изоморфна прямой сумме циклической группы порядка $q - 1$ и циклической группы порядка q^{r-1}, так что существует подполе $L'(q)$ поля $L(q)$, которое является циклическим круговым расширением поля $\mathbf{Q}$ степени q^{r-1}. Далее,

$$[L(q) : L'(q)] = q - 1,$$

и потому, локализуя по фиксированному нормированию $p \neq \infty$ поля $\mathbf{Q}$, мы получаем

$$[L(q)^{(p)} : L'(q)^{(p)}] \leqslant q - 1;$$

так как $[L(q)^{(p)} : \mathbf{Q}_p] \to \infty$ при $r \to \infty$ (это следует, например, из того, что каждое конечное расширение поля $\mathbf{Q}_p$ содержит лишь конечное число корней из единицы), то отсюда вытекает, что $[L'(q)^{(p)} : \mathbf{Q}_p] \to \infty$ при $r \to \infty$. Следовательно, так как $[L'(q)^{(p)} : \mathbf{Q}_p]$ всегда является степенью числа q, то $[L'(q)^{(p)} : \mathbf{Q}_p]$ делится на достаточно большую степень q, если взять r достаточно большим.

Положим теперь $q = 2$ и $L(2) = \mathbf{Q}(\sqrt[2^r]{1})$ для достаточно большого r. Поле $L(2)$ имеет группу Галуа, изоморфную прямой сумме циклической группы порядка 2 и циклической группы порядка 2^{r-2}. Пусть ζ — первообразный корень из единицы степени 2^r, и пусть $\xi = \zeta - \zeta^{-1}$ и $L'(2) = \mathbf{Q}(\xi)$. Автоморфизмы $\mathbf{Q}(\zeta)$ над $\mathbf{Q}$ имеют вид $\sigma_\mu\colon \zeta \mapsto \zeta^\mu$ при μ нечетном и $\sigma_\mu(\xi) = \zeta^\mu - \zeta^{-\mu}$. Так как $\zeta^{2^{r-1}} = -1$, то $\sigma_{-\mu+2^{r-1}}(\xi) = \sigma_\mu(\xi)$, а так как либо μ, либо $-\mu + 2^{r-1}$ сравнимо с $1 \pmod 4$, то отсюда следует, что автоморфизмы $\mathbf{Q}(\xi)/\mathbf{Q}$ индуцированы теми σ_μ, для которых $\mu \equiv 1 \pmod 4$, и что они образуют циклическую группу порядка 2^{r-2}. Кроме того, так как $\sigma_{-1}\xi =$

$= -\xi$, то поле $\mathbf{Q}(\xi)$ не вещественно, и потому его локальная степень в бесконечном вещественном нормировании равна 2.

Далее, $[L(2) : L'(2)] = 2$, и те же рассуждения, что и выше, показывают, что при $p \neq \infty$ мы можем заставить $[L'(2)^{(p)}:\mathbf{Q}_p]$ делиться на сколь угодно высокую степень числа 2, если выберем r достаточно большим.

Если теперь простые делители числа m равны $q_1, \ldots, q_n$ и, возможно, 2, то для достаточно большого r композит полей $L'(q_1), \ldots, L'(q_n)$ и, возможно, $L'(2)$ является комплексным циклическим круговым расширением поля $\mathbf{Q}$, локальная степень которого над $\mathbf{Q}_p$ делится на m для всех p из конечного множества S.

Циклические круговые расширения играют главную роль в доказательствах общего закона взаимности. Мы смогли очень просто вывести лемму существования, потому что в нашем распоряжении были и когомологии, и локальная теория. В своем первоначальном доказательстве Артин использовал более тонкую лемму; см., например, [4], стр. 89. (Заметим, что в этой лемме не предполагается неразветвленность дивизора $\mathfrak{p}$.)

Мы можем доказать закон взаимности для функциональных полей аналогичным образом, но только вместо «циклических круговых расширений» нужно будет рассматривать «расширения поля констант».

Этап 3 проходит, если мы заменим «циклическое круговое расширение» на «расширение поля констант»; мы только должны принять в лемме за поле L расширение поля констант, степень которого равна наименьшему общему кратному степеней нормирований из S, умноженному на m.

Для этапа 1 мы непосредственно проверяем закон взаимности для расширений поля констант; действительно, если мы обозначим через σ автоморфизм Фробениуса расширения $\bar{k}/k$, где k — поле констант, то $F(v)$ для каждого нормирования v поля K действует на $\bar{k}$ по формуле $\sigma^{\deg v}$, где $\deg v = [k(v): k]$ — степень v. Значит, $\theta(a)$ действует на $\bar{k}$ по формуле $\prod_v \sigma^{v(a)\deg v} = \sigma^{\sum v(a)\deg v} = \sigma^{\deg a} = 1$, так как $\deg a = 0$ для всех $a \in K^*$ (число нулей алгебраической функции a равно числу полюсов).

§ 11. КОГОМОЛОГИИ КЛАССОВ ИДЕЛЕЙ

III. ФУНДАМЕНТАЛЬНЫЙ КЛАСС

11.1. Пусть $E/L/K$ — конечные расширения Галуа поля K; тогда мы имеем точную коммутативную диаграмму

$$\begin{array}{ccccc}
 & & 0 & 0 & 0 \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & H^2(L/K, L^*) & \to H^2(L/K, J_L) & \to H^2(L/K, G_L) \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & H^2(E/K, E^*) & \to H^2(E/K, J_E) & \to H^2(E/K, C_E) \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & H^2(E/L, E^*) & \to H^2(E/L, J_E) & \to H^2(E/L, C_E)
\end{array} \qquad (1)$$

где мы пишем $H^2(L/K, L^*)$ вместо $H^2(G(L/K), L^*)$ и т. д. В этой диаграмме столбцы образованы последовательностями, состоящими из инфляций и ограничений; они (столбцы) точные, так как $H^1(E/L, E^*) = (0)$ («теорема Гильберта 90», гл. V, п. 2.7), $H^1(E/L, J_E) = (0)$ (следствие 7.4) и $H^1(E/L, C_E) = (0)$ (теорема 9.1) [см. гл. IV, предложение 5.5]. Горизонтальные строки происходят из последовательности $0 \to L^* \to J_L \to C_L \to 0$; они точные, так как снова $H^1(L/K, C_L) = (0)$, и т. д.

Переходя к пределу при $E \to \bar{K}$, где $\bar{K}$ — алгебраическое замыкание поля K, мы получаем новую коммутативную диаграмму

$$\begin{array}{ccccc}
 & & 0 & 0 & 0 \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & H^2(L/K, L^*) & \xrightarrow{\gamma_1} H^2(L/K, J_L) & \xrightarrow{\varepsilon_1} H^2(L/K, C_L) \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & H^2(K, \bar{K}^*) & \xrightarrow{\gamma_2} H^2(K, J_{\bar{K}}) & \xrightarrow{\varepsilon_2} H^2(K, C_{\bar{K}}) \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & H^2(L, \bar{K}^*) & \xrightarrow{\gamma_3} H^2(L, J_{\bar{K}}) & \xrightarrow{\varepsilon_3} H^2(L, C_{\bar{K}})
\end{array} \qquad (2)$$

где мы пишем $H^2(K, \bar{K}^*)$ вместо $H^2(G(\bar{K}/K), \bar{K}^*)$ и т. д. Некоторые отображения, с которыми мы встретимся ниже, отмечены на этой диаграмме.

11.2. Мы собираемся расширить эту диаграмму. Для расширения Галуа L/K существует отображение

$$\mathrm{inv}_1 = \sum_v \mathrm{inv}_v \colon H^2(L/K, J_L) \to \mathbf{Q}/\mathbf{Z},$$

и теорема Б из 10.2 утверждает, что последовательность

$$0 \to H^2(L/K, L^*) \xrightarrow{\gamma_1} H^2(L/K, J_L) \xrightarrow{\mathrm{inv}_1} \mathbf{Q}/\mathbf{Z} \qquad (3)$$

является комплексом [1]).

Так как $\mathrm{inv}_v(\mathrm{infl}\,\alpha) = \mathrm{inv}_v(\alpha)$ для всех $\alpha \in H^2(L/K, J_L)$ (см. п. 9.7 (14)), то мы получаем отображение $\mathrm{inv}_2 \colon H^2(K, J_{\bar K}) \to \mathbf{Q}/\mathbf{Z}$, такое, что диаграмма

$$\begin{array}{ccc} H^2(L/K, J_L) & \xrightarrow{\mathrm{inv}_1} & \mathbf{Q}/\mathbf{Z} \\ {\scriptstyle \mathrm{infl}}\downarrow & & \downarrow{\scriptstyle i} \\ H^2(K, J_{\bar K}) & \xrightarrow{\mathrm{inv}_2} & \mathbf{Q}/\mathbf{Z} \end{array} \qquad (4)$$

где i — тождественное отображение, коммутативна. Кроме того, последовательность

$$0 \to H^2(K, \bar K^*) \xrightarrow{\gamma_2} H^2(K, J_{\bar K}) \xrightarrow{\mathrm{inv}_2} \mathbf{Q}/\mathbf{Z} \qquad (5)$$

является комплексом. Аналогично мы получаем комплекс

$$0 \to H^2(L, \bar K^*) \xrightarrow{\gamma_3} H^2(L, J_{\bar K}) \xrightarrow{\mathrm{inv}_3} \mathbf{Q}/\mathbf{Z}. \qquad (6)$$

Далее, $\mathrm{inv}_w(\mathrm{Res}\,\alpha) = n_{w|v}\,\mathrm{inv}_v(\alpha)$, где $\alpha \in H^2(K, J_{\bar K})$ и w — нормирование поля L, лежащее над v, причем $n_{w|v} = [L_w\colon K_v]$ (см. п. 9.7 (15)). Итак, мы имеем коммутативную диаграмму

$$\begin{array}{ccc} H^2(K, J_{\bar K}) & \xrightarrow{\mathrm{inv}_2} & \mathbf{Q}/\mathbf{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & & \downarrow{\scriptstyle n} \\ H^2(L, J_{\bar K}) & \xrightarrow{\mathrm{inv}_3} & \mathbf{Q}/\mathbf{Z} \end{array} \qquad (7)$$

потому что $\sum_{w|v} n_{w|v} = n = [L\colon K]$.

Теперь образ $\mathrm{Im}\,\varepsilon_2$ отображения ε_2 в группе $H^2(K, C_{\bar K})$ обозначим через $H^2(K, C_{\bar K})_{\mathrm{reg}}$, а $\mathrm{Im}\,\varepsilon_3$ — через

[1]) То есть образ каждого отображения лежит в ядре следующего.

$H^2(L, C_{\bar K})_{\mathrm{reg}}$. Отсюда следует, что мы имеем отображение β_2 (соответственно β_3), индуцированное inv_2 (соответственно inv_3), группы $H^2(K, C_{\bar K})_{\mathrm{reg}}$ в $\mathbf{Q}/\mathbf{Z}$ (соответственно $H^2(L, C_{\bar K})_{\mathrm{reg}}$ в $\mathbf{Q}/\mathbf{Z}$). Таким образом, для $a \in H^2(K, C_{\bar K})_{\mathrm{reg}}$ имеет место $\beta_2(a) = \mathrm{inv}_2(b)$, где $\varepsilon_2(b) = a$ (независимо от выбора b). Мы сейчас объясним устройство двух нижних строк в приведенной ниже диаграмме (9).

Положим

$$H^2(L/K, C_L)_{\mathrm{reg}} = \{a \in H^2(L/K, C_L) \mid \mathrm{infl}\, a \in H^2(K, C_{\bar K})_{\mathrm{reg}}\}. \qquad (8)$$

Тогда $n\beta_2\,\mathrm{infl}\,a = 0$, и потому β_2 индуцирует гомоморфизм

$$\beta_1 \colon H^2(L/K, C_L)_{\mathrm{reg}} \to \frac{1}{n}\mathbf{Z}/\mathbf{Z},$$

такой, что

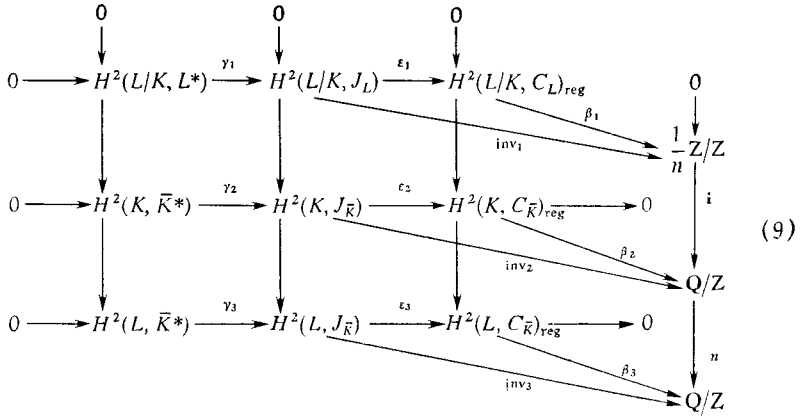
$$\beta_1(a) = \beta_2(\mathrm{infl}\, a).$$

Если $a = \varepsilon_1 b$, причем $b \in H^2(L/K, J_L)$, то

$$\beta_1(a) = \beta_2(\mathrm{infl}\, b) = \mathrm{inv}_2(\mathrm{infl}\, b) = \mathrm{inv}_1(b).$$

(Отметим различие в построении β_1 и β_2: дело в том, что $H^2(L/K, C_L)_{\mathrm{reg}} \supset \mathrm{Im}\,\varepsilon_1$, но, вообще говоря, равенство не имеет места.)

Поместив всю информацию из формул (3) — (6) в диаграмму (2), мы получим новую коммутативную (трехмерную) диаграмму (9)



(9)

в которой i — отображение вложения, n — умножение на n, горизонтальные и вертикальные последовательности точны, а «изогнутые» последовательности являются комплексами.

11.2. (bis) Мы предполагаем показать, что

$$H^2(K, C_K)_{\mathrm{reg}} = H^2(K, C_K) \cong \mathbf{Q}/\mathbf{Z}. \tag{10}$$

$\mathrm{Im}(\mathrm{inv}_1)$ в $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ является в силу следствия 7.4 подгруппой $\frac{1}{n_0}\mathbf{Z}/\mathbf{Z}$, где n_0 — наименьшее общее кратное всех локальных степеней расширения L/K, и потому, так как $\mathrm{Im}\,\beta_1 \supset (\mathrm{inv}_1)$, мы имеем неравенства

$$n \geqslant [H^2(L/K, C_L)] \geqslant [H^2(L/K, C_L)_{\mathrm{reg}}] \geqslant$$
$$\geqslant [\mathrm{Im}\,\beta_1] \geqslant [\mathrm{Im}(\mathrm{inv}_1)] = n_0$$

в силу второго неравенства теоремы 9.1. Отсюда следует, что если $n = n_0$ для этого частного конечного расширения L/K, то *тогда* мы имеем сквозное равенство, так что β_1 — изоморфизм, и последовательность

$$0 \to H^2(L/K, L^*) \xrightarrow{\gamma_1} H^2(L/K, J_L) \xrightarrow{\mathrm{inv}_1} \mathbf{Q}/\mathbf{Z} \tag{11}$$

точная (ибо если $0 = \mathrm{inv}_1(b) = \beta_1\varepsilon_1 b$, то $\varepsilon_1 b = 0$ и $b \in \mathrm{Im}\,\gamma_1$).

Если теперь L/K — конечное циклическое расширение, то $n = n_0$, потому что элементы $F_{L/K}(v)$, степени которых равны локальным степеням n_v, порождают циклическую группу $G(L/K)$ по следствию 8.7. Таким образом, если, в частности, расширение L/K — круговое циклическое, то (11) — точная последовательность. Но лемма из п. 10.5 утверждает, что группы $H^2(K, \bar{K}^*)$ и $H^2(K, J_{\bar{K}})$ являются объединением изоморфных образов относительно инфляции групп $H^2(L/K, L^*)$ и $H^2(L/K, J_L)$ соответственно, где L пробегает все циклические круговые расширения поля K. Следовательно, в нашей коммутативной диаграмме (9) комплексы

$$0 \to H^2(K, \bar{K}^*) \xrightarrow{\gamma_2} H^2(K, J_{\bar{K}}) \xrightarrow{\mathrm{inv}_2} \mathbf{Q}/\mathbf{Z}$$

и

$$0 \to H^2(L, \bar{K}^*) \xrightarrow{\gamma_3} H^2(L, J_{\bar{K}}) \xrightarrow{\mathrm{inv}_3} \mathbf{Q}/\mathbf{Z}$$

точные. Следовательно, $\ker(\mathrm{inv}_2) = \ker(\varepsilon_2)$, так что β_2 (и аналогично β_3) должно быть вложением в $\mathbf{Q}/\mathbf{Z}$. Они сюръективны, так как существуют конечные расширения произвольно высокой локальной степени и, следовательно, inv_2 и inv_3 также сюръективны. Значит, как β_2, так и β_3 — изоморфизмы. Теперь, принимая за L произвольное конечное расширение Галуа, мы заключаем, что β_1 — изоморфизм:

$$H^2(L/K, C_L)_{\mathrm{reg}} \cong \frac{1}{n}\mathbf{Z}/\mathbf{Z};$$

но $H^2(L/K, C_L)_{\mathrm{reg}}$ является подгруппой группы $H^2(L/K, C_L)$, порядок которой делит n. Таким образом, $H^2(L/K, C_L)_{\mathrm{reg}}$ совпадает с $H^2(L/K, C_L)$. Устремляя $L \to \bar{K}$, мы видим, что

$$H^2(L/K, C_{\bar{K}})_{\mathrm{reg}} = H^2(L, C_{\bar{K}}).$$

Следовательно, мы можем удалить значок «reg» из нашей диаграммы (9). Кроме того, мы получили следующий

Результат. *Группа $H^2(L/K, C_L)$ — циклическая порядка n, причем она имеет каноническую образующую $u_{L/K}$ с инвариантом $1/n$, т. е.* $\mathrm{inv}_v(u_{L/K}) = 1/n$.

Этот элемент $u_{L/K}$ называется фундаментальным классом расширения L/K. Его впервые ввел Вейль (см. ниже рассуждения в п. 11.6). Полное описание структуры группы $H^2(L/K, C_L)$ принадлежит Накаяма. Он и Хохшильд первыми дали систематическую когомологическую трактовку теории полей классов; см. [9] и содержащиеся там ссылки.

Две нижние строчки диаграммы (9) и вертикальные стрелки между ними имеют смысл для произвольного сепарабельного расширения L/K конечной степени n, и в этом более общем случае диаграмма все еще коммутативна, потому что рассуждения, показывающие коммутативность диаграммы (7), не требуют нормальности расширения. Используя это и заменяя L на K', мы видим, что если $L \supset K' \supset K$, причем L/K — расширение Галуа, то ограничение $u_{L/K}$ с L/K до L/K' дает фундаментальный класс $u_{L/K'}$.

11.3. *Приложения.* Полученные результаты показывают, что классы иделей образуют *формацию классов*. В частности (см. гл. IV, § 10), $\cup$-умножение на фундаментальный

класс $u_{L/K}$ дает изоморфизм

$$\hat{H}^r(G(L/K), \mathbf{Z}) \cong \hat{H}^{r+2}(G(L/K), C_L)$$

при $-\infty < r < \infty$, так что для $L \supset K' \supset K$ с нормальным расширением L/K диаграммы

$$\begin{array}{ccc} \hat{H}^r(G, \mathbf{Z}) \cong \hat{H}^{r+2}(G, C_L) & & \hat{H}^r(G, \mathbf{Z}) \cong \hat{H}^{r+2}(G, C_L) \\ \text{Res}\downarrow \qquad\qquad \text{Res}\downarrow & \text{и} & \uparrow \text{Cor} \qquad\qquad \uparrow \text{Cor} \\ H^r(G', \mathbf{Z}) \cong \hat{H}^{r+2}(G', C_L) & & \hat{H}^r(G', \mathbf{Z}) \cong \hat{H}^{r+2}(G, C_L) \end{array} \tag{12}$$

где $G = G(L/K)$ и $G' = G(L/K')$, коммутативны.

Случай $r = -2$. Существует канонический изоморфизм

$$G(L/K)^{\text{ab}} \to C_K/N_{L/K}C_L$$

(см. гл. IV, § 3), обратный к отображению Артина. Используя это как *определение* в локальном случае, Серр вывел формулу $\text{inv}(\bar{a}\cdot\delta\chi) = \chi(\theta(a))$ (см. гл. VI, п. 2,3); мы доказали формулу в глобальном случае, поэтому можно обратить рассуждения. (Изоморфизм $G^{\text{ab}} \cong H^{-2}(G, \mathbf{Z})$ выбирается таким образом, что для $\chi \in \text{Hom}(G, \mathbf{Q}/\mathbf{Z}) \cong H^1(G, \mathbf{Q}/\mathbf{Z})$ и $\sigma \in G$ мы имеем $\chi\cdot\sigma = \chi(\sigma)$ при обычном отождествлении $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ с $H^{-1}(G, \mathbf{Q}/\mathbf{Z})$.)

Обращая горизонтальные стрелки в (12) при $r = -2$ и устремляя $L \to \overline{K}$, мы получаем коммутативные диаграммы

$$\begin{array}{ccc} C_K \xrightarrow{\psi} G(K^{\text{ab}}/K) & & C_K \xrightarrow{\psi} G(K^{\text{ab}}/K) \\ \text{Con}\downarrow \qquad\qquad \downarrow V & \text{и} & N\uparrow \qquad\qquad \uparrow \\ C_{K'} \xrightarrow{\psi'} G((K')^{\text{ab}}/K') & & C_{K'} \xrightarrow{\psi'} G((K')^{\text{ab}}/K') \end{array} \tag{13}$$

где ψ — отображения Артина и V — перенесение. Правая диаграмма выражает так называемую *теорему перенесения* и в действительности следует также непосредственно из предложения 4.3, которое выводится из почти очевидного свойства 3.2 автоморфизмов Фробениуса $F(v)$. Коммутативность левой диаграммы (13) может быть доказана непосредственно, но несколько больше дают вычисления с автоморфизмами Фробениуса, что было впервые проделано Артином в связи с «теоремой главных идеалов» (см. упражнение 3 и [7], стр. 130).

Случай $r = -3$. Это приводит к изоморфизму, использованному Рокеттом в гл. IX, § 2.

11.4. *Приложение к когомологиям группы* L^*. Общая идея состоит в определении когомологий L^* через когомологии иделей и классов иделей.

Пусть L/K — конечное расширение с группой Галуа G. Тогда точная последовательность $0 \to L^* \to J_L \to C_L \to 0$ порождает точную последовательность

$$\to \hat{H}^{r-1}(G, J_L) \xrightarrow{g} \hat{H}^{r-1}(G, C_L) \to$$

$$\to \hat{H}^r(G, L^*) \xrightarrow{f} \hat{H}^r(G, J_L) \to \dots,$$

в которой ядро отображения f изоморфно коядру отображения g. Мы знаем, что

$$\hat{H}^{r-1}(G, J_L) = \coprod_{v\in\mathfrak{M}_K} \hat{H}^{r-1}(G^v, L^{v*}) = \coprod_{v\in\mathfrak{M}_K} H^{r-3}(G^v, \mathbf{Z})$$

(см. предложение 7.3) и

$$\hat{H}^{r-1}(G, C_L) = \hat{H}^{r-3}(G, \mathbf{Z}),$$

так что ядро отображения

$$f\colon \hat{H}^r(G, L^*) \to \prod \hat{H}^r(G^v, L^{v*})$$

изоморфно коядру отображения

$$g_1\colon \prod \hat{H}^{r-3}(G^v, \mathbf{Z}) \to \hat{H}^{r-3}(G, \mathbf{Z}).$$

Легко видеть, что отображение g_1 задается формулой

$$g_1\left(\sum_v z_v\right) = \sum_v \text{Cor}_{G^v}^{G} z_v.$$

Используя фундаментальную теорему двойственности о когомологиях конечных групп, которая утверждает, что спаривание относительно $\cup$-умножения

$$\hat{H}^r(G, \mathbf{Z}) \times \hat{H}^{-r}(G, \mathbf{Z}) \to \hat{H}^0(G, \mathbf{Z}) \cong \mathbf{Z}/n\mathbf{Z}$$

дает точную двойственность конечных групп, мы видим, что коядро отображения g_1 двойственно ядру отображения

$$h\colon \hat{H}^{3-r}(G, \mathbf{Z}) \to \prod_v \hat{H}^{3-r}(G^v, \mathbf{Z}),$$

которое определяется формулой $(h(z))_v = \mathrm{Res}^G_{G_v}(z)$ для всех $v \in \mathfrak{M}_K$.

Случай $r = 0$.

$$\ker f = \left(\frac{a \mid a \in K^*,\ a \text{ всюду является локальной нормой}}{a \mid a \in K^*,\ a \text{—глобальная норма}}\right),$$

а $\operatorname{coker} g$ двойственно к $\ker(H^3(G, \mathbf{Z}) \xrightarrow{\mathrm{Res}} \prod_v H^3(G^v, \mathbf{Z})$. Например, если $G = G^v$ для некоторого v, то это — вложение, так что локальные нормы совпадают с глобальными. Если группа G циклическая, то $H^3(G, \mathbf{Z}) \cong H^1(G, \mathbf{Z}) = 0$, так что локальные нормы являются и глобальными нормами, и мы вернулись к теореме Хассе 9.6. С другой стороны, если, например, G — четвертая группа (Vierergruppe), то возможно, что G^v всегда одна из подгрупп порядка 2, так что $\hat{H}^3(G^v, \mathbf{Z}) = 0$, но $H^3(G, \mathbf{Z}) = \mathbf{Z}/2\mathbf{Z}$. Мы можем рассмотреть $\mathbf{Q}(\sqrt{13}, \sqrt{17})/\mathbf{Q}$; здесь $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = 1$, и расширение не разветвлено относительно числа 2, потому что $13 \equiv 17 \equiv 1 \pmod 4$; таким образом, все группы разложения циклические. Поэтому множество элементов K^*, которые всюду локально являются нормами, не совпадает с множеством глобальных норм (см. упражнение 5).

Случай $r = 3$. Группа $H^3(G, L^*)$ — циклическая порядка n/n_0 (глобальная степень, деленная на наименьшее общее кратное локальных степеней); эта группа порождается элементом $\delta u_{L/K}$ ($\delta\colon H^2(C_L) \to H^3(L^*)$), называемым «коциклом Тейхмюллера». Она может быть аннулирована инфляцией (заменим L на большее поле L', такое, что n_0 для L' делится на n); таким образом, $H^3(\bar{K}/K, \bar{K}^*) = 0$.

О более точном описании, анонсированном в Amsterdam Congress (Proc. II, 66—67), см. [8].

Расширения групп. Рассмотрим расширения $M/L/K$, где L/K — нормальное расширение с группой Галуа G, расширение M/K имеет группу Галуа E и M — поле классов поля L с абелевой группой Галуа A; таким образом, последовательность $1 \to A \to E \to G \to 1$ точна. В силу изоморфизма Артина имеет место $A \cong C_L/N_{M/L}C_M$ (см. теорему из п. 10.2 и следствие 9.4). Мы хотим изучить группу E.

11.5. Т е о р е м а. (i) *Пусть* $\sigma \in E$ *имеет образ* $\bar{\sigma} \in G$, *и пусть* $x \in C_L$; *тогда* $\psi(\bar{\sigma}x) = \sigma\psi(x)\sigma^{-1}$, *где* $\psi\colon G_L \to A$ — *отображение Артина.*

(ii) *Пусть* $v \in H^2(G, A)$ — *класс расширений, содержащий группу* E; *тогда* $v = \psi_*(u_{L/K})$, *где* ψ_* — *отображение* $H^2(G, C_L) \to H^2(G, A)$, *индуцированное отображением* $\psi\colon C_L \to A$, *и* $u_{L/K}$ — *фундаментальный класс для* L/K.

Утверждение (i) очевидно. Как обычно в таких случаях, ситуация становится яснее, если рассмотреть произвольный изоморфизм полей $\sigma\colon M \to M'$, а не автоморфизм. Обозначим σL через L' и ограничение σ на L — через $\bar{\sigma}$; мы получаем следующую картину:

$$\begin{array}{ccc} M & \xrightarrow{\sigma} & M' \\ | & & | \\ L & \xrightarrow{\bar{\sigma}} & L' \end{array}$$

Перенося структуру M/L на M'/L', мы видим что если $x \in C_L$ и $y \in M$, то $(\psi'(\bar{\sigma}x))(\sigma y) = \sigma(\psi(x)(y))$.

Утверждение (ii) нетривиально, Шафаревич доказал это в локальном случае (см. [10]), но по существу это общая теорема о *формациях классов* (см. [1], стр. 246). Мы не будем доказывать этого здесь и не будем пользоваться какими-либо результатами этих работ.

11.6. Когда структура группы $H^2(G, C_L)$ была еще неизвестна, Вейль [3] рассматривал эту ситуацию с противоположной точки зрения. Приняв за M поле L^{ab} — максимальное абелево расширение поля K (так что $A = G(L^{\mathrm{ab}}/L)$ — проконечная абелева группа), Вейль спро-

сил себя, существует ли расширение $\mathscr{E}$ группы $G = G(L/K)$ с помощью C_L, которое входит в коммутативную диаграмму вида

$$\begin{array}{ccccccc} 1 & \to & C_L & \to & \mathscr{E} & \to & G \to 1 \\ & & \downarrow \psi_L & & \downarrow W & & \downarrow \mathrm{id} \\ 1 & \to & A & \to & E & \to & G \to 1 \end{array} \tag{14}$$

где $E = G(L^{ab}/K)$, и если это так, то единственно ли такое расширение? В случае функционального поля ψ_L является изоморфизмом и существование такой диаграммы очевидно. Более того, в этом случае теоретико-групповое отображение перенесения группы $\mathscr{E}$ в C_L (образ которого содержится в C_K), дает коммутативную диаграмму

$$\begin{array}{ccc} \mathscr{E} & \xrightarrow{V} & C_K \subset C_L \\ {\scriptstyle W}\downarrow & & \downarrow \psi_K \\ E & \to & E^{ab} \end{array} \tag{15}$$

что следует из коммутативности левой диаграммы (13). Вдохновленный функциональным случаем, Вейль доказал, что в случае числового поля диаграмма (14) тоже существует и однозначно определена тем условием, что диаграмма (15) (вместе с аналогичными диаграммами, в которых K заменено на произвольное промежуточное между K и L поле K') коммутативна. В частности, класс $u \in H^2(G, C_L)$ такого расширения однозначно определен, что проясняет структуру фундаментального класса.

Теперь можно действовать более непосредственно, просто конструируя $\mathscr{E}$ как расширение группы G с помощью C_L, соответствующее фундаментальному классу $u_{L/K}$, и интерпретируя единственность как следствие того, что $H^1(G, C_L) = 0$ (см. [1], гл. XIV).

Ядро отображения $W: \mathscr{E} \to E$ — это связная компонента D_L в C_L. Как заметил Вейль, поиск интерпретации $\mathscr{E}$ на языке теории Галуа (или даже просто «естественной» конструкции, без обращения к факторсистемам, вместе с «естественным» отображением $W: \mathscr{E} \to E$), по-видимому, является одной из фундаментальных задач теории чисел.

Для обоснования предположения, что $\mathscr{E}$ ведет себя как группа Галуа, Вейль описал также, как связать L-ряды с характерами χ унитарных представлений группы $\mathscr{E}$.

Эти L-ряды Вейля одновременно обобщают L-ряды Гекке характеров Гекке (которые получаются из представлений через посредство C_K с помощью стрелки V в диаграмме (15)) и «неабелевы» L-ряды Артина (которые получаются из представлений через посредство E или, в частности, через посредство изоморфизма $G \cong E/A$ с помощью стрелки W в (15)). («Пересечением» рядов Артина и Гекке являются ряды Вебера, полученные из представлений группы $E^{ab} \cong C_K/D_K$, т. е. из обычных характеров.) Используя теорему Брауэра о характерах групп, Вейль показал, что его L-ряды могут быть выражены в виде произведения целых (положительных и отрицательных) степеней L-рядов Гекке и, следовательно, мероморфны.

§ 12. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ СУЩЕСТВОВАНИЯ

Мы еще должны доказать теорему существования (Г) из п. 5.1. Наше доказательство, более традиционное, чем доказательство, использованное Серром в гл. VI, так же хорошо проходит и в локальном случае.

Пусть H — открытая подгруппа группы C_K конечного индекса; мы будем называть подгруппу H *норменной*, если существует абелево расширение L/K, такое, что $H = N_{L/K}C_L$. Теорема существования утверждает, что любая открытая подгруппа H конечного индекса в C_K является норменной. (Мы уже показали, что если L/K — абелево расширение, то $N_{L/K}C_L$ — открытая подгруппа группы C_K конечного индекса; фактически норменные подгруппы являются в точности прообразами открытых подгрупп группы $G(K^{ab}/K)$ относительно отображения Артина ψ_K: $C_K \to G(K^{ab}/K)$.

Прежде всего два очевидных замечания: если $H_1 \supset H$ и подгруппа H — норменная, то подгруппа H_1 — тоже норменная (поле L, соответствующее H, обладает подполем L_1, соответствующим H_1). Если подгруппы H_1 и H_2 — норменные, то и подгруппа $H_1 \cap H_2$ тоже норменная (соответствует композиту L_1L_2).

Вернемся к 9.5, чтобы доказать следующее утверждение.

Ключевая лемма. *Пусть n — простое число и K — поле характеристики, отличной от n, содержащее*

корни n-й степени из единицы. Тогда каждая открытая подгруппа H индекса n в C_K — норменная.

Доказательство. Действительно, предположим, что H открыта в C_K, причем $[C_K : H] = n$. Пусть H' — прообраз H в J_K. Тогда H' открыта в J_K, так что существует конечное множество $S \subset \mathfrak{M}_K$, такое, что H' содержит $\prod_{v \in S} (1) \times \prod_{v \notin S} U_v = U^S$. Более того, так как H имеет индекс n в C_K, то $H' \supset J_K^n$. Следовательно, $H' \supset \prod_{v \in S} K^{*n} \times \prod_{v \notin S} U_v$; обозначим последнее произведение через E. Таким образом, $H = H'/K^* \supset EK^*/K^*$, и из следствия 9.5 мы получаем, что H — норменная подгруппа.

Если L — расширение поля K, то существует норменное отображение $N: C_L \to C_K$; следовательно, если мы начинали с $H \subset C_K$, то мы получаем подгруппу $N^{-1}(H) \subset C_L$.

Лемма. *Если L/K — циклическое расширение и $H \subset C_K$, и если $N_{L/K}^{-1}(H) \subset C_L$ — норменная подгруппа для поля L, то H — норменная для поля K.*

Доказательство. Обозначим $N_{L/K}^{-1}(H)$ через H'. Пусть M/L — поле классов подгруппы H'. Мы утверждаем, что M абелево над K и $N_{M/K}C_M \subset H$, так что подгруппа H — норменная. Ясно, что $N_{M/K}C_M \subset H$, так как N транзитивно; труднее показать, что M/K — абелево расширение.

(На самом деле норменная подгруппа неабелева расширения является норменной подгруппой уже для его максимального абелева подрасширения (см. упражнение 8). Но это не было здесь доказано; если бы это было сделано, нам была бы не нужна цикличность расширения L/K и мы уже завершили бы доказательство леммы.)

M/K — расширение Галуа, так как H' инвариантна относительно $G(L/K)$. Группа Галуа E расширения M/K является расширением группы G: $0 \to A \to E \to G \to 0$; так как $E/A \cong G$ — циклическая группа, то достаточно показать, что $A = G(M/L)$ лежит в центре группы E.

Мы можем воспользоваться первой частью теоремы 11.5. Пусть ψ — отображение Артина $C_L \to A$. Для того чтобы показать, что A лежит в центре, достаточно проверить, что

$$\psi(x) = \sigma\psi(x)\sigma^{-1} = \psi(\sigma x)$$

для всех $x \in C_L$ и $\sigma \in E$. Далее, ядро отображения ψ: $C_L \to A$ равно H', так что нужно лишь проверить, что $\sigma x/x \in H'$, а это очевидно, так как $N(\sigma x/x) = 1$.

Доказательство теоремы. (В случае функционального поля мы можем рассматривать только тот случай, когда индекс взаимно прост с характеристикой; об общем случае см. [1], стр. 78.)

Мы проведем индукцию по индексу подгруппы H.

Если индекс равен 1, то утверждение очевидно.

Теперь пусть n — простой делитель индекса. Присоединив корни n-й степени из единицы к полю K, получим поле K'; заменим H на $H' = N_{K'/K}^{-1}(H)$. В силу последней леммы достаточно рассмотреть H'. Индекс H' делит индекс H; мы можем считать, что $(C_{K'} : H') = (C_K : H)$, в противном случае H' будет норменной подгруппой по предположению индукции.

Таким образом, n делит $(C_{K'} : H')$. Выберем H_1' так, чтобы $H_1' \supset H$ и $(C_{K'} : H') = n$. По ключевой лемме подгруппа H_1' — норменная. Пусть L — ее поле классов, т. е. $H_1' = N_{L/K'}C_L$. Положим $H'' = N_{L/K'}^{-1}(H')$. Тогда

$$[C_L : H''] < [C_{K'} : H'] = [C_K : H].$$

(Действительно, отображение $C_L/H'' \xrightarrow{N_{L/K'}} C_{K'}/H'$ является вложением с образом H_1'/H', собственно содержащимся в $C_{K'}/H'$.)

Следовательно, подгруппа H'' — норменная по предположению индукции; L/K' — циклическое расширение, так что мы можем снова применить лемму; поэтому H' — норменная подгруппа.

СПИСОК ОБОЗНАЧЕНИЙ

Цифры обозначают номера пунктов этой главы, в которых символ был впервые использован. Напомним: (i) $[A]$ — мощность множества A, (ii) $\supset$ обозначает включение с возможностью равенства.

1.1. K, K^* (ненулевые элементы из K)
$G(L/K)$, G
$v, v_1, \ldots; w, w_1, \ldots$
$\mathfrak{O}_v$, $\mathfrak{O}_w$
$\mathfrak{P}_v$
K_v, L_w
G_w

1.2. $\mathfrak{M}_K$

2.1. $k(v)$
$N(v)$

2.2. $F_{L/K}(v)$
S

3.1. I^S

3.2. $N_{K'/K}$
$(a)^S$

4. J_K, J_K^S
$(x)^S$

4.1. ψ
C_K
$(x)_S$
U^S

4.2. $\psi_{L/K}$
$\operatorname{Im}\psi$

5.1. Нормированная группа

5.5. $\hat{\mathbf{Z}}$

5.7. $\mathbf{Q}^{mc}$, $\mathbf{R}_+^*$

6.1. ψ_v

7.1. $w \mid v$, $\coprod_{w|v}$

7.2. G^v
L^v

7.3. $\coprod$
$J_{K,\,S}$, $S \subset \mathfrak{M}_K$
$J_{L,\,S}$, $S \subset \mathfrak{M}_K$
N_v

8.1. $h(G, A)$, $h(A)$
S-единицы $= K_S$

9.1. Конорма $=$ Con

9.7. inv_v
inv_v (infl)
inv_v (Res)
inv_v (Cor)
$\operatorname{Br}(K)$

10.1. θ_v, θ — отображения Артина

10.3. $\cup$-умножение
G^{ab}

ЛИТЕРАТУРА

Артин, Тэйт (Artin E., Tate J.)
[1] Class field theory, Harvard, 1961.

Ванг (Wang S.)
[2] On Grundwald's theorem, *Ann. Math.*, **51** (1950), 471—484.

Вейль (Weil H.)
[3] Sur la théorie du corps de classes, *J. Math. Soc. Japan*, **3** (1951), 1—35.

Ленг (Lang S.)
[4] Algebraic numbers, Addison Wesley, 1964. (Русский перевод: Ленг С., Алгебраические числа, «Мир», М., 1966.)
[5] Sur les séries L d'une variété algébrique, *Bull. Soc. Math. Fr.*, **84** (1956), 385—407.

Серр (Serre J.-P.)
[6] Groupes algébriques et corps de classes, Hermann, Paris, 1959. (Русский перевод: Серр Ж.-П., Алгебраические группы и поля классов, «Мир», М., 1968.)
[7] Corps locaux, Hermann, Paris, 1962.

Тэйт (Tate J).
[8] The cohomology groups of tori in finite Galois extensions of number fields, *Nagaya Math. J.*, **27** (1966), 709—719.

Хохшильд, Накаяма (Hochschild G., Nakayama T.)
[9] Comology in class field theory, *Ann. Math.*, **55** (1952), 348—366.

Шафаревич И. Р.
[10] О группах Галуа P-адических полей, *ДАН*, **53** (1946), 15—16.

Шевалле (Chevalley C.)
[11] La theorie du corps de classes, *Ann. Math.*, **41** (1940), 394—418.

Шимура (Shimura G.)
[12] A reciprocity law in non-solvable extensions, *Crelle's J.*, **221** (1966), 209—220.
[13] On the field of definition for a field of automorphic functions, II, *Ann. Math.*, **81** (1965), 124—165.

Шимура, Танияма (Shimura G., Taniyama J.)
[14] Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, № 6, 1961.

ГЛАВА VIII

ζ-функции и L-функции

Х. Хейльброн

Тема этой главы — изучение распределения простых идеалов в различных полях алгебраических чисел. Основные результаты будут собраны в так называемых «теоремах плотности». Такова, например, теорема о простых идеалах (теорема 2.3) и теорема Чеботарева (§ 3). Как и при изучении законов распределения простых чисел, в этих исследованиях важную роль играют L-ряды, связанные с некоторыми групповыми характерами.

Бóльшая часть этих результатов восходит к началу века и описана у Хассе [14].

§ 1. ХАРАКТЕРЫ

Пусть k — конечное расширение поля $\mathbf{Q}$ степени ν. Обозначим через S некоторое множество, состоящее из всех бесконечных (архимедовых) нормирований поля k и еще из конечного числа простых идеалов (неархимедовых нормирований) поля k. S часто будет называться *исключительным* множеством.

Произведем небольшое изменение принятых ранее обозначений: идель x поля k будем записывать в виде

$$x=(x_{\mathfrak{p}_1}, \ldots, x_{\mathfrak{p}_a}; x_{\mathfrak{p}_{a+1}}, \ldots, x_{\mathfrak{p}_b}; x_{\mathfrak{p}_{b+1}}, \ldots),$$

где $\mathfrak{p}_1, \ldots, \mathfrak{p}_a$ — бесконечные нормирования, $\mathfrak{p}_{a+1}, \ldots, \mathfrak{p}_b$ — конечные нормирования из S, а оставшиеся $\mathfrak{p}_i$ нормирований не содержатся в S. Через J будет обозначаться группа иделей.

[1]) Подготовлено для печати Б жиёдсом и Хальберштамом.

Под характером ψ группы классов иделей мы понимаем гомоморфизм группы J в единичную окружность на комплексной плоскости, обладающий следующими свойствами:

(i) $\psi(x)=1$, если $x\in k^*$ (т. е. $x_{\mathfrak{p}}=x$ для всех $\mathfrak{p}$);

(ii) $\psi(x)$ непрерывна на J (в топологии иделей);

(iii) $\psi(x)=1$, если $x_{\mathfrak{p}}=1$ для $\mathfrak{p}\in S$ и $|x_{\mathfrak{p}}|_{\mathfrak{p}}=1$ для $\mathfrak{p}\notin S$.

Как было указано в гл. VII, § 4, ψ индуцирует характер на группе идеалов I^S (свободной абелевой группе на множестве всех $\mathfrak{p}\notin S$) следующим образом.

Пусть

$$\mathfrak{a}=\prod_{i>b}\mathfrak{p}_i^{\alpha_i}\quad(\alpha_i\in\mathbf{Z})$$

— произвольный элемент из I^S (почти все показатели α_i равны 0). Для каждого $i>b$ обозначим через π_i элемент из k с максимальной нормой $|\pi_i|_{\mathfrak{p}_i}$, удовлетворяющей условию $|\pi_i|_{\mathfrak{p}_i}<1$. Это позволит ассоциировать с идеалом $\mathfrak{a}$ некоторый идель $x^{\mathfrak{a}}$, а именно:

$$(x^{\mathfrak{a}})_{\mathfrak{p}_i}=\begin{cases}1, & i=1, 2, \ldots, b,\\ \pi_i^{\alpha_i}, & i=b+1, \ldots;\end{cases}$$

положим теперь

$$\chi(\mathfrak{a})=\psi(x^{\mathfrak{a}}).$$

Заметим, что хотя выбор $x^{\mathfrak{a}}$ не однозначен, характер $\chi(\mathfrak{a})$ определен однозначно ввиду свойства (iii). Очевидно, что функция χ мультипликативна в том смысле, что для всех пар идеалов $\mathfrak{a}$, $\mathfrak{b}$, взаимно простых с простыми идеалами из S,

$$\chi(\mathfrak{ab})=\chi(\mathfrak{a})\chi(\mathfrak{b}).$$

Каждый характер, полученный таким образом, называется характером Гекке. Такие характеры впервые изучались Гекке [6] и позже Шевалле [16] в рамках теории иделей.

Пусть S и S' —два исключительных множества, а χ и χ'— характеры на I^S и $I^{S'}$ соответственно. Мы скажем, что χ и χ' *согласованы*, если $\chi(\mathfrak{a})=\chi'(\mathfrak{a})$ там, где оба характера определены. Это определение задает отношение экви-

валентности между характерами [1]). В классе эквивалентности χ существует единственный характер χ', соответствующий наименьшему возможному исключительному множеству S' (S' будет пересечением всех множеств S, соответствующих характерам, согласованным с χ); этот характер χ' будем называть *примитивным* характером, согласованным с χ.

Главный характер χ_0 группы I^S определяется равенством $\chi_0(\mathfrak{a}) = 1$ для всех $\mathfrak{a} \in I^S$. Главные характеры образуют класс эквивалентности, и примитивный характер в этом классе равен 1 для всех ненулевых конечных идеалов.

Сейчас мы рассмотрим более тщательно структуру характера на группе идеалов I^S, чтобы определить в дальнейшем важные классы характеров Гильберта и Дирихле.

Мы можем записать всякий идель x в виде

$$x = \prod_{\mathfrak{p}} x(\mathfrak{p}),$$

где каждый сомножитель $x(\mathfrak{p})$ — это идель, определенный следующим образом:

$$x(\mathfrak{p})_{\mathfrak{p}_i} = \begin{cases} x_{\mathfrak{p}_i}, & \mathfrak{p} = \mathfrak{p}_i; \\ 1, & \mathfrak{p} \neq \mathfrak{p}_i. \end{cases}$$

Тогда

$$\psi(x) = \prod_{\mathfrak{p}} \psi_{\mathfrak{p}}(x),$$

где $\psi_{\mathfrak{p}}$ — это характер на J, определенный формулой

$$\psi_{\mathfrak{p}}(x) = \psi(x(\mathfrak{p}));$$

его мы будем называть локальной компонентой ψ (Шевалле [16]). Заметим, что $\psi_{\mathfrak{p}}$ непрерывен и удовлетворяет свойству (iii). Выведем теперь несколько следствий из непрерывности ψ.

[1]) Чтобы доказать транзитивность отношения, достаточно показать, что если $\psi(y) = 1$ для всех иделей y, у которых $y_{\mathfrak{p}_i} = 1$, $i = 1, 2, \ldots, m$, то $\psi(x) = 1$ для всех иделей x. Заметим, что по «китайской теореме об остатках» для любого $\varepsilon > 0$ существует такое $\alpha \in k^*$, что

$$|\alpha - x_{\mathfrak{p}_i}|_{\mathfrak{p}_i} < \varepsilon, \quad i = 1, 2, \ldots, m.$$

Следовательно, $\psi(x) = \psi(\alpha^{-1}x)$ стремится к 1 при $\varepsilon \to 0$.

Пусть $\mathscr{N}$ — окрестность единицы, не содержащая подгрупп группы $\psi(J)$, исключая $\{1\}$. По непрерывности ψ в J существует такая окрестность единицы $\mathscr{N}'$, т. е. множество иделей x, удовлетворяющих условиям

$$|x_{\mathfrak{p}} - 1|_{\mathfrak{p}} < \varepsilon_{\mathfrak{p}}, \qquad \mathfrak{p} \in E, \tag{1}$$

$$|x_{\mathfrak{p}}|_{\mathfrak{p}} = 1, \qquad \mathfrak{p} \notin E, \tag{2}$$

где E — некоторое конечное множество нормирований, что

$$\psi(\mathscr{N}') \subset \mathscr{N}.$$

Выберем $\mathscr{N}'$ канонически, рассмотрев сначала минимально возможное E, и при этом фиксированном E такое максимальное $\varepsilon_{\mathfrak{p}}$, что $\varepsilon_{\mathfrak{p}} \leqslant 1$ для конечных $\mathfrak{p} \in E$. Для конечного $\mathfrak{p}$ условие (1) эквивалентно тому, что $x_{\mathfrak{p}} \in 1 + \mathfrak{p}^{\mu_{\mathfrak{p}}}$, где $\mu_{\mathfrak{p}}$ положительно. Но так как множество $1 + \mathfrak{p}^{\mu_{\mathfrak{p}}}$ — группа, то $\psi_{\mathfrak{p}}(1 + \mathfrak{p}^{\mu_{\mathfrak{p}}})$ также группа, и потому $\psi_{\mathfrak{p}}(1 + \mathfrak{p}^{\mu_{\mathfrak{p}}}) = 1$, а это не может иметь места, если показатель степени $< \mu_{\mathfrak{p}}$. Рассмотрим идеал

$$\mathfrak{f}_\chi = \prod_{\substack{\mathfrak{p} \text{ конечно} \\ \mathfrak{p} \in E}} \mathfrak{p}^{\mu_{\mathfrak{p}}};$$

назовем его *кондуктором* характера χ, произведенного характером ψ. Если $\mathfrak{p}$ конечно и принадлежит E, то из формулы (1) и свойства (iii) следует, что $\mathfrak{p} \in S$. Более того, если $\mathfrak{p}$ конечно и не лежит в E, условие (2) показывает, что ввиду (iii) $\mathfrak{p}$ не обязательно включать в S. Поэтому конечные $\mathfrak{p}$ из E — это неархимедовы нормирования из исключительного множества для примитивного характера, согласованного с χ.

Пусть $\mathfrak{m}$ — некоторый целый идеал из k, а χ — такой характер, что $\mathfrak{f}_\chi \mid \mathfrak{m}$. Пусть далее $\mathfrak{a} = (\alpha)$, где $\alpha \equiv 1 \pmod{\mathfrak{m}}$; тогда

$$\chi(\mathfrak{a}) = \psi(1, \ldots, 1; 1, \ldots, 1; \alpha, \alpha, \ldots) = \\ = \psi(\alpha^{-1}, \ldots, \alpha^{-1}; \alpha^{-1}, \ldots, \alpha^{-1}; 1, 1, \ldots) =$$

в силу (i)

$$= \psi(\alpha^{-1}, \ldots, \alpha^{-1}; 1, \ldots, 1; 1, 1, \ldots),$$

потому что $\alpha^{-1} \in 1 + \mathfrak{p}^{\mu_\mathfrak{p}}$ для конечных $\mathfrak{p} \in S$. Следовательно,

$$\chi(\mathfrak{a}) = \prod_{\mathfrak{p} \in S_0} \psi_\mathfrak{p}(\alpha^{-1}),$$

где S_0 — множество архимедовых нормирований.

Теперь мы ограничимся изучением таких характеров χ, для которых $\psi_\mathfrak{p}(J)$ — дискретное подмножество единичной окружности при всех $\mathfrak{p} \in S_0$. Рассмотрим какой-нибудь идеал $\mathfrak{p} \in S_0$. Существует такое целое число m, что

$$\psi_\mathfrak{p}(x^m) = 1 \quad \text{для всех } x \in J;$$

в частности, это верно для всех $x \in k^*$. Пополнением $k_\mathfrak{p}$ является $\mathbf{R}$ или $\mathbf{C}$ в зависимости от того, вещественен или комплексен идеал $\mathfrak{p}$. Каждое x из k^* отображается в некоторый $\mathfrak{p}$-сопряженный к нему элемент $x_\mathfrak{p}$. Гомоморфное, имеющее конечный порядок отображение $\mathbf{C}^*$ в единичную окружность должно всю группу $\mathbf{C}^*$ отображать в $\{1\}$ и аналогично гомоморфное отображение $\mathbf{R}^*$ конечного порядка в единичную окружность должно всю группу $\mathbf{R}^*$ отображать либо в $\{1\}$, либо в $\{\pm 1\}$ (посредством отображения $x \to \operatorname{sgn} x$). Таким образом, если $\mathfrak{p}$ — комплексное нормирование, то $\psi_\mathfrak{p}$ — тождественная единица, а если $\mathfrak{p}$ вещественно, то компонента $\psi_\mathfrak{p}$ или тождественно равна 1, или равна ± 1. В последнем случае мы имеем для $x \in k^*$

$$\psi_\mathfrak{p}(x) = \begin{cases} 1, & x^{(\mathfrak{p})} > 0; \\ -1, & x^{(\mathfrak{p})} < 0. \end{cases}$$

Если $x^{(\mathfrak{p})} > 0$ для всех вещественных $\mathfrak{p} \in S_0$, мы скажем, что x *всюду положителен*, и запишем это так: $x \gg 0$. Таким образом, если ψ имеет дискретные бесконечные компоненты, то χ — это характер, определенный на подгруппе всюду положительных главных идеалов, которые $\equiv 1 \pmod{\mathfrak{m}}$. Такой характер называется *характером Дирихле* по модулю $\mathfrak{m}$; если $\mathfrak{m} = 1$, то χ называется *характером Гильберта*.

Сейчас мы покажем, что, обратно, каждый характер на группе идеалов I^S, равный 1 на подгруппе $H^{(\mathfrak{m})}$ всюду положительных главных идеалов, сравнимых с 1 по модулю $\mathfrak{m}$, получается из некоторого характера χ на группе классов иделей с исключительным множеством S. (Здесь S состоит из архимедовых нормирований и простых идеалов, делящих $\mathfrak{m}$.) Пусть χ — такой характер, а χ^*, χ_1 — его ограничения соответственно на группу A^S главных идеалов, взаимно простых с $\mathfrak{m}$, и на группу главных идеалов, сравнимых с 1 по модулю $\mathfrak{m}$. Тогда $\chi_1(\alpha)$ определяется знаком элементов, вещественно сопряженных к α. Доопределим этот характер для всех элементов α из k^* очевидным образом. Рассмотрим $\chi_2 = \chi^* \chi^{-1}$; очевидно, что χ_2 — характер на A^S, равный 1 на $B^{(\mathfrak{m})}$.

Определим характер ψ, соответствующий χ, постепенно. Для всякого иделя x и каждого $\mathfrak{p}$, не принадлежащего S, положим

$$\psi_\mathfrak{p}(x) = \chi(\mathfrak{p}^{\nu_\mathfrak{p}}), \quad \text{где} \quad \mathfrak{p}^{\nu_\mathfrak{p}} \| x_\mathfrak{p}\ ^1). \tag{3}$$

Эта часть определения ψ уже достаточна, чтобы проверить, что ψ обладает свойством (iii).

Рассмотрим теперь конечные простые идеалы из S, т. е. простые $\mathfrak{p} \in S - S_0$. Выберем $y \in k^*$ так, чтобы $y \equiv x_\mathfrak{p} \pmod{\mathfrak{p}^{\nu_\mathfrak{p}}}$ для всех $\mathfrak{p} \in S - S_0$, где $\mathfrak{p}^{\nu_\mathfrak{p}} \| \mathfrak{m}$ (это возможно в силу «китайской теоремы об остатках»). Определим далее

$$\prod_{\mathfrak{p} \in S - S_0} \psi_\mathfrak{p}(x) = \chi_2^{-1}(y) \tag{4}$$

для тех иделей x, у которых $|x_\mathfrak{p}|_\mathfrak{p} = 1$ при всех $\mathfrak{p} \in S - S_0$. Чтобы завершить определение ψ на этом подмножестве из J, мы должны определить $\psi_\mathfrak{p}(x)$ для $\mathfrak{p} \in S_0$.

Если $\mathfrak{p}$ — вещественное, то пусть χ — характер на k^*, определенный формулой $\chi^{(\mathfrak{p})}(\alpha) = \operatorname{sgn} \alpha_\mathfrak{p}$. Тогда χ_1 будет произведением некоторого числа таких характеров, а именно

$$\chi_1 = \prod_{\mathfrak{p} \in T} \chi^{(\mathfrak{p})} \quad (T \subset S_0), \tag{5}$$

[1]) Запись $\mathfrak{p}^\nu \| x_\mathfrak{p}$ означает, что $x_\mathfrak{p} \in \mathfrak{p}^\nu - \mathfrak{p}^{\nu+1}$.

и мы определим $\psi_\mathfrak{p}(x)$ для $\mathfrak{p} \in S_0$ и $x \in k^*$ так:

$$\psi_\mathfrak{p}(x) = \begin{cases} \chi^{(\mathfrak{p})}(x_\mathfrak{p})^{-1}, & \text{если } \mathfrak{p} \in T, \\ 1, & \text{если } \mathfrak{p} \in S_0 - T, \end{cases} \tag{6}$$

и расширим это определение по непрерывности для всех $x_\mathfrak{p} \in k_\mathfrak{p}^*$.

Осталось определить ψ для таких x, у которых $|x_\mathfrak{p}|_\mathfrak{p} \neq 1$ для некоторого $\mathfrak{p} \in S - S_0$. Мы сделаем это позже.

Из нашей конструкции ясно, что функция ψ мультипликативна. Проверим, что ψ удовлетворяет условиям (i) и (ii) (условие (iii) выполнено по построению). Рассмотрим сначала (i). Тогда

$$\prod_{\mathfrak{p} \in S_0} \psi_\mathfrak{p}(\alpha) = \chi_1^{-1}(\alpha)$$

в силу (5) и (6),

$$\prod_{\mathfrak{p} \in S - S_0} \psi_\mathfrak{p}(\alpha) = \chi_2^{-1}(\alpha)$$

в силу (4) и

$$\prod_{\mathfrak{p} \in S} \psi_\mathfrak{p}(\alpha) = \chi(\alpha) = \chi^*(\alpha)$$

в силу (3). Так как $\chi^* = \chi_1\chi_2$, то $\psi = 1$ на k^*.

Осталось рассмотреть (ii). Но мы знаем, что $\psi(x) = 1$, если

$$|x_\mathfrak{p} - 1|_\mathfrak{p} < 1, \quad \mathfrak{p} \in S_0,$$

$$x_\mathfrak{p} \in 1 + \mathfrak{p}^{\mu_\mathfrak{p}}, \quad \mathfrak{p} \in S - S_0,$$

$$|x_\mathfrak{p}|_\mathfrak{p} = 1, \quad \mathfrak{p} \notin S,$$

а это множество открыто в топологии иделей.

Наконец, мы должны расширить наше определение ψ на такие идели, для которых при некотором $\mathfrak{p} \in S - S_0$ имеет место $|x_\mathfrak{p}|_\mathfrak{p} \neq 1$. Пусть x — такой идель и $\mathfrak{p} \in S - S_0$. Если $\mathfrak{p}^{u_\mathfrak{p}} \| x_\mathfrak{p}$ (где $u_\mathfrak{p}$, разумеется, не обязательно положительное число), то выберем такое $\alpha \in k^*$, что

$$\mathfrak{p}^{-u_\mathfrak{p}} \| \alpha \text{ для всех } \mathfrak{p} \in S - S_0.$$

Определим теперь ψ, положив

$$\psi(x) = \psi(\alpha x)$$

(заметим, что правая часть уже была определена). Проверим, что такое определение $\psi(x)$ однозначно. Действительно, если β — другой элемент из k^*, такой, что $\mathfrak{p}^{-u_\mathfrak{p}} \| \beta$ для каждого $\mathfrak{p} \in S - S_0$, то

$$\psi(\beta x) = \psi(\beta/\alpha)\psi(\alpha x) = \psi(\alpha x),$$

так как $\beta/\alpha \in k^*$, а ψ мультипликативна. Этим завершается построение ψ как характера на группе классов иделей.

Напомним, что I^S — группа всех идеалов поля k, взаимно простых с S, через A^S обозначена подгруппа главных идеалов в I^S, через $B^{(\mathfrak{m})}$ — подгруппа в A^S, состоящая из таких главных идеалов (α), для которых $\alpha \equiv 1 \pmod{\mathfrak{m}}$, и через $H^{(\mathfrak{m})}$ — подгруппа в $B^{(\mathfrak{m})}$, состоящая из таких главных идеалов (α), для которых

$$\alpha \equiv 1 \pmod{\mathfrak{m}} \quad \text{и} \quad \alpha \gg 0.$$

Заметим, что $H^{(\mathfrak{m})}$ является пересечением ядер всевозможных характеров Дирихле по модулю $\mathfrak{m}$, а число $h_\mathfrak{m}$ таких характеров равно индексу $H^{(\mathfrak{m})}$ в I^S.

Индекс A^S в I^S равен так называемому *абсолютному числу классов* h. Индекс $B^{(\mathfrak{m})}$ в $H^{(S)}$ равен числу единиц в кольце вычетов по $\bmod \mathfrak{m}$; обозначим его через $\phi(\mathfrak{m})$. Индекс $H^{(\mathfrak{m})}$ в $B^{(\mathfrak{m})}$ — это число всюду положительных единиц, сравнимых с $1 \pmod{\mathfrak{m}}$; это число равно $H/(h\phi_1(\mathfrak{m}))$, где $\phi_1(\mathfrak{m})$ есть число классов вычетов по $\bmod \mathfrak{m}$, содержащих всюду положительные единицы, а H — число классов идеалов в «узком смысле», т. е. по отношению к подгруппе I^S, состоящей из всюду положительных главных идеалов в k. Тогда число $h_\mathfrak{m}$ различных характеров Дирихле по $\bmod \mathfrak{m}$ задается формулой

$$h_\mathfrak{m} = \frac{H}{\phi_1(\mathfrak{m})}\phi(\mathfrak{m}).$$

§ 2. L-РЯДЫ ДИРИХЛЕ И ТЕОРЕМЫ ПЛОТНОСТИ

В этом параграфе термин «характер» будет всегда означать «характер Дирихле». Пусть χ — характер; определим χ на S равенством $\chi(\mathfrak{p}) = 0$, если $\mathfrak{p} \in S$.

Пусть $\mathfrak{a}$ — некоторый главный целый идеал поля k. Рассмотрим его разложение на простые идеалы

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}, \text{ где } \nu_{\mathfrak{p}} \geqslant 0, \ \nu_{\mathfrak{p}} = 0 \text{ для почти всех } \mathfrak{p}.$$

Через $N(\mathfrak{a})$ обозначим абсолютную норму идеала $\mathfrak{a}$, т. е. $N_{k/\mathbf{Q}}(\mathfrak{a})$.

Определим дзета-функцию Дедекинда $\zeta_k(s)$:

$$\zeta_k(s) = \sum_{\mathfrak{a} \neq 0} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \quad (s = \sigma + it).$$

Кроме того, каждому характеру χ сопоставим L-ряд

$$L(s, \chi) = \sum_{\mathfrak{a} \neq 0} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1}.$$

Каждое рациональное простое число является произведением самое большее $[k : \mathbf{Q}]$ простых идеалов $\mathfrak{p}$, поэтому в обоих случаях сходимость суммы и произведения при $\sigma > 1$ и равенство между ними следует из абсолютной сходимости суммы и произведения при $\sigma > 1$.

Заметим, что $L(s, \chi_0)$ и $\zeta_k(s)$ различаются только в множителях, соответствующих разветвленным простым числам, и что $\zeta_k(s)$ совпадает с L-рядом для примитивного характера, согласованного с χ_0.

Как и в классической теории рациональных чисел, L-функции вводятся для доказательства различных теорем плотности (например, следующей дальше теоремы 2.3). Важнейшее свойство таких функций заключается в том, что их область определения может быть аналитически расширена влево от прямой $\sigma = 1$. Продолжение в полосу $\sigma > 1 - \frac{1}{\nu}$ можно осуществить элементарным способом (используя только преобразование Абеля и то, что $\zeta(s)$ регулярна всюду, кроме точки $s = 1$, где она имеет простой полюс) на основании следующей теоремы.

Теорема 2.1.

$$\sum_{N(\mathfrak{a}) \leqslant x} \chi(\mathfrak{a}) = \begin{cases} O\left(x^{1-\frac{1}{\nu}}\right), & \chi \neq \chi_0, \\ \varkappa x + O\left(x^{1-\frac{1}{\nu}}\right), & \chi = \chi_0, \end{cases}$$

где $\varkappa$ зависит от степени, числа классов, дискриминанта и единиц поля k.

Мы кратко наметим доказательство. Пусть C — класс смежности $H^{(\mathfrak{m})}$ в I^S. Тогда сумма, рассматриваемая в теореме, равна

$$\sum_C \chi(C) \sum_{\substack{N(\mathfrak{a}) \leqslant x \\ \mathfrak{a} \in C}} 1.$$

Вследствие того, что

$$\sum_C \chi(C) = \begin{cases} h_{\mathfrak{m}}, & \chi = \chi_0, \\ 0 \text{ в остальных случаях,} \end{cases}$$

достаточно оценить внутреннюю сумму. Пусть $\mathfrak{b}$ — некоторый идеал в C^{-1}. Тогда $\mathfrak{a}\mathfrak{b} = (a)$, где a — всюду положительный элемент из k, причем такой, что $a \equiv 1 \pmod{\mathfrak{m}}$. При изменении $\mathfrak{a}$ целое число a будет изменяться в идеале $\mathfrak{b}$. Кроме того,

$$|N(a)| = |N((a))| = N(\mathfrak{a})\, N(\mathfrak{b});$$

поэтому внутренняя сумма может быть записана в виде

$$\sum_{\substack{|N(a)| \leqslant xN(\mathfrak{b}) \\ a \in \mathfrak{b}}}^{*} 1,$$

где звездочка означает, что $a \equiv 1 \pmod{\mathfrak{m}}$, $a \gg 0$ и что в каждом множестве ассоциированных целых берется только один элемент. Целые числа a идеала $\mathfrak{b}$ могут быть представлены точками некоторой n-мерной решетки. Наша задача — это по существу классический вопрос об оценке числа этих точек в некотором симплексе (Дедекинд [8], Вебер [5], Гекке [7]). Оценка принимает вид [1])

$$\frac{\varkappa}{h_{\mathfrak{m}}} x + O\left(x^{1-\frac{1}{\nu}}\right).$$

[1]) Лучшую оценку остаточного члена можно получить так же, как в книге Ландау ([10], предложение 210).

Результат такого типа можно получить и для характеров Гекке, но доказательство будет более сложным (Гекке [6]).

Так же как и в классической теории, более глубокие методы связаны с возможностью аналитического продолжения L-функций на всю комплексную плоскость и с функциональным уравнением для этих функций.

Для обычной ζ-функции имеется представление (Титчмарш [13])

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) =$$

$$= \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty (x^{-\frac{1}{2}s-\frac{1}{2}} + x^{\frac{1}{2}s-1})\frac{1}{2}(\theta(x)-1)\,dx = \Phi(s),$$

где

$$\theta(x) = \sum_{m=-\infty}^{\infty} e^{-\pi m^2 x},$$

из которого сразу получается функциональное уравнение

$$\Phi(s) = \Phi(1-s).$$

Гекке [6] принадлежит далеко идущее обобщение этого классического результата для L-рядов с характерами Гекке. Не так давно Тэйт (см. Ленг [11]) обобщил результат Гекке на более широкие пространства. Для характеров Дирихле результат Гекке формулируется ниже (Хассе [14]).

Пусть

$$\Phi(s,\chi) = \prod_{q=1}^{r_1}\Gamma\left(\frac{s+a_q}{2}\right)\cdot\Gamma(s)^{r_2}\left\{\frac{|d|N(\mathfrak{f}_\chi)}{4^{r_2}\pi^{\nu}}\right\}^{s/2} L(s,\chi);$$

тогда функция $\Phi(s,\chi)$ мероморфна и удовлетворяет функциональному уравнению

$$\Phi(s,\chi) = W(\chi)\,\Phi(1-s,\bar{\chi}),$$

где W — константа, по абсолютной величине равная 1,
d — дискриминант;

r_1, r_2 — соответственно число вещественных и комплексных нормирований;

$a_q = 0$ или 1 в зависимости от того, зависят или не зависят значения χ на области всех главных идеалов (α) с $\alpha \equiv 1 \pmod{\mathfrak{f}_\chi}$ от знака q-й вещественной сопряженной числа α.

Явное выражение для W содержится в [14], § 9, теорема 15. Существование этого множителя в функциональном уравнении приводит к интересной информации алгебраического характера, например к обобщению гауссовых сумм ([14], § 9.2 и далее). Из доказательства функционального уравнения следует, что $L(s,\chi)$ является целой функцией всюду, за исключением полюса при $s=1$, если $\chi = \chi_0$.

Мы увидим, что информация о нулях L-функции играет важную роль при исследовании плотности. Распределение нулей в «критической» полосе $0 < \sigma \leqslant 1$ особенно важно в связи с *обобщенной гипотезой Римана* о том, что $L(s,\chi) \neq 0$, если $\sigma > \frac{1}{2}$; однако эта гипотеза еще далека до своего доказательства.

Несмотря на это, важную информацию можно извлечь из несравненно более слабого результата.

Теорема 2.2.

$$L(s,\chi) \neq 0, \qquad \textit{если} \quad \sigma \geqslant 1.$$

Доказательство. Из представления L в виде произведения при $\sigma > 1$ следует, что мы можем ограничиться случаем $\sigma = 1$. Доказательство разбивается на две части, первая из которых принадлежит Адамару, а вторая Ландау. Предположим противное: $1 + it$ является нулем функции $L(s,\chi)$.

1 (Адамар). Пусть $\chi^2 \neq \chi_0$, если $t = 0$. При $\sigma > 1$ из представления в виде произведения следует, что

$$L(s,\chi) = \exp\left\{\sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\frac{1}{m}N(\mathfrak{p})^{-m\sigma}e^{-itm\ln N(\mathfrak{p})}\chi(\mathfrak{p}^m)\right\}.$$

Если $\mathfrak{p}$ взаимно просто с $\mathfrak{f}_\chi$, введем обозначения $\chi(\mathfrak{p}) = e^{i\varphi_\mathfrak{p}}$, $\beta_\mathfrak{p} = t \ln N(\mathfrak{p}) + c_\mathfrak{p}$ и рассмотрим функцию

$$|L^3(\sigma, \chi_0) L^4(\sigma+it, \chi) L(\sigma+2it, \chi^2)| =$$

$$= \exp\left\{ \sum_{\substack{\mathfrak{p} \text{ взаимно} \\ \text{просто} \\ \text{с } \mathfrak{f}_\chi}} \sum_{m=1}^{\infty} \frac{1}{m} N(\mathfrak{p})^{-m\sigma} \times \right.$$

$$\left. \times (3 + 4\cos m\beta_\mathfrak{p} + \cos 2m\beta_\mathfrak{p}) \right\} \geqslant 1.$$

(неравенство следует из того, что $3 + 4\cos\omega + \cos 2\omega \geqslant 0$ при всех вещественных ω). Зафиксируем t и перейдем к пределу при $\sigma \to 1 + 0$.

Рассмотрим сомножители в левой части равенства. Первый из них равен $O((\sigma - 1)^{-3})$, второй $O((\sigma - 1)^4)$, а третий $O(1)$, потому что если $t = 0$, то $\chi^2 \neq \chi_0$. Таким образом, выражение слева стремится к нулю и мы пришли к противоречию.

2 (Ландау). Осталось рассмотреть случай $\chi^2 = \chi_0$ (таким образом, характер χ веществен). Предположим, что $L(1, \chi) = 0$. Рассмотрим произведение

$$\zeta_k(s) L(s, \chi) = \sum_\mathfrak{a} N(\mathfrak{a})^{-s} \lambda(\mathfrak{a}) = \sum_{u=1}^{\infty} a_u u^{-s},$$

где

$$a_u = \sum_{N(\mathfrak{a})=u} \lambda(\mathfrak{a})$$

и

$$\lambda(\mathfrak{a}) = \sum_{\mathfrak{b} \mid \mathfrak{a}} \chi(\mathfrak{b}) = \prod_{\mathfrak{p}^m \| \mathfrak{a}} \{1 + \chi(\mathfrak{p}) + \ldots \chi(\mathfrak{p}^m)\} \geqslant 0,$$

где запись $\mathfrak{p}^m \| \mathfrak{a}$ означает, что $m = m_\mathfrak{p}$ — наибольший показатель степени, при котором $\mathfrak{p}^m$ делит $\mathfrak{a}$. Более того, если $m_\mathfrak{p}$ четны для всех $\mathfrak{p}$, делящих $\mathfrak{a}$, то

$$\lambda(\mathfrak{a}) \geqslant 1.$$

Следовательно, если σ вещественно и оба ряда сходятся, то

$$\sum N(\mathfrak{a})^{-\sigma} \lambda(\mathfrak{a}) \geqslant \sum_\mathfrak{a} N(\mathfrak{a})^{-2\sigma}. \qquad (1)$$

Теперь нам понадобится следующий простой результат из теории рядов Дирихле.

Ряд Дирихле вида

$$f(s) = \sum_{u=1}^{\infty} a_u \cdot u^{-s}, \quad a_u \geqslant 0 \qquad (u = 1, 2, \ldots),$$

имеет своей областью сходимости полуплоскость $\operatorname{Re} > \sigma_0$, *и если* σ_0 *— конечное вещественное число, то функция* $f(s)$ *нерегулярна в точке* $s = \sigma_0$ ([12], теорема из § 9.2).

По предположению $f(s) = \zeta_k(s) L(s, \chi)$ — всюду регулярная функция (так как существующий по предположению нуль функции $L(s, \chi)$ в точке 1 «съедает» полюс функции $\zeta_k(s)$. Следовательно, ряд в левой части равенства (1) сходится при всех вещественных σ. Но ряд в правой части этого равенства есть $\zeta_k(2\sigma)$, а это функция, которая стремится к $+\infty$ при $\sigma \to \frac{1}{2} + 0$. Итак, мы пришли к противоречию.

Доказательство Ландау совершенно неконструктивно, в то время как рассуждения Адамара можно использовать для получения количественных результатов относительно свободных от нулей областей и порядка роста L-функции (см. [18], [9]).

Теперь мы в состоянии доказать следующий результат.

Теорема 2.3 (*теорема о простых идеалах*).

$$\sum_{N(\mathfrak{p}) \leqslant x} \chi(\mathfrak{p}) = \begin{cases} \frac{x}{\ln x}(1 + o(1)), & \chi = \chi_0; \\ o\left(\frac{x}{\ln x}\right), & \chi \neq \chi_0. \end{cases}$$

Доказательство. При $\operatorname{Re} s > 1$ логарифмическая производная функции $L(s, \chi)$ представляется в виде

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_\mathfrak{p} \sum_{m=1}^{\infty} N(\mathfrak{p})^{-ms} \ln N(\mathfrak{p}) \cdot \chi(\mathfrak{p}^m) =$$

$$= \sum_\mathfrak{p} \chi(\mathfrak{p}) \frac{\ln N(\mathfrak{p})}{N(\mathfrak{p})^s} + g(s, \chi),$$

где g — функция, регулярная при $\operatorname{Re} s > \frac{1}{2}$. Нашим первым и самым важным шагом будет оценка суммы коэффициентов

$$\sum_{N(\mathfrak{p}) \leqslant x} \chi(\mathfrak{p}) \ln N(\mathfrak{p}).$$

Один из способов такой оценки состоит в том, чтобы представить сумму в виде интеграла от функции

$$\frac{x^s L'(s, \chi)}{sL(s, \chi)}$$

вдоль контура, состоящего из прямой $(c - i\infty,\ c + i\infty)$ при каком-нибудь $c > 1$, и оценить затем этот интеграл, сдвигая контур к прямой $\operatorname{Re} s = 1$ с вырезом около точки $s = 1$. Как мы знаем теперь, полюс может быть только в одной точке (и он действительно имеется в случае $\chi = \chi_0$, причем вычет тогда и дает нам главный член); подробности, связанные с этим подходом, см. в [10]. Даже из этого наброска видно, что необращение в 0 функции $L(s, \chi)$ на прямой $\operatorname{Re} s = 1$ весьма существенно.

Другой подход основан на тауберовой теореме Винера — Икеара.

Пусть $f(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}$ $(a_m \geqslant 0)$ *и* $g(s) = \sum_{m=1}^{\infty} \frac{b_m}{m^s}$ — *ряды Дирихле, сходящиеся при* $\operatorname{Re} s > 1$, *регулярные на прямой* $\operatorname{Re} s = 1$, *имеющие простые полюсы в точке* $s = 1$ *с вычетом, равным* 1 *в случае функции* f *и равным* η *в случае функции* g, *где* η *может быть равно* 0. *Предположим, что существует такая константа* c, *что* $|b_m| \leqslant c a_m$. *Тогда*

$$\sum_{m \leqslant x} b_m \sim \eta x \text{ при } x \to \infty.$$

Мы применим этот результат к случаю

$$f(s) = -\frac{\zeta'(s)}{\zeta(s)}, \quad g(s) = -\frac{L'(s, \chi)}{L(s, \chi)}, \quad c = [k : \mathbf{Q}].$$

Ясно, что $\eta = 1$, если $\chi = \chi_0$, и $\eta = 0$ в остальных случаях. Легко показать далее (например, посредством частичного суммирования), что

$$\frac{1}{\ln x} \sum_{N(\mathfrak{p}) \leqslant x} \chi(\mathfrak{p}) \ln N(\mathfrak{p}) \sim \sum_{N(\mathfrak{p}) \leqslant x} \chi(\mathfrak{p}),$$

а это и доказывает теорему. Такой подход изложен в книге Ленга [11].

Стоит заметить, что аналитический метод можно применить для получения оценок остаточных членов (Гекке [6]). Оба метода распространяются на характеры Гекке.

В тесной связи со знаменитым доказательством Дирихле бесконечности числа простых чисел в арифметической прогрессии находится утверждение о том, что в каждом классе Дирихле C простых идеалов содержится бесконечное число простых идеалов из k. Действительно, используя теорему о простых идеалах, можно показать, что простые идеалы $\mathfrak{p}$ равномерно распределены по классам, в частности имеет место

Теорема 2.4.

$$\sum_{\substack{N(\mathfrak{p}) \leqslant x \\ \mathfrak{p} \in C}} \sim \frac{1}{h_{\mathfrak{m}}} \frac{x}{\ln x}, \quad x \to \infty.$$

Доказательство. Заметим, что

$$\sum_{\chi} \bar{\chi}(C) \chi(\mathfrak{p}) = \begin{cases} h_{\mathfrak{m}}, & \mathfrak{p} \in C, \\ 0 \text{ в остальных случаях.} \end{cases}$$

Из этой формулы ортогональности следует, что

$$h_{\mathfrak{m}} \sum_{\substack{N(\mathfrak{p}) \leqslant x \\ \mathfrak{p} \in C}} 1 = \sum_{\chi} \bar{\chi}(C) \sum_{N(\mathfrak{p}) \leqslant x} \chi(\mathfrak{p}).$$

С другой стороны, по теореме о простых идеалах правая сумма асимптотически равна $x/\ln x$ при $x \to \infty$.

Пусть B — произвольное множество идеалов в поле k и существует предел

$$l = \lim_{x \to \infty} \frac{\ln x}{x} \operatorname{card} \{\mathfrak{p} \in B \mid N(\mathfrak{p}) \leqslant x\}.$$

В этом случае l называется *плотностью* простых идеалов в B. В частности, плотность всех простых идеалов в k равна 1.

При исследовании плотности простых идеалов в данном множестве достаточно рассматривать лишь простые идеалы $\mathfrak{p}$ абсолютной степени 1, т. е. такие $\mathfrak{p}$, для которых $N_{k/\mathbb{Q}}(\mathfrak{p})$ является рациональным простым числом. Число тех простых идеалов $\mathfrak{p}$, норма которых есть степень простого числа с показателем, большим единицы, и которые удовлетворяют условию $N(\mathfrak{p}) \leqslant x$, имеет порядок $O(x^{1/2})$. По тем же соображениям мы можем не рассматривать конечное число разветвленных простых идеалов поля.

Мы используем это замечание для доказательства следующего результата, известного в классической литературе под названием первого фундаментального неравенства теории полей классов (см. гл. VII, § 9, и гл. XI, п. 1).

Теорема 2.5. *Пусть K — конечное нормальное расширение поля k. Обозначим через n степень $[K : k]$. Пусть S—исключительное множество в k. Поле K определяет в I^S подгруппу H_S конечного индекса h_S, образованную теми элементами из H^m, которые содержат нормы относительно k идеалов из K, взаимно простых с S. Тогда*

$$h_S \leqslant n.$$

Доказательство. Выразим $1/n$ и $1/h_S$ как плотности простых идеалов в двух множествах из k.

Прежде всего, если C — множество всех простых идеалов $\mathfrak{p}$ из k, принадлежащих H_S, то по предыдущей теореме плотность C равна $1/h_S$.

Далее, ввиду нормальности K/k разложение идеала $\mathfrak{p}$ в поле K имеет вид

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

где все $\mathfrak{P}_i$ имеют *одну и ту же* степень f относительно $\mathfrak{p}$, причем

$$efr = n.$$

Так как число разветвленных простых идеалов конечно, мы можем рассматривать только те $\mathfrak{p}$, для которых $e = 1$. Рассмотрим теперь множество B всех тех простых идеалов,

для которых $e = f = 1$, т. е. $r = n$. С одной стороны, по теореме о простых идеалах для поля K (заметим, что все простые идеалы $\mathfrak{P}_i$ имеют абсолютную степень 1) плотность в B равна, очевидно, $1/n$; с другой стороны, если $\mathfrak{p} \in B$ и $\mathfrak{P} \mid \mathfrak{p}$, то $N_{K/k}(\mathfrak{P}) = \mathfrak{p}$, так что $B \subset H_S$; отсюда следует наш результат.

Замечание. Полезно заметить, что теорему 2.5 можно доказать, не используя сравнительно глубоких результатов теорем 2.3 и 2.4 и, в частности, того, что $L(s, \chi) \neq 0$ при $\operatorname{Re} s = 1$. Ниже излагаются более элементарные соображения, использующие лишь теорию функций вещественного переменного.

Пусть s вещественно и больше 1. С помощью теоремы 2.1 и частичного суммирования можно получить, что

$$\lim_{s \to 1} (s-1) L(s, \chi_0) = \varkappa; \qquad \text{(а)}$$

$$\lim_{s \to 1} L(s, \chi) \text{ существует и конечен, если } \chi \neq \chi_0. \qquad \text{(б)}$$

Из представления $L(s, \chi)$ в виде произведения следует, что

$$\ln L(s, \chi) = \sum \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} + g(s, \chi),$$

где $g(s, \chi)$ — ряд Дирихле, абсолютно сходящийся при $\operatorname{Re} s > 1/2$. Из ортогональности характеров χ следует, что

$$\sum_{\mathfrak{p} \in H_S} \frac{1}{H(\mathfrak{p})^s} = \frac{1}{h_s} \ln \frac{1}{s-1} + f(s), \qquad \text{(в)}$$

где

$$h_s f(s) = \sum_{\chi \neq \chi_0} \{\ln L(s, \chi) - g(s, \chi)\} + \ln (s-1) L(s, \chi_0) - g(s, \chi_0).$$

В силу (а) и (б) $\overline{\lim_{s \to 1}} f(s)$ не равен $+\infty$; он конечен, если только $L(s, \chi)$ $(\chi \neq \chi_0)$ не обращается в 0 при $s = 1$.

Пусть теперь K — поле из условия теоремы 2.5. По аналогии с (а) существует конечный предел $\lim_{s \to 1} \zeta_K(s)$ $(s-1)$. Взяв логарифм от представления $\zeta_K(s)$ в виде произведе-

ния, получим

$$\sum_{\mathfrak{p}\in B}\frac{1}{N(\mathfrak{p})^s}=\frac{1}{n}\ln\frac{1}{s-1}+G(s), \qquad (г)$$

где $\lim\limits_{s\to 1}G(s)$ существует и конечен. Вычитая (г) из (в) и учитывая, что $B\subset H_S$, мы убеждаемся, что

$$\left(\frac{1}{h_s}-\frac{1}{n}\right)\ln\frac{1}{s-1}+f(s)-G(s)\geqslant 0$$

для всех $s>1$. Устремив $s\to 1+0$, получим требуемый результат.

Для следующей теоремы нам нужны некоторые сведения из теории полей классов.

Теорема 2.6. *Пусть K — конечное абелево расширение поля k; тогда*

$$\zeta_K(s)=\prod_{\chi}L(s,\chi,k), \qquad (2)$$

где, в обозначениях предыдущей теоремы, произведение справа распространяется на все примитивные характеры, согласованные с характерами группы классов I^S/H_S.

Доказательство. Доказательство проводится в терминах локальных множителей, причем мы рассмотрим по отдельности неразветвленный и разветвленный случаи.

1. Пусть $\mathfrak{p}$ — неразветвленный простой идеал из k, т. е.

$$\mathfrak{p}=\mathfrak{P}_1\mathfrak{P}_2\dots\mathfrak{P}_l,$$

где $\mathfrak{P}_1\mathfrak{P}_2\dots\mathfrak{P}_l$ — различные простые идеалы в K. Согласно теории полей классов,

$$N_{K/\mathbf{Q}}(\mathfrak{P}_i)=N_{k/\mathbf{Q}}(\mathfrak{p})^f, \text{ где } lf=[K:k]=n.$$

Поэтому соответствующий локальный множитель слева равен

$$(1-N(\mathfrak{p})^{-fs})^{-n/f},$$

в то время как соответствующий локальный множитель справа равен

$$\prod_{\chi}(1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}.$$

Ввиду того что f — наименьшее положительное число, такое, что $\chi(\mathfrak{p}^f)=1$ для всех χ, имеет место следующее легко проверяемое тождество (достаточно взять логарифмы от обеих частей и использовать, что $h_S=n$):

$$(1-y)^{f-n/f}=\prod_{\chi}(1-\chi(\mathfrak{p})\cdot y)^{-1};$$

отсюда, если положить $y=N(\mathfrak{p})^{-s}$, следует нужное равенство.

2. Доказательство для разветвленных простых идеалов сложнее и использует функциональные уравнения, которым удовлетворяют различные L-функции. Начнем с равенства

$$\zeta_K(s)=g(s)\prod_{\chi}L(s,\chi,k)$$

и докажем, что функция $g(s)$ тождественно равна единице. Из доказанного раньше следует, что $g(s)$ равна произведению конечного числа выражений вида

$$\frac{\prod\limits_{\chi}\{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}\}}{\prod\limits_{\mathfrak{P}\mid\mathfrak{p}}\{1-N(\mathfrak{P})^{-s}\}},$$

соответствующих разветвленным идеалам $\mathfrak{p}$.

Если это произведение не постоянно, оно имеет полюс или нуль в некоторой чисто мнимой точке it_0, где $t_0\neq 0$. В силу функционального уравнения $g(1-s)/g(s)$ представляет собой отношение гамма-функций и, следовательно, имеет только вещественные нули и полюсы. Поэтому $1-it_0$ также является полюсом или нулем функции g. Мы знаем, однако, что $1-it_0$ не является нулем или полюсом ни для L-рядов, ни для функций $\zeta_K(s)$. Следовательно, g постоянна, а именно равна 1.

Пример 1 [1]). Пусть $k=\mathbf{Q}$, $K=\mathbf{Q}(\omega)$, где ω — первообразный корень из 1 степени m. Тогда

$$\zeta_K(s)=\zeta(s)\prod_{\chi}L(s,\chi),$$

[1]) Так как функции $\zeta_k(s)$ и $L(s,\chi_0,k)=\zeta_K(s)$ имеют простой полюс в точке $s=1$, а остальные функции $L(s,\chi,k)$ из правой части равенства (2) регулярны, то отсюда следует, что эти функции $L(s,\chi,k)$ не обращаются в 0 в точке $s=1$. В частности, в ситуа-

где произведение справа распространяется на все неглавные рациональные характеры по mod m.

Доказательство см. гл. III, § 1.

Пример 2. Пусть $k = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{d})$, где d — дискриминант поля K; тогда

$$\zeta_K(s) = \zeta(s) \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) m^{-s},$$

где $\left(\frac{d}{m}\right)$ обозначает символ Кронекера (Гекке [7], гл. VII).

Отметим еще одно следствие из теоремы 2.6. Вспомним, что функциональное уравнение для L-функции содержит множитель

$$\{|d|N(\mathfrak{f}_\chi)\}^{s/2}.$$

Применив функциональное уравнение к $\zeta_K(s)$ в левой части равенства (2) и ко всем L-рядам справа, мы получаем соотношение

$$\prod_\chi |d|N(\mathfrak{f}_\chi) = |D|,$$

где D — дискриминант поля K (Хассе [14], § 9.3). Если предположить, что $k = \mathbf{Q}$, то получается равенство

$$\prod_\chi \mathfrak{f}_\chi = \mathrm{Disc}(K/k). \tag{3}$$

Эти рассуждения не проходят, если $k \neq \mathbf{Q}$, потому что два разных идеала в k могут иметь равные нормы. Тем не менее можно доказать (Хассе [14], § 9.3, формула (1.2) и замечание 4.4), что равенство (3) справедливо и в общем случае.

§ 3. L-ФУНКЦИИ ДЛЯ НЕАБЕЛЕВЫХ РАСШИРЕНИЙ

Предположим теперь, что K — конечное, нормальное, но не обязательно абелево расширение степени n поля k. Поставим себе задачу распространить на этот случай изложенную выше теорию L-рядов, образованных с помощью характеров абелевых групп.

Пусть, как обычно, G — группа Галуа поля K над полем k. Пусть $\{M(\mu)\}_{\mu\in G}$ — представление группы G матрицами над комплексным полем (эта запись означает, что каждому элементу μ из G сопоставлена матрица $M(\mu)$). Значение характера $\chi(\mu)$ на элементе μ определяется как след матрицы $M(\mu)$. Это значение зависит только от того класса сопряженности $\langle\mu\rangle$, в котором лежит μ.

Два представления $\{M(\mu)\}_{\mu\in G}$ и $\{N(\mu)\}_{\mu\in G}$ [1]) называются *эквивалентными*, если существует такая обратимая матрица P, что

$$PM(\mu)P^{-1} = N(\mu) \text{ для всех } \mu \in G.$$

Представление $\{M(\mu)\}$ называется *приводимым* в том случае, если $\{M(\mu)\}$ эквивалентно представлению $\{N(\mu)\}$, имеющему вид

$$N(\mu) = \begin{pmatrix} N^{(1)}(\mu) & 0 \\ 0 & N^{(2)}(\mu) \end{pmatrix} \text{ для всех } \mu \in G,$$

где $\{N^{(1)}(\mu)\}$, $\{N^{(2)}(\mu)\}$ сами являются представлениями группы G.

Характер *неприводимого* представления называется простым. Из общей теории представлений групп (см. книгу Холла [15]) известно, что число g простых характеров группы G равно числу классов сопряженных элементов в G. Кроме того, известны следующие соотношения ортогональности:

$$\sum_{\mu\in G} \chi(\mu)\bar{\chi}'(\mu) = \begin{cases} n, & \chi = \chi', \\ 0, & \chi \neq \chi'; \end{cases} \tag{1}$$

в частности,

$$\sum_{\mu\in G} \chi(\mu) = \begin{cases} n, & \text{если } \chi \text{ — главный характер,} \\ 0 & \text{в остальных случаях,} \end{cases}$$

где *главный* характер — это характер представления $M(\mu) = I$ (через I обозначена единичная матрица) для

ции примера 1 L-функции, образованные неглавными характерами Дирихле по mod m, не обращаются в 0 в точке $s = 1$. Это обстоятельство лежит в основе одного из подходов к проведению основного шага в доказательстве теоремы Дирихле о бесконечности числа простых чисел в арифметических прогрессиях.

[1]) Из контекста должно быть ясно, что N здесь используется не для обозначения нормы!

всех $\mu \in G$. В дальнейшем главный характер будет обозначаться через χ_0. Кроме того, если $\psi_1, \ldots, \psi_g$ — простые характеры группы G, то

$$\sum_{i=1}^{q} \psi_i(\mu)\,\bar{\psi}(\mu') = \begin{cases} n/l_\mu, & \mu' \in \langle\mu\rangle, \\ 0, & \mu' \notin \langle\mu\rangle, \end{cases} \tag{2}$$

где l_μ — число элементов в классе сопряженности $\langle\mu\rangle$ элемента μ. В частности, взяв $\mu' = \mu = 1$, мы получаем

$$\sum n_i^2 = n, \tag{3}$$

где n_i — размерность характера ψ_i (это означает, что ψ_i — характер представления группы матрицами порядка $(n_i \times n_i)$).

Если группа G абелева, то каждое $l_\mu = 1$, т. е. $g = n$ и все $n_i = 1$. Следовательно, каждый характер χ представляет собой гомоморфизм группы G в единичную окружность и, таким образом, является обычным коммутативным характером.

Пусть $\mathfrak{P}$ — неразветвленный простой идеал поля K, а $\mathfrak{p}$ — простой идеал из k, лежащий под $\mathfrak{P}$. Мы будем обозначать автоморфизм Фробениуса расширения K/k, относящийся к $\mathfrak{P}$ (определение см. в гл. VII, § 2) через $\left[\frac{K/k}{\mathfrak{P}}\right]$. Если

$$|I - M(\mu)\,x|$$

— характеристический многочлен матрицы $M(\mu)$, рассмотрим в качестве локального множителя для нашей L-функции выражение

$$\left|I - M\left(\left[\frac{K/k}{\mathfrak{P}}\right]\right) N_{K/\mathbb{Q}}(\mathfrak{P})^{-s}\right|^{-1}.$$

Заметим, что это определение не может быть распространено на случай разветвленного $\mathfrak{P}$, поскольку в этом случае не существует соответствующего автоморфизма Фробениуса.

Важно отметить, что этот локальный множитель зависит только от характера χ представления и не зависит от явного вида матрицы. Действительно, каждое подобное преобразование матрицы $M(\mu)$ не меняет ее характеристического многочлена. Группа G конечная, поэтому нормальная жорданова форма матрицы $M(\mu)$ является диагональной матрицей, причем диагональные элементы являются корнями из единицы. Поэтому, не нарушая общности, мы можем в качестве матрицы

$$M\left(\left[\frac{K/k}{\mathfrak{P}}\right]\right)$$

рассмотреть матрицу

$$M\left(\left[\frac{K/k}{\mathfrak{P}}\right]\right) = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_b \end{pmatrix}.$$

Тогда локальный множитель равен

$$\prod_{i=1}^{b} (1 - \varepsilon_i N(\mathfrak{P})^{-s})^{-1} = \exp\left\{\sum_{i=1}^{b}\sum_{m=1}^{\infty} \frac{1}{m}\varepsilon_i^m N(\mathfrak{P})^{-ms}\right\} =$$

$$= \exp\left\{\sum_{m=1}^{\infty} \frac{1}{m}\chi\left(\left[\frac{K/k}{\mathfrak{P}}\right]^m\right) N(\mathfrak{P})^{-ms}\right\}, \tag{4}$$

так как $\sum_{i=1}^{l} \varepsilon_i^m$ равна следу матрицы $\left\{M\left[\frac{K/k}{\mathfrak{P}}\right]^m\right\}$, который по определению есть $\chi\left(\left[\frac{K/k}{\mathfrak{P}}\right]\right)$.

Соберем локальные множители, соответствующие неразветвленным $\mathfrak{P}$, и определим так называемую L-функцию Артина (см. [2])

$$L(s, \chi) = L(s, \chi, K/k) = \prod_{\substack{\text{неразв.} \\ \mathfrak{P}}} \left|I - M\left(\left[\frac{K/k}{\mathfrak{P}}\right]\right) N(\mathfrak{p})^{-s}\right|^{-1};$$

позже мы введем множитель, соответствующий разветвленным простым идеалам.

Сделаем теперь несколько замечаний о функции $L(s, \chi)$.

(I) $L(s, \chi)$ регулярна при $\sigma > 1$, так как произведение абсолютно и равномерно сходится в каждом замкнутом подмножестве полуплоскости $\operatorname{Re} s > 1$.

(II) Если расширение K/k абелево, а χ — простой характер, то определение функции $L(s, \chi)$ за вычетом множителей, относящихся к разветвленным простым идеалам, совпадает с данным в § 2.

(III) Пусть Ω — промежуточное поле между K и k, являющееся нормальным над k. Пусть $H = \operatorname{Gal}(K/\Omega)$, так что H — нормальный делитель в G и

$$G/H = \operatorname{Gal}(\Omega/k).$$

Тогда каждый характер χ группы G/H можно очевидным образом рассматривать как характер группы G, причем

$$L(s, \chi, K/k) = L(s, \chi, \Omega/k).$$

Доказательство. Рассмотрим характер группы G, определенный с помощью представления

$$M'(\mu) = M(\mu H).$$

Тогда

$$X^{\left[\frac{K/k}{\mathfrak{P}}\right]} \equiv X^{N(\mathfrak{P})} \pmod{\mathfrak{P}} \tag{5}$$

для всех целых $X \in K$, в частности для всех целых $X \in \Omega$. Так как Ω является нормальным расширением поля k, то имеет место импликация

$$X \in \Omega \Rightarrow X^{\mu} \in \Omega \text{ для всех } \mu \in G.$$

Таким образом, (5) можно рассматривать как сравнение в Ω, а так как идеал $\mathfrak{P}$ не разветвлен, то, если $\mathfrak{P}$ лежит над $\mathfrak{q}$ в Ω, мы имеем

$$X^{\left[\frac{K/k}{\mathfrak{P}}\right]} \equiv X^{N(\mathfrak{p})} \pmod{\mathfrak{q}}.$$

Следовательно, также

$$X^{\left[\frac{K/k}{\mathfrak{P}}\right]H} \equiv X^{N(\mathfrak{p})} \pmod{\mathfrak{q}},$$

т. е. $\left[\frac{K/k}{\mathfrak{P}}\right] H$ является автоморфизмом Фробениуса в Ω. Таким образом,

$$\left| I - M'\left(\left[\frac{K/k}{\mathfrak{P}}\right]\right) N(\mathfrak{p})^{-s} \right| = \left| I - M\left(\left[\frac{K/k}{\mathfrak{P}}\right] H\right) N(\mathfrak{p})^{-s} \right| = \left| I - M\left(\left[\frac{\Omega/k}{\mathfrak{P}}\right]\right) N(\mathfrak{p})^{-s} \right|.$$

(IV). Предположим, что χ непростой характер в G, а именно $\chi = \chi_1 + \chi_2$. Тогда

$$L(s, \chi) = L(s, \chi_1)\, L(s, \chi_2),$$

так как ввиду равенства (4) $\ln L$ линеен по χ.

(V). Предположим снова, что Ω — поле между K и k, но уже не обязательно нормальное над k. Пусть $H = \operatorname{Gal}(K/\Omega)$, и пусть

$$G = \sum_i H\alpha_i$$

есть разложение группы G на правые классы смежности. Каждому характеру χ группы H соответствует *индуцированный* характер χ^* группы G:

$$\chi^*(\mu) = \sum_{\alpha_i \mu \alpha_i^{-1} \in H} \chi(\alpha_i \mu \alpha_i^{-1}), \quad \mu \in G; \tag{6}$$

при этом

$$L(s, \chi^*, K/k) = L(s, \chi, K/\Omega).$$

Доказательство[1]. Пусть $\mathfrak{P}$ — неразветвленный простой идеал в K, а $\mathfrak{p}$ — простой идеал в k, лежащий под $\mathfrak{P}$. Предположим, что $\mathfrak{p}$ имеет в Ω следующее разложение на простые идеалы:

$$\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{q}_i, \quad N_{\Omega/\mathbf{Q}}(\mathfrak{q}_i) = (N_{k/\mathbf{Q}}\mathfrak{p})^{f_i}. \tag{7}$$

Пусть τ_i — такой элемент из группы G, что $\mathfrak{q}_i$ лежит под $\tau_i\mathfrak{P}$. Тогда (см. [14], § 23, I) группа G может быть представлена в виде

$$G = \sum_{i=1}^{r} \sum_{x_i=0}^{f_i-1} H\tau_i\mu_0^{x_i},$$

[1]) Другое доказательство см. в [14], § 27, VII.

где

$$\mu_0 = \left[\frac{K/k}{\mathfrak{P}}\right].$$

Из определения индуцированного характера, данного выше, имеем

$$\chi^*(\mu^m) = \sum_{i=1}^{r} \sum_{\substack{x_i=0 \\ \tau_i \mu_0^{x_i} (\mu_0^m) \mu_0^{-x_i} \tau_i^{-1} \in H}}^{f_i - 1} \chi(\tau_i \mu_0^{x_i} \mu_0^m \mu_0^{-x_i} \tau_i^{-1}) =$$

$$= \sum_{\substack{i=1 \\ \tau_i \mu_0^m \tau_i^{-1} \in H}}^{r} f_i \chi(\tau_i \mu_0^m \tau_i^{-1}) =$$

$$= \sum_{\substack{i=1 \\ f_i \mid m}}^{r} f_i \chi(\tau_i \mu_0^m \tau_i^{-1}),$$

так как $(\tau_i \mu_0 \tau_i^{-1})^m \in H$ тогда и только тогда, когда $f_i \mid m$.

Логарифм $\mathfrak{p}$-компоненты ($\mathfrak{p}$ не разветвлено) функции $L(s, \chi^*, K/k)$ в силу соотношения (7) равен

$$\sum_{m=1}^{\infty} \frac{1}{m} \chi^*(\mu_0^m) N(\mathfrak{p})^{-ms} = \sum_{m=1}^{\infty} \frac{1}{m} N(\mathfrak{p})^{-ms} \sum_{\substack{i=1 \\ f_i \mid m}}^{r} f_i \chi(\tau_i \mu_0^m \tau_i^{-1}) =$$

$$= \sum_{i=1}^{r} \sum_{\substack{m=1 \\ f_i \mid m}}^{\infty} \frac{f_i}{m} \chi(\tau_i \mu_0^m \tau_i^{-1}) N(\mathfrak{p})^{-ms} =$$

$$= \sum_{i=1}^{r} \sum_{t=1}^{\infty} t^{-1} \{\chi(\tau_i \mu_0^{f_i} \tau^{-1})\}^t N(\mathfrak{q}_i)^{-ts},$$

причем во внутренней сумме мы положили $m = f_i t$. Теперь выражение равно сумме логарифмов тех q-компонент, которые по равенству (7) соответствуют идеалу $\mathfrak{p}$.

Рассмотрим теперь утверждение (V) в некоторых специальных случаях.

(V, i) $\Omega = K$. Тогда $H = \mathrm{Gal}(K/\Omega) = \{1\}$, и мы имеем только один характер, а именно главный характер χ_0.

В этом случае $L(s, \chi_0, K/\Omega)$ редуцируется к функции $\zeta_K(s)$. Согласно равенству (6), соответствующий индуцированный характер χ_0^* группы G задается формулой

$$\chi_0^*(\mu) = \begin{cases} n, & \text{если } \mu \text{ — единичный элемент,} \\ 0 & \text{в остальных случаях.} \end{cases} \tag{8}$$

Пусть $\psi_1, \psi_2, \ldots, \psi_g$ — все простые характеры группы G. В силу равенства (2), полагая $\mu' = 1$, мы получим $l_1 = 1$ и на основании (8)

$$\sum_{i=1}^{g} \psi_i(\mu) \psi_i(1) = \chi_0^*(\mu). \tag{9}$$

Заметим, что $\psi_i(1)$ должно быть, конечно, положительным числом. Из утверждения (IV) тогда сразу следует, что

$$\zeta_K(s) = \prod_{i=1}^{g} L(s, \psi_i, K/k)^{\psi_i(1)}. \tag{10}$$

(V, ii) $\Omega = k$. Согласно п. (III) (полагая $\Omega = k$ и потому $G = H$), мы получаем

$$L(s, \chi_0, K/k) = L(s, \chi_0, k/k) = \zeta_k(s).$$

Сейчас мы выведем из предыдущих теорем замечательное следствие, заключающееся в том, что общая L-функция Артина $L(s, \chi, K/k)$ может быть выражена как произведение рациональных степеней абелевых L-функций $L(s, \psi, K/\Omega)$, где Ω — различные поля, промежуточные между K и k и такие, что расширение K/Ω абелево.

Используя те же обозначения, что и в (V, i), запишем каждый характер χ группы G в виде

$$\chi = \sum_{i=1}^{g} r_i \psi_i, \tag{11}$$

где r_i — неотрицательные целые рациональные числа. Отсюда и из п. (IV) сразу следует, что для доказательства предложения достаточно рассматривать только *простые* L-функции Артина

$$L(S, \psi_i, K/k).$$

Пусть H — некоторая подгруппа группы G, и пусть ξ_i пробегает простые характеры группы G. Каждый характер ξ_i индуцирует характер ξ_j группы G, определяемый формулой

$$\xi_j^*(\mu) = \sum_i r_{ji}\psi_i(\mu) \text{ для всех } \mu \in G. \tag{12}$$

Ограничение ψ_i на H само является характером группы H и, следовательно, имеет разложения типа (11) по характерам ξ_j. Более того, согласно теории индуцированных характеров, это представление принимает вид

$$\psi_i(\tau) = \sum_j r_{ji}\xi_j(\tau) \text{ для всех } \tau \in H, \tag{13}$$

где коэффициенты r_{ji} *те же*, что и в равенстве (12).

Пусть теперь H — *циклическая* подгруппа группы G. Обозначим через Ω подполе поля K, состоящее из элементов, инвариантных относительно H; тогда K/Ω является абелевым расширением, и, следовательно, согласно п. (V),

$$L(s, \xi_j^*, K/k) = L(s, \xi_j, K/\Omega).$$

Здесь правая часть является абелевой L-функцией. Для того чтобы доказать наше утверждение, теперь достаточно выразить каждый характер ψ_i в виде линейной комбинации индуцированных характеров типа ξ_j^*.

Каждый элемент γ из G порождает циклическую подгруппу H_γ группы G. Обозначим простые характеры H_γ через $\xi_{\gamma;\,j}$. Тогда в силу (12) мы будем иметь

$$\xi_{\gamma;\,j}^*(\mu) = \sum_{i=1}^{g} r_{\gamma;\,ji}\psi_i(\mu) \text{ для всех } \mu \in G. \tag{14}$$

Система уравнений (14) описывается матрицей, в которой каждая фиксированная пара (γ, j) определяет строку, а каждое i — столбец. Мы докажем, что ранг этой матрицы равен g.

Предположим, что ранг этой матрицы меньше g. Тогда ее столбцы линейно зависимы, т. е. существуют такие числа $c_1, c_2, \ldots, c_g$, не все равные нулю, что

$$\sum_{i=1}^{g} c_i r_{\gamma;\,ji} = 0 \text{ для всех } \gamma \in G \text{ и всех } j.$$

Из (13) следует тогда, что

$$\sum_i c_i\psi_i(\tau) = \sum_i c_i \sum_j r_{\gamma;\,ji}\xi_{\gamma;\,j} = 0 \text{ для всех } \tau \in H_\gamma.$$

В частности, полагая $\tau = \gamma$, мы получим равенство

$$\sum_i c_i\psi_i(\gamma) = 0 \text{ для всех } \gamma \in G, \tag{15}$$

что противоречит линейной независимости простых характеров $\psi_1, \ldots, \psi_g$. Другой способ прийти к противоречию состоит в следующем. Умножим равенство (15) на $\overline{\psi}_k(\gamma)$ и просуммируем по всем элементам γ группы G. Из соотношений (1) тогда следует, что

$$nc_k = 0 \qquad (k = 1, 2, \ldots, g), \tag{16}$$

т. е. $c_1 = c_2 = \ldots = c_9 = 0$.

Таким образом, система уравнений (14) может быть разрешена относительно ψ_i; пусть

$$\psi_i = \sum_{\gamma \in G} \sum_j u_{\gamma;\,ij}\xi_{\gamma;\,i}^*,$$

где $u_{\gamma;\,ji} \in \mathbf{Q}$.

Рассуждения, с помощью которых были выведены равенства (16), могут быть проведены по модулю любого простого числа p, не делящего n; отсюда следует, что знаменатели коэффициентов $u_{\gamma;\,ji}$ состоят из простых сомножителей числа n.

Таким образом, мы доказали следующую теорему.

Теорема 3.1. *Для любого характера χ группы G L-функция Артина $L(s, \chi, K/k)$ может быть представлена в виде*

$$L(s, \chi, K/k) = \prod_l \prod_j L(s, \xi_{lj}, K/\Omega_l)^{n_{lj}},$$

где каждое расширение K/Ω_l имеет циклическую группу Галуа; через ξ_{lj} обозначены характеры (абелевых) групп $\mathrm{Gal}(K/\Omega_l)$ и через n_{lj} — рациональные числа, знаменатели которых состоят из простых сомножителей числа n.

Брауэр [3] доказал, что в качестве показателей n_{lj} могут быть взяты целые числа; отсюда, в частности, следует, что L-функции Артина мероморфны. Более того, если

характер χ неглавный, то характеры ξ также можно выбрать неглавными. Отсюда вытекает, что L-функция Артина, образованная неглавным характером, является регулярной и не обращается в нуль при $\sigma \geqslant 1$.

С другой стороны, если $\chi = \chi_0$ является главным характером, функция $L(s, \chi_0, K/k)$ имеет простой полюс в точке $s = 1$. Артин предположил, что, за исключением этого простого полюса при $\chi = \chi_0$, все функции $L(s, \chi, K/k)$ являются целыми.

Из справедливости этой гипотезы следовало бы, что отношение $\zeta_K(s)/\zeta_k(s)$ является целой функцией, когда $k \subset K$. Если расширение K/k нормально, это действительно так в силу (10), (V, ii) и основной теоремы Брауэра о групповых характерах (см. [11]).

Гипотеза Артина доказана для случаев, когда группа G является группой одного из следующих типов: $G = S_3$ или, более общо, G есть группа, порядок которой свободен от квадратов; G — любая группа, порядок которой есть степень простого числа; G — любая группа, коммутатор которой абелев (Шпейзер [17]); $G = S_4$ (Артин [1]). Истинность гипотезы не установлена даже в случае $G = A_5$.

Из теоремы 3.1 следует, что каждая L-функция Артина удовлетворяет некоторому функциональному уравнению. Это следует из того, что каждый сомножитель в правой части удовлетворяет своему собственному функциональному уравнению. Это уравнение имеет вид

$$\Phi(s, \chi) = W(\chi)\,\Phi(1 - s, \overline{\chi}),$$

где W — константа, по модулю равная 1, и

$$\Phi(s, \chi) = A(\chi)^s\,\Gamma\left(\frac{s}{2}\right)^{a(\chi)}\Gamma\left(\frac{s+1}{2}\right)^{b(\chi)} L(s, \chi),$$

где a и b — рациональные числа и A — положительная константа.

Напомним, что предшествующие рассуждения проводились для L-функций, в разложении которых не рассматривались члены, соответствующие разветвленным простым идеалам. Добавим теперь к правой части равенства (17) локальные множители, соответствующие разветвленным простым идеалам для абелевых L-рядов (см. начало § 2), и рассмотрим новое произведение как определение функции L. Тогда написанное выше функциональное уравнение автоматически будет удовлетворяться определенными таким образом L-функциями.

Недостатком теории L-функций Артина является невозможность нелокального подхода (в абелевом случае такой подход осуществляется с помощью определения L-функций рядами). С этим недостатком L-функций и связана трудность их продолжения на комплексную плоскость.

Пример. Случай $G = S_3$.

Элементы группы S_3 распадаются на три класса сопряженности:

C_1: (1); C_2: (1, 2, 3), (3, 2, 1); C_3: (1, 2), (2, 3), (3, 1).

Таким образом, имеются три простых характера. Пусть ψ_1 — главный характер, а ψ_2 — другой характер, определенный множеством C_2. Оба они одномерны, следовательно, согласно (3), ψ_3 — двумерный характер. Поэтому в силу (2) с $\mu' = 1$ мы имеем

$$\psi_1(\mu) + \psi_2(\mu) + 2\psi_3(\mu) = \begin{cases} 6, & \mu = 1, \\ 0 \text{ в остальных случаях.} \end{cases}$$

Отсюда видно, что таблица значений характеров группы устроена следующим образом:

	ψ_1	ψ_2	ψ_3
C_1	1	1	2
C_2	1	1	−1
C_3	1	−1	0.

Используя определение (6), мы можем вычислить характеры χ^*, индуцированные характерами χ на следующих циклических подгруппах группы S_3:

(i) $H = A_3$:

	χ_1^*	χ_2^*	χ_3^*
C_1	2	2	2
C_2	2	−1	−1
C_3	0	0	0

(ii) $H=\{1, (1, 2)\}$:

	χ_4^*	χ_5^*
C_1	3	3
C_2	0	0
C_3	1	-1

(iii) $H=\{1\}$:

	χ_6^*
C_1	6
C_2	0
C_3	0

Из этих таблиц видно, что

$$\chi_1^*=\psi_1+\psi_2,\quad \chi_2^*=\chi_3^*=\psi_3,$$
$$\chi_4^*=\psi_1+\psi_3,\quad \chi_5=\psi_2+\psi_3,\quad \chi_6^*=\psi_1+\psi_2+2\psi_3.$$

Группа S_3 является группой Галуа некоторого неабелева нормального расширения K поля k степени 6. Пусть Ω_1, Ω_2 — промежуточные расширения, неподвижные относительно действия подгрупп A_3 и $\{(1), (1, 2)\}$ соответственно. Тогда Ω_1 — квадратичное расширение поля k, а Ω_2 — кубическое расширение этого поля; K является абелевым расширением каждого из этих двух полей. Ввиду абелевости расширения Ω_1/k на основании (V, ii) и (IV) мы получаем, что

$$\zeta_K(s)=L(s, \chi_0, K/K)=L(s, \psi_1+\psi_2+2\psi_3, K/k)=L_{\psi_1}L_{\psi_2}L_{\psi_3}^2;$$
$$\zeta_{\Omega_1}(s)=L(s, \chi_0, K/\Omega_1)=L(s, \psi_1+\psi_2, K/k)=L_{\psi_1}L_{\psi_2};$$
$$\zeta_{\Omega_2}(s)=L(s, \chi_0; K/\Omega_2)=L(s, \psi_1+\psi_3, K/k)=L_{\psi_1}L_{\psi_3};$$
$$\zeta_k(s)=L(s, \chi_0, K/k)=L_{\psi_1}.$$

Заметим теперь, что в силу (III)

$$L_{\psi_2}=L(s, \psi_2, K/k)=L(s, \chi_5, \Omega_1/k)$$

и в силу (V)

$$L_{\psi_3}=L(s, \psi_3, K/k)=L(s, \chi_2, K/\Omega_1).$$

Следовательно, L_{ψ_2} и L_{ψ_3} являются целыми функциями.

Попутно мы получили доказательство гипотезы Артина для случая $\mathrm{Gal}\,(K/k)=S_3$.

Мы закончим это обозрение неабелева случая формулировкой *теоремы плотности Чеботарева*.

Пусть K/k — нормальное расширение и $G=\mathrm{Gal}\,(K/k)$. Пусть, далее, C — некоторый класс сопряженных элементов в G. Тогда класс неразветвленных простых идеалов $\mathfrak{p}$, обладающих тем свойством, что $\left[\frac{K/k}{\mathfrak{P}}\right]\in C$ для некоторого простого $\mathfrak{P}$, лежащего над $\mathfrak{p}$ [1]), имеет плотность, равную

$$\frac{\mathrm{Gard}\,C}{\mathrm{Gard}\,G}.$$

Посредством рассуждений, подобных проводившимся выше (см. § 2), этот результат можно получить исходя из отсутствия нулей у L-функции Артина на прямой $\mathrm{Re}\,s=1$.

Пример. В качестве иллюстрации этой теоремы рассмотрим случай кубического расширения K_3/k, не являющегося нормальным. Неразветвленный простой идеал может разлагаться на множители в K_3 следующими способами:

1. $\mathfrak{p}=\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$;
2. $\mathfrak{p}=\mathfrak{P}_1\mathfrak{P}_2$, где $\deg \mathfrak{P}_1/\mathfrak{p}=1$, $\deg \mathfrak{P}_2/\mathfrak{p}=2$;
3. $\mathfrak{p}=\mathfrak{P}$.

Мы определим плотность простых идеалов, принадлежащих к каждой из этих категорий.

Пусть K_6 обозначает минимальное расширение поля K_3, являющееся нормальным расширением поля k. Рассмотрим разложение $\mathfrak{p}$ в K_6, принимая во внимание, что все сомножители имеют одинаковую степень. В случае 1 идеал $\mathfrak{p}$ разлагается либо в произведение шести сомножителей степени 1, либо идеалы $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3$ остаются простыми в K_6 и каждый имеет там степень 2. Последняя возможность исключается, потому что K_3/k не является нормальным расширением.

(Предположим, что каждый идеал $\mathfrak{P}_i$ остается простым в K_6 и, следовательно, имеет там степень 2. Пусть

$$\sigma_i=\left[\frac{K/k}{\mathfrak{P}_i}\right].$$

[1]) Действительно, C состоит из автоморфизмов Фробениуса, соответствующих таким $\mathfrak{P}_i$, лежащим над $\mathfrak{p}$.

Каждое σ_i имеет порядок 2 и, следовательно, является 2-циклом (заметим, что $\mathrm{Gal}\,(K_6/k) = S_3$). Ввиду того что σ_i порождают класс сопряженных элементов, они являются разными транспозициями.

K_3 — это множество элементов из K_6, инвариантное относительно некоторого 2-цикла, например σ_1; поэтому

$$\sigma_1(\mathfrak{P}_i \cap K_3) = \mathfrak{P}_i \cap K_3.$$

Ввиду того что существует три различных простых идеала в K_3, каждый из которых имеет единственное расширение до K_6 (при котором он остается простым), имеет место

$$\sigma_1 \mathfrak{P}_i = \mathfrak{P}_i \qquad (i = 1, 2, 3).$$

Пусть K_3' и K_3'' — поля, инвариантные относительно σ_2 и σ_3. Тогда аналогичные соображения покажут (так как поля K_3' и K_3'' сопряжены полю K_3), что

$$\sigma_j \mathfrak{P}_i = \mathfrak{P}_i \qquad (i, j = 1, 2, 3).$$

Транспозиции порождают всю группу S, поэтому

$$S_3 \mathfrak{P}_i = \mathfrak{P}_i.$$

Таким образом, не существует автоморфизма τ, такого, что

$$\tau \mathfrak{P}_1 = \mathfrak{P}_2,$$

а это невозможно.)

В случае 2 разложение для $\mathfrak{p}$ в поле K_6 должно иметь вид $\mathfrak{p} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{P}_1$, причем каждый сомножитель имеет степень 2 и $\mathfrak{q}_1\mathfrak{q}_2 = \mathfrak{P}$. В случае 3 идеал $\mathfrak{p}$ или остается простым, или разлагается в произведение двух простых идеалов степени 3.

Если бы выполнялось первое, то $\left[\frac{K_6/k}{\mathfrak{p}}\right]$ порождал бы всю группу S_3, что невозможно; поэтому остается второе разложение. 38

Примем теперь во внимание, что порядок автоморфизма $\left[\frac{K_6/k}{\mathfrak{q}}\right]$ равен степени идеала $\mathfrak{q}$ (гл. VII, § 2). Отсюда следует, что для каждого $\mathfrak{q}$ из K_6, лежащего над $\mathfrak{p}$, автоморфизм $\left[\frac{K_6/k}{\mathfrak{q}}\right]$ является j-циклом в случае j ($j = 1, 2, 3$). Значит, по теореме Чеботарева искомые плотности для каждого из случаев 1, 2, 3 соответственно равны $\frac{1}{6}$, $\frac{1}{2}$ и $\frac{1}{3}$.

Следующий результат является прямым следствием теоремы Куммера (см. гл. III, добавление, или Вайс [4], 4.9, в частности 4.9.2).

Пусть $f \in k[x]$ неприводим и θ — нуль многочлена f. Пусть, далее, $\mathfrak{p}$ — простой идеал поля k. Тогда почти все $\mathfrak{p}$ разлагаются в $k[\theta]$ точно так же, как $f(x)$ разлагается над полем вычетов поля k по модулю $\mathfrak{p}$.

Пусть теперь $n(\mathfrak{p}, f)$ обозначает число решений сравнения

$$f(x) \equiv 0 \pmod{\mathfrak{p}};$$

тогда $n(\mathfrak{p}, f)$ можно рассматривать для почти всех $\mathfrak{p}$ как число простых сомножителей идеала $\mathfrak{p}$ в $k(\theta)$, имеющих степень 1 относительно k. Применяя теорему о простых идеалах (теорема 2.3) к простым идеалам из $k(\theta)$, мы приходим к следующему результату.

Теорема 3.2. *В обозначениях, введенных выше,*

$$\sum_{N(\mathfrak{p}) \leqslant x} n(\mathfrak{p}, f) \sim \frac{x}{\ln x} \quad \textit{при } x \to \infty.$$

Следствие 1. *Если f — произведение l различных неприводимых сомножителей, то*

$$\sum_{N(\mathfrak{p}) \leqslant x} n(\mathfrak{p}, f) \sim l \frac{x}{\ln x} \quad \textit{при } x \to \infty.$$

Следствие 2. *Если f полностью разлагается по* mod $\mathfrak{p}$ *для почти всех $\mathfrak{p}$, то f полностью разлагается в $k[x]$.*

Доказательство. Пусть n' — степень многочлена f; тогда $n(\mathfrak{p}, f) = n'$ для почти всех $\mathfrak{p}$. Следовательно, $l = n'$ по теореме о простых идеалах для поля k.

На первый взгляд кажется правдоподобным, что многочлен, имеющий по крайней мере один линейный сомножитель по mod $\mathfrak{p}$ для почти всех $\mathfrak{p}$, имеет хотя бы один линейный сомножитель в $k[x]$. Тем не менее следующие контрпримеры показывают, что это не всегда верно.

1. $f(x) = (x^2 - a)(x^2 - b)(x^2 - c)$,

где abc — полный квадрат в $\mathbf{Z}$, в то время как ни a, ни b, ни c таковыми не являются.

Действительно, если a и b — квадратичные невычеты, то c — квадратичный вычет, и по mod $\mathfrak{p}$ выделяются два

линейных сомножителя.

$$2.\ f(x) = (x^2 + 3)(x^3 + 2).$$

Если $\mathfrak{p} \equiv 1 \pmod 3$, то $x^2 + 3$ разлагается по mod $\mathfrak{p}$, а если $\mathfrak{p} \equiv 2 \pmod 3$, то $x^3 + 2$ разлагается по mod $\mathfrak{p}$. Следующее утверждение, однако, все же имеет место.

Теорема 3.3. *Если f — многочлен над k, не являющийся линейным, который имеет по крайней мере один линейный сомножитель по* mod $\mathfrak{p}$ *для почти всех* $\mathfrak{p}$, *то f приводим в $k[x]$.*

Доказательство. Предположим, что f неприводим. Тогда из теоремы 3.2 и теоремы о простых идеалах (теорема 2.3) для поля k следует, что

$$\sum_{N(\mathfrak{p}) \leqslant x} (n(\mathfrak{p}, f) - 1) = o\left(\frac{x}{\ln x}\right).$$

Поэтому, так как $n(\mathfrak{p}, f) \geqslant 1$, то $n(\mathfrak{p}, f) = 1$ для почти всех $\mathfrak{p}$.

Пусть K — поле, получающееся из k присоединением корней многочлена f, и $\mathfrak{q}$ — простой идеал в k, полностью разлагающийся в k. Тогда $\mathfrak{q}$ полностью разлагается в $k(\theta)$ и $n(\mathfrak{q}, f)$ равно степени f для почти всех $\mathfrak{q}$. По теореме о простых идеалах эти идеалы $\mathfrak{q}$ имеют положительную плотность, следовательно, многочлен f линеен.

ЛИТЕРАТУРА

Артин (Artin E.)
[1] Über eine neue Art von L-Reihen, *Abh. Math. Semin. Univ. Hamburg*, **3** (1923), 89—108 (Collected Papers, Addison-Wesley, 1965, 105—124).
[2] Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren, *Abh. math. Semin. Univ. Hamburg*, **8** (1930), 292—306 (Collected Papers, Addison-Wesley, 1965, 165—179).

Брауэр (Brauer R.)
[3] On Artin's L-series with general group characters, *Ann. Math.*, **48** (1947), 502—514.

Вайс (Weiss E.)
[4] Algebraic number theory, McGraw-Hill, New York, 1963.

Вебер (Weber H.)
[5] Über einen in der Zahletheorie angewandten Satz der Integralrechnung, *Göttingen Nachrichten*, (1896), 275—281.

Гекке (Hecke E.)
[6] Eine neue Art von Zeta funktionen und ihre Beziehungen zur Verteilung der Primzahlen (Zweite Mitteilung), *Math. Z.*, **6** (1920), 11—51 (Mathematische Werke, Vandenholck und Ruprecht, 1959, 249—289).
[7] Vorlesungen uber die Theorie der algebraischen Zahlen, Leipzig, 1954. (Русский перевод: Гекке Е., Лекции по теории алгебраических чисел, ГИТТЛ, М., 1940.)

Дедекинд (Dedekind R.)
[8] Vorlesungen uber Zahlentheorie von P. G. Lejeune Dirichlet, Braunschweig, 1871—1894, Supplement 11. (Русский перевод: Лежен Дирихле П. Г., Лекции по теории чисел, в обработке и с добавлением Р. Дедекинда, ОНТИ НКТП, 1936.)

Ландау (Landau E.)
[9] Über die Verteilung der Primideale in den Idealklassen eines algebraischen Zahlkörpers, *Math. Ann.*, **63** (1907), 145—204.
[10] Einführung in die elementare und analitische Theorie der algebraischen Zahlen und der Ideale, Leipzig, 1927.

Ленг (Lang S.)
[11] Algebraic numbers, Addison-Wesley, 1964. (Русский перевод: Ленг С., Алгебраические числа, «Мир», М., 1966.)

Титчмарш (Titchmarsh E.)
[12] The theory of functions, 2nd edition, Oxford University Press, London, 1939. (Русский перевод: Титчмарш Е. К., Теория функций, ГИТТЛ, М., 1951.)
[13] The theory of the Riemann Zeta-function, Oxford University Press, London, 1951. (Русский перевод: Титчмарш Е. К., Теория ζ-функции Римана, ИЛ, М., 1953.)

Хассе (Hasse H.)
[14] Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, *Jber. dt. Math. Verein.*, **35** (1926), **36** (1927), **39** (1930).

Холл (Hall M.)
[15] The theory of groups, Macmillan, New York, 1959. (Русский перевод: Холл М., Теория групп, ИЛ, М., 1962.)

Шевалле (Chevalley C.)
[16] La théorie du corps de classes, *Ann. Math.*, **41** (1940), 394—418.

Шпейзер (Speiser A.)
[17] Die Theorie der Gruppen von endlicher Ordnung, Berlin, 1927.

Эстерман (Estermann T.)
[18] Introduction to modern prime number theory, *Camb. Tracts in Math.*, **41** (1952).

ГЛАВА IX

О башне полей классов

П. Роккетт

§ 1. ВВЕДЕНИЕ

Обозначим через k поле алгебраических чисел конечной степени и через h_k — его число классов, т. е. порядок конечной группы Cl_k классов дивизоров поля k. Одной из самых замечательных особенностей теории алгебраических чисел — по сравнению с теорией рациональных чисел — является существование полей k с числом классов $h_k > 1$, т. е. полей, у которых кольцо целых элементов не есть кольцо главных идеалов.

Возникает вопрос, можно ли любое такое поле k вложить в поле алгебраических чисел K конечной степени, для которого $h_K = 1$. Мы будем называть эту задачу задачей вложения для поля k, а поле K — решением задачи вложения.

Пусть k_1 — гильбертово поле классов поля k, т. е. максимальное неразветвленное абелево расширение поля k. Группа Галуа k_1 над k изоморфна в силу изоморфизма взаимности теории полей классов группе Cl_k. В частности,

$$[k_1 : k] = h_k.$$

Теорема главных дивизоров утверждает, что любой дивизор поля k становится главным в поле k_1. Но в поле k_1 могут существовать неглавные дивизоры; обозначим через k_2 гильбертово поле классов поля k_1. Продолжая этот процесс, мы получаем башню полей

$$k \subset k_1 \subset k_2 \subset k_3 \subset \ldots,$$

в которой каждое поле есть гильбертово поле классов предшествующего поля. Эта конструкция называется *башней гильбертовых полей классов* поля k. Мы обозначим через

k_∞ объединение всех полей k_i. Это поле алгебраических чисел конечной или бесконечной степени.

Предложение 1.1. *Если поле K является решением задачи вложения для поля k, т. е. $k \subset K$, $h_k = 1$, то $k_\infty \subset K$. В частности, степень поля k_∞ конечна.*

Обратно, если степень поля k_∞ конечна, то $h_{k_\infty} = 1$ и, следовательно, k_∞ является минимальным решением задачи вложения для поля k.

Доказательство. (i) Покажем сначала, что $k_i \subset K$ для всех i. Можно считать, что $i = 1$, так как затем проходит индукция по i. Расширение k_1/k неразветвленное и абелево, оба эти свойства переносятся на расширение k_1K/K. Следовательно, композит k_1K содержится в гильбертовом поле классов K_1 поля K. По предположению $[K_1 : K] = h_K = 1$, из чего следует, что $k_1 \subset K$.

(ii) Теперь мы предположим, что степень поля k_∞ конечна. Тогда $k_\infty = k_i$ для достаточно большого i.

Следовательно,

$$h_{k_\infty} = h_{k_i} = [k_{i+1} : k_i] = 1,$$

что и требовалось доказать.

Предложение 1.1 показывает, что задача вложения для поля k эквивалентна вопросу о конечности башни полей классов поля k. Эта проблема была поставлена Фуртвенглером и упоминается в работе Хассе [11] в связи с теоремой главных дивизоров (тогда еще не доказанной). Хотя теорема главных дивизоров была доказана уже в 1930 г. (Фуртвенглер), вопрос о конечности башни полей классов не был решен до 1964 г. Решение было дано Шафаревичем (совместно с Голодом), который показал, что ответ на этот вопрос отрицателен, т. е. башня полей классов может быть бесконечной.

Целью этой лекции является сообщение о результатах Шафаревича, а также о связанной с ними работе Брумера.

Пусть p — простое число. Расширение K/k называется *p-расширением*, если оно нормально и его группа Галуа есть p-группа. (Предостережение: если K/k не является расширением Галуа, то оно не называется p-расширением, даже если его степень есть степень числа p.)

Пусть $k_1^{(p)}$ — максимальное p-расширение поля k, содержащееся в k_1; оно называется *гильбертовым полем p-классов* поля k. Пусть $k_2^{(p)}$ — гильбертово поле p-классов поля $k_1^{(p)}$ и т. д. Мы получаем башню полей

$$k \subset k_1^{(p)} \subset k_2^{(p)} \subset k_3^{(p)} \subset \ldots,$$

в которой каждое поле есть гильбертово поле p-классов предшествующего поля. Эта конструкция называется *башней гильбертовых полей p-классов* поля k. Объединение полей $k_i^{(p)}$ обозначим через $k_\infty^{(p)}$.

Легко видеть, что $k_i^{(p)} \subset k_i$ и $k_i^{(p)}$ есть *максимальное* p-расширение поля k, содержащееся в k_i. Отсюда следует, что $k_\infty^{(p)} \subset k_\infty$. В частности, если степень поля $k_\infty^{(p)}$ бесконечна, то k_∞ — также бесконечное расширение.

Нас интересует следующий вопрос: при каких условиях $k_\infty^{(p)}$ имеет конечную степень, где p — фиксированное простое число. То, что мы имеем дело с $k_\infty^{(p)}$, а не с k_∞, объясняется лишь тем, что нам легче оперировать с p-группами, чем с произвольными разрешимыми группами.

Следующее предложение является аналогом предложения 1.1 для башни полей p-классов и доказывается так же, причем используется тот факт, что $[k_i^{(1)} : k] = h_k^{(p)}$ есть p-компонента числа классов h_k. Доказательство оставляется читателю.

Предложение 1.2. *Пусть p — простое число. Если задача вложения $k \subset K$ имеет решение относительно p, такое, что $p \nmid h_K$, то $h_\infty^{(p)} \subset K$. В частности, степень поля $k_\infty^{(p)}$ тогда конечна.*

Обратно, если степень поля $k_\infty^{(p)}$ конечна, то его число классов не делится на p и, следовательно, $k_\infty^{(p)}$ является минимальным решением задачи вложения для поля k относительно p.

Теперь мы сформулируем главный результат. Сначала дадим определение: если G — любая группа, мы обозначим через G/p максимальную абелеву факторгруппу показателя p группы G, рассматриваемую как векторное пространство над полем из p элементов. Мы определим p-ранг $d^{(p)}G$ как размерность факторгруппы G/p:

$$d^{(p)}G = \dim G/p.$$

Если G — конечная абелева группа, то $d^{(p)}G$ равен числу циклических примарных p-компонент в разложении группы G.

Теорема 1.1 (Голод — Шафаревич). *Существует функция $\gamma(n)$, такая, что*

$$d^{(p)} \mathrm{Cl}_k < \gamma(n)$$

для любого поля алгебраических чисел степени n, имеющего конечную башню полей p-классов.

Замечание. Как будет видно из доказательства теоремы 1.1, имеет место неравенство

$$d^{(p)} \mathrm{Cl}_k < 2 + 2\sqrt{r_k + \delta_k^{(p)}}, \tag{1}$$

где через r_k обозначено число бесконечных нормирований поля k, и $\delta_k^{(p)} = 1$ или 0 в зависимости от того, содержатся корни p-й степени из единицы в поле k или нет. Так как $r_k \leqslant n$ и $\delta_k^{(p)} \leqslant 1$, можно положить

$$\gamma(n) = 2 + 2\sqrt{n+1}.$$

Для того чтобы сформулировать следующую теорему, мы введем новое обозначение. Пусть q — дискретное нормирование поля рациональных чисел $\mathbf{Q}$, и пусть $\mathfrak{Q}$ — некоторое продолжение нормирования q на k с индексом ветвления $e(\mathfrak{Q})$. Тогда мы положим

$$e_k(q) = \text{н. о. д.}_{\mathfrak{D}|q} e(\mathfrak{Q}),$$

где $\mathfrak{D}$ пробегает все продолжения нормирования q на поле k (н.о.д. означает «наибольший общий делитель»). Мы назовем q *полностью разветвленным* в k, если $e_k(q) > 1$. Пусть $t_k^{(p)}$ — число полностью разветвленных нормирований q, таких, что p делит $e_k(q)$.

Теорема 1.2 (Брумер). *Существует функция* $c(n)$, *такая, что*

$$d^{(p)}\,\mathrm{Cl}_k \geqslant t_k^{(p)} - c(n)$$

для всех полей алгебраических чисел k *степени* n.

Замечание. Можно показать, что

$$d^{(p)}\,\mathrm{Cl}_k \geqslant t_k^{(p)} - r_k n,$$

где r_k имеет то же значение, что и в замечании к теореме 1.1. Так как $r_k \leqslant n$, можно положить

$$c(n) = n^2.$$

Мы докажем, следуя Брумеру, несколько ослабленную формулировку теоремы 1.2; мы будем рассматривать только нормальные расширения k поля $\mathbf{Q}$ и построим функцию $c'(n)$, такую, что для любого нормального расширения $k/\mathbf{Q}$ степени n имеет место неравенство

$$d^{(p)}\,\mathrm{Cl}_k \geqslant t_k^{(p)} - c'(n).$$

Доказательство теоремы 1.2 в общем случае нуждается в использовании когомологий Амицура в числовых полях, которые мы не предполагаем известными в этой главе.

Для расширений Галуа мы покажем, что

$$d^{(p)}\,\mathrm{Cl}_k \geqslant t_k^{(p)} - \left(\frac{r_k - 1}{p-1} + w_p(n)\cdot\delta_k^{(p)}\right), \qquad (2)$$

где $w_p(n)$ обозначает p-показатель числа n. Так как $w_p(n) \leqslant n - 1$, мы можем положить

$$c'(n) = (n-1) + (n-1) = 2(n-1).$$

Комбинируя теоремы 1.1 и 1.2, мы получаем

Следствие. *Если* k *есть поле алгебраических чисел степени* n *и*

$$t_k^{(p)} \geqslant \gamma(n) + c(n),$$

то башня полей p*-классов бесконечна.*

В частности, для любой данной степени $n > 1$ *и любого простого числа* p, *делящего* n, *существует бесконечно много полей алгебраических чисел* k *степени* n, *имеющих бесконечную башню полей* p*-классов. Таковы, например, поля*

$$k = \mathbf{Q}\left(\sqrt[n]{q_1 \dots q_N}\right),$$

где $N \geqslant \gamma(n) + c(n)$ *и все* $q_i > 0$ — *различные простые числа из* $\mathbf{Q}$.

Численный пример. Рассмотрим случай $n = p = 2$ и используем оценки, данные формулами (1) и (2). Мы имеем $\delta_k^{(2)} = 1$, $w_2(2) = 1$. Кроме того, $t_k^{(2)}$ есть в точности число разветвленных в поле k простых дивизоров поля $\mathbf{Q}$. Отсюда следует: *квадратичное поле* k *имеет бесконечную башню полей 2-классов, если число разветвленных в* k *простых дивизоров поля* $\mathbf{Q}$ *удовлетворяет неравенству*

$$t_k^{(2)} \geqslant 2 + 2\sqrt{r_k + 1} + r_k.$$

Если поле k мнимое, то $r_k = 1$. Так как $2 + 2\sqrt{2} + 1 < 6$, то любое мнимое квадратичное поле, в котором разветвлено по крайней мере шесть простых дивизоров поля $\mathbf{Q}$, имеет бесконечную башню полей 2-классов. Наименьший численный пример таков:

$$k = \mathbf{Q}\left(\sqrt{-2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13}\right) = \mathbf{Q}\left(\sqrt{-30\,030}\right).$$

Если поле k вещественное, то $r_k = 2$. Так как $2 + 2\sqrt{3} + 2 < 8$, то любое вещественное квадратичное поле, в котором разветвлено по крайней мере восемь простых дивизоров поля $\mathbf{Q}$, имеет бесконечную башню полей 2-классов. Наименьший численный пример:

$$k = \mathbf{Q}\left(\sqrt{2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19}\right) = \mathbf{Q}\left(\sqrt{9\,699\,690}\right).$$

§ 2. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1.1

Мы будем использовать следующие обозначения:

k — поле алгебраических чисел конечной степени;
Cl_k — группа классов дивизоров поля k;
C_k — группа классов иделей поля k;
U_k — группа единичных иделей;
$E_k = U_k \cap k$ — группа единиц поля k;
W_k — группа корней из единицы, содержащихся в поле k;

p — фиксированное простое число;
$K = k_\infty^{(p)}$ — было объяснено в § 1;
$G = G(K/k)$ — группа Галуа расширения K/k.

Мы собираемся доказать неравенство (1) § 1 в предположении, что степень $[K : k]$ конечна.

Доказательство состоит из двух частей. Сначала мы редуцируем теорему 1.1 к теоретико-групповому утверждению о конечных p-группах, а во второй части доказываем это утверждение.

Теорема Дирихле о единицах утверждает, что E_k является прямым произведением конечной циклической группы W_k и свободной абелевой группы с $r_k - 1$ свободным образующим (см. гл. II, § 18). Это дает нам, что

$$d^{(p)}E_k = (r_k - 1) + d^{(p)}W_k = (r_k - 1) + \delta_k^{(p)};$$

следовательно, доказываемое неравенство (1) § 1 можно записать в виде

$$d^{(p)}\mathrm{Cl}_k < 2 + 2\sqrt{d^{(p)}E_k + 1},$$

или, избавляясь от иррациональности,

$$\frac{1}{4}(d^{(p)}\mathrm{Cl}_k)^2 - d^{(p)}\mathrm{Cl}_k < d^{(p)}E_k. \qquad (1)$$

Сначала мы заметим, что

$$d^{(p)}\mathrm{Cl}_k = d^{(p)}G.$$

Действительно, мы имеем

$$d^{(p)}G = d^{(p)}(G^{\mathrm{ab}}),$$

где G^{ab} обозначает максимальную абелеву факторгруппу группы G. Это непосредственно следует из определения p-ранга группы G, данного в § 1. Кроме того, G^{ab} является группой Галуа максимального абелева над k подполя поля K. Это подполе совпадает с гильбертовым полем p-классов $k_1^{(p)}$. В силу изоморфизма взаимности теории полей классов мы имеем равенство

$$G^{\mathrm{ab}} = \mathrm{Cl}_k^{(p)},$$

где $\mathrm{Cl}_k^{(p)}$ обозначает p-силовскую подгруппу Cl_k. По определению p-ранга

$$d^{(p)}\mathrm{Cl}_k^{(p)} = d^{(p)}\mathrm{Cl}_k.$$

Это доказывает наше утверждение.

Следовательно, доказываемое неравенство (1) может быть записано в виде

$$\frac{1}{4}(d^{(p)}G)^2 - d^{(p)}G < d^{(p)}E_k. \qquad (2)$$

Любая факторгруппа E_k имеет p-ранг $\leqslant d^{(p)}E_k$. В частности, это верно для норменной факторгруппы

$$E_k/N_{K/k}(E_K) = \hat{H}^0(G, E_K).$$

Следовательно, достаточно показать, что

$$\frac{1}{4}(d^{(p)}G)^2 - d^{(p)}G < d^{(p)}\hat{H}^0(G, E_k). \qquad (3)$$

Для вычисления правой части мы используем точную последовательность

$$1 \to E_K \to U_K \to U_K/E_K \to 1.$$

Так как расширение K/k не разветвлено, то U_K — когомологически тривиальный G-модуль (для доказательства нужно разложить U_K на локальные компоненты и доказать аналогичное утверждение для группы единиц локального расширения Галуа; см. гл. VI, п. 2.5) [1]).

Отсюда следует, что

$$\hat{H}^0(G, E_K) = H^{-1}(G, U_K/E_K).$$

Теперь мы используем точную последовательность

$$1 \to U_K/E_K \to C_K \to \mathrm{Cl}_K \to 1.$$

Порядок группы Cl_K взаимно прост с p; это следует из того, что $K = k_\infty^{(p)}$ является максимальным полем в гильбертовой башне p-классов; см. предложение 1.2. Так как G — p-группа, то мы можем заключить, что Cl_K — когомологи-

[1]) Напомним, что неразветвленность *бесконечного* дивизора означает, что соответствующее локальное расширение тривиально, т. е. имеет степень 1.

чески тривиальный G-модуль. Следовательно,

$$H^{-1}(G, U_K/E_K) = H^{-1}(G, C_K) = H^{-3}(G, \mathbf{Z})$$

в силу фундаментальной теоремы Тэйта о когомологиях в теории полей классов (гл. VII, п. 11.3).

Отсюда следует, что неравенство (3) может быть записано в виде

$$\frac{1}{4}(d^{(p)}G)^2 - d^{(p)}G < d^{(p)}H_2(G, \mathbf{Z}). \tag{4}$$

Мы использовали равенство

$$H_2(G, \mathbf{Z}) = H^{-3}(G, \mathbf{Z}),$$

являющееся просто определением когомологий групп в отрицательных размерностях.

Неравенство (4) представляет собой уже чисто теоретико-групповое утверждение: *мы увидим, что* (4) *верно для любой конечной p-группы G.*

Согласно нашим обозначениям, введенным в § 1, $\mathbf{Z}/p$ обозначает циклическую группу из p элементов. Группы гомологий $H_i(G, Z/p)$ аннулируются умножением на p и, следовательно, могут рассматриваться как векторное пространство над полем из p элементов. Мы положим

$$d_i^{(p)}G = \dim H_i(G, \mathbf{Z}/p).$$

Лемма 2.1. *Для любой группы G существует естественный изоморфизм $H_1(G, \mathbf{Z}/p) = G/p$. В частности, $d_1^{(p)}G = d^{(p)}G$.*

Лемма 2.2. *Для любой конечной группы G имеет место равенство*

$$d^{(p)}H_2(G, \mathbf{Z}) = d_2^{(p)}G - d_1^{(p)}G.$$

Доказательство. Рассмотрим точную последовательность

$$0 \to \mathbf{Z} \xrightarrow[p]{} \mathbf{Z} \to \mathbf{Z}/p \to 0,$$

где $\xrightarrow[p]{}$ обозначает отображение «умножение на p», и соответствующую точную последовательность гомологий

$$H_i(\mathbf{Z}) \xrightarrow[p]{} H_i(\mathbf{Z}) \to H_i(\mathbf{Z}/p) \to H_{i-1}(\mathbf{Z}) \to H_{i-1}(\mathbf{Z})$$

(для краткости мы пишем $H_i(\mathbf{Z})$ вместо $H_i(G, \mathbf{Z})$).

Вообще если A — абелева группа, то через A_p будет обозначаться ядро отображения $A \xrightarrow[p]{} A$, его коядро — через A/p. В этих обозначениях мы получаем точную последовательность

$$0 \to H_i(\mathbf{Z})/p \to H_i(\mathbf{Z}/p) \to H_{i-1}(\mathbf{Z})_p \to 0. \tag{5}$$

Во-первых, положим $i = 1$. Группа $H_0(\mathbf{Z}) = \mathbf{Z}$ не имеет p-кручения, поэтому $H_0(\mathbf{Z})_p = 0$ и, следовательно,

$$H_1(\mathbf{Z})/p = H_1(\mathbf{Z}/p). \tag{6}$$

Имеет место равенство $H_1(\mathbf{Z}) = H_1(G, \mathbf{Z}) = G^{ab}$, где G^{ab} — максимальная абелева факторгруппа G (см. гл. IV). По определению G/p мы имеем $G/p = G^{ab}/p$. Это доказывает лемму 2.1.

Во-вторых, положим $i = 2$ в формуле (5). Так как G — конечная группа, то все фигурирующие здесь группы конечны; следовательно, они являются конечномерными векторными пространствами над полем из p элементов. Их размерности связаны соотношением

$$d_2^{(p)}G = d^{(p)}H_2(\mathbf{Z}) + \dim H_1(\mathbf{Z})_p.$$

Вообще если A — конечная абелева группа, то $\dim A_p = \dim A/p$, что доказывается разложением A на циклические прямые слагаемые. Применяя это к группе $A = H_1(\mathbf{Z})$ и используя формулу (6), мы получаем

$$\dim H_1(\mathbf{Z})_p = \dim H_1(\mathbf{Z}/p) = d_1^{(p)}G.$$

Это доказывает лемму 2.2.

Используя леммы 2.1 и 2.2, мы видим, что доказываемое неравенство (4) эквивалентно следующему утверждению.

Теорема 2.1. *Пусть G — конечная p-группа (p — простое число). Тогда*

$$d_2^{(p)}G > \frac{1}{4}(d_1^{(p)}G)^2.$$

Введем следующие обозначения:

$\Lambda = \mathbf{Z}(G)$ — групповое кольцо группы G над $\mathbf{Z}$;

I — пополняющий идеал Λ, т. е. ядро пополняющего отображения $\Lambda \to \mathbf{Z}$;

Λ/p — групповое кольцо группы G над полем из p элементов.

Теперь мы докажем две подготовительные леммы.

Лемма 2.3. *Пусть G — конечная p-группа и A — такой G-модуль, что $pA = 0$. Тогда минимальное число образующих A как G-модуля равно*

$$\dim H_0(G, A) = \dim A/IA,$$

где размерность рассматривается над полем из p элементов.

Более точно: пусть $a_i \in A$. Тогда a_i порождают A как G-модуль в том и только том случае, если их образы в A/IA порождают A/IA как векторное пространство.

Доказательство. Предположим, что a_i порождают A/IA. Пусть B есть G-подмодуль модуля A, порожденный элементами a_i. Тогда естественное отображение $B/IB \to A/IA$, которое совпадает с отображением $H_0(B) \to H_0(A)$, сюръективно. Точная последовательность

$$0 \to B \to A \to A/B \to 0$$

дает нам точную последовательность гомологий

$$H_0(B) \to H_0(A) \to H_0(A/B) \to 0,$$

из которой мы заключаем, что $H_0(A/B) = 0$. Так как A/B аннулируется умножением на p и G является p-группой, то $A/B = 0$, т. е. $A = B$ (см. гл. IV, § 9).

Лемма 2.4. *Пусть G — конечная p-группа и A — такой G-модуль, что $pA = 0$. Тогда существует резольвента*

$$\ldots \to Y_2 \to Y_1 \to Y_0 \to A \to 0,$$

обладающая следующими свойствами:

(i) *все Y_n — свободные модули над Λ/p;*

(ii) *число свободных образующих модулей Y_n над Λ/p равно* $\dim H_n(G, A)$;

(iii) *образ* $\operatorname{Im}(Y_{n+1})$ *содержится в IY_n.*

Доказательство. Положим $d = \dim H_0(G, A)$. По лемме 2.3 существует свободный Λ-модуль X с d образующими и эпиморфизм $X \to A$. Так как $pA = 0$, то отображение $X/p \to A$ — тоже эпиморфизм. Положим $Y = X/p$. Тогда Y является свободным Λ/p-модулем с d образующими. В частности,

$$H_i(Y) = 0 \text{ для } i \geqslant 1.$$

Пусть B — ядро отображения $Y \to A$; тогда последовательность

$$0 \to B \to Y \to A \to 0$$

точная. Из точной последовательности гомологий

$$\ldots \to H_{i+1}(Y) \to H_{i+1}(A) \to H_i(B) \to H_i(Y) \to \ldots$$

мы получаем, что

$$H_i(B) = H_{i+1}(A) \tag{7}$$

для $i \geqslant 1$. В случае $i = 0$ мы имеем точную последовательность

$$0 \to H_1(A) \to H_0(B) \to H_0(Y) \to H_0(A) \to 0.$$

По построению Y и A как G-модули имеют одно и то же минимальное число образующих, следовательно, по лемме 2.3 $\dim H_0(Y) = \dim H_0(A)$, откуда видно, что $H_0(Y) \to H_0(A)$ — изоморфизм. Таким образом, (7) верно и в случае $i = 0$.

Так как $H_0(Y) \to H_0(A)$ — изоморфизм, то отображение

$$B/IB = H_0(B) \to H_0(Y) = Y/IY$$

нулевое; следовательно,

$$B \subset IY. \tag{8}$$

Теперь положим $Y = Y_0$. Тогда $Y_0 \to A \to 0$ является первым шагом в построении резольвенты. Второй шаг получается применением той же операции к модулю B. Мы получаем $Y_1 \to B \to 0$ с ядром C, таким, что

$$H_i(C) = H_{i+1}(B) = H_{i+2}(A)$$

для $i \geqslant 0$ и

$$C \subset IY_1.$$

Y_1 — свободный Λ/p модуль с $\dim H_0(B) = \dim H_1(A)$ образующими. Если мы определим $Y_1 \to Y_0$ как сквозное отображение $Y_1 \to B \to Y_0$, то из (8) следует, что $\operatorname{Im}(Y_1) \subset IY_0$.

Продолжая этот процесс, мы по индукции получаем утверждение леммы 2.4.

Применим теперь лемму 2.4 к случаю $A = \mathbf{Z}/p$. Тогда $\dim H_0(G, \mathbf{Z}/p) = \dim \mathbf{Z}/p = 1$. Следовательно, Y_0 — свободный модуль с одной образующей. Из (iii) следует, что ядро отображения $Y_0 \to \mathbf{Z}/p$ содержится в IY_0. Так как $\dim (Y_0/IY_0) = 1$, то это ядро в точности совпадает с IY_0. Значит, последовательность $Y_1 \to IY_0 \to 0$ точна. Изменяя обозначения, мы получаем

Следствие. *Пусть G — конечная p-группа; положим $d = d_1^{(p)}G$, $r = d_2^{(p)}G$. Тогда существует точная последовательность*

$$R \to D \to IE \to 0, \text{ причем } \operatorname{Im}(R) \subset ID,$$

где E, D, R обозначают свободные Λ/p-модули соответственно с 1, d, r образующими.

Доказательство теоремы 2.1. Мы используем обозначения только что сформулированного следствия.

Для любого конечного G-модуля A, такого, что $pA = 0$, введем многочлен Пуанкаре

$$P_A(t) = \sum_{0 \leqslant n} c_n(A) \cdot t^n, \text{ где } c_n(A) = \dim I^n A/I^{n+1}A.$$

(Заметим, что $c_n(A) = 0$, если n достаточно велико.) Положим

$$P(t) = P_E(t).$$

Так как $c_0(E) = \dim E/IE = 1$, мы получаем

$$P_{IE}(t) = \frac{P(t) - 1}{t}.$$

Кроме того, так как $D = E^d$ является d-кратным прямым произведением модуля E, мы имеем $c_n(D) = d \cdot c_n(E)$ и, следовательно,

$$P_D(t) = d \cdot P(t).$$

Аналогично

$$P_R(t) = r \cdot P(t).$$

Вообще если $0 < t < 1$ — вещественная переменная, то

$$P_A(t) \frac{1}{1-t} = \sum_{0 \leqslant n} s_n(A) t^n,$$

где $s_n(A) = \sum_{0 \leqslant i \leqslant n} c_i(A) = \dim A/I^{n+1}A$. Кроме того,

$$P_A(t) \frac{t}{1-t} = \sum_{0 \leqslant n} s_{n-1}(A) t^n,$$

где мы полагаем $s_{-1}(A) = 0$.

Из следствия из леммы 2.4 мы получаем эпиморфизм $I^{n+1}D \to I^{n+2}E$. Следовательно, если обозначить через R_{n+1} прообраз $I^{n+1}D$ в R, то последовательность

$$0 \to R/R_{n+1} \to D/I^{n+1}D \to IE/I^{n+2}E \to 0$$

точна. Это дает нам равенство

$$s_n(D) = s_n(IE) + \dim R/R_{n+1}.$$

Следствие к лемме 2.4 показывает, что $\operatorname{Im} R \subset ID$, значит $\operatorname{Im}(I^n R) \subset I^{n+1}D$ и $I^n R \subset R_{n+1}$. Поэтому

$$\dim R/R_{n+1} \leqslant \dim R/I^n R = s_{n-1}(R).$$

Это дает нам неравенства

$$s_n(D) \leqslant s_n(IE) + s_{n-1}(R).$$

Числа, входящие в эти неравенства, являются коэффициентами рассмотренных выше степенных рядов. Отсюда следует, что

$$P_D(t) \frac{1}{1-t} \leqslant P_{IE}(t) \frac{1}{1-t} + P_R(t) \frac{t}{1-t},$$

или, что равносильно,

$$d \cdot P(t) \leqslant \frac{P(t) - 1}{t} + r \cdot t \cdot P(t) \text{ при } 0 < t < 1.$$

Иначе говоря, мы имеем

$$1 \leqslant P(t) \cdot (rt^2 - dt + 1) \text{ при } 0 < t < 1.$$

Так как $P(t)$ — многочлен с положительными коэффициентами, мы можем заключить, что

$$0 < rt^2 - dt + 1 \quad \text{при} \quad 0 < t < 1.$$

Сделав подстановку $t = \frac{d}{2r}$, мы получаем

$$r > \frac{1}{4} d^2,$$

что и утверждалось. Подстановка $t = \frac{d}{2r}$ допустима, так как по лемме 2.2 нам известно, что $d \leqslant r < 2r$, и потому $0 < \frac{d}{2r} < 1$.

Замечание 1. Фактически Голод и Шафаревич доказали в своей работе, что $d_2^{(p)}G > \frac{1}{4}(d_1^{(p)}G - 1)^2$. Доказанное здесь неравенство было получено независимо Гашуцем и Винбергом.

Замечание 2. Теорема 2.1 имеет значение не только для задачи о башне полей классов, но и для различных других задач в теории p-групп. Это объясняется тем, что гомологические инварианты $d_1^{(p)}G$ и $d_2^{(p)}G$ допускают для конечной p-группы G следующую теоретико-групповую интерпретацию: $d_1^{(p)}G$ — это минимальное число образующих группы G (теорема Бернсайда, см. гл. V, п. 2.5) и $d_2^{(p)}G$ — минимальное число соотношений между этими образующими, определяющих G как p-группу (см. Серр [6]).

§ 3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1.2 ДЛЯ РАСШИРЕНИЙ ГАЛУА

Пусть $k/\mathbf{Q}$ — расширение Галуа конечной степени n, и p — простое число. Как было сказано в § 1, мы собираемся доказать неравенство

$$d^{(p)}\mathrm{Cl}_k \geqslant t_k^{(p)} - \left(\frac{r_k - 1}{p-1} + w_p(n)\cdot\delta_k^{(p)}\right). \qquad (1)$$

Доказательство снова распадается на две части. Во-первых, мы редуцируем задачу к теоретико-групповому утверждению о когомологиях конечных групп; во-вторых, мы докажем это утверждение.

Пусть $K = k_1$ — гильбертово поле классов поля k;
G — группа Галуа расширения K/k;
G^* — группа Галуа расширения $K/\mathbf{Q}$;
g — группа Галуа расширения $k/\mathbf{Q}$.

Тогда $g = G^*/G$, и мы можем написать когомологическую последовательность с отображениями инфляции и ограничения:

$$1 \to H^1(g, E_k) \to H^1(G^*, E_K) \to H^1(G, E_K),$$

где E_k обозначает, как и в § 2, группу единиц поля k. Мы можем заключить, что

$$d^{(p)}H^1(G^*, E_K) \leqslant d^{(p)}H^1(G, E_K) + d^{(p)}H^1(g, E_k).$$

Следовательно, доказываемое неравенство (1) есть немедленное следствие следующих трех утверждений:

$$H^1(G, E_K) = \mathrm{Cl}_k; \qquad (2)$$

$$d^{(p)}H^1(G^*, E_K) = t_k^{(p)}; \qquad (3)$$

$$d^{(p)}H^1(g, E_k) \leqslant \frac{r_k - 1}{p-1} + w_p(n)\,\delta_k^{(p)}. \qquad (4)$$

Докажем эти утверждения.

Для любого поля алгебраических чисел K конечной степени мы рассмотрим коммутативную и точную диаграмму

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & E_K & \to & U_K & \to & U_K/E_K & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & K^* & \to & I_K & \to & C_K & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & P_K & \to & D_K & \to & \mathrm{Cl}_K & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

где K^* — мультипликативная группа поля K, I_K — группа иделей, D_K — группа дивизоров, P_K — группа главных дивизоров, а остальные группы имеют то же значение, что и в § 2. Все стрелки обозначают естественные отобра-

жения. (В § 2 мы уже использовали первую строку и последний столбец этой диаграммы.)

Так как K/k — нормальное расширение с группой Галуа G, то все группы и отображения этой диаграммы G-допустимы, и мы получаем соответствующую коммутативную и точную когомологическую диаграмму

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & E_K & \longrightarrow & U_k & \xrightarrow[\varepsilon]{} & (U_K/E_K)^G & \xrightarrow[\delta]{} & H^1(G, E_K) \xrightarrow[\varphi]{} H^1(G, U_K) \\
 & & \downarrow & & \zeta\downarrow & & \downarrow\gamma & & \downarrow \\
1 & \to & k^* & \longrightarrow & I_k & \xrightarrow[\eta]{} & C_k & \longrightarrow & 1 \\
 & & \downarrow & & \xi\downarrow & & \downarrow\beta & & \\
1 & \to & P_K^G & \longrightarrow & D_K^G & \xrightarrow[\alpha]{} & \mathrm{Cl}_K^G & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & H^1(G, E_K) & \xrightarrow[\varphi]{} & H^1(G, U_K) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}$$

Здесь мы дважды использовали «теорему Гильберта 90»:

$$H^1(G, K^*) = 1,$$

а также соответствующее локальное утверждение:

$$H^1(G, I_K) = 1.$$

Лемма 3.1. *Пусть K — поле алгебраических чисел конечной степени, нормальное над своим подполем k с группой Галуа G.*

Предположим, что $D_K^G \subset P_K$, т. е. что любой инвариантный дивизор главный. Тогда существует естественная точная последовательность

$$1 \to \mathrm{Cl}_k \to H^1(G, E_K) \xrightarrow[\varphi]{} H^1(G, U_K) \to 1.$$

Доказательство. Мы используем уже построенную когомологическую диаграмму. Заметим, что естественное отображение

$$\varphi\colon H^1(G, E_K) \to H^1(G, U_K)$$

дважды встречается в этой диаграмме. Мы должны показать, что при предположении леммы 3.1 φ является эпиморфизмом и его ядро равно Cl_k.

Предположение леммы 3.1 дает нам $P_K^G = D_K^G$. Из рассмотрения левого нижнего угла когомологической диаграммы мы получаем сюръективность отображения φ.

С другой стороны, равенство $P_K^G = D_K^G$ показывает, что $\alpha = 1$. Значит, $\alpha \circ \xi = \beta \circ \eta = 1$. Так как φ сюръективно, то $\beta = 1$. Следовательно, γ — изоморфизм. Из рассмотрения правого верхнего угла нашей диаграммы мы получаем

$$\ker(\varphi) = \mathrm{Im}(\delta) = (U_K/E_K)^G/\mathrm{Im}(\varepsilon);$$

пользуясь изоморфизмом γ, мы можем продолжить цепочку равенств:

$$C_k/\mathrm{Im}(\gamma\circ\varepsilon) = C_k/\mathrm{Im}(\eta\cdot\zeta) = I_k/k\cdot U_k = \mathrm{Cl}_k.$$

Доказательство утверждения (2). Мы применим лемму 3.1 в случае, когда поле K (как и в (2)) является гильбертовым полем классов поля k. Так как K/k — неразветвленное расширение, то, как уже было замечено в § 2, $H^1(G, U_K) = 1$. Следовательно, в силу леммы 3.1 достаточно показать, что предположение леммы 3.1 выполняется, если K — гильбертово поле классов поля k.

Так как $H^1(G, U_K) = 1$, мы можем заключить из нашей когомологической диаграммы, что отображение $\xi\colon I_k \to D_K^G$ сюръективно. С другой стороны, его образ равен $I_k/U_k = D_k$. Следовательно, $D_k = D_K^G$. По теореме главных дивизоров для гильбертова поля классов мы получаем $D_k \subset P_K$, что и требовалось доказать.

Доказательство утверждения (3). Мы хотим применить лемму 3.1 к нормальному расширению $K/\mathbf{Q}$, где K (как и в (3)) — гильбертово поле классов поля k. Сначала мы должны показать, что предположение леммы 3.1 выполняется для $K/\mathbf{Q}$.

G^* — это группа Галуа расширения $K/\mathbf{Q}$, а G — группа Галуа расширения K/k. Следовательно, $G \subset G^*$ и $D_K^{G^*} \subset D_K^G$. Предшествующее доказательство показывает, что $D_K^G \subset P_K$. Значит, $D_K^{G^*} \subset P_K$.

Так как $\mathrm{Cl}_{\mathbf{Q}} = 1$, то лемма 3.1 дает нам изоморфизм

$$H^1(G^*, E_K) \cong H^1(G^*, U_K).$$

Для любого конечного дивизора q поля $\mathbf{Q}$ обозначим через $e_K(q)$ индекс ветвления какого-нибудь делителя $\mathfrak{Q}$ дивизора q в поле K. (Так как $K/\mathbf{Q}$ — нормальное расширение, то $e_K(q)$ не зависит от выбора $\mathfrak{Q} \mid q$.) Пусть $\mathbf{Z}/e_K(q)$ обозначает циклическую группу порядка $e_K(q)$. Тогда

$$H^1(G^*, U_K) = \coprod_q \mathbf{Z}/e_K(q).$$

(Для доказательства нужно разложить U_K на локальные компоненты и доказать аналогичное утверждение для локального расширения Галуа и соответствующей группы единиц.)

Так как расширение K/k неразветвлено, то

$$e_K(q) = e_k(q)$$

для любого q. Следовательно, мы получаем

$$H^1(G^*, E_K) = \coprod_q \mathbf{Z}/e_k(q).$$

У прямого произведения в правой части p-ранг равен числу таких q, что $p \mid e_K(q)$, т. е. равен $t_k^{(p)}$, что и требовалось доказать.

Доказательство утверждения (4). Группой кручения в E_k является группа W_k корней из единицы, содержащихся в E_k; это циклическая группа p-ранга $\delta_k^{(p)}$. Теорема о единицах утверждает, что E_k/W_k — свободная абелева группа с $r_k - 1$ образующими. Следовательно, (4) немедленно вытекает из следующего теоретико-группового утверждения.

Лемма 3.2. *Пусть G — конечная группа порядка n и p — простое число. Пусть A — конечно порожденный G-модуль с группой кручения tA, и $\rho(A)$ обозначает число свободных образующих у A/tA как абелевой группы. Тогда*

$$d^{(p)}H^1(G, A) \leqslant \frac{\rho(A)}{p-1} + w_p(n) \cdot d^{(p)}tA.$$

Доказательство. Рассмотрим отображение ограничения

$$H^1(G, A) \to H^1(G^{(p)}, A)$$

группы G на ее p-силовскую подгруппу $G^{(p)}$. Это мономорфизм p-примарных компонент (см. гл. IV, следствие 3 из предложения 6.3). В частности,

$$d^{(p)}H^1(G, A) \leqslant d^{(p)}H^1(G^{(p)}, A).$$

Следовательно, мы можем в дальнейшем считать, что $G = G^{(p)}$ является p-группой. (Заметим, что $w_p(n) = w_p(n^{(p)})$, где $n^{(p)}$ обозначает порядок группы $G^{(p)}$.)

Мы рассмотрим точную последовательность

$$0 \to tA \to A \to A/tA \to 0$$

и соответствующую точную последовательность когомологий

$$H^1(G, tA) \to H^1(G, A) \to H^1(G, A/tA).$$

Из нее следует, что

$$d^{(p)}H^1(G, A) \leqslant d^{(p)}H^1(G, tA) + d^{(p)}H^1(G, A/tA).$$

Мы покажем, что

$$d^{(p)}H^1(G, tA) \leqslant w_p(n) \cdot d^{(p)}tA$$

и

$$d^{(p)}H^1(G, A/tA) \leqslant \frac{\rho(A)}{p-1}.$$

Иначе говоря, *мы рассмотрим отдельно следующие два случая*: (I) A является модулем кручения; (II) A — модуль без кручения.

(I) *Случай модуля кручения.* Мы имеем

$$d^{(p)}G = \dim G/p \leqslant w_p(n),$$

и, следовательно, достаточно показать, что

$$d^{(p)}H^1(A) \leqslant d^{(p)}G \cdot d^{(p)}A. \tag{5}$$

(Для краткости мы опускаем символ G в обозначениях групп когомологий.) Пусть $Z^1(A)$ обозначает модуль скрещенных гомоморфизмов $f\colon G \to A$. Пусть $g_1, \ldots, g_d$ образуют минимальную систему образующих в G; теорема Бернсайда для p-групп утверждает, что $d = d^{(p)}G$. Любой скрещенный гомоморфизм однозначно определяется своими значениями $f(g_i)$, $1 \leqslant i \leqslant d$. Иначе говоря, отображение

$$f \to (f(g_1), \ldots, f(g_d))$$

является вложением $Z^1(A)$ в d-кратное прямое произведение A^d модулей A. Отсюда следует, что

$$d^{(p)}Z^1(A) \leqslant d^{(p)}(A^d) = d\cdot(d^{(p)}A) = d^{(p)}G\cdot d^{(p)}A.$$

Так как $H^1(A)$ — фактормодуль модуля $Z^1(A)$, то неравенство (5) доказано.

Замечание. В приведенном доказательстве мы нигде не пользовались тем, что A — модуль кручения. Следовательно, неравенство (5) выполняется для *любого* конечно порожденного G-модуля. Это значит, что вместо (4) мы уже доказали неравенство

$$d^{(p)}H^1(g, E_k) \leqslant w_p(n)(r_k - 1 + \delta_k^{(p)})$$

и, следовательно, вместо (1) — неравенство

$$d^{(p)}\mathrm{Cl}_k \geqslant t_k^{(p)} - w_p(n)(r_k - 1 + \delta_k^{(p)}).$$

Этого достаточно для получения функции $c'(n)$, такой, что

$$d^{(p)}\mathrm{Cl}_k \geqslant t_k^{(p)} - c'(n).$$

Так как $w_p(n) \leqslant n-1$, мы можем положить

$$c'(n) = (n-1)n.$$

Следующее доказательство позволяет получить более точную оценку для модулей без кручения; оно необходимо только для того, чтобы получить более точную оценку $c'(n) = 2(n-1)$, указанную в замечании к формулировке теоремы 1.2.

(II) *Случай модуля без кручения.*

Лемма 3.3 (Шевалле). *Пусть G — группа порядка p и A — конечно порожденный G-модуль. Тогда*

$$d^{(p)}H^1(G, A) - d^{(p)}H^2(G, A) \quad \frac{\rho(A) - p\rho(A^G)}{p-1}.$$

Доказательство. (i) Введем обозначение

$$d_{1-2}(A) = d^{(p)}H^1(A) - d^{(p)}H^2(A).$$

Заметим, что $p\cdot H^i(A) = 0$, так как G имеет порядок p. Значит, $d^{(p)}H^i(A)$ — размерность группы $H^i(A)$ над полем из p элементов; следовательно, порядок $h^i(A)$ группы $H^i(A)$ равен p в степени $d^{(p)}H^i(A)$. Введем в рассмотрение индекс Эрбрана:

$$h_{1/2}(A) = h^1(A)/h^2(A);$$

тогда

$$h_{1/2}(A) = p^{d_{1-2}(A)}.$$

Следовательно, мы можем рассматривать $d_{1-2}(A)$ как аддитивный аналог индекса Эрбрана. Свойства индекса Эрбрана, сформулированные в гл. IV, § 8, могут быть, таким образом, приложены *с необходимыми изменениями* к d_{1-2}. В частности, верно следующее утверждение.

Если $0 \to A \to B \to C \to 0$ — точная последовательность G-модулей, то

$$d_{1-2}(B) = d_{1-2}(A) + d_{1-2}(C).$$

Таким образом, мы можем сказать, что d_{1-2} является *аддитивной функцией* на G-модулях.

Мы будем говорить, что два конечно порожденных G-модуля A, B *рационально эквивалентны*, если $A \otimes \mathbf{Q}$ и $B \otimes \mathbf{Q}$ изоморфны как $\mathbf{Q}(G)$-модули. (Рассматриваются тензорные произведения над $\mathbf{Z}$, а $\mathbf{Q}(G) = \mathbf{Z}(G) \otimes \mathbf{Q}$ обозначает групповое кольцо G над $\mathbf{Q}$.) Мы можем рассматривать A/tA как подмодуль из $A \otimes \mathbf{Q}$ и фактически как G-инвариантную решетку в пространстве рациональных представлений $A \otimes \mathbf{Q}$ группы G. В силу предложений 8.1 и 8.2 гл. IV мы имеем:

Если A и B рационально эквивалентны, то $d_{1-2}(A) = d_{1-2}(B)$.

Следовательно, мы можем сказать, что $d_{1-2}(A)$ есть *функция на классах рациональной эквивалентности.*

(ii) Для сокращения записи определим функцию

$$\tau(A) = \frac{\rho(A) - \rho\cdot\rho(A^G)}{p-1}.$$

Мы утверждаем, что $\tau(A)$ — тоже аддитивная функция на классах рациональной эквивалентности, и чтобы в этом убедиться, покажем, что таковыми являются как $\rho(A)$, так и $\rho(A^G)$.

Из определения ρ следует, что

$$\rho(A) = \dim_{\mathbf{Q}} A \otimes \mathbf{Q} \quad \text{и} \quad \rho(A^G) = \dim_{\mathbf{Q}} A^G \otimes \mathbf{Q}.$$

Из первого соотношения мы заключаем, что $\rho(A)$ — функция на классах рациональной эквивалентности. Из второго соотношения мы можем заключить то же про $\rho(A^G)$, так как

$$A^G \otimes \mathbf{Q} = (A \otimes \mathbf{Q})^G.$$

Если $0 \to A \to B \to C \to 0$ — точная последовательность, то последовательность

$$0 \to A \otimes \mathbf{Q} \to B \otimes \mathbf{Q} \to C \otimes \mathbf{Q} \to 0$$

тоже точная. Это доказывает аддитивность функции $\rho(A)$. Аддитивность функции $\rho(A^G)$ следует из того, что последовательность

$$0 \to (A \otimes \mathbf{Q})^G \to (B \otimes \mathbf{Q})^G \to (C \otimes \mathbf{Q})^G \to 0$$

также точная, так как $H^1(G, A \otimes \mathbf{Q}) = 0$ в силу того, что $A \otimes \mathbf{Q}$ — модуль с однозначным делением.

(iii) Мы видим теперь, что d_{1-2} и τ являются аддитивными функциями на классах рациональной эквивалентности. Кроме того, простые вычисления дают, что

$$d_{1-2}(\mathbf{Z}) = \tau(\mathbf{Z}) = -1,$$
$$d_{1-2}(\Lambda) = \tau(\Lambda) = 0,$$

где кольцо целых $\mathbf{Z}$ и групповое кольцо $\Lambda = \mathbf{Z}(G)$ рассматриваются как G-модули. Поэтому лемма 3.3 вытекает из следующего утверждения:

Любая аддитивная функция на классах рациональной эквивалентности конечно порожденных G-модулей A однозначно определяется своими значениями на модулях $\mathbf{Z}$ и Λ.

(iv) Докажем утверждение (iii). Из точной последовательности

$$0 \to I \to \Lambda \to \mathbf{Z} \to 0$$

мы получаем $f(I) = f(\Lambda) - f(\mathbf{Z})$, так что $f(I)$ однозначно определяется по $f(\mathbf{Z})$ и $f(\Lambda)$. Следовательно, осталось показать, что любой конечно порожденный G-модуль A рационально эквивалентен прямой сумме G-модулей, каждый из которых изоморфен $\mathbf{Z}$ или I. Иначе говоря,

$$A \otimes \mathbf{Q} = \sum_i A_i \otimes \mathbf{Q},$$

где $A_i = \mathbf{Z}$ или $A_i = I$. Вследствие того, что $A \otimes \mathbf{Q}$ как пространство представления G над $\mathbf{Q}$ есть прямая сумма пространств V_i *неприводимых* представлений, достаточно показать, что любое пространство $V \neq 0$ неприводимого представления G над $\mathbf{Q}$ изоморфно либо $\mathbf{Z} \otimes \mathbf{Q} = \mathbf{Q}$, либо $I \otimes \mathbf{Q}$.

Но каждое такое V изоморфно прямой сумме групповых колец $\mathbf{Q}(G) = \Lambda \otimes \mathbf{Q}$. Значит, мы должны определить прямое разложение для $\mathbf{Q}(G)$. Точная последовательность пополнения

$$0 \to I \otimes \mathbf{Q} \to \mathbf{Q}(G) \to \mathbf{Q} \to 0$$

расщепляется; соответствующее отображение $\mathbf{Q} \to \mathbf{Q}(G)$ задается правилом

$$x \to x \cdot e \qquad (x \in \mathbf{Q}),$$

где e — идемпотент

$$e = \frac{1}{p} \sum_{g \in G} g.$$

Следовательно, мы имеем прямое разложение

$$\mathbf{Q}(G) = (I \otimes \mathbf{Q}) \oplus \mathbf{Q} \cdot e,$$

и нам осталось показать, что $I \otimes \mathbf{Q}$ неприводимо, т. е. что $I \otimes \mathbf{Q}$, рассматриваемое как $\mathbf{Q}$-алгебра, является полем.

Пусть K — поле, порожденное над $\mathbf{Q}$ корнями p-й степени из единицы, и пусть χ — изоморфизм G на группу корней p-й степени из единицы в K. По линейности χ однозначно продолжается до гомоморфизма алгебры $\mathbf{Q}(G)$ в K, в ядре которого содержится e, так как сумма всех корней p-й степени из единицы в K равна 0. Следовательно, χ определяет гомоморфизм алгебры $\mathbf{Q}(G)/e = I \otimes \mathbf{Q}$ в K. Так как

$$\dim_{\mathbf{Q}} K = p - 1 = \dim_{\mathbf{Q}} I \otimes \mathbf{Q},$$

то изоморфизм между $I \otimes \mathbf{Q}$ и K установлен, что и требовалось сделать.

Лемма 3.4. *Пусть G — конечная p-группа и A — конечно порожденный G-модуль, который как абелева группа*

не имеет кручения. Тогда

$$d^{(p)}H^1(G, A) \leqslant \frac{\rho(A)-\rho(A^G)}{p-1}.$$

В частности, отсюда следует неравенство

$$d^{(p)}H^1(G, A) \leqslant \frac{\rho(A)}{p-1},$$

которое мы и хотим доказать.

Доказательство. Пусть сначала G имеет порядок p. Тогда по лемме 3.3

$$d^{(p)}H^1(G, A) \leqslant \frac{\rho(A)-p\cdot\rho(A^G)}{p-1} + d^{(p)}H^2(G, A).$$

Так как группа G циклическая, $H^2(G, A) = \hat{H}^0(G, A)$ является некоторой факторгруппой группы A^G и потому имеет p-ранг $\leqslant d^{(p)}A^G = \rho(A^G)$; последнее равенство следует из того, что A^G не имеет кручения.

Отсюда следует, что

$$d^{(p)}H^1(G, A) \leqslant \frac{\rho(A)-p\cdot\rho(A^b)}{p-1} + \rho(A^G);$$

это доказывает наше утверждение, если G имеет порядок p.

Теперь пусть G имеет порядок $\geqslant p^2$.

Обозначим через U собственный нормальный делитель. Точная последовательность инфляции и ограничения

$$1 \longrightarrow H^1(G/U, A^U) \longrightarrow H^1(G, A) \longrightarrow H^1(U, A)$$

показывает, что

$$d^{(p)}H^1(G, A) \leqslant d^{(p)}H^1(G/U, A^U) + d^{(p)}H^q(U, A).$$

Используя индукцию, мы можем считать, что

$$d^{(p)}H^1(G/U, A^U) \leqslant \frac{\rho(A^U)-\rho(A^G)}{p-1}$$

и

$$d^{(p)}H^1(U, A) \leqslant \frac{\rho(A)-\rho(A^U)}{p-1}.$$

Складывая эти неравенства, мы получаем наше утверждение.

ЛИТЕРАТУРА

Брумер (Brumer A.)
[1] Ramification and class towers of number fields, *Mich. math. J.*, **12** (1965), 129—131.

Брумер, Розен (Brumer A., Rosen M.)
[2] Class number and ramification in number fields, *Nagoya Math. J.*, **23** (1963), 97—101.

Голод Е. С., Шафаревич И. Р.
[3] О башне полей классов, *ИАН*, **28** (1964), 261—272.

Ивасава (Iwasava K.)
[4] A note on the group of units of an algebraic number field, *J. Math. pures appl.*, **35** (1956), 189—192.

Кох (Koch H.)
[5] Über den 2-Klassenkörperturm eines quadratischen Zahlkörpers, *J. reine angew. Math.*, **214/215** (1964), 201—206.

Серр (Serre J.-P.)
[6] Cohomologie Galoisienne, Lecture notes, Paris, 1963, reprinted by Springer, Berlin. (Русский перевод: Серр Ж.-П., Когомологии Галуа, «Мир», М., 1968.)

Фрёлих (Fröhlich A.)
[7] On fields of class two, *Proc. Lond. Math. Soc.* (3), **4** (1954), 235—256.
[8] On the absolute class group of abelian fields, *J. Lond. Math. Soc.*, **29** (1954), 211—217.
[9] A note on the class field tower, *Q. Jl. Math.* (2), **5** (1954), 141—144.
[10] On non-ramified extensions with prescribed Galois group, *Mathematica*, **9** (1962), 133—134.

Хассе (Hasse H.)
[11] Bericht über neuere Untersuchungen und Probleme der Theorie der algebraischen Zahlkörper, Teil 1, *Jber. dt. Math. Verein*, **35** (1926), 46.

Шафаревич И. Р.
[12] Поля алгебраических чисел, Int. Congr. Math. Stockholm, 1962, 163—176.
[13] Расширения с предписанными точками ветвления, *Publ. Math. IHES, Paris*, **18**, 1963, 71—95.

Шольц (Scholz A.)
[14] Zwei Bemerkungen zum Klassenkörperturmproblem, *J. reine angew. Math.*, **161** (1929), 201—207.

Шольц, Таусски (Scholz A., Taussky O.)
[15] Die Hauptideale der kubischen Klassenkörper imaginärquadratischer Zahlkörper usw., *J. reine angew. Math.*, **171** (1934), 19—41.

ГЛАВА X

Полупростые алгебраические группы

М. Кнезер [1])

ВВЕДЕНИЕ

В § 1 содержатся основные определения и формулировки фундаментальных результатов алгебраического характера, а § 2 и 3 посвящены некоторым арифметическим вопросам, связанным с алгебраическими группами, определенными над локальным или глобальным полем. Мы приводим очень мало доказательств, но даем ссылки на литературу.

За дальнейшей информацией о новых достижениях в теории алгебраических групп читатель отсылается к трудам следующих конференций:

Коллоквиум по теории алгебраических групп, Брюссель, 1962 (Colloque sur la théorie des groupes algébriques, Bruxelles, 1962);

Международный математический конгресс, Стокгольм, 1962 (International congress of mathematicians, Stockholm, 1962);

Летняя школа по алгебраическим группам и дискретным подгруппам, Баулдер, 1965 (Summer institute on algebraic groups and discontinuous subgroups, Boulder, 1965).

§ 1. АЛГЕБРАИЧЕСКАЯ ТЕОРИЯ

Основная литература — Шевалле [21]

1.1. Алгебраические группы над алгебраически замкнутым полем (Шевалле [21], Розенлихт [15])

Пусть k — алгебраически замкнутое поле. *Алгебраической группой*, определенной над k, называется алгебраическое многообразие G, определенное над k, вместе с отображениями $(x, y) \mapsto xy$ прямого произведения $G \times G$ в G и $x \mapsto x^{-1}$ G в G, являющимися морфизмами алгебраических многообразий и удовлетворяющими обычным групповым аксиомам. В дальнейшем всюду термины «группа», «подгруппа» и т. д. будут употребляться в смысле «алгебраическая группа», «алгебраическая подгруппа» (т. е. замкнутая подгруппа в топологии Зарисского) и т. д.

Алгебраическая группа G называется *линейной*, если она аффинна как алгебраическое многообразие. Например, $GL_n(k)$ является линейной группой, так как она может быть представлена множеством точек (x_{ij}, y) в k^{n^2+1}, удовлетворяющих уравнению $y \cdot \det(x_{ij}) = 1$. Значит, любая замкнутая подгруппа группы $GL_n(k)$ является линейной алгебраической группой, и легко показать, что, обратно, любая линейная алгебраическая группа получается таким способом. Аддитивная и мультипликативная группы поля k, рассматриваемые как одномерные алгебраические группы, будут обозначаться соответственно через G_a и G_m; обе они линейны ($G_m = GL_1$). *Тором* называется прямое произведение групп G_m. Линейная алгебраическая группа G называется *унипотентной*, если любое алгебраическое представление G состоит из унипотентных матриц (т. е. матриц, все собственные числа которых равны 1). Связная алгебраическая группа, являющаяся проективным алгебраическим многообразием, называется *абелевым многообразием*. Любое абелево многообразие коммутативно. Например, любая неособая проективная эллиптическая кривая допускает структуру абелева многообразия.

Если G — алгебраическая группа, то связная компонента G_0 ее единицы является нормальным делителем конечного индекса. Компонента G_0 обладает единственной максимальной связной линейной подгруппой G_1, которая является нормальным делителем, причем G_0/G_1 — абелево многообразие (теорема Шевалле; доказательство см. в [15]). Группа G_1 обладает единственным максимальным связным линейным разрешимым нормальным делителем G_2, называемым *радикалом* группы G_1, и G_1/G_2 — *полупростая группа*, т. е. связная линейная группа, радикал которой есть (1). Группа G_2 обладает единственной максимальной связной унипотентной подгруппой G_3, которая является нор-

[1]) Подготовлено для печати Макдональдом.

мальным делителем, причем G_2/G_3 — тор. Группа G_3 называется *унипотентным радикалом* группы G_2.

Таким образом, мы получили следующую цепочку подгрупп группы G:

$$
\begin{array}{ll}
 & G \\
 & \big| \quad \text{конечная группа} \\
\text{связная} & G_0 \\
 & \big| \quad \text{абелево многообразие} \\
\text{линейная} & G_1 \\
 & \big| \quad \text{полупростая группа} \\
\text{разрешимая} & G_2 \\
 & \big| \quad \text{тор} \\
 & G_3 \\
 & \big| \quad \text{унипотентная группа} \\
 & (1)
\end{array}
$$

Пример. Группа $G = GL_n$ линейная и связная, значит, $G = G_1$. Радикал G_2 совпадает с центром группы GL_n, состоящим из скалярных матриц ($\cong G_m$), группа G/G_2 — *простая*.

Мы сконцентрируем наше внимание главным образом на полупростых группах.

1.2. Полупростые группы над алгебраически замкнутым полем (Шевалле [21])

Пусть k — алгебраически замкнутое поле и G — полупростая группа, определенная над k. *Подгруппой Картана* группы G называется максимальный тор в G, а *подгруппой Бореля* группы G — максимальная связная разрешимая подгруппа. Например, если G — специальная линейная группа SL_n, то группа диагональных матриц, содержащихся в G, является подгруппой Картана (она, очевидно, тор, причем максимальный, так как она совпадает со своим централизатором), а группа верхних треугольных матриц в G является подгруппой Бореля.

Гомоморфизм $\varphi\colon G \to H$ называется *изогенией*, если G и H — связные группы одинаковой размерности, а размерность ядра равна 0 (т. е. ядро конечно). Отсюда следует, что φ — эпиморфизм, так как $\varphi(G)$ связно и имеет ту же размерность, что и H. (Например, $SL_n \to PGL_n$ — изогения, ядром является группа корней n-й степени из единицы.) Если характеристика поля k равна нулю, то ядро гомоморфизма φ содержится в центре группы G. В случае характеристики $p > 0$ возникают трудности, связанные с автоморфизмом Фробениуса. Например, пусть $G = H = SL_n$; обозначим через φ отображение $x = (x_{ij}) \mapsto (x_{ij}^p)$, которое является изогенией. Если x_{ij} принадлежат полю k и $\varphi(x) = 1$, то $x = 1$; отображение φ биективно, но не является изоморфизмом, так как отображение φ^{-1} не является алгебраическим. Если мы примем за x_{ij}, например, элементы k-алгебры $k[\varepsilon]$, где $\varepsilon^2 = 0$, то $x = 1 + \varepsilon y$ принадлежит ядру φ для любого $y \in G$, но не принадлежит центру. Чтобы исключить подобные случаи, мы определим *центральную изогению* как изогению, ядро которой содержится в центре, для точек с координатами в любой k-алгебре. Если $\varphi\colon G \to H$ — центральная изогения, то G называется *центральной накрывающей* группы H.

Среди центральных накрывающих группы G существует одна максимальная $\tilde{G}$, которая не имеет собственных центральных накрывающих, а среди всех групп, для которых G является центральной накрывающей, существует одна минимальная $\bar{G}$, которая не является центральной накрывающей для других групп.

$\tilde{G}$ называется *односвязной*, или *универсальной накрывающей*, а $\bar{G}$ — *присоединенной группой* группы G. Например, $\tilde{G} = SL_n$, $\bar{G} = PGL_n$.

Для того чтобы классифицировать полупростые группы, достаточно классифицировать односвязные группы и затем рассмотреть всевозможные центральные изогении.

Любая односвязная группа однозначно представляется в виде произведения *почти простых* групп (т. е. групп G с конечным центром C, таких, что G/C — простая группа). Группа SL_n является почти простой.

Классификация почти простых групп та же, что и для простых групп Ли:

A_n : SL_{n+1};
C_n : Sp_{2n};
B_n, D_n : изогенны ортогональным группам;
E_6, E_7, E_8, F_4, G_2: исключительные группы.

1.3. Полупростые группы над совершенным полем

(о группах над несовершенными полями см. [8])

Пусть k — совершенное поле и некоторый объект определен над k; это означает, что коэффициенты определяющих уравнений лежат в k. Назовем *k-тором* алгебраическую группу, определенную над k, которая над алгебраическим замыканием $\bar{k}$ поля k становится тором, т. е. изоморфна произведению групп $G_m = GL_1$; по определению тор *расщепляется* над k, если он изоморфен такому произведению над k.

Полупростая группа называется *расщепляемой* над k, если она обладает максимальным k-тором, расщепляемым над k; она называется *квазирасщепляемой* над k, если ее подгруппа Бореля определена над k. Как следует из терминологии, всякая расщепляемая группа квазирасщепляема. Например, группа SL_n расщепляема, а группа элементов с нормой 1 в алгебре кватернионов над k не является ни расщепляемой, ни квазирасщепляемой.

В разложении односвязной полупростой группы $\tilde{G}$ в произведение $G_1 \times \ldots \times G_r$ почти простых групп множители G_i и изоморфизм $\tilde{G} \cong \prod G_i$ определены над $\bar{k}$, но не обязательно над k. Группа Галуа $\Gamma = \mathrm{Gal}(\bar{k}/k)$ переставляет сомножители G_i, и произведение всех G_i, принадлежащих данному классу транзитивности, является группой, определенной над k. Значит, мы можем считать, что Γ переставляет G_i транзитивно. Стационарная подгруппа G_1 является подгруппой конечного индекса в Γ, причем ее поле неподвижных элементов l является конечным расширением поля k и G_1 определена над l. Про $\tilde{G}$ говорят, что она получена из G_1 *ограничением поля определения* с l до k: $\tilde{G} = R_{l/k}(G_1)$ (Вейль [3]). Этот метод позволяет

свести многие вопросы к случаю почти простых групп, поэтому в дальнейшем мы будем считать, что $\tilde{G}$ — почти простая группа.

В силу классификации почти простых групп над $\bar{k}$, указанной в § 2, естественно поставить вопрос: существует ли для каждого из типов A_n, . . ., G_2 группа G, определенная над k. В действительности для каждого типа существует группа G, определенная над k и расщепляющаяся над k, причем G определена однозначно с точностью до k-изоморфизма, если мы потребуем еще, чтобы она была односвязной или присоединенной (см. [20], [8]). Классификация различных k-форм группы G, т. е. групп G', изоморфных G над k, представляет собой задачу когомологий Галуа.

§ 2. КОГОМОЛОГИИ ГАЛУА

Основная литература — Серр [16].

2.1. Некоммутативные когомологии

Пусть G — группа и A — G-группа, т. е. группа (не обязательно коммутативная), на которой действует G. (Если G — проконечная группа, мы требуем, чтобы действие группы G было непрерывным относительно дискретной топологии на A.) Действие $s \in G$ на $a \in A$ мы обозначим через ${}^s a$.

Определим $H^0(G, A)$ как группу A^G, состоящую из G-инвариантных элементов из A. Затем мы определим *коцикл* как функцию $s \mapsto a_s$ на G со значениями в A, которая удовлетворяет условию

$$a_{st} = a_s \cdot {}^s a_t \qquad (s, t \in G).$$

Два коцикла a_s, b_s называются *эквивалентными*, если существует $c \in A$, такое, что

$$b_s = c^{-1} a_s {}^s c \qquad (s \in G).$$

Множество классов эквивалентности коциклов называется *множеством когомологий* $H^1(G, A)$. Оно является множеством с отмеченным элементом, а именно классом единичного коцикла. Как $H^0(G, A)$, так и $H^1(G, A)$ функториальны по A.

Если $1 \to A \to B \to C \to 1$ — точная последовательность G-групп и G-гомоморфизмов, то можно определить кограничное отображение $H^0(G, C) \to H^1(G, A)$, и последовательность (множеств с отмеченными элементами)

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, G) \to$$
$$\to H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

точна (точность понимается в обычном смысле, ядро определяется как прообраз отмеченного элемента). Если A содержится в центре B (следовательно, группа A абелева и определено $H^2(G, A)$), то можно определить кограничное отображение $H^1(G, C) \to H^2(G, A)$, расширяющее точную последовательность еще на один шаг.

Пусть K — совершенное поле и L — нормальное расширение поля K с группой Галуа G. Пусть, далее, A — алгебраическая группа, определенная над K, и A_L — группа точек из A, рациональных над L. Тогда A_L является G-группой, и мы вместо $H^i(G, A_L)$ будем писать $H^i(L/K, A)$. Если $\overline{K}$ — алгебраическое замыкание поля K, мы будем вместо $H^i(\overline{K}/K, A)$ писать $H^i(K, A)$.

2.2. K-формы

Пусть V, V' — алгебраические многообразия с некоторой дополнительной алгебраической структурой (например, алгебраические группы, или векторные пространства с квадратичной формой, или алгебры), причем все определено над совершенным полем K. Предположим, что $f\colon V \to V'$ есть изоморфизм рассматриваемой структуры, определенный над нормальным расширением L поля K. Если s — любой элемент группы Галуа G расширения L/K, то s преобразует f в изоморфизм ${}^s f\colon V \to V'$ и $a_s = f^{-1} \circ {}^s f$ есть коцикл группы G со значениями в Aut (V). Легко видеть, что такая K-форма V' многообразия V K-изоморфна другой K-форме V'' тогда и только тогда, когда соответствующие коциклы эквивалентны, и, следовательно, мы имеем вложение множества K-форм V (по модулю K-изоморфизма) в множество когомологий $H^1(L/K, \mathrm{Aut}\,(V))$. Во многих важных случаях (алгебраические группы, векторные пространства с конечным числом тензоров) это отображение является *изоморфизмом*. В таком случае задача классификации K-форм решается следующими средствами: (i) классификацией над алгебраическим замыканием $\overline{K}$ поля K и (ii) вычислением $H^1(K, \mathrm{Aut}\,(V))$.

Рассмотрим, например, классификацию K-форм односвязной полупростой линейной алгебраической группы. Как мы видели в § 1, достаточно рассмотреть почти простые группы, и тогда мы будем знать классификацию над $\overline{K}$. Пусть G — расщепляемая группа данного типа; тогда группа внутренних автоморфизмов группы G изоморфна присоединенной группе $\overline{G} \cong G/C$, где C — центр группы G, а факторгруппа $\mathrm{Aut}\,(G)/\overline{G}$ изоморфна группе $\mathrm{Sym}\,(G)$ симметрий диаграммы Дынкина группы G. Таким образом, мы получаем точную последовательность

$$1 \to \overline{G} \to \mathrm{Aut}\,G \to \mathrm{Sym}\,(G) \to 1$$

и производную когомологическую последовательность

$$H^0(K, \mathrm{Sym}\,(G)) \to H^1(K, \overline{G}) \to$$
$$\to H^1(K, \mathrm{Aut}\,(G)) \xrightarrow{\varphi} H^1(K, \mathrm{Sym}\,(S)).$$

Группа Галуа $\mathfrak{g}$ расширения $\overline{K}/K$ тривиально действует на $\mathrm{Sym}\,(G)$, так что коцикл группы $\mathfrak{g}$ со значениями в $\mathrm{Sym}\,(G)$ является гомоморфизмом $\mathfrak{g} \to \mathrm{Sym}\,(G)$ и, следовательно, $H^1(K, \mathrm{Sym}\,(G))$ — это фактор множества $\mathrm{Hom}\,(\mathfrak{g}, \mathrm{Sym}\,(G))$. На самом деле φ — эпиморфизм, и для каждого $\alpha \in H^1(K, \mathrm{Sym}\,(G))$ слой $\varphi^{-1}(\alpha)$ содержит квазирасщепляемую K-форму G_α группы G, которая определена однозначно с точностью до K-изоморфизма (Стейнберг [17]); элементы $\varphi^{-1}(\alpha)$ соответствуют K-формам G' группы G, таким, что существует изоморфизм $f\colon G_\alpha \to G'$, определенный над $\overline{K}$, для которого $f^{-1} \circ {}^s f$ является внутренним автоморфизмом G_α при всех $s \in \mathfrak{g}$. Из соображений скручивания (см. Серр [16], I, 5.5) $\varphi^{-1}(\alpha)$ является фактором множества когомологий $H^1(K, \overline{G}_\alpha)$.

2.3. Поля размерности $\leqslant 1$

Мы говорим, что поле K имеет размерность $\leqslant 1$, если группа Брауэра $\mathrm{Br}\,(L)$ равна нулю для любого алгебраического расширения L поля K. Примерами таких полей

являются конечные поля, а также максимальное неразветвленное расширение K_m полного относительно дискретного нормирования поля K.

Теорема 2.1 (Стейнберг [18]). *Если K — совершенное поле размерности $\leqslant 1$ и G — связная линейная алгебраическая группа, определенная над K, то $H^1(K, G) = 1$.*

В случае когда K — конечное поле, эта теорема была доказана ранее Ленгом.

Из теоремы Стейнберга и результатов, изложенных в § 2, следует, что $\varphi^{-1}(\alpha)$ содержит ровно один элемент, так что любая K-форма G квазирасщепляема и K-формы классифицируются группой $H^1(K, \mathrm{Sym}(G))$.

2.4. $\mathfrak{p}$-адические поля

Если K — $\mathfrak{p}$-адическое поле (т. е. пополнение глобального поля относительно дискретного нормирования), то уже не верно, что $H^1(K, G) = 1$ для любой связной группы G. Однако имеет место следующий результат.

Теорема 2.2 (Кнезер [12]). *Если K — $\mathfrak{p}$-адическое поле и G — односвязная полупростая линейная алгебраическая группа, определенная над K, то $H^1(K, G) = 1$.*

В доказательстве Кнезера производится редукция к случаю почти простых групп и отдельное рассмотрение каждого типа $A_n, \ldots, G_2$. Для классических групп эта теорема тесно связана с известными результатами о классификации квадратичных, эрмитовых и т. д. форм над $\mathfrak{p}$-адическими полями. Позднее Брюа и Титс [2] дали единообразное доказательство, основанное на результатах Ивахори и Мацумото [10].

Если G — универсальная накрывающая ортогональной группы, то теорема 2.2 по существу эквивалентна классификации квадратичных форм над $\mathfrak{p}$-адическим полем. Пусть q — невырожденная квадратичная форма от $n \geqslant 3$ переменных над $\mathfrak{p}$-адическим полем характеристики $\neq 2$, пусть O — ортогональная группа для q, и SO — специальная ортогональная группа для q. Все невырожденные квадратичные формы от n переменных эквивалентны над алгебраическим замыканием $\bar{K}$ поля K, так что классификация над K невырожденных квадратичных форм от n переменных эквивалентна вычислению $H^1(K, O)$.

Мы имеем точную последовательность

$$1 \to SO \to O \to \mu_2 \to 1,$$

где $\mu_2 = \{\pm 1\}$; далее, отображение $H^0(K, O) \to H^0(K, \mu_2)$, т. е. $O_K \to \mu_2$, сюръективно, значит, мы имеем точную последовательность (множеств)

$$1 \to H^1(K, SO) \xrightarrow{\alpha} H^1(K, O) \xrightarrow{d} H^1(K, \mu_2). \qquad (1)$$

Методом скручивания можно показать, что α инъективно. Для вычисления $H^1(K, \mu_2)$ мы используем точную последовательность

$$1 \to \mu_2 \to \bar{K}^* \xrightarrow{2} \bar{K}^* \to 1,$$

где $\bar{K}^* \xrightarrow{2} \bar{K}^*$ — отображение $x \to x^2$. Эта точная последовательность порождает когомологическую точную последовательность (групп)

$$K^* \xrightarrow{2} K^* \to H^1(K, \mu_2) \to 1 \to 1 \to$$
$$\to H^2(K, \mu_2) \to \mathrm{Br}(K) \xrightarrow{2} \mathrm{Br}(K)$$

(так как $H^1(K, \bar{K}^*) = 1$ по «теореме Гильберта 90»). Мы заключаем, что

$$H^1(K, \mu_2) \cong K^*/K^{*2}, \qquad H^2(K, \mu_2) \cong \mathrm{Br}(K)_2,$$

где $\mathrm{Br}(K)_2$ обозначает группу элементов порядка 2 в группе Брауэра $\mathrm{Br}(K)$. (Так как $\mathrm{Br}(K) = \mathbf{Q}/\mathbf{Z}$, мы имеем $\mathrm{Br}(K)_2 = \mu_2$.) Точная последовательность (1) теперь принимает вид

$$1 \to H^1(K, SO) \xrightarrow{\alpha} H^1(K, O) \xrightarrow{d} K^*/K^{*2}.$$

Здесь d по существу *дискриминант*; точнее, если $\xi \in H^1(K, O)$, то $d(\xi)$ есть дискриминант (по модулю квадратов) квадратичной формы, соответствующей ξ, деленный на дискриминант q (следовательно, d сюръективно). Квадратичные формы, определенные над K и имеющие тот же дискриминант, что и q, классифицируются группой $H^1(K, SO)$.

Универсальной накрывающей SO является спинорная группа $Spin$. Мы имеем точную последовательность

$$1 \to \mu_2 \to Spin \to SO \to 1$$

и, значит, когомологическую точную последовательность (множеств)

$$Spin_K \to SO_K \xrightarrow{\delta} K^*/K^{*2} \to H^1(K, Spin) \to$$
$$\to H^1(K, SO) \xrightarrow{\Delta} \mathrm{Br}(K)_2.$$

Здесь δ обозначает *спинорную норму*, а Δ тесно связано с инвариантом Витта квадратичной формы. Из теоремы 2.2 мы имеем, что $H^1(K, Spin) = 1$; поэтому

(i) спинорная норма δ: $SO_K \to K^*/K^{*2}$ является эпиморфизмом;

(ii) любая квадратичная форма с тем же дискриминантом d и тем же инвариантом Витта, что и q, K-изоморфна форме q. Обратно, из (i) и (ii) следует, что $H^1(K, Spin) = 1$.

2.5. Числовые поля

Пусть K — поле алгебраических чисел и G — линейная алгебраическая группа, определенная над K. Если v — нормирование поля K и K_v обозначает пополнение K относительно v, то мы получаем отображение ограничения

$$H^1(K, G) \to H^1(K_v, G),$$

соответствующее вложению $G_{\overline{K}} \to G_{\overline{K}_v}$, и, следовательно, отображение

$$\theta\colon H^1(K, G) \to \prod_v H^1(K_v, G).$$

Теорема Минковского — Хассе утверждает, что две квадратичные формы, определенные над K, изоморфны над K тогда и только тогда, когда они изоморфны над K_v для всех v (дискретных и архимедовых). В терминах когомологий Галуа эта теорема эквивалентна инъективности отображения

$$\theta\colon H^1(K, O) \to \prod_v H^1(K_v, O),$$

где O обозначает ортогональную группу квадратичной формы.

Отображение θ, определенное посредством (1), не всегда инъективно, даже если G — связная полупростая группа (Серр [16]). Однако, если группа G односвязна, следующая теорема, по-видимому, всегда справедлива.

Теорема 2.3. *Пусть K — поле алгебраических чисел и G — односвязная полупростая линейная алгебраическая группа, определенная над K. Тогда отображение*

$$\theta\colon H^1(K, G) \to \prod H^1(K_v, G)$$

взаимно однозначно.

Действительно, $H^1(K_v, G)$ тривиальна для всех дискретных v (теорема 2.2), так что теорема 2.3 эквивалентна следующей:

Теорема 2.3′. *Отображение*

$$H^1(K, G) \to \prod_{v \in \infty} H^1(K_v, G),$$

где ∞ обозначает множество всех архимедовых нормирований поля K, взаимно однозначно.

Доказательство теоремы 2.3 получается сведением к случаю почти простых групп и дальнейшим рассмотрением каждого типа A_n, . . ., G_2 в отдельности. Для классических групп это связано с известными результатами о квадратичных, эрмитовых и т. д. формах. Об исключительных группах, кроме E_8, см. Хардер [19]. Случай E_8 еще не исследован.

§ 3. ЧИСЛА ТАМАГАВА

Основная литература — Вейль [3].

ВВЕДЕНИЕ

Пусть K — поле алгебраических чисел и A — кольцо аделей поля K. Обозначим через v нормирование (дискретное или архимедово) поля K, через K_v — пополнение K по v и через $\mathfrak{o}_v$ — кольцо целых элементов в K_v, если v дискретно.

Пусть G — связная линейная алгебраическая группа, определенная над K. Группа G изоморфна подгруппе полной

линейной группы GL_n, и, следовательно, мы можем рассматривать G как замкнутое подмножество m-мерного аффинного пространства ($m = n^2 + 1$, см. п. 1.1). *Группой аделей* G_A группы G называется множество точек в A^m, удовлетворяющих уравнениям группы G.

Мы введем на G_A топологию, индуцированную топологией прямого произведения на A^m; тогда G_A будет локально компактной топологической группой. G_A можно также определить как ограниченное прямое произведение групп G_{K_v} относительно их компактных подгрупп $G_{\mathfrak{o}_v}$, где G_{K_v} (соответственно $G_{\mathfrak{o}_v}$) обозначает множество точек из G с координатами в K_v (соответственно $\mathfrak{o}_v$). На первый взгляд G_A зависит от вложения G в аффинное пространство, но легко показать, что, изменяя вложение, мы изменяем $G_{\mathfrak{o}_v}$ только для конечного числа нормирований v, и, значит, G_A остается неизменной.

Пример. Если $G = G_a$, то $G_A = A$. Если $G = G_m$, то G_A является группой иделей поля K.

Так как K является дискретной подгруппой в A, то из этого следует, что G_K — дискретная подгруппа в G_A. Так как G_A локально компактна, то на G_A существует левоинвариантная мера Хаара, единственная с точностью до постоянного множителя. Формула произведения показывает, что умножение справа на элемент из G_K не меняет меры на G_A, и, следовательно, мы получаем индуцированную левоинвариантную меру на однородном пространстве G_A/G_K.

Существует канонически выбранная мера Хаара на G_A, называемая *мерой Тамагава* τ (§ 1). После этого возникает задача о вычислении *числа Тамагава* $\tau(G) = \tau(G_A/G_K)$ (§ 2). Для случая ортогональной группы это эквивалентно классическим арифметическим результатам Минковского и Зигеля о квадратичных формах.

3.1. Мера Тамагава

Пусть V — алгебраическое многообразие размерности n, определенное над K. Пусть x^0 — неособая точка на V, пусть $x_1, \ldots, x_n$ — локальные координаты на V в x^0 (не обязательно равные 0 в x^0). *Дифференциальная n-форма*

на V определяется в окрестности x^0 выражением

$$\omega = f(x)\, dx_1 \ldots dx_n,$$

где f обозначает рациональную функцию на V, определенную в точке x^0. Форма ω называется определенной над K, если f и координатные функции x_i определены над K. При замене координат ω изменяется по обычному правилу. Если $\varphi\colon W \to V$ — морфизм алгебраических[1] многообразий, то ω поднимается до дифференциальной формы $\varphi^*(\omega)$ на W.

Предположим теперь, что V является связной линейной алгебраической группой G. Левый сдвиг $\lambda_a\colon x \mapsto ax$ ($a \in G$) является морфизмом $V \to V$ и, следовательно, преобразует дифференциальную форму ω на G в дифференциальную форму $\lambda_a^*(\omega)$. Таким образом, мы можем определить левоинвариантную дифференциальную форму на G, и основное утверждение заключается в том, что существует ненулевая левоинвариантная дифференциальная n-форма ω на G, определенная над K, и ω определена однозначно с точностью до постоянного множителя $c \in K^*$.

Примеры.

$$G = G_a, \quad \omega = dx, \quad G = G_m, \quad \omega = dx/x;$$

$$G = GL_n, \quad \omega = \left(\prod dx_{ij}\right)/(\det x_{ij})^n.$$

Мы используем ω для построения меры ω_v на локальных группах G_{K_v}. Для этой цели нам необходимо зафиксировать меру Хаара μ_v на аддитивной группе K_v^+. Если $K = \mathbf{Q}$, то мы фиксируем μ_p (p — простое число) соотношением $\mu_p(\mathbf{Z}_p) = 1$, а за μ_∞ мы примем обычную меру Лебега на $\mathbf{R}$. Если K — произвольное числовое поле, то существуют различные способы нормализации; мы потребуем только, чтобы выполнялись условия:

(i) $\mu_v(\mathfrak{o}_v) = 1$ для почти всех дискретных v;

(ii) если $\mu = \prod \mu_v$ — мера на A, то $\mu(A_K/K) = 1$.

(Одну из таких нормализаций можно получить, если принять $\mu_v(\mathfrak{o}_v) = 1$ для всех дискретных v, а μ_v для архимедовых нормирований выбрать пропорциональными лебеговой мере с коэффициентами c_v, где c_v — положитель-

ные вещественные числа, такие, что

$$\prod_{v\in\infty} c_v = 2^{r_2} |\, d_K \,|^{-1/2},$$

причем ∞ обозначает множество бесконечных нормирований поля K, через r_2 обозначено число комплексных нормирований и через d_K — дискриминант поля K.)

Для определения ω_v мы поступим следующим образом. Рациональную функцию f можно записать как формальный степенной ряд от $t_i = x_i - x_i^0$ с коэффициентами из K. Если x_i^0 принадлежат полю K_v, то f является степенным рядом от x_i с коэффициентами из K_v, сходящимися в некоторой окрестности начала координат в K_v^n. Значит, существует окрестность U точки x^0 в G_{K_v}, такая, что $\varphi\colon x \longmapsto (t_1, \ldots, t_n)$ является гомеоморфизмом U на окрестность U' начала координат в K_v^n, причем вышеупомянутый степенной ряд сходится в U'. В U' мы имеем положительную меру $|f(t)|_v\, dt_1 \ldots dt_n$ (где $dt_1 \ldots dt_n$ является произведением мер $\mu_v \times \ldots \times \mu_v$ на K_v^n); поднимая ее на U с помощью φ, мы получаем положительную меру ω_v на U. В явной форме, если g — непрерывная вещественнозначная функция на G_{K_v} с компактным носителем, то

$$\int_U g\omega_v = \int_{U'} g(\varphi^{-1}(t))\, |f(t)|_v\, dt_1 \ldots dt_n.$$

Мера ω_v на самом деле не зависит от выбора локальных координат x_i. В архимедовом случае это следует из формулы Якоби замены переменных в кратном интеграле, а в дискретном случае — из ее $\mathfrak{p}$-адического аналога.

Если произведение

$$\prod_{v\notin\infty} \omega_v(G_{\mathfrak{o}_v})$$

абсолютно сходится, мы определим *меру Тамагава* формулой

$$\tau = \prod_v \omega_v.$$

В явном виде если S — конечное множество нормирований, такое, что $\infty \subset S$, и если U_v является открытым множеством в G_{K_v} с компактным замыканием для любого $v \in S$, то τ — единственная мера Хаара на G_A, для которой

$$\tau\Big(\prod_{v\in S} U_v \times \prod_{v\notin S} G_{\mathfrak{o}_v}\Big) = \prod_{v\in S} \omega_v(U_v) \times \prod_{v\notin S} \omega_v(G_{\mathfrak{a}_v}).$$

Если произведение

$$\prod_{v\notin\infty} \omega_v(G_{\mathfrak{o}_v})$$

не сходится абсолютно, то мы должны ввести множители, обеспечивающие сходимость. Система (λ_v) строго положительных вещественных чисел, соответствующих нормированиям v поля K, называется множеством *множителей сходимости*, если произведение

$$\prod_{v\notin\infty} \lambda_v^{-1}\omega_v(G_{\mathfrak{o}_v})$$

абсолютно сходится. Мера Тамагава τ (относительно λ_v) определяется формулой

$$\tau = \prod_v \lambda_v^{-1}\omega_v.$$

В любом случае τ не зависит от выбора формы ω, ибо если мы заменим ω на $c\omega$ $(c \in K^*)$, то $(c\omega)_v = |c|_v\omega_v$ и $\prod_v |c|_v = 1$ в силу формулы произведения.

Пусть $k(v)$ обозначает поле вычетов относительно v (v дискретно), и пусть $G^{(v)}$ обозначает алгебраическую группу, определенную над конечным полем $k(v)$, полученную редукцией уравнений G по модулю максимального идеала $\mathfrak{p}_v$ кольца $\mathfrak{o}_v$. Тогда можно показать, обобщая лемму Гензеля, что для почти всех v имеет место равенство

$$\omega_v(G_{\mathfrak{o}_v}) = (Nv)^{-n}\,\mathrm{Card}\,[G_{k(v)}^{(v)}], \tag{1}$$

где Nv обозначает число элементов в $k(v)$, а $G_{k(v)}^{(v)}$ — группа точек из $G^{(v)}$, рациональных над $k(v)$.

Примеры. Если $G = G_a$, то

$$\omega_v(G_{\mathfrak{o}_v}) = 1;$$

если $G = G_m$, то

$$\omega_v(G_{\mathfrak{o}_v}) = 1 - \frac{1}{Nv};$$

если $G = GL_m$, то

$$\omega_v(G_{\mathfrak{o}_v}) = \left(1 - \frac{1}{Nv}\right) \dots \left(1 - \frac{1}{(Nv)^m}\right);$$

если $G = SL_m$, то

$$\omega_v(G_{\mathfrak{o}_v}) = \left(1 - \frac{1}{(Nv)^2}\right) \dots \left(1 - \frac{1}{(Nv)^m}\right).$$

Так как

$$\prod_v \left(1 - \frac{1}{(Nv)^s}\right) = \zeta_K(s)^{-1}$$

сходится при $\operatorname{Re} s > 1$, но расходится при $s = 1$, то отсюда следует, что произведение $\prod_v \omega_v(G_{\mathfrak{o}_v})$ сходится для $G = SL_m$, но не сходится для $G = GL_m$. В последнем случае мы можем взять в качестве множителей сходимости числа

$$\lambda_v = 1 - \frac{1}{Nv}.$$

Предложение 3.1. *Если G — полупростая группа, то произведение $\prod_v \omega_v(G_{\mathfrak{o}_v})$ абсолютно сходится (и потому множители сходимости не нужны).*

В общих словах доказательство проводится следующим образом (детали см. Оно [14]). Учитывая последовательность (1) из § 2, мы должны доказать, что произведение

$$\prod_v \{(Nv)^{-n} [G^{(v)}_{k(v)}]\} \tag{2}$$

абсолютно сходится. Используя теорему (принадлежащую Ленгу) о том, что изогенные группы над конечным полем имеют одинаковое число рациональных точек, мы можем свести задачу к случаю, когда G — простая группа над алгебраическим замыканием $\bar{K}$ поля K, т. е. G не имеет нетривиальных алгебраических нормальных делителей, определенных над $\bar{K}$. Для такой группы порядок $G^{(v)}_{k(v)}$ может быть явно определен; он имеет вид

$$(Nv)^n \{1 + O((Nv)^{-2})\}.$$

Сходимость в (2) следует теперь из сходимости ряда для дзета функции $\zeta_K(s)$ при $\operatorname{Re} s > 1$.

3.2. Число Тамагава

Число Тамагава $\tau(G)$ по определению равно $\tau(G_A/G_K)$.

Теорема 3.1 (Борель, Харишд-Чандра [11]). *Если G — полупростая группа, то число $\tau(G)$ конечно.*

Другое доказательство этой теоремы имеется в работе Годмана [7].

Теорема 3.2 (Оно [14]). *Пусть G — полупростая группа, $\tilde{G}$ — ее универсальная (т. е. односвязная) накрывающая, C — ядро (конечное) накрывающего отображения $\tilde{G} \to G$ и $\hat{C}$ — группа характеров* $\operatorname{Hom}(C, G_m)$. *Тогда*

$$\frac{\tau(G)}{\tau(\tilde{G})} = \frac{h^0(\hat{C})}{i^1(\hat{C})},$$

где $h^0(\hat{C}) = \operatorname{Card} H^0(K, \hat{C})$ и $i^1(\hat{C})$ обозначает порядок ядра отображения $H^1(K, \hat{C}) \to \prod_v H^1(K_v, \hat{C})$.

Следовательно, достаточно вычислить одно число Тамагава для каждого класса изогенных групп, например $\tau(\tilde{G})$. В этом направлении имеется принадлежащая А. Вейлю

Гипотеза. $\tau(\tilde{G}) = 1$.

Эта гипотеза доказана для многих классических групп (Вейль [3], [5], [6]), для всех групп типов B_n и C_n, для некоторых типов A_n и D_n и (Марс [13]; Вейль [3]) для некоторых исключительных групп. Ленглендс привел единое доказательство для всех расщепляемых полупростых групп (Брюа, Титс [2]).

Пример: $G = SO_n$ $(n \geqslant 3)$. Здесь C имеет порядок 2, и можно показать, что $h^0(\hat{C})/i^1(\hat{C}) = 2$. Поэтому в данном случае $\tau(\tilde{G}) = 1$ эквивалентно тому, что $\tau(G) = 2$. А как мы увидим далее (п. 3), $\tau(G) = 2$ эквивалентно теореме Минковского — Зигеля о квадратичных формах.

3.3. Теорема Минковского — Зигеля

Пусть K — поле алгебраических чисел, V — n-мерное векторное пространство над K $(n \geqslant 3)$, q — невырожденная квадратичная форма на V, определенная над K, $G =$

$= SO(q)$ — группа всех автоморфизмов векторного пространства V с определителем 1, сохраняющих q. Мы рассмотрим действие G на V *справа*. Выберем фиксированный базис пространства V и отождествим V с K^n; тогда элементы G представляются матрицами порядка $n \times n$.

Решеткой M в V называется конечно порожденный $\mathfrak{o}$-подмодуль пространства V ранга n, где $\mathfrak{o}$ — кольцо целых элементов в K. В частности, $L = \mathfrak{o}^n$ — решетка, называемая *стандартной* решеткой (относительно выбранного базиса V). Две решетки M, M' называются *изоморфными*, если $M' = Mx$ для некоторого $x \in G_K$. Для каждого конечного нормирования v положим $M_v = \mathfrak{o}_v \otimes M$; это решетка в K_v^n. Можно показать, что M однозначно определена решетками M_v (а именно, $M = \bigcap_v (M_v \cap V)$), что $M_v = \mathfrak{o}_v^n$ для почти всех v и что, обратно, если M_v для каждого конечного v — решетка в K_v^n, такая, что $M_v = \mathfrak{o}_v^n$ для почти всех v, то существует единственная решетка M в K^n, у которой локальные компоненты совпадают с M_v.

Группа аделей G_A действует на множестве решеток в K^n следующим образом: если M — решетка и $x \in G_A$, то $(Mx)_v = M_v x_v$ (заметим, что так как $M_v = \mathfrak{o}_v^n$ для почти всех v и $x_v \in G_{\mathfrak{o}_v}$ для почти всех v, то $(Mx)_v = \mathfrak{o}_v^n$ для почти всех v). Орбита решетки M относительно G_A называется *родом* решетки M, который, следовательно, состоит из решеток в V, локально изоморфных M для всех конечных нормирований. *Класс* решетки M — это орбита M относительно G_K, т. е. множество решеток, глобально изоморфных M.

Стационарной подгруппой стандартной решетки L в G_A является открытая подгруппа

$$G_{A_\infty} = \Big(\prod_{v \notin \infty} G_{\mathfrak{o}_v}\Big) \times \Big(\prod_{v \in \infty} G_{K_v}\Big) = G_{\mathfrak{o}} \times G_\infty,$$

где ∞ обозначает множество архимедовых нормирований поля K. Значит, решетки рода L взаимно однозначно соответствуют классам смежности $G_{A_\infty} x$ в G_A, а классы рода — двойным классам смежности $G_{A_\infty} x G_K$ в G_A. Для любой полупростой группы число двойных классов $G_{A_\infty} x G_K$ в G_A конечно (Борель, Хариш-Чандра [1]). В нашем частном случае $G = SO(q)$ это—хорошо известное свойство конечности числа классов рода. Обозначим через h это число.

Мы имеем

$$\tau(G) = \tau(G_A/G_K) = \sum_{i=1}^{h} \tau(G_{A_\infty} x_i G_K/G_K) = \sum_{i=1}^{h} \tau(x_i^{-1} G_{A_\infty} x_i G_K/G_K), \qquad (3)$$

так как τ — левоинвариантная мера. Группа $x_i^{-1} G_{A_\infty} x_i$ является стационарной подгруппой Lx_i в G_A. Значит, нам нужно рассмотреть только один член этой суммы, скажем $\tau(G_{A_\infty} G_K/G_K)$. Мы имеем $G_{A_\infty} G_K/G_K \simeq G_{A_\infty}/G_{\mathfrak{o}}$ (так как $G_{A_\infty} \cap G_K = G_{\mathfrak{o}}$). Следовательно,

$$\tau(G_{A_\infty} G_K/G_K) = \tau(G_{A_\infty}/G_{\mathfrak{o}}) = \tau(F),$$

где F обозначает фундаментальную область для $G_{\mathfrak{o}}$ в G_{A_∞}, т. е. борелевское множество в G_{A_∞}, содержащее ровно по одному элементу из каждого класса смежности $xG_{\mathfrak{o}}$. Проекция $G_{A_\infty} = G_{\mathfrak{o}} \times G_\infty \to G_\infty$, ограниченная на $G_{\mathfrak{o}}$, вкладывает $G_{\mathfrak{o}}$ в G_∞, и мы можем принять за F множество вида $G_{\mathfrak{o}} \times F_\infty$, где F_∞ — фундаментальная область для $G_{\mathfrak{o}}$ в G_∞. Значит, имеет место равенство

$$\tau(G_{A_\infty} G_K/G_K) = \tau(G_{\mathfrak{o}} \times F_\infty) = \prod_{v \notin \infty} \omega_v(G_{\mathfrak{o}_v}) \times \omega_\infty(G_\infty/G_{\mathfrak{o}}),$$

где

$$\omega_\infty = \prod_{v \in \infty} \omega_v.$$

Если мы заменим L на Lx_i, то $G_{\mathfrak{o}_v}$ заменится на $x_{i,v}^{-1} G_{\mathfrak{o}_v} x_{i,v}$ и, следовательно, член $\omega_v(G_{\mathfrak{o}_v})$ не изменится (так как для полупростой группы ω как левоинвариантна, так и правоинвариантна), а $G_{\mathfrak{o}} = G_K \cap G_{A_\infty}$ заменится на

$$G_{\mathfrak{o}}(x_i) = G_K \cap x_i^{-1} G_{A_\infty} x_i.$$

Значит,

$$\tau(x_i^{-1} G_{A_\infty} x_i G_K/G_K) = \prod_{v \notin \infty} \omega_v(G_{\mathfrak{o}_v}) \times \omega_\infty(G_\infty/G_{\mathfrak{o}}(x_i)), \qquad (4)$$

и, следовательно, из (3) и (4) вытекает, что

$$2=\tau(G)=\prod_{v\notin\infty}\omega_v(G_{\mathfrak{o}_v})\times\sum_{i=1}^{h}\omega_\infty(G_\infty/G_{\mathfrak{o}}(x_i)),$$

или

$$\sum_{i=1}^{h}\omega_\infty(G_\infty/G_{\mathfrak{o}}(x_i))=2\prod_{v\notin\infty}\omega_v(G_{\mathfrak{o}_v})^{-1}. \tag{5}$$

Предположим теперь, что форма q *вполне определенная*, т. е. что каждое архимедово нормирование v вещественно, и форма q — положительно определенная для каждого архимедова пополнения K_v. Тогда группа

$$G_\infty=\prod_{v\in\infty}G_{k_v}$$

является произведением вещественных ортогональных групп и, следовательно, компактна, а $G_{\mathfrak{o}}(x_i)$ — *группа единиц* $E(Lx_i)$ решетки Lx_i, т. е. группа всех целочисленных матриц, отображающих Lx_i на себя, причем она конечна. (Если S_i — матрица формы q в базисе Lx_i, то $E(Lx_i)$ — группа всех целочисленных матриц X, таких, что $X'S_iX=S_i$; так как S_i положительно определена, то $E(Lx_i)$, очевидно, конечна.) Значит, теперь равенство (5) можно переписать в виде

$$\sum_{i=1}^{h}\operatorname{Card}\frac{1}{E(Lx_i)}=\frac{2}{\omega_\infty(G_\infty)}\prod_{v\notin\infty}\frac{1}{\omega_v(G_{\mathfrak{o}_v})}=\frac{2}{\tau(G_{A_\infty})}. \tag{6}$$

При $K=\mathbf{Q}$ это эквивалентно формуле Минковского для веса рода определенных квадратичных форм.

Точно так же мы можем получить теорему Зигеля [9] о числе представлений одной квадратичной формы (от n переменных) другой (от m переменных), рассматривая m-мерное векторное пространство V вместе с невырожденной квадратичной формой q, его n-мерное подпространство W и число Тамагава группы G всех q-ортогональных преобразований, тождественных на W. Подробности см. в [11] и [4].

ЛИТЕРАТУРА

Борель, Харишд-Чандра (Borel A., Harish-Chandra)

[1] Arithmetic subgroups of algebraic groups, *Ann. Math.*, **75** (1962), 485—535. (Русский перевод: *Математика*, **8** : 2 (1964), 3—17.)

Брюа, Титс (Bruhat F., Tits J.)

[2] Summer institute on algebraic groups and discontinuous subgroups, A.M.S., Boulder, 1965.

Вейль (Weil A.)

[3] Adeles and algebraic groups, Lecture notes, Princeton, 1961. (Русский перевод: *Математика*, **8** : 4 (1964), 3—74.)

[4] Sur la théorie des formes quadratiques. Colloque sur la théorie des Groupes Algébriques, Bruxelles, 1962, 9—22.

[5] Sur certains groups d'opérateurs unitaires, *Acta Math. Stockh.*, **111** (1964), 143—211.

[6] Sur la formula de Siegel dans la théorie des groupes classiques, *Acta Math. Stockh.*, **113** (1965), 1—87.

Годман (Godement R.)

[7] Domaines fondamentaux des groupes arithmetiques, Seminaire Bourbaki, № 257, 1962—1963.

Демазур, Гротендик (Demazure M., Grothendieck A.)

[8] Schémas en groupes, Séminaire de Géometrie Algebrique I.H.E.S., 1963—1964.

Зигель (Siegel C. L.)

[9] Über die analytische Theorie der quadratischen Formen, *Ann. Math.*, **36** (1935), 527—606; **37** (1936), 230—263; **38** (1937), 212—291.

Ивахори, Мацумото (Iwahori N., Matsumoto H.)

[10] On some Bruhat decomposition and the structure of the Hecke ring of p-adic Chevalley groups, Publ. Math., I.H.E.S., № 25, 1965.

Кнезер (Kneser M.)

[11] Darstellungsmaße indefiniter quadratischer Formen, *Math. Z.*, **77** (1961), 188—194.

[12] Galois-Kohomologie halbeinfacher algebraischer Gruppen über p-adischen Körpern, *Math. Z.*, **88** (1965), 40—47; **89** (1965), 250—272.

Марс (Mars J.M.G.)

[13] Les nombres de Tamagawa de certains groups exceptionnels, в печати.

Оно (Опо Т.).
[14] On the relative theory of Tamagawa numbers, *Ann. Math.*, **82** (1965), 88—111.

Розенлихт (Rosenlicht M.)
[15] Some basic theorems on algebraic groups, *Am. J. Math.*, **78** (1956), 401—443.

Серр (Serre J.-P.)
[16] Cohomologie Galoisienne, Lecture notes, Collège de France, 1962—1963, 2nd edition, Springer-Verlag. (Русский перевод: Серр Ж.-П., Когомологии Галуа, «Мир», М., 1968.)

Стейнберг (Steinberg R.)
[17] Variations on a theme of Chevalley, *Pacif. J. Math.*, **9** (1959), 875—891.
[18] Regular elements of semi-simple algebraic groups, Publ. Math., I.H.E.S., № 25, 1965.

Хардер (Harder G.)
[19] Über die Galoiskohomologie halbeinfacher Matrizengruppen, *Math. Z.*, I, **90** (1965), 404—428, II, **92** (1966), 396—415.

Шевалле (Chevalley C.)
[20] Sur certains groupes simples, *Tohoku Math. J.*, **7** (1955), 14—66. (Русский перевод: *Математика*, **2** : 1 (1958), 3—53.)
[21] Classification des groupes de Lie algébriques, Séminaire E.N.S., 1956—1958.

ГЛАВА XI

История теории полей классов

Г. Хассе [1])

1. Понятие *поля классов* обычно связывается с именем Гильберта. На самом деле это понятие неявно присутствовало уже у Кронекера, а термин был введен Вебером до появления фундаментальной работы Гильберта.

Кронекер [23] в своем большом трактате «*Основания арифметической теории алгебраических чисел*», 1882, подробно обсуждает «zu assoziierenden Gattungen» («роды ассоциаций»). Под этим он подразумевает, если пользоваться современной терминологией, алгебраическое расширение K заданного поля алгебраических чисел k, такое, что все дивизоры [2]) из k становятся главными дивизорами в K. В этих исследованиях он обнаружил, что если k — мнимое квадратичное поле, то такое расширение K порождается «сингулярными модулями». Этим понятием Кронекер предвосхитил теорему о главных дивизорах теории полей классов, установленную и в частных случаях доказанную Гильбертом.

Вебер в работах [6] и [7] (1891, 1897, 1898, 1908), однако, определил понятие поля классов не на этой основе, которая, как мы знаем сегодня, не удобна для построения теории. То, что он постулировал, составляет часть *закона разложения*. Но в то время как Гильберт в своих более поздних

[1]) Подготовлено для печати Лю на основе рукописи автора.
[2]) Я всюду использую термин «дивизор» вместо классического термина «идеал», потому что теория нормирований, развившаяся из понятия дивизора Кронекера — Гензеля, сейчас широко распространена как более подходящий фундамент алгебраической теории чисел, чем теория идеалов Дедекинда.

определениях рассматривал только случай абсолютного поля классов, Вебер дал определение в полной общности:

Пусть k — поле алгебраических чисел и A/H — относительная группа классов дивизоров в k. Алгебраическое расширение K поля k называется полем классов для группы A/H, если в поле K вполне распадаются те и только те простые дивизоры из k первой степени, которые принадлежат главному классу H.

Чтобы определить веберовское понятие относительной группы классов дивизоров A/H поля k, рассмотрим целые модули дивизоров m поля k, т. е. формальные конечные произведения, составленные из конечного числа точек (простых дивизоров) поля k с целыми положительными показателями и вещественных бесконечных простых точек поля k с показателями единица. Назовем число (дивизор) поля k взаимно простым с модулем m, если оно (он) взаимно просто с каждым из простых дивизоров, входящих в m, и будем понимать сравнимость по модолю m как сравнимость по модулю степеней простых дивизоров, входящих в m, и равенство знака для всех вещественных простых точек, входящих в m. Рассмотрим далее факторгруппу A_m/H_m, где A_m — группа всех дивизоров поля k, взаимно простых с модулем m (для заданного целого модуля дивизоров m), и H_m — ее подгруппа, состоящая из всех чисел a, сравнимых с единицей по модулю m в поле k (рассматриваемых как главные дивизоры поля k). Назовем две факторгруппы A_{m_1}/H_{m_1} и A_{m_2}/H_{m_2} «равными» между собой, если для наименьшего общего кратного $m = [m_1, m_2]$ (и, значит, для любого общего кратного) модулей m_1 и m_2 имеет место равенство $H_{m_1} \cap A_m = H_{m_2} \cap A_m$, которое влечет за собой изоморфизм $A_{m_1}/H_{m_1} \cong A_{m_2}/H_{m_2}$. Любое множество факторгрупп A_{m_1}/H_{m_1}, A_{m_2}/H_{m_2}, . . ., которые «равны» между собой, определяют относительную группу классов дивизоров A/H в смысле Вебера. Индивидуальные факторгруппы A_{m_1}/H_{m_1}, A_{m_2}/H_{m_2}, . . . называются *интерпретациями* (Erklärungen) по $\bmod m_1$, $\bmod m_2$, . . . группы A/H. Наименьший возможный *интерпретационный модуль* f (Erklärungsmodul), который оказывается наибольшим общим делителем всех возможных модулей m_1, m_2, . . ., называется ведущим модулем (Führer) группы A/H. Иногда

индивидуальные *интерпретации* также называют относительными группами классов дивизоров.

Кроме доказательства ряда теорем о полях классов, которые мы вскоре приведем, Вебер в рассматривавшихся им случаях установил основную *теорему изоморфизма*:

Группа Галуа $\mathfrak{G}(K/k)$ *изоморфна группе классов A/H и, значит, обязательно абелева.*

Уже Кронекер ([21] (1853), [22] (1877)) знал, что поля деления круга являются полями классов в указанном выше смысле. Он сформулировал знаменитую *теорему полноты*:

Всякое абелево расширение поля рациональных чисел является полем деления круга и, следовательно, полем классов.

Эта теорема была впервые полностью доказана Вебером [4] (1886, 1887) и позже, более просто, Гильбертом [12] (1896), [13] (1897); дальнейшие доказательства были даны Вебером [8] (1909), Шпейзером [53] (1919) и Делоне [20] (1923) [1]).

В дальнейшем Кронекер [24] (1883—1890) в своих исследованиях по модулярным и эллиптическим функциям с «сингулярными модулями» установил, что их преобразования и уравнения деления порождают относительно абелевы расширения K над мнимыми квадратичными полями k. Его «заветной мечтой юности» («liebster Jugendtraum») [25] (1880) было доказать также и в этом случае *теорему полноты*, а именно *любое абелево расширение K мнимого квадратичного поля k* получается из таких преобразований и уравнений деления. Она была доказана позже впервые в частном случае Вебером [7] (1908) и Фютером [38] (1914), затем полностью Такаги [28] (1920) и вновь Фютером (совместно с Гутом) [39] (1927).

Вебер [6] (1897, 1898) пришел к понятию поля классов из рассмотрения этих примеров. Используя аналитические методы Дирихле (L-ряды), он вывел из своего определения поля классов *первое* [2]) *основное неравенство* теории полей классов:

$$[A:H] = h \leqslant n = [K:k],$$

[1]) См. также Шафаревич И. Р., Новое доказательство теоремы Кронекера — Вебера, Тр. Матем. ин-та им. В. А. Стеклова, 38 (1951), 382—387.— *Прим. ред.*

[2]) В современной терминологии — второе.

а затем *теорему единственности*:

$$H = H' \Leftrightarrow K = K',$$

теорему вложения:

$$H \supseteq H' \Leftrightarrow K \subseteq K'$$

и следующую предпосылку к теореме изоморфизма:

K нормально над полем k.

Из введения к работе [6] (1897, 1898) Вебера можно с уверенностью заключить, что он был уверен в справедливости общей теоремы существования:

Всякой относительной группе классов дивизоров A/H поля k соответствует поле классов K над k.

Вебер заметил, что из существования поля классов K над k следует существование бесконечного множества простых дивизоров в единичном классе группы A/H; это представляет собой далеко идущее обобщение знаменитой теоремы Дирихле о простых числах в данном взаимно простом с модулем классе вычетов. Ему, однако, не было известно иных примеров существования полей классов, чем те, которые возникли в теории полей деления круга и в теории модулярных и эллиптических функций.

2. Подчеркивание роли Вебера в возникновении теории полей классов отнюдь не означает умаления огромных заслуг Гильберта в развитии этой теории, но лишь способствует их правильному освещению. Гильберт сам высоко ценил Вебера; он часто цитировал его и отмечал значение его идей и результатов, относящихся к полям классов.

Публикации Гильберта [14] — [17] (1898, 1899, 1900, 1902) по теории полей классов ограничивались только частным случаем абсолютного поля классов, т. е. случаем, когда главный класс H содержит все главные дивизоры (с условием на знак или без него). Более того, он проводил доказательства только для *относительно квадратичных* числовых полей, т. е. для $n = 2$, с числом классов $h = 2$. Перед его мысленным взором, однако, стоял более общий случай. В частности, в лекциях [15] (1899) перед собранием DMV (Немецкой математической Ассоциации), происходивших в Брауншвейге в 1897 году, он произнес (в вольном переводе) следующие слова:

«В этой лекции мы ограничим наше рассмотрение относительно абелевыми полями второй степени. Однако это ограничение только временное, и так как все выводы в доказательствах теорем можно обобщить, то следует надеяться, что трудности создания теории относительно абелевых полей не будут непреодолимыми». Гильберт имел в виду при этом уже упоминавшиеся основные теоремы теории полей классов в их полной общности (*теорема существования*, *теорема единственности*, *теорема вложения*, *теорема изоморфизма* и *закон взаимности*)».

Для Гильберта теория полей классов не была, как для Кронекера и Вебера, только средством доказательства теоремы полноты или обобщения теоремы Дирихле о простых числах. Как ясно видно из отрывков, подобных цитированному выше, и из заголовка к его статьям [14] (1898, 1902) в Göttinger Nachrichten, он всегда рассматривал ее как «теорию относительно абелевых полей». Дальней целью его было нахождение *высшего закона взаимности* — задача, навеянная идеями Гаусса, Якоби, Эйзенштейна и Куммера и сформулированная в его знаменитой парижской лекции в 1900 г. как 9-я проблема. Действительно, одним из самых глубоких достижений Гильберта является установление закона взаимности в виде формулы произведения для его символа норменного вычета:

$$\prod_{\mathfrak{p}} \left(\frac{a, b}{\mathfrak{p}}\right)_n = 1.$$

Здесь предполагается, что поле k содержит корни n-й степени из единицы, а $\mathfrak{p}$ пробегает все простые дивизоры поля k, включая те, которые мы теперь называем бесконечными простыми точками и которые Гильберт ввел как символы $1, 1', 1'', \ldots$. Он подметил аналогию этой формулы (выведенной им только в специальных случаях) с теоремой о вычетах алгебраических функций — простые точки $\mathfrak{p}$ с символом норменного вычета $\neq 1$ соответствуют точкам ветвления на римановой поверхности [1]). Эта ана-

[1]) С сегодняшней точки зрения это не вполне точно. В числовом случае символ норменного вычета может быть отличен от единицы и без ветвления, а именно за счет инерции. В полях алгебраических функций над полем комплексных чисел это не так, там играет роль только ветвление.

логия была позднее блестяще подтверждена объединением указанной формулы с формулой произведения для полей алгебраических функций с конечным полем констант в теореме о вычетах Шмида [51] (1936) и Витта [10] (1937). Далее, Гильберт установил (опять только в частном случае) *теорему о нормах*:

Равенство $\left(\frac{a, b}{\mathfrak{p}}\right)_n = 1$ *имеет место для всех* $\mathfrak{p}$ *тогда и только тогда, когда* a *— относительная норма элемента из поля* $k(\sqrt[n]{b})$,

столь важную для дальнейшего развития теории. Эта теорема была доказана позже в полной общности мною [42] (1930).

При уже указанном ограничении — для случая абсолютной группы классов дивизоров — гильбертовский список теорем о полях классов содержит, помимо уже упомянутых, теорему о дискриминанте:

Поле K *имеет относительный дискриминант* $\mathfrak{d} = 1$ *над полем* k.

Далее, он установил *теорему о главных дивизорах*, о которой уже говорилось ранее в этой главе:

Все дивизоры поля k *становятся главными дивизорами в* K.

Более того, он утверждал, что

число классов поля K *не делится на* 2,

причем это верно не только при его исходном ограничении, состоящем в том, что число классов h поля k равно 2, но и при $h = 4$.

За исключением этого последнего утверждения, которое оказалось верным лишь при $h = 2$, но не обязательно при $h = 4$, все утверждения Гильберта о полях классов были доказаны в общем случае. Однако что касается теоремы о главных дивизорах, то здесь положение оказалось гораздо более сложным, чем, по-видимому, думал Гильберт. Нельзя не испытывать величайшего восхищения перед остротой его мысли и проницательностью, которые позволили ему предугадать столь тонкий общий закон на основании довольно специальных случаев.

3. Что касается *закона взаимности*, то в 1899 году Геттингенское королевское научное общество, вероятно по предложению Гильберта, назначило премию за детальное рассмотрение к 1901 году этого закона для случая простого показателя $l \neq 2$. Эта задача была решена Фуртвенглером. В трактате, удостоенном премии [33] (1902, 1904), он дал решение только для полей k, число классов которых не делится на l, причем он не делал различия между $l - 1$ разными классами невычетов. В позднейших работах [35, 36] (1909, 1912, 1913, 1928), однако, Фуртвенглер доказал закон взаимности для простого показателя l (включая $l = 2$) в полной общности. Он не только доказал его в классическом виде:

$\left(\frac{a}{b}\right)_l = \left(\frac{b}{a}\right)_l$, *если* a *и* b *примарны (и в случае* $l = 2$ *всюду положительны)*,

но также и в виде гильбертовой формулы произведения для символа норменного вычета. Согласно его замечательной идее, закон в его классической форме — через переход к расширению $\bar{k} = k(\sqrt[l]{ab^{-1}})$, над которым поле $\bar{k}(\sqrt[l]{a}) = \bar{k}(\sqrt[l]{b})$ неразветвлено и потому содержится в абсолютном поле классов $\bar{K}$, — превращается в *закон разложения* в расширении $\bar{K}/\bar{k}$. Иными словами, $\left(\frac{a}{\mathfrak{p}}\right)_l = \left(\frac{b}{\mathfrak{p}}\right)_l$ над полем $\bar{k}$ зависит только от абсолютного класса в $\bar{k}$, к которому принадлежит дивизор $\mathfrak{p}$. Этот закон разложения уже был в его распоряжении, поскольку он ранее доказал теорему существования абсолютного поля классов [34] (1907).

4. Решающий шаг вперед был сделан Такаги [28], [29] (1920, 1922) в двух весьма важных работах по теории полей классов и закону взаимности. Такаги в начале века изучал работы Гильберта по теории чисел и исследовал относительно абелевы поля над полем гауссовых чисел. Результатом этого явилось решение им для этого поля [27] (1903) знаменитой проблемы полноты Кронекера средствами тео-

рии деления эллиптических функций в случае лемнискаты (т. е. когда параллелограмм периодов — квадрат).

В 1920 году Такаги большой работой о полях классов ознаменовал новый решающий поворот в теории полей классов, введя новое определение понятия «поле классов». Это определение было более удачным, чем веберовское, потому что оно позволяло рассматривать важный вопрос о теореме полноты с самого начала.

Для произвольного расширения K поля k им было установлено соответствие между целыми модулями дивизоров m поля k и относительными группами классов дивизоров, *интерпретирующими* $\bmod m$; именно модулю m соответствует наименьшая факторгруппа A_m/H_m, главный класс H_m которой содержит все нормы $N(\mathfrak{A})$ над k дивизоров $\mathfrak{A}$ из поля K, взаимно простых с модулем m, и, значит, содержит все дивизоры $\mathfrak{a}$ поля k, взаимно простые с модулем m, для которых

$$\mathfrak{a} \sim N(\mathfrak{A}) \pmod m, \text{ т. е. } \frac{\mathfrak{a}}{N(\mathfrak{A})} \cong a \equiv 1 \pmod m \quad (a \in k).$$

Если модуль m достаточно высок, более точно, для всех m, кратных наименьшему $\mathfrak{f}$ (где $\mathfrak{f}$ — ведущий модуль расширения K поля k), то группы классов A_m/H_m становятся «равными» и, значит, образуют относительную группу классов дивизоров A/H в смысле Вебера с ведущим модулем $\mathfrak{f}$. Как и у Вебера, здесь выполняется уже упоминавшееся первое основное неравенство

$$[A:H] = h \leqslant n = [K:k],$$

доказанное аналитическими средствами. Теперь определение Такаги поля классов выглядит так:

Расширение K поля k называется полем классов, соответствующим относительной группе классов дивизоров A/H, если выполняется равенство $h = n$.

Основная теорема теории полей классов, доказанная Такаги и базирующаяся на этом определении, может быть сформулирована следующим образом:

Понятие поля классов устанавливает взаимно однозначное соответствие между всеми абелевыми расширениями поля k и всеми относительными группами классов дивизоров этого поля.

Это утверждение охватывает теорему существования, теорему единственности, теорему полноты в старой терминологии, а также *теорему ограничения*:

если расширение K поля k неабелево, то $h < n$,

которая была добавлена позже.

«Партнерами» описанного взаимно однозначного соответствия выступают далее следующие утверждения.

$K \subseteq K' \Leftrightarrow H \supseteq H'$ (*теорема вложения*);

$\mathfrak{G}(K/k) \simeq A/H$ (*теорема изоморфизма*);

дивизор $\mathfrak{p}$ вполне распадается в поле K на простые дивизоры относительной степени $\mathfrak{f}$ с индексами ветвления e тогда и только тогда, когда $\mathfrak{p}^f$ является наименьшей степенью дивизора $\mathfrak{p}$, лежащей в $H_\mathfrak{p}$, где $A/H_\mathfrak{p}$ — максимальная факторгруппа группы A/H с ведущим модулем, взаимно простым с $\mathfrak{p}$, и $e = [H_\mathfrak{p} : H]$ (*закон разложения*).

Значит,

$\mathfrak{p} \mid \mathfrak{d}$ тогда и только тогда, когда $\mathfrak{p} \mid \mathfrak{f}$

— утверждение, которое впоследствии было уточнено и дополнено мною [40], [43] (1926, 1927, 1930) и приняло следующий вид:

$$\mathfrak{d} = \prod_\chi \mathfrak{f}_\chi, \quad \mathfrak{f} = \mathop{\mathsf{M}}_\chi \mathfrak{f}_\chi$$

(*теорема о дискриминанте и ведущем модуле*), где χ пробегает все характеры группы A/H, через $\mathfrak{f}_\chi$ обозначены их ведущие модули, а через $\mathop{\mathsf{M}}_\chi$ — наименьшее общее кратное всех характеров χ.

В то время как теорема существования получается из теоремы единственности и теоремы полноты несложными преобразованиями, доказательство теоремы полноты нуждается во втором [1]) основном неравенстве

$$h \geqslant n.$$

Оно является далеко идущим обобщением классической теории родов из «*Арифметических исследований*» Гаусса. В настоящее время теория когомологий позволяет систе-

[1]) В современной терминологии — первое неравенство.

матизировать довольно сложную цепь заключений, ведущих к установлению этого неравенства.

5. Возвращаясь к закону взаимности, отметим, что упоминавшаяся выше работа Такаги (1922) уже дала довольно сильные упрощения сравнительно сложных рассуждений Фуртвенглера (всего лишь 40 страниц вместо 80!). Эти упрощения стали возможными благодаря использованию полной теории полей классов вместо теории только абсолютных полей классов. Однако лишь Артину принадлежит совершенно новая идея фундаментальной важности, которая полностью вскрыла суть этого закона. Речь идет о том, что Артин понял значение явного выражения для *канонического изоморфизма группы классов A/H на группу Галуа* $\mathfrak{G}(K/k)$.

Артин [2] (1927) показал, что такой изоморфизм получается установлением соответствия между простыми дивизорами $\mathfrak{p} \nmid \mathfrak{d}$, или вернее их классами в A/H, и так называемыми автоморфизмами Фробениуса $F_\mathfrak{p}$ расширения K/k по отношению к дивизору $\mathfrak{p}$. Всякий такой автоморфизм определяется условием

$$a^{F_\mathfrak{p}} \equiv a^{\mathfrak{N}(\mathfrak{p})} \pmod{\mathfrak{p}} \text{ для всех целых } a \in K,$$

где $\mathfrak{N}(\mathfrak{p})$ — абсолютная норма дивизора $\mathfrak{p}$. Сейчас пишут

$$F_\mathfrak{p} = \left(\frac{K/k}{\mathfrak{p}}\right)$$

и отсюда определяют символ Артина $\frac{K/k}{\mathfrak{a}}$ как мультипликативную функцию на группе $A_\mathfrak{f}$ всех дивизоров $\mathfrak{a}$ поля k, взаимно простых с $\mathfrak{d}$ или, что то же самое, с ведущим модулем $\mathfrak{f}$. Изоморфизм между группами A/H и $\mathfrak{G}(K/k)$ можно выразить тогда *законом взаимности Артина*:

$$\left(\frac{K/k}{\mathfrak{A}}\right) = 1 \text{ } \textit{тогда и только тогда, когда } \mathfrak{a} \in H_\mathfrak{f}.$$

Артин [1] (1924) получил этот закон взаимности четырьмя годами раньше и доказал его в несложных частных случаях. Однако лишь когда Артин ознакомился с методом Чеботарева пересечения классов из группы A/H с относительными классами, соответствующими круговым расширениям, он достиг успеха в своих поисках общего доказательства. Чеботарев [47] (1926) разработал свой метод в целях усиления одной теоремы Фробениуса [32] (1896), а именно:

Простые дивизоры $\mathfrak{P}$ нормального расширения K поля k с автоморфизмом Фробениуса $F_\mathfrak{P}$ из заданного отдела (Abteilung) $S^{-1}F_\mathfrak{P}^\nu S$ (*где ν взаимно просто с порядком автоморфизма $F_\mathfrak{P}$, а S пробегает всю группу $\mathfrak{G}(K/k)$*) *встречаются с плотностью, равной относительной частоте элементов из этого отдела во всей группе* $\mathfrak{G}(K/k)$. Указанный метод позволил Чеботареву обобщить эту теорему на индивидуальный сопряженный класс $S^{-1}F_\mathfrak{P}S$.

Для расширения Куммера $K = k(\sqrt[n]{b})$ (где k содержит корни n-й степени из единицы) автоморфизм Фробениуса $\left(\frac{K/k}{\mathfrak{p}}\right)$ переводит элемент $\sqrt[n]{b}$ в $\left(\frac{b}{\mathfrak{p}}\right)_n \cdot \sqrt[n]{b}$, что очевидно из определения символа норменного вычета $\left(\frac{b}{\mathfrak{p}}\right)_n$ с помощью критерия Эйлера. Поэтому закон взаимности Артина дает нам следующее утверждение:

Значение символа $\left(\frac{b}{\mathfrak{p}}\right)_n$ зависит только от класса, к которому принадлежит идеал $\mathfrak{p}$ в группе относительных классов по $\bmod \mathfrak{f}_b$, *соответствующей полю* $k(\sqrt[n]{b})$.

Здесь $\mathfrak{f}_b$ обозначает ведущий модуль поля $k(\sqrt[n]{b})$.

С другой стороны, из определения символа $\left(\frac{b}{\mathfrak{p}}\right)_n$ ясно, что он зависит только от класса вычетов по $\bmod \mathfrak{p}$, к которому принадлежит b. Отсюда легко получить взаимность в ее классической форме, а также в форме гильбертовской формулы произведения. Таким образом, становится понятно, почему Артин назвал описанный выше изоморфизм «общим законом взаимности».

С помощью своего закона Артин [3] (1930) смог также свести теорему о главных дивизорах, предсказанную Гильбертом, но еще не доказанную Такаги, к чисто теоретико-групповому предложению, которое затем было доказано Фуртвенглером [37] (1930). В дальнейшем доказательства этого предложения были даны Магнусом [26] (1934), Янага

[57] (1934), Виттом [9, 11] (1936, 1954) и Шуманом и Францем [54] (1938), в то время как Таусски и Шольц [31] (1932, 1934) исследовали более внимательно процесс превращения дивизоров из подполей в главные дивизоры в абсолютном поле классов. Окончательных результатов в этой последней задаче не получено, однако, по сей день.

6. Аналогично переходу от степенного символа вычета $\left(\frac{b}{a}\right)_n$ к более общему символу Артина $\left(\frac{K/k}{\mathfrak{A}}\right)$ я перешел от символа норменного вычета $\left(\frac{a,\ b}{\mathfrak{p}}\right)_n$ Гильберта (где поле k содержит корни n-й степени из единицы) к символу $\left(\frac{a,\ K/k}{\mathfrak{p}}\right)$ над произвольным полем k (которое необязательно содержит корни n-й степени из единицы) [40], [41] (1926, 1927, 1930). Первоначально вместо всех простых точек $\mathfrak{p}$ поля k мое определение, следуя обходному пути Гильберта, вынуждено было использовать лишь простые дивизоры $\mathfrak{p}/n$. Как следствие этого, связь символа с норменным вычетом становилась видимой только в силу закона взаимности Артина. Вскоре, однако, мне удалось дать [46] (1933) новое определение, из которого эта связь стала ясной непосредственно. Мое новое определение основывалось на теории алгебр.

Предварительно я показал [45] (1931), что любая центральная простая алгебра степени n над локальным полем $k_\mathfrak{p}$ с простым элементом π допускает неразветвленное (и, значит, циклическое) поле разложения $Z_\mathfrak{p}$. Следовательно, такая алгебра имеет канонические образующие

$$u_\mathfrak{p}^n = \pi^{v_\mathfrak{p}},\quad u_\mathfrak{p}^{-1} Z_\mathfrak{p} u_\mathfrak{p} = Z_\mathfrak{p}^{F_\mathfrak{p}}$$

(где $F_\mathfrak{p}$ — автоморфизм Фробениуса). Таким образом, класс вычетов $v_\mathfrak{p}/n \,(\mathrm{mod}^+ 1)$ инвариантно связан с алгеброй. Для глобальных циклических расширений K поля k я положил

$$\left(\frac{a,\ K/k}{\mathfrak{p}}\right) = S^{-v_\mathfrak{p}},$$

если циклическая алгебра над полем k, порожденная элементами

$$u^n = a,\quad u^{-1} K u = K^S,$$

после расширения до пополнения $k_\mathfrak{p}$ имеет инвариант $v_\mathfrak{p}/n \,(\mathrm{mod}^+ 1)$. В частности, для расширения Куммера $K = k(\sqrt[n]{b})$ (где поле k содержит корни n-й степени из единицы) автоморфизм $\left(\frac{a,\ K/k}{\mathfrak{p}}\right)$ переводит элемент $\sqrt[n]{b}$ в $\left(\frac{a,\ b}{\mathfrak{p}}\right)_n \sqrt[n]{b}$.

Из этого определения немедленно извлекается *локальное* свойство:

$$\left(\frac{a,\ K/k}{\mathfrak{p}}\right) = 1 \text{ } \textit{тогда и только тогда, когда } a \textit{ есть}$$

$$\textit{норма из } K^\mathfrak{p}/k_\mathfrak{p},$$

где $K^\mathfrak{p}$ обозначает тип (с точностью до изоморфизма) пополнения $K_\mathfrak{P}$ по простому дивизору $\mathfrak{P} \mid \mathfrak{p}$. Поэтому символ $\left(\frac{a,\ K/k}{\mathfrak{p}}\right)$ можно называть просто *норменным символом*. В *глобальном* случае мне удалось доказать [40, 41] (1926, 1927, 1930) *теорему о нормах*:

Равенство $\left(\frac{a,\ K/k}{\mathfrak{p}}\right) = 1$ *имеет место для всех дивизоров* $\mathfrak{p}$ *тогда и только тогда, когда* a *— норма элемента из расширения* K *поля* k.

Эта теорема была предвосхищена Гильбертом для своего символа, как уже упоминалось ранее. Таким образом, формула произведения Гильберта для его символа превратилась в формулу произведения для норменного символа:

$$\prod_\mathfrak{p} \left(\frac{a,\ K/k}{\mathfrak{p}}\right) = 1.$$

Она эквивалентна моей *теореме о сумме для центральных простых алгебр* [46] (1933):

$$\sum_\mathfrak{p} \frac{v_\mathfrak{p}}{n} \equiv 0 \,(\mathrm{mod}^+ 1).$$

В то время как определение норменного символа обобщалось с циклических до произвольных абелевых расширений K/k с помощью формальных построений, я показал [44]

(1931), что теорема о нормах становится в такой общности неверной.

В связи с локальным свойством норменного символа мне удалось установить [42] (1930) *основную теорему теории полей классов над локальными полями* $k_\mathfrak{p}$. Здесь существует взаимно однозначное соответствие между абелевыми расширениями $K^\mathfrak{p}$ поля $k_\mathfrak{p}$ и относительными группами классов чисел $A_\mathfrak{p}/H_\mathfrak{p}$ поля $k_\mathfrak{p}$, такое, что $\frac{a,\, K^\mathfrak{p}/k_\mathfrak{p}}{\mathfrak{p}}$ дает канонический изоморфизм группы $A_\mathfrak{p}/H_\mathfrak{p}$ на $\mathfrak{G}(K^\mathfrak{p}/k_\mathfrak{p})$. Связь с теорией полей классов над глобальным полем k устанавливается следующими предложениями:

(1) расширение $K^\mathfrak{p}$ поля $k_\mathfrak{p}$ представляет тип (с точностью до изоморфизма) пополнения по дивизору $\mathfrak{P}/\mathfrak{p}$ расширения K поля k;

(2) группа $\mathfrak{G}(K^\mathfrak{p}/k_\mathfrak{p})$ является группой разложения дивизора $\mathfrak{P}/\mathfrak{p}$ в поле K над k.

Впоследствии Шмидт [52] (1930) и Шевалле [48] (1933) дали систематическое развитие локальной теории полей классов без ссылки, как сделал я, на эту связь с глобальной теорией полей классов. Здесь я должен также упомянуть особую роль работ Эрбрана [55], [56] (1931, 1932) о теоретико-групповом механизме некоторых доказательств в локальной, равно как и в глобальной теории полей классов и в теории высшего ветвления нормальных расширений.

7. В теории полей классов, развитой Такаги, характеризация абелевых расширений K поля k посредством групп классов дивизоров поля k обладает неприятным дефектом. Этот дефект проистекает от аппроксимации группы A/H группами A_m/H_m — некоего предельного процесса по возрастающим модулям дивизоров m. После того как $\mathfrak{p}$-адические понятия и методы описанным выше образом раскрыли сущность теории полей классов, Шевалле [49] (1933) пришел к счастливой идее заменить конструкцию Вебера — Такаги в терминах относительных групп классов дивизоров A/H более изящной $\mathfrak{p}$-адической конструкцией. Ему удалось добиться успеха путем введения *идеальных элементов* или сокращенно *иделей*, а именно векторов

$$\mathbf{a} = (\ldots, a_\mathfrak{p}, \ldots)$$

с компонентами $a_\mathfrak{p}$ из отдельных пополнений $k_\mathfrak{p}$, удовлетворяющих некоторым условиям конечности, а именно

$$a_\mathfrak{p} \cong 1 \text{ для почти всех } \mathfrak{p}.$$

Шевалле заменил относительные группы классов дивизоров Вебера — Такаги A/H факторгруппами $\mathbf{A}/\mathbf{H}$ *абсолютной группы классов иделей* $\mathbf{A}/k^*$, где k^* обозначает группу главных иделей $(\ldots, a, \ldots)$, соответствующих числам $a \neq 0$ из поля k. Он доказал, что символ

$$\left(\frac{K/k}{\mathbf{a}}\right) = \prod_\mathfrak{p} \left(\frac{a_\mathfrak{p},\, K^\mathfrak{p}/k_\mathfrak{p}}{\mathfrak{p}}\right),$$

названный впоследствии *символом Шевалле*, осуществляет изоморфизм между группой классов иделей $\mathbf{A}/\mathbf{H}$ и группой Галуа $\mathfrak{Z}(K/k)$. Здесь главный класс $\mathbf{H}$ состоит из всех тех абсолютных классов иделей поля k, которые содержат нормы иделей из поля K. В теории полей классов Шевалле эти группы классов иделей играют роль относительных групп классов дивизоров A/H Такаги. Множеству всех абелевых расширений K поля k соответствует, таким образом, множество всех групп классов иделей $\mathbf{A}/\mathbf{H}$, где главный класс $\mathbf{H}$ открыт в подходящей топологии группы $\mathbf{A}$, а именно в той, для которой полную систему окрестностей единицы составляют идели единиц, сравнимых с единицей по модулю m для всевозможных модулей дивизоров m.

Таким образом, можно сказать, что идеи (но не идели) Шевалле позволили укорениться в теории полей классов *локально-глобальному принципу*.

При всей красоте построения теории полей классов Такаги в нем был один изъян, устраненный Шевалле [50] (1940). Этот изъян состоял в обращении к аналитическим средствам (L-ряды Дирихле) для доказательства первого основного неравенства $h \leqslant n$. Шевалле нашел чисто арифметическое доказательство этого неравенства.

8. Можно было бы еще много рассказать о дальнейшем развитии теории, возникшей из теории полей классов, обрисованной до этого. В частности, остались не затронутой особенно дорогая моему сердцу *явная формула взаимности* (определение норменного символа $\left(\frac{a, b}{\mathfrak{p}}\right)_n$ для простых дивизоров $\mathfrak{p}/n$), затем *допущение бесконечных алгебраических расширений* K поля k, теория полей классов над функциональными полями (поля алгебраических функций с конечным полем констант), L-ряды Артина и ведущие модули и т. д. Я должен, однако, воздержаться здесь от обсуждения всех этих предметов, поскольку оно заставило бы перешагнуть границы данной лекции.

Я также не могу касаться дальнейшего развития теории полей классов после войны, так как полагаю, что должен закончить мой очерк исторического развития на этом месте.

Если я правильно понял, моей задачей было нарисовать для математиков послевоенного поколения яркую и живую картину великого и прекрасного здания теории полей классов, воздвигнутого предвоенными поколениями. Как мне кажется, четкий контур и яркие детали этого замечательного здания теряют что-то от их блеска и гибкости при проникновении в теорию полей классов когомологических понятий и методов, которые стали столь могущественными после войны.

Я был бы рад думать, что преуспел в какой-то степени в выполнении своей задачи.

ЛИТЕРАТУРА

Артин (Artin E.)

[1] Über eine neue Art von L-Reihen, *Abh. Math. Semin. Univ. Hamburg*, **3** (1924), 89—108. (Collected Papers, Addison Wesley, 1965, 105—124.)

[2] Beweis des allgemeinen Reziprozitätsgesetzes, *Abh. Math. Semin. Univ. Hamburg*, **5** (1927), 353—363. (Collected Papers, Addison Wesley, 1965, 131—141.)

[3] Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, *Abn. Math. Semin. Univ. Hamburg*, **7** (1930), 46—51. (Collected Papers, Addison Wesley, 1965, 159—164.)

Вебер (Weber H.)

[4] Theorie der Abel'schen Zahlkörper, I, II, *Acta Math. Stockh.*, **8** (1886), 193—263; **9** (1887), 105—130.

[5] Elliptische Funktionen und algebraische Zahlen, Braunschweig, 1891.

[6] Über Zahlengruppen in algebraischen Körper 1, 2, 3, *Math. Ann.*, **48** (1897), 433—473; **49** (1897), 83—100; **50** (1898), 1—26.

[7] Lehrbuch der Algebra 3, Braunschweig, 1908.

[8] Zur Theorie der zyklischen Zahlkörper, *Math. Ann.*, 1909, 32—60.

Витт (Witt E.)

[9] Bemerkungen zum Beweis des Hauptidealsatzes von S. Iyanada, *Abh. Math. Semin. Univ. Hamburg*, **11** (1936), 221.

[10] Zyklische Körper und Algebren der Charakteristik p vom Grade p^n, *J. reine angew. Math.*, **176** (1937), 126—140.

[11] Verlagerung von Cruppen und Hauptidealsatz, Proc. Internat. Math. Congress II, Amsterdam, 1954, 71—73.

Гильберт (Hilbert D.)

[12] Neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper, *Nachr. Ges. Wiss. Göttingen* (1896), 29—39.

[13] Bericht: Die Theorie der algebraischen Zahlkörper, *Jber. dt. Mat. Verein.*, **4** (1897), 175—546.

[14] Über die Theorie der relativ-Abel'schen Zahlkörper, *Nachr. Ges. Wiss. Göttingen* (1898), 377—399; *Acta Math. Stockh.*, **26** (1902), 99—132.

[15] Über die Theorie der relativguadratischen Zahlkörper, *Jber. dt. Math. Verein.*, **6** (1899), 88—94.

[16] Über die Theorie des relativquadratischen Zahlkörpers, *Math. Ann.*, **51** (1899), 1—127.

[17] Theorie der algebraischen Zahlkörper, Enzykl. math. Wiss., IC4a, 1900, 675—698.

[18] Theorie des Kreiskörpers, Enzykl. math. Wiss., IC4b, 1900, 699—732.

[19] Mathematische Probleme. Vortrag auf internat. Math. Kongr., Paris, 1900, Nachr. Ges. Wiss. Göttingen, 1900, 253—297. (Перепечатано в «A Collection of Modern Mathematical Classics, Analysis», R. Bellman, Dover, 1961.)

Делоне (Delaunay B.)

[20] Zur Bestimmung algebraiscsher Zahlkörper durch Kongruenzen; eine Anwendung auf die Abelschen Gleichungen, *J. reine angew. Math.*, **152** (1923), 120—123.

Кронекер (Kronecker L.)

[21] Über die algebraisch auflösbaren Gleichuengen I, Sber. preuss. Akad. Wiss., 1853, 365—374; Werke, IV, 1—11.

[22] Über Abel'sche Gleichungen. Sber. preuss. Akad. Wiss., 1877, 845—851; Werke, IV, 63—72.

[23] Grundzüge einer arithmetischen Theorie der algebraischen Grössen, *J. reine angew. Math.*, **92** (1882), 1—2; Werke II, 237—388. См. там же § 19, 1882, 65—68 (321—324).
[24] Zur Theorie der elliptischen Funktionen I—XXII, Sber. preuss. Akad. Wiss.; Werke, IV, 345—496; V, 1—132, 1883—1890.
[25] Auszug aus Brief an R. Dedekind vom 15 März 1880, Werke, 5, 453—458. См. также мое подробное «Zusatz», ibid., 510—515.

Магнус (Magnus W.)
[26] Über den Beweis des Hauptidealsatzes, *J. reine angew. Math.*, **170** (1934), 235—240.

Такаги (Takagi T.)
[27] Über die im Bereich der rationalen komplexen Zahlen Abel'schen Zahlkörper, *J. Coll. Sci. imp. Univ. Tokyo*, **19**, 5 (1903), 1—42.
[28] Über eine Theorie des relativ-Abel'schen Zahlkörpers, *J. Coll. Sci. imp. Univ. Tokyo*, **41**, 9 (1920), 1—133.
[29] Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper, *J. Coll. Sci. imp. Univ. Tokyo*; **44**, 5 (1922), 1—50.

Таусски (Taussky O.)
[30] Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper, *J. reine angew. Math.*, **168** (1932), 193—210.

Таусски, Шольц (Taussky O., Scholz A.)
[31] Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf deh Klassenkörperturm, *J. reine angew. Math.*, **171** (1934), 19—41.

Фробениус (Frobenius G.)
[32] Über die Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, Sber. preuss. Akad. Wiss., 1896, 689—703.

Фуртвенглер (Furtwängler Rh.)
[33] Über die Reziprozitätsgesetze zwischen l^{ten} Potenzresten in algebraischen Zahlkörpern, wenn L eine ingerade Primzahl bedeutet, Abh. K. Ges. Wiss. Göttingen (Neue Folge), **2**, **3**, 1902, 1—82; *Math. Ann.*, **58** (1904), 1—50.
[34] Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers, *Math. Ann.*, **63** (1907), 1—37.
[35] Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern, I, II, III, *Math. Ann.*, **67** (1909), 1—31; **72** (1912), 346—386; **74** (1913), 413—429.
[36] Über die Reziprozitätsgesetze für ungerade Primzahlexponenten, Math. Ann., **98** (1928), 539—543.

[37] Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper, *Abh. Math. Semin. Univ. Hamburg*, **7** (1930), 14—36.

Фютер (Fueter R.)
[38] Abel'sche Gleichungen in quadratisch-imaginären Zahlkörpern, *Math. Ann.*, **75** (1914), 177—255.
[39] Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen (unter Mitwirkung von M. Gut), Leipzig-Berlin, 1927.

Хассе (Hasse H.)
[40] Bericht über neuere Untersuchungen und Probleme aus der algebraischen Zahlkörper, I, Ia, II, *Jber. dt. Math. Verein.*, **35** (1926), 1—55; **36** (1927), 233—311; Exg. **6** (1930), 1—204.
[41] Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols, *J. reine angew. Math.*, **162** (1930), 134—144.
[42] Die Normenresttheorie relativ-Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen, *J. reine angev. Math.*, **162** (1930), 145—154.
[43] Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper, *J. reine angew. Math.*, **162** (1930), 169—184.
[44] Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol, Nachr. Ges. Wiss. Göttingen, 1931, 64—69.
[45] Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, *Math. Ann.* 1931, 495—534.
[46] Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, *Math. Ann.*, **107** (1933), 731—760.

Чеботарев Н. Г. (Tchebotarev N.)
[47] Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, *Math. Ann.*, **95** (1926), 191—228.

Шевалле (Chevalley C.)
[48] La thèorie du symbole de restes normiques, *J. reine angew. Math.*, **169** (1933), 140—157.
[49] Sur la théorie du corps de classes dans les corps finis et les corps locaux, *J. Fac. Sci. Tokyo Univ.*, **2** (1933), 365—476.
[50] La théorie du corps de classes, *Ann. Math.*, **41** (1940), 394—417.

Шмид (Schmid H. L.)
[51] Ziklische algebraische Funktionenkorper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p, *J. reine angew. Math.*, **175** (1936), 108—123.

Шмидт (Schmidt F. K.)
[52] Zur Klassenkörpertheorie im Kleinen, *J. reine angew. Math.*, **162** (1930), 155—168.

Шпейзер (Speiser A.)
[53] Die Zerlegungsgruppe, *J. reine angew. Math.*, **149** (1919), 174—188.

Шуман (Schumann H. G.)
[54] Zum Beweis des Hauptidealsatzes (unter Mitwirkung von W. Franz), *Abh. Math. Semin. Univ. Hamburg*, **12** (1938), 42—47.

Эрбран (Herbrand J.)
[55] Sur la théorie des groupes de décomposition, d'inertie et de ramification, *J. Math. pures appl.*, **10** (1931), 481—498.
[56] Sur le théorèmes du genre principal et des idéaux principaux, *Abh. Math. Semin. Univ. Hamburg*, **9** (1932), 84—92.

Янага (Iyanaga S.)
[57] Zum Beweis des Hauptidealsatzes, *Abh. Math. Semin. Univ. Hamburg*, **10** (1934), 349—357.

ГЛАВА XII

Применение вычисления в теории полей классов

Свиннертон-Дайер

Пусть G — связная алгебраическая группа. Шевалле показал, что G содержит нормальный делитель R, являющийся связной линейной группой, причем факторгруппа G/R — абелево многообразие [1]); эти свойства определяют R однозначно. Общая теория алгебраических групп зависит, следовательно, от теории линейных групп и абелевых многообразий. В гл. X этой книги Кнезер описал известные теоретико-числовые свойства линейных групп, здесь будет сделано то же самое для абелевых многообразий. Но между двумя этими темами существует фундаментальное различие. Кнезер изложил теорию вполне исчерпывающую и удовлетворительную — главные результаты уже получены или близки к завершению, и нет оснований полагать, что существуют еще не обнаруженные важные теоремы. С другой стороны, пока еще доказано очень мало теоретико-числовых теорем об абелевых многообразиях. Большинство интересных утверждений являются гипотезами, основанными на вычислениях, проделанных лишь в частных случаях, и неприступность этих гипотез говорит о том, что должны существовать важные теоремы, которые еще даже не сформулированы.

Первоначальные вычисления принадлежат в основном Берчу и Свиннертон-Дайеру; их результаты могут быть

[1]) Абелевым многообразием называется связная алгебраическая группа, полная как алгебраическое многообразие; групповая операция на абелевом многообразии обязательно коммутативна. Простейшим примером абелева многообразия является неособая кубическая кривая на проективной плоскости вместе с отмеченной точкой на кривой, которая является единицей групповой операции.

удобно сформулированы благодаря усилиям Касселса и Тэйта. Цель этой главы — описать численные методы, показать, насколько далеко гипотезы основаны на них, и объяснить, почему формулировка гипотез в самом общем виде выглядит обоснованной, хотя все вычисления имеют отношение к случаям одного частного вида.

С появлением электронных машин многие ранее недоступные вычисления стали легко осуществимыми в тех случаях, когда они могут быть запрограммированы. В теории чисел существует много вопросов, в которых прямые вычисления приводили к ценным результатам. (Однако в настоящее время большинство теоретико-числовых вычислений чрезвычайно громоздко и не позволяет рассчитывать на получение результатов общего характера.)

Другая цель этой главы — показать, что именно действительно может быть сделано путем вычислений и что должен рассмотреть теоретико-числовик, прежде чем обратиться с просьбой сделать нужные ему вычисления.

Когда современный алгебраист что-либо определяет, он обычно начинает с рассмотрения отношения одного бесконечного объекта к другому. Процессы такого рода редко могут быть доведены до конца даже теоретически и никогда практически. Поэтому объекты, определенные таким образом, не являются эффективно вычислимыми. Если же что-либо должно быть вычислено, то оно должно быть определено более упрощенным способом, пусть даже и менее канонически. Это относится не только к окончательному результату вычислений, но и ко всему, что встречается в процессе вычислений. Это может быть трудным или даже невозможным: например, для группы Тэйта — Шафаревича (рассматриваемой ниже) в настоящее время нет конструктивного определения.

Когда теоретико-числовик выразил свою задачу в поддающейся вычислениям форме, он может оценить, сколько потребуется машинного времени для выполнения вычислений. Это зависит от числа выполняемых операций — подразумеваются операции сложения, вычитания, умножения и деления. (Это грубый метод оценки, он не учитывает, например, время, затраченное на организационную часть программы, но он дает правильный порядок величины.) Вычисления, требующие 10^6 операций, тривиальны, и их

стоит выполнить, даже если ценность их результатов вызывает сомнения. Вычисления порядка 10^9 операций реальны, но неблагоразумны. Их стоит сделать в погоне за какой-либо серьезной идеей, но они не могут быть обоснованы надеждой на счастливую случайность; кроме того, метод вычислений должен быть достаточно эффективным, поскольку в небольших задачах выбирают способ, требующий минимальных усилий для написания программы. Наконец, вычисления, требующие 10^{12} операций, находятся на границе физических возможностей; они могут быть оправданы только важнейшими научными достижениями, такими, как высадка человека на Луне.

Когда вычисления закончены, нужно убедиться в их достоверности. Типичная программа, записанная в машинном коде, содержит тысячи различных символов, и ошибка в одном из них может повлиять на результат вычислений. Большинство ошибок приводит к полному искажению результатов и может быть, следовательно, обнаружено и исправлено; но некоторые ошибки аналогичны опечаткам в формулах и могут быть причиной неправильных ответов. Некоторые вычисления самоконтролируемы: ниже приведен один пример, в котором целое число получается как значение сложного аналитического выражения, и если вычисления содержат ошибку, результат не всегда будет близок к целому числу. Во многих вычислениях полученный ответ может быть проверен с относительно небольшими усилиями, например решение диафантова уравнения. Но вообще желательно либо получить несколько типичных результатов вручную для сравнения с такими же результатами, полученными машиной, либо повторить все вычисления по другой программе на другой машине.

Если Γ — кривая, определенная над полем рациональных чисел $\mathbf{Q}$, то при каких условиях мы можем утверждать, что Γ содержит рациональную точку? Эта задача полностью решена для кривых рода 0, ибо тогда кривая Γ бирационально эквивалентна над полем $\mathbf{Q}$ прямой или кривой второго порядка; естественно рассмотреть случай, когда Γ имеет род 1. Это эквивалентно утверждению, что для любых точек $P_1, \ldots, P_n, Q_1, \ldots, Q_{n-1}$ на Γ существует единственная точка Q_n, такая, что P_i являются полюсами, а Q_i — нулями некоторой функции на Γ. Отсюда следует,

что для любой данной точки O на Γ мы можем снабдить Γ групповой структурой с единичным элементом O; таким образом, если P_1, P_2 — точки на кривой Γ, то мы определим $Q = P_1 + P_2$ так, чтобы P_1, P_2 были полюсами, а O, Q — нулями некоторой функции на Γ. Более того, если O и Γ определены над $\mathbf{Q}$, то и групповой закон определен над $\mathbf{Q}$; следовательно, множество рациональных точек на Γ образует группу, которую мы обозначим через $\Gamma_{\mathbf{Q}}$.

Мы можем сопоставить кривой Γ ее якобиеву кривую J следующим образом. На $\Gamma \times \Gamma$ мы определим соотношение эквивалентности: $P_1 \times Q_1 \sim P_2 \times Q_2$ тогда и только тогда, когда P_1, Q_2 являются полюсами, а P_2, Q_1 — нулями функции на Γ. Кривая J определяется (с точностью до бирациональной эквивалентности) как кривая, каждая точка которой соответствует классу эквивалентности на $\Gamma \times \Gamma$. При этом J определено над $\mathbf{Q}$ и, несомненно, содержит рациональную точку, соответствующую классу точек $P \times P$ на $\Gamma \times \Gamma$; мы можем записать уравнение для J в форме

$$y^2z = x^3 - Axz^2 - Bz^3. \tag{1}$$

Мы скажем, что Γ является *главным однородным пространством* над J. Очевидно, что Γ бирационально эквивалентна J над $\mathbf{Q}$ тогда и только тогда, когда она содержит рациональную точку; а так как J имеет каноническую рациональную точку, то на Γ существует каноническая групповая структура.

Задача о рациональных точках на Γ распадается теперь на две части: (i) существует ли рациональная точка на Γ? (ii) какова структура группы рациональных точек на J? Из них более привлекателен второй вопрос, так как с ним связано много проблем. Морделл в 1922 г. доказал следующую теорему.

Теорема Морделла. *Группа рациональных точек на J является конечно порожденной.*

В этой группе легко найти элементы конечного порядка в каждом частном случае. Естественно искать способ нахождения g — числа независимых образующих бесконечного порядка и, если возможно, самого множества таких образующих. Доказательство Морделла полуконструктивно, оно дает в каждом численном примере верхнюю

границу для g, которая, однако, абсурдно велика; но, используя основные идеи этого доказательства, можно обычно найти g и действительное множество образующих. Однако этот процесс может оказаться очень утомительным и нет гарантий, что он приведет к цели. Более того, число g ни с чем больше в теории не связано. С чем же оно все-таки могло бы быть связано?

Мы можем рассмотреть решение уравнения (1) как результат объединения согласованного множества решений сравнений

$$y^2z \equiv x^3 - Axz^2 - Bz^3 \pmod{p^n}. \tag{2}$$

Можно предположить, что если эти сравнения имеют большое количество решений, то будет относительно легко найти согласованное множество решений, и поэтому уравнение (1) будет иметь много решений и g будет велико. Следовательно, мы ищем меру плотности решений сравнений (2). Пусть N_{p^n} — число существенно различных примитивных решений сравнений (2). Исключая конечное множество плохих простых p, мы получаем отсюда по лемме Гензеля, что

$$N_{p^n} = p^{n-1}N_p,$$

и мы можем, следовательно, рассмотреть бесконечное произведение

$$\prod (N_p/p). \tag{3}$$

Мы можем также определить N_p как число точек на кривой (1), рассматриваемой над конечным полем из p элементов. Для конечного числа простых чисел множители в (3) определены, по-видимому, неправильно, но пока еще не ясно, что поставить на их место.

Существуют более глубокие соображения для рассмотрения произведения (3), хотя в конце концов и они вводят в заблуждение. Мы имеем

$$N_p = p - \alpha_p - \bar{\alpha}_p + 1,$$

где $|\alpha_p| = p^{1/2}$; и локальная дзета-функция кривой Γ определяется так:

$$\zeta_{\Gamma, p}(s) = \frac{(1-\alpha_p p^{-s})(1-\bar{\alpha}_p p^{-s})}{(1-p^{-s})(1-p^{1-s})}.$$

Числитель правой части принимает значение N_p/p при $s=1$; если мы напишем

$$L_\Gamma(s)=\prod[(1-\alpha_p p^{-s})(1-\bar{\alpha}_p p^{-s})]^{-1}, \tag{4}$$

то

$$\zeta_\Gamma(s)=\prod\zeta_{\Gamma,p}(s)=\frac{\zeta(s)\zeta(s-1)}{L_\Gamma(s)},$$

и формально

$$[L_\Gamma(1)]^{-1}=\prod(N_p/p).$$

Про произведение (4) известна только сходимость при $\operatorname{Re} s>3/2$, хотя существует гипотеза (доказанная в некоторых специальных случаях), что $L_\Gamma(s)$ может быть аналитически продолжена на всю плоскость. Кроме того, можно надеяться, что произведение (3) ограничено, так как предполагают, что $L_\Gamma(s)$ имеет комплексные нули только на прямой $\operatorname{Re} s=1$. Легко вычислить конечное произведение

$$f(P)=\Pi(N_p/p),$$

взятое по всем $p<P$ для значений P, достигающих нескольких тысяч [1]). Результаты наводят на мысль, что $f(P)$ ограничено при $g=0$ и стремится к бесконечности при $g>0$; это делает правдоподобными следующие две гипотезы:

$f(P)$ заключено между константами, умноженными на $(\ln P)^g$;

$L_\Gamma(s)$ имеет нуль порядка g при $s=1$.

(Разумеется, константы в первой гипотезе зависят от Г.) Рассматривая поведение $f(P)$, Берч и Свиннертон-Дайер смогли предсказать значение g для индивидуальных кривых, и предсказания оказались верными приблизительно в 90% случаев; это были кривые, для которых $g=1$, 2 или 3. Но, по-видимому, не существует стандартного численного методд точной оценки числа g таким способом.

[1]) Простейший способ вычисления N_p таков: полагаем $z=1$ в (1) и проверяем всевозможные пары x, y; это потребует $O(p^2)$ операций и непозволительно много машинного времени. Но так как (1) может быть записано в виде $y^2=w=x^3-Ax-B$, то нужно рассматривать только значения w, являющиеся квадратами; тогда можно вычислить число решений при каждом значении x. Таким способом N_p может быть найдено посредством лишь $O(p)$ операций.

Чтобы улучшить этот метод, мы должны больше узнать о $L_\Gamma(s)$. Поэтому естественно рассмотреть кривые J с комплексным умножением, так как в этом случае существует явная формула для N_p и $L_\Gamma(s)$ является произведением L-рядов Гекке. Простейшие из таких кривых записываются в виде

$$y^2z=x^3-Dxz^2, \tag{5}$$

причем мы можем предположить, что D — целое число, не делящееся на биквадраты; если мы обозначим через $(\ldots)_4$ биквадратичный вычет в $\mathbf{Q}(i)$, то мы получим следующую формулу.

Теорема Давенпорта — Хассе. *Для кривой $y^2z=x^3-Dxz^2$*

$$N_p=\begin{cases} p+1 & \text{для } p\equiv 3 \pmod 4,\\ p+1-\pi\left(\frac{D}{\bar{\pi}}\right)_4-\bar{\pi}\left(\frac{D}{\pi}\right)_4 & \text{для } p\equiv 1 \pmod 4,\end{cases}$$

где во втором случае $p=\pi\bar{\pi}$ в $\mathbf{Q}(i)$, причем π, $\bar{\pi}\equiv 1 \pmod{(2+2i)}$.

Полностью доказать эту теорему нелегко. То, что α_p/π является степенью числа i, указал Джекобсталь, который привел элементарное доказательство, кажущееся счастливой удачей. Такая формула справедлива в данном случае потому, что $\mathbf{Q}(i)$ является здесь кольцом эндоморфизмов кривой J в характеристике 0. Если $p\equiv 1 \pmod 4$, то $\mathbf{Q}(i)$ должно быть полным кольцом эндоморфизмов кривой J в характеристике p; известная структурная теорема исключает строго бо́льшие кольца. Значит, α_p, будучи образом эндоморфизма Фробениуса, должно лежать в $\mathbf{Q}(i)$, а так как $\alpha_p\bar{\alpha}_p=p$, то мы находим, что α_p/π является единицей в $\mathbf{Q}(i)$.

Используя приведенные выше значения N_p, мы получаем

$$L_\Gamma(s)=L_D(s)=\prod_{p\equiv 3 \bmod 4}(1+p^{1-2s})^{-1}\times$$

$$\times\prod_{p\equiv 1 \bmod 4}\left[1-\pi p^{-s}\left(\frac{D}{\bar{\pi}}\right)_4\right]^{-1}\cdot\left[1-\bar{\pi}p\left(\frac{D}{\pi}\right)_4\right]^{-1}=$$

$$=\prod\left[1-\left(\frac{D}{\pi}\right)_4\bar{\pi}(N\bar{\pi})^{-s}\right]^{-1}=\sum\left(\frac{D}{\sigma}\right)_4\bar{\sigma}(N\sigma)^{-s},$$

где произведение берется по всем простым гауссовым числам $\pi \equiv 1 \pmod{(2+2i)}$, сумма — по всем гауссовым целым числам $\sigma \equiv 1 \pmod{(2+2i)}$, а N — норма в $\mathbf{Q}(i)/\mathbf{Q}$. Полагая $\sigma = 16D\lambda + \mu$, где λ пробегает все целые гауссовы числа, а μ — подходящим образом выбранное конечное множество значений, мы получаем

$$L_D(s) = \sum_{\mu} \left(\frac{D}{\mu}\right)_4 \sum_{\lambda} \bar{\sigma}\,(N\sigma)^{-s}.$$

Мы не можем пока положить $s=1$, ибо внутренний ряд расходится; поэтому мы запишем

$$\psi(\alpha, s) = \frac{\bar{\alpha}}{|\alpha|^{2s}} + \sum_{\nu \neq 0} \left\{ \frac{\bar{\alpha}+\bar{\nu}}{|\alpha+\nu|^{2s}} - \frac{\bar{\nu}}{|\nu|^{2s}} \left[1 - \frac{s\alpha}{\nu} + \frac{\bar{\alpha}(1-s)}{\bar{\nu}} \right] \right\},$$

где сходимость имеет место при $\operatorname{Re} s > 1/2$, и после некоторых преобразований мы получаем

$$L_D(s) = (16D)^{1-2s} \times$$

$$\times \left[\sum_{\mu} \left(\frac{D}{\mu}\right)_4 \psi\left(\frac{\mu}{16D}, s\right) + 4(1-s)\,\zeta_{\mathbf{Q}(i)}(s) \sum_{\mu} \frac{\bar{\mu}}{16D} \left(\frac{D}{\mu}\right)_4 \right].$$

Здесь мы, наконец, можем устремить s к 1, а так как $\psi(\alpha, 1) = \xi(\alpha)$, где ξ — дзета-функция Вейерштрасса, мы получаем

$$L_D(1) = \frac{1}{16D} \sum \left(\frac{D}{\mu}\right)_4 \xi\left(\frac{\mu}{16D}\right) - \frac{\pi}{(16D)^2} \sum \bar{\mu} \left(\frac{D}{\mu}\right)_4.$$

Это явная конечная формула, по которой можно вычислить $L_D(1)$.

Для простоты мы вывели лишь относительно громоздкую формулу для $L_D(1)$. Действительно, если Δ — произведение различных нечетных простых чисел, делящих D, то $L_D(1)$ может быть выражено в виде суммы $O(\Delta^2)$ членов вместо $O(D^2)$, как было указано выше, и, следовательно, может быть вычислено $O(\Delta^2)$ операциями. Константа, входящая в эту формулу, довольно велика, потому что каждый член очень сложный; но все же возможно вычислить $L_D(1)$ для всех $|\Delta| < 108$, что дает некоторые очень большие значения D. Кроме того, при условии $|\Delta| > 1$ второй член в (6) исчезает при подходящем выборе μ, и $L_D(1)$

может быть записано как сумма членов, содержащих $\wp$-функции Вейерштрасса. Таким образом, можно показать, что

$D^{1/4} L_D(1)/\omega$ — *целое рациональное число, если* $D > 0$;

здесь ω — вещественный период $\wp$-функции Вейерштрасса, определенной уравнением

$$\wp'^2 = 4\wp^3 - 4\wp.$$

Доказательство состоит из двух частей: число $2^{3/4}\Delta L_D(1)/\omega$ — целое алгебраическое, что следует из аддитивной формулы для $\wp$, а $D^{1/4}L_D(1)/\omega$ — рациональное число в силу «Jugendtraum» [1]) Кронекера. Подобные результаты имеют место и при $D < 0$. Отсюда, вычислив с точностью до 10^{-5}, мы можем получить точное значение $L_D(1)$ для большого числа конкретных кривых; все это дает основание предположить, что

$L_D(1) = 0$ *тогда и только тогда, когда* $g > 0$.

Однако численные результаты все же оставляют открытым для теоретических исследований вопрос о целом рациональном числе $D^{1/4}L_D(1)/\omega$ при $g = 0$. Возможные нетривиальные множители, из которых он состоит, следующие: (i) $\eta(D)$ — число рациональных точек конечного порядка на J; (ii) $Ш(D)$ — порядок группы Тэйта — Шафаревича кривой J; (iii) «вздорные» множители, соответствующие конечному множеству «плохих» простых чисел. Для кривой (5) $\eta(D)$ равно 4, если D — квадрат, и равно 2 в остальных случаях. «Плохими» называются те простые числа p, для которых J имеет плохую редукцию по модулю p; они являются делителями числа $2D$. Мы оставляем за собой право считать «бесконечное простое число» «плохим», если это будет целесообразно.

Мы должны теперь определить группу Тэйта — Шафаревича. Между главными однородными пространствами Γ фиксированной якобиевой кривой J существует отношение эквивалентности, определенное бирациональной эквивалентностью над $\mathbf{Q}$. Классы эквивалентности относительно

[1]) См. гл. XI, стр. 399.— *Прим. перев.*

этого соотношения образуют группу Вейля — Шатле [1]), которая является бесконечной коммутативной группой, все элементы которой имеют конечный порядок. Кривые Γ, содержащие точки, определенные над всеми p-адическими полями и над полем вещественных чисел, заполняют некоторые классы эквивалентности; эти классы и образуют группу Тэйта-Шафаревича. Существует гипотеза, что эта группа всегда конечна; однако эта гипотеза не доказана пока ни в одном случае; Касселс показал, что если эта группа конечна, то ее порядок должен быть точным квадратом. Вся группа определена неконструктивно и невычислима; но теоретически можно вычислить все ее элементы данного порядка (которых может быть только конечное число), и для кривой (5) полезно найти по крайней мере элементы порядков 2 и 4.

«Вздорные» множители должны быть чисто локальными, и существуют две возможности: (i) найти недостающие множители с помощью функционального уравнения — это возможно ввиду наличия комплексного умножения, (ii) получить недостающие множители произведения $\Pi\,(N_p/p)$ из рассмотрения меры Тамагава на кривой J.

Нужно подчеркнуть, что эти два подхода приводят к различным численным результатам и что второй подход применялся в работах, тогда как первый определенно нет. Чтобы определить меру Тамагава, обозначим через ω дифференциальную форму первого рода на J; она индуцирует меру ω_p на J над каждым p-адическим полем, и мера Тамагава на J по определению равна произведению

$$\prod \int_J \omega_p, \tag{7}$$

взятому по всем простым дивизорам, включая бесконечный. Здесь ω определено с точностью до произвольного множителя, и очевидно, что вклад этой константы в бесконечное произведение в итоге уничтожается.

[1]) Она может быть также определена как группа когомологий $H^1(\mathbf{Q}, J)$ — см. в гл. X подробности в аналогичном случае. Групповой закон можно определить геометрически следующим образом. Существует отображение $\Gamma \times \Gamma \to J$, которое может быть записано в обычных обозначениях как $P \times Q \to (P - Q)$. На $\Gamma_1 \times \Gamma_2$ мы определим отношение эквивалентности: $P_1 \times P_2 \sim Q_1 \times Q_2$ тогда и только тогда, когда $P_1 - Q_1 = Q_2 - P_2$. Теперь определим $\Gamma_1 + \Gamma_2$ как кривую Γ_3, каждая точка которой взаимно однозначно соответствует классу эквивалентности на $\Gamma_1 \times \Gamma_2$.

Лемма. *Если p — «хорошее» простое число, то* $\int_J \omega_p = N_p/p$.

Здесь термин «хорошее» означает, что как J, так и ω имеют хорошие редукции по mod p. Мы можем принять за ω дифференциальную форму

$$\frac{dx}{2y} = \frac{dy}{3x_2 - D}, \tag{8}$$

возможно, умноженную на p-адическую единицу. Пусть (x_0, y_0) — решение сравнения

$$y^2 \equiv x^3 - Dx \pmod{p},$$

где $y_0 \not\equiv 0 \pmod{p}$. По лемме Гензеля для каждого p-адического $x \equiv x_0 \pmod{p}$ существует единственное $y \equiv y_0 \pmod{p}$, удовлетворяющее $y^2 = x^3 - Dx$; все эти решения вносят в $\int \omega_p$ вклад, значение которого равно p-адической мере множества $x \equiv x_0 \pmod{p}$, т. е. p^{-1}. Применив аналогичные рассуждения к решениям с $y_0 = 0$ или ∞, мы и получаем доказательство леммы.

Если мы выберем дифференциальную форму на J в канонической форме (8), то множеством плохих простых чисел будут в точности те, которые делят $2D\infty$. Можно показать, что

$$\int \omega_\infty = 2\omega D^{-1/4}, \quad \text{если} \quad D > 0,$$

и аналогичный результат для $D < 0$. Тогда мера Тамагава J, определенная равенством (7), формально равна

$$2\omega D^{-1/4}\,[L_D(s)]^{-1} \prod \int \omega_p = \tau(D), \tag{9}$$

где произведение берется по всем плохим простым p. Вклад плохих простых чисел может быть найден рассуждениями, аналогичными рассуждениям в лемме, но более утомительными; можно показать, что $\int \omega_p$ для плохих простых p равен в точности числу компонент редукции J по модулю p в смысле Нерона (Modèles minimaux..., Publ. IHES, 21).

Вычисления приводят к предположению, что мера Тамагава (9) равна

$$[\eta(D)]^2/Ш(D). \tag{10}$$

Мы не можем привести прямых доводов в пользу этой гипотезы, так как $Ш(D)$ нам неизвестно; но если мы положим

$$\gamma(D) = [\eta(D)]^2/\tau(D),$$

то гипотетическое значение $Ш(D)$ обладает следующими свойствами во всех случаях, когда оно может быть вычислено. (i) $\gamma(D)$ — точный квадрат, и обычно не содержит простых множителей, отличных от 2; в большинстве случаев $\gamma(D) = 1$. (ii) Когда точная степень числа 2, на которую делится $Ш(D)$, может быть вычислена, она совпадает со степенью числа 2, на которую делится $\gamma(D)$. В особых случаях $Ш(D)$ должно делиться, а $\gamma(D)$ действительно делится на некоторую степень числа 2. Более того, сравнение гипотез для изогенных кривых $y^2 = x^3 - Dx$ и $y^2 = x^3 + 4Dx$ дает явную формулу для $Ш(-4D)/Ш(D)$, которая была впоследствии доказана Касселсом.

Удивительным в этой гипотезе является присутствие квадрата в формуле (10). Мы предполагаем найти объединение представителей элементов группы Тэйта — Шафаревича по модулю группы рациональных точек в этом объединении; мера оказывается равной скорее $\eta(D)$, чем константе.

Для описания ситуации при $g > 0$, или для более общих кривых Γ, нужно определить модифицированные L-ряды

$$L^*_\Gamma(s) = L_\Gamma(s) \Big/ \prod \int \omega_p, \tag{11}$$

в которых произведение берется по всем плохим простым числам, включая бесконечность, а $L_\Gamma(s)$ определяется по формуле (4), в которой произведение берется по всем хорошим простым числам. Если J допускает комплексное умножение, то мы можем дать явную формулу для коэффициентов степенных рядов разложения $L_\Gamma(s)$ при $s = 1$ с помощью рассуждений, аналогичных приведенным выше; единственное изменение состоит в использовании вместо дзета-функций Вейерштрасса некоторых сходящихся степенных рядов, которые, однако, не обладают интересными теоретическими свойствами.

Нелсон Стефенс, ученик Бёрча, провел вычисления для кривых вида

$$J : y^3 = x^3 - Dz^3, \tag{12}$$

которые тоже допускают комплексное умножение. Его результаты выражаются следующей формулой:

$$L^*_\Gamma(s) \approx 2^g (s-1)^g k \cdot Ш(J)/[\eta(J)]^2, \tag{13}$$

где g обозначает число независимых образующих группы $J_{\mathbf{Q}}$ бесконечного порядка, $\eta(J)$ — порядок подгруппы кручения группы $J_{\mathbf{Q}}$, $Ш(J)$ — порядок группы Тэйта — Шафаревича кривой J и k — меру образующих бесконечного порядка $J_{\mathbf{Q}}$ в следующем смысле. Пусть $P = (x, y, z)$ — рациональная точка на J, причем x, y, z — взаимно простые целые числа; положим

$$R(P) = \ln[\mathrm{Max}(|x|, |y|, |z|)].$$

Тэйт определил каноническую высоту P по формуле

$$R^*(P) = \lim n^{-2} R(nP);$$

он показал, что этот предел существует и ведет себя как квадратичная форма на аддитивной группе $J_{\mathbf{Q}}$. В частности, это дает нам билинейную форму

$$\langle P_1, P_2\rangle = \tfrac{1}{2}[R^*(P_1 + P_2) - R^*(P_1) - R^*(P_2)].$$

Если $P_1, \ldots, P_g$ — образующие бесконечного порядка в $J_{\mathbf{Q}}$, то

$$k = \det(\langle P_i, P_j\rangle);$$

это число, очевидно, не зависит от выбора базиса.

Гипотеза (13) имеет смысл для любой эллиптической кривой, хотя все доводы в ее пользу приведены для кривых с комплексным умножением. Шимура показал, что $L_\Gamma(s)$ допускает аналитическое продолжение для тех эллиптических кривых, которые могут быть параметризованы модулярными функциями, и предположил, что можно будет проверить гипотезу для некоторых из них. Все такие кривые, рассматривавшиеся в литературе, имеют $g = 0$, и легко показать, что $L_\Gamma(1) \neq 0$. Бёрч вычислил $L^*_\Gamma(1)$ для одной

из них и показал, что значение именно такое, как требует гипотеза. Но у нас нет еще ни алгоритма для нахождения таких кривых — хотя они появляются одинаковым образом,— ни возможности вычислить $L_\Gamma^*(1)$.

Естественно обобщить эти гипотезы на другие многообразия. Пусть V — полное неособое многообразие размерности n; тогда, согласно гипотезе Вейля, его локальная дзета-функция может быть записана в форме

$$\zeta_{V,p}(s) = \frac{L_{p,0}(s)\,L_{p,2}(s)\dots L_{p,2n}(s)}{L_{p,1}(s)\dots L_{p,2n-1}(s)},$$

где

$$L_{p,m}(s) = \prod (1-\alpha_{mj}p^{-s})^{-1}. \qquad (14)$$

Здесь $|\alpha_{mj}| = p^{m/2}$, и произведение (14) содержит B_m множителей, где B_m есть m-е число Бетти многообразия V. Более того, имеет место равенство

$$L_m(s) = \prod L_{p,m}(s),$$

где произведение берется по всем простым числам p, для которых V имеет хорошую редукцию по модулю p. Вообще мы не знаем, как определить множители, соответствующие плохим простым числам, и поэтому не можем получить $L_m^*(s)$; исключение составляет случай, когда V является абелевым многообразием A и $m = 1$ или $2n-1$. В этом случае мы можем действовать, как и в случае эллиптической кривой J; мы должны только теперь различать A и его дуальное многообразие $\hat{A}$, тогда как для эллиптических кривых $J = \hat{J}$. В случае когда A является произведением эллиптических кривых, непосредственное обобщение результата (13) дает нам, что

$$L_{2n-1}^*(s+n-1) = L_1^*(s) \approx 2^g (s-1)^g\, k\text{Ш}(A)/\eta(A)\eta(\hat{A}). \qquad (15)$$

Выражение знаменателя в правой части было получено из соображений двойственности, на которых основано доказательство Касселса соотношения между Ш (J_1) и Ш (J_2) для двух изогенных эллиптических кривых J_1 и J_2.

Исключая этот специальный случай, мы можем только пытаться обобщить гипотезу о том, что $L_\Gamma(s)$ имеет нуль порядка g при $s = 1$. Естественным аналогом формулы (15) для любого V является следующее утверждение.

$L_{2n-1}(s)$ имеет нуль порядка g при $s = n$, где g обозначает ранг группы рациональных точек на многообразии Пикара многообразия V.

Но дальнейшее обобщение ложно, так как, по-видимому, $L_{2n-1}(s)$ зависит не от многообразия V, а только от его многообразия Пикара.

Тэйт в своей работе [1]) высказал новую замечательную гипотезу:

$L_{2r}(s)$ имеет полюс порядка v при $s = r+1$, где v обозначает ранг группы r-циклов на V, определенных над **Q**, *по модулю алгебраической эквивалентности.*

Заметим, что $L_{2r}(s)$ сходится при $\mathrm{Re}\, s > r+1$, так что эта гипотеза имеет смысл, даже если $L_{2r}(s)$ не имеет аналитического продолжения в противоположность остальным гипотезам, которые имеют дело с точками, находящимися на расстоянии 1/2 от известной области сходимости. Гипотеза Тэйта выполняется для рациональных поверхностей и доказана им для других многообразий некоторых специальных типов. Более того, применяя ее к n-кратному произведению эллиптической кривой Г на себя, Тэйт смог описать характеристические корни α_p и $\bar{\alpha}_p$ кривой Г для различных p, и эти предсказания были проверены численно.

Существует ли аналогичная гипотеза для $L_{2r-1}(s)$? Можно надеяться ассоциировать $L_{2r}(s)$ с r-циклами по модулю алгебраической эквивалентности, а $L_{2r-1}(s)$ — с $(r-1)$-циклами, алгебраически эквивалентными нулю. Кроме того, такая гипотеза должна обобщать сформулированную выше гипотезу о $L_{2n-1}(s)$ и должна учитывать двойственность между $L_m(s)$ и $L_{2n-m}(s)$. Учитывая эти факты, можно высказать одну правдоподобную формулировку гипотезы. Пусть a_1 и a_2 — два алгебраически эквивалентных r-цикла на V; это значит, что существует неособое многообразие W, точки которого соответствуют r-циклам на V, и точки P_1 и P_2 на W, соответствующие a_1 и a_2. Мы будем говорить,

[1]) Как ни странно, опубликованной в Arithmetical algebraic geometry, Proceedings of a conference held in Purdue University, December, 5—7, 1963.

что $\mathfrak{a}_1$ и $\mathfrak{a}_2$ абелево эквивалентны, если можно выбрать W, P_1 и P_2 так, чтобы образ $P_1 \times P_2$ был единицей многообразия Альбанезе многообразия W. Известно, что это дает отношение эквивалентности, но вообще по этим вопросам доказано пока еще очень мало фактов. Наиболее естественная форма гипотезы такова:

L_{2r-1} имеет нуль порядка по крайней мере ν при $s = r$, где ν обозначает ранг группы $(r-1)$-циклов на V, определенных над $\mathbf{Q}$ и алгебраически эквивалентных 0 по модулю абелевой эквивалентности.

Это опирается на неопубликованные результаты Бомбьери и Свиннертона-Дайера о поверхностях третьего порядка и о пересечении двух квадрик размерности $2n+1$. В обоих этих случаях в гипотезе выполняется равенство. Однако вычисления показывают, что для n-кратного произведения эллиптической кривой на себя может иметь место либо неравенство, либо равенство в зависимости от вида кривой.

ГЛАВА XIII

Комплексное умножение

Ж.-П. Серр [1])

ВВЕДЕНИЕ

Центральная проблема алгебраической теории чисел состоит в том, чтобы дать явную конструкцию абелевых расширений заданного поля K. В частности, если K — поле рациональных чисел $\mathbf{Q}$, то теорема Кронекера — Вебера гласит, что максимальным абелевым расширением $\mathbf{Q}^{ab}$ поля $\mathbf{Q}$ является объединение $\mathbf{Q}^{cycl}$ всех круговых расширений. Имеет место канонический изоморфизм

$$\mathrm{Gal}\,(\mathbf{Q}^{cycl}/\mathbf{Q}) \cong \prod_p U_p.$$

Так получается в явном виде теория полей классов над полем $\mathbf{Q}$ (гл. VII, п. 5.7).

Если K — мнимое квадратичное поле, то аппарат комплексного умножения дает нам в сущности то же самое. Мы получаем расширения $K^{ab} \supset \widetilde{K} \supset K$ (здесь $\widetilde{K}$ — абсолютное поле классов, т. е. максимальное неразветвленное абелево расширение) по существу присоединением точек конечного порядка на эллиптической кривой с правым комплексным умножением.

§ 1. ТЕОРЕМЫ

Пусть E — эллиптическая кривая над полем комплексных чисел $\mathbf{C}$; ее уравнение в нормальной форме записывается так: $y^2 = 4x^3 - g_2x - g_3$. Известно, что $E \cong \mathbf{C}/\Gamma$,

[1]) Подготовлено для печати Бёрчем.

где Γ — решетка в $\mathbf{C}$. Эндоморфизмами кривой E будут умножения на элементы $z \in \mathbf{C}$, такие, что $z\Gamma \subset \Gamma$. В общем случае $\mathrm{End}\,(E) = \mathbf{Z}$; если $\mathrm{End}\,(E)$ больше, чем $\mathbf{Z}$, то $\mathrm{End}\,(E) \otimes \mathbf{Q} = K$ является мнимым квадратичным полем.

Пусть R — кольцо всех целых чисел в таком поле K; тогда $\mathrm{End}\,(E)$ образует подкольцо конечного индекса в R. Любое такое подкольцо имеет вид $R_f = \mathbf{Z} + fR$ (число $f \geqslant 1$ называется «кондуктором»); итак, если E — кривая с комплексным умножением, то найдется комплексное квадратичное поле K с кольцом целых чисел R и такое целое число f, что $\mathrm{End}\,(E) \cong R_f$. Обратно, любому подкольцу R_f соответствуют эллиптические кривые.

Теорема 1.1. *Эллиптические кривые с заданным кольцом эндоморфизмов R_f находятся во взаимно однозначном соответствии (с точностью до изоморфизма) с элементами группы* $\mathrm{Cl}\,(R_f)$.

($\mathrm{Cl}\,(R_f)$ обозначает то же самое, что и $\tilde{K}_0\,(R_f)$, а именно группу проективных модулей ранга 1 над R_f. Если $f = 1$, то это просто группа классов идеалов кольца R.)

Набросок доказательства. Кривая E определяет в силу $E \cong \mathbf{C}/\Gamma$ решетку Γ (по существу Γ — это фундаментальная группа $\pi_1\,(E)$). Решетка Γ является R_f-модулем ранга 1, кольцо эндоморфизмов которого совпадает с R_f; следовательно, Γ — проективный модуль ранга 1. Обратно, если задана решетка Γ, то $\mathbf{C}/\Gamma$ будет эллиптической кривой и $\mathrm{End}\,(\mathbf{C}/\Gamma) \cong R_f$.

Следствие. *Число h_f кривых с заданным кольцом эндоморфизмов R_f (с точностью до изоморфизма) конечно, а именно равно* $\mathrm{Card}\,(\mathrm{Cl}\,(R_f))$.

Каждой кривой E отвечает ее инвариант $j\,(E)$, так что кольцу R_f соответствует h_f таких чисел. Для простоты мы рассмотрим случай $f = 1$.

Теорема 1.2 (Вебер — Фютер).

(i) *$j\,(E)$ — целые алгебраические числа.*

(ii) *Если $\alpha = j\,(E)$ — одно из этих чисел, то поле $K\,(\alpha)$ является абсолютным полем классов поля K.*

(iii) *Группа $\mathrm{Gal}\,(K\,(\alpha)/K)$ действует на множестве чисел $\{j\,(E)\}$, соответствующих кольцу R, транзитивно.*

Аналогично обстоит дело и при $f > 1$; в частности, $j\,(E)$ остаются целыми алгебраическими числами. Сформулируем имеющиеся здесь результаты более точно. Обозначим через $\mathrm{Ell}\,(R_f)$ множество эллиптических кривых с данным кольцом эндоморфизмов R_f; если $E \cong \mathbf{C}/\Gamma \in \mathrm{Ell}\,(R_f)$, то инвариант кривой E обозначим через $j\,(\Gamma)$; решетка Γ является обратимым идеалом кольца R_f, и $j\,(\Gamma)$ зависит только от ее класса. Хассе [4] доказал следующую теорему.

Теорема 3.1. *Пусть $\mathfrak{p}$ —«хороший» простой идеал поля K, для которого $(\mathfrak{p}, f) = (1)$; пусть, далее, $\mathfrak{p}_f = \mathfrak{p} \cap R_f$ — соответствующий идеал кольца R_f. Тогда элемент Фробениуса $F\,(\mathfrak{p})$ действует на $j\,(\Gamma)$ по формуле*

$$(j\,(\Gamma))^{F(\mathfrak{p})} = j\,(\Gamma \cdot \mathfrak{p}_f^{-1}).$$

Следствие ($f = 1$). *Если $E \leftrightarrow e \in \mathrm{Cl}\,(R)$ и отображение Артина переводит $c \in \mathrm{Cl}\,(R)$ в $\sigma_c \in \mathrm{Gal}\,(K\,(\alpha)/K)$, то $\sigma_c\,(e) = e - c$.*

Короче говоря, $\mathrm{Cl}\,(R)$ действует на $\mathrm{Ell}\,(R)$ сдвигами с обратным знаком.

§ 2. ДОКАЗАТЕЛЬСТВА

Мы приведем алгебраическое доказательство этих теорем, данное Дойрингом ([1], [2]); обобщения см. в [5].

Вначале мы должны убедиться в том, что все используемое нами, определено алгебраически. Пусть, как и раньше, K будет комплексным квадратичным полем с кольцом целых чисел R. Кривая E, заданная над алгебраическим замыканием $\bar{K}$ уравнением $y^2 = 4x^3 - g_2x - g_3$, имеет инвариант $j = 1728\, g_2^3/\Delta$, где $\Delta = g_2^3 - 27g_3^2$; кольцо $\mathrm{End}\,(E)$ также корректно определено алгебраически. Мы рассматриваем множество $\mathrm{Ell}\,(R_f)$ (классов) кривых с заданным кольцом эндоморфизмов R_f.

Наше соответствие $\mathrm{Ell}\,(R_f) \leftrightarrow \mathrm{Cl}\,(R_f)$ было получено с использованием топологии поля $\mathbf{C}$; это соответствие нужно заменить каким-нибудь условием алгебраического характера. Мы утверждаем, что $\mathrm{Ell}\,(R_f)$ является аффинным пространством над $\mathrm{Cl}\,(R_f)$ (иными словами, для любых $x \in \mathrm{Ell}$ и $y \in \mathrm{Cl}$ можно определить $x - y \in \mathrm{Ell}$). Действительно,

если E — кривая и M — проективный модуль ранга 1 над R_f, то можно определить $M * E = \mathrm{Hom}(M, E)$. Более точно, возьмем резольвенту

$$R_f^m \xrightarrow{\phi} R_f^n \to M \to 0;$$

тогда $\mathrm{Hom}(R_f, E) = E$, так что $\mathrm{Hom}(M, E)$ совпадает с ядром отображения ${}^t\phi\colon E^n \to E^m$.

Доказательство теоремы 1.2. Число $j(E)$ является, конечно, алгебраическим; в самом деле, если бы оно было трансцендентным, то нашлось бы бесконечно много кривых с кольцом эндоморфизмов R_f, однако $\mathrm{Cl}(R_f)$ конечно. На самом деле числа $j(E)$ — *целые* алгебраические, но мы этого доказывать не будем (для этого необходимы иные методы; например, нужно показать существование такой модели кривой E над конечным расширением поля K, у которой всюду есть «хорошие редукции»).

Группа $G = \mathrm{Gal}(\bar{K}/K)$ действует на множестве $\mathrm{Ell}(R_f)$, сохраняя его структуру $\mathrm{Cl}(R_f)$-аффинного пространства; следовательно, G действует сдвигами. Это означает, что найдется гомоморфизм $\phi\colon G \to \mathrm{Cl}(R_f)$, такой, что действие $\sigma \in G$ в $\mathrm{Ell}(R_f)$ есть сдвиг на $\phi(\sigma)$.

Мы утверждаем следующее:

$$\phi \text{ является отображением «на».} \tag{1}$$

Если $\mathfrak{p}$ —«хороший» простой идеал, то обозначим через $F_\mathfrak{p} \in \mathrm{Cl}(R_\mathfrak{p})$ образ элемента Фробениуса при гомоморфизме ϕ:

$$F_\mathfrak{p} = \mathrm{Cl}(\mathfrak{p}). \tag{2}$$

Очевидно, что (2) влечет за собой (1); действительно, если верно (2), то $\mathrm{Cl}(\mathfrak{p}) \in \phi(G)$ для всякого хорошего $\mathfrak{p}$ и, очевидно, $\mathrm{Cl}(R_f)$ порождается всеми $\mathrm{Cl}(\mathfrak{p})$. Утверждение (1) состоит в том, что группа Галуа переставляет числа $j(E)$ транзитивно, а (1) и (2) вместе дают, что $K(j(E))$ есть абсолютное поле классов (при $f = 1$). Заметим, что фактически достаточно доказать (2) для почти всех простых идеалов $\mathfrak{p}$ степени 1; тогда из теории полей классов будет следовать справедливость (2) и для остальных $\mathfrak{p}$.

Доказательство утверждения (2). Пусть E — эллиптическая кривая, определенная над L, где L — абелево расширение поля K. Если $\mathfrak{P}$ — простой идеал поля L, не входящий в конечное множество S' «плохих» идеалов, то у E есть хорошая редукция $\tilde{E}_\mathfrak{P}$ по модулю $\mathfrak{P}$. Предположим, что $\mathfrak{P} \mid \mathfrak{p}$, где $\mathfrak{p}$ — простой идеал поля K. Если $N\mathfrak{p}$ — абсолютная норма идеала $\mathfrak{p}$, то $(\tilde{E}_\mathfrak{P})^{N\mathfrak{p}}$ получается возведением всех коэффициентов в $N\mathfrak{p}$-ю степень. Мы утверждаем, что

$$(\tilde{E}_\mathfrak{P})^{N\mathfrak{p}} \cong \mathfrak{p} * \tilde{E}_\mathfrak{P} \cong (\widetilde{\mathfrak{p} * E})_\mathfrak{P}. \tag{3}$$

Из (3) следует (2), потому что, согласно (3), $j(E)^{N\mathfrak{p}} \equiv j(\mathfrak{p} * E)$ (по модулю $\mathfrak{P}$), так что отображение Фробениуса $j(E) \mapsto j(E)^{N\mathfrak{p}}$ есть сдвиг $j(E) \mapsto j(\mathfrak{p} * E)$.

Доказательство утверждения (3). Отображение включения $\mathfrak{p} \to R_f$ индуцирует отображение $\mathfrak{p} * E \to R_f * E = E$. Это отображение является изогенией эллиптических кривых, и легко видеть, что степень его равна $N\mathfrak{p}$. Беря редукцию по модулю $\mathfrak{P}$, получаем изогению $\tilde{E} \to \widetilde{\mathfrak{p} * E}$.

Случай 1. Степень идеала $\mathfrak{p}$ равна 1, так что $N\mathfrak{p} = p$. Степень отображения $\tilde{E} \to \widetilde{\mathfrak{p} * E}$ равна p и можно показать (рассматривая касательное пространство), что оно несепарабельно. Значит, это отображение не может быть ничем иным, как отображением $\tilde{E} \to \tilde{E}^p$, задаваемым формулой $x \mapsto x^p$. Для наших приложений этого фактически достаточно, но мы разберем и второй случай.

Случай 2. Степень идеала $\mathfrak{p}$ равна 2, так что $N\mathfrak{p} = p^2$, где p — простой идеал из $\mathbf{Q}$, остающийся простым в K. Тогда можно показать, что инвариант Хассе для $\tilde{E}$ равен нулю, т. е. эта кривая не имеет точек порядка p. Отображение $\tilde{E} \to \widetilde{\mathfrak{p} * E}$, таким образом, имеет тривиаль-

ное ядро, так что оно опять чисто несепарабельно и потому является отображением $\tilde{E}$ в $\tilde{E}^{p^2}$.

Пример. Существуют 13[1]) квадратичных колец R_f с числом классов 1, а именно: для $f=1$ это $\mathbf{Q}(\sqrt{-d})$, где $d=1, 2, 3, 7, 11, 19, 43, 67, 163$; для $f=2$ это $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-3})$ и $\mathbf{Q}(\sqrt{-7})$; наконец, $\mathbf{Q}(\sqrt{-3})$ для $f=3$. Следовательно, имеются 13 кривых с комплексным умножением с рациональным инвариантом. Значения инварианта для них таковы:

$j = 2^6\cdot 3^3,\ 2^6\cdot 5^3,\ 0,\ -3^3\cdot 5^3,\ -2^{15},\ -2^{15}\cdot 3^3,\ -2^{18}\cdot 3^3\cdot 5^3,\ -2^{15}\cdot 3^3\cdot 5^3\cdot 11^3,\ -2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3,\ 2^3\cdot 3^3\cdot 11^3,\ 2^4\cdot 3^3\cdot 5^3,\ 3^3\cdot 5^3\cdot 17^3,\ -3\cdot 2^{15}\cdot 5^3.$

§ 3. МАКСИМАЛЬНОЕ АБЕЛЕВО РАСШИРЕНИЕ

Мы хотим описать максимальное абелево расширение K^{ab} поля K. Сначала испробуем $K^?$ — объединение всех полей, порожденных инвариантами эллиптических кривых из Ell (R_f), $f=1, 2, \ldots$; это поле порождается числами $j(\tau)$, где $\mathrm{Im}(\tau)>0$ и $\tau\in K$. Теперь увеличим $K^?$ добавлением корней из единицы; получаем поле $K^{??}=\mathbf{Q}^{\mathrm{cycl}}\cdot K^?$, весьма близкое к K^{ab}. Точный смысл этого высказывания устанавливает следующая теорема.

Теорема 3.1. *Группа* $\mathrm{Gal}(K^{\mathrm{ab}}/K^{??})$ *является произведением групп порядка* 2.

Теорема легко выводится из теории полей классов и результатов § 2.

Пусть теперь $\tilde{K}$ — абсолютное поле классов поля K, и пусть E — эллиптическая кривая, определенная над $\tilde{K}$, с кольцом эндоморфизмов $\mathrm{End}(E)=R$. Обозначим через L_E расширение поля $\tilde{K}$, порожденное координатами точек

[1]) Старк показал (*Proc. Nat. Acad. Sci. U.S.A.*, **57** (1967), 216—221), что не существует десятого мнимого квадратичного поля с числом классов 1. Практически одновременно Бейкер доказал (*Mathematika*, **13** (1966), 204—216) важную общую теорему, которая сводит вопрос о существовании этого поля к конечному числу операций.

конечного порядка на кривой E. Это расширение поля $\tilde{K}$ абелево, и его группа Галуа естественным образом погружается в группу $U(K)=\prod U_v(K)$, где $U_v(K)$ обозначает группу единиц поля K в конечной точке v. Согласно теории полей классов, L_E в этом случае описывается гомоморфизмом

$$\theta_E\colon I_{\tilde{K}}\to U(K),$$

где $I_{\tilde{K}}$ — группа иделей поля $\tilde{K}$. Пусть U — группа (глобальных) единиц поля K, так что $U=\{\pm 1\}$, за исключением случаев $K=\mathbf{Q}(\sqrt{-1})$ или $K=\mathbf{Q}(\sqrt{-3})$. Без особого труда можно доказать, что ограничение гомоморфизма θ_E на группу $U(\tilde{K})$ имеет вид

$$\theta_E(x)=N_{\tilde{K}/K}(x^{-1})\cdot\rho_E(x),$$

где ρ_E — гомоморфизм группы $U(\tilde{K})$ в U.

Расширение L_E и гомоморфизм ρ_E зависят от выбора кривой E. Чтобы избавиться от этого, положим $X=E/U$ (фактор кривой E по группе U — проективная прямая), и пусть L будет расширением поля $\tilde{K}$, порожденным координатами образов в X точек конечного порядка на кривой E. Это расширение не зависит от выбора E.

Теорема 3.2. *L является максимальным абелевым расширением поля K.*

Это вытекает с помощью теории полей классов из свойств гомоморфизма θ_E, отмеченных выше.

Замечание. Если порядок группы U равен 2 (соответственно 4, 6), то отображение $E\to X$ задается координатой x (соответственно x^2, x^3). Следовательно, K^{ab} порождается числами $j(E)$ и координатами x (соответственно x^2, x^3) точек конечного порядка кривой E; это легко переформулировать в аналитических терминах, используя j- и $\wp$-функции.

(Дальнейшие и более глубокие результаты, аналогичные результатам Куммера в случае полей деления круга, см. в работе [3].)

ЛИТЕРАТУРА

Дойринг (Deuring M.)
[1] Algebraische Begründung der komplexen Multiplikation, *Abh. Math. Sem. Univ. Hamburg*, **16** (1949), 32—47.
[2] Die Struktur der elliptischen Funktionenkörper und die Klassenkörper der imaginären quadratischen Zahlkörper, *Math. Ann.*, **124** (1952), 393—426.
Рамачандра (Ramachandra K.)
[3] Some applications of Kronecker's limit formulas, *Ann. Math.*, **80** (1964), 104—148.
Хассе (Hasse H.)
[4] Neue Begründung der komplexen Multiplikation, *J. reine angew. Math.*, **157** (1927), 115—139, **165** (1931), 64—88.
Шимура, Танияма (Shimura G., Tanijama V.)
[5] Complex multiplication of abelian varieties, *Publ. Math. Soc. Japan*, **6** (1961).

ГЛАВА XIV

l-расширения

К. Хёхсман

ВВЕДЕНИЕ

Пусть l — рациональное простое число, Ω — группа порядка l (запись операции мультипликативная). Если G — проконечная группа, то группу когомологий $H^i(G, \Omega)$ мы будем обозначать через $H^i(G)$, предполагая, что G действует на Ω тривиально. Если G — группа Галуа расширения K поля k, то мы иногда будем вместо $H^i(G)$ писать $H^i(K/k)$. Эти группы будут особенно интересовать нас для $i = 1, 2$ в случае, когда k есть локальное или глобальное поле, а K — его максимальное l-расширение, т. е. максимальное нормальное расширение, группа Галуа которого является про-l-группой.

§ 1. ДВЕ ЛЕММЫ

Лемма 1.1. *Рассмотрим семейство* (φ_v) *морфизмов точных последовательностей про-l-групп*

$$\begin{array}{ccccccccc} 1 & \to & R & \to & F & \to & G & \to & 1 \\ {\scriptstyle\varphi_v}\uparrow & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \to & R_v & \to & F_v & \to & G_v & \to & 1 \end{array}$$

причем предположим, что

(а) F, F_v *свободны* [1]) $(H^2(F) = H^2(F_v) = 1)$;

(б) F, F_v *построены по минимальной системе образующих; те же предположения делаются относительно* G, G_v *(отображения* $H^1(G) \to H^1(F)$ *и т. д. сюръективны).*

[1]) Определения понятий, встречающихся в этой главе, см. в [5].

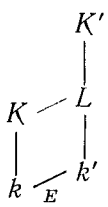
Тогда R порождается (как замкнутый нормальный делитель в F) совокупностью образов $\varphi_v(R_v)$; или, что то же самое, отображение $H^2(G) \to \coprod_v H^2(G_v)$ инъективно.

Доказательство. Аналогично предложению 26 в книге Серра [5] доказывается эквивалентность следующих утверждений: 1) R порождается образами $\varphi_v(R_v)$ и 2) отображение $H^1(R)^G \to \coprod_v H^1(R_v)$ инъективно. С другой стороны, трансгрессии (Tg) в диаграмме

$$\begin{array}{ccc} H^1(R)^G & \xrightarrow{\mathrm{Tg}} & H^2(G) \\ \downarrow & & \downarrow \\ H^1(R_v)^G & \xrightarrow{\mathrm{Tg}} & H^2(G_v) \end{array}$$

являются изоморфизмами ввиду точности последовательностей Хохшильда—Серра и наших предположений (а) и (б).

Лемма 1.2. *Пусть заданы расширения полей, связанные между собой, как показано в диаграмме (все поля — расширения Галуа поля k), причем K/k и K'/k' являются l-расширениями, а $E = \mathrm{Gal}(k'/k)$ — конечная группа порядка, взаимно простого с l. Рассмотрим естественное отображение*



$$\theta\colon \mathrm{Gal}(K'/k') \to \mathrm{Gal}(K/k).$$

Предположим, что

а) $H^1(K'/K) = 1$;

б) Res: $H^2(K'/k) \to H^2(K'/L)$ — *тривиальное отображение. Тогда θ индуцирует изоморфизм*

$$\theta^*\colon H^2(K/k) \to H^2(K'/k')^E.$$

Доказательство. θ^* есть композиция отображений

$$\mathrm{Inf}\colon H^2(K/k) \to H^2(K'/k)$$

и

$$\mathrm{Res}\colon H^2(K'/k) \to H^2(K'/k')^E.$$

Биективность отображения Res вытекает из того, что число l и порядок группы E взаимно просты. Чтобы убедиться в этом, можно использовать сдвиг размерности в конечных подрасширениях и последовательность Хохшильда — Серра. Условие (а) дает точность соответствующей Inf-Res-последовательности в размерности 2 и, следовательно, инъективность отображения Inf. Его сюръективность следует теперь из условия (б) и инъективности ограничения коцикла с группы $\mathrm{Gal}(K'/K)$ на подгруппу $\mathrm{Gal}(K'/L)$.

§ 2. ЛОКАЛЬНЫЕ ПОЛЯ

Пусть k — конечное расширение поля рациональных p-адических чисел $\mathbf{Q}_p$, а K — максимальное l-расширение поля k, и пусть $G = \mathrm{Gal}(K/k)$.

Пусть δ—ранг подгруппы элементов порядка l группы k^* и

$$n = \begin{cases} [k\colon \mathbf{Q}_p], & \text{если } l = p, \\ 0 & \text{в противном случае.} \end{cases}$$

Обозначим через d^1 и d^2 соответственно число образующих и число определяющих соотношений в группе G, т. е. ранги групп $H^1(G)$ и $H^2(G)$.

Теорема 2.1. $d^1 = n + \delta + 1$, $d^2 = \delta$.

Доказательство. По теореме Бернсайда о базисе достаточно подсчитать число образующих в группе $G/G^l[G, G]$, что, согласно теории полей классов, сводится к рассмотрению группы $k^*/(k^*)^l$.

Слагаемое 1 в формуле для d^1 появляется за счет бесконечной циклической группы, порожденной простым элементом, а $n + \delta$ — за счет группы U единиц; действительно, U является прямым произведением конечной циклической группы и свободного $\mathbf{Z}_p$-модуля ранга $[k : \mathbf{Q}_p]$ (см. [6], ч. II, 15.5). Итак, d^1 вычислено.

Чтобы найти d^2, рассмотрим два случая.

(1) $\delta = 1$. Вложение Ω в K дает точную последовательность

$$1 \to \Omega \xrightarrow{i} K^* \xrightarrow{l} K^* \to 1,$$

где l обозначает возведение в l-ю степень. В силу «теоремы Гильберта 90» мы получаем изоморфизм

$$i\colon H^2(G) \to H^2(G, K^*)_l,$$

где индекс l обозначает подгруппу элементов порядка l. Это, согласно локальной теории полей классов для групп порядка l, брауэровы классы порядка l.

(2) $\delta = 0$. Обозначив поле, полученное присоединением всех корней l-й степени из единицы, через k', мы получим с помощью конструкции его максимального l-расширения K' диаграмму, аналогичную диаграмме в лемме 1.2. Выполнение условий этой леммы легко проверяется.

(а) $H^1(K'/K) = \mathrm{Hom}(\mathrm{Gal}(K'/K), \Omega) = 1$, так как существование нетривиального элемента повлекло бы за собой существование собственного l-расширения поля K.

(б) Отображение ограничения группы $H^2(K'/k')$ в $H^2(K'/L)$ тривиально, так как элементы этих групп, согласно случаю (1), можно отождествить с брауэровыми классами порядка l, которые представляют единицу группы Брауэра поля L.

По лемме 1.2

$$H^2(G) \cong H^2(K'/k')^E.$$

Группа E — циклическая; пусть ε — ее образующая. Наше вложение

$$i\colon \Omega \to K'^*$$

не является ε-отображением. В самом деле, для ω из Ω мы имеем

$$i(\varepsilon\omega) = i(\omega) = [\varepsilon i(\omega)]^m,$$

где $m \in \mathbf{Z}$ таково, что $\varepsilon^{-1}\zeta = \zeta^m$, если ζ — корень l-й степени из единицы. Соответственно этому мы получаем коммутативную диаграмму

$$\begin{array}{ccc} H^2(K'/k') & \xrightarrow{i} & \mathrm{Br}(k') \\ {\scriptstyle\varepsilon}\downarrow & & \downarrow{\scriptstyle\varepsilon\cdot m} \\ H^2(K'/k') & \xrightarrow{i} & \mathrm{Br}(k') \end{array}$$

т. е. для любого $\alpha \in H^2(K'/k')$ имеет место

$$\mathrm{inv}\,[i(\alpha^\varepsilon)] = m \cdot \mathrm{inv}\,[(i\alpha)^\varepsilon] = m \cdot \mathrm{inv}\,[i\alpha];$$

это показывает, что если $\alpha \in H^2(K'/k')^E$, то $i\alpha = 1$, и потому $\alpha = 1$.

Замечание. Инварианты d^1 и d^2 и показатель l^s подгруппы элементов порядка l в группе k^* определяют группу G полностью, кроме случая $\delta = 1$, $l^s = 2$. Если $\delta = 0$, то мы имеем дело со свободной группой, и замечание тривиально. Если $\delta = 1$, то группа G обладает следующими свойствами:

(1) $H^2(G) \cong \Omega$;

(2) спаривание $H^1(G) \times H^1(G) \to \Omega$, определяемое $\cup$-умножением и свойством (1), невырождено. (В силу изоморфизма Куммера $H^1(G) \simeq k^*/(k^*)^l$ это спаривание соответствует символу Гильберта для вычета степени l.) Про-l-группы, имеющие конечное число d образующих и удовлетворяющие условиям (1) и (2), называются группами Демушкина. Если G — группа Демушкина, причем показатель l^s подгруппы элементов конечного порядка группы $G/[G, G]$ больше, чем 2, то образующие $x_1, \ldots, x_d$ в G можно выбрать так, что все соотношения, определяющие G, примут вид

$$x_1^{l^s}[x_1, x_2] \ldots [x_{d-1}, x_d] = 1,$$

где квадратные скобки обозначают коммутаторы. Если $l^s = 2$, то существуют различные типы групп, зависящие от более тонких инвариантов. Подробности см. в [3] и [5].

В настоящем контексте вся эта техника необходима только при $l = p$. Если $l \neq p$, то для того чтобы δ было равно единице, порядок q поля вычетов поля k должен быть сравним с единицей по модулю l. Пусть $l^s \mid q - 1$, причем s максимально, и ζ — первообразный корень l^s-й степени из единицы в k. Тогда G имеет две образующие σ и τ, символы норменных вычетов которых будут π (простой элемент) и ζ. Каждое конечное подрасширение L над k метабелево, и его неразветвленная часть T остается неподвижной при действии τ. Поэтому $\tau = (\xi, L/T)$, где за $\xi \in T$ может быть выбран корень из единицы. Значит, $\sigma\tau\sigma^{-1} = (\sigma\xi, L/T) = (\xi^q, L/T) = \tau^q$, причем это соотношение выполняется для каждого конечного расширения поля L и, следовательно, для k.

§ 3. ГЛОБАЛЬНЫЕ ПОЛЯ

Пусть k — конечное расширение поля $\mathbf{Q}$, а K — максимальное l-расширение поля k с группой Галуа G.

Для каждого нормирования v из k рассмотрим пополнение k_v и его максимальное l-расширение K_v (здесь мы отклоняемся от стандартных обозначений !) с группой Галуа G_v.

Мы фиксируем продолжение w нормирования v на K и получаем вложение

$$\varphi_v\colon\ G_v \longrightarrow G,$$

образ которого является группой разложения для w.

Пусть δ, δ_v — ранги подгрупп элементов порядка l соответственно в группах k^* и k_v^*.

Теорема 3.1. *φ_v индуцируют мономорфизм*

$$\varphi^*\colon\ H^2(G) \longrightarrow \coprod_v H^2(G_v),$$

коядро которого имеет ранг δ.

Доказательство. Мы будем действовать так же, как при доказательстве теоремы 2.1.

(1) $\delta = 1$. Вложение $i\colon \Omega \to K^*$ и определяемые им вложения $i_v\colon \Omega \to K_v^*$ позволяют написать коммутативные диаграммы

$$\begin{array}{ccc} H^2(G) & \longrightarrow & H^2(G,\ K^*)_l \\ \downarrow & & \downarrow \\ H^2(G_v) & \longrightarrow & H^2(G_v,\ K_v^*)_l \end{array}$$

биективность горизонтальных стрелок в которых доставляется «теоремой Гильберта 90» при помощи точной последовательности

$$1 \longrightarrow \Omega \xrightarrow{i} K^* \xrightarrow{l} K^* \longrightarrow 1$$

и ее локальных копий. Мы используем правые стороны этих диаграмм вместе с характеризацией Хассе брауэровых классов их локальными инвариантами для того, чтобы получить точную последовательность

$$1 \longrightarrow H^2(G) \xrightarrow{\varphi^*} \coprod_v H^2(G_v) \xrightarrow{\chi} \Omega \longrightarrow 1,$$

где χ обозначает сумму инвариантов, записанных мультипликативно.

(2) $\delta = 0$. Вновь мы присоединяем корни l-й степени из единицы, получая поле k'. Расширим каждую точку v' поля k' до точки w' максимального l-расширения K', так что w' согласуется с уже выбранным нормированием w поля K. Мы получаем такую же диаграмму, как в лемме 2, для глобальных полей и для каждой точки v' — аналогичные локальные диаграммы для расширений K_v над k_v и K'_v над k'_v соответственно с группами Галуа G_v и $G'_{v'}$. Правило действия $\varphi_v \circ \theta_{v'} = \theta \circ \varphi'_{v'}$ $(v' \mid v)$ доставляет коммутативную диаграмму

$$\begin{array}{ccc} H^2(G') & \xrightarrow{\varphi^*_{v'}} & H^2(G'_{v'}) \\ {\scriptstyle\theta^*}\downarrow & & \downarrow{\scriptstyle\theta^*_{v'}} \\ H^2(G) & \xrightarrow{\varphi^*_v} & H^2(G_v) \end{array}$$

для каждого v'.

Собирая все эти диаграммы вместе и принимая во внимание инъективность θ^* (ибо $H^1(K'/K) = 1$ опять-таки ввиду максимальности K), мы выводим инъективность отображения $\varphi^* = \coprod_v \varphi_v^*$ из инъективности отображения $\coprod_{v'} \varphi_{v'}^*$, которая была установлена в (1).

Чтобы доказать сюръективность, заметим, что, согласно лемме 1.2, образ отображения θ^* совпадает с $H^2(G')^E$; условия (б) проверяются, как и раньше, после отождествления групп $H^2(K'/k')$, $H^2(K'/L)$ с подгруппами элементов порядка l групп Брауэра над полями k' и L соответственно; эти группы становятся тривиальными (локально всюду) после ограничения на L. Затем заметим, что $H^2(G_v) \neq 1$, т. е. $\delta_v = 1$, или, что то же самое, v вполне распадается в поле k', так что мы можем сосредоточить внимание на множестве S_0 только таких точек. Мы имеем диаграмму

$$\begin{array}{ccc} H^2(G')^E & \longrightarrow & \coprod_{v'} H^2(G'_{v'}) \\ {\scriptstyle\theta^*}\uparrow & & \uparrow \\ H^2(G) & \xrightarrow{\varphi^*} & \coprod_{v \in S_0} H^2(G_v) \end{array}$$

где θ^* — изоморфизм, и докажем сюръективность φ^* следующим образом: мы покажем, что отображение

$$H^2(G) \to \coprod_{v \in S_0 \setminus b} H^2(G_v)$$

перестанет быть инъективным, если из произведения справа изъять хотя бы одну точку $b \in S_0$. Это сводится к нахождению нетривиального элемента $\alpha \in H^2(G)^E$, такого, что $\varphi_{v'}^*(\alpha) = 1$ для всех v', не лежащих над b.

Используя те же соображения, что и в конце доказательства теоремы 2.1, и введенные там обозначения, находим

$$\mathrm{inv}_{\varepsilon v'}[i(\alpha^\varepsilon)] = m \cdot \mathrm{inv}_{v'}[i\alpha]$$

(*N.B.*: на этот раз ε действует на точках тоже). Поэтому $\alpha \in H^2(G')^E$ тогда и только тогда, когда $\mathrm{inv}_{\varepsilon v'}[i\alpha] = m \cdot \mathrm{inv}_{v'}[i\alpha]$. Нужное нам α мы определим, задав все инварианты для $i\alpha$:

$$\mathrm{inv}_{v'}[i\alpha] = \begin{cases} 0, & \text{если } v' \nmid b, \\ \dfrac{m^j}{l}, & \text{если } v' = \varepsilon^j b' \ (j = 0, \ldots, r-1), \end{cases}$$

где b' — фиксированная точка, лежащая над b, а $r = [k' : k]$. Так как

$$\sum_{j=0}^{r-1} m^j \equiv 0 \pmod{l},$$

то этим определен брауэров класс $i\alpha$ порядка l.

Замечание. По лемме 1.1 этот результат может быть интерпретирован как теорема Коха (см. [2]) о соотношениях, определяющих группу G. Если представить G и G_v как факторгруппы свободных групп F и F_v и расширить φ_v до морфизма соответствующих точных последовательностей, как в лемме 1.1, то из теоремы 3.1 будет следовать, что R порождается образами $\varphi_v(R_v)$. Далее, R_v порождается единственным соотношением r_v, которое становится тривиальным при $\delta_v = 0$ (ср. теорему 2.1). Теорема 3.1 утверждает также, что $\varphi_v(r_v)$ образуют минимальную систему соотношений, если $\delta = 0$, а если $\delta = 1$, то минимальная система получается из этой исключением одного из них.

Добавление

ОГРАНИЧЕННОЕ ВЕТВЛЕНИЕ

Пусть S — множество точек поля k, рассматривавшееся в предыдущем параграфе, и пусть $K(S)$ — максимальное l-расширение поля k, неразветвленное вне S. Таким образом, мы уже имели дело с этими понятиями в случае, когда S — совокупность всех точек; другой крайний случай, когда S пусто, составляет предмет гл. IX. Мы хотим закончить наше изложение несколькими замечаниями об общем случае.

Кох в работе [2] изучает $G(S) = \mathrm{Gal}(K(S)/k)$ как факторгруппу группы G. Образующие группы G получаются из символов норменного вычета для образующих группы I/k^*I^l (I — группа иделей поля k). Более подробно: рассматривается точная последовательность

$$1 \to U/(k^*I^l \cap U) \to I/k^*I^l \to \mathrm{Cl}/\mathrm{Cl}^l \to 1$$

(U — группа иделей единиц; Cl — группа классов идеалов), и в качестве образующих выбираются: (1) прообразы базиса конечного коядра; (2) для каждой точки v — базис B_v группы U_v/U_v^l. Естественное отображение

$$G \to G(S)$$

теперь можно задать, положив $\tau = 1$, коль скоро $\tau \in B_v$, $v \notin S$ (элементы из B_v лежат в группе инерции точки v).

Если бы у нас было описание группы G в терминах этих образующих и некоторых определенных соотношений, мы получили бы соответствующее описание $G(S)$ простыы вычеркиванием всюду ненужного τ. Но теорема 3.1 дает соотношения для G, только если мы исходим из минимальной системы образующих; а наша система не минимальна! Действительно, некоторое конечное число элементов из $\bigcup_v B_v$ должно быть исключено, чтобы добиться минимальности, а для применимости описанного метода нужно, чтобы S было достаточно велико, т. е. содержало те v, которые соответствуют этим элементам. Тем не менее этот метод достаточно силен, он дает основное неравенство Шафаревича ([7], теорема 5), а в некоторых специальных слу-

чаях ведет к удовлетворительному описанию группы $G(S)$. Подробности см. в [2].

У Брумера [1] методы, использованные нами для доказательства теоремы 3.1 (случай (1)), непосредственно применяются к более общей задаче. Предполагается, что $\delta_k = 1$ и что S содержит все нормирования, лежащие над l. Тогда извлечение корней l-й степени из S-единиц ведет к расширениям, не разветвленным вне S и, таким образом, к точной последовательности

$$1 \to \Omega \xrightarrow{i} E(S) \xrightarrow{l} E(S) \to 1,$$

где $E(S)$ обозначает S-единицы поля $K(S)$. Переходя к когомологиям, получим точную последовательность

$$1 \to {}_lH^1(G(S),\ E(S)) \to H^2(G(S)) \xrightarrow{i} H^2(G(S),\ E(S))_l \to 1,$$

где для абелевой группы X через ${}_lX$ обозначена факторгруппа X/X^l. Нетрудно отождествить последний член с подгруппой группы $\mathrm{Br}(k)_l$, а более точно — с теми брауэровыми классами порядка l, чьи локализации тривиальны вне S. Далее, если $H^1(G(S), E(S))$ заменить на изоморфную ей группу классов идеалов поля k по модулю классов, содержащих элементы из S, и обозначить эту последнюю группу через $A(S)$, то получается точная последовательность

$$1 \to {}_lA(S) \to H^2(G(S)) \to \coprod_{v \in S} H^2(G_v) \xrightarrow{\chi} \Omega \to 1,$$

аналогичная последовательности в доказательстве теоремы 2.1 (случай (1)).

Более трудный случай ($\delta = 0$) пока еще не поддается исследованию этими методами.

ЛИТЕРАТУРА

Брумер (Brumer A.)
[1] Galois groups of extensions of algebraic number fields with given ramification (не опубликовано).

Кох (Koch H.)
[2] L-Erweiterungen mit vorgegebenen Verzweigungsstellen, *J. reine angew. Math.*, **219** (1965), 30—61.

Лабют (Labute J.)
[3] Classifikation des groupes de Demuškin, *Comptes rendues*, **260** (1965), 1043—1046.

Серр (Serre J.-P.)
[4] Strukture de certains pro-p-groupes, Séminaire Bourbaki, exp. 252, 1963.
[5] Cohomologie galoisienne, Lecture notes in Mathematics, 5. Springer-Verlag, Berlin, 1964. (Русский перевод: Серр Ж.-П., Когомологии Галуа, «Мир», М., 1968.)

Хассе (Hasse H.)
[6] Zahlentheorie, Akademie-Verlag, Berlin, 1962.

Шафаревич И. Р. (Šafarevič I. R.)
[7] Extensions with given ramification, *Publs. IHES*, **18** (1963), 71—95.

Упражнения [1]

УПРАЖНЕНИЕ 1. СИМВОЛ СТЕПЕННОГО ВЫЧЕТА (ЛЕЖАНДР, ГАУСС И ДР.)

Это упражнение опирается на гл. VII, § 3, и теорию Куммера (гл. III, § 2). Пусть m — фиксированное натуральное число и K — фиксированное глобальное поле, содержащее группу μ_m корней m-й степени из единицы. Пусть далее S — множество тех нормирований поля K, которые или делят m, или являются архимедовыми. Если $a_1, \ldots, a_r$ — элементы из K^*, мы обозначим через $S(a_1, \ldots, a_r)$ множество всех элементов из S и тех нормирований v, для которых $|a_i|_v \neq 1$ при некотором i. Для $a \in K^*$ и $\mathfrak{b} \in I^{S(a)}$ мы определим символ $\left(\frac{a}{\mathfrak{b}}\right)$ следующим равенством:

$$\left(\sqrt[m]{a}\right)^{F_{L/K}(\mathfrak{b})} = \left(\frac{a}{\mathfrak{b}}\right)\sqrt[m]{a},$$

где $L = K\left(\sqrt[m]{a}\right)$.

Упражнение 1.1. Показать, что $\left(\frac{a}{\mathfrak{b}}\right)$ является корнем m-й степени из 1 и не зависит от выбора $\sqrt[m]{a}$.

Упражнение 1.2. Вычисляя в поле $L' = K\left(\sqrt[m]{a}, \sqrt[m]{a'}\right)$ и используя результаты из гл. VII, п. 3.2, при $K' = K$ и $L = K\left(\sqrt[m]{a}\right)$, показать, что

$$\left(\frac{aa'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a'}{\mathfrak{b}}\right), \quad \text{если } \mathfrak{b} \in I^{S(a, a')}.$$

[1]) Эти упражнения относятся главным образом к гл. VII. Их подготовили Тэйт и Серр уже после конференции. Упражнения описывают в общих чертах некоторые важные результаты и интересные приложения, для обсуждения которых на конференции, к сожалению, не хватило времени.

Упражнение 1.3. Показать, что

$$\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a}{\mathfrak{b}'}\right), \quad \text{если } \mathfrak{b} \in I^{S(a)}.$$

Следовательно,

$$\left(\frac{a}{\mathfrak{b}}\right) = \prod_{v \notin S(a)} \left(\frac{a}{v}\right)^{n_v}, \quad \text{если } \mathfrak{b} = \sum n_v v.$$

Упражнение 1.4 (*обобщение критерия Эйлера*). Если $v \notin S(a)$, то $m \mid (Nv - 1)$, где $Nv = [k(v)]$, и $\left(\frac{a}{v}\right)$ является именно тем корнем m-й степени из единицы, для которого

$$\left(\frac{a}{v}\right) \equiv a^{\frac{Nv-1}{m}} \pmod{\mathfrak{p}_v}.$$

Упражнение 1.5 (*объяснение термина «символ степенного вычета»*). Для $v \notin S(a)$ следующие утверждения эквивалентны:

(i) $\left(\frac{a}{v}\right) = 1$;

(ii) сравнение $x^m \equiv a \pmod{\mathfrak{p}_v}$ разрешимо при $x \in \mathfrak{o}_v$;

(iii) уравнение $x^m = a$ разрешимо при $x \in K_v$.

(Воспользоваться тем, что $k(v)^*$ — циклическая группа порядка $(Nv - 1)$, а также леммой Гензеля, гл. II, добавление B.)

Упражнение 1.6. Если $\mathfrak{b}$ — целый идеал, взаимно простой с m, то

$$\left(\frac{\zeta}{\mathfrak{b}}\right) = \zeta^{\frac{N\mathfrak{b}-1}{m}} \quad \text{для } \zeta \in \mu_m.$$

Сделать это сначала с помощью упражнения 1.4 в случае, когда $\mathfrak{b} = v$ — простой идеал. Затем в общем случае $\mathfrak{b} = \sum n_v v$ заметить, что при $Nv = 1 + mr_v$ имеет место сравнение

$$N\mathfrak{b} = \prod (1 + mr_v)^{n_v} \equiv 1 + m \sum n_v r_v \pmod{m^2}.$$

Упражнение 1.7. Если a и $\mathfrak{b} \in I^{S(a)}$ — целые и $a' \equiv a \pmod{\mathfrak{b}}$, то

$$\left(\frac{a'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right).$$

Упражнение 1.8. Показать, что закон взаимности Артина (гл. VII, п. 3.3) для простого куммерова расширения $L=K(\sqrt[m]{a})$ включает следующее утверждение: *если* $\mathfrak{b}$, $\mathfrak{b}'\in I^{S(a)}$ *и* $\mathfrak{b}'\mathfrak{b}^{-1}=(c)$ — *главный идеал такого элемента* $c\in K^*$, *что* $c\in(K_v^*)^m$ *при всех* $v\in S(a)$, *то* $\left(\frac{a}{\mathfrak{b}'}\right)=\left(\frac{a}{\mathfrak{b}}\right)$. Заметить, что для $v\notin S$ условие $c\in(K_v^*)^m$ выполняется, если $c\equiv 1\pmod{\mathfrak{p}_v}$.

Упражнение 1.9. Обратимся к случаю $K=\mathbf{Q}$ и $m=2$. Пусть a, b, ... обозначают произвольные ненулевые целые рациональные числа, и пусть P, Q, ... — *положительные* нечетные целые рациональные числа. Для $(a, P)=1$ символ $\left(\frac{a}{P}\right)=\left(\frac{a}{(P)}\right)=\pm 1$ определен, мультипликативен по каждому аргументу в отдельности и удовлетворяет неравенству

$$\left(\frac{a}{P}\right)=\left(\frac{b}{P}\right),\quad \text{если } a\equiv b\pmod P.$$

Закон взаимности Артина для $\mathbf{Q}(\sqrt{a})/\mathbf{Q}$ влечет за собой то, что

$$\left(\frac{a}{P}\right)=\left(\frac{a}{Q}\right),\quad \text{если } P\equiv Q\pmod{8a_0}, \qquad (*)$$

где a_0 — «нечетная часть от a», т. е. $a=2^n a_0$, где a_0 нечетно. (Использовать то, что числа, которые $\equiv 1\pmod 8$, являются 2-адическими квадратами.)

Упражнение 1.10. Из упражнения 1.9 легко вывести классический квадратичный закон взаимности:

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}},\quad \left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}} \text{ и } \left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

В самом деле, формула (*), указанная выше, позволяет вычислить символ $\left(\frac{a}{P}\right)$ как функцию от P при каждом фиксированном a за конечное число шагов; полагая $a=-1$ и 2, можно легко проверить первые два утверждения. Для

доказательства третьего определим символ

$$\langle P, Q\rangle=\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)\quad \text{при}\quad (P, Q)=1.$$

После этого проверим, что если $P\equiv Q\pmod 8$, то

$$\langle P, Q\rangle=\left(\frac{-1}{Q}\right)$$

и исследуемая формула верна. Полагая $Q=P+8a$, можно найти с помощью утверждения 1.9, что в действительности

$$\left(\frac{Q}{P}\right)=\left(\frac{8a}{P}\right)=\left(\frac{8a}{Q}\right)=\left(\frac{-P}{Q}\right).$$

Если теперь даны произвольные взаимно простые числа P и Q, то можно найти такое R, что $RP\equiv Q\pmod 8$ и $(R, Q)=1$ (и даже такое, что $R\equiv 1\pmod Q$) и, как мы видели,

$$\langle P, Q\rangle\langle R, Q\rangle=\langle PR, Q\rangle=\left(\frac{-1}{Q}\right).$$

Фиксируя R и изменяя P с сохранением условия $(P, Q)=1$, мы убеждаемся, что символ $\langle P, Q\rangle$ зависит только от $P \pmod 8$. В силу симметрии (и того факта, что классы вычетов нечетных чисел по mod 8 могут быть представлены числами, взаимно простыми с произвольно заданным числом) мы видим, что символ $\langle P, Q\rangle$ зависит только от $Q \pmod 8$. Таким образом, все свелось к небольшому конечному числу шагов, проверку которых мы оставляем читателю. Следующие упражнения описывают общий метод, которым могут быть заменены эти рассмотрения частного порядка.

УПРАЖНЕНИЕ 2. СИМВОЛ НОРМЕННОГО ВЫЧЕТА (ГИЛЬБЕРТ, ХАССЕ)

Мы предположим известным закон взаимности для куммеровых расширений и используем результаты § 6 из гл. VII. Символы m, K, S и $S(a_1, \ldots, a_r)$ имеют тот же смысл, что и в упражнении 1. Для a и $b\in K^*$ и любого нормирования v поля K определим символ $(a, b)_v$ следующим равенством:

$$(\sqrt[m]{a})^{\psi_v(b)}=(a, b_v\cdot)\sqrt[m]{a},$$

где ψ_v: $K_v^* \to G^v$ — локальное отображение Артина, ассоциированное с куммеровым расширением $K(\sqrt[m]{a})/K$.

Упражнение 2.1. Показать, что $(a, b)_v$ является корнем m-й степени из 1, который не зависит от выбора $\sqrt[m]{a}$.

Упражнение 2.2. Показать, что $(a, b)_v (a, b')_v = (a, bb')_v$ и $(a, b)_v (a', b)_v = (aa', b)_v$.

Таким образом, для каждого нормирования v поля K мы имеем билинейное отображение из $K^* \times K^*$ в группу μ_m корней m-й степени из 1.

Упражнение 2.3. Показать, что $(a, b)_v = 1$, если либо a, либо b принадлежит $(K_v^*)^m$ и, следовательно, что существует единственное билинейное продолжение символа $(a, b)_v$ на $K_v^* \times K_v^*$.

Это продолжение непрерывно в v-адической топологии и может быть описано конечной таблицей значений, потому что группа $K_v^*/(K_v^*)^m$ конечна (порядка $m^2/|m|_v$, где $|m|_v$ — значение нормирования v для числа m). Более того, продолженная на $K_v^* \times K_v^*$ функция может быть описана чисто локально, т. е. она не зависит от поля K, пополнением которого является K_v (потому что то же верно и для ψ_v), и индуцирует *невырожденное* спаривание группы $K_v^*/(K_v^*)^m$ с собой в группу μ_m; мы, однако, не будем использовать эти факты из локальной теории полей классов в большинстве пунктов этого упражнения. Для общего рассмотрения символа $(a, b)_v$, а также для некоторых явных формул, на которых основывается это рассмотрение в специальных случаях, можно обратиться к [9], стр. 53—123, [8], стр. 212—221, и [1], гл. 12. Символ $(a, b)_v$, определенный здесь, совпадает с символом Хассе и Серра, но отличается от символа, введенного в книге Артина — Тэйта. В этой же связи укажем на то, что локальные отображения Артина ψ_v совпадают с введенными в книгах Серра и Артина — Тэйта, но отличаются от тех, что введены в книге Хассе.

Упражнение 2.4. Показать, что $(a, b)_v = 1$, если b является нормой из расширения $K_v(\sqrt[m]{a})/K_v$ (см. гл. VII, п. 6.2; обратное утверждение также верно в силу локальной теории полей классов, но это не следует непосредственно из глобального закона взаимности).

Упражнение 2.5. Если $a + b \in (K_v^*)^m$, то $(a, b)_v = 1$; в частности, $(a, -a)_v = 1 = (a, 1-a)_v$. (Это следует из чисто алгебраической леммы: *пусть F — поле, содержащее группу μ_m корней m-й степени из единицы, и пусть $a \in F^*$. Тогда для каждого $x \in F$ элемент $x^m - a$ является нормой из $F(\sqrt[m]{a})$.* В самом деле, пусть $\alpha^m = a$.

Отображение $\sigma \mapsto \alpha^\sigma/\alpha$ есть изоморфизм группы Галуа на подгруппу $\mu_d \subset \mu_m$ и не зависит от выбора α. Следовательно, если (ζ_i) является системой представителей классов смежности группы μ_m по подгруппе μ_d, то для каждого $x \in F$ имеет место равенство

$$x^m - a - \prod_{\zeta \in \mu_m} (x - \zeta a) = N_{F(\alpha)/F}\left(\prod_{i=1}^{m/d} (x - \zeta_i \alpha)\right),$$

что и требовалось доказать.)

Упражнение 2.6. Показать, что $(a, b)_v (b, a)_v = 1$. (Воспользоваться билинейностью для $1 = (ab, -ab)_v$.)

Упражнение 2.7. Если нормирование v архимедово, то $(a, b)_v = 1$, за исключением случая, когда поле K_v вещественно, $m = 2$ и $a < 0$, $b < 0$ в K_v. (В этом случае на самом деле $(a, b)_v = -1$; см. замечание в упражнении 2.4. Обратить внимание на то, что при $m > 2$ поле K_v комплексно при каждом архимедовом нормировании v.)

Упражнение 2.8. (*Связь между символами норменного и степенного вычетов.*) Если $v \notin S(a)$, то $(a, b)_v = \left(\frac{a}{v}\right)^{v(b)}$; в частности, $(a, b)_v = 1$, если $v \notin S(a, b)$. (Определение символов S, $S(a)$ и др. см. в первых строках упражнения 1. Результат следует из описания локального отображения Артина в терминах автоморфизма Фробениуса для неразветвленного случая. Более общо

$$v \in S \Rightarrow (a, b)_v = \left(\frac{c}{v}\right),$$

где $c = (-1)^{v(a)v(b)} a^{v(b)} b^{-v(a)}$ является единицей в K_v, били-

нейно зависящей от a и b. Чтобы это доказать, положим $a=\pi^{v(a)}a_0$ и $b=\pi^{v(b)}b_0$, где $v(\pi)=1$, и преобразуем $(a, b)_v$ по вышеуказанным правилам; о геометрической аналогии, упомянутой в п. 3.6 гл. VII см. [8], гл. III, § 4).

Упражнение 2.9. (*Формула произведения.*) Для $a, b \in K^*$ имеет место равенство $\prod (a, b)_v = 1$, где произведение берется по всем нормированиям поля K.

Упражнение 2.10. (*Общий закон степенной взаимности.*) Для любых a и b в группе K^* положим

$$\left(\frac{a}{b}\right)=\prod_{v\notin S(a)}\left(\frac{a}{v}\right)^{v(b)}=\left(\frac{a}{(b)^{S(a)}}\right),$$

где $(b)^s$ определено в гл. VII, п. 3.2.

Предостережение. Для символа $\left(\frac{a}{b}\right)$, определенного в такой общности, правило $\left(\frac{aa'}{b}\right)=\left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$ не всегда выполняется, но оно справедливо в случае, когда $S(b)\cap S(a, a')=S$, и, в частности, если b взаимно просто с a и a'. Другое правило — $\left(\frac{a}{bb'}\right)=\left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$ — выполняется в общем случае.

Используя упражнения 2.6, 2.8 и 2.9, доказать, что

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1}=\prod_{v\in S(a)\cap S(b)}(b, a)_v.$$

В частности,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1}=\prod_{v\in S}(b, a)_v, \text{ если } S(a)\cap S(b)=S, \qquad (*)$$

и

$$\left(\frac{\lambda}{b}\right)=\prod_{v\in S}(\lambda, b)_v, \quad \text{если } S(\lambda)=S.$$

Упражнение 2.11. Если $K=\mathbf{Q}$ и $m=2$, то $S=\{2, \infty\}$ и для $P>0$, как и в упражнении 1.10, мы имеем $(x, P)_\infty=1$. Следовательно, результаты упражнения 1.10

эквивалентны следующим соотношениям:

$$(-1, P)_2=(-1)^{\frac{P-1}{2}}, \quad (2, P)_2=(-1)^{\frac{P^2-1}{8}},$$
$$(P, Q)_2=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

для нечетных P и Q. С другой стороны, эти формулы легко устанавливаются при локальных рассмотрениях в поле $\mathbf{Q}_2$. В частности, тот факт, что $(1+4c, b)_2=(-1)^{v_2(b)c}$, из которого легко вычисляется значение $(a, b)_2$ для всех a и b на основе упражнений 2.2, 2.5 и 2.6, является специальным случаем следующего упражнения.

Упражнение 2.12. Элемент $a\in K$ называется *v-примарным* (относительно m), если расширение $K(\sqrt[m]{a})/K$ неразветвлено в точке v. Для $v\notin S$ очевидно, что элемент a v-примарен тогда и только тогда, когда $v(a)\equiv 0 \pmod m$. Предположим теперь, что v делит m и что $m=p$ — простое число. Пусть ζ — образующая группы μ_p и $\lambda=1-\zeta$. Проверить, что λ^{p-1}/p является единицей относительно нормирования v и, более точно, что $\lambda^{p-1}\equiv -p \pmod{p\lambda}$, т. е. $\lambda^{p-1}/p\equiv -1 \pmod{\mathfrak{p}_v}$. Пусть a таково, что $a\equiv 1 \pmod{p\lambda\mathfrak{o}_v}$, так что $a=1+\lambda^p c$ при $c\in\mathfrak{o}_v$. Доказать, что элемент a является v-примарным и что для всех b

$$(a, b)_v=\zeta^{-S(\bar{c})\cdot v(b)},$$

где S означает след из поля $k(v)$ в простое поле и $\bar{c}$ — это v-вычет элемента c. Кроме того, если $a\equiv 1 \pmod{p\lambda\mathfrak{p}_v}$, то элемент a v-примарен, т. е. $a\in(K_v^*)^m$.

(Пусть $\alpha^p=a$ и $\alpha=1+\lambda x$. Проверить, что x является корнем такого многочлена $f(X)\in\mathfrak{o}_v[X]$, что $f(X)\equiv X^p-X-c \pmod{\mathfrak{p}_v}$. Таким образом, $f'(x)\equiv -1\not\equiv 0 \pmod{\mathfrak{p}_v}$, так что расширение $K_v(x)=K_v(\sqrt[m]{a})$ неразветвлено. Если же $c\equiv 0 \pmod{\mathfrak{p}_v}$, то многочлен $f(X)$ распадается в силу леммы Гензеля и $K_v(\sqrt[m]{a})=K_v$. Теперь $x^p\equiv x+c \pmod{\mathfrak{p}_v}$ и если $Nv=p^f$, то

$$x^F=x^{Nv}\equiv x+c+c^p+\ldots+c^{p^{f-1}}\equiv x+S(c) \pmod{\mathfrak{p}_v}.$$

С другой стороны, если $\alpha'=\zeta\alpha=1+\lambda x'$, то $x'\equiv x-1 \pmod{\mathfrak{p}_v}$. Все эти факты вместе дают формулу для $(a, b)_v$.)

Упражнение 2.13. Пусть p — нечетное простое число, ζ — первообразный корень p-й степени из единицы, $K=\mathbf{Q}(\zeta)$ и $m=p$. Тогда p вполне разветвлено в поле K и $\lambda=1-\zeta$ порождает простой идеал, соответствующий тому единственному нормированию v поля K, которое лежит над p. Пусть U_i обозначает группу единиц $\equiv 1 \pmod{\lambda^i}$ в группе K_v^*, $i=1, 2, \ldots$. Тогда образ элемента $\eta_i = 1-\lambda^i$ порождает группу U_i/U_{i+1}, являющуюся циклической группой p-го порядка, а образ элемента λ порождает группу $K_v^*/(K_v^*)^p U_1$. На основании предыдущего упражнения $U_{p+1} \subset (K_v^*)^p$. Следовательно, элементы λ, $\zeta=\eta_1$, $1-\lambda^2=\eta_2, \ldots, 1-\lambda^p=\eta_p$ порождают группу $(K_v^*)/(K_v^*)^p$. Но она имеет порядок $p^2/|p|_v = p^{1+p}$, так что эти образующие — независимые по mod p степени. Показать, что:

(а) $(\eta_i, \eta_j)_v = (\eta_i, \eta_{i+j})_v \cdot (\eta_{i+j}, \eta_j)_v \cdot (\eta_{i+j}, \lambda)_v^{-j}$ для всех $i, j \geqslant 1$.

(б) Если $i+j \geqslant p+1$, то $(a, b)_v = 1$ для всех $a \in U_i$, $b \in U_j$.

(в) $(\eta_i, \lambda)_v = \begin{cases} 1, & \text{если } 1 \leqslant i \leqslant p-1, \\ \zeta, & \text{если } i=p. \end{cases}$

(г) $(a, b)_v$ — единственное кососимметрическое спаривание $K_v^* \times K_v^* \to \mu_p$, удовлетворяющее условиям (а) и (в).

(Для доказательства утверждения (а) заметить, что $\eta_j + \lambda^j \eta_i = \eta_{i+j}$, разделить это равенство на η_{i+j} и воспользоваться упражнением 2.5 и билинейностью; принять во внимание нечетность числа p, благодаря которой $(a, b) = (a, -b)$ в общем случае и $(a, a)=1$ в частности. Остальное получается легко, за исключением пункта (в), вытекающего из предыдущего упражнения. Заметить, что первые $(p-1)$ случаев пункта (в) тривиальны, потому что $(\eta_i, \lambda)_v^i = (1-\lambda^i, \lambda^i)_v = 1 \Rightarrow (\eta_i, \lambda)_v = 1$ для $1 \leqslant i \leqslant p-1$.)

Упражнение 2.14. (*Кубический закон взаимности.*) Рассмотрим случай $p=3$ в предыдущем упражнении. Кольцо целых элементов $R=\mathbf{Z}+\mathbf{Z}\zeta$ является областью главных идеалов, ненулевые элементы которой могут быть записаны в виде $\lambda^v \zeta^u a$, где $a \equiv \pm 1 \pmod{3R}$. Доказать, что

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) \qquad (*)$$

для взаимно простых a и b, каждый из которых $\equiv \pm 1 \pmod{3R}$, а также, что

$$\left.\begin{aligned} \left(\frac{\zeta}{a}\right) &= \zeta^{-m-n} \\ \left(\frac{\lambda}{a}\right) &= \zeta^m \end{aligned}\right\} \quad \text{для} \quad a = \pm(1+3(m+n\zeta)). \qquad (**)$$

В качестве приложения доказать следующее: если q — рациональное простое число $\equiv 1 \pmod 3$, то 2 является кубическим вычетом по $(\mathrm{mod}\ q)$ тогда и только тогда, когда q имеет вид x^2+27y^2, где $x, y \in \mathbf{Z}$. (Положить $q=\pi\bar{\pi}$, где $\pi \equiv \pm \pmod{3R}$. Тогда $\mathbf{Z}/q\mathbf{Z} \cong R/\pi R$, так что 2 является кубическим вычетом по mod q в том и только том случае, если $\left(\frac{2}{\pi}\right) = 1$. Воспользоваться равенством (*) и выразить соотношение $\left(\frac{2}{\pi}\right) = 1$ как некоторое утверждение о q.)

Упражнение 2.15. Пусть L — поле разложения многочлена X^3-2 над $\mathbf{Q}$. Группа Галуа расширения $L/\mathbf{Q}$ является симметрической группой третьей степени. Используя предыдущее упражнение, показать, что при $p \neq 2,3$ эндоморфизм Фробениуса задается следующими правилами:

$F_{L/\mathbf{Q}}(p) = (1)$, если $p \equiv 1 \pmod 3$ и p имеет вид x^2+27y^2;

$F_{L/\mathbf{Q}}(p) = 3$-цикл, если $p \equiv 1 \pmod 3$ и p не представимо в виде x^2+27y^2;

$F_{L/\mathbf{Q}}(p) = 2$-цикл, если $p \equiv -1 \pmod 3$.

Следовательно, по теореме Чеботарева плотности этих множеств простых чисел равны соответственно 1/6, 1/3 и 1/2.

Упражнение 2.16. Рассмотрим вновь случай произвольного поля K и любого m. Пусть $a_1, \ldots, a_r$ — конечное семейство элементов из K^*, и пусть L — куммерово расширение, порожденное корнями m-й степени из этих элементов. Пусть, далее, T — конечное множество нормирований поля K, содержащее множество $S(a_1, \ldots, a_r)$ и являющееся настолько большим, что $J_K = K^* J_{K,T}$ и $J_L = L^* J_{L,T'}$, где T' — множество нормирований поля L, лежащее над T. Предположим, что заданы такие элементы $\zeta_{v,i} \in \mu_m$ для $v \in T$ и $1 \leqslant i \leqslant r$, что

(i) для каждого i имеет место равенство $\prod_{v\in T}\zeta_{v,i}=1$;

(ii) для каждого $v\in T$ существует такой элемент $x_v\in K_v^*$, что $(x_v, a_i)_v=\zeta_{v,i}$ при всех i.

Показать, что существует такая T-единица $x\in K_T$, что $(x, a_i)_v=\zeta_{v,i}$ при всех $v\in T$ и всех $1\leqslant i\leqslant r$. Дополнительное условие на T, касающееся множества T', необходимо, что видно из примера $K=\mathbf{Q}$, $m=2$, $T=\{\infty, 2, 7\}$, $r=1$, $a_1=-14$, $\zeta_{\infty,1}=-1$, $\zeta_{2,1}=-1$, $\zeta_{7,1}=1$. Чтобы это доказать, рассмотрим группу $X=\prod_{v\in T}(K_v^*)/(K_v^*)^m$, подгруппу A, порожденную образом множества K_T, и меньшую подгруппу A_0, порожденную образами элементов a_i, $1\leqslant i\leqslant r$. Форма $\langle x, y\rangle=\prod_{v\in T}(x_v, y_v)_v$ задает невырожденное спаривание группы X с собой в группу μ_m, относительно которого группа A ортогональна к себе самой, потому что $[X]=m^{2t}$ и $[A]=m^t$, где $t=[T]$. (См. шаг 4 в доказательстве второго неравенства в гл. VII, § 9, причем обозначения S, n и s заменены в данном случае на T, m и t.) Итак, $X/A\cong\mathrm{Hom}(A, \mu_m)$ (заметить это на основании того, что обе группы изоморфны группе $\mathrm{Gal}(K(\sqrt[m]{K_T})/K)$ в силу теории полей классов и теории Куммера соответственно), и обратно, $A\cong\mathrm{Hom}(X/A, \mu_m)$. До сих пор мы не использовали условия о том, что $J_L=L^*J_{L,T'}$. Воспользоваться им для того, чтобы показать, что если $a\in A$ и $\pi_v(a)\in\pi_v(A_0)$ для всех v, где π_v — проекция из X на группу $K_v^*/(K_v^*)^m$, то $a\in A_0$, т. е. $\sqrt[m]{a}\in L$. Затем показать, что в силу двойственности и ортогональности, о которых говорилось выше, этот последний факт эквивалентен тому утверждению, которое надо доказать.

УПРАЖНЕНИЕ 3. ГИЛЬБЕРТОВО ПОЛЕ КЛАССОВ

Пусть L/K — глобальное абелево расширение, v — нормирование поля K и $i_v\colon K_v^*\to J_K$ — каноническое вложение. Показать, что v *полностью распадается* в L тогда и только тогда, когда $i_v(K_v^*)\subset K^*N_{L/K}J_L$; для неархимедова v показать, что v *неразветвлено* в L тогда и только тогда, когда $i_v(U_v)\subset K^*\cdot N_{L/K}J_L$, где U_v — группа единиц поля K_v (см. гл. VII, п. 5.1, 6.3). Следовательно, максимальное абелево расширение поля K, являющееся неразветвленным во всех неархимедовых нормированиях и полностью распадающееся во всех архимедовых нормированиях, представляет собой поле классов для группы $K^*J_{K,S}$, где S теперь обозначает множество архимедовых нормирований. (Воспользоваться главной теоремой (гл. VII, п. 5.1) и тем фактом, что группа $K^*N_{L/K}J_L$ замкнута.) Это расширение называется гильбертовым полем классов поля K; мы будем обозначать его через K'. Показать, что гомоморфизм Фробениуса $F_{K'/K}$ индуцирует некоторый изоморфизм групп классов идеалов $H_K=L_K/P_K$ поля K на группу Галуа $G(K'/K)$. (Воспользоваться главной теоремой и изоморфизмом $J_K/J_{K,S}\cong I_K$.) Итак, степень $[K':K]$ равна числу классов $h_K=[H_K]$ поля K. Простые дивизоры поля K разлагаются в расширении K' в соответствии с их классами дивизоров, и, в частности, простые дивизоры, распадающиеся полностью, — это в точности главные простые дивизоры. Произвольный идеал $\mathfrak{a}$ поля K является главным тогда и только тогда, когда $F_{K'/K}(\mathfrak{a})=1$.

Башня полей классов $K\subset K'\subset K''=(K')'\subset\ldots$ может быть бесконечной (см. гл. IX). Используя ее первые два этажа, а также коммутативную диаграмму (см. гл. VII, п. 11.3, диаграмма (13))

$$\begin{array}{ccc} I_K & \xrightarrow{F_{K'/K}} & G(K'/K) \\ {\scriptstyle\mathrm{con}}\downarrow & & \downarrow{\scriptstyle V} \\ I_{K'} & \xrightarrow{F_{K''/K'}} & G(K''/K') \end{array}$$

Артин установил, что гипотеза Гильберта о том, что каждый идеал в K становится главным в K', эквивалентна утверждению о том, что перенесение является в этой ситуации нулевым отображением. Далее, группа $G(K''/K')$ является коммутантом группы $G(K''/K)$ (почему?), и, таким образом, Артин высказал «теорему о главных идеалах» из теории групп: *если G — конечная группа и G^c — ее коммутант, то отображение V: $(G/G^c)\to G^c/(G^c)^c$ является нулевым*. Эта

теорема, а вместе с ней и гипотеза Гильберта были затем доказаны Фуртвенглером. Простое доказательство см. в [3].

Первые пять мнимых квадратичных расширений с числом классов $\neq$ являются расширениями с дискриминантами -15, -20, -23, -24 и -31, имеющими соответственно числа классов 2, 2, 3, 2, 3. Показать, что их гильбертовы поля классов получаются присоединением соответственно корней уравнений X^2+3, X^2+1, X^3-X-1, X^2+3 и X^3+X-1. В общем случае, когда поле K является мнимым квадратичным расширением, гильбертово поле классов K' порождается над K j-инвариантами эллиптических кривых, которые имеют кольцо целых элементов поля K в качестве кольца эндоморфизмов (см. гл. XIII).

Пусть J_S^+ — группа иделей, которые положительны в вещественных нормированиях поля K и являются единицами в неархимедовых нормированиях. Поле классов над полем K с норменной группой $K^*J_{K,S}^+$ является максимальным абелевым расширением, не разветвленным во всех неархимедовых нормированиях, но не подчиненным никаким условиям в архимедовых нормированиях; обозначим его через K_1. Пусть P_K^+ — группа главных идеалов вида (a), где a — всюду положительный элемент поля K. Показать, что $F_{K_1/K}$ задает изоморфизм: $I_K/P_K^+ \cong G(K_1/K)$. Итак, группа $G(K_1/K')$ является элементарной абелевой 2-группой, изоморфной P_K/P_K^+. Показать, что $[P_K : P_K^+]\,[K_S : K_S^+] = 2^{r_1}$, где $K_S^+ = K^* \cap J_{K,S}^+$ — группа всюду положительных единиц из поля K и r_1 — число вещественных нормирований поля K.

Мы, очевидно, имеем, что $\mathbf{Q}_1 = \mathbf{Q}$, но этот результат слаб с точки зрения теоремы Минковского о том, что поле $\mathbf{Q}$ не имеет нетривиальных расширений (*абелевых или нет*), которые не разветвлены во всех неархимедовых нормированиях (см. [5], [6]). Рассмотрим теперь случай, когда K является вещественным квадратичным, т. е. $[K : \mathbf{Q}] = 2$ и $r_1 = 2$. Показать, что $[K_1 : K'] = 1$ или 2 в зависимости от того, будет ли $N\varepsilon = -1$ или $N\varepsilon = 1$, где ε — основная единица в поле K и $N = N_{K/\mathbf{Q}}$. Например, в случае $K = \mathbf{Q}(\sqrt{2})$ или $K = \mathbf{Q}(\sqrt{5})$ мы имеем $K' = K$, потому что число классов равно 1, и, следовательно, $K_1 = K$, потому что единицы $\varepsilon = 1+\sqrt{2}$ и $\varepsilon = 1/2\,(1+\sqrt{5})$ имеют норму -1. С другой стороны, если $K = \mathbf{Q}(\sqrt{3})$, то снова $K' = K$, но $K_1 \neq K$, потому что $\varepsilon = 2+\sqrt{3}$ имеет норму 1; показать, что $K_1 = K(\sqrt{-1})$. В общем случае, если -1 не всюду является локальной нормой (как в случае $K = \mathbf{Q}(\sqrt{3})$, только что рассмотренном), то $N\varepsilon = 1$ и $K_1 \neq K'$. Однако если -1 всюду является локальной нормой, а потому и нормой некоторого числа из K, то до сих пор не существует общего правила для определения того, является ли или нет -1 нормой какой-нибудь *единицы*.

УПРАЖНЕНИЕ 4. ЧИСЛА, ПРЕДСТАВИМЫЕ КВАДРАТИЧНЫМИ ФОРМАМИ

Пусть K — поле характеристики, отличной от 2 и

$$f(X) = \sum a_{ij} X_i X_j$$

— некоторая (невырожденная) квадратичная форма от n переменных с коэффициентами из поля K. Мы говорим, что f *представляет элемент* c *в поле* K, если уравнение $f(X) = c$ имеет решение $X = x \in K^n$, такое, что не все x_i равны нулю. *Если* f *представляет* 0 *в* K, *то* f *представляет все элементы из* K. В самом деле,

$$f(tX+Y) = t^2 f(X) + tB(X, Y) + f(Y).$$

Если $f(x) = 0$, но $x \neq (0, 0, \ldots, 0)$, то в силу невырожденности существует $y \in K^n$, такой, что $B(x, y) \neq 0$, так что $f(tx+y)$ — не постоянная линейная функция от t, а потому она принимает все значения из K, когда t пробегает поле K.

Линейное преобразование координат не влияет на вопрос о представимости; таким преобразованием мы всегда можем привести f к диагональному виду: $f = \sum a_i X_i^2$, где $a_i \neq 0$. Если $f = cX_1^2 - g(X_2, \ldots, X_n)$, то f представляет 0 тогда и только тогда, когда g представляет c, потому что если f представляет 0, то она представляет и c. Следовательно, вопрос о представимости ненулевых элементов с формами от $n-1$ переменной эквивалентен вопросу о представимости нуля формами от n переменных. Ответ на последний вопрос не изменится, если умножить f на нену-

левую константу; следовательно, мы можем предположить, что f приведена к диагональному виду, причем $a_1 = 1$. В дальнейших упражнениях мы будем это предполагать.

Упражнение 4.1. Форма $f = X^2$ не представляет 0.

Упражнение 4.2. Форма $f = X^2 - bY^2$ представляет 0 тогда и только тогда, когда $b \in (K^*)^2$.

Упражнение 4.3. Форма $f = X^2 - bY^2 - cZ^2$ представляет 0 тогда и только тогда, когда c является нормой из расширения $K(\sqrt{b})$.

Упражнение 4.4. Следующие утверждения эквивалентны:

(i) форма $f = X^2 - bY^2 - cZ^2 + acT^2$ представляет 0 в K;

(ii) c является произведением нормы из $K(\sqrt{a})$ и нормы из $K(\sqrt{b})$;

(iii) c, как элемент из $K(\sqrt{ab})$, является нормой из поля $L = K(\sqrt{a}, \sqrt{b})$;

(iv) форма $g = X^2 - bY^2 - cZ^2$ представляет 0 в поле $K(\sqrt{ab})$.

(Мы, очевидно, можем предположить, что ни a, ни b не являются квадратами в поле K. Тогда эквивалентность утверждений (i) и (ii) очевидна, потому что элемент, обратный к норме, является нормой, а эквивалентность утверждений (iii) и (iv) следует из упражнения 4.3 при K, замененном на $K(\sqrt{ab})$. Остается доказать, что (ii) $\Leftrightarrow$ (iii), причем мы можем предположить, что $ab \notin (K^*)^2$, так как иначе факт эквивалентности тривиален. Тогда $\mathrm{Gal}(L/K)$ является группой из четырех элементов 1, ρ, σ, τ, таких, что ρ, σ и τ оставляют неподвижными, соответственно, $\sqrt{ab}$, $\sqrt{a}$ и $\sqrt{b}$. Далее, (ii) эквивалентно утверждению (ii′): существуют x, $y \in L$ такие, что $x^\sigma = x$, $y^\tau = y$ и $x^{1+\rho}\, y^{1+\rho} = c$; кроме того, (iii) эквивалентно утверждению (iii′): существует $z \in L$, такое, что $z^{1+\rho} = c$. Следовательно, (ii) $\Rightarrow$ (iii). Предположим поэтому, что имеет место (iii′), положим $u = c^{-1}z^{\sigma+1}$ и проверим, что $u^\sigma = u$, т. е. что $u \in K(\sqrt{a})$ и $u^{\rho+1} = 1$. Следовательно, по «теореме Гильберта 90» (гл. V, п. 2.7) для расширения $K(\sqrt{a})/K$ существует такое $x \neq 0$, что $x^\sigma = x$ и $x^{\rho-1} = u$. Положим теперь $y = z^\rho/x$ и проверим, что (ii′) имеет место.)

До сих пор мы занимались алгеброй, а не арифметикой. С этого момента предположим, что поле K — *глобальное поле* с характеристикой $\neq 2$.

Упражнение 4.5. Форма f из упражнения 4.3 представляет 0 в локальном поле K_v тогда и только тогда, когда символ квадратичного норменного вычета $(b, c)_v$ равен 1. Следовательно, f представляет 0 в K_v для всех, кроме конечного числа, нормирований v и число тех нормирований v, для которых f не представляет 0 в K_v, четно. Более того, последние два утверждения инвариантны относительно умножения формы f на скаляр и, следовательно, выполняются для произвольной невырожденной формы от трех переменных над K.

Упражнение 4.6. Пусть f — форма из упражнения 4.4. Показать, что если f *не* представляет 0 в локальном поле K_v, то $a \notin (K_v^*)^2$ и $b \notin (K_v^*)^2$, но $ab \in (K_v^*)^2$ и c *не* является нормой из квадратичного расширения $K_v(\sqrt{a}) = K_v(\sqrt{b})$. (Воспользоваться тем, что норменные группы из различных квадратичных расширений поля K_v являются подгруппами индекса 2 в K_v^*, каждые две из которых не совпадают.) Обратно, предположим теперь, что эти условия выполняются. Показать, что множество элементов из K_v, представимых формой f, равно $N - cN$, где N — группа ненулевых норм из $K_v(\sqrt{a})$ и, в частности, что f не представляет 0 в поле K_v. Показать, далее, что если $N - cN \neq K_v^*$, то $-1 \notin N$ и $N + N \subset N$. Следовательно, форма f представляет каждый ненулевой элемент из K_v, *за исключением случая*, когда имеет место изоморфизм $K_v \cong \mathbf{R}$ и f является положительно определенной.

Упражнение 4.7. Любая форма f с числом переменных $n \geqslant 5$ над локальным полем K_v представляет нуль, за исключением случая, когда K_v является вещественным полем, а форма f положительно определена.

Упражнение 4.8. *Теорема: пусть K — глобальное поле и f — невырожденная квадратичная форма от n*

переменных над K, представляющая 0 в K_v для каждого нормирования v поля K. Тогда f представляет 0 в поле K. (Для $n = 1$ тривиально; для $n = 2$ см. гл. VII, п. 8.8; для $n = 3$ см. гл. VII, п. 9.6 и упражнение 4.3; для $n = 4$ использовать упражнение 4.4 для того, чтобы свести все к случаю $n = 3$; наконец, для $n \geqslant 5$ продолжить по индукции: пусть

$$f(X) = aX_1^2 + bX_2^2 - g(X_3, \ldots, X_n),$$

где форма g имеет $n - 2 \geqslant 3$ переменных. Из упражнения 4.5 мы знаем, что g представляет 0 и, следовательно, каждое число из K_v для всех v вне конечного множества S. Далее, $(K_v^*)^2$ — открытая подгруппа в K_v^*. Следовательно, по теореме об аппроксимации существуют элементы $x_1, x_2 \in K$, такие, что элемент $c = ax_1^2 + bx_2^2 \neq 0$ представляется формой g в поле K_v для всех $v \in S$ и, значит, вообще для всех v. По индукции форма $cY^2 - g(X_3, \ldots X_n)$ от $n - 1$ переменной представляет 0 в K. Следовательно, f представляет нуль.)

Упражнение 4.9. *Следствие: если $n \geqslant 5$, то f представляет 0 в поле K, если только не существует вещественного нормирования v, в котором форма f положительно определена.*

Упражнение 4.10. Рациональное число c является суммой трех рациональных квадратов в том и только том случае, если $c = 4^n r$, где r — рациональное число > 0 и $\not\equiv 7 \pmod 8$; каждое рациональное число является суммой четырех (рациональных) квадратов.

Упражнение 4.11. Утверждения предыдущего упражнения остаются справедливыми, если всюду заменить слово «рациональный» на «целый рациональный». (Факт о 4 квадратах немедленно следует из факта о трех квадратах, так что мы обратимся лишь к последнему, хотя имеется много доказательств для случая четырех квадратов, не опирающихся на «более глубокий» результат о трех. Пусть c — положительное целое число из упражнения 4.10, так что сфера $|X|^2 = X_1^2 + X_2^2 + X_3^2 = c$ имеет точку с рациональными координатами $x = (x_1, x_2, x_3)$. Мы должны показать, что она имеет точку с *целыми* координатами.

Считая, что точка x — не целая, возьмем целую точку z в 3-мерном пространстве, которая максимально возможно близка к x, т. е. $x = z + a$, где $0 < |a|^2 \leqslant 3/4 < 1$. Прямая l, соединяющая x и z, не касается сферы; если бы это произошло, то $|a|^2 = |z|^2 - |x|^2 = |z|^2 - c$ было бы целым числом, что дает противоречие. Следовательно, прямая l пересекается со сферой в некоторой рациональной точке $x' \neq x$. Теперь нужно показать, что если координаты точки x могут быть записаны с общим знаменателем $d > 0$, то координаты точки x' могут записаны с общим знаменателем $d' = |a|^2 d < d$, так что последовательность x, x', $(x')'$, ... должна сходиться к целой точке. Заметим, что d' на самом деле — целое число, потому что

$$d' = |a|^2 d = |x - z|^2 d = (|x|^2 - 2(x, z) + |z|^2) d = \\ = cd - 2(dx, z) + |z|^2 d.)$$

Упражнение 4.12. Пусть f — форма от трех переменных над K. Показать, что если f не представляет 0 локально в K_v, то другие числа из K_v, не представимые формой f, образуют класс смежности группы K_v^* по подгруппе $(K_v^*)^2$. (Очевидно, можно предположить, что $f = X^2 - bY^2 - cZ^2$; затем надо воспользоваться упражнением 4.6.) Используя это, показать, что если $K = \mathbf{Q}$ и форма f положительно определена, то f не представляет все положительные целые числа. (Обратить внимание на последнюю фразу в упражнении 4.5.)

О дальнейших фактах и работах, связанных с этим материалом, см. [2] или [7].

УПРАЖНЕНИЕ 5. ОТЛИЧИЕ ЛОКАЛЬНЫХ НОРМ ОТ ГЛОБАЛЬНЫХ И Т. Д.

Пусть L/K — расширение Галуа с группой $G = (1, \rho, \sigma, \tau) \cong (\mathbf{Z}/2\mathbf{Z})^2$, и пусть K_1, K_2 и K_3 — три квадратичных промежуточных расширения, являющиеся неподвижными полями элементов ρ, σ и δ соответственно. Пусть $N_i = N_{K_i/K}(K_i^*)$ для $i = 1, 2, 3$ и $N = N_{L/K}(L^*)$.

Упражнение 5.1. Показать, что $N_1 N_2 N_3 = \{x \in K^* \mid x^2 \in N\}$. (Это — чистая алгебра, а не арифме-

тика; одно включение тривиально, другое же может быть доказано методами, использованными в упражнении 4.3.)

Упражнение 5.2. Предположим теперь, что K — глобальное поле. Показать, что если локальная степень поля L над K равна 4 для некоторого нормирования, то $N_1N_2N_3 = K^*$ (см. гл. VII, п. 11.4). Предположим теперь, что все локальные степени равны 1 или 2. Для простоты допустим, что характеристика поля K отлична от 2, и пусть $K_i = K(\sqrt{a_i})$ для $i = 1, 2, 3$. Для каждого i обозначим через S_i (бесконечное) множество простых дивизоров поля K, распадающихся в расширении K_i, и для $x \in K^*$ положим

$$\varphi(x) = \prod_{v \in S_1} (a_2, x)_v = \prod_{v \in S_1} (a_3, x)_v = \prod_{v \in S_2} (a_3, x)_v =$$

$$= \prod_{v \in S_2} (a_1, x)_v = \prod_{v \in S_3} (a_1, x)_v = \prod_{v \in S_3} (a_2, x)_v = \pm 1,$$

где $(x, y)_v$ — символ квадратичного норменного вычета. Показать, что $N_1N_2N_3 = \ker \varphi$ является подгруппой индекса 2 в K^*. (Включение $N_1N_2N_3 \subset \ker \varphi$ тривиально. Из упражнения 5.1 и результатов гл. VII, п. 11.4 видно, что индекс группы $N_1N_2N_3$ в K^* не больше 2. Но в силу упражнения 2.16 существует такой x, что $\varphi(x) = -1$.)

Упражнение 5.3. Пусть $K = \mathbf{Q}$ и $L = \mathbf{Q}(\sqrt{13}, \sqrt{17})$. Показать, что если x является произведением тех простых чисел p, для которых $\left(\frac{p}{13}\right) = -1$ (например, $p = 2, 5, 7, 11 \ldots$), то $\varphi(x) = \left(\frac{x}{17}\right)$. Следовательно, 5^2, 7^2, 10^2, 11^2, 14^2, ... — примеры чисел, которые всюду являются локальными нормами из расширения $\mathbf{Q}(\sqrt{13}, \sqrt{17})$, но глобальными нормами не являются. Впрочем, не всякое число такого сорта представляет собой некоторый квадрат; например, -14^2 является глобальной нормой числа $\frac{1}{2}(7 + 2\sqrt{13} + \sqrt{17})$ и, сопоставляя это с вышесказанным, мы видим, что число -1 всюду является локальной нормой, но глобальной нормой -1 не является.

Упражнение 5.4. Предположим теперь, что наше глобальное расширение L/K с группой Галуа из четырех элементов обладает следующим свойством: существует *точно одно* нормирование v поля K, в котором локальная степень равна 4. Пусть w — нормирование поля L, продолжающее v; показать, что $\hat{H}^{-1}(G, L^*) = 0$, но $\hat{H}^{-1}(G, L_w^*) \cong \mathbf{Z}/2\mathbf{Z}$. (Воспользоваться точной последовательностью, выписанной в начале п. 11.4 гл. VII.) Отображение g сюръективно, что всегда бывает, когда наименьшее общее кратное локальных степеней равно глобальной степени. Отображение g: $\hat{H}^{-1}(G, J_L) \to \hat{H}(G, C_L)$ кроме того и инъективно, потому что наше предположение о том, что локальная степень равна 4, касается только одного нормирования.)

Пусть A, соответственно A_w — группа элементов из L^*, соответственно из L_w^*, норма которых в поле K, соответственно в поле K_v, равна 1, и пусть $\bar{A}$ — замыкание группы A в группе L_w^*. Из вышесказанного следует, что

$$A = (L^*)^{\rho-1}(L^*)^{\sigma-1}(L^*)^{\tau-1},$$

а также то, что

$$\bar{A} = (L_w^*)^{\rho-1}(L_w^*)^{\sigma-1}(L_w^*)^{\tau-1}$$

имеет в группе A_w порядок 2. Как хорошо известно, существует некоторая алгебраическая группа T, определенная над полем K (скрученный тор размерности 3, определенный уравнением $N_{L/K}(X) = 1$), такая, что, $T(K) = A$ и $T(K_v) = A_w$. Следовательно, мы получаем примеры, которые показывают, что *группа рациональных точек тора T не обязательно плотна в группе v-адических точек* (см. ниже последнее упражнение). Нетрудно, однако, показать, что если T — тор над K, распадающийся над расширением Галуа L/K, то группа $T(K)$ плотна в $T(K_v)$ для каждого такого нормирования v поля K, что существует нормирование $v' \neq v$ с той же группой разложения, что и у v; в частности, так бывает, когда группа разложения для v циклична и, в еще более частном случае, когда v архимедово.

В качестве конкретной иллюстрации рассмотрим случай $K = \mathbf{Q}$ и $L = \mathbf{Q}(\sqrt{-1}, \sqrt{2}) = \mathbf{Q}(\zeta)$, где $\zeta^4 = -1$. Тогда расширение L всюду, кроме точки 2, неразветвлено, а в точке 2 оно вполне разветвлено и, следовательно, существует ровно один простой дивизор, локальная степень которого равна 4. Пусть $M = \mathbf{Q}(i)$, где $i = \zeta^2 = \sqrt{-1}$, и пусть

L_w и M_v — пополнения относительно нормирований, продолжающих 2-адическое нормирование. Легко дать прямое доказательство того факта, что элементы из L с нормой 1 не образуют плотного подмножества в L_w^*; непосредственно проверяется, что элемент $z = (2 + i)/(2 - i) \in M_v$ является нормой из L_w в L_v, но множество $z\,(M_v^*)^2$ не содержит ни одного элемента $y \in M$, такого, что y является глобальной нормой из L в M, *причем* $N_{M/Q}(y) = 1$.

УПРАЖНЕНИЕ 6. О РАЗЛОЖЕНИИ НОРМИРОВАНИЙ

Пусть L/K — конечное глобальное расширение, и пусть S — некоторое конечное множество нормирований поля K. Мы будем обозначать через $\mathrm{Spl}_S(L/K)$ множество таких нормирований $v \notin S$, что v полностью распадается в L (т. е. таких, что $L \underset{K}{\otimes} K_v \cong K^{[L:K]}$), и через $\mathrm{Spl}'_S(L/K)$ — множество нормирований $v \notin S$, которые имеют распадающийся в L множитель (т. е. для которых существует K-изоморфизм $L \to K_v$). Итак, $\mathrm{Spl}_S(L/K) \subseteq \mathrm{Spl}'_S(L/K)$ всегда и равенство имеет место, если K — расширение Галуа, причем в этом случае $\mathrm{Spl}'_S(L/K)$ имеет плотность $[L:K]^{-1}$ по теореме Чеботарева о плотности (сформулирована в конце § 3, гл. VIII).

Упражнение 6.1. Показать, что если L и M — расширения Галуа над K, то

$$L \subset M \Leftrightarrow \mathrm{Spl}_S(M) \subset \mathrm{Spl}_S(L).$$

(Действительно, имеет место

$$\mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K),$$

так что

$$\{L \subset M\} \Rightarrow \{\mathrm{Spl}_S(M) \subset \mathrm{Spl}_S(L)\} \Rightarrow \{\mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(M/K)\} \Rightarrow \{[LM:K] = [M:K]\} \Rightarrow \{L \subset M\}.$$

Попутный вопрос: где использовалось то обстоятельство, что данные расширения являются расширениями Галуа?) Следовательно,

$$\{L = M\} \Leftrightarrow \{\mathrm{Spl}_S(L) = \mathrm{Spl}_S(M)\}.$$

Приложение, *если сепарабельный многочлен* $f(X) \in K[X]$ *распадается на линейные множители по* mod $\mathfrak{p}$ *для всех, кроме конечного числа, простых дивизоров* $\mathfrak{p}$ *поля* K, *то* f *распадается на линейные множители и в поле* K. (Взять в качестве L поле разложения многочлена $f(X)$, положить $M = K$, а S взять настолько большим, чтобы f имел целые коэффициенты и единичный дискриминант вне множества S.) Наконец, заметим, что в этом упражнении все равно проходят все рассуждения, если заменить «все нормирования $v \notin S$» и «все, кроме конечного числа, нормирования v» на «все v во множестве плотности 1».

Упражнение 6.2. Пусть L/K — расширение Галуа с группой G, пусть H — подгруппа в G и E — ее неподвижное поле. Для каждого нормирования v поля K обозначим через G^v группу разложения для v. Показать, что v полностью распадается в поле E тогда и только тогда, когда все сопряженные с G^v группы содержатся в H; показать, что v имеет распадающийся множитель в расширении E в том и только том случае, если хотя бы одна из сопряженных с G^v групп принадлежит H. Следовательно, надо показать, что множество нормирований $\mathrm{Spl}'_S(E/K)$ имеет плотность $[\bigcup_{\rho \in G} \rho H \rho^{-1}]/[G]$. Затем доказать лемму о конечных группах, которая утверждает, что объединение подгрупп, сопряженных с некоторой собственной подгруппой, не равно всей группе (потому что они немного перекрываются в единице!), и заключить отсюда, что если множество $\mathrm{Spl}'_S(E/K)$ имеет плотность 1, то $E = K$. Приложение: *если неприводимый многочлен* $f(X) \in K[X]$ *имеет корень по* mod $\mathfrak{p}$ *для всех, кроме конечного числа, простых дивизоров* $\mathfrak{p}$, *или даже только для множества простых дивизоров* $\mathfrak{p}$ *плотности* 1, *то* f *имеет корень и в* K. Это утверждение неверно для приводимых многочленов; рассмотреть пример: $f(X) = (X^2 - a)(X^2 - b)(X^2 - ab)$, где a, b и ab не являются квадратами в K. Кроме того, множество $\mathrm{Spl}'_S(E/K)$ в общем случае не определяет E с точностью до K-изоморфизма; см. ниже упражнение 6.4.

Упражнение 6.3. Пусть H и H' — подгруппы конечной группы G. Показать, что перестановочные представления группы G, соответствующие группам H и H', изоморфны как линейные представления в том и только том случае, если каждый класс сопряженных элементов

группы G пересекается с H и H' на одном и том же числе элементов. Заметить, что если H — нормальный делитель, то условие не имеет места, если только не выполняется равенство $H' = H$. Однако имеются примеры подгрупп H и H', удовлетворяющих указанному выше условию, которые не сопряжены (см. [4]); взять в качестве G симметрическую группу степени 6 и положить

$$H = \{1, (X_1X_2)(X_3X_4), (X_1X_3)(X_2X_4), (X_1X_4)(X_2X_3)\};$$
$$H' = \{1, (X_1X_2)(X_3X_4), (X_1X_2)(X_5X_6), (X_3X_4)(X_5X_6)\}.$$

(H оставляет неподвижными X_5 и X_6, а H' не оставляет на месте ни одного символа; но все элементы, отличные от 1 в H и H', сопряжены в G.) Заметить, что существуют расширения Галуа поля $\mathbf{Q}$ с группой Галуа, равной симметрической группе степени 6.

Упражнение 6.4. Пусть L — конечное расширение Галуа поля $\mathbf{Q}$, пусть $G = G(L/\mathbf{Q})$ и E, E' — подполя расширения L, соответствующие подгруппам H, H' группы G. Показать, что следующие условия эквивалентны:

(а) группы H и H' удовлетворяют эквивалентным условиям упражнения 6.3;

(б) в расширении E разветвлены те же простые числа p, что и в расширении E', а неразветвленные числа p имеют одинаковые разложения в E и E' в том смысле, что набор степеней множителей числа p в E совпадает с набором степеней множителей числа p в E', или, что то же самое, в том смысле, что $A/pA \cong A'/pA'$, где A и A' — кольца целых элементов соответственно в E и E';

(в) дзета-функции расширений E и E' совпадают (включая множители, соответствующие разветвленным нормированиям и ∞).

Более того, если эти условия выполняются, то E и E' имеют одинаковые дискриминанты. Если группы H и H' не сопряжены в G, то E и E' не изоморфны. Следовательно, в силу упражнения 6.3 существуют неизоморфные расширения поля $\mathbf{Q}$ с одинаковыми законами разложения и одинаковыми дзета-функциями. Однако такого быть не может, если одно из расширений поля $\mathbf{Q}$ является расширением Галуа.

УПРАЖНЕНИЕ 7. ЛЕММА О ДОПУСТИМЫХ ОТОБРАЖЕНИЯХ

Пусть K — глобальное поле, S — конечное множество нормирований поля K, включающее архимедовы нормирования, H — конечная абелева группа и φ: $I^S \to H$ — некоторый гомоморфизм, который *допустим* в смысле п. 3.7 гл. VII. Мы будем рассматривать «пары» (L, α), состоящие из конечного абелева расширения L/K и *инъективного* гомоморфизма α: $G(L/K) \to H$.

Упражнение 7.1. Показать, что существует пара (L, α), такая, что L/K не разветвлено вне S и $\varphi(\mathfrak{a}) = \alpha(F_{L/K}(\mathfrak{a}))$ для всех $\mathfrak{a} \in I^S$, где $F_{L/K}$ — отображение из гл. VII, § 3 (воспользоваться предложением 4.1 и теоремой 5.1).

Упражнение 7.2. Показать, что если $\varphi(v) = 1$ для всех нормированный v во множестве плотности 1 (например, для всех, кроме конечного числа, нормирований степени 1 над $\mathbf{Q}$), то φ тождественно равно 1. (Воспользоваться теоремой Чеботарева о плотности и упражнением 7.1.) Следовательно, если два допустимых отображения групп дивизоров в одну и ту же конечную группу совпадают на множестве простых дивизоров плотности 1, то они совпадают всюду, где определены одновременно.

Упражнение 7.3. Предположим, что пара (L', α') такова, что $\alpha'(F_{L'/K}(v)) = \varphi(v)$ для всех v во множестве плотности 1. Показать, что (L', α') имеет те же свойства, что пара (L, α), построенная в упражнении 7.1; в действительности же надо показать, что если L' и L содержатся в общем расширении M, то $L' = L$ и $\alpha' = \alpha$. (Очевидно, мы можем предположить, что M/K — конечное абелево расширение. Пусть θ, соответственно θ' — каноническая проекция из $G(M/K)$ на $G(L/K)$, соответственно на $G(L'/K)$. Согласно упражнению 7.2 и п. 3.2 из гл. VII, мы имеем $\alpha \circ \theta \circ F_{M/K} = \alpha' \circ \theta' \circ F_{M/K}$. Так как α и α' инъективны, а $F_{M/K}$ сюръективно, то $\ker\theta = \ker\theta'$; следовательно, $L = L'$ и, наконец, $\alpha = \alpha'$.)

УПРАЖНЕНИЕ 8. НОРМЫ ИЗ НЕАБЕЛЕВЫХ РАСШИРЕНИЙ

Пусть E/K — глобальное расширение, не обязательно являющееся расширением Галуа, и пусть M — максимальное абелево подрасширение. Доказать, что $N_{E/K}C_E = N_{M/K}C_M$, и проверить, что этот результат несколько упрощает доказательство теоремы существования, как указывалось при доказательстве леммы в § 12, гл. VII. (Пусть L — расширение Галуа поля K, содержащее E, с группой G; пусть H — подгруппа, соответствующая расширению E; рассмотрим следующую коммутативную диаграмму (см. § 11, 3, гл. VII):

$$\begin{array}{ccccccc} \hat{H}^{-2}(H, \mathbf{Z}) & \cong & H^{ab} & \rightrightarrows & C_E/N_{L/E}C_L & \cong & \hat{H}^0(H, C_L) \\ \Big\downarrow{\scriptstyle \mathrm{cor}} & & \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle N_{E/K}} & & \Big\downarrow{\scriptstyle \mathrm{cor}} \\ \hat{H}^{-2}(G, \mathbf{Z}) & \cong & G^{ab} & \rightrightarrows & C_K/N_{L/K}C_L & \cong & \hat{H}^0(G, C_L). \end{array}$$

Так как $G^{ab}/\theta(H^{ab}) \cong G(M/K)$, то это дает требуемый результат.)

ЛИТЕРАТУРА

Артин, Тэйт (Artin E., Tate J.)
[1] Class field theory, Harvard, 1961.

Боревич З. И., Шафаревич И. Р.
[2] Теория чисел, «Наука», М., 1964.

Витт (Witt E.)
[3] Verlagerung von Gruppen und Hauptidealsatz, Proc. Intern. Math. Congress II, Amsterdam, 1954, 71—73.

Гассман (Gassmann F.)
[4] Beziehungen zwischen den Primidealen eines algebraischen Körpers, *Math. Z.*, **25** (1926), 661—675.

Минковский (Minkowski H.)
[5] Geometrie der Zahlen, Leipzig — Berlin, 1910.
[6] Diophantische Approximationen, Leipzig, 1907.

О'Мира (O'Meara O.)
[7] Introduction to quadratic forms, Springer-Verlag, 1963.

Серр (Serre J.-P.)
[8] Corps locaux, Hermann, Paris, 1962.

Хассе (Hasse H.)
[9] Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II, *Jber. dt. Math. Verein*, **36** (1927).

СОДЕРЖАНИЕ

АЛГЕБРАИЧЕСКАЯ ТЕОРИЯ ЧИСЕЛ

Редактор *В. Демьянов*
Художник *В. Медников*
Художественный редактор *В. Шаповалов*
Технический редактор *Е. Потапенкова*
Корректор *Е. Литвак*

Сдано в производство 26/III 1969 г.
Подписано к печати 30/X 1969 г.
Бумага № 1 84×108¹/₃₂=7,56 бум. л.
25,41 усл. печ. л.
Уч.-изд. л. 20,97. Изд. № 1/5013
Цена 1 р. 70 к. Зак. 999

ИЗДАТЕЛЬСТВО «МИР»
Москва, 1-й Рижский пер., 2

Московская типография № 16
Главполиграфпрома Комитета по печати
при Совете Министров СССР
Москва, Трехпрудный пер., 9