Н. Г. ЧЕБОТАРЁВ

# ТЕОРИЯ АЛГЕБРАИЧЕСКИХ ФУНКЦИЙ

ОГИЗ
ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1948 ЛЕНИНГРАД

11 — 5 — 4

Редактор *А. И. Узков* Техн. редактор *Н. Я. Мурашова.*

Подписано к печати 26/III 1948 г. Тип. зн. в печ. л. 48160. Печ. л. 24¾.
Уч.-издат. л. 29,78. А-01744. Цена 18 р. Переплет 2 р. Заказ № 964. Тираж 6000.

4-я типография им. Евг. Соколовой треста «Полиграфкнига» ОГИЗа при Совете Министров СССР. Ленинград. Измайловский пр., 29.

## ОГЛАВЛЕНИЕ

## ПРЕДИСЛОВИЕ

Появление в свет настоящей книжки вызвано желанием несколько восполнить пробел в нашей литературе по теории алгебраических функций. Это обширное направление, которое во второй половине прошлого века владело умами весьма многих, притом лучших, математиков, затем одно время как будто было забыто, теперь снова возрождается в модернизированном виде, и связано с новыми интересными проблемами. У нас и раньше были специалисты, посвятившие себя теории алгебраических функций, как, например, Долбня (интегрирование абелевых интегралов в конечном виде), Покровский (теория гиперэллиптических функций); у нас был довольно обстоятельный учебник Тихомандрицкого и краткий курс Ермакова, правда, не свободный от ошибок. Однако в последнее время теория и её способ изложения настолько изменили своё лицо, что перечисленные книги надо считать устаревшими.

Впрочем, мы должны сделать существенную оговорку: в сущности, теория алгебраических функций не имеет единого лица. Её представители делятся на три довольно резко отграниченные группы или направления, имеющие характер почти сект: функциональную, геометрическую и арифметическую, в которых и метод выводов, и терминология совершенно различны. Я буду придерживаться, главным образом, арифметического направления; арифметическое изложение теории отличается исключительной красотой и законченностью. Однако не следует закрывать глаз на то, что большинство результатов было получено представителями двух других направлений, причём некоторые из результатов функционального направления по существу не могут быть получены методами других направлений. С другой стороны, современные исследования не ограничиваются случаем, когда числовое поле коэффициентов рассматриваемых алгебраических функций алгебраически замкнуто; это делает методы арифметического направления незаменимыми при постановке современных проблем теории алгебраических функций.

Эта особенность теории алгебраических функций создаёт при её изложении специфические трудности. Чтобы познакомить читателя, по возможности, со всем богатством результатов этой теории, я, следуя примеру Гензеля и Ландсберга, отказываюсь от проведения арифметических методов во всей их чистоте, изложив в главах

VI — VIII основы теории римановых поверхностей и связанных с ними результатов. В первых же главах книги я ближе придерживаюсь «классического» изложения Дедекинда и Вебера, чем современного «абстрактного» изложения, проведённого Ф. К. Шмидтом, имея в виду читателей неалгебраистов. Современные же результаты я сосредоточил в особых параграфах: 15-м, 21-м и 27-м, а также в главе X.

Глава I посвящена общей теории полей и неалгебраистом может быть пропущена без ущерба для понимания дальнейшего.

В главах II — V изложена арифметическая теория алгебраических функций с основными приложениями. Последние даны в несколько бо́льшем объёме, чем у Гензеля и Ландсберга, исключая геометрические приложения, которых у меня почти не дано. При этом чистота арифметического метода у меня сохранена в гораздо большей мере, чем у Гензеля и Ландсберга.

Главы VI — VIII посвящены методам и результатам функционального направления и требуют предварительных сведений из теории аналитических функций. Поскольку их изложение не является основной задачей книги, я ограничился конспективным изложением. К этому меня также принуждал жёсткий лимит в объёме книги.

Главы IX и X содержат обзор дальнейших результатов и направлений теории, классических и современных. Здесь тоже лимит в объёме не дал мне возможности развить материал так, как я этого бы желал. Пришлось ограничиться формулировкой результатов и ссылками на литературу.

В конце я поместил «Систематический путеводитель по литературе», который имеет задачей ориентировать в существующих книгах и журнальных статьях читателя, желающего подробнее познакомиться с теорией алгебраических функций. Далее приложен «алфавитный указатель литературы», ссылки на который в тексте помещены в скобочках.

Льщу себя надеждой, что книга окажется полезной для осуществления факультативных курсов и семинаров для студентов, для подготовки аспирантов, а также как справочник при работе над диссертациями.

В заключение считаю своим приятным долгом выразить глубокую признательность А. И. Узкову за исключительно внимательный просмотр рукописи и за ряд ценных критических указаний.

*Н. Чеботарёв*

Казань
Август 1945 г.

## ВВЕДЕНИЕ

Теория алгебраических функций имеет предметом изучения рациональные функции $\varphi(x, y)$ от переменных $x$, $y$, связанных алгебраическим соотношением

(1) $$f(x, y) = 0,$$

где $f(x, y)$ есть полином относительно обеих переменных. Эта теория исторически возникла из попыток интегрировать в конечном виде интегралы вида

(2) $$\int \varphi(x, y)dx,$$

которые в честь великого норвежского математика Абеля (N. H. Abel, 1802—1829), положившего начало их теории, носят название *абелевых интегралов*.

Вопрос об их интегрировании в конечном виде связан с удачным подбором преобразования вида

(3) $$x = \psi_1(u, v), \quad y = \psi_2(u, v),$$

где $\psi_1$, $\psi_2$ — рациональные функции, после которого интеграл (2) превратился бы в интеграл от рациональной функции одной переменной. Свойство интеграла (2) быть интегрируемым в конечном виде не зависит от произвольного преобразования типа (3), производимого над этим интегралом. Таким образом из задачи интегрирования в конечном виде возникла общая идея изучать свойства и величины, связанные с функциями $\varphi(x, y)$, *инвариантные* относительно всевозможных преобразований типа (3). В том особенно важном случае, когда преобразования (3) рационально обратимы, они носят название *бирациональных преобразований*. Таким образом, теорию алгебраических функций можно характеризовать как науку об инвариантных бирациональных преобразований. Это даёт право считать её одной из систем геометрии в смысле Клейна, который определил геометрию как науку об инвариантах той или иной группы (см. § 28) преобразований (см. также § 8).

Уточняя и упрощая постановку основной задачи теории алгебраических функций, формулируем её так. Даны два уравнения типа (1):

$$f_1(x, y) = 0, \quad f_2(x, y) = 0.$$

Найти системы из конечного числа величин, связанных с каждым

из этих уравнений и обладающих тем свойством, что их совпадение для обоих уравнений необходимо и достаточно для того, чтобы существовало преобразование типа (3), переводящее одно уравнение в другое.

Формулированную в таком виде задачу до сих пор не удалось решить. Известен один наиболее важный инвариант соотношения (1) — целое неотрицательное число $p$, называемое *жанром* уравнения [или, как говорят геометры, кривой (1)]. Кроме того, известно, что уравнение жанра $p$ при $p > 1$ зависит от $3p-3$ инвариантных параметров, которые Риман назвал *модулями* кривой (1); однако для них не дано более или менее удобных явных представлений.

Теория алгебраических функций исторически развивалась другими путями, притом независимо в нескольких различных направлениях. Одно из них, *функциональное*, ведёт своё начало от Абеля и получило совершенную форму у Римана (B. Riemann, 1824—1866), которому принадлежит гениальная идея изображать многозначную функцию комплексной переменной не на плоскости, а на особого рода многолистной поверхности, получившей название римановой. Эти поверхности, изученные Риманом на простейшем случае алгебраических функций, впоследствии сделались основным инструментом при изучении обширных классов общих функций и многих специальных функций (модулярных, автоморфных, интегралов линейных дифференциальных уравнений и т. п.).

Почти одновременно с Риманом, и в близком направлении, теория алгебраических функций была развита Вейерштрассом (K. Weierstrass, 1815—1897), который изучал поведение многозначных функций при помощи их разложений в степенные ряды. Впоследствии, узнав о результатах Римана, он переработал свои лекции, введя в них понятие римановой поверхности.

В связи с общим увлечением синтетической геометрией в середине прошлого века большая группа геометров предприняла систематическое изучение алгебраических кривых чисто геометрическими методами, и таким образом в теории аналитических функций возникло *геометрическое направление*, называемое также *алгебраической геометрией*. Из его пионеров мы должны назвать Плюккера, Клебша, Гордана, Брилля и Нётера. В настоящее время это направление было воспринято итальянской школой геометров (Кастельнуово, Энриквес, Севери и др.), перенесших своё внимание на алгебраические поверхности и получивших для них много результатов фундаментального значения.

Начало *арифметического направления* в теории алгебраических функций положено Дедекиндом (R. Dedekind), одним из творцов теории идеалов, написавшим совместно с Вебером (H. Weber) большую статью. Исходя из того, что совокупность функций типа $\varphi(x, y)$, обращающихся в нуль в какой-нибудь точке «абсолютной римановой поверхности», образует простой идеал, авторы

приходят к однозначному представлению функций $\varphi(x, y)$ в виде произведения простых идеалов (точнее, в виде частного от произведений простых идеалов).

Подобно тому как рациональную функцию от одной переменной можно представить в виде частного от произведений линейных множителей, т. е. определить её заданием значений, в которых она обращается в 0 и в $\infty$, и алгебраическую функцию можно представить в виде частного от произведений простых идеалов, причём числитель и знаменатель содержат одно и то же число простых множителей (являются идеалами одного и того же порядка). Их существенное различие состоит в том, что, произвольно задав нули и бесконечности (полюсы) рациональной функции, мы всегда найдём эту функцию; нули же и бесконечности алгебраической функции не могут быть заданы по произволу. Переходя к выработанному в теории чисел понятию эквивалентных идеалов и идеальных классов, мы скажем, что не всякие идеалы одного и того же порядка эквивалентны. Далее, эквивалентные классы образуют линейные семейства, и Дедекинд и Вебер устанавливают связь между порядком и измерением класса, который этот идеал образует (т. е. числом входящих в него линейно независимых идеалов). Вводя понятие класса дифференциалов, который имеет тесную связь с абелевыми интегралами, они чисто арифметическим путём приходят к центральному результату всей теории — теореме Римана-Роха. Вообще арифметическая теория даёт возможность вывести и представить большинство результатов из теории абелевых интегралов и теории алгебраических кривых чисто арифметическим, притом совершенно общим путём. Основное преимущество арифметической теории перед геометрической состоит в полной общности получаемых в ней результатов, в то время как в геометрической теории приходится вводить ограничения относительно характера особых точек, которые может иметь кривая (1).

В самое недавнее время выяснилось новое, притом вполне принципиальное, преимущество арифметической теории. Оказалось возможным распространить её на алгебраические функции, коэффициенты которых не являются произвольными комплексными числами, как это делалось в классической теории, а элементами любого заданного числового поля (например, рациональными числами или даже классами сравнений по простому модулю). Важность изучений такого рода алгебраических функций была осознана при попытках приложить теорию алгебраических функций к нахождению рациональных систем значений $x$, $y$, удовлетворяющих уравнению (1), т. е. при решении диофантовых уравнений весьма общего вида. Эта проблема является одной из наиболее ярких, хотя вовсе не единственной проблемой, характеризующей современное направление в теории алгебраических функций.

ГЛАВА I

# ТЕОРИЯ ПОЛЕЙ

## § 1. Понятия поля и кольца

*Полем* называют совокупность некоторых предметов (которые мы будем называть *элементами* поля), над которыми установлены два действия. Эти действия мы, по аналогии с арифметикой, будем называть *сложением* и *умножением*. При этом действия должны быть подчинены нижеследующим правилам:

1. *Сложение.* Установлено правило сопоставления с двумя любыми элементами $a$, $b$ поля третьего элемента, называемого их суммой и обозначаемого через $a+b$. При этом:

Сложение ассоциативно:

$$(a+b)+c=a+(b+c), \tag{1}$$

коммутативно:

$$a+b=b+a, \tag{2}$$

и однозначно обратимо. Последнее означает, что для произвольных $a$, $b$ можно указать, притом только один, элемент $x$ поля, для которого

$$a+x=b. \tag{3}$$

В частности, существует элемент $y$, для которого

$$a+y=a. \tag{4}$$

Докажем, что элемент $y$ независим от выбора элемента $a$. Для этого прибавим к обеим частям равенства (4) элемент $x$, определённый из равенства (3). Тогда в силу (1) и (2)

$$b+y=b,$$

где $b$ — произвольный другой элемент поля. Определённый таким образом элемент $y$ называют *нулём* и обозначают через 0.

Определённый из равенства (3) элемент $x$ называют *разностью* $b$ и $a$ и обозначают через $b-a$. В частности, разность $0-a$ называют обратным к $a$ элементом и обозначают просто через $-a$.

Отсюда легко выводятся обычные правила действий со скобками, ассоциативный закон для вычитания и т. п.

II. *Умножение.* Установлено другое правило сопоставления с двумя произвольными элементами $a$, $b$ поля третьего элемента, называемого их *произведением* и обозначаемого через $a \cdot b$. При этом:

Умножение ассоциативно:

$$(ab)\,c = a\,(bc); \tag{5}$$

оно коммутативно:

$$ab = ba; \tag{6}$$

наконец, сложение и умножение подчиняются дистрибутивному закону:

$$(a+b)\,c = ac + bc. \tag{7}$$

Заметим, что выражение в правой части могло бы привести к недоразумениям, так как в нём не указано, какие действия надо производить раньше. Ввиду этого принято считать, что в тех случаях, когда порядок действий не указан при помощи скобок, надо сначала произвести действия умножения, а затем уже действия сложения и вычитания.

Нетрудно доказать, что дистрибутивный закон распространяется также на вычитание:

$$(a-b)\,c = ac - bc. \tag{8}$$

Из дистрибутивного закона выводится правило умножения на нуль:

$$a \cdot 0 = a\,(b-b) = ab - ab = 0. \tag{9}$$

Совокупность элементов, удовлетворяющих этим правилам, носит название *кольца*. В кольце, вообще говоря, не предположена однозначная обратимость умножения или, как мы будем выражаться, выполнимость *деления*. Примерами колец могут служить:

1) совокупность всех целых чисел, положительных и отрицательных;

2) совокупность целых комплексных чисел, т. е. чисел вида $a+bi$, где $i = \sqrt{-1}$, а $a$ и $b$ принимают всевозможные целые значения;

3) совокупность всех полиномов от переменной $x$ (а также от нескольких независимых переменных $x_1, x_2, \ldots, x_n$).

Более частное понятие, чем кольцо, представляет *поле*. Чтобы совокупность рассматриваемых элементов составляла поле, надо, чтобы выполнялась:

III. *Однозначная обратимость умножения.* Это означает, что при любых заданных элементах $a$, $b$ существует, притом единственный, элемент $x$, для которого имеет место

$$ax = b. \tag{10}$$

Этот элемент принято обозначать через $b:a$ или $\frac{b}{a}$ ($b$, делённое на $a$, или частное от деления $b$ на $a$, или дробь с числителем $b$ и знаменателем $a$).

При этом мы должны исключить случай, когда $a = 0$. В самом деле, поскольку $0 \cdot x = 0$ при всяком $x$, уравнение $0 \cdot x = b$ при $b \neq 0$ не может иметь решения.

В частности, решение уравнения

$$ay = a$$

не зависит от выбора $a$. Его называют *единицей* и обозначают через 1. В некоторых случаях, когда это обозначение может привести к недоразумению, принято обозначать единицу буквой $e$ (см. § 2).

Ни одно из приведённых выше в виде примеров колец не является полем. Примером полей могут служить:

1) совокупность всех (положительных и отрицательных) *рациональных дробей*, т. е. чисел вида $\frac{b}{a}$, где $a$, $b$ — целые числа, причём $a \neq 0$;

2) совокупность чисел вида $a + bi$, где $i = \sqrt{-1}$, а $a$, $b$ принимают всевозможные рациональные значения;

3) совокупность всех рациональных функций, т. е. дробей, у которых числитель и знаменатель являются полиномами от переменной $x$ (или от нескольких переменных).

На этих трёх примерах мы видим, что по заданному кольцу бывает возможно определить поле, формально вводя в качестве его элементов частные от элементов заданного кольца и определяя действия над ними при помощи следующих правил:

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}; \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}; \quad \frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}.$$

Нетрудно проверить для таких элементов справедливость законов, установленных для поля. Далее,

$$\frac{a}{b} = \frac{c}{d}$$

тогда и только тогда, если

$$ad = bc.$$

Для доказательства транзитивности равенства при таком определении необходимо ещё следующее свойство кольца

IV. *Отсутствие делителей нуля.* Если $a \cdot b = 0$, то или $a = 0$, или $b = 0$.

В то время как для колец это свойство необходимо предположить, для полей оно доказывается. В самом деле, из $ab = 0$ и из существования элемента $\frac{1}{b}$ получаем:

$$ab \cdot \frac{1}{b} = a = 0.$$

Таким образом, если $b \neq 0$, то $a = 0$.

С другой стороны, существуют кольца, у которых условие IV не соблюдается, и тогда для них невозможно построить описанным образом поле, носящее название *поля частных* (Quotientenkörper).

## § 2. Подполя. Простые поля. Характеристика

Если часть элементов какого-нибудь поля $K$ сама образует поле $k$, то $k$ называется *подполем* поля $K$; говорят также, что $k$ входит в $K$, и обозначают это так:

$$k \subset K.$$

Поле $K$ иногда называют *надполем* поля $k$.

*Пример.* Если $K$ — поле рациональных функций от переменных $x_1, x_2, \ldots, x_n$, то поля рациональных фуикций от переменных

$$x_1, x_2, \ldots, x_k \qquad (k = 1, 2, \ldots, n-1)$$

могут служить примерами подполей.

Если $k \subset K$ и притом поля $k$ и $K$ не совпадают, то $k$ называется *истинным подполем* поля $K$. Поле, не содержащее истинных подполей, называется *простым полем*.

*Всякое поле $K$ содержит в качестве подполя одно единственное простое поле.* Для его нахождения возьмём единицу $e$ поля $K$ (которая должна входить во все подполя) и образуем элементы

$$(1) \qquad \begin{gathered} e+e=2e, \quad 2e+e=3e, \quad \ldots, \\ 0, -e, \quad -2e, \quad -3e, \quad \ldots, \end{gathered}$$

составляющие кольцо, которое, очевидно, содержится во всяком подполе поля $K$. Здесь нам придётся различать две возможности:

1) Все элементы (1) различны между собой. В этом случае они образуют кольцо, элементы которого отличаются от целых рациональных чисел только множителем $e$, который в силу $e^2 = e$ не играет никакой роли. В этом случае мы можем полагать $e = 1$. Дополним полученное кольцо целых рациональных чисел до поля отношений, т. е. до поля дробных рациональных чисел. Это поле входит во все подполя поля $K$ и потому является простым полем. В этом случае мы будем говорить, что поле $K$ есть поле *характеристики нуль*.

2) Может случиться, что не все элементы отличны друг от друга. Пусть

$$me = ne \qquad (m \neq n).$$

Тогда

$$(m - n)\, e = 0.$$

Пусть $p$ есть наименьшее из целых положительных чисел, для которых имеет место

$$p \cdot e = 0.$$

Число $p$ должно быть простым числом, так как в противном случае из

$$p = qr \qquad (q < p,\ r < p)$$

мы бы имели:

$$qe \neq 0, \quad re \neq 0, \quad qe \cdot re = 0,$$

что противоречит условию IV.

Простое число $p$ носит название *характеристики* поля $K$. Выделенное нами кольцо $R_p$ состоит из $p$ различных элементов

$$0,\ e,\ 2e,\ \ldots,\ (p-1)\, e. \tag{2}$$

Эти элементы при сложении и умножении ведут себя как вычеты по модулю $p$. Кольцо $R_p$ является также полем и потому не нуждается в дополнении до поля частных. В самом деле, если умножить весь ряд (2) на один и тот же элемент типа (2), например, на $ae$ $(0 < a < p)$, то ряд

$$0,\ ae,\ 2ae,\ \ldots,\ (p-1)\, ae \tag{3}$$

будет состоять из $p$ различных элементов (из $ake = ale$, т. е. $al\,(k-l)\, e = 0$, в силу $ae \neq 0$ и свойства IV следует $ke = le$), а потому он только порядком отличается от ряда (2). Из этого следует, что уравнение

$$ae \cdot xe = be$$

при $0 < a < p$ всегда имеет, притом единственное, решение $xe$. Деление всегда возможно.

Поле $R_p$ является простым полем. Таким образом:

*Всякое поле содержит в качестве простого подполя или поле $R$ рациональных чисел, или конечное поле $R_p$ сравнений по простому модулю $p$.*

Введём понятие *изоморфизма* двух полей:

Два поля $K$ и $k$ называются изоморфными, если между элементами $A,\ B,\ C, \ldots$ поля $K$ и элементами $a,\ b,\ c, \ldots$ поля $k$ можно установить такое взаимно однозначное соответствие:

$$A \longleftrightarrow a, \quad B \longleftrightarrow b, \quad C \longleftrightarrow c, \ \ldots,$$

что при этом

$$A+B \longleftrightarrow a+b, \quad A\cdot B \longleftrightarrow a\cdot b, \quad \ldots$$

Тогда полученный только что результат может быть формулирован так:

Всякое поле содержит одно единственное простое подполе, которое изоморфно или с полем $R$ рациональных чисел, или с полем $R_p$ сравнений по простому модулю $p$.

Во втором из этих случаев будем говорить, что поле $k$ есть поле *характеристики* $p$.

## § 3. Расширения полей. Трансцендентные расширения

Пусть дано какое-нибудь поле $k$ и какой-нибудь элемент $x$, не входящий в $k$, но над которым вместе с элементами из $k$ установлены правила действий, подчиняющиеся условиям I — IV. Наименьшее поле, содержащее как $k$, так и $x$, есть поле рациональных функций от $x$ с коэффициентами из поля $k$. (Рациональной функцией мы называем частное от деления двух полиномов.) Его называют *расширением* поля $k$ присоединением элемента $x$ и обозначают через $k(x)$. Расширяя поле $k(x)$ при помощи нового элемента $y$, мы получим расширение $k(x, y)$ поля $k$ при помощи двух элементов $x$, $y$. Таким путём можно расширить поле $k$ при помощи любого числа элементов.

Остановимся на поле $k(x)$. Будем различать два типа расширений. К первому типу относятся поля $k(x)$ в том случае, когда $x$ удовлетворяет соотношению

$$(1) \qquad f(x) = A_0x^n + A_1x^{n-1} + \ldots + A_{n-1}x + A_n = 0,$$

где $A_0$, $A_1$, $\ldots$, $A_{n-1}$, $A_n$ суть элементы поля $k$, не равные одновременно нулю. Расширения этого типа называются *алгебраическими расширениями*. В том же случае, когда соотношений типа (1) не существует, расширения $k(x)$ носят название *трансцендентных расширений*.

Трансцендентное расширение $k(x)$ есть совокупность дробных рациональных функций вида

$$\frac{\varphi(x)}{\psi(x)},$$

где $\varphi(x)$ и $\psi(x)$ — полиномы от $x$ с коэффициентами из $k$. Для полного определения этого поля необходимо установить, какие из этих элементов мы должны считать равными. Предварительно остановимся на элементах кольца полиномов от $x$ с коэффициентами из $k$, составляющих подкольцо поля $k(x)$. Два полинома

$$\varphi(x) = a_0 + a_1x + \ldots + a_mx^m,$$
$$\psi(x) = b_0 + b_1x + \ldots + b_nx^n$$

равны тогда и только тогда, когда их степени $m$ и $n$ равны: $m = n$, и притом равны коэффициенты при одинаковых степенях $x$:

$$a_k = b_k \qquad (k = 0,\ 1,\ 2,\ \ldots,\ m).$$

В самом деле, если бы имело место

$$\varphi(x) = \psi(x) \tag{2}$$

при несоблюдении этих условий, то равенство (2) привело бы нас к нетождественному соотношению типа (1), что противоречит условию.

Возвратимся к элементам общего вида поля $k(x)$.

Пусть

$$\frac{\varphi(x)}{\psi(x)} = \frac{\varphi_1(x)}{\psi_1(x)}. \tag{3}$$

Умножая это равенство на полином $\psi(x) \cdot \psi_1(x)$, мы получим равенство

$$\varphi(x) \cdot \psi_1(x) = \varphi_1(x) \cdot \psi(x). \tag{4}$$

Это равенство полиномов должно соблюдаться в определённом выше смысле. Оно также достаточно для того, чтобы имело место (3), в чём мы убедимся, деля (4) на $\psi(x) \cdot \psi_1(x)$.

Если имеет место (3), то не обязательно, чтобы были равны друг другу числители и знаменатели левой и правой частей этого равенства. В этом легко убедиться, умножая числитель и знаменатель какой-нибудь дроби на один и тот же полином. Мы покажем, однако, что всякую дробь можно привести к такому *нормальному* (*несократимому*) виду, что две нормальные дроби равны друг другу только тогда, когда отдельно равны их числители и знаменатели.

Если частное двух полиномов $f(x)$ и $g(x)$ есть тоже полином, будем говорить, что $f(x)$ *делится* на $g(x)$. Очевидно, что

I. *Если* $f_1(x)$ и $f_2(x)$ *делятся на* $g(x)$, *то и* $f_1(x) \pm f_2(x)$ *делятся на* $g(x)$.

II. *Если* $f(x)$ *делится на* $g(x)$, *а* $g(x)$ *делится на* $h(x)$, *то и* $f(x)$ *делится на* $h(x)$.

Для вывода нетривиальных теорем о делимости введём алгоритм Эвклида. Предварительно заметим, что если степени полиномов $f(x)$ и $g(x)$ равны $m$ и $n$, то можно (при помощи деления), притом единственным образом, определить полином $q(x)$ (частное) и полином $r(x)$ степени $< n$ (остаток) так, чтобы для них имело место

$$f(x) = g(x) \cdot q(x) + r(x).$$

Коэффициенты полиномов $q(x)$ и $r(x)$ тоже будут лежать в $k$.

Пользуясь этим приёмом, будем постепенно находить для каждой пары последовательных полиномов

$$f,\ g,\ r_1,\ r_2,\ \ldots$$

остатки, связанные друг с другом так:

$$
\begin{aligned}
f &= g \cdot q + r, \\
g &= r \cdot q_1 + r_1, \\
r &= r_1 \cdot q_2 + r_2, \\
&\cdots\cdots\cdots\cdots
\end{aligned}
\tag{5}
$$

Степени полиномов этой последовательности постепенно убывают, так что процесс должен оборваться на конечном месте. Последний из остатков, $r_k$ (на который $r_{k-1}$ делится нацело), есть *общий наибольший делитель* полиномов $f$ и $g$, в чём нетрудно убедиться. Кроме того, исключая из тождеств (5) промежуточные остатки $r$, $r_1$, $\ldots$, $r_{k-1}$, мы придём к соотношению

$$f \cdot X + g \cdot Y = r_k, \tag{6}$$

где $X$, $Y$ — некоторые полиномы с коэффициентами из поля $k$.

Если $r_k = \text{const.}$, то полиномы $f$ и $g$ называются *взаимно простыми*. Пользуясь (6), нетрудно доказать следующие теоремы о делимости:

III. *Если произведение $f \cdot g$ делится на $h$, и притом $f$ и $h$ взаимно просты, то $g$ делится на $h$.*

IV. *Если каждый из полиномов $f_1$, $f_2$ взаимно прост с $g$, то и их произведение $f_1 \cdot f_2$ взаимно просто с $g$.*

Эту теорему легко распространить на любое число множителей.

V. *Если полином $f$ делится на каждый из полиномов $g$, $h$, взаимно простых друг с другом, то $f$ делится на произведение $g \cdot h$.*

Из этих теорем весьма просто выводится однозначность разложения полиномов на простые множители. Под *неприводимым* (простым) в поле $k$ полиномом мы будем разуметь полином с коэффициентами в $k$, не имеющий, кроме самого себя и постоянных, делителей с коэффициентами из $k$. Из этого определения следует *):

Любой полином или делится на неприводимый полином, или взаимно прост с ним.

В частности:

Два различных (т. е. отличающихся друг от друга не только постоянным множителем) неприводимых полинома взаимно просты.

Предположим, что полином разложен на неприводимые множители двумя различными путями:

$$f = f_1 \cdot f_2 \cdots f_s = g_1 \cdot g_2 \cdots g_t \tag{7}$$

Предположив, что $f_1$ не совпадает ни с одним из полиномов $g_1$, $g_2, \ldots, g_t$, мы, в силу доказанного, убеждаемся в его взаимной

*) В дальнейшем под «полиномом» мы будем разуметь полином с коэффициентами из $k$.

простоте с ними и, в силу IV, во взаимной простоте с их произведением, т. е. с $f$, что невозможно. Таким образом $f_1$ совпадает с одним из $g_1, g_2, \ldots, g_t$. Сокращая на него равенство (7) и продолжая рассуждение, мы придём к теореме:

VI. *Всякий полином однозначно разлагается на простые множители.*

Пусть дана дробь

$$\frac{f(x)}{g(x)},$$

где $f(x)$ и $g(x)$ — полиномы. Сокращая её, т. е. деля $f(x)$ и $g(x)$ на их общий наибольший делитель, мы получим:

$$\frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)},$$

где $f_1(x)$ и $g_1(x)$ — взаимно простые полиномы. Будем говорить, что в этом случае элемент $\frac{f(x)}{g(x)}$ поля $k(x)$ приведён к *нормальному виду*. Если

$$\frac{f_1(x)}{g_1(x)} = \frac{f_2(x)}{g_2(x)},$$

где $f_1(x)$, $g_1(x)$, а также $f_2(x)$, $g_2(x)$ взаимно просты, то $f_1(x)$ и $f_2(x)$, а также $g_1(x)$ и $g_2(x)$ отличаются постоянными множителями. В самом деле, мы имеем:

$$f_1(x)g_2(x) = g_1(x)f_2(x).$$

Но так как $f_1(x)$ и $g_1(x)$ взаимно просты, то, в силу III, $g_2(x)$ делится на $g_1(x)$, а также $f_2(x)$ делится на $f_1(x)$. Точно так же, в силу взаимной простоты $f_2(x)$ и $g_2(x)$, полином $g_1(x)$ делится на $g_2(x)$, а $f_1(x)$ делится на $f_2(x)$. Поэтому элементы

$$\frac{g_2(x)}{g_1(x)}, \quad \frac{f_2(x)}{f_1(x)}$$

являются полиномами, причём обратные им элементы — тоже полиномы. Отсюда следует, что оба эти элемента — константы. В самом деле, если $\varphi(x)$ и $\psi(x)$ — полиномы и

$$\varphi(x) \cdot \psi(x) = 1,$$

то, в силу того, что степень $\varphi(x) \cdot \psi(x)$ равна сумме степеней $\varphi(x)$ и $\psi(x)$, и из неотрицательности последних степеней следует, что степени $\varphi(x)$ и $\psi(x)$ равны нулю.

Результат, выраженный в формуле (6), важен ещё с другой точки зрения: из него вытекает, что неопределённое уравнение

$$a \cdot X + b \cdot Y = c, \tag{8}$$

где $a$, $b$, $c$ — полиномы от $x$, имеет решение в полиномах тогда и только тогда, когда $c$ делится на общий наибольший делитель полиномов $a$ и $b$. В частности, если $a$, $b$ — взаимно простые полиномы и $c$ — произвольный полином, то уравнение (8) всегда имеет решение в полиномах.

На практике удобнее всего решать уравнение (8) следующим образом. Пусть степень $a$ выше (или равна) степени $b$ и пусть

$$a = bq + r, \quad c = bq_1 + r_1,$$

где степени $r$ и $r_1$ ниже степени $b$. Подставляя в (8), получим:

$$r \cdot X + b \cdot Z = r_1, \tag{9}$$

где

$$Z = qX + Y - q_1.$$

Очевидно, что если $X$, $Y$ — полиномы, то и $X$, $Z$ — полиномы, и обратно. Таким образом, мы привели задачи к решению неопределённого уравнения (9), у которого степени коэффициентов ниже, чем у (8). Продолжая процесс, мы в конце концов придём к уравнению, у которого один из коэффициентов при неизвестных — константа. Такое уравнение решается элементарно.

## § 4. Расширения полей алгебраические

Если элемент $\alpha$, не принадлежащий полю $k$, удовлетворяет алгебраическому уравнению

$$f(x) = A_0x^n + A_1x^{n-1} + \ldots + A_{n-1}x + A_n = 0, \tag{1}$$

где коэффициенты $A_0, A_1, \ldots, A_{n-1}, A_n$ лежат в $k$, то расширение $k(\alpha)$ поля $k$, т. е. совокупность рациональных функций от $x$ с коэффициентами из $k$, знаменатели которых взаимно просты с $f(x)$, является полем, которое мы будем называть *простым алгебраическим расширением поля $k$*.

Будем предполагать полином $f(x)$ неприводимым в поле $k$. В противном случае мы из

$$f(\alpha) = \varphi(\alpha) \cdot \psi(\alpha) = 0,$$

в силу предполагаемого отсутствия делителей нуля в поле $k(\alpha)$ (см. § 1, IV), заключили бы, что или $\varphi(\alpha) = 0$, или $\psi(\alpha) = 0$; тогда в качестве $f(x)$ мы могли бы взять один из этих множителей. Полином $f(x)$ с указанными свойствами определён однозначно с точностью до множителя из поля $k$.

Теорема 1. *Всякий элемент поля $k(\alpha)$ может быть представлен, и притом однозначно, в форме полинома $x$ степени $< n$.*

Доказательство. Пусть

$$y = \frac{g(\alpha)}{h(\alpha)},$$

где $g(x)$, $h(x)$ — полиномы, которые мы можем считать взаимно простыми. Полиномы $h(x)$ и $f(x)$ взаимно просты, так как иначе $h(x)$ делился бы на $f(x)$ (в силу неприводимости последнего), и тогда $h(\alpha) = 0$; но мы исключили деление на нуль. Поэтому неопределённое уравнение

$$h(x) \cdot U + f(x) \cdot V = g(x)$$

имеет решение в полиномах. Полагая $x = \alpha$, получим:

$$U(\alpha) = \frac{g(\alpha)}{h(\alpha)} = y.$$

Если степень полинома $U(x)$ не меньше $n$, то, деля $U(x)$ на $f(x)$ с остатком:

$$U(x) = f(x) \cdot q(x) + U_1(x),$$

мы получим при $x = \alpha$:

$$y = U(\alpha) = U_1(\alpha),$$

причём степень полинома $U_1(x)$ уже $< n$.

Пусть $y$ можно представить в виде двух различных полиномов степени $< n$:

$$y = U_1(\alpha) = U_2(\alpha).$$

Полином

$$U_1(x) - U_2(x)$$

степени $< n$ не может быть взаимно прост к $f(x)$, так как тогда неопределённое уравнение

$$[U_1(x) - U_2(x)]\, X + f(x) \cdot Y = 1$$

решалось бы в полиномах. Полагая в нём $x = \alpha$, мы пришли бы к равенству

$$0 = 1.$$

Таким образом, $U_1(x) - U_2(x)$ должен делиться на $f(x)$, что невозможно, так как степень первого полинома $< n$.

Теорема 2. *Всякий элемент поля $k(x)$ удовлетворяет уравнению степени $n$ с коэффициентами из поля $k$.*

Доказательство. Пусть

$$y = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1},$$

где $c_i \subset k$ [из теоремы 1 следует возможность такого представления для любого элемента поля $k(x)$]. Умножим это равенство на $\alpha$ и приведём его правую часть при помощи соотношения $f(\alpha) = 0$ к виду:

$$y \cdot \alpha = c_{10} + c_{11}\alpha + \ldots + c_{1,\,n-1}\alpha^{n-1},$$

где $c_{ij} \subset k$. Продолжим процесс:

$$y \cdot \alpha^2 = c_{20} + c_{21}\alpha + \ldots + c_{2,\,n-1}\alpha^{n-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$y \cdot \alpha^{n-1} = c_{n-1,\,0} + c_{n-1,\,1}\alpha + \ldots + c_{n-1,\,n-1}\alpha^{n-1}.$$

Перепишем эти равенства так:

$$(c_0 - y) + c_1\alpha + \ldots + c_{n-1} \cdot \alpha^{n-1} = 0,$$
$$c_{10} + (c_{11} - y)\alpha + \ldots + c_{1,\,n-1} \cdot \alpha^{n-1} = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$c_{n-1,\,0} + c_{n-1,\,1} \cdot \alpha + \ldots + (c_{n-1,\,n-1} - y)\,\alpha^{n-1} = 0.$$

Исключая из этой системы $1, \alpha, \ldots, \alpha^{n-1}$, получим уравнение

$$(2) \qquad \begin{vmatrix} c_0 - y, & c_1, & \ldots, & c_{n-1} \\ c_{10}, & c_{11} - y, & \ldots, & c_{1,\,n-1} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ c_{n-1,\,0}, & c_{n-1,\,1}, & \ldots & c_{n-1,\,n-1} - y \end{vmatrix} = 0,$$

которое имеет степень $n$ относительно $y$.

Поле $k(y)$, в котором элемент $y$ удовлетворяет соотношению (2), является в общем случае частью поля $k(\alpha)$. В каком случае оба поля совпадают?

Теорема 3. *Чтобы поля $k(y)$ и $k(\alpha)$ совпадали, необходимо и достаточно, чтобы уравнение* (2) *было неприводимо в поле $k$.*

Доказательство. Условие необходимо. В самом деле, если уравнение (2) приводимо, то $y$ удовлетворяет неприводимому в поле $k$ уравнению степени $n_1 < n$. Тогда, предположив, что $k(y) = k(\alpha)$, мы должны иметь рациональное выражение элемента $\alpha$ через $y$. Применяя теоремы 1 и 2, мы получим для $\alpha$ уравнение степени $n_1$, что противоречит неприводимости полинома $f(x)$.

Условие достаточно. С самом деле, представим степени элемента $y$ в виде полиномов степени $< n$ относительно $\alpha$:

$$1 = 1,$$
$$y = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1},$$
$$y^2 = c^*_{20} + c^*_{21}\alpha + \ldots + c^*_{2,\,n-1}\alpha^{n-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(3) \qquad y^{n-1} = c^*_{n-1,0} + c^*_{n-1,1}\alpha + \ldots + c^*_{n-1,\,n-1}\alpha^{n-1}.$$

Если определитель

$$(4) \qquad \begin{vmatrix} 1, & 0, & \ldots, 0 \\ c_0, & c_1, & \ldots, c_{n-1} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ c^*_{n-1,\,0}, & c^*_{n-1,\,1}, & \ldots, c^*_{n-1,\,n-1} \end{vmatrix},$$

не равен нулю, то мы можем решить относительно $\alpha$ систему (3), рассматриваемую как система линейных относительно

$$1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}$$

уравнений, и таким образом получить рациональное выражение элемента $\alpha$ через $y$. Отсюда следует

$$k(\alpha) = k(y).$$

Если же определитель (4) равен нулю, то правые части уравнений (3) будут находиться в линейной зависимости с коэффициентами из $k$, откуда мы получим:

$$C_0 y^{n-1} + C_1 y^{n-2} + \ldots + C_{n-1} = 0,$$

где $C_i \subset k$. Таким образом $y$ будет удовлетворять уравнению степени $< n$. Из этого следует, что уравнение (2) не может быть неприводимым, ч. т. д.

Будем называть систему из $n$ элементов

$$[\omega_1,\ \omega_2,\ \ldots,\ \omega_n]$$

поля $k(\alpha)$ *базисом* поля $k(\alpha)$ относительно $k$ в том случае, если всякий элемент поля $k(\alpha)$ может быть представлен в форме

$$b_1\omega_1 + b_2\omega_2 + \ldots + b_n\omega_n,$$

где $b_i \subset k$. В частности, из теоремы 1 следует, что $[1, \alpha, \ldots, \alpha^{n-1}]$ есть базис поля $k(\alpha)$. Очевидна

Теорема 4. *Чтобы система элементов* $[\omega_1, \omega_2, \ldots, \omega_n]$ *поля* $k(\alpha)$ *была базисом этого поля, необходимо и достаточно, чтобы элементы* $\omega_1, \omega_2, \ldots, \omega_n$ *выражались через базис* $[1, \alpha, \ldots, \alpha^{n-1}]$ *линейной подстановкой с не равным нулю определителем.*

Присоединяя к полю $k$ несколько (конечное число) элементов, каждый из которых удовлетворяет алгебраическому уравнению с коэффициентами из $k$, мы получим новое поле, которое будем называть *конечным алгебраическим расширением* поля $k$. Для него всегда можно построить базис. В самом деле, если $\alpha_k$ удовлетворяет неприводимому уравнению степени $n_k$ $(k = 1, 2, \ldots, s)$, то всякий элемент поля $k(\alpha_1, \alpha_2, \ldots, \alpha_s)$ можно линейно (с коэффициентами из $k$) выразить через систему элементов

$$(5)\quad \alpha_1^{r_1}\alpha_2^{r_2}\ldots\alpha_s^{r_s} \qquad (r_k = 0, 1, \ldots, n_k - 1;\ k = 1, 2, \ldots, s).$$

Это очевидно для элементов, выражаемых полиномами от $\alpha_1, \alpha_2, \ldots, \alpha_s$. С другой стороны, если элемент выражен как частное от таких полиномов, то, применяя теорему 1 сначала к знаменателю, рассматриваемому как полином от $\alpha_s$ в поле $k(\alpha_1, \alpha_2, \ldots, \alpha_{s-1})$, мы представим знаменатель в виде полиинома от $\alpha_1, \alpha_2, \ldots, \alpha_{s-1}$; избавляясь в его выражении от $\alpha_{s-1}$ и продолжая процесс, мы в конце концов освободимся от знаменателя.

Элементы (5) могут быть связаны линейными соотношениями с коэффициентами из $k$. Число линейно независимых элементов (5) носит название *степени* поля $k(\alpha_1, \alpha_2, \ldots, \alpha_s)$ относительно $k$, или просто *степени* поля $k(\alpha_1, \alpha_2, \ldots, \alpha_s) : k$. Ясно, что эта степень, равная числу элементов базиса поля, не зависит от выбора базиса. Повторяя рассуждения теоремы 2, мы убедимся, что всякий элемент поля $k(\alpha_1, \alpha_2, \ldots, \alpha_s)$ удовлетворяет уравнению степени, не превышающей степени поля. Если для какого-нибудь элемента $\alpha$ этого поля построенное таким образом уравнение окажется неприводимым, то поле $k(\alpha_1, \alpha_2, \ldots, \alpha_s)$ есть простое расширение поля $k$: $k(\alpha_1, \alpha_2, \ldots, \alpha_s) = k(\alpha)$. В самом деле, в этом случае элементы $1, \alpha, \ldots, \alpha^{n-1}$ линейно независимы и потому выразятся через элементы первоначального базиса с не равным нулю определителем, откуда следует, что и элементы первоначального базиса выражаются через базис $[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$.

Теорема 5. *Если поле $k_1 : k$ имеет степень $n_1$, а поле $k_2 : k_1$ — степень $n_2$, то поле $k_2$ тоже является конечным алгебраическим расширением поля $k$, и степень $k_2 : k$ равна $n$, $n_2$.*

Доказательство. Пусть $[\omega_1, \omega_2, \ldots, \omega_{n_1}]$ будет базис поля $k_1 : k$, а $[\alpha_1 \alpha_2, \ldots, \alpha_{n_2}]$ — базис поля $k_2 : k_1$. Тогда всякий элемент поля $k_2$ может быть представлен в форме

$$c_1\alpha_1 + c_2\alpha_2 + \ldots + c_{n_2}\alpha_{n_2},$$

где $c_k \subset k_1$. С другой стороны, каждый элемент $c_k$ может быть представлен в форме

$$a_1\omega_1 + a_2\omega_2 + \ldots + a_{n_1}\omega_{n_1},$$

где $a_k \subset k$.

Таким образом, всякий элемент поля $k_2$ может быть линейно представлен через систему элементов

$$\omega_\mu \alpha_\nu \qquad (\mu = 1, 2, \ldots, n_1;\ \nu = 1, 2, \ldots, n_2) \tag{6}$$

с коэффициентами из $k$. С другой стороны, система элементов (6) линейно независима. В самом деле, если бы существовала зависимость

$$\sum_{\mu,\ \nu} c_{\mu\nu}\omega_\mu\alpha_\nu = 0, \tag{7}$$

где $c_{\mu\nu} \subset k$, то её можно было бы переписать так:

$$\sum_{\nu} b_\nu \alpha_\nu = 0, \tag{8}$$

где

$$b_\nu = \sum_{\mu} c_{\mu\nu}\omega_\mu. \tag{9}$$

Но так как элементы $\alpha_\nu$ независимы относительно поля $k_1$, в котором лежат $b_\nu$, то из (8) следует $b_\nu = 0$; тогда из (9), в силу независимости элементов $\omega_\mu$ относительно $k$, следует $c_{\mu\nu} = 0$. Таким образом степень $k_2 : k$, т. е. число элементов базиса (6) поля $k_2 : k$, равна $n_1$, $n_2$, ч. т. д.

## § 5. Кратные корни. Совершенные поля

Пусть дан неприводимый в поле $k$ полином $f(x)$. Присоединяя к полю $k$ корень $\alpha_1$ этого полинома (хотя бы формально), мы придём к полиному

$$f_1(x) = \frac{f(x)}{x - \alpha_1}$$

с коэффициентами из поля $k(\alpha_1)$ *). Присоединяем к полю $k(\alpha_1)$ корень этого полинома $\alpha_2$. Получится полином

$$f_2(x) = \frac{f(x)}{(x - \alpha_1)(x - \alpha_2)}$$

с коэффициентами из поля $k(\alpha_1, \alpha_2)$. Продолжая процесс, мы в конце концов получим для $f(x)$ выражение

$$f(x) = a_0 (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

Для заданного полинома $f(x)$ важно установить, можно ли считать все корни $\alpha_1, \alpha_2, \dots, \alpha_n$ различными или они частично или полностью должны совпадать друг с другом. Казалось бы, что этот вопрос, в силу формального определения корней $\alpha_1, \alpha_2, \dots, \alpha_n$, не имеет определённого смысла. Однако оказывается, что он допускает вполне определённое решение, выражаемое в виде условия, налагаемого на коэффициенты полинома $f(x)$. Это условие проще всего формулировать, введя чисто формально понятие производной от полинома. Под *производной* $f'(x)$ от $f(x)$ мы будем разуметь коэффициент при $h$ в разложении $f(x + h)$ по степеням $h$. Из этого определения мы легко выведем следующие общеизвестные формулы:

$$c' = 0, \quad (u + v)' = u' + v', \quad (cu)' = c \cdot u',$$
$$(uv)' = uv' + vu', \quad (x^m)' = mx^{m-1}.$$

Пусть $\alpha$ есть корень полинома $f(x)$, имеющий точно $s$-ю кратность. Это значит, что имеет место

$$f(x) = (x - \alpha)^s \cdot f_1(x), \qquad f_1(\alpha) \neq 0.$$

*) В современных курсах алгебры доказывается, что формальное присоединение корней $\alpha_1, \alpha_2, \dots, \alpha_n$ к полю $k$ приводит к полю, в котором соблюдаются все аксиомы. Этот факт рассматривается как замена «фундаментальной теоремы алгебры».

Беря от обеих частей производную, будем иметь:

$$(1)\qquad f'(x) = s(x-\alpha)^{s-1} f_1(x) + (x-\alpha)^s f_1'(x) = \\ = (x-\alpha)^{s-1}\{sf_1(x) + (x-\alpha)f_1'(x)\}.$$

Таким образом, производная $f'(x)$ имеет $\alpha$ корнем по крайней мере $(s-1)$-й кратности. В частности, при $s=1$ корень $\alpha$ не является корнем производной $f'(x)$. Отсюда следует

Теорема 6. *Чтобы полином $f(x)$ имел кратные корни, необходимо и достаточно, чтобы его общий наибольший делитель с производной $f'(x)$ был отличен от константы.*

Пусть $f(x)$ есть неприводимый полином. Если при этом поле $k$ имеет нулевую характеристику, то производная $f'(x)$ не равна тождественно нулю. Будучи степенью ниже, чем $f(x)$, она, в силу неприводимости полинома $f(x)$, взаимно проста с ним, в силу чего $f(x)$ не имеет кратных корней.

Если же поле $k$ имеет характеристику $p$, то производная от не равного константе полинома может быть равна нулю. Это имеет место тогда и только тогда, если показатель при $x$ в любом члене, входящем в полином, делится, на $p$; другими словами, если полином $f(x)$ имеет вид $g(x^p)$.

Поле, в котором всякий полином, имеющий кратные корни, приводим, называется *совершенным*. Таким образом мы имеем:

Теорема 7. *Всякое поле характеристики нуль совершенно.*

Пусть теперь $k$ будет поле характеристики $p$. Тогда для каждого элемента $a \subset k$ имеет место

$$p \cdot a = 0,$$

а потому

$$(a+b)^p = a^p + b^p, \quad (ab)^p = a^p \cdot b^p,$$

так что $p$-е степени всех элементов поля образуют поле, которое мы будем обозначать через $k^p$. Подобным же образом определим поля

$$k^{p^2},\ k^{p^3},\ \ldots.$$

Теорема 8. *Чтобы поле $k$ характеристики $p$ было совершенным, необходимо и достаточно, чтобы имело место*

$$(2)\qquad k^p = k.$$

Доказательство. Условие достаточно. В самом деле, всякий полином с равной нулю производной имеет вид

$$g(x^p) = a_0 + a_1 x^p + \ldots + a_n x^{pn}.$$

Из условия (2) следует, что поле $k$ содержит элементы $b_0, b_1, \ldots, b_n$, для которых имеет место

$$b_0^p = a_0,\ b_1^p = a_1,\ \ldots,\ b_n^p = a_n.$$

Вводя обозначение

$$h(x) = b_0 + b_1 x + \ldots + b_n x^n,$$

мы будем иметь

$$[h(x)]^p = (b_0 + b_1 x + \ldots + b_n x)^p = \\ = a_0 + a_1 x^p + \ldots + a_n x^{pn} = g(x^p),$$

так что $g(x^p)$ не может быть неприводимым полиномом.

Условие необходимо. В самом деле, пусть $a \subset k$, и притом $a$ не равно $p$-й степени элемента из $k$. Рассмотрим полином $f(x) = x^p - a$. Присоединяя к полю $k$ элемент $b = \overline{a^{\frac{1}{p}}}$, будем иметь:

$$f(x) = x^p - a = (x - b)^p.$$

Предположим, что $f(x)$ разлагается в поле $k$ на множители:

$$f(x) = x^p - a = \varphi(x) \cdot \psi(x).$$

Тогда в поле $k(b)$ должно иметь место

$$\varphi(x) = (x - b)^\mu, \quad \psi(x) = (x - b)^{p-\mu}.$$

Подставляя $x = 0$, получим:

$$\varphi(0) = (-b)^\mu \subset k.$$

Решая неопределённое уравнение

$$\mu u - pv = 1,$$

будем иметь

$$a = a^{\mu u} : a^{pv} = b^{\mu u p} : a^{pv} = (-1)^{\mu u p} [\varphi(0)]^{up} : a^{pv},$$

откуда следует, что $a$ равно $p$-й степени элемента из $k$, что противоречит предположению. Итак, $x^p - a$ — неприводимый полином с равной нулю производной.

Пусть теперь $k$ будет *конечное поле*, т. е. поле, состоящее из конечного числа элементов. Докажем, что $k^p = k$. Возьмём в $k$ произвольный элемент $a$. В неограниченном ряду степеней

$$a, \ a^p, \ a^{p^2}, \ \ldots$$

в силу конечности $k$ элементы должны повторяться. Поэтому при каких-то $m$ и $n > 0$ должно иметь место

$$a^{p^{m+n}} = a^{p^m}, \quad n > 0.$$

Докажем, что $a^{p^n} = a$. В полях характеристики $p$ имеет место

$$(a + b)^p = a^p + b^p, \quad (a + b)^{p^2} = (a^p + b^p)^p = a^{p^2} + b^{p^2}, \ \ldots,$$
$$(a + b)^{p^m} = a^{p^m} + b^{p^m}, \ \ldots,$$

так что

$$(a^{p^n} - a)^{p^m} = a^{p^{n+m}} - a^{p^m} = 0$$

(мы предполагаем $p$ нечётным простым числом), откуда на основании свойства полей мы имеем

$$a^{p^n} - a = 0.$$

Таким образом, $a$ есть $p$-я степень элемента $a^{p^{n-1}}$. То же самое мы получим в случае $p = 2$, поскольку тогда $a = -a$. Таким образом, для конечных полей условие теоремы 8 всегда соблюдается, и они являются совершенными полями.

Примером несовершенного поля может служить совокупность рациональных функций, коэффициенты которых являются классами сравнений по модулю $p$. В несовершенных полях мы будем различать *расширения 1-го рода*, производимые корнями неприводимых полиномов без кратных корней, и *расширения 2-го рода*, производимые корнями неприводимых полиномов типа $g(x^p)$. Отметим, что полиномы этого типа делаются приводимыми, если присоединить к полю $k$ корни $p$-й степени из всех элементов поля.

Теорема 9. *Всякое конечное алгебраическое расширение совершенного поля $k$ есть простое расширение.*

Доказательство. Предположим, что поле $k$ содержит бесконечное множество элементов. Докажем, что поле $k(\alpha_1, \alpha_2, \ldots, \alpha_m)$, полученное путём присоединения к $k$ корней неприводимых уравнений

$$f_1(x) = 0, \quad f_2(x) = 0, \ldots, \quad f_m(x) = 0,$$

может быть получено присоединением к $k$ корня одного единственного уравнения. Достаточно доказать справедливость этого утверждения для $m = 2$. Пусть $\alpha$, $\beta$ являются корнями неприводимых уравнений

$$f(x) = 0, \quad g(x) = 0$$

степеней $m$ и $n$ и пусть $\alpha_1 = \alpha$, $\alpha_2, \ldots, \alpha_m$ и $\beta_1 = \beta$, $\beta_2, \ldots, \beta_n$ будут все корни этих уравнений. Выберем элемент $c \subset k$ так, чтобы

$$(3) \quad \alpha_i + c\beta_j \neq \alpha_1 + c\beta_1 \qquad (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n),$$

т. е. чтобы $c$ было отлично от

$$\frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \qquad (i = 1, 2, \ldots, m;\ \ j = 1, 2, \ldots, n).$$

Это возможно, так как $k$ содержит бесчисленное множество элементов. Составим уравнение, которому удовлетворяет

$$\xi = \alpha_1 + c\beta_1.$$

Это возможно сделать, построив для поля $k(\alpha, \beta)$ базис и поступая, как при доказательстве теоремы 2. Уравнения

$$f(\xi - cy) = 0, \quad g(y) = 0$$

(относительно $y$) имеют общий корень $y = \beta_1$. В силу условия (3) они не могут иметь других общих корней. Поэтому общий наибольший делитель полиномов $f(\xi - cy)$ и $g(y)$ линеен относительно $y$, может быть найден посредством алгоритма Эвклида и имеет вид

$$A(\xi) \cdot y + B(\xi).$$

Поскольку он обращается в нуль при $y = \beta_1$, мы имеем

$$\beta_1 = -\frac{B(\xi)}{A(\xi)},$$

откуда

$$\alpha_1 = \xi + c \cdot \frac{B(\xi)}{A(\xi)}.$$

Таким образом через элемент $\xi$ рационально выражаются $\alpha_1$, $\beta_1$, а потому и все элементы поля $k(\alpha_1\beta)$.

Пусть теперь $k$ — конечное поле. Тогда и после присоединения корней нескольких алгебраических уравнений мы получим конечное поле. Познакомимся ближе со структурой конечных алгебраических полей. Всякое конечное поле характеристики $p$ содержит простое подполе $R_p$, изоморфное с полем классов вычетов по модулю $p$. Пусть $[\alpha_1, \alpha_2, \ldots, \alpha_n]$ есть базис поля $k : R_p$. Тогда всякий элемент поля $k$ может быть представлен, притом однозначно, в форме

$$a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n,$$

где $a_1, a_2, \ldots, a_n$ пробегают систему элементов поля $R_p$. Таким образом, в поле $k$ содержится $p^n$ элементов, из которых $\sigma = p^n - 1$ отличны от нуля. Пусть это будут $\omega_1, \omega_2, \ldots, \omega_\sigma$. Выбрав любой элемент $\alpha \subset k$, $\alpha \neq 0$, мы убедимся, что произведения

$$\omega_1\alpha, \ \omega_2\alpha, \ \ldots, \ \omega_\sigma\alpha$$

совпадают с $\omega_1, \omega_2, \ldots, \omega_\sigma$ с точностью до порядка, откуда

$$\omega_1 \cdot \omega_2 \ldots \omega_\sigma \cdot \alpha^\sigma = \omega_1 \cdot \omega_2 \ldots \omega_\sigma.$$

Сокращая на $\omega_1 \cdot \omega_2 \ldots \omega_\sigma$, получим:

$$\alpha^\sigma = 1. \tag{4}$$

Если наименьший показатель, при котором $\alpha^\delta = 1$, есть $\delta$, то говорят, что $\alpha$ принадлежит к показателю $\delta$. Ясно, что $\delta$ есть делитель числа $\sigma$. Уравнение $x^\sigma - 1 = 0$ имеет ровно $\sigma$ корней $\omega_1, \omega_2, \ldots, \omega_\sigma$. Из того, что при всяком $\delta/\sigma$ полином $x^\delta - 1$ есть делитель $x^\sigma - 1$, следует, что $x^\delta - 1$ имеет ровно $\delta$ корней.

Пусть $\sigma = q_1^{\pi_1} \cdot q_2^{\pi_2} \dots q_s^{\pi_s}$. Уравнение

$$x^{q_i^{\pi_i}} - 1 = 0 \qquad (i = 1, 2, \dots, s) \tag{5}$$

имеет $q_i^{\pi_i}$ корней, а уравнение

$$x^{q_i^{\pi_i - 1}} - 1 = 0 \tag{6}$$

— $q_i^{\pi_i - 1}$ корней, которые все являются корнями уравнения (5). Отсюда, в силу $q_i^{\pi_i - 1} < q_i^{\pi_i}$, следует, что существуют корни уравнения (5), не являющиеся корнями уравнения (6). Такой корень (пусть это будет $\beta_i$) принадлежит к показателю $q_i^{\pi_i}$. Нетрудно убедиться, что произведение

$$\gamma = \beta_1 \cdot \beta_2 \dots \beta_s$$

принадлежит к показателю $\sigma$. Но тогда все элементы

$$1, \gamma, \gamma^2, \dots, \gamma^{\sigma - 1}$$

различны между собой и, значит, исчерпывают все отличные от нуля элементы поля $k$. Таким образом во всяком конечном поле все элементы выражаются степенями одного элемента. В частности, это имеет место для любого конечного алгебраического расширения конечного поля, которое в силу этого является простым расширением, ч. т. д.

## § 6. След, норма, дискриминант

Пусть $K$ — конечное алгебраическое расширение поля $k$ и пусть $[\omega_1, \omega_2, \dots, \omega_n]$ — базис поля $K$. С каждым элементом $\alpha$ поля $K$ можно сопоставить матрицу $A$, получаемую при выражении произведений $\alpha\omega_1, \alpha\omega_2, \dots, \alpha\omega_n$ через базис:

$$\begin{aligned}
\alpha\omega_1 &= a_{11}\omega_1 + a_{12}\omega_2 + \dots + a_{1n}\omega_n, \\
\alpha\omega_2 &= a_{21}\omega_1 + a_{22}\omega_2 + \dots + a_{2n}\omega_n, \\
&\dots\dots\dots\dots\dots\dots\dots \\
\alpha\omega_n &= a_{n1}\omega_1 + a_{n2}\omega_2 + \dots + a_{nn}\omega_n,
\end{aligned}$$

где $a_{ik} \subset k$. Считая $[\omega_1, \omega_2, \dots, \omega_n]$ матрицей, состоящей из одной строки, мы можем записать эту систему равенств в виде одного матричного равенства

$$\alpha\,[\omega_1, \omega_2, \dots, \omega_n] = [\omega_1, \omega_2, \dots, \omega_n] \cdot \begin{Vmatrix} a_{11}, & \dots, a_{n1} \\ \dots & \dots \\ a_{1n}, & \dots, a_{nn} \end{Vmatrix},$$

или так:

$$\alpha \cdot \Omega = \Omega \cdot A. \tag{1}$$

Известно, что операции над матрицами подчиняются ассоциативному и дистрибутивному законам, так что если, наряду с (1), мы имеем

$$\beta\Omega = \Omega \cdot B, \tag{2}$$

то отсюда можно заключить, что

$$\alpha\beta\Omega = \Omega AB, \tag{3}$$

$$(\alpha + \beta)\,\Omega = \Omega\,(A + B). \tag{4}$$

Из (3) и из того, что умножение элементов поля коммутативно, мы заключаем, что матрицы, соответствующие элементам поля $K$, тоже подчиняются коммутативному закону относительно умножения:

$$AB = BA. \tag{5}$$

***Нормой*** $N(\alpha)$ элемента $\alpha$ поля $K$ относительно поля $k$ называется определитель соответствующей ему матрицы:

$$N(\alpha) = |A|. \tag{6}$$

Из (3) следует, что произведению элементов соответствует произведение их матриц. Поэтому, если

$$N(\alpha) = |A|, \quad N(\beta) = |B|,$$

то

$$N(\alpha\beta) = |AB| = |A| \cdot |B|,$$

откуда

$$N(\alpha\beta) = N(\alpha) \cdot N(\beta). \tag{7}$$

Если мы присоединим к полям $k$ и $K$ переменную $t$ (трансцендентное расширение), то норма от разности $t - \alpha$ даст как раз полином, введённый нами при доказательстве теоремы 2, корнем которого является элемент $\alpha$:

$$N(t - \alpha) = f(t), \quad f(\alpha) = 0. \tag{8}$$

Если $\alpha \subset k$, то матрица $A$ будет иметь диагональную форму

$$A = \begin{Vmatrix} \alpha, & 0, & \ldots, & 0 \\ 0, & \alpha, & \ldots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & \ldots, & \alpha \end{Vmatrix},$$

так что

$$N(\alpha) = \alpha^n. \tag{9}$$

*Следом* $S(\alpha)$ элемента $\alpha$ поля $K$ относительно поля $k$ называется сумма диагональных элементов соответствующей ему матрицы:

$$S(\alpha) = a_{11} + a_{22} + \ldots + a_{nn}. \tag{10}$$

Из линейности этого выражения относительно элементов матрицы $A$ и из формулы (4) вытекает следующее:
если

$$S(\beta) = b_{11} + b_{22} + \ldots + b_{nn},$$

то

$$S(\alpha+\beta) = (a_{11}+b_{11}) + (a_{22}+b_{22}) + \ldots + (a_{nn}+b_{nn}) =$$
$$= (a_{11}+a_{22}+\ldots+a_{nn}) + (b_{11}+b_{22}+\ldots+b_{nn}),$$

откуда

$$S(\alpha+\beta) = S(\alpha) + S(\beta). \tag{11}$$

В случае, когда $\alpha \subset k$, имеем:

$$S(\alpha) = n \cdot \alpha. \tag{12}$$

Докажем, что выражения нормы и следа не зависят от выбора базиса. Пусть $\Omega'$ будет другой базис поля $K$ относительно $k$, получающийся из базиса путём линейной подстановки $U$, определитель которой не равен нулю:

$$\Omega' = \Omega \cdot U. \tag{13}$$

Из того, что $|U| \neq 0$, следует существование обратной матрицы $U^{-1}$, связанной с $U$ соотношением

$$U \cdot U^{-1} = U^{-1} \cdot U = \mathfrak{E},$$

где $\mathfrak{E}$ — *единичная матрица*, т. е.

$$\mathfrak{E} = \begin{Vmatrix} 1, & 0, & \ldots, & 0 \\ 0, & 1, & \ldots, & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & \ldots, & 1 \end{Vmatrix}.$$

Равенство (13) можно переписать так:

$$\Omega = \Omega' \cdot U^{-1}.$$

Найдём матрицу, соответствующую элементу $\alpha$ при базисе $\Omega'$:

$$\alpha\Omega' = \alpha\Omega U = \Omega A U = \Omega' U^{-1} A U,$$

откуда следует, что это будет матрица $U^{-1}AU$. Для нахождения $N(\alpha)$ при базисе $\Omega'$ найдём определитель этой матрицы:

$$N(\alpha) = |U^{-1}AU| = |U|^{-1} \cdot |A| \cdot |U| = |A|.$$

Мы видим, что в самом деле выражение $N(\alpha)$ не зависит от выбора базиса.

Чтобы доказать то же самое для следа $S(\alpha)$, обратим внимание на то, что след равен коэффициенту при $u^{n-1}$ в разложении определителя

$$|A_{+u}\mathfrak{E}|$$

по степеням $u$. Но

$$|U^{-1}AU_{+u}\mathfrak{E}| = |U^{-1}AU_{-u}U^{-1}\mathfrak{E}U| = |U|^{-1}\cdot|A_{-u}\mathfrak{E}|\cdot|U| = |A_{-u}\mathfrak{E}|$$

при любом $u$, откуда следует, что суммы диагональных элементов матриц $A$ и $U^{-1}AU$ равны. Таким образом выражение для следа тоже не зависит от выбора базиса.

*Дискриминант* базиса $\Omega = [\omega_1, \omega_2, \ldots, \omega_n]$ определяется при помощи формулы

$$(14)\quad \Delta[\omega_1, \omega_2, \ldots, \omega_n] = \begin{vmatrix} S(\omega_1^2), & S(\omega_1\omega_2), & \ldots; & S(\omega_1\omega_n) \\ S(\omega_2\omega_1), & S(\omega_2^2), & \ldots, & S(\omega_2\omega_n) \\ \ldots & \ldots & \ldots & \ldots \\ S(\omega_n\omega_1), & S(\omega_n\omega_2), & \ldots, & S(\omega_n^2) \end{vmatrix}.$$

Посмотрим, как изменится дискриминант, если мы от базиса $\Omega$ перейдём к новому базису

$$H = [\eta_1, \eta_2, \ldots, \eta_n],$$

связанному с $\Omega$ линейной подстановкой

$$H = \Omega\cdot U,$$

т. е.

$$(15)\qquad \eta_i = \sum_{\nu=1}^{n} \omega_\nu u_{\nu i} \qquad (i = 1, 2, \ldots, n).$$

Отсюда имеем:

$$S(\eta_i\eta_k) = \sum_{\nu=1}^{n} u_{\nu i} S(\omega_\nu\eta_k).$$

Подставляя в выражение для $\Delta[\eta_1, \eta_2, \ldots, \eta_n]$, получим:

$$\Delta[\eta_1, \eta_2, \ldots, \eta_n] = \begin{vmatrix} \sum_\nu u_{\nu 1} S(\omega_\nu\eta_1), & \ldots, & \sum_\nu u_{\nu 1} S(\omega_\nu\eta_n) \\ \ldots & \ldots & \ldots \\ \sum_\nu u_{\nu n} S(\omega_\nu\eta_1), & \ldots, & \sum_\nu u_{\nu n} S(\omega_\nu\eta_n) \end{vmatrix} =$$

$$= \begin{vmatrix} S(\omega_1\eta_1), & \ldots, & S(\omega_1\eta_n) \\ \ldots & \ldots & \ldots \\ S(\omega_n\eta_1), & \ldots, & S(\omega_n\eta_n) \end{vmatrix} \cdot \begin{vmatrix} u_{11}, & \ldots, & u_{1n} \\ \ldots & \ldots & \ldots \\ u_{n1}, & \ldots, & u_{nn} \end{vmatrix}.$$

Первый множитель этого выражения подобным же образом может быть преобразован при помощи формулы

$$S(\eta_i\omega_k) = \sum_{\nu=1}^{n} c_{\nu i} S(\omega_k\omega_\nu)$$

в произведение

$$\begin{vmatrix} S(\omega_1\eta_1), & \ldots, & S(\omega_1\eta_n) \\ \ldots\ldots\ldots\ldots \\ S(\omega_n\eta_1), & \ldots, & S(\omega_n\eta_n) \end{vmatrix} = \begin{vmatrix} S(\omega_1^2), & \ldots, & S(\omega_1\omega_n) \\ \ldots\ldots\ldots\ldots \\ S(\omega_n\omega_1), & \ldots, & S(\omega_n^2) \end{vmatrix} \cdot \begin{vmatrix} u_{11}, & \ldots, & u_{1n} \\ \ldots\ldots\ldots \\ u_{n1}, & \ldots, & u_{nn} \end{vmatrix},$$

откуда окончательно

$$\Delta(H) = \Delta(\Omega) \cdot |U|^2, \tag{16}$$

где

$$H = \Omega U.$$

Из формулы (16) вытекает весьма простой критерий того, чтобы система $n$ элементов поля $K$ была базисом этого поля относительно $k$. Этот критерий годится в том и только в том случае, если $K$ есть расширение 1-го рода над $k$.

Дискриминант степенного базиса $[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$ может быть представлен так:

$$\Delta[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}] = \begin{vmatrix} n, & s_1, & \ldots, & s_{n-1} \\ s_1, & s_2, & \ldots, & s_n \\ \ldots\ldots\ldots\ldots \\ s_{n-1}, & s_n, & \ldots, & s_{2n-2} \end{vmatrix}, \tag{17}$$

где $s_\nu = S(\alpha^\nu)$. Если $\alpha_1, \alpha_2, \ldots, \alpha_n$ — корни уравнения, которому удовлетворяет $\alpha$, то

$$S(\alpha^\nu) = \alpha_1^\nu + \alpha_2^\nu + \ldots + \alpha_n^\nu. \tag{18}$$

Подставляя эти выражения в (17), мы убедимся, что дискриминант может быть представлен в виде квадрата определителя Вандермонда (Vandermonde):

$$\Delta[1, \alpha, \ldots, \alpha^{n-1}] = \begin{vmatrix} 1, & \alpha_1, & \ldots, & \alpha_1^{n-1} \\ 1, & \alpha_2, & \ldots, & \alpha_2^{n-1} \\ \ldots\ldots\ldots\ldots \\ 1, & \alpha_n, & \ldots, & \alpha_n^{n-1} \end{vmatrix} = \prod_{\mu>\nu} (\alpha_\mu - \alpha_\nu)^2,$$

а поэтому обращается в нуль тогда и только тогда, когда среди корней уравнения, которому удовлетворяет $\alpha$, имеются кратные. Из этого

мы заключаем, что дискриминант степенного базиса для расширений 1-го рода отличен от нуля.

Теорема 10. *Чтобы система* $[\omega_1, \omega_2, \ldots, \omega_n]$ *элементов поля* $K$ *(расширение 1-го рода поля* $k$*) была базисом этого поля, необходимо и достаточно, чтобы её дискриминант был отличен от нуля.*

Доказательство. Для того чтобы система $[\omega_1, \omega_2, \ldots, \omega_n]$ была базисом поля $K$, необходимо и достаточно, чтобы она выражалась через степенной базис $[1, \alpha, \ldots, \alpha^{n-1}]$, где $\alpha$ — примитивный элемент поля $K$ при помощи линейной подстановки с не равным нулю определителем:

$$[\omega_1, \omega_2, \ldots, \omega_n] = [1, \alpha, \ldots, \alpha^{n-1}] \cdot U, \quad |U| \neq 0.$$

В самом деле, тогда эта подстановка обратима, и таким образом $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, а с ними и все элементы поля $K$ линейно выражаются через систему $[\omega_1, \omega_2, \ldots, \omega_n]$; в противном же случае между элементами этой системы имеет место линейное соотношение, и если бы она была базисом, то все элементы поля $K$ удовлетворяли в силу теоремы 2 уравнениям степеней $< n$, что противоречит условию.

Формула (16) даёт:

$$\Delta[\omega_1, \omega_2, \ldots, \omega_n] = \Delta[1, \alpha, \ldots, \alpha^{n-1}] \cdot |U|^2.$$

В правой части первый множитель отличен от нуля, а второй не равен нулю тогда и только тогда, когда система $[\omega_1, \omega_2, \ldots, \omega_n]$ есть базис. Отсюда вытекает справедливость теоремы.

## § 7. Теорема Люрота

Простое трансцендентное расширение поля $k$, т. е. поле $k(x)$, получаемое присоединением к $k$ элемента $x$, не удовлетворяющего никакому алгебраическому уравнению с коэффициентами из $k$, имеет бесчисленное множество подполей. Примером таких подполей могут служить поля, состоящие из рациональных функций от какой-нибудь одной рациональной функции $\varphi(x)$. Нетрудно видеть, что поле $k[\varphi(x)]$ изоморфно с $k(x)$. В самом деле, ясно, что $k[\varphi(x)]$ является трансцендентным расширением поля $k$, так как уравнение

$$F[\varphi(x)] = 0$$

можно рассматривать как уравнение относительно $x$, которое притом не может быть тождественным. Далее, если мы будем сопоставлять с каждым элементом $\psi(x)$ поля $k(x)$ элемент $\psi[\varphi(x)]$ поля $k[\varphi(x)]$, то из этого сопоставления следует, что сумме (а также произведению) элементов поля $k(x)$ будет соответствовать сумма (и произведение) элементов поля $k[\varphi(x)]$, причём разным элементам будут

соответствовать разные элементы. Этим изоморфизм обоих полей установлен.

Возникает вопрос, содержит ли $k(x)$ подполя другого типа? Если ограничиться рассмотрением подполей, содержащих поле $k$, то ответ получается отрицательный. Он даётся знаменитой теоремой Люрота (Lüroth). Для её доказательства введём определение *степени* для каждого элемента поля $k(x)$ и докажем одну вспомогательную теорему.

Определение. *Степенью элемента*

$$\varphi(x)=\frac{g(x)}{h(x)}$$

*поля* $k(x)$, *где* $g(x)$, $h(x)$ — *взаимно простые полиномы, называется наибольшая из степеней полиномов* $g(x)$ *и* $h(x)$.

Теорема 11 (Штейница). *Если функции* $\Phi(x)$ *и* $\varphi(x)$ *имеют, соответственно, степени* $n$ *и* $\nu$, *то степень функции* $\Phi[\varphi(x)]$ *равна* $n\cdot\nu$.

Доказательство. Очевидно, что степень функции $\Phi[\varphi(x)]$ не может быть выше $n\cdot\nu$. Докажем, что она не может быть меньше $n\cdot\nu$. Пусть

$$\Phi(x)=\frac{F(x)}{H(x)},\qquad \varphi(x)=\frac{f(x)}{h(x)},$$

где $F(x)$, $H(x)$ и $f(x)$, $h(x)$ — взаимно простые пары полиномов. Если

$$F(x)=A_0x^n+A_1x^{n-1}+\ldots,\quad H(x)=B_0x^n+B_1x^{n-1}+\ldots,$$
$$f(x)=a_0x^\nu+a_1x^{\nu-1}+\ldots,\quad h(x)=b_0x^\nu+b_1x^{\nu-1}+\ldots,$$

то из каждой пары чисел $A_0$, $B_0$ и $a_0$, $b_0$ хотя бы по одному числу должно быть отлично от нуля. Тогда

$$(1)\qquad \Phi[\varphi(x)]=\frac{h(x)^n\cdot F\left(\frac{f(x)}{h(x)}\right)}{h(x)^n\cdot H\left(\frac{f(x)}{h(x)}\right)}=\frac{A_0f^n+A_1f^{n-1}h+\ldots+A_nh^n}{B_0f^n+B_1f^{n-1}h+\ldots+B_nh^n},$$

где под $f$, $h$ мы разумеем $f(x)$, $h(x)$. В числителе и знаменателе выражения (1) получаются полиномы степени $n\cdot\nu$, причём при старшей степени стоят коэффициенты

$$C_0=A_0a_0^n+A_1a_0^{n-1}b_0+\ldots+A_nb_0^n=b_0^nF\left(\frac{a_0}{b_0}\right),$$

$$D_0=B_0a_0^n+B_1a_0^{n-1}b_0+\ldots+B_nb_0^n=b_0^nH\left(\frac{a_0}{b_0}\right),$$

если $b_0\neq 0$, и

$$C_0=A_0a_0^n,\quad D_0=B_0a_0^n,$$

если $b_0=0$, и тогда непременно $a_0\neq 0$.

Докажем, что из чисел $C_0$, $D_0$ по крайней мере одно отлично от нуля. При $b_0 = 0$ это очевидно. При $b_0 \neq 0$, в силу взаимной простоты $F(x)$ и $H(x)$, можно найти такие полиномы $U(x)$, $V(x)$ степеней не выше $n-1$, что

$$F(x) \cdot U(x) + H(x) \cdot V(x) = 1; \tag{2}$$

подставляя $x = \frac{a_0}{b_0}$ и умножая на $b_0^{2n-1}$, получим

$$b_0^n F\left(\frac{a_0}{b_0}\right) \cdot b_0^{n-1} U\left(\frac{a_0}{b_0}\right) + b_0^n H\left(\frac{a_0}{b_0}\right) \cdot b_0^{n-1} V\left(\frac{a_0}{b_0}\right) = b_0^{2n-1},$$

или

$$C_0 \cdot b_0^{n-1} U\left(\frac{a_0}{b_0}\right) + D_0 \cdot b_0^{n-1} V\left(\frac{a_0}{b_0}\right) = b_0^{2n-1} \neq 0,$$

откуда видно, что $C_0$ и $D_0$ одновременно не могут быть равны нулю.

Чтобы доказать, что степень функции $\Phi[\varphi(x)]$ равна $n\nu$, остаётся только убедиться во взаимной простоте полиномов, стоящих в числителе и знаменателе выражения (1). Из (2) мы получим

$$F\left(\frac{f(x)}{h(x)}\right) \cdot U\left(\frac{f(x)}{h(x)}\right) + H\left(\frac{f(x)}{h(x)}\right) \cdot V\left(\frac{f(x)}{h(x)}\right) = 1,$$

откуда, умножая на $h^{2n-1}$, будем иметь:

$$(A_0 f^n + A_1 f^{n-1} h + \ldots + A_n h^n) \cdot h^{n-1} U\left(\frac{f}{h}\right) +$$
$$+ (B_0 f^n + B_1 f^{n-1} h + \ldots + B_n h^n) \cdot h^{n-1} V\left(\frac{f}{h}\right) = h^{2n-1};$$

поскольку $h^{n-1} U\left(\frac{f}{h}\right)$ и $h^{n-1} V\left(\frac{f}{h}\right)$ — полиномы от $x$, отсюда следует, что общий наибольший делитель числителя и знаменателя выражения (1) является делителем полинома $h^{2n-1}$. Если бы числитель, знаменатель выражения (1) и полином $h(x)$ имели общий делитель $d(x)$, то из выражений

$$A_0 f^n + A_1 f^{n-1} h + \ldots + A_n h^n, \quad B_0 f^n + B_1 f^{n-1} h + \ldots + B_n h^n \tag{3}$$

первых двух полиномов и того, чтобы один из коэффициентов $A_0$, $B_0$ был непременно отличен от нуля, следовало бы, что и $f^n$ делится на $d(x)$. Но так как $f^n$ и $h$ взаимно просты, то $d(x) = 1$. С другой стороны, если полиномы (3) и $h$ не имеют общего делителя, то и полиномы (3) не имеют с $h^{2n-1}$ общего делителя, а это показывает, что оба полинома (3) взаимно просты, ч. т. д.

Следствие 1. *Поле $k[\varphi(x)]$ совпадает с $k(x)$ только тогда, когда $\varphi(x)$ есть дробная линейная функция:*

$$\varphi(x) = \frac{ax+b}{cx+d}. \tag{4}$$

Доказательство. Из теоремы 11 следует, что если степень элемента $\varphi(x)$ есть $\nu$, то степени всех элементов поля $k[\varphi(x)]$ кратны $\nu$. Но так как степени элементов поля $k(x)$ имеют всевозможные целые положительные значения, то для совпадения обоих полей необходимо, чтобы имело место $\nu = 1$, а это возможно только в том случае, когда $\varphi(x)$ имеет форму (4).

Если $k[\varphi(x)] = k(x)$, то, сопоставляя в поле $k(x)$ каждому элементу $\Phi(x)$ элемент $\Phi[\varphi(x)]$, мы придём к изоморфизму поля $k(x)$ с самим собой, или, как это принято называть, к *автоморфизму* поля $k(x)$. Таким образом следствие 1 может быть ещё формулировано так:

Поле $k(x)$ имеет $\infty^3$ автоморфизмов, получаемых сопоставлением с $x$ каждого из элементов $\frac{ax+b}{cx+d}$, где хоть один из коэффициентов $a$, $c$ отличен от нуля.

Мы сказали: $\infty^3$, а не $\infty^4$, хотя в выражение $\frac{ax+b}{cx+d}$ входят четыре константы. Мы сделали это потому, что от одной из констант (если она не равна нулю) мы можем всегда избавиться, деля на неё числитель и знаменатель выражения $\frac{ax+b}{cx+d}$.

Применяя этот результат к произвольным подполям $k[\varphi(x)]$ поля $k(x)$, мы придём к следующему заключению:

Следствие 2. *Два подполя $k[\varphi(x)]$ и $k[\psi(x)]$ поля $k(x)$ совпадают тогда и только тогда, когда*

$$\psi(x) = \frac{a\varphi(x)+b}{c\varphi(x)+d}. \tag{5}$$

Таким образом все подполя

$$k[\varphi(x)], \quad k[\psi(x)],$$

у которых производящие функции не связаны соотношением типа (5), различны.

Теорема 12 (Люрота). *Всякое подполе $\overline{K}$ поля $K = k(x)$, содержащее поле $k$, содержит элемент $y$ такого рода, что $\overline{K} = k(y)$.*

Доказательство. Выберем в поле $\overline{K}$ элемент

$$y = \frac{g(x)}{h(x)},$$

степень которого, $m$, была бы возможно мала. Уравнение степени $m$

$$g(t) - y\,h(t) = 0,$$

корнем которого является $x$, имеет коэффициенты из поля $k(y) \subset \overline{K}$. Пусть

$$F(t) = 0$$

есть неприводимое в поле $\overline{K}$ уравнение, которому удовлетворяет $x$, и пусть его степень относительно $t$ есть $M$. Очевидно, что $M \leqslant m$. Коэффициенты при различных степенях $t$ в полиноме $F(t)$ суть элементы поля $\overline{K}$, а потому их степени относительно $x$ не могут быть меньше $m$. Умножив полином $F(t)$ на общий знаменатель его коэффициентов, мы получим полином $F(t; x)$, степень которого относительно $x$ не может быть меньше $m$. Коэффициенты этого полинома при различных степенях $t$ суть полиномы от $x$, не имеющие общего делителя. В силу неприводимости этого полинома в поле $\overline{K}$ полином

$$g(t) - yh(t) = g(t) - \frac{g(x)}{h(x)} \cdot h(t)$$

делится на $F(t)$ по переменной $t$, а потому полином

$$h(x)\{g(t) - yh(t)\} = h(x) \cdot g(t) - g(x)h(t)$$

делится на $F(t; x)$ по обеим переменным $t$, $x$:

$$h(x)g(t) - g(x) \cdot h(t) = F(x; t) \cdot Q(t; x),$$

где $Q(t; x)$ — полином от $t$ и $x$ (это следует из леммы Гаусса о произведении примитивных полиномов, распространённой на кольцо полиномов от $x$). Но степень левой части относительно $x$ есть $m$, а $F(t; x)$ имеет относительно $x$ степень $\geqslant m$. Отсюда следует, что $Q(t; x)$ не может содержать переменной $x$:

$$Q(t; x) = Q(t).$$

Однако мы предположили, что $g(t)$ и $h(t)$ взаимно просты. Если бы $Q(t)$ содержал $t$, то мы могли бы разделить $g(t)$ и $h(t)$ на $Q(t)$ с остатками:

$$g(t) = Q(t)u(t) + g_1(t), \quad h(t) = Q(t)v(t) + h_1(t);$$

отсюда следовало бы:

$$g(t) - yh(t) = Q(t)\{u(t) - yv(t)\} + \{g_1(t) - yh_1(t)\}.$$

Из этого равенства вытекало бы, что $g_1(t) - yh_1(t)$, имея меньшую, чем $Q(t)$, степень, делится на $Q(t)$. Это возможно только при

$$g_1(t) = h_1(t) = 0,$$

т. е. если $g(t)$ и $h(t)$ делятся на $Q(t)$. Таким образом $Q(t) = 1$, откуда следует, что полином

$$g(t) - yh(t)$$

неприводим в поле $\overline{K}$.

Пусть теперь в поле $\overline{K}$ содержится элемент

$$z = \frac{u(x)}{v(x)}.$$

Полином

$$u(t) - zv(t)$$

должен делиться на $g(t) - yh(t)$ в силу неприводимости последнего полинома. При проведении алгоритма деления в остатке получится полином от $t$ степени $m-1$, все коэффициенты которого обращаются в нуль. Но эти коэффициенты содержат $z$ линейно. Приравнивая их нулю, мы получим рациональные выражения $z$ через $y$ (которые все должны совпадать). Таким образом все элементы поля $\bar{K}$ рационально выражаются через $y$, т. е.

$$\bar{K} = k(y),$$

что требовалось доказать.

Это доказательство не обладает эффективностью: оно не даёт средства найти в $\bar{K}$ элемент $y$ возможно меньшей степени. Попытаемся модифицировать это доказательство так, чтобы сделать его эффективным. Но для этого нам надо эффективно задать поле $\bar{K}$. Обычно оно задаётся как поле рациональных функций от *нескольких* элементов поля $k(x)$

$$y_i = \frac{g_i(x)}{h_i(x)} \qquad (i = 1, 2, \ldots, n), \tag{6}$$

между которыми, очевидно, имеют место $n-1$ независимых алгебраических соотношений. Пусть среди элементов (6) наименьшую степень имеет элемент

$$y_\nu = \frac{g_\nu(x)}{h_\nu(x)}.$$

Если не все полиномы

$$g_i(t) - y_i h_i(t)$$

делятся на

$$g_\nu(t) - y_\nu h_\nu(t),$$

то их общий наибольший делитель имеет относительно $t$ более низкую степень. Умножая его на общий знаменатель коэффициентов при степенях $t$, мы получим полином $F(x; t)$, на который делятся все полиномы

$$g_i(x) \cdot h_i(t) - h_i(x) g_i(t) \qquad (i = 1, 2, \ldots, n), \tag{7}$$

притом относительно обеих переменных $t$, $x$:

$$g_i(x) h_i(t) - h_i(x) g_i(t) = Q_i(x; t) \cdot F(x; t) \qquad (i = 1, 2, \ldots, n).$$

Поскольку, как мы уже убедились, полиномы (7) не имеют не зависящих от $t$ множителей, полином $F(x; t)$ имеет более низкую, чем $m$, степень относительно $x$. Деля его на коэффициент при старшей степени $t$, мы получим полином относительно $t$, у которого коэффи-

циенты как функции от $x$ имеют степени $< m$. Вместе с тем, будучи получены из полиномов $g_i(t) - y_i h_i(t)$ алгоритмом Эвклида, эти коэффициенты рационально зависят от $y_i$. Пусть один из них есть

$$v_{n+1} = \frac{g_{n+1}(x)}{h_{n+1}(x)}.$$

Присоединяя его к системе (6) и повторяя процесс при меньшем значении числа $m$, мы или выразим все элементы $y_1, y_2, \ldots, y_n$ через $y_{n+1}$, или опять уменьшим значение $m$. После конечного числа шагов мы найдём функцию, через которую рационально выразятся все элементы (6).

*Пример.* Пусть поле $\overline{K}$ образовано элементами

$$y = x^3 + \frac{1}{x^3}, \qquad z = x^2 + \frac{1}{x^2}.$$

Здесь $m = 4$. Деля друг на друга полиномы

$$t^6 - yt^3 + 1, \quad t^4 - yt^2 + 1, \tag{8}$$

получим в остатке полином

$$t^3 - ut^2 + v,$$

где

$$u = \frac{z^2 - 1}{y} = \frac{x^4 + x^2 + 1}{x(x^2 + 1)}, \qquad v = \frac{z - 1}{y} = \frac{x}{x^2 + 1}.$$

Степень элемента $v$ равна 2, т. е. $< m$. Поэтому мы должны составить для $v$ соответствующий полином. Это удобнее сделать для элемента

$$w = \frac{1}{v} = \frac{x^2 + 1}{x}.$$

Получим полином

$$t^2 - wt + 1.$$

Разделим на него полиномы (8). При делении первого получится остаток

$$(w^2 - 1)(w^3 - 3w - y)t - w(w^3 - 3w - y),$$

который при подстановке вместо $w$, $y$ их выражений через $x$ обращается в нуль. Именно,

$$w^3 - 3w - y = 0.$$

Таким образом $y$ рационально выражается через $w$:

$$y = w^3 - 3w.$$

Аналогично поступим со вторым полиномом (8). Здесь остаток равен

$$w(w^2 - 2 - z)t - (w^2 - 2 - z),$$

После подстановки вместо $w$, $z$ их выражений через $x$ множитель $w^2 - 2 - z$ обратится в нуль, откуда

$$z = w^2 - 2.$$

Отсюда мы заключаем, что поле $\overline{K}$ может быть образовано присоединением к $k$ элемента

$$w = \frac{x^2+1}{x} = \frac{y}{z^2-1}.$$

Штейниц (Steinitz) [99] сделал предположение о справедливости теоремы Люрота для полей рациональных функций от любого числа независимых переменных. Для двух переменных его предположение оправдывается результатом Кастельнуово (Castelnuovo) [27], но для случая трёх переменных оно было опровергнуто Энриквесом (Enriques) [35]. См. также Фано (G. Fano) [37].

Интересно выяснить, в каких случаях в качестве «элемента Люрота» (т. е. элемента, могущего образовать точно поле $\overline{K}$) можно взять полином от $x$. Оказывается, что это возможно во всех случаях, когда $\overline{K}$ вообще содержит полиномы от $x$. Для доказательства введём новое понятие *порядка* элемента

$$y = \frac{g(x)}{h(x)}$$

поля $k(x)$. Именно, под порядком элемента $y$ мы будем разуметь разность между степенями полиномов $g(x)$ и $h(x)$. Здесь несущественно, сократима ли дробь $\frac{g(x)}{h(x)}$. Очевидно, что между степенью $m$ и порядком $\mu$ одного и того же элемента имеет место неравенство

$$\mu \leqslant m,$$

причём знак равенства имеет место в том и только в том случае, если этот элемент есть полином от $x$. Для порядка имеет место теорема, аналогичная теореме 11 для степени:

Теорема 13. *Если порядок функции* $\Phi(x)$ *равен* $r$, *а порядок функции* $\varphi(x)$ *равен* $\rho > 0$, *то порядок функции* $\Phi[\varphi(x)]$ *равен* $r \cdot \rho$.

Доказательство. Очевидно, что порядок произведения равен сумме порядков сомножителей. Представим $\Phi[\varphi(x)]$ в виде

$$\Phi[\varphi(x)] = [\varphi(x)]^r \cdot \Phi_0[\varphi(x)],$$

где $\Phi_0(x)$ — функция нулевого порядка. Порядок первого множителя, очевидно, равен $r \cdot \rho$. С другой стороны, функция $\Phi_0(x)$ может быть представлена как частное двух полиномов одинаковой ($m$-й) степени:

$$\Phi_0(x) = \frac{F(x)}{H(x)}.$$

Степень полиномов

$$[h(x)]^m \cdot F[\varphi(x)], \quad [h(x)]^m \cdot H[\varphi(x)],$$

где

$$\varphi(x) = \frac{f(x)}{h(x)},$$

точно равна $m\rho$, так как их старшие члены в силу $\rho > 0$ ни с чем не могут быть сокращены. Отсюда следует, что порядок функции

$$\Phi_0[\varphi(x)] = \frac{[h(x)]^m \cdot F[\varphi(x)]}{[h(x)]^m \cdot H[\varphi(x)]}$$

равен нулю, что и доказывает теорему.

**Теорема 14.** (Э. Нётер, E. Noether). *Если поле $\overline{K}$ содержит полиномы от $x$, то в качестве его элемента Люрота тоже можно взять полином от $x$.*

Доказательство. Пусть $\psi(x)$ — какой-нибудь элемент Люрота поля $\overline{K}$. Если его порядок положителен, положим $\varphi(x) = \psi(x)$; если он отрицателен, положим $\varphi(x) = \frac{1}{\psi(x)}$; наконец, если он равен нулю, подберём константу $a$ так, чтобы порядок $\psi(x) - a$ был отрицателен, и тогда положим

$$\varphi(x) = \frac{1}{\psi(x) - a}.$$

Во всех трёх случаях $\varphi(x)$ будет элементом Люрота положительного порядка: $\rho > 0$. Пусть степень элемента $\varphi(x)$ есть $m$.

Согласно условию, поле $\overline{K}$ содержит полином $P(x)$, степень (и порядок) которого пусть будет $p$. Имеет место равенство

$$P(x) = \Phi[\varphi(x)],$$

где $\Phi(x)$ — функция, степень которой пусть будет $\nu$, а порядок — $n$. Здесь

$$\nu \geqslant n, \quad m \geqslant \rho. \tag{9}$$

Из теоремы 11 мы заключаем:

$$p = \nu \cdot m,$$

а из теоремы 13:

$$p = n \cdot \rho.$$

Равенство $\nu m = n\rho$, соединённое с неравенствами (9), даёт:

$$\nu = n, \quad m = \rho.$$

Из второго равенства мы заключаем, что $\varphi(x)$ есть полином от $x$, ч. т. д.

## Упражнения к главе I

Доказать:

1. Число элементов во всяком конечном поле (порядок поля) равно $p^n$, где $p$ — простое число.

2. Чтобы элемент $\alpha$ конечного поля был корнем неприводимого в рациональном поле уравнения $k$-й степени, необходимо и достаточно, чтобы $k$ было наименьшим числом, при котором имеет место $\alpha^{p^k} - \alpha = 0$.

3. Все конечные поля, имеющие одинаковый порядок $p^n$, изоморфны.

4. Сравнение

$$x^{p^n} - x \equiv 0 \pmod{p}$$

имеет неприводимые множители степеней, являющихся делителями числа $n$. Определить число этих множителей для каждой степени.

5. Если полиномы $A_1, A_2, \ldots, A_m$ взаимно просты, т. е. не имеют общего делителя, то неопределённое уравнение

$$A_1X_1 + A_2X_2 + \ldots + A_mX_m = B,$$

где $B$ — произвольный полином, может быть решено в полиномах.

6. Если элемент

$$y = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}$$

не есть примитивный элемент поля $k(\alpha)$, то уравнение $n$-й степени, которому он удовлетворяет (см. теорему 2), имеет кратные корни. Более того его левая часть есть степень неприводимого полинома.

7. Если $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ — корни неприводимого уравнения $f(x) = 0$, то для поля $k(\alpha)$

$$S(\alpha) = \alpha_1 + \alpha_2 + \ldots + \alpha_n, \quad N(\alpha) = \alpha_1 \cdot \alpha_2 \ldots \alpha_n.$$

8. Пусть $K_1$ есть алгебраическое расширение поля $k$, а $K_2$ — алгебраическое расширение поля $K_1$, причём степень $K_2 : K_1$ есть $n$. Пусть $S_1(\ldots)$ $N_1(\ldots)$ обозначают след и норму для поля $K_1$, а $S_2(\ldots)$, $N_2(\ldots)$ — для поля $K_2$. Тогда, если $\alpha \subset K_1$, то

$$S_2(\alpha) = n \cdot S_1(\alpha), \quad N_2(\alpha) = [N_1(\alpha)]^n.$$

9. Найти элемент Люрота для поля, образованного полиномами

$$x^6 + 3x^5 + 7x^4 + 9x^3 + 9x^2 + 5x + 1,$$
$$x^4 + 2x^3 + 4x^2 + 3x + 1.$$

10. Будем называть полином $f$ импримитивным, если между $k(x)$ и $k(f)$ имеется промежуточное поле. Найти условие, которому подчиняются коэффициенты импримитивного полинома 4-й степени

$$A_0x^4 + A_1x^3 + A_2x^2 + A_3x + A_4.$$

ГЛАВА II

# ПОЛЕ АЛГЕБРАИЧЕСКИХ ФУНКЦИЙ

## § 8. Определение поля алгебраических функций

Полем алгебраических функций над числовым полем $k$ называется конечное алгебраическое расширение простого трансцендентного расширения поля $k$. Если это трансцендентное расширение образовано путём присоединения к $k$ $m$ элементов, не связанных алгебраическими зависимостями, то говорят, что получаемое поле алгебраических функций содержит $m$ независимых переменных. В настоящей книге мы ограничимся случаем $m = 1$. Соответствующее этому случаю поле алгебраических функций одной независимой переменной мы, не боясь недоразумений, будем называть просто полем алгебраических функций.

Пусть трансцендентное расширение есть $k(x)$. Если поле $k(x)$ совершенно, то из теоремы 9 следует, что поле алгебраических функций есть простое расширение поля $k(x)$, т. е. может быть образовано присоединением к $k(x)$ одного элемента $y$, связанного с $x$ соотношением

$$f(x, y) = 0, \tag{1}$$

где $f(x, y)$ — полином от двух переменных с коэффициентами из поля $k$.

Элементы $x$, $y$ поля $k(x, y)$ не являются единственной парой, при помощи которой можно определить это поле: мы увидим, что существует бесконечное множество пар, определяющих поле $k(x, y)$. Не нарушая общности, можно считать уравнение (1) неприводимым. Применим к алгебраическому расширению $k(x, y) : k(x)$ поля $k(x)$ результаты § 4.

Пусть уравнение (1) имеет степень $n$ относительно элемента $y$. Применяя теорему 2, мы убедимся, что любой элемент $z$ поля $k(x, y)$ связан с элементом $x$ уравнением степени $n$ относительно $z$ и что в случае, когда это уравнение неприводимо, $z$ есть примитивный элемент расширения $k(x, y) : k(x)$, т. е. пара $x$, $z$ образует всё поле $k(x, y)$. Будем называть такого рода пару *примитивной парой*. Рассматривая $k(x, z)$ как расширение поля $k(z)$, мы при помощи теоремы 2 можем заменить в примитивной паре $x$ другим элемен-

том, $u$. Переход от пары $x, y$ к паре $u, z$ осуществляется при помощи обратимого рационально преобразования

$$u = g(x, y), \quad z = h(x, y),$$

а также

$$x = \varphi(u, z), \quad y = \psi(u, z),$$

где $g$, $h$, $\varphi$, $\psi$ — рациональные функции. Такого рода преобразование носит название *бирационального*.

Имеет место

Теорема 15. *Если $k$ — совершенное поле, то к любому элементу поля $k(x, y)$, трансцендентному над $k$, можно подобрать другой элемент, составляющий с ним примитивную пару.*

Доказательство. Пусть $z$ — произвольный элемент поля $k(x, y)$, не входящий в $k$, но такой, что $k(z)$ есть трансцендентное расширение поля $k$ (или, как мы для простоты будем говорить, непостоянный). Докажем прежде всего, что $k(x, y) : k(z)$ есть конечное алгебраическое расширение. Элементы $x$ и $z$ в силу теоремы 2 связаны алгебраическим соотношением, которое должно содержать $x$, так как в противном случае мы имели бы $f(z) = 0$, откуда заключили бы, что $z$ есть постоянный элемент (т. е. $k(z)$ есть алгебраическое расширение поля $k$). Отсюда следует, что $k(x, z) : k(z)$ есть конечное алгебраическое расширение. С другой стороны, согласно определению, $k(x, y) : k(x)$, а в силу $k(x) \subset k(x, z)$ и $k(x, y) : k(x, z)$ есть конечное алгебраическое расширение. Но тогда в силу теоремы 5 и $k(x, y) : k(z)$ есть конечное алгебраическое расширение.

Если $k$ есть поле характеристики нуль, то $k(z)$ есть тоже совершенное поле, а потому $k(x, y) : k(z)$ в силу теоремы 9 есть простое расширение. Это значит, что в $k(x, y)$ содержится такой элемент $u$, что $k(z, u) = k(x, y)$, т. е. что $z$, $u$ является примитивной парой для $k(x, y)$.

Пусть теперь $k$ — совершенное поле характеристики $p$. В силу теоремы 8 имеет место

$$k^p = k,$$

а потому всякий элемент поля $k$ можно представить в виде $p$-й степени элемента из $k$. Поэтому неприводимое уравнение не может содержать только $p$-е степени переменных: в самом деле,

$$f(u^p, v^p) = \sum_{\mu,\nu} a_{\mu\nu} u^{p\mu} v^{p\nu} = \sum_{\mu,\nu} b_{\mu\nu}^p u^{p\mu} v^{p\nu} = \Big(\sum_{\mu,\nu} b_{\mu\nu} u^\mu v^\nu\Big)^p.$$

Если $k(x, y) : k(z)$ есть расширение 1-го рода, то теорема доказана. В противном случае существует элемент $\xi \subset k$, связанный с $z$ неприводимым уравнением вида

$$\varphi(\xi^p, z) = 0. \tag{2}$$

Подстановка $z = z_1^p$ приводит к уравнению

$$\varphi(\xi^p, z_1^p) = [\varphi_1(\xi, z_1)]^p = 0.$$

Поскольку подстановка $z = z_1^p$ приводит уравнение $\varphi(\xi, z_1) = 0$ к неприводимому уравнению (2) той же степени относительно $z_1$ или $z$, $z$ есть примитивный элемент поля $k(z_1, \xi)$, откуда

$$k(z_1, \xi) = k(z, \xi),$$

т. е.

$$z_1 \subset k(z, \xi) \subset k(x, y).$$

Заменяя $z$ через $z_1$ и продолжая процесс, мы после конечного числа операций или придём к элементу $\zeta$ такого рода, что

$$\zeta^{p^s} = z, \quad \zeta \subset k(x, y), \quad \zeta^{\frac{1}{p}} \not\subset k(x, y),$$

или установим возможность решения внутри поля $k$ уравнения $\zeta^{p^s} = z$ при сколь угодно большом $s$.

В первом случае $k(x, y) : k(\zeta)$ есть расширение 1-го рода, а потому к нему применима теорема 9, так что существует такой элемент $u \subset k(x, y)$, что $k(\zeta, u) = k(x, y)$. Неприводимое уравнение $F(\zeta, u) = 0$ непременно содержит степени $u$, $\zeta$, не кратные $p$. Возвышая его в $p$-ю степень и заменяя $\zeta^p$ через $\zeta_1$, мы получим:

$$F_1(\zeta_1, u^p) = 0.$$

Это уравнение имеет ту же степень относительно $\zeta_1$, что и $F(\zeta, u) = 0$ относительно $\zeta$. Докажем, что оно неприводимо. Поскольку после подстановки $\zeta_1 = \zeta^p$ его левая часть превращается в $p$-ю степень неприводимого полинома $F(\zeta, u)$, её неприводимый множитель после этой подстановки должен превратиться в $s$-ю степень полинома $F(\zeta, u)$, где $1 \leqslant s \leqslant p$. Все неприводимые множители полинома $F_1(\zeta, u^p)$, таким образом, не взаимно просты и потому совпадают, откуда следует, что $s$ есть делитель $p$, т. е. $s = 1$ или $s = p$. В первом случае $F_1(\zeta_1, u^p)$ должен быть $p$-й степенью полинома, что невозможно, поскольку он содержит степени $\zeta_1$, не кратные $p$. Во втором случае сам полином $F_1(\zeta, u^p)$ неприводим. Из этого в силу теоремы 2 следует, что

$$k(\zeta_1, u) = k(\zeta, u) = k(x, y).$$

Продолжая рассуждение для $\zeta_2 = \zeta_1^p$, $\zeta_3 = \zeta_2^p, \ldots$, мы в конце концов убедимся, что

$$k(z, u) = k(x, y),$$

т. е. что $z$, $u$ образуют примитивную пару.

Во втором случае уравнение $\zeta^{p^s} = z$ при сколь угодно большом $s$ имеет корень в поле $k(x, y)$. Но полином $\zeta^{p^s} - z$ неприводим, так

как его множители должны быть полиномами $u$ относительно $z$; $u$ остаётся неприводимым в поле $k(z)$, поскольку $z$ не удовлетворяет никаким алгебраическим уравнениям в поле $k$. Это противоречит теореме 2, поскольку $k(x,y):k(z)$ есть конечное алгебраическое расширение. Таким образом второй случай невозможен, и теорема доказана.

Если $k$ — несовершенное поле характеристики $p$, то теорема 15 не имеет места. В самом деле, пусть элементы $x$, $y$ поля $k(x,y)$ связаны неприводимым уравнением $f(x^p, y^p) = 0$. Тогда всякий элемент $z$ поля $k(x,y)$ такого рода, что $k(x,z) = k(x,y)$, связан с $x$ неприводимым уравнением типа $g(x^p, y^p) = 0$. В самом деле, если $z = \varphi(x,y)$, то $z^p = \varphi_1(x^p, y^p)$. Исключая, как в теореме 2, из $f(x^p, y^p) = 0$ элемент $y^p$, мы придём к уравнению той же степени относительно $z^p$. Если $k(x,z) = k(x,y)$, то это уравнение неприводимо.

Докажем, что $x^p$ является таким элементом, к которому нельзя подобрать примитивной пары. Допустим, что $k(x^p, u) = k(x,y)$. Тогда a fortiori $k(x,u) = k(x,y)$. В силу доказанного неприводимое уравнение, связывающее $x$, $u$, имеет вид $g(x^p, u^p) = 0$. Расширение $k(x_1, u):k(u)$, где $x_1 = x^p$, имеет меньшую степень, чем $k(x,u):k(u)$, так как $x_1$ удовлетворяет в поле $k(u)$ уравнению $g(x_1, u^p) = 0$, более низкой степени относительно $x_1$, чем

$$g(x^p, u^p) = 0$$

относительно $x$. Поэтому $k(x_1, u) \neq k(x,u)$, ч. т. д.

Теория алгебраических функций имеет целью изучить природу полей алгебраических функций независимо от того, при помощи каких примитивных пар они определены. Другими словами, теория алгебраических функций занимается нахождением *инвариантов* бирациональных преобразований, т. е. величин, остающихся неизменными при бирациональных преобразованиях. Можно формулировать как основную задачу теории алгебраических функций задачу о нахождении полной системы инвариантов, значения которых совпадают только для тождественных (изоморфных) полей. Мы ещё весьма далеки от решения этой задачи, и нам придётся вводить в рассмотрение вспомогательные объекты, не обладающие свойством инвариантности.

Такое определение теории алгебраических функций даёт право рассматривать её как геометрию бирациональных преобразований в смысле, формулированном Клейном (F. Klein), который определяет всякую геометрию как науку об инвариантах заданной совокупности (группы) преобразований. Заметим, что бирациональные преобразования не составляют группы (см. ниже, § 28), поскольку мы не можем определить понятие «произведения» двух бирациональных преобразований. Это не мешает, однако, определить понятие «инварианта»

для совокупности бирациональных преобразований (см. Введение, третий абзац).

В то же время мы встречаемся с термином алгебраическая геометрия, присвоенным теории алгебраических функций, изучаемой геометрическими методами. Здесь слово «геометрия» употреблено не совсем в том же смысле.

Алгебраическая геометрия исторически возникла из высшей аналитической геометрии и широко пользуется как обычными геометрическими понятиями точки, прямой, касательной и т. п., так и понятиями, введёнными в аналитической геометрии: пучка, связки и т. п. В алгебраической геометрии весьма часто рассматриваются *проективные преобразования*, более частные, чем бирациональные, и их инварианты, весьма полезные для чисто геометрических вопросов, но не имеющие прямого отношения к основным задачам теории алгебраических функций.

## § 9. Кольца и дивизоры в поле рациональных функций

*Кольцом* называется такая совокупность $A$ элементов поля, что из $a \subset A$, $b \subset A$ следует

$$a \pm b \subset A, \quad ab \subset A.$$

Другими словами, элементы кольца воспроизводятся при первых трёх арифметических действиях (поле определяется как совокупность, элементы которой воспроизводятся при всех четырёх арифметических действиях).

В дальнейшем нам окажутся полезными следующие типы колец:

I. Совокупность полиномов от элемента $x$ с коэффициентами из поля $k$, или, как мы будем говорить, совокупность *целых элементов* поля $k(x)$. Это кольцо неинвариантно определяется в поле $k(x)$, поскольку зависит от выбора примитивного элемента $x$. Будем обозначать его через $\Omega$.

II. Совокупность элементов типа

$$y = \frac{g(x)}{h(x)},$$

где $g(x)$ и $h(x)$ — взаимно простые полиномы с коэффициентами из $k$, причём $h(x)$ взаимно прост с некоторым заданным полиномом $f(x)$, определяющим кольцо. Эта совокупность представляет собой кольцо, так как сумма и произведение элементов

$$\frac{g_1(x)}{h_1(x)}, \quad \frac{g_2(x)}{h_2(x)},$$

где $h_1(x)$, $h_2(x)$ взаимно просты с $f(x)$, представляются в виде дробей со знаменателем

$$h_1(x) \cdot h_2(x),$$

который тоже взаимно прост с $f(x)$.

Будем называть это кольцо *полулокальным кольцом*, определённым при помощи полинома $f(x)$, и обозначать его через $\mathfrak{O}_f$.

Кольцо $\mathfrak{O}_f$ может быть определено независимо от выбора примитивного элемента $x$, если мы условимся при переходе от $x$ к элементу $\xi$, где

$$x = \frac{\alpha\xi + \beta}{\gamma\xi + \delta},$$

брать в роли полинома $f(x)$ полином

$$(\gamma\xi + \delta)^n f\left(\frac{\alpha\xi + \beta}{\gamma\xi + \delta}\right),$$

где $n$ — степень полинома $f(x)$. При этом мы должны сделать дополнение к определению локальных колец. Предварительно рассмотрим пример: пусть $f(x) = x$. После преобразования

$$x = \frac{1}{\xi}$$

функция $x$ переходит в

$$\frac{1}{\xi}$$

и её числитель, единица, не определяет никакого локального кольца.

Исследуем, чем можно охарактеризовать элементы поля, в которые переходят элементы кольца $\mathfrak{O}_\infty$ после преобразования $x = \frac{1}{\xi}$. Другими словами, каковы должны быть функции

$$\frac{g(\xi)}{h(\xi)},$$

чтобы после преобразования $\xi = \frac{1}{x}$ они переходили в функции

$$\frac{g_1(x)}{h_1(x)},$$

где $g_1(x)$, $h_1(x)$ — взаимно простые полиномы, причём $h_1(x)$ не делится на $x$? Очевидно, что для этого необходимо и достаточно, чтобы степень $g(\xi)$ не превышала степени $h(\xi)$. Таким образом мы видим, что при дробных линейных преобразованиях линейные множители полинома $f(x)$ могут пропадать, и требование взаимной простоты с ними знаменателя будет переходить в условие, чтобы степень числителя не превышала степени знаменателя. Поэтому определение колец $\mathfrak{O}_f$ будет инвариантным, если мы в качестве множителей полинома $f(x)$ будем также допускать фиктивный множитель; под взаимной простотой с этим множителем знаменателя $h(x)$ мы будем разуметь то, что степень $g(x)$ не превышает степени $h(x)$.

Определению локальных колец можно придать более естественную форму, вводя понятие *точки*. Для простоты будем считать

поле $k$ алгебраически замкнутым. Под точкой мы будем разуметь сопоставление с каждым элементом $\alpha$ поля $k(x)$ «численного значения» $\alpha_0$ (не исключая бесконечно большого), причём это сопоставление удовлетворяет условиям

$$(\alpha \pm \beta)_0 = \alpha_0 \pm \beta_0, \quad (\alpha\beta)_0 = \alpha_0\beta_0,$$

а элементам, входящим в $k$ (постоянным), сопоставляются эти самые элементы.

Каждому полиному $n$-й степени $f(x)$ соответствует $n$ точек $P_1$, $P_2$, ..., $P_k$, в которых он обращается в нуль. Тогда кольцо $\Omega_f$ будет состоять из элементов поля $k(x)$, принимающих в точках $P_1$, $P_2$, ..., $P_n$ конечные значения. Будем считать это определением локального кольца, причём будем также рассматривать случай, когда одна из точек $P_1$, $P_2$, ..., $P_n$ есть $P_x$, т. е. в ней $x$ принимает значение $\infty$ (или, что то же, $\frac{1}{x}$ принимает значение нуль). В этом случае элементы кольца $\Omega_f$ являются рациональными функциями от $x$, у которых степень числителя не превышает степени знаменателя.

Рассмотренные до сих пор кольца обладали тем свойством, что они содержали все элементы поля (константы). Этим свойством, вообще говоря, не обладают особые кольца, называемые *идеалами* и *дивизорами*, к изучению которых мы приступим.

III. Под *идеалом* $U$, определённым в каком-нибудь кольце $\Omega'$, мы будем разуметь совокупность элементов кольца $\Omega'$, обладающую следующими двумя свойствами:

1) Из $\alpha \subset U$, $\beta \subset U$ следует $\alpha + \beta \subset U$, $\alpha - \beta \subset U$.

2) Из $\alpha \subset U$, $\beta \subset \Omega$ следует $\alpha\beta \subset U$.

Нетрудно видеть, что в кольце $\Omega$ полиномов совокупность полиномов, делящихся на какой-нибудь определённый полином, есть идеал. С другой стороны, для кольца $\Omega$ такого рода идеалы составляют самый общий тип идеалов. В самом деле, пусть $U$ — какой-нибудь идеал и пусть $g(x)$ есть входящий в него полином самой меньшей степени. Тогда в силу 2) всякий делящийся на $g(x)$ полином входит в $U$. С другой стороны, если $h(x) \subset U$, то, деля $h(x)$ с остатком на $g(x)$:

$$h(x) = g(x) \cdot q(x) + r(x),$$

мы в силу 1) убедимся, что $r(x) \subset U(x)$. Но так как степень $r(x)$ ниже, чем степень $g(x)$, то в силу нашего условия относительно $g(x)$ полином $r(x)$ есть нуль, так что $h(x)$ делится на $g(x)$. Будем говорить, что идеал $U = U_g$ определяется полиномом $g(x)$.

Если идеалы $U_g$ и $U_h$ определяются полиномами $g(x)$ и $h(x)$, причём $h(x)$ делится на $g(x)$, то всякий элемент $U_h$ входит в $U_g$:

$$U_h \subset U_g.$$

Будем в этом случае говорить, что $U_h$ делится на $U_g$.

Если полином $g(x)$ разлагается на неприводимые множители:

$$g(x) = g_1(x) \cdot g_2(x) \dots g_s(x),$$

то идеал $U_g$ делится на идеалы

$$U_{g_1},\ U_{g_2},\ \dots,\ U_{g_s}.$$

Если мы под *произведением* двух идеалов $U$, $V$ будем разуметь совокупность элементов, представляемых в форме $\sum_\nu \alpha_\nu \cdot \beta_\nu$, где $\alpha_\nu \subset U$, $\beta_\nu \subset V$, то ясно, что

$$U_{g \cdot h} = U_g \cdot U_h,$$

так что для разложения полинома $g$ на неприводимые множители, $g = g_1 \cdot g_2 \dots g_s$, будем иметь:

$$U_g = U_{g_1} \cdot U_{g_2} \dots U_{g_s}. \tag{1}$$

Идеалы $U_{g_\nu}$ обладают следующими свойствами:

1. Нет идеалов, отличных от $\mathfrak{O}$ и $U_{g_\nu}$ и являющихся делителями $U_{g_\nu}$.

В силу этого свойства идеалы $U_{g_\nu}$ называются *лишёнными делителей.*

2. Если

$$\alpha \cdot \beta \subset U_{g_\nu},$$

то или $\alpha \subset U_{g_\nu}$, или $\beta \subset U_{g_\nu}$. Это свойство, которым $U_{g_\nu}$ обладает в силу неприводимости $g_\nu(x)$, даёт им название *простых идеалов.*

Свойства простоты и лишённости делителей, в данном случае совпадающие, в случае общей теории идеалов независимы. Так, в кольце *целочисленных* полиномов идеал $(x)$, т. е. совокупность полиномов вида

$$f(x) = x \cdot \psi(x),$$

где $\psi(x)$ — целочисленный полином, есть простой идеал. В самом деле, принадлежность $f(x)$ к идеалу характеризуется равенством нулю числа $f(0)$. Если

$$f(x) = g(x) \cdot h(x),$$

то

$$f(0) = g(0) \cdot h(0).$$

Но если произведение равно нулю, то один из множителей должен быть равен нулю.

С другой стороны, идеал $(x)$ делится на идеал $(2, x)$, т. е. на совокупность целочисленных полиномов с чётным свободным членом, и потому не лишён делителей.

Равенство (1) может быть высказано так:

В кольце полиномов всякий идеал разлагается в произведение простых идеалов, и притом однозначно.

IV. Если мы расширим кольцо $\Omega$ до $\Omega_f$, то, умножая элементы идеала $U_f$, определённого при помощи полинома $f(x)$, на всевозможные элементы кольца $\Omega_f$, мы расширим его до идеала (который мы попрежнему будем обозначать через $U_f$), определённого в кольце $\Omega_f$. Элементы этого идеала характеризуются тем, что при представлении в виде несократимой дроби их числители делятся на $f(x)$. Теперь определение идеала $U_f$ инвариантно относительно выбора кольца поскольку кольцо $\Omega_f$ определяется заданием того же полинома $f(x)$, что и $U_f$. Будем называть определённый таким образом идеал *дивизором*.

Можно определять дивизор также при помощи точек, в которых полином $f(x)$ обращается в нуль: дивизор $U_f$ есть совокупность функций, обращающихся в нуль во всех точках

$$P_1,\ P_2,\ \ldots,\ P_s$$

(учитывая кратность), в которых обращается в нуль $f(x)$. При таком определении легко учесть и тот случай, когда одна из точек

$$P_1,\ P_2,\ \ldots,\ P_s$$

есть точка, обращающая $x$ в бесконечность.

Заслуживает особого внимания случай, когда $f(x)$ есть неприводимый в поле $k$ полином. Если $k$ — алгебраическое замкнутое поле, $f(x)$ есть линейный полином. В этом случае все элементы поля делятся на три категории: 1) элементы $\alpha$ кольца $\Omega_f$, обратные к которым элементы $\frac{1}{\alpha}$ тоже входят в кольцо $\Omega_f$; такие элементы называются *единицами* кольца $\Omega_f$; 2) не-единицы кольца $\Omega_f$; 3) элементы, не входящие в кольцо $\Omega_f$. Тогда кольцо $\Omega_f$ состоит из элементов первых двух категорий. Элементы же второй категории, т. е. не-единицы кольца $\Omega_f$, составляют простой дивизор $U_f$. Они характеризуются тем, что обращаются в нуль в нулевых точках полинома $f(x)$. В случае алгебраически замкнутого поля $k$ они характеризуются одной точкой, в которой они обращаются в нуль.

Можно определять дивизор $U_f$ не только в кольце $\Omega_f$, но также во всяком кольце $\Omega_g$, если $g(x)$ делится на $f(x)$. Более того, дивизор $U_f$ вполне определится, если будут известны его элементы, входящие в кольцо $\Omega$, за исключением того случая, если в числе точек, определяющих $U_f$, содержится бесконечная точка $P_\infty$; в этом последнем случае кольцо $\Omega$ вообще не содержит элементов дивизора $U_f$.

Если дивизоры $U$, $V$ определяются точками $P_1, P_2, \ldots, P_s$ и $P_1', P_2', \ldots, P_{s'}'$, то под произведением $U \cdot V$ мы будем понимать дивизор, определяемый всеми точками

$$P_1,\ P_2,\ldots,\ P_s;\ P_1',\ P_2',\ldots,\ P_{s'}'.$$

При этом, если какие-нибудь из этих точек совпадают, то следует учитывать кратность их вхождения в систему.

Введём понятие дробного дивизора. Будем говорить, что элемент $\alpha$ поля $k(x)$ делится на дивизор $\frac{1}{Q}$, если в его выражении через $x$ в виде несократимой дроби в знаменателе содержится или полином, определяющий дивизор $Q$, или его делитель.

Каждому элементу $\alpha$ поля $k(x)$ можно поставить в соответствие вполне определённый дробный дивизор. В самом деле, если $\alpha$ обращается в нуль в точках

$$P_1, P_2, \ldots, P_s$$

и в бесконечность в точках $Q_1, Q_2, \ldots, Q_{s_1}$, то мы будем сопоставлять ему частное дивизоров $P$ и $Q$, определяемых этими системами точек:

$$\alpha \asymp \frac{P}{Q}.$$

Очевидно, что из

$$\alpha_1 \asymp \frac{P_1}{Q_1}, \quad \alpha_2 \asymp \frac{P_2}{Q_2}$$

следует

$$\alpha_1 \cdot \alpha_2 \asymp \frac{P_1 \cdot P_2}{Q_1 \cdot Q_2}, \quad \alpha_1 : \alpha_2 \asymp \frac{P_1 \cdot Q_2}{Q_1 \cdot P_2}.$$

Отсюда следует, что одному и тому же дробному дивизору соответствует не более одного элемента поля $k(x)$ с точностью до постоянного множителя. В самом деле, из

$$\alpha \asymp \frac{P}{Q}, \quad \beta \asymp \frac{P}{Q}$$

следует

$$\alpha : \beta \asymp 1,$$

а это означает, что элемент $\alpha : \beta$ ни в одной точке не обращается ни в нуль, ни в бесконечность и потому есть константа.

Возникает вопрос: каким дивизорам соответствуют элементы поля, а каким нет? Чтобы ответить на него, представим элемент $\alpha$ в виде несократимой дроби

$$\alpha = \frac{\varphi(x)}{\psi(x)}.$$

Пусть степень числителя есть $m$, а степень знаменателя — $n$. Тогда, если мы расширим поле $k$ настолько, чтобы в нём $\varphi(x)$ и $\psi(x)$ разложились на линейные множители, то окажется, что $\alpha$ обращается в нуль в $m$, а в бесконечность — в $n$ конечных точках. Вместе с тем в $P_\infty$ элемент $\alpha$ обращается в нуль с кратностью $n - m$ (если $n \geqslant m$) или в бесконечность с кратностью $m - n$ (если $m \geqslant n$). Отсюда следует, что $\alpha$ обращается в нуль и в бесконечность одинаковое число раз, или:

1. Дробный дивизор соответствует элементу поля только в том случае, если числа точек, соответствующие его числителю и знаменателю, равны.

Можно формулировать этот результат иначе, не прибегая к расширению поля $k$. Представим себе числитель и знаменатель элемента $\alpha$ разложенными на неприводимые множители. Каждому из них соответствует простой дивизор. Будем называть *весом* простого дивизора степень определяющего его неприводимого полинома и, в частности, весом дивизора $P_\infty$ — число 1. Тогда

1′. Дробный дивизор соответствует элементу поля только в том случае, если его числитель и знаменатель суть произведения простых дивизоров, суммы весов которых равны.

Для полей рациональных функций справедливо и обращение этой теоремы (ниже мы убедимся, что для полей алгебраических функций это уже не имеет места). В самом деле, пусть сумма весов простых делителей дивизора $P$ равна $s = \sigma + \sigma_\infty$, где $\sigma$ — сумма весов его конечных простых делителей, а сумма весов простых делителей дивизора $Q$, которые мы все предположим конечными, тоже равна $s$. Тогда конечная часть дивизора $P$ определяется полиномом $\varphi(x)$ степени $\sigma$, а дивизор $Q$ — полиномом $\psi(x)$ степени $s$. Элементу

$$\alpha = \frac{\varphi(x)}{\psi(x)}$$

будет соответствовать в точности дивизор $\frac{P}{Q}$. Это очевидно относительно его конечных дивизоров; кроме того, $\alpha$ в точке $P_\infty$ обращается в нуль в кратности $s - \sigma = \sigma_\infty$, а числитель дивизора $P$ содержит $P_\infty$ $\sigma_\infty$ раз. Таким образом

$$\alpha \equiv \frac{P}{Q},$$

и мы приходим к теореме:

2. Чтобы дробный дивизор соответствовал элементу поля $k(x)$, необходимо и достаточно, чтобы суммы весов простых делителей его числителя и знаменателя были равны друг другу.

## § 10. Кольца в поле алгебраических функций

Рассмотрим поле $k(x, y)$ алгебраических функций, в котором мы предполагаем элементы $x$, $y$ связанными неприводимым в числовом поле $k$ уравнением

$$(1) \qquad f(x, y) = a_0(x)y^n + a_1(x) \cdot y^{n-1} + \ldots + a_n(x) = 0,$$

где $a_i(x)$ — полиномы. Временно будем считать $x$ особо выделенным элементом (независимой переменной) и таким образом считать $k(x, y)$ алгебраическим расширением поля $k(x)$.

Деля уравнение (1) на $a_0(x)$, мы приведём его к виду

$$y^n + c_{n-1}(x)y^{n-1} + \ldots + c_0(x) = 0. \tag{2}$$

Если при этом коэффициенты $c_i(x)$ лежат в кольце $\mathfrak{Q}'$ поля $k(x)$ (или в кольце $\mathfrak{Q}$ полиномов, или в локальном кольце $\mathfrak{Q}_g$), будем говорить, что $y$ лежит в совокупности $\mathfrak{Q}'$ поля $k(x, y)$. Докажем, что совокупность элементов $y$, $z$, $u$, ..., удовлетворяющих уравнению типа (2), составляет кольцо (мы не ввели для него особого обозначения). В частности, если $c_i(x)$ — полиномы, будем говорить, что $\mathfrak{Q}' = \mathfrak{Q}$ есть совокупность *целых элементов* поля $k(x, y)$. Предварительно докажем

Теорему 16 (Гаусса). *Если $y$ удовлетворяет приводимому уравнению вида* (2), *где $c_i(x)$ принадлежат некоторому кольцу $\mathfrak{Q}'$ поля $k(x)$, и его левая часть разлагается в поле $k(x)$ на множители*

$$y^n + c_{n-1}y^{n-1} + \ldots + c_0 = (y^u + s_{u-1}y^{u-1} + \ldots + s_0)(y^v + t_{v-1}y^{v-1} + \ldots + t_0),$$

*где $u + v = n$, то коэффициенты $s_i$, $t_j$ тоже принадлежат кольцу $\mathfrak{Q}'$ поля $k(x)$.*

Доказательство. Допустим противное: пусть $s_i$, $t_j$ являются дробями и пусть в их знаменатели входит неприводимый полином $h = h(x)$ (в случае $\mathfrak{Q} = \mathfrak{Q}_g$ надо дополнительно потребовать, чтобы $h$ был делителем полинома $g$). Пусть в знаменатели коэффициентов $s_1, s_2, \ldots, s_{u-1}$ $h$ входит самое большее в $\rho$-й степени и пусть $s_\mu$ есть первый из $s_i$, в знаменатели которого $h$ точно входит в $\rho$-й степени. Точно так же пусть $t_\nu$ будет первый из $t_j$, в знаменатель которого $h$ входит в возможно более высокой, $\sigma$-й степени. Тогда коэффициент $c_{\mu+\nu}$ полинома (2) выразится через $s_i$, $t_j$ так:

$$c_{\mu+\nu} = S_\mu \cdot t_\nu + s_{\mu-1} \cdot t_{\nu+1} + \ldots \ldots + s_{\mu+1} \cdot t_{\nu-1} + \ldots$$

В этом выражении первый член $s_\mu t_\nu$ содержит в знаменателе точно $h^{\rho+\sigma}$, а остальные члены — $h$ не выше, чем в $(\rho + \sigma - 1)$-й степени. Отсюда следует, что в знаменателе коэффициента $c_{\mu+\nu}$ содержится точно $h^{\rho+\sigma}$, что не противоречит условию теоремы только в случае $\rho = \sigma = 0$. Но тогда все $s_i$, $t_j$ лежат в $\mathfrak{Q}'$, ч. т. д.

Таким образом, если $y$ удовлетворяет какому-нибудь уравнению с коэффициентами из $\mathfrak{Q}'$, то и неприводимое уравнение, которому удовлетворяет $y$, имеет коэффициенты из $\mathfrak{Q}'$.

Теорема 17. *Если $y$ и $z$ удовлетворяют уравнениям типа* (2) *с коэффициентами из $\mathfrak{Q}'$, то это же имеет место для $y \pm z$ и $y \cdot z$.*

Доказательство. Пусть

$$y^m + a_1 y^{m-1} + \ldots + a_m = 0, \tag{3}$$

$$z^n + b_1 z^{n-1} + \ldots + b_n = 0, \tag{4}$$

где $a_i \subset \Omega'$, $b_j \subset \Omega'$. Обозначая через $u$ один из элементов $y + z$, $y - z$, $yz$, мы сможем выразить каждый из элементов

$$u \cdot y^\mu \cdot z^\nu \qquad (\mu = 0, 1, \ldots, m-1; \quad \nu = 0, 1, \ldots, n-1)$$

в виде линейной функции от

$$\sigma_{\mu\nu} = y^\mu z^\nu \qquad (\mu = 0, 1, \ldots, m-1; \quad \nu = 0, 1, \ldots, n-1)$$

с коэффициентами из $\Omega'$. Для этого в тех случаях, когда по крайней мере один из показателей $\mu$, $\nu$ соответственно равен $m-1$, $n-1$, мы должны освободиться от степеней $y^m$, $z^n$ в выражении $u y^\mu z^\nu$ через $y$ и $z$ при помощи уравнений (3) и (4). Получим

$$u \cdot \sigma_{ik} = \sum_{\mu,\nu} s^{(i,k)}_{\mu,\nu} \cdot \sigma_{\mu\nu},$$

где $s^{(i,k)}_{\mu,\nu} \subset \Omega'$. Исключая $\sigma_{\mu\nu}$, получим уравнение в виде определителя $m \cdot n$-го порядка:

$$\begin{vmatrix} s^{(00)}_{00} - u, & s^{(00)}_{01}, & \ldots, & s^{(00)}_{m-1,\,n-1} \\ s^{(01)}_{00}, & s^{(01)}_{01} - u, & \ldots, & s^{(01)}_{m-1,\,n-1} \\ \ldots & \ldots & \ldots & \ldots \\ s^{(m-1,\,n-1)}_{00}, & s^{(m-1,\,n-1)}_{01}, & \ldots, & s^{(m-1,\,n-1)}_{m-1,\,n-1} - u \end{vmatrix} = 0.$$

Это уравнение степени $mn$ относительно $u$ с коэффициентами из $\Omega'$, причём при $u^{mn}$ стоит коэффициент $(-1)^{mn}$. В силу теоремы 16 неприводимое уравнение, которому удовлетворяет $u$, тоже должно иметь старший коэффициент $\pm 1$, а остальные коэффициенты — из $\Omega'$. В силу определения, $u$ таким образом лежит в совокупности $\Omega'$ поля $k(x, y)$, которая в силу этого составляет кольцо, ч. т. д.

## § 11. Базис и дискриминант кольца

В § 4 мы имели определение базиса расширения $k(x, y) : k(x)$. Теперь дадим определение базиса кольца $\Omega'$. Если все элементы базиса

$$[\omega_1, \omega_2, \ldots, \omega_n]$$

лежат в кольце $\Omega'$, то всякий элемент

$$u = a_1(x) \cdot \omega_1 + a_2(x) \cdot \omega_2 + \ldots + a_n(x) \cdot \omega_n, \tag{1}$$

где $a_i(x) \subset \Omega'$, лежит в кольце $\Omega'$. Обратное не всегда имеет место: бывают случаи, когда элементы кольца $\Omega'$ выражаются в форме (1), где $a_i(x)$ не лежат в кольце $\Omega'$. Покажем, что можно найти базис, для которого такой случай невозможен и который мы и назовём базисом кольца $\Omega'$.

Сначала рассмотрим случай, когда $k(x, y) : k(x)$ есть расширение 1-го рода. Тогда в силу теоремы 10 (§ 6) любой его базис имеет отличный от нуля дискриминант. Возьмём произвольный базис (например, степенной), составленный из элементов кольца $\Omega'$. Его дискриминант $D(x)$ есть элемент кольца $\Omega'$ поля $k(x)$, т. е. полином от $x$, если $\Omega' = \Omega$, и функция от $x$, знаменатель которой взаимно прост с $g(x)$, если $\Omega' = \Omega_g$.

Пусть первоначально выбранный нами базис есть

$$[1, y, y^2, \ldots, y^{n-1}].$$

Возьмём в качестве $\omega_1$ элемент 1. В качестве $\omega_2$ возьмём элемент вида

$$\omega_2 = \frac{b_0(x) + y}{d_2(x)},$$

где $b_0(x)$ и $d_2(x)$ подобраны так, чтобы $\omega_2 \subset \Omega'$, и притом чтобы $d_2(x)$ был возможно более высокой степени. В случае $\Omega' = \Omega_g$ $d_2(x)$ должен, кроме того, состоять лишь из неприводимых множителей полинома $g(x)$.

Это определение может быть оправдано тем, что при $\omega_2 \subset \Omega'$ степень полинома $d_2(x)$ не может быть сколь угодно большой. В самом деле, дискриминанты базисов $[1, \omega_2, \omega_2^2, \ldots, \omega_2^{n-1}]$ и $[1, y, y^2, \ldots, y^{n-1}]$ связаны соотношением

$$\Delta[1, \omega_2, \omega_2^2, \ldots, \omega_2^{n-1}] = \frac{1}{[d_2(x)]^{n(n-1)}} \cdot D(x).$$

Но так как оба дискриминанта лежат в $\Omega'$, то полином $[d_2(x)]^{n(n-1)}$ должен быть делителем полинома $D(x)$.

Лемма 1. *Если*

$$\omega_k = \frac{c_0(x) + c_1(x)\, y + \ldots + y^{k-1}}{D_k(x)} \tag{2}$$

*лежит в $\Omega'$ и притом $D_k(x)$ имеет возможно более высокую степень среди знаменателей элементов вида* (2), *лежащих в $\Omega'$, то у лежащего в $\Omega'$ элемента*

$$\theta_k = \frac{c_0'(x) + c_1'(x)\, y + \ldots + y^{k-1}}{D_k'(x)} \tag{3}$$

*знаменатель $D_k'(x)$ есть делитель полинома $D_k(x)$.*

Доказательство. Допустим противное: пусть $D_k(x)$ и $D'_k(x)$ имеют общим наибольшим делителем $H_k(x)$, так что

$$D_k(x) = H_k(x) \cdot Q_k(x), \quad D'_k(x) = H_k(x) \cdot Q'_k(x),$$

где $Q_k(x)$, $Q'_k(x)$ взаимно просты, причём $Q'_k(x)$ не есть константа. Подберём полиномы $U(x)$ и $V(x)$ так, чтобы

$$Q_k(x)\ U(x) + Q'_k(x)\ V(x) = 1.$$

Элемент

$$V(x)\ \omega_k + U(x)\ 0_k = \frac{[c_0 Q'_k\ V + c'_0 Q_k U] + [c_1 Q'_k\ V + c'_1 Q_k U]\ y + \ldots + y^{k-1}}{H_k(x) \cdot Q_k(x) \cdot Q'_k(x)}$$

лежит в $\Omega'$, имеет форму (2), причем его знаменатель имеет более высокую степень, чем $D_k(x)$, что невозможно.

Следующий элемент, $\omega_3$, мы будем подбирать в форме (2), положив $k = 3$. Из того, что

$$\omega_2^2 = \frac{b_0(x) + 2b_0(x) \cdot y + y^3}{d_2^2(x)}$$

лежит в $\Omega'$ и имеет форму (2), мы в силу леммы 1 заключаем, что $D_3(x)$ делится на $d_2^2(x)$. Пусть

$$D_3(x) = d_2^2(x) \cdot d_3(x).$$

Дискриминант базиса $[1, \omega_2, \omega_3, \omega_2\,\omega_3, \omega_3^2, \ldots]$ связан с дискриминантом базиса $[1, \omega_2, \omega_2^2, \ldots, \omega_2^{n-1}]$ так:

$$\Delta[1, \omega_2, \omega_3, \omega_2\,\omega_3 + \omega_3^2, \ldots] = \frac{1}{[d_3(x)]^{m_3}} \cdot \Delta[1, \omega_2, \omega_2^2, \ldots, \omega_2^{n-1}],$$

где

$$m_3 = (0 + 0 + 1 + 1 + 2 + 2 + \ldots) \cdot 2 = \frac{n(n-2)}{2} \text{ при } n \text{ чётном},$$

$$= \frac{(n-1)^2}{2} \text{ при } n \text{ нечётном}.$$

Возьмём в качестве базиса систему элементов (2) при $k = 1, 2, \ldots, n$. Чтобы доказать, что это будет базис кольца $\Omega'$, предварительно докажем ещё одну лемму.

Лемма 2. *Если мы при нахождении элементов* (2) *будем допускать в качестве* $c_i(x)$ *дробные рациональные функции, то всё-таки не придём ни к каким новым решениям задачи, кроме* (2).

Доказательство. Будем доказывать лемму по индукции.

Предварительно заметим, что, повторяя лемму 1 для дробных $c_i(x)$, мы должны предположить, что в решении

$$\tilde{\omega}_k = \frac{\tilde{c}_0(x) + \tilde{c}_1(x)\cdot y + \ldots + y^{k-1}}{\tilde{D}_k(x)},$$

в котором $\tilde{c}_i(x)$ могут быть и дробными, $\tilde{D}_k(x)$ делится на $D_k(x)$. При $k=2$, если

$$\tilde{\omega}_2 \subset \Omega', \quad \omega_2 \subset \Omega',$$

то

$$\tilde{\omega}_2 \cdot \frac{\tilde{D}_2(x)}{D_2(x)} - \omega_2 = \frac{\tilde{c}_0(x)}{D_2(x)} - \frac{c_0(x)}{D_2(x)} \subset \Omega',$$

что невозможно, так как даже

$$\tilde{c}_0(x) - c_0(x)$$

не лежит в $\Omega'$.

Предположим, что наше утверждение правильно для $i=1, 2, 3, \ldots, k$, и докажем его справедливость для $i=k+1$. Допустим противное: пусть в $\Omega'$ содержится

$$\tilde{\omega}_{k+1} = \frac{\tilde{c}_0 + \tilde{c}_1 y + \ldots + \tilde{c}_{k-1} y^{k-1} + y^k}{\tilde{D}_{k+1}}, \tag{4}$$

где некоторые из $\tilde{c}_0, \tilde{c}_1, \ldots, \tilde{c}_{k-1}$ не лежат в $\Omega'$. Поскольку $\tilde{D}_{k+1}$ делится на $D_{k+1}$, мы без нарушения общности можем принять

$$\tilde{D}_{k+1} = D_{k+1}.$$

Пусть

$$\omega_{k+1} = \frac{c_0 + c_1 y + \ldots + c_{k-1} y^{k-1} + y^k}{D_{k+1}}.$$

Тогда

$$\tilde{\omega}_{k+1} - \omega_{k+1} = \frac{(\tilde{c}_0 - c_0) + (\tilde{c}_1 - c_1) y + \ldots + (\tilde{c}_{k-1} - c_{k-1}) y^{k-1}}{D_{k+1}} \subset \Omega'. \tag{5}$$

Пусть $D_{k+1} = D_k \cdot d_{k+1}$,

$$\tilde{c}_{k-1} - c_{k-1} = \frac{\varphi}{\psi},$$

где $\varphi, \psi$ — взаимно простые полиномы. Далее, обозначим через $\delta$ общий наибольший делитель полиномов $d_{k+1}\psi$ и $\varphi$, и пусть $u, v$ — полиномы, для которых

$$u\varphi + v\, d_{k+1}\psi = \delta.$$

Тогда, если

$$(6)\quad \omega_k = \frac{b_0 + b_1 y + \ldots + y^{k-1}}{D_k} = \frac{b_0 d_{k+1}\psi + b_1 d_{k+1}\psi \cdot y + \ldots + d_{k+1}\psi y^{k-1}}{D_{k+1}\cdot\psi},$$

то

$$(7)\quad u(\tilde{\omega}_{k+1} - \omega_{k+1}) + v\omega_k =$$

$$= \frac{[u(\tilde{c}_0 - c_0) + v b_0 d_{k+1}\psi] + [u(\tilde{c}_1 - c_1) + v b_1 d_{k+1}\psi] y + \ldots + \delta y^{k-1}}{D_{k+1}\cdot\psi} \subset \Omega'.$$

Положим

$$d_{k+1}\cdot\psi = \delta\cdot\delta'.$$

Тогда элемент (7) может быть представлен в виде

$$\frac{\tilde{u}_0 + \tilde{u}_1 y + \ldots + \tilde{u}_{k-2} y^{k-2} + y^{k-1}}{D_k\cdot\delta'} \subset \Omega'.$$

Если $\delta'$ отлично от константы, то полученное соотношение будет противоречить нашему индуктивному предположению. Если же $\delta' = \text{const.}$, т. е. если

$$d_{k+1}\cdot\psi = \delta,$$

то это означает, что $\varphi$ делится на $d_{k+1}\psi$. Это возможно лишь в том случае, если

$$\psi = \text{const.},$$

т. е. если

$$\tilde{c}_{k-1} \subset \Omega'.$$

Пусть в этом случае

$$\varphi = d_{k+1}\cdot\psi\cdot q.$$

Тогда элемент (5) можно представить в виде

$$\tilde{\omega}_{k+1} - \omega_{k+1} = \frac{\tilde{v}_0 + \tilde{v}_1 y + \ldots + \tilde{v}_{k-2} + q y^{k-1}}{D_k} \subset \Omega',$$

причём не все $\tilde{v}_i$ лежат в $\Omega'$. Отсюда

$$\tilde{\omega}_{k+1} - \omega_{k+1} - q\omega_k =$$

$$= \frac{(\tilde{v}_0 - b_0) + (\tilde{v}_1 - b_1) y + \ldots + (\tilde{v}_{k-2} - b_{k-2}) y^{k-2}}{D_k} \subset \Omega',$$

причём не все коэффициенты $\tilde{v}_i - b_i$ лежат в $\Omega'$. Применяя к этому элементу такой же процесс совместно с $\omega_{k-1}$, мы опять или придём к противоречию с индуктивным предположением, или

$$\tilde{v}_{k-2} - b_{k-2}$$

будет лежать в $\Omega'$ и делиться на $d_k$, где

$$D_k = D_{k-1} \cdot d_k.$$

Продолжая процесс, мы в конце концов придём к противоречию с индуктивным предположением, поскольку не все $\widetilde{v_i} - b_i$ лежат в $\Omega'$. Лемма доказана.

Докажем, что система элементов (2) составляет базис кольца $\Omega'$. Допустим противное: пусть

$$c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n \subset \Omega',$$

где не все коэффициенты $c_1, c_2, \ldots, c_n$ лежат в $\Omega'$. Пусть $c_k = \frac{\varphi}{\psi}$ — последний из этих коэффициентов, не лежащий в $\Omega'$. Тогда

$$\theta = c_1\omega_1 + c_2\omega_2 + \ldots + c_{k-1}\omega_{k-1} + \frac{\varphi}{\psi} \cdot \omega_k \subset \Omega'.$$

$\varphi$ и $\psi$ можно предположить взаимно простыми полиномами, причём $\psi$ не есть постоянная. Найдём такие полиномы $u$, $v$, чтобы

$$u \cdot \varphi + v \cdot \psi = 1.$$

Тогда

$$u \cdot \theta + v \cdot \omega_k = uc_1\omega_1 + uc_2\omega_2 + \ldots + uc_{k-1}\omega_{k-1} + \frac{\omega_k}{\psi} \subset \Omega'.$$

С другой стороны, подставляя в это выражение вместо $\omega_1, \omega_2, \ldots, \omega_k$ их выражения из (2), получим:

$$u \cdot \theta + v\omega_k = \frac{w_0\omega_1 + w_1 y + \ldots + w_{k-2}y^{k-2} + y^{k-1}}{D_k \cdot \psi} \subset \Omega'.$$

Полученное соотношение противоречит выбору элемента $\omega_k$, что доказывает наше утверждение. Итак:

Теорема 18. *Всякое кольцо $\Omega'$ имеет базис, причём элементы базиса могут быть выбраны в форме*

$$(8) \qquad \omega_k = \frac{c_{k0} + c_{k1}y + \ldots + c_{k,k-2}y^{k-2} + y^{k-1}}{D_k} \qquad (k = 1, 2, \ldots, n),$$

*где все $c_{ki} \subset \Omega'$, $D_k \subset \Omega'$, причём $D_k$ делятся на $D_{k-1}$.*

Остановимся на случае $\Omega' = \Omega$. Базис этого кольца носит название *фундаментального базиса*. Существует бесчисленное множество фундаментальных базисов. Однако

Теорема 19. *Дискриминанты всех фундаментальных базисов равны друг другу с точностью до постоянных множителей.*

Доказательство. Пусть $Z$ и $H$ — два базиса кольца $\Omega$. Тогда элементы каждого из них выражаются через элементы другого

с коэффициентами из кольца $\Omega$:

$$\eta_i = b_{i1}\zeta_1 + b_{i2}\zeta_2 + \ldots + b_{in}\zeta_n \qquad (i = 1, 2, \ldots, n)$$

и

$$\zeta_i = c_{i1}\eta_1 + c_{i2}\eta_2 + \ldots + c_{in}\eta_n \qquad (i = 1, 2, \ldots, n),$$

где

$$Z = [\zeta_1, \zeta_2, \ldots, \zeta_n],$$
$$H = [\eta_1, \eta_2, \ldots, \eta_n],$$
$$b_{ik} \subset \Omega, \quad c_{ik} \subset \Omega.$$

Для матриц

$$B = \|b_{ik}\|, \quad C = \|c_{ik}\|$$

имеет место очевидное соотношение

$$B \cdot C = \mathcal{E},$$

откуда

$$|B| \cdot |C| = 1.$$

В этом равенстве каждый множитель левой части входит в $\Omega$, т. е. является полиномом от $x$. Равенство может иметь место только тогда, когда каждый из множителей входит в $k$, т. е. является постоянной. Обращаясь к формуле (16) § 6, мы увидим, что дискриминанты $\Delta(Z)$ и $\Delta(H)$ отличаются постоянным множителем, что требовалось доказать.

Дискриминант фундаментального базиса носит название *дискриминанта поля* $k(x, y)$, хотя это название не совсем точно: этот дискриминант в силу теоремы 19 не зависит от выбора фундаментального базиса, но он зависит от выбора элемента $x$ в поле $k(x, y)$.

Заметим, что выражение дискриминанта базиса $Z$ останется тем же, если мы вместо $x$ возьмём другой элемент, определяющий поле $k(x)$, т. е. элемент вида $\frac{ax+b}{cx+d}$. В самом деле, из формулы (14) § 6 следует, что дискриминант базиса выражается через следы от произведений его элементов, $S(\omega_\mu \omega_\nu)$. Но след $S(z)$, выражаемый через коэффициенты уравнения, которому удовлетворяет $z$ в поле $k(x)$, не изменится, если в роли $x$ мы возьмём $\frac{ax+b}{cx+d}$.

Из этого, однако, не следует, что выражение дискриминанта *поля* не изменится, если мы заменим $x$ на $\frac{ax+b}{cx+d}$. В самом деле, после этой замены кольцо $\Omega$ изменится, а базис $Z$ перестанет быть базисом кольца $\Omega$. В следующем параграфе мы увидим, что при такой замене переменной произойдёт с дискриминантом поля.

В заключение остановимся на вопросе о фактическом нахождении фундаментального базиса при помощи конечного числа действий. Здесь основная трудность заключается в том, как узнать, суще-

ствует или нет элемент $w$ кольца $\Omega$, выражающийся через данный базис с коэффициентами, содержащими в знаменателе полиномы $h(x)$. Из формулы (2) следует, что в этом случае полином $h(x)$ является делителем полинома $\Delta(Z)$ и притом входит в него по крайней мере во второй степени. Таким образом нам остаётся испытать лишь конечное число неприводимых полиномов в роли $h(x)$. Пусть степень одного из них есть $s$. Тогда в роли $w$ мы можем рассмотреть только элементы вида

$$w = \frac{1}{h(x)} \{\zeta_1 + b_2(x)\zeta_2 + \ldots + b_n(x) \cdot \zeta_n\},$$

где в качестве $b_i(x)$ можно взять полиномы $(s-1)$-й степени с неопределёнными коэффициентами (при этом мы должны в качестве $\zeta_1$ рассмотреть по очереди все элементы $\zeta_1, \zeta_2, \ldots, \zeta_n$).

Составляя для $w$ уравнение, мы увидим, что условие $w \subset \Omega$ приведётся к условию делимости нескольких полиномов с неопределёнными коэффициентами на ту или иную степень полинома $h(x)$. Эти условия запишутся в виде алгебраических соотношений между неопределёнными коэффициентами. Их совместность проверяется при помощи приёмов теории исключения. Проверка их совместности внутри числового поля $k$ представляет более трудную задачу. Эта задача отпадает в том случае, если $k$ есть алгебраически замкнутое поле. В этом случае вообще вся задача упрощается благодаря тому, что $h(x)$ есть линейный полином $s = 1$, так что в качестве $b_i(x)$ можно взять просто неопределённые константы.

## § 12. Нормальный базис

В этом параграфе мы даём другой приём построения фундаментального базиса, который не требует никаких ограничений для рассматриваемых полей. В то же время он вводит новое понятие *нормального базиса*, весьма важное для всей дальнейшей теории. Что касается фактического проведения излагаемого приёма, то он может быть осуществлён при помощи так называемой *диаграммы Ньютона*, которая будет изложена в одной из дальнейших глав книги.

Будем наряду с кольцом $\Omega$ целых элементов от $x$ рассматривать кольцо $\Omega_1$ целых элементов от $x_1 = \frac{1}{x}$.

Теорема 20. *Общими элементами колец $\Omega$ и $\Omega_1$ являются только константы.*

Доказательство. Пусть $y \subset \Omega$ и одновременно $y \subset \Omega_1$. Тогда в силу определения кольца $\Omega$ $y$ удовлетворяет уравнению вида

$$y^n + a_1(x)\, y^{n-1} + \ldots + a_n(x) = 0, \tag{1}$$

где $a_i(x)$ — полиномы от $x$. В силу определения кольца $\mathfrak{Q}$ коэффициенты $a_i(x)$ должны быть также элементами кольца $\mathfrak{Q}_1$, т. е. полиномами от $\frac{1}{x}$. Это возможно лишь тогда, когда все $a_i(x) \subset k$. Но тогда корни уравнения (1) постоянны, ч. т. д.

Теорема 21. *Всякий элемент $y$ кольца $\mathfrak{Q}$ можно умножением на некоторую степень $x_1^r = x^{-r}$ сделать элементом кольца $\mathfrak{Q}_1$.*

Доказательство. Пусть в уравнении (1) степень каждого полинома $a_i(x)$ есть $k_i (i = 1, 2, \ldots, n)$. Это значит, что $k_i$ есть показатель наименьшей степени элемента $x_1$, умножением на которую $a_i\left(\frac{1}{x_1}\right)$ превратится в полином от $x_1$.

Сделаем в уравнении (1) подстановку

$$x = \frac{1}{x_1}, \quad y + \frac{y_1}{x_1^r},$$

где $r$ — пока неопределённый показатель, и умножим всё уравнение на $x_1^{nr}$. Получим:

$$y_1^n + x_1^r a_1\left(\frac{1}{x_1}\right) y_1^{n-1} + x_1^{2r} a_2\left(\frac{1}{x_1}\right) y_1^{n-2} + \ldots + x_1^{nr} a_n\left(\frac{1}{x_1}\right) = 0.$$

Чтобы элемент $y_1$ входил в $\mathfrak{Q}_1$, необходимо и достаточно, чтобы соблюдались неравенства

$$r \geqslant k_1, \quad 2r \geqslant k_2, \ldots, nr \geqslant k_n. \tag{2}$$

Поэтому, если мы в качестве $r$ возьмём

$$\rho = \operatorname{Max}\left\{\frac{k_1}{1}, \frac{k_2}{2}, \ldots, \frac{k_n}{n}\right\}, \tag{3}$$

то увидим, что $\rho$ является наименьшим значением $r$, при котором

$$y \cdot x_1^r \subset \mathfrak{Q}_1.$$

Будем называть число $\rho$ *дробным показателем* элемента $y$ относительно $x$. Ближайшее же целое число, не меньшее $\rho$, будем называть *целым показателем* элемента $y$. Оба показателя совпадают в том и только в том случае, если выражение (3) равно целому числу. Целый показатель $r$ есть наименьший показатель, при котором

$$y \cdot x_1^r \subset \mathfrak{Q}_1.$$

Теорема 21. *Если $g(x)$ — полином степени $s$, то оба показателя (и дробный и целый) элемента $y \cdot g(x)$ точно на $s$ превышают соответствующие показатели элемента $y$.*

Доказательство. Элемент $z = y \cdot g(x)$ удовлетворяет уравнению

$$z^n + g(x)a_1(x)z^{n-1} + [g(x)]^2 a_2(x) z^{n-2} + \ldots + [g(x)]^n \cdot a_n(x) = 0,$$

так что для $z$ роль показателей $k_1, k_2, \ldots, k_n$ играют

$$k_1 + s, \quad k_2 + 2s, \quad \ldots, \quad k_n + ns,$$

в силу чего дробный показатель элемента $z$ равен

$$\operatorname{Max}\left\{\frac{k_1+s}{1}, \frac{k_2+2s}{2}, \ldots, \frac{k_n+ns}{n}\right\} = \operatorname{Max}\left\{\frac{k_1}{1}, \frac{k_2}{2}, \ldots, \frac{k_n}{n}\right\} + s.$$

Из этой формулы следует, что и дробный и целый показатели элементов $y$ и $z$ отличаются точно на $s$.

В настоящем параграфе мы будем рассматривать исключительно целые показатели, которые будем называть просто показателями.

Будем говорить, что $\alpha$ делится на $\beta$, если

$$\frac{\alpha}{\beta} \subset \Omega.$$

Далее, будем говорить, что $\alpha$ сравнимо с $\beta$ по модулю $\gamma$:

$$\alpha \equiv \beta \pmod{\gamma},$$

если разность $\alpha - \beta$ делится на $\gamma$. Бо́льшая часть свойств, присущих равенствам, имеет место также для сравнений. Для знакомства со сравнениями можно рекомендовать читателю любой курс теории чисел.

Теорема 22. *Если (дробные) показатели элементов неравны, то показатель их суммы точно равен наибольшему из этих показателей. Если же они равны, то показатель их суммы равен или меньше, чем показатель слагаемых.*

*Примечание.* Утвержденне теоремы касается как дробных, так и целых показателей. Заметим, что если дробные показатели двух элементов равны, то равны и их целые показатели. Обратное может и не иметь места.

Пусть дробные показатели элементов $y$, $z$ равны $\rho, \sigma$ и пусть $\rho \geqslant \sigma$. Тогда

$$y \cdot x_1^{\rho} \subset \Omega_1, \quad z \cdot x_1^{\sigma} \subset \Omega_1,$$

откуда

$$(y + z) x_1^{\sigma} \subset \Omega_1,$$

так что показатель $y + z$ не превышает $\rho$.

Пусть теперь $\rho > \sigma$. Допустим, что показатель $u = y + z$ равен $\rho_1$, где $\rho > \rho_1 \geqslant \sigma$. Тогда $u \cdot x_1^{\rho_1} \subset \Omega_1$, $z \cdot x_1^{\rho_1} \subset \Omega_1$, откуда

$$yx^{\rho_1} = ux^{\rho_1} - zx^{\rho_1} \subset \Omega_1,$$

что противоречит предположению. Теорема доказана.

Нормальный базис кольца $\Omega$ строится так. В качестве его первого элемента возьмём $\lambda_1 = 1$; в качестве его второго элемента, $\lambda_2$, возьмём целый элемент, не входящий в $k(x)$, возможно более низкого показателя, в качестве третьего элемента — $\lambda_3$ — целый элемент, непредставимый в форме

$$c_1\lambda_1 + c_2\lambda_2,$$

где $c_1 \subset k(x)$, $c_2 \subset k(x)$, опять с возможно более низким показателем и т. д. Очевидно, что

$$r_1 = 0, \quad 1 \leqslant r_2 \leqslant r_3 \leqslant \ldots \leqslant r_n \tag{4}$$

(отсюда следует и существование таких элементов).

Теорема 23. *$[\lambda_1, \lambda_2, \ldots, \lambda_n]$ есть фундаментальный базис кольца $\Omega$.*

Доказательство. Прежде всего докажем, что $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ есть базис поля $k(x, y)$. В противном случае (см. § 4) между $\lambda_1, \lambda_2, \ldots, \lambda_n$ имело бы место соотношение

$$c_1(x)\lambda_1 + c_2(x)\lambda_2 + \ldots + c_n(x)\lambda_n = 0.$$

Пусть $s$ есть наибольший значок, для которого $c_s(0) \neq 0$. Тогда это соотношение можно переписать так:

$$c_1\lambda_1 + c_2\lambda_2 + \ldots + c_s\lambda_s = x \cdot \alpha,$$

где $c_i \subset k$, $\alpha \subset \Omega$, $c_s \neq 0$. Из неравенств (4) и теоремы 22 следует, что показатель левой части не превышает $r_s$ и в силу теоремы 21 показатель элемента $\alpha$ не превышает $r_s - 1$. Это показывает, что в базисе $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ элемент $\lambda_s$ выбран неправильно: вместо него можно было взять $\alpha$, показатель которого ниже.

Допустим, что в кольце $\Omega$ содержится элемент $\alpha$, представимый в форме

$$\alpha = b_1\lambda_1 + b_2\lambda_2 + \ldots + b_n\lambda_n, \tag{5}$$

где не все $b_1, b_2, \ldots, b_n$ полиномы. Пусть $g(x)$ есть общий знаменатель дробей $b_1, b_2, \ldots, b_n$ и пусть он содержит неприводимый множитель $h(x)$ степени $t$:

$$g(x) = g_1(x) \cdot h(x).$$

Вводя обозначение $g_1(x) \cdot h = \beta$, где опять $\beta \subset \Omega$, перепишем равенство (5) так:

$$\beta \cdot h(x) = c_1\lambda_1 + c_2\lambda_2 + \ldots + c_n\lambda_n, \tag{6}$$

где не все полиномы $c_1, c_2, \ldots, c_n$ делятся на $h(x)$. Деля каждый из $c_i$ на $h(x)$ с остатками:

$$c_i = h(x) \cdot q_i + u_i(x) \qquad (i = 1, 2, \ldots, n),$$

перепишем равенство (6) так

$$(7)\quad h(x)[\beta - q_1\lambda_1 - q_2\lambda_2 - \ldots - q_n\lambda_n] = u_1\lambda_1 + u_2\lambda_2 + \ldots + u_n\lambda_n,$$

где степени полиномов $u_i = u_i(x)$ ниже, чем $t$, и не все они равны нулю. Пусть $u_s$—последний из $u_i$, не равный нулю. Перепишем равенство (7) так:

$$h(x)\cdot\gamma = u_1\lambda_1 + u_2\lambda_2 + \ldots + u_s\lambda_s,$$

где $\gamma \subset \Omega$, а полином $u_s$ взаимно прост с $h(x)$ в силу неприводимости последнего. Найдём полиномы $v$, $w$, для которых

$$wh(x) + v\cdot u_s(x) = 1.$$

Тогда

$$h(x)[\gamma v + \lambda_s w] = vu_1\lambda_1 + vu_2\lambda_2 + \ldots + \lambda_s,$$

где $\gamma v + \lambda_s w \subset \Omega$. В силу теоремы 22 показатель правой части не превышает наибольшего из чисел

$$r_{s-1} + t - 1,\quad r_s,$$

откуда в силу теоремы 21 показатель элемента $\gamma v + \lambda_s w$ не превышает наибольшего из чисел

$$r_{s-1} - 1,\quad r_s - t,$$

т. е. меньше $r_s$. Это показывает, что выбор $\lambda_s$ был произведён неправильно. Таким образом при правильном выборе $\lambda_1, \lambda_2, \ldots, \lambda_n$ система $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ есть фундаментальный базис кольца $\Omega$.

Теорема 24. *Система элементов*

$$(8)\qquad \lambda_1' = \lambda_1\cdot x^{-r_1},\quad \lambda_2' = \lambda_2\cdot x^{-r_2},\quad \ldots,\quad \lambda_n' = \lambda_n\cdot x^{-r_n}$$

*составляет нормальный базис кольца* $\Omega_1$.

Доказательство. Каждый элемент $\lambda_i'$, рассматриваемый как элемент кольца $\Omega_1$, имеет показатель $r_i$, так как

$$\lambda_i'\cdot x_1^{-r_i} = \lambda_i \subset \Omega,\quad \lambda_i'\cdot x_1^{-(r_i-1)} = \frac{\lambda_i}{x} \not\subset \Omega$$

(второе в силу того, что $\frac{\lambda_i}{x}$ в силу условия своего выбора не может лежать в $\Omega$: иначе, в роли $\lambda_i$ мы должны были бы выбрать $\frac{\lambda_i}{x}$).

Предварительно докажем, что $[\lambda_1', \lambda_2', \ldots, \lambda_n']$ есть фундаментальный базис кольца $\Omega_1$. В противном случае в кольце $\Omega_1$ существует элемент $\alpha'$, представимый в форме

$$(9)\qquad \alpha' = c_1'\lambda_1' + c_2'\lambda_2' + \ldots + c_n'\lambda_n',$$

где не все $c_i'$ полиномы от $x_1$. Если в знаменатели элементов $c_i'$ входят множители, взаимно простые с $x_1$, то, делая в этом равенстве подстановку (8), а также $\alpha' = \alpha \cdot x^{-p}$, где $\alpha \subset \Omega$, мы получим выражение элемента $x^u \cdot \alpha$ $(u \geqslant 0)$ через $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ с дробными коэффициентами. Но это противоречит тому, что $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ есть фундаментальный базис кольца $\Omega$.

Пусть в представлении (9) в знаменатели коэффициентов $c_i'$ входят степени $x_1$. Не нарушая общности, можно предположить, что

$$\beta' = \frac{c_1'\lambda_1' + c_2'\lambda_2' + \ldots + c_n'\lambda_n'}{x_1},$$

где $\beta' \subset \Omega_1$, и не все $c_i'$ делятся на $x_1$. Перенося кратности $x_1$ в правую часть, мы представим это равенство в виде

$$x_1\gamma' = c_1\lambda_1' + c_2\lambda_2' + \ldots + c_t\lambda_t',$$

где $\gamma' \subset \Omega_1$, а $c_i$ — константы, из которых $c_t$ последняя, не равная нулю. Подстановка (8) даёт:

$$x^{r_t - 1} \cdot \gamma' = c_1 x^{r_t - r_1} \cdot \lambda_1 + c_2 x^{r_t - r_2} \cdot \lambda_2 + \ldots + c_t\lambda_t. \tag{10}$$

Левая часть, как элемент кольца $\Omega$, имеет показатель $\leqslant r_t - 1$. Это показывает, что $\lambda_t$ был выбран неправильно, так как вместо него можно взять правую часть (10), которая имеет меньший показатель.

Теперь предположим, что $[\lambda_1', \lambda_2', \ldots, \lambda_n']$ не есть нормальный базис кольца $\Omega_1$. Это значит, что для какого-нибудь $s_1$ найдётся элемент $\alpha' \subset \Omega_1$, имеющий показатель $< r_s$ и не представимый в форме

$$c_1'\lambda_1' + c_2'\lambda_2' + \ldots + c_{s_1-1}'\lambda_{s_1-1}',$$

где $c_i'$ — полиномы от $x_1$. Представим $\alpha'$ через фундаментальный базис $[\lambda_1', \lambda_2', \ldots, \lambda_n']$:

$$\alpha' = c_1'\lambda_1' + c_2'\lambda_2' + \ldots + c_s'\lambda_s', \tag{11}$$

где $s$ — наибольший значок, для которого $c_i' \not\equiv 0$. Ясно, что $s \geqslant s_1$, т. е. что $\alpha'$ имеет порядок $< r_s$. Умножая (11) на $x^{r_s - 1}$ и производя подстановку (8), получим:

$$x^{r_s-1} \cdot \alpha' = c_1' x^{r_s - r_1 - 1}\lambda_1 + c_2' x^{r_s - r_2 - 1}\lambda_2 + \ldots + c_s' x^{-1}\lambda_s.$$

Левая часть есть элемент кольца $\Omega$, правая же даёт его представление через $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ с коэффициентами, из которых последний не равен нулю и не может быть полиномом от $x$. Это противоречит теореме 23, ч. т. д.

Обратимся к случаю, когда $k(x, y) : k(x)$ расширение 1-го рода и, следовательно, дискриминант всякого базиса отличен от нуля (см. теорему 10).

Интересное соотношение имеет место между дискриминантами колец $\Omega$ и $\Omega_1$. Возьмём в качестве их фундаментальных базисов соответственно $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ и $[\lambda_1', \lambda_2', \ldots, \lambda_n']$. Матрица подстановки (8), переводящей первый базис во второй, есть

$$C = \begin{Vmatrix} x^{-r_1} & 0 & \ldots & 0 \\ 0 & x^{-r_2} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & x^{-r_n} \end{Vmatrix},$$

откуда

$$|C| = x^{-r_1 - r_2 - \cdots - r_n}.$$

В силу этого формула (16) § 6 даёт:

$$(12)\quad \Delta[\lambda_1', \lambda_2', \ldots, \lambda_n'] = x^{-2r_1 - 2r_2 - \cdots - 2r_n} \cdot \Delta[\lambda_1, \lambda_2, \ldots, \lambda_n].$$

Но в силу теоремы 23 $\Delta[\lambda_1, \lambda_2, \ldots, \lambda_n]$ есть дискриминант кольца $\Omega$, а $\Delta[\lambda_1', \lambda_2', \ldots, \lambda_n']$ в силу теоремы 24 и третьего с конца абзаца § 11 есть дискриминант кольца $\Omega_1$. Таким образом между дискриминантами $\Delta(\Omega)$ и $\Delta(\Omega_1)$ колец $\Omega$ и $\Omega_1$ имеет место связь

$$(13)\qquad \Delta(\Omega_1) = x^{-2r_1 - 2r_2 - \cdots - 2r_n} \cdot \Delta(\Omega).$$

Пусть $\Delta(\Omega)$ есть полином от $x$ степени $\delta$ и пусть полином $\Delta(\Omega_1)$ от переменной $x_1$ имеет $\delta_0$ нулевых корней, т. е. представляется в виде

$$c_{\delta_0} x_1^{\delta_0} + c_{\delta_0} x_1^{\delta_0 + 1} + \ldots + c_{\delta'} x_1^{\delta'} \qquad (c_{\delta_0} \neq 0).$$

Подстановка $x_1 = \frac{1}{x}$ превращает $\Delta(\Omega_1)$ в выражение

$$c_{\delta_0} x^{-\delta_0} + c_{\delta_0 + 1} x^{-\delta_0 - 1} + \ldots + c_{\delta'} x^{-\delta'}, \qquad (c_{\delta_0} \neq 0),$$

в котором наивысшая степень $x$ есть $x^{-\delta_0}$. Правая же часть равенства (13) содержит член наивысшей степени

$$x^{-2r_1 - 2r_2 - \cdots - 2r_n} \cdot x^{\delta},$$

откуда

$$(14)\qquad \delta + \delta_0 = 2(r_1 + r_2 + \ldots + r_n).$$

Число $\delta + \delta_0$, т. е. степень дискриминанта кольца $\Omega$, сложенная с числом нулевых корней в дискриминанте кольца $\Omega_1$, играет в

дальнейшем большую роль. Оно называется *порядком критичности* элемента $x$ и обозначается через $w_x$. Формула (14) показывает, что $w_x$ есть чётное число.

## § 13. Дивизоры и идеалы в поле алгебраических функций

Сначала рассмотрим случай, когда $k$ есть алгебраически замкнутое поле. Пусть поле $k(x, y)$ задано элементами $x$, $y$, связанными алгебраической зависимостью

$$(1) \qquad f(x, y) = a_0(x) \cdot y^n + a_1(x) \cdot y^{n-1} + \ldots + a_n(x) = 0,$$

где $a_i(x)$ — полиномы. Придадим элементу $x$ какое-нибудь значение, т. е. приравняем его какому-нибудь элементу $\alpha$ поля $k$. Тогда, подставляя $x = \alpha$ в уравнение (1), получим в силу замкнутости поля $k$ $n$ различных или частично одинаковых значений $y$. Каждая пара значений $x = \alpha$, $y = \beta$, удовлетворяющая соотношению (1), называется *точкой поля* $k(x, y)$ или, как это принято у Дедекинда и Вебера, *точкой римановой поверхности*. Задав значения элементов $x$ и $y$, мы можем получить, хотя и неоднозначно, значения всех элементов поля $k(x, y)$, которые будут называться значениями элементов в этой точке. При этом для определения точки мы можем исходить не только от значений элементов $x$, $y$, но от значений любой примитивной пары элементов поля $k(x, y)$.

Мы не должны исключать возможности принятия элементами поля $k(x, y)$ бесконечных значений. Будем говорить, что в точке $P$ элемент $z$ принимает значение $\infty$, если в этой точке элемент $\frac{1}{z}$ принимает значение нуль. В частности, значению $x = \alpha$ соответствует, среди прочих значений, значение $y = \infty$ тогда и только тогда, если

$$(2) \qquad a_0(\alpha) = 0.$$

В самом деле, сделаем в уравнении (1) подстановку $y = \frac{1}{y_1}$ и умножим его на $y_1^n$. Получим:

$$a_n(x) \cdot y_1^n + a_{n-1}(x) \cdot y_1^{n-1} + \ldots + a_1(x) \cdot y_1 + a_0(x) = 0.$$

Подставим сюда $x = \alpha$. Полученное численное уравнение будет иметь нулевые корни тогда и только тогда, если имеет место (2).

Чтобы получить точки, соответствующие бесконечным значениям элемента $x$, мы должны сделать в уравнении (1) подстановку $x = \frac{1}{x_1}$, умножить его на некоторую степень элемента $x_1$, достаточную для того, чтобы все коэффициенты уравнения (1) превратились в полиномы от $x_1$, но не все делились на $x_1$, и в полученное уравнение подставить $x_1 = 0$. Решая это численное уравнение, мы и получим искомые значения элемента $y_1$.

Это определение страдает некоторой неполнотой, зависящей от того, что значения примитивной пары не всегда определяют значения всех элементов поля. Так, если в точке $P$ имеет место $x=x_0$, $y=y_0$, то значение элемента $\frac{y-y_0}{x-x_0}$ остаётся неопределённым. Поэтому мы введём нижеследующее определение, принадлежащее Дедекинду и Веберу:

Определение. Будем называть точкой поля $k(x, y)$ сопоставление каждому элементу $u, v, w, \ldots$ поля $k(x, y)$ элемента числового поля $k$: $u_0, v_0, w_0, \ldots$ (не исключая бесконечных значений), при котором соблюдаются следующие условия:

$$(3) \qquad (u+v)_0 = u_0 + v_0, \quad (uv)_0 = u_0 \cdot v_0.$$

Другими словами, каждой точке отвечает гомоморфное (см. ниже § 3) отображение поля $k(x, y)$ на числовое поле $k$. Очевидно, что две точки должны считаться различными в том и только в том случае, если в поле $k(x, y)$ существует хотя бы один элемент, принимающий в этих точках различные значения.

Каждая точка $P$ поля $k(x, y)$ даёт возможность распределить все элементы поля $k(x, y)$ по трём следующим категориям:

1) элементы, принимающие в точке $P$ конечные и отличные от нуля значения;

2) элементы, обращающиеся в точке $P$ в нуль;

3) элементы, обратные к которым обращаются в точке $P$ в нуль (т. е. элементы, обращающиеся в точке $P$ в бесконечность).

В силу (3) элементы первых двух категорий вместе образуют кольцо; будем обозначать его через $\Omega_P$.

Элементы второй категории образуют идеал в кольце $\Omega_P$. В самом деле, сумма и разность элементов, обращающихся в точке $P$ в нуль, тоже обращается в нуль, а произведение элемента, обращающегося в нуль, на элемент, принимающий конечное значение, обращается в нуль.

Будем называть этот идеал *простым дивизором*, соответствующим точке $P$, и обозначать его просто через $P$.

Будем говорить, что элемент $u$ $P$-делится на элемент $v$, если частное $\frac{u}{v}$ есть элемент кольца $\Omega_P$. Заметим, что на элемент $v$ первой категории делится всякий элемент кольца $\Omega_P$, поскольку тогда обратный к нему элемент $\frac{1}{v}$ есть тоже элемент первой категории. Будем говорить, что элементы первой категории являются *единицами* кольца $\Omega_P$.

Когда мы будем иметь дело с несколькими простыми дивизорами, над которыми будем производить операции умножения и т. п., нам будет необходимо определять их в одном и том же кольце. Чтобы осуществить это, обратим внимание на то, что кольцо $\Omega_{P_1P_2\ldots P_s}$, состоящее из элементов, не обращающихся в бесконечность ни в одной

из точек $P_1, P_2, \ldots, P_s$, входит как часть в каждое из колец $\mathfrak{O}_{P_1}$, $\mathfrak{O}_{P_2}, \ldots, \mathfrak{O}_{P_s}$, а потому каждый из дивизоров $P_1, P_2, \ldots, P_s$ может быть определён в кольце $\mathfrak{O}_{P_1P_2\ldots P_s}$ и будет внутри его идеалом, причём теперь надо, например, под простым дивизором $P_1$ понимать совокупность элементов, обращающихся в нуль в точке $P_1$ и принимающих в остальных точках $P_2, P_3, \ldots, P_s$ конечные значения. С другой стороны, если дивизор $P_s$ определён в кольце $\mathfrak{O}_{P_1P_2\ldots P_s}$, то можно получить дивизор $P_1$ в кольце $\mathfrak{O}_{P_1}$, умножая его элементы на всевозможные элементы кольца $\mathfrak{O}_{P_1}$ и всевозможным образом суммируя полученные произведения.

Более того: можно определить дивизор $P$ и в кольце $\mathfrak{O}$, если только в точке $P$ $x$ не обращаются в бесконечность. В самом деле, можно определить $\mathfrak{O}$ как совокупность элементов, принимающих конечные значения во всех точках, в которых $x$ принимает конечные значения. В таком кольце тоже может быть определён дивизор $P$, если только в точке $P$ $x$ принимает конечное значение.

Строго говоря, идеалы в различных кольцах не могут считаться тождественными, и в некоторых работах по теории идеалов речь идёт лишь о соответствии между идеалами в различных кольцах [см., например, Грелль (H. Grell) [40']]. В частности, переход от более объемлющего к менее объемлющему кольцу носит название *сужения идеала*, а обратный переход — *расширение идеала*. Оба процесса были только что описаны. Важные для дальнейшего утверждения:

1) Оба процесса взаимно обратимы.

2) При каждом из процессов простые (лишённые делителей) идеалы остаются простыми (лишёнными делителей); в общей теории идеалов они нетривиальны. В нашем случае эти утверждения не понадобятся. В самом деле, в каком бы кольце элемент $u$ ни лежал, его делимость на простой дивизор $P$ однозначно определяется его обращением в нуль в точке $P$. Аналогично определяется его делимость на произведение степеней простых дивизоров (см. далее, стр. 80). Точно так же простота дивизора $P$ в любом кольце вытекает из того, что произведение значений в точке $P$ равно нулю только тогда, если одно из этих значений равно нулю (см. далее, теорема 27). Поэтому мы можем, не прибегая к вспомогательным кольцам, определять дивизор как формальное произведение степеней простых дивизоров, делимость на которое всякого элемента поля может быть проверена описанным выше путём [ср. Шмидт (T. K. Schmidt) [93]. Это также даёт нам право вводить для обозначения простого дивизора (а также соответствующей точки) один и тот же символ, независимо от того, в каком кольце он определён.

В дальнейшем мы при определении кольца $\mathfrak{O}_{P_1P_2\ldots P_s}$ будем в качестве $P_1, P_2, \ldots, P_s$ принимать систему точек, в которых элемент $x$ принимает одно и то же значение. Это представляет технические удобства

при построении доказательства и в то же время не делает существенных ограничений. В самом деле, пусть в точках $P_1, P_2, \ldots, P_s$ элемент $x$ принимает значения $x_1, x_2, \ldots, x_s$. Возьмём в качестве независимой переменной

$$\xi = (x - x_1)(x - x_2)\ldots(x - x_s) \cdot \frac{ay + b}{cy + d}, \tag{4}$$

где константы $a$, $b$, $c$, $d$ подберём так, чтобы элемент $\frac{ay+b}{cy+d}$ принимал во всех точках $P_1, P_2, \ldots, P_s$ конечные значения. Тогда $\xi$ во всех этих точках обращается в нуль. В то же время ясно, что, наряду с парой $(x, y)$, пара $(\xi, x)$ тоже является примитивной для поля $k(x, y)$.

Итак, будем рассматривать простые дивизоры в кольце $\Omega_{x=x_0}$, элементы которого принимают конечные значения во всех точках, в которых $x = x_0$. Число этих точек конечно; чтобы узнать, какие значения принимает в этих точках $y$ [равно как и всякий другой элемент поля $k(x, y)$], подставим в уравнение (1) $x = x_0$ и решим полученное таким образом численное уравнение относительно $y$. Можно также, производя над $y$ соответствующую дробную линейную подстановку, добиться того, чтобы ни в одной из этих точек $y$ не принимал бесконечных значений. Для этого необходимо и достаточно, чтобы коэффициент $a_0(x)$ в точке $x = x_0$ не обращался в нуль.

Если $u \subset P$ и в точке $P$ $x = x_0$, то свободный член в уравнении, которому удовлетворяет $u$ в поле $k(x)$, обращается при $x = x_0$ в нуль, т. е. делится на $x - x_0$. Если при этом старший коэффициент не обращается при $x - x_0$ в нуль, то норма $N(u)$ обращается при $x = x_0$ в нуль. Но указанному условию удовлетворяют все элементы кольца $\Omega_{x=x_0}$.

Будем говорить, что $u$ $P$-делится на $v$, где $u$, $v$ — элементы кольца $\Omega_P = \Omega_{x=x_0}$, если частное $\frac{u}{v}$ лежит в кольце $\Omega_P$, т. е. не обращается в бесконечность в точках, в которых $x = x_0$. В этом случае

$$N\left(\frac{u}{v}\right) = \frac{N(u)}{N(v)}$$

не обращается при $x = x_0$ в бесконечность, а потому множитель $x - x_0$ входит в $N(u)$ не в меньшей степени, чем в $N(v)$. Это утверждение не допускает обращения.

Докажем важную теорему, восходящую ещё к Золотарёву. Имея в виду её дальнейшие приложения (в § 15), мы докажем её в несколько более общем виде, чем это необходимо для ближайших целей: мы предположим $k$ самым общим полем, в частности, не требуя его алгебраической замкнутости (только случай конечного $k$ вызовет известные затруднения). В связи с этим мы вместо $x - x_0$ будем рассматривать неприводимый в поле $k$ полином $g(x)$, считая, что нормы всех элементов простого дивизора $P$ делятся на $g(x)$.

В следующем параграфе мы увидим, что нормы элементов дивизора не могут быть взаимно просты.

Теорема 25 (Золотарёва). *Если в кольце $\Omega$ целых элементов поля $k(x, y)$ нормы всех элементов простого дивизора $P$ делятся на $g(x)$ и и есть такой элемент из $P$, который делится на возможно меньшую степень $g(x)$ {скажем на $[g(x)]^\mu$}, то любой элемент из $P$ р-делится на и.*

Доказательство. Пусть $w \subset \Omega \cdot w \subset P$. Тогда элемент

$$tu - w,$$

где под $t$ мы будем разуметь произвольный полином от $x$, имеет норму, делящуюся на $[g(x)]^\mu$. Отсюда следует, что

$$\frac{N(tu-w)}{N(u)} = N\left(t - \frac{w}{u}\right) = t^n + A_1 t^{n-1} + \ldots + A_n \tag{5}$$

является дробной рациональной функцией от $x$, не содержащей в знаменателе множителя $g(x)$, т. е. лежит в кольце $\Omega_P$. Если мы сумеем подобрать $n+1$ полиномов $t_0, t_1, t_2, \ldots, t_n$ так, чтобы составленный из них определитель Вандермонда

$$\begin{vmatrix} 1, & t_0, & t_0^2, & \ldots, & t_0^n \\ 1, & t_1, & t_1^2, & \ldots, & t_1^n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1, & t_n, & t_n^2, & \ldots, & t_n^n \end{vmatrix} \tag{6}$$

не делился на $g(x)$, то из соотношений

$$\begin{aligned} &t_0^n + A_1 t_0^{n-1} + \ldots + A_n \subset \Omega_P, \\ &t_1^n + A_1 t_1^{n-1} + \ldots + A_n \subset \Omega_P, \\ &\cdots\cdots\cdots\cdots\cdots \\ &t_n^n + A_1 t_n^{n-1} + \ldots + A_n \subset \Omega_P \end{aligned}$$

будут вытекать соотношения

$$1 \subset \Omega_P, \ A_1 \subset \Omega_P, \ \ldots, \ A_n \subset \Omega_P. \tag{7}$$

Но элемент $\frac{w}{u}$, как видно из (5), удовлетворяет уравнению

$$t^n + A_1 t^{n-1} + \ldots + A_n = 0,$$

и соотношения (7) показывают, что $\frac{w}{u} \subset \Omega_P$, откуда следует, что $w$ $p$-делится на $u$.

Остаётся показать возможность подбора $t_0, t_1, \ldots, t_n$ так, чтобы определитель (6) не делился на $g(x)$. Если числовое поле $k$ содер-

жит бесчисленное множество элементов или хотя бы число элементов, превышающее $n$, то мы удовлетворим нашему требованию, если возьмём в качестве $t_0, t_1, \ldots, t_n$ различные элементы поля $K$ (константы).

Это условие не выполняется только в случае, когда $k$ есть конечное поле порядка $p^f$, где $p^f \leqslant n$. Тогда нам надо расширить числовое поле до $k^* \supset k$, где $k^*$ — поле порядка $f^*$, причём $p^{f^*} > n$. При этом простые дивизоры, вообще говоря, будут другими, например $P^*$, и лежащий в $P^*$ элемент с наименьшей нормой пусть будет $u^*$. В § 15, где будет исследована связь между простыми дивизорами при различных числовых полях, мы покажем, что существует простой дивизор $P^*$, содержащий $P$, и что в этом случае $u$ $p$-делится на $u^*$. Кроме того, всякий элемент кольца $\Omega$, $p$-делящийся (в кольце $\Omega^*$) на $u^*$, $p$-делится на $u$.

Таким образом идеал $P$ в кольце $\Omega_P$ есть не что иное, как совокупность произведений одного элемента (в настоящем случае $u$) на всевозможные элементы кольца $\Omega_P$. Идеалы, имеющие такую структуру, называются *главными идеалами*. Теорема 25 может быть выражена так: в каждом *полулокальном кольце* все простые идеалы главные. При этом мы будем называть локальным (полулокальным) кольцом множество элементов, принимающих конечные значения в одной точке (соответственно, в конечном числе точек). На стр. 121 — 122 мы видели, что всё сводится к рассмотрению колец, $\Omega_{x=x_0}$.

Теорема 25 уже не имеет места для кольца $\Omega$. Это следует из того, что в $k(x, y)$, как мы увидим ниже, не существует элементов, обращающихся в нуль только в одной точке.

Теорема 25 даёт возможность весьма просто определить понятие непростого дивизора. Прежде всего определим степень $P^k$ простого дивизора $P$. Для этого введём рассмотренный уже нами элемент $u$, на который делятся все элементы дивизора $P$, и определим дивизор $P^k$ как совокупность элементов, $p$-делящихся на $u^k$. Далее, чтобы определить дивизор $Q = P_1^{k_1} P_2^{k_2}, \ldots, P_s^{k_s}$ в кольце $\Omega_{QQ'}$ (здесь важно, чтобы дивизор $QQ'$, определяющий полулокальное кольцо $\Omega_{QQ'}$, содержал все точки $P_1, P_2, \ldots, P_s$), надо найти элементы $u_1, u_2, \ldots, u_s$, определяющие главные идеалы $P_1, P_2, \ldots, P_s$, и определить дивизор $Q$ как совокупность элементов, $p$-делящихся на $u_1^{k_1} u_2^{k_2} u_s^{k_s}$.

Докажем, что дивизоры описанного типа исчерпывают все возможные идеалы в полулокальных кольцах. Пусть $U$ — какой-нибудь идеал в кольце $\Omega_{P_1 P_2 \ldots P_s}$. Мы можем предположить, что $x$ принимает в точках $P_1, P_2, \ldots, P_s$ одно и то же значение $x_0$, и определим идеал $U$ сначала в более узком кольце $\Omega_{x=x_0}$. Если в идеале $U$ содержатся элементы, норма которых не делится на $x - x_0$, то

$U=\Omega_{x=x_0}$. В самом деле, пусть $u$ — такой элемент. Тогда для $\frac{w}{u}$, где $w$ — произвольный элемент кольца $\Omega_{x=x_0}$, имеет место уравнение

$$N\left(t-\frac{w}{u}\right)=\frac{N(ut-w)}{N(u)}.$$

В его левой части числитель есть полином от $t$ с коэффициентами из $\Omega_{x=x_0}$, а знаменатель есть единица этого кольца. Поэтому $N\left(t-\frac{w}{u}\right)$ есть полином от $t$ с коэффициентами из $\Omega_{x=x_0}$ и старшим коэффициентом единица. Отсюда следует

$$\frac{w}{u}\subset\Omega_{x=x_0}$$

и из $u\subset U$ вытекает $w\subset U$, т. е.

$$U=\Omega_x.$$

Пусть $u$ будет элемент идеала $U$, делящийся на наиболее низкую, $\mu$-ю степень элемента $x-x_0$. Повторяя доказательство теоремы 25, мы убедимся, что всякий элемент идеала $U$ $p$-делится на $u$. Обозначая через $\frac{U}{u}$ совокупность частных от деления элементов идеала $U$ на $u$, мы видим, что она содержит элемент $\frac{u}{u}=1$ и потому совпадает с $\Omega_{x=x_0}$.

Умножая $u$ на всевозможные элементы более широкого кольца $\Omega_{P_1P_2\dots P_s}$, мы получим идеал $U$, определённый в кольце $\Omega_{P_1P_2\dots P_s}$. Итак:

Теорема 26. *Всякий идеал полулокального кольца есть главный идеал.*

Теорема 27. *Идеал $P$ кольца $\Omega_{x=x_0}$ есть простой и лишённый делителей идеал.*

Доказательство. Если произведение $u\cdot v$ элементов кольца $\Omega_{x=x_0}$ входит в $P$, то это означает, что $u_0v_0=0$, откуда или $u_0=0$, или $v_0=0$. Таким образом или $u\subset P$, или $v\subset P$.

Допустим, что $P$ содержится в идеале $\Pi$, и пусть

$$u\not\subset P,\quad u\not\subset\Pi.$$

Из первого соотношения следует $u_0\neq 0$. Пусть $u$ — элемент из $\Pi$, в норму которого $x-x_0$ входит в возможно меньшей степени. Если $N(u)$ вовсе не делится на $x-x_0$, то, как мы только что доказали, $\Pi=\Omega_{x=x_0}$. Если же $N(u)$ делится на $x-x_0$, то из $u_0\neq 0$ следует, что $u$ обращается в нуль в другой точке $P_1$, в которой $x-x_0$ тоже обращается в нуль. Тогда существует элемент $w$,

принимающий в $P_1$ другое значение, $w_1$, чем в $P$, где $w = w_0$. Таким образом, $w - w_0 \subset P$ и потому $w - w_0 \subset \Pi$. Но в силу теоремы 25 $w - w_0$ $p$-делится на $u$. Это, однако, невозможно, поскольку $w - w_0$ принимает в точке $P$ значение $w_1 - w_0 \neq 0$, а $u$ обращается в нуль, ч. т. д.

*Базисом* идеала $U$ в кольце $\Omega_{x=x_0}$ называется система $n$ элементов $[\theta_1, \theta_2, \ldots, \theta_n]$ такого рода, что $\theta_i \subset U$ $(i = 1, 2, \ldots, n)$, и, кроме того, всякий элемент идеала $U$ может быть представлен в форме

$$c_1\theta_1 + c_2\theta_2 + \ldots + c_n\theta_n,$$

где $c_i \subset \Omega_{x=x_0}$ $(i = 1, 2, \ldots, n)$. Если даны два базиса одного и того же идеала $U$, то один из них переходит в другой при помощи подстановки с коэффициентами из $\Omega_{x=x_0}$. Обозначая матрицу этой подстановки через $C$, мы получим для её определителя $|C|$:

$$|C| \subset \Omega_{x=x_0}.$$

С другой стороны, если $C'$ — матрица подстановки, переводящей второй базис в первый, то

$$|C'| \subset \Omega_{x=x_0}.$$

Но $C \cdot C' = \mathfrak{E}$, где $\mathfrak{E}$ — единичная матрица, откуда

$$|C| \cdot |C'| = 1.$$

Таким образом, определитель $|C|$ есть единица кольца, т. е. взаимн прост с $x = x_0$.

Построим двумя различными путями базис простого дивизора $P$. Пусть $Z = [\omega_1, \omega_2, \ldots, \omega_n]$ есть фундаментальный базис кольца $\Omega$. Тогда, если $U$ есть элемент идеала $P$, в норму которого $x - x_0$ входит в возможно меньшей степени, то

$$[u\omega_1, u\omega_2, \ldots, u\omega_n]$$

есть базис идеала $P$. В самом деле, $u\omega_i \subset P$ $(i = 1, 2, \ldots, n)$. С другой стороны, если $w \subset P$, то в силу теоремы 25 $\frac{w}{u} \subset \Omega_{x=x_0}$, в силу чего

$$\frac{w}{u} = c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n,$$

где $c_i \subset \Omega_{x=x_0}$ $(i = 1, 2, \ldots, n)$, откуда

$$w = c_1u\omega_1 + c_2u\omega_2 + \ldots + c_nu\omega_n.$$

Пусть базис $[u\omega_1, u\omega_2, \ldots, u\omega_n]$ выражается через базис $[\omega_1, \omega_2, \ldots, \omega_n]$ при помощи подстановки с матрицей $B = \|b_{ik}\|$:

$$u\omega_i = b_{i1}\omega_1 + b_{i2}\omega_2 + \ldots + b_{in}\omega_n \qquad (i = 1, 2, \ldots, n).$$

Тогда $u$ удовлетворяет уравнению

$$\begin{vmatrix} b_{11}-u, & b_{12}, & \ldots, & b_{1n} \\ b_{21}, & b_{22}-u, & \ldots, & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{n1}, & b_{n2}, & \ldots, & b_{nn}-u \end{vmatrix} = 0,$$

откуда

$$N(u) = |b_{ik}| = |B|.$$

Формула (16) § 6 даёт:

$$\Delta(uZ) = [N(u)]^2 \cdot \Delta(Z). \tag{6'}$$

Не нарушая общности, можно положить $\omega_1 = 1$. Будем обозначать значения элементов $\omega_i$ в точке $P$ через $\bar{\omega}_i$ $(i = 2, 3, \ldots, n)$. Опять-таки, не нарушая общности, можно предположить, что они равны нулю

$$\bar{\omega}_i = 0 \qquad (i = 2, 3, \ldots, n). \tag{7}$$

Тогда система

$$[x - x_0, \omega_2, \ldots, \omega_n]$$

является базисом идеала $P$. В самом деле, с одной стороны, все её элементы обращаются в точке $P$ в нуль и потому лежат в $P$. С другой стороны, если $u \subset P$, то выразим $u$ через $[1, \omega_2, \ldots, \omega_n]$:

$$u = c_1(x) + c_2(x)\omega_2 + \ldots + c_n(x)\omega_n,$$

где $c_i(x) \subset \Omega_{x=x_0}$ $(i = 1, 2, \ldots, n)$. В точке $P$ значение $u$ равно нулю, откуда в силу (7)

$$0 = c_1(x_0).$$

Обозначая $c_1(x)$ через $(x - x_0)\gamma_1(x)$, где $\gamma_1(x) \subset \Omega_{x=x_0}$, мы тем самым выразим $u$ через базис $[x - x_0, \omega_2, \ldots, \omega_n]$. Матрица подстановки, выражающей этот базис через $Z$, такова:

$$\begin{Vmatrix} x - x_0, & 0, & \ldots, & 0 \\ 0, & 1, & \ldots, & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & \ldots, & 1 \end{Vmatrix},$$

и её определитель равен $x - x_0$. Формула (16) § 6 даёт:

$$\Delta[x - x_0, \omega_2, \ldots, \omega_n] = (x - x_0)^2 \cdot \Delta(Z). \tag{8}$$

Сопоставляя формулы (6') и (8), мы убедимся, что

Теорема 28. *Простой дивизор всегда содержит элемент, норма которого делится точно на первую степень* $x - x_0$.

Будем называть $x - x_0$ *нормой* простого идеала $P$.

Наконец отметим важное следствие из теоремы Золотарёва, носящее название *теоремы о независимости простых дивизоров*:

Теорема 28′ (*теорема о независимости простых дивизоров*). *Каковы бы ни были простые дивизоры* $P_1, P_2, \ldots, P_k$ *и целые неотрицательные показатели* $\alpha_1, \alpha_2, \ldots, \alpha_k$, *в кольце* $\Omega$ *существует элемент, делящийся точно на* $P_1^{\alpha_1}, P_2^{\alpha_2} \ldots P_k^{\alpha_k}$.

Доказательство. Не нарушая общности, можно считать, что независимая переменная $x - x_0$ делится на каждый из простых дивизоров $P_1, P_2, \ldots, P_k$. Найдём для каждого из этих простых дивизоров элементы $u_1, u_2, \ldots, u_k$, соответственно делящиеся на $P_1, P_2, \ldots, P_k$, и нормы которых точно делятся на $x - x_0$. Это возможно в силу теорем 25 и 28. Тогда элемент

$$u = u_1^{\alpha_1} \cdot u_2^{\alpha_2} \ldots u_k^{\alpha_k}$$

делится на $P_1^{\alpha_1} P_2^{\alpha_2} P_k^{\alpha_k}$. С другой стороны, его норма точно делится на

$$(x - x_0)^{\alpha_1 + \alpha_2 + \ldots + \alpha_k},$$

а потому и не может делиться ни на один из дивизоров

$$P_1^{\alpha_1 + 1}, \; P_2^{\alpha_2 + 1}, \; \ldots, \; P^{\alpha_k + 1},$$

так как тогда бы его норма делилась по крайней мере на

$$(x - x_0)^{\alpha_1 + \alpha_2 + \ldots + \alpha_k + 1}.$$

Заметим, что некоторые из заданных показателей $\alpha_1, \alpha_2, \ldots, \alpha_k$ могут быть нулями, и тогда можно формулировать эту теорему так:

Заданы два взаимно простых дивизора $U$, $V$. В кольце $\Omega$ существует элемент, делящийся точно на $U$ и взаимно простой с $V$.

## § 14. Представление элементов поля через дивизоры

Мы видели в § 9, что всякую рациональную функцию можно представить в виде частного от произведений неприводимых полиномов, которые в случае алгебраически замкнутого числового поля $k$ являются линейными полиномами. Этот факт имеет место и для элементов поля $k(x, y)$, если заменить неприводимые полиномы простыми дивизорами.

В этом параграфе мы будем предполагать, что числовое поле $k$ или алгебраически замкнуто, или во всяком случае настолько расширено, что поле $k(x, y)$ имеет примитивную пару. В § 8 мы видели, что последнее не всегда имеет место.

Рассмотрим элемент $x$, который является «независимой переменной» поля $k(x, y)$. В этом выборе нет никакого ограничения, поскольку любой непостоянный элемент может быть выбран в

качестве независимой переменной. Если $(x, y)$ есть примитивная пара поля $k(x, y)$ и $x, y$ связаны неприводимым уравнением степени $n$ относительно $y$, то число $n$ вполне определяется заданием элемента $x$, не меняясь при переходе от $y$ к другому элементу поля $k(x, y)$, составляющему вместе с $x$ примитивную пару (см. § 4, теорема 2). Будем называть $n$ *порядком* элемента $x$. Ясно, что все элементы $\frac{ax+b}{cx+d}$ $(ad-bc \neq 0)$ имеют один и тот же порядок.

Пусть $P_1, P_2, \ldots, P_s$ — точки, в которых $x$ обращается в нуль, и пусть $u_1, u_2, \ldots, u_s$ — элементы соответствующих простых дивизоров, определяющие эти дивизоры в кольце $\Omega_{x=0}$. Элемент $\frac{x}{u_1}$ лежит в кольце $\Omega_{x=0}$. Если при этом $\frac{x}{u} \subset P_1$, опять разделим этот элемент на $u_1$ и т. д. Если $\frac{x}{u_1^k} \subset \Omega_{x=0}$, то $N\left(\frac{x}{u_1^k}\right) \subset \Omega_{x=0}$. Но так как $N(x) = x^n$, а $N(u_1^k)$ делится точно на $k$-ю степень $x$ (см. теорему 28), то $k \leqslant n$. Пусть $e_1$ — наибольший показатель, при котором

$$\frac{x}{u_1^{e_1}} \subset \Omega_{x=0}.$$

$\frac{x}{u_1^{e_1}}$ не может лежать в $P_1$, т. е. принимает в точке $P_1$ конечное и отличное от нуля значение. Далее, будем делить полученный элемент на возрастающие степени элемента $u_2$ и придём к элементу $\frac{x}{u_1^{e_1}u_2^{e_2}}$, принимающему в точках $P_1$, $P_2$ конечные и отличные от нуля значения. Продолжая процесс относительно $u_3, \ldots, u_s$, мы получим элемент

$$\frac{x}{u_1^{e_1}u_2^{e_2}u_s^{e_s}} \subset \Omega_{x=0},$$

не обращающийся в нуль ни в одной точке $P_1, P_2, \ldots, P_s$ и потому являющийся единицей кольца $\Omega_{x=0}$. Его норма не может делиться на $x$, но норма его числителя равна $x^n$, а норма знаменателя делится точно на $x^{e_1+e_2+\ldots+e_s}$. Отсюда следует формула

$$e_1 + e_2 + \ldots + e_s = n. \tag{1}$$

Но так как $x - x_0$ и $\frac{1}{x}$ при всяком $x_0 \subset k$ имеют порядок $n$, то для них можно получить такое же соотношение. Если мы будем говорить, что $x$ принимает в точке $P_\nu$ значение $x_0$ $e$ раз, если $x - x_0$ точно $p$-делится на $u_\nu^e$, то полученный результат можно формулировать так:

Теорема 29. *Всякий элемент поля $k(x, y)$ порядка $n$ принимает каждое значение (не исключая бесконечного) $n$ раз, если учитывать кратности, с которыми эти значения принимаются в отдельных точках.*

Следствие к теореме 29. *Если $P_1, P_2, \ldots, P_s$ — те простые делители элемента $x - x_0$, в которых $y = y_0$, и если $x - x_0$ точно делится на $P_1^{e_1} P_2^{e_2} \ldots P_s^{e_s}$, то полином*

$$f(x_0, y)$$

*точно делится на*

$$(y - y_0)^{e_1+e_2+\ldots+e_s}.$$

Доказательство. Сначала возьмём в роли $y$ элемент $u$ поля $k(x, y)$, который в точках $P_1, P_2, \ldots, P_s$ принимает различные значения $c_1, c_2, \ldots, c_s$, притом отличные от бесконечности, и каждое из них по одному разу *). Пусть

$$F(x, u) = 0 \tag{2}$$

*) Элемент $u(P)$ нетрудно построить, если только предположить, что числовое поле $k$ бесконечно или, по крайней мере, число его элементов превышает $s$. Для этого найдём элементы

$$v_1(P), v_2(P), \ldots, v_s(P)$$

такого рода, чтобы каждый $v_i(P)$ делился точно на первую степень $P_i$ и не делился на остальные простые дивизоры $P_1, P_2, \ldots, P_s$. Тогда

$$v_i(P_i) = 0, \quad v_i(P_j) \neq 0 \quad (i \neq j).$$

Выберем произвольно $s$ различных элементов

$$c_1, c_2, \ldots, c_s$$

поля $k$ и построим элемент

$$u(P) = v_1(P) v_2(P) \ldots v_s(P) \left\{ \frac{c_1}{v_1(P) \cdot v_2(P_1) \cdot v_3(P_1) \ldots v_s(P_1)} + \right.$$
$$+ \frac{c_2}{v_2(P) \cdot v_1(P_2) \cdot v_3(P_2) \ldots v_s(P_2)} + \ldots$$
$$\left. \ldots + \frac{c_s}{v_s(P) \cdot v_1(P_s) \cdot v_2(P_s) \ldots v_{s-1}(P_s)} + c \right\},$$

где $c$ — элемент поля $k$, находящийся пока в нашем распоряжении.

Очевидно, что

$$u(P_i) = c_i \qquad (i = 1, 2, \ldots, s).$$

Чтобы элемент

$$u(P) - c_i$$

не делился на $P_i^2$, необходимо и достаточно, чтобы

$$\left(\frac{u(P) - c_i}{v_i(P)}\right)_{P=P_i} \neq 0,$$

будет неприводимое уравнение степени $n$, связывающее $x$ с $u$. Выделяя в нём члены, делящиеся на $x - x_0$, приведём его к виду

$$F(x, u) = (x - x_0) \cdot \psi(x, u), \tag{3}$$

где $\psi(x, u)$ — полином. Пусть

$$F(x_0, u) = (u - c_1)^{e_1'}(u - c_2)^{e_2'} \dots (u - c_s)^{e_s'}, \tag{4}$$

где

$$e_1' + e_2' + \dots + e_s' = n. \tag{5}$$

Левая часть (3) как элемент поля $k(x, y)$ в силу (4) точно делится на $P_1^{e'}$, а правая часть (3) — по крайней мере на $P_1^{e_1}$. Отсюда следует

$$e_1' \geqslant e_1$$

и точно так же

$$e_2' \geqslant e_2, \quad e_3' \geqslant e_3, \quad \dots, \quad e_s' \geqslant e_s.$$

Принимая во внимание (1) и (5), мы получаем:

$$e_1' = e_1, \quad e_2' = e_2, \quad \dots, \quad e_s' = e_s, \tag{6}$$

и наше утверждение доказано для частного случая, когда элемент $y$ принимает во всех точках $P_1, P_2, \dots, P_s$ различные значения, и каждое по одному разу.

Перейдём к общему случаю. Пусть $y$ принимает значение $y_0$ в точках $P_1, P_2, \dots, P_s$, причём пусть $y - y_0$ делится на произ-

---

т. е. чтобы соблюдалось неравенство

$$\frac{c_1}{v_1(P_i) \cdot v_2(P_1) \dots v_s(P_1)} + \dots + \frac{c_{i-1}}{v_{i-1}(P_i) \cdot v_1(P_{i-1}) \dots v_s(P_{i-1})} + \\ + \frac{-c_{i+1}}{v_{i+1}(P_i) v_1(P_{i+1}) \dots} + \dots + \frac{c_s}{v_s(P_i) v_1(P_s) \dots v_{s-1}(P_s)} + \\ + \left( \frac{c_i}{v_i(P) v_1(P_i) \dots v_s(P_i)} - \frac{c_i}{v_i(P) v_1(P) \dots v_s(P)} \right)_{P = P_i} + c \neq 0,$$

т. е. чтобы $c$ не равнялось одному определённому элементу поля $k$. Если число элементов поля $k$ превышает $s$, то мы сможем найти для $c$ такое значение, чтобы при $i = 1, 2, \dots, s$ каждое из таких неравенств удовлетворялось. Тогда ни один из элементов

$$u(P) - c_i \qquad (i = 1, 2, \dots, s)$$

не будет делиться на $P_i^2$, что требовалось доказать.

В том случае, если в поле $k$ нехватит различных элементов, расширим поле $k$ так, чтобы при этом $P_1, P_2, \dots, P_s$ остались простыми дивизорами (см. далее, стр. 89—90).

вольные степени простых дивизоров $P_1, P_2, \ldots, P_s$. Пусть подстановка

$$y = \varphi(x, u) \tag{7}$$

переводит уравнение (2) в уравнение

$$f(x, y) = 0\ ^*). \tag{8}$$

Тогда подстановка

$$y = \varphi(x_0, u) \tag{9}$$

будет переводить уравнение

$$F(x_0, u) = (u - c_1)^{e_1}(u - c_2)^{e_2} \ldots (u - c_s)^{e_s} = 0 \tag{10}$$

в уравнение

$$f(x_0, y) = 0. \tag{11}$$

Но условие, что $y - y_0$ делится на $P_1, P_2, \ldots, P_s$, выражается в равенствах

$$\varphi(x_0, c_1) = \varphi(x_0, c_2) = \ldots = \varphi(x_0, c_s) = y_0,\ \varphi(x_0, c_i) \neq y_0\ (i > s). \tag{12}$$

С другой стороны, левая часть уравнения (11) получается из полинома (4) подстановкой (9), которая переводит каждый корень полинома (4) в корень (11):

$$f(x_0, y) = [y - \varphi(x_0, c_1)]^{e_1}[y - \varphi(x_0, c_2)]^{e_2} \ldots [y - \varphi(x_0, c_s)]^{e_s}.$$

В силу (12) это показывает, что $f(x_0, y)$ точно делится на

$$(y - y_0)^{e_1 + e_2 + \cdots + e_s},$$

что требовалось доказать.

Пусть какой-нибудь элемент $u$ поля $k(x, y)$ обращается в нуль в точках $P_1, P_2, \ldots, P_m$, причём в каждой ($i$-й) точке в нуль $\alpha_i$-й кратности и в бесконечность $\beta_i$-й кратности в каждой точке $P_i'$ $(i = 1, 2, \ldots, n)$. Из теоремы 29 следует:

$$\alpha_1 + \alpha_2 + \ldots + \alpha_m = \beta_1 + \beta_2 + \ldots + \beta_n.$$

---

*) Для существования подстановки (7) необходимо, чтобы $x$, $u$ составляли примитивную пару поля $k(x, y)$. Покажем, что это всегда имеет место. В противном случае неприводимое уравнение, связывающее $x$ и $u$, было бы степени $< n$, и элемент $x - x_0$ делился бы внутри поля $k(x, u)$ на простые дивизоры в степенях, сумма показателей которых была бы меньше $n$. Из этого следовало бы, что в поле $k(x, u)$ не существует элементов, делящихся точно на первую степень $P_i$ и не делящихся более ни на один из простых дивизоров $P_1, P_2, \ldots, P_s$. Но элементы $u_i - c_i$ $(i = 1, 2 \ldots, s)$ лежат в поле $k_s^*(x, u)$ и как раз обладают этим свойством. Таким образом $k(x, u) = k(x, y)$, что требовалось доказать.

Будем сопоставлять с элементом $u$ дробный дивизор

$$u \asymp \frac{P_1^{\alpha_1} P_2^{\alpha_2} \dots P_m^{\alpha_m}}{P_1'^{\beta_1} \cdot P_2'^{\beta_2} \dots P_m'^{\beta_m}} = \frac{Q}{Q'},$$

где под $Q$, $Q'$ мы разумеем произведения простых дивизоров, т. е. дивизоры высшего порядка. Такое сопоставление описывает поведение элемента $u$ во всех точках поля $k(x, y)$, т. е. показывает, в каких точках $u$ обращается в нуль и в каких в бесконечность. При этом мы можем и не считать числитель и знаменатель сопоставления (представления, как мы будем выражаться в дальнейшем) взаимно простыми, поскольку мы можем умножить его числитель и знаменатель на один и тот же дивизор. Если

$$u \asymp \frac{Q}{Q'}, \quad v \asymp \frac{R}{R'},$$

то очевидно, что

$$uv \asymp \frac{QR}{Q'R'}, \quad u : v \asymp \frac{QR'}{Q'R}.$$

Теорема 30. *Представление элемента через дивизоры определяет элемент с точностью до мультипликативной постоянной.*

Доказательство. Пусть

$$u \asymp \frac{Q}{Q'}, \quad v \asymp \frac{Q}{Q'}.$$

Тогда

$$u : v \asymp 1.$$

Это представление показывает, что элемент $u : v$ нигде не обращается ни в нуль, ни в бесконечность. Но каждый непостоянный элемент может быть выбран членом примитивной пары, так что, придавая ему значение нуль, мы получим значения для всех остальных элементов поля $k(x, y)$, т. е. определённую точку. Отсюда следует, что элемент $u : v$ есть постоянная

$$u : v = c,$$

откуда

$$u = c \cdot v,$$

что требовалось доказать.

*Примечание.* Из того, что $u : v = \text{const}$., ещё не следует

$$u : v \subset k, \tag{13}$$

так как не исключена возможность, что поле $k(x, y)$ содержит элементы, удовлетворяющие порознь алгебраическим уравнениям с коэффициентами из $k$, т. е. постоянные. Впрочем, если поле $k$ алгебраически замкнуто, то это не может произойти, и тогда имеет

место (13). Такого же положения можно достичь, если обозначить через $k$ наибольшее числовое поле, содержащееся в $k(x, y)$.

Пусть

$$x \equiv \frac{Q}{Q'}, \quad y = \frac{R}{R'}.$$

Выясним, каким условиям должны быть подчинены дивизоры для того, чтобы $y$ был *целой* функцией от $x$, т. е. чтобы в соотношении между $x$, $y$ коэффициент при старшей степени элемента $y$ был постоянным. Пусть

$$a_0(x) \cdot y^n + a_1(x) \cdot y^{n-1} + \ldots + a_n(x) = 0, \tag{14}$$

где $a_0(x)$, $a_1(x), \ldots, a_n(x)$ — полиномы, не имеющие общих им всем множителей. Если $y$ есть целая функция от $x$, то, согласно определению, $a_0(x) = 1$. Тогда любому конечному числовому значению элемента $x$ будут соответствовать $n$ (различных или частично совпадающих) конечных значений элемента $y$. Это означает, что точки, не входящие в дивизор $Q'$, не могут также войти в дивизор $R'$. Другими словами, дивизор $R'$ может содержать только те простые множители, которые содержатся в $Q'$. Выражаясь абстрактно, существует такой показатель $\alpha$, что $Q'^{\alpha}$ делится на $R'$.

Если же $a_0(x)$ содержит $x$, то существует конечное значение $x = x_0$, при котором $a_0(x_0) = 0$. Если подставить это значение в уравнение (3), то среди значений $y$ будут бесконечные (т. е. $\left(\frac{1}{y}\right)_0 = 0$). Соответствующая такому значению точка входит в дивизор $R'$, но не входит в дивизор $Q'$. Итак:

Теорема 31. *Чтобы элемент $y$ поля $k(x, y)$ был целой функцией от элемента $x$, необходимо и достаточно, чтобы в представлении элементов через дивизоры знаменатель, соответствующий элементу $y$, содержал только те простые множители, которые входят в знаменатель представления элемента $x$.*

## § 15. Случай алгебраически незамкнутого числового поля

Если числовое поле $k$ алгебраически не замкнуто и, возможно, не совершенно, то приведённое в § 13 определение простого дивизора не годится, хотя бы уже потому, что в этом случае нельзя установить понятие «точка»: если

$$f(x, y) = 0,$$

то, полагая $x = x_0$, мы в общем случае не будем иметь корней уравнения

$$f(x_0, y) = 0,$$

лежащих в $k$.

Положим в основу определения простого дивизора поля $k(x, y)$ распределение элементов этого поля на три категории, описанные в § 13:

1) ни одна из трёх категорий не пуста,

2) совокупность первых двух категорий образует кольцо $\mathfrak{O}_p$,

3) совокупность 2-й категории образует идеал в кольце $\mathfrak{O}_p$,

4) элементы, обратные к элементам 2-й (1-й) категории, и только они являются элементами 3-й (1-й) категории.

Будем говорить, что элемент поля $k(x, y)$ делится на заданный простой дивизор в том и только в том случае, если он относится ко второй категории. Обратимся к целым элементам поля, т. е. к элементам кольца $\mathfrak{O}$. Назовём конечными дивизоры $P$, для которых $\mathfrak{O}_p \supset \mathfrak{O}$. Тогда имеет место

Лемма 1. *Нормы всех элементов кольца $\mathfrak{O}$, делящихся на один и тот же конечный* *) *простой дивизор, делятся на один и тот же полином.*

Доказательство. Допустим противное. Тогда среди элементов, делящихся на простой дивизор $P$, существует конечное число таких, нормы которых не имеют общего делителя. Пусть это будут

$$w_1, w_2, \ldots, w_m.$$

Тогда существуют полиномы $\varphi_1(x)$, $\varphi_2(x)$, $\ldots$, $\varphi_m(x)$, для которых

$$(1)\quad \varphi_1(x) \cdot N(w_1) + \varphi_2(x) \cdot N(w_2) + \ldots + \varphi_m(x) \cdot N(w_m) = 1.$$

С другой стороны, элементы $N(w_k)$ вместе с $w_k$ принадлежат ко второй категории: поскольку элементы, принадлежащие к последней, образуют идеал относительно совокупности элементов двух первых категорий, к которым принадлежат $\varphi_k(x)$, левая часть равенства (1), т. е. единица, принадлежит ко второй категории. Но это невозможно, так как тогда 1-я и 3-я категории были бы пустыми.

Пусть $f(x)$ — общий делитель норм элементов, делящихся на $P$. Предположим, что он разлагается в произведение взаимно простых полиномов с коэффициентами из $k$:

$$f(x) = g(x) \cdot h(x).$$

Один из полиномов $g(x)$, $h(x)$, рассматриваемых как элементы поля $k(x, y)$, должен принадлежать ко 2-й категории, так как, если бы оба они принадлежали к первой категории, то это же в силу 4) имело бы место для элементов

$$\frac{1}{g(x)}, \quad \frac{1}{h(x)},$$

*) Т. е. такой, что $x$ входит в $\mathfrak{O}_p$.

откуда бы следовало, что произведение

$$\frac{1}{g(x)\cdot h(x)} = \frac{1}{f(x)}$$

принадлежит к 1-й или 2-й категории, и $f(x)$ не мог бы принадлежать ко 2-й категории. Но $f(x)$ как общий наибольший делитель полиномов $N(w_k)$, являющихся элементами 2-й категории, тоже принадлежит ко 2-й категории. Противоречие доказывает невозможность предположения. Пусть $g(x)$ принадлежит ко 2-й категории, т. е. делится на $P$. Его норма

$$N(g(x)) = [g(x)]^n,$$

а это противоречит предположению, что $f(x) = g(x)\cdot h(x)$ есть общий наибольший делитель норм элементов кольца $\mathfrak{Q}$, делящихся на $P$. Отсюда следует

Лемма 2. *Общий наибольший делитель норм всех элементов кольца $\mathfrak{Q}$, делящихся на простой дивизор $P$, есть степень неприводимого полинома.*

Пусть степень полинома $g(x)$ есть $m$ и пусть общий наибольший делитель норм всех целых элементов простого дивизора $P$ есть $[g(x)]^\mu$. В этом случае будем говорить:

$$N(P) = [g(x)]^\mu.$$

Будем называть произведение $m\cdot\mu$ *весом* простого дивизора $P$. Мы покажем, что вес простого дивизора не зависит от выбора переменной $x$ и что при присоединении к полю $k$ его алгебраического замыкания простой дивизор $P$ в известном смысле распадается в произведение $m\cdot\mu$ простых дивизоров.

*Примечание.* Следует уточнить понятие расширения числового поля. Пусть мы должны расширить числовое поле $k$ поля алгебраических функций $k(x, y, z, \ldots)$ до $k^*$ (в общем случае несовершенных полей мы не имеем права предполагать, что в поле $k(x, y, z, \ldots)$ существует примитивная пара элементов). Под полем $k^*(x, y, z, \ldots)$ мы должны разуметь совокупность рациональных функций от $x, y, z, \ldots$ с коэффициентами из поля $k^*$. Однако при этом мы не избежим некоторой двусмысленности, которая будет иметь место в том случае, когда в поле $k(x, y, z, \ldots)$ существуют элементы, алгебраические относительно $k$, но не лежащие в $k$. Пусть такой элемент $u$ удовлетворяет уравнению $\varphi(u) = 0$ с коэффициентами из поля $k$. Пусть, с другой стороны, поле $k^*$ содержит элемент, удовлетворяющий тому же уравнению. Должны ли мы считать, что эти элементы тождественны? Другими словами, что после расширения поля $k$ до $k^*$ элемент $u$ должен считаться элементом числового поля $k^*$? Вообще говоря, относительно этого необходимо сделать дополнительное условие, и таким образом поле $k^*(x, y, z, \ldots)$ не вполне определяется заданием полей $k(x, y, z, \ldots)$ и $k^*$. Этой двусмысленности мы

можем избежать, если потребуем, чтобы расширение $k^*/k$ было *нормальным*, т. е. чтобы всякое уравнение с коэффициентами из поля $k$, у которого хоть один корень лежит в $k^*$, имело все корни, лежащими в $k^*$ (см., например, Чеботарёв, Основы теории Галуа, ч. I, стр. 87). Тогда мы обязательно должны считать элемент $u$ лежащим в $k^*$. Это требование не содержит существенного ограничения, так как из теории Галуа (см. там же) следует, что всякое алгебраическое расширение является подполем нормального расширения.

Сначала рассмотрим случай совершенного поля $k$. Пусть

$$x_1, x_2, \ldots, x_m \tag{2}$$

— корни уравнения

$$g(x) = 0, \tag{3}$$

которые, в силу неприводимости этого уравнения в совершенном поле $k$, все различны. Будем считать элемент $y$ подобранным так, чтобы каждое из уравнений

$$f(x_k, y) = 0 \qquad (k = 1, 2, \ldots, m) \tag{4}$$

имело возможно большее число различных корней. Другими словами, в каждой из различных точек, для которых $x = x_k$ $(k = 1, 2, \ldots, m)$, значения $y$ должны быть различны.

Это всегда возможно сделать. В самом деле, пусть $k^*$ будет алгебраическое расширение поля $k$, содержащее все $x_k$ $(k = 1, 2, \ldots, m)$ и все корни уравнений (4), и пусть $P_1, P_2, \ldots, P_s$ — все различные точки, для которых $x = x_k$ $(k = 1, 2, \ldots, m)$. Тогда для каждой пары значков $i, j$ $(i \neq j)$ существует такой элемент $v_{ij}(P)$, что

$$v_{ij}(P_i) \neq v_{ij}(P_j) \qquad (i \neq j;\ i, j = 1, 2, \ldots, s).$$

Поэтому ни одно из $\frac{s(s-1)}{2}$ уравнений

$$\sum_{\mu,\nu=1}^{s} c_{\mu\nu} v_{\mu\nu}(P_i) = \sum_{\mu,\nu=1}^{s} c_{\mu\nu} v_{\mu\nu}(P_j) \quad (i \neq j;\ i, j = 1, 2, \ldots, s)$$

не тождественно относительно $c_{\mu\nu}$, а потому мы можем подобрать значения $c_{\mu\nu}$ так, чтобы ни одно из этих уравнений не удовлетворялось. Тогда элемент

$$y = \sum_{\mu,\nu=1}^{s} c_{\mu\nu} v_{\mu\nu}(P)$$

будет удовлетворять поставленному условию. Поскольку мы можем неограниченно расширять поле $k^*$, мы не испытаем недостатка в выборе различных значений, которые мы можем придавать величинам $c_{\mu\nu}$. При таком выборе элемента $y$ каждая из точек $P_1, P_2, \ldots, P_s$,

в которых $x = x_k$ $(k = 1, 2, \ldots, m)$, вполне определяется значениями элементов $x$ и $y$. Рассуждая так, как в выноске на стр. 83, мы убедимся, что $x$ и $y$ составляют примитивную пару поля $k(x, y)$.

Пусть

$$u = u(x, y)$$

будет произвольный целый элемент дивизора $P$ и пусть

$$\Phi(x, u) = 0$$

будет уравнение с коэффициентом 1 при старшей степени $u$ и коэффициентами из поля $k$, которому этот элемент удовлетворяет. Поскольку его член, не зависящий от $u$, равен $\pm N(u)$ и потому делится на $g(x)$, из этого следует, что каждый полином

$$u(x_k, y) \qquad (k = 1, 2, \ldots, m)$$

обращается в нуль, если $y$ принимает значение некоторых из корней уравнения (4); другими словами, он делится на один из неприводимых в поле $k(x_k)$ множителей полинома $f(x_k, y)$, например на $f^*(x_k, y)$. Пусть

$$u(x_k, y) = f^*(x_k, y) \cdot Q(x_k, y). \tag{5}$$

Полином

$$u(x, y) - f^*(x, y) \cdot Q(x, y)$$

при любом значении $y$ обращается в нуль, если положить $x = x_k$, и потому делится на неприводимый в поле $k$ полином $g(x)$. Отсюда следует, что соотношение (5) имеет место для всех значений $x_k : x_1, x_2, \ldots, x_m$. Если мы обозначим корни уравнений

$$f^*(x_k, y) = 0 \qquad (k = 1, 2, \ldots, m) \tag{6}$$

через

$$y_{k1}, y_{k2}, \ldots, y_{k\nu}, \tag{7}$$

то из (5) следует, что $u(x, y)$ обращается в нуль во всех $m \cdot \nu$ точках

$$P_{k_i}(x = x_k, y = y_{k_i}) \qquad (k = 1, 2, \ldots, m;\ i = 1, 2, \ldots, \nu). \tag{8}$$

Расширим числовое поле до поля $k^*$, в котором лежат все величины (2) и (7). Можно считать $k^*$ алгебраически замкнутым полем. В поле $k^*(x, y)$ элемент $u(x, y)$ и, следовательно, любой элемент поля $k(x, y)$, входящий в дивизор $P$, делится на каждый из (различных) простых дивизоров $P_{k_i}$, соответствующих точкам (8) *). Но

$$N(P_{k_i}) \doteq x - x_k \qquad (k = 1, 2, \ldots, m;\ i = 1, 2, \ldots, \nu),$$

*) Соответствие между дивизорами в полях, получающихся при расширении числовых полей, установлено на стр. 90 и след.

откуда следует, что $N(P)$ делится на

$$\prod_{k=1}^{m}(x-x_k)^{\nu}=[g(x)]^{\nu},$$

т. е.

$$\mu \geqslant \nu. \tag{9}$$

С другой стороны, в силу теоремы 28 мы можем найти в числовом поле $k(x_1, y_{11})$ элемент

$$u_{11}^{*}(x, y)=u^{*}(x_1; y_{11}; x, y),$$

делящийся точно на $P_{11}$ и не делящийся на остальные $P_{k_i}$. Тогда $N[u^{*}(x_k, y_{k_i} : x, y)]$ точно делится на первую степень $x-x_k$ и не делится на $x-x_1, \ldots, x-x_{k-1}, x-x_{k+1}, \ldots, x-x_m$. Таким образом произведение

$$\prod_{k=1}^{m}\prod_{i=1}^{\nu}u^{*}(x_k, y_{k_i}; x, y) \tag{10}$$

точно делится на $[g(x)]^{\nu}$. Впоследствии мы будем называть выражение (10) *арифметической нормой* от $u^{*}(x_1, y_{11}; x, y)$. Внутреннее произведение в этом выражении есть симметрическая функция от

$$y_{k1}, y_{k2}, \ldots, y_{k\nu}$$

и потому рационально выражается через $x_k$. Поэтому внешнее произведение, как симметрическая функция от $x_1, x_2, \ldots, x_m$, есть элемент поля $k(x, y)$. Как таковой он должен делиться на простой дивизор $P$, так как иначе он должен был бы принадлежать к 1-й категории относительно $P$ и также его норма, которая в силу этого не могла бы делиться на $g(x)$. Вспоминая определение $\mu$, мы получим

$$\nu \geqslant \mu;$$

сопоставляя с (9), будем иметь

$$\mu=\nu. \tag{11}$$

Таким образом всякому простому дивизору $P$ поля $k$ соответствует некоторое число $m\cdot\mu$ простых дивизоров $P_{k_i}$ поля $k^{*}(x, y)$ в том смысле, что всякий целый элемент поля $k(x, y)$ делится на $P$ тогда и только тогда, если он, рассматриваемый как элемент поля $k^{*}(x, y)$, делится на все дивизоры $P_{k_i}(k=1, 2, \ldots, m; i=1, 2, \ldots, \nu)$. В этом смысле мы будем говорить, что простой дивизор $P$ поля $k(x, y)$ при расширении числового поля до $k^{*}$ разлагается в произведение $m\cdot\mu$ простых дивизоров $P_{k_i}$.

Поскольку разложение простого дивизора в произведение простых дивизоров не зависит от того, какой элемент мы выберем в качестве независимой переменной $x$, вес простого дивизора $P$ тоже не зависит от выбора независимой переменной. При перемене независимой

переменной числа $m$ и $\mu$ могут измениться, но их произведение $m\mu$ останется тем же. Очевидно также, что в поле $k(x, y)$ могут содержаться простые дивизоры различных весов.

Обратимся к случаю несовершенного поля $k$. Заметим, что поле $k$ может быть несовершенным только в том случае, если оно содержит трансцендентные элементы $u, v, w, \ldots$ (см. § 5, в частности теорему 8). Самое общее поле алгебраических функций над $k$ может быть представлено как конечное алгебраическое расширение поля $k(x)$, причём элементы базиса этого поля над $k(x)$ связаны с $x$ неприводимыми в поле $k$ уравнениями (здесь может не существовать примитивной пары переменных). Часть элементов базиса может быть связана с $x$ уравнениями, содержащими эти элементы в степенях, не кратных $p$. Пусть эти элементы образуют поле $k(x, y)$ (в § 8 мы видели, что для таких полей можно находить примитивные пары). Если другие элементы базиса связаны с $x$ неприводимыми уравнениями, в которых $x$ входит в степенях, не кратных $p$ (например $z$), то, поменяв ролями $x$ и $z$ и находя при помощи исключения уравнения, связывающие остальные элементы базиса с $z$, мы в конце концов придём к полю, образованному при помощи $x$, затем переменной $y$ (присоединение 1-го рода) и, наконец, переменными $z_1$, $z_2, \ldots$, каждая из которых связана с $x$ неприводимым уравнением, содержащим все переменные в степенях, кратных $p$. Обозначим это поле через

$$K = k(x, y, z_1, z_2, \ldots).$$

Если мы присоединим к числовому полю $k$ элементы $u^{\frac{1}{p}}$, $v^{\frac{1}{p}}$, $w^{\frac{1}{p}}$, то уравнения, связывающие $x$ с $z_i$, превратятся в $p$-е степени неприводимых уравнений. Действительно, в силу выведенных в § 5 формул

$$(a+b)^p = a^p + b^p; \quad (ab)^p = a^p \cdot b^p$$

всякий элемент поля $K$ может быть представлен, как $p$-я степень элемента из $k^{\frac{1}{p}} = k(u^{\frac{1}{p}}, v^{\frac{1}{p}}, w^{\frac{1}{p}}, \ldots)$. Поэтому уравнение

$$f_i(u, v, w, \ldots; x^p, z_i^p) = 0$$

в силу теоремы Шёненманна может быть представлено так:

$$[f_i(u^{\frac{1}{p}}, v^{\frac{1}{p}}, w^{\frac{1}{p}}, \ldots; x, z_i)]^p = 0.$$

Из этого следует, что степень расширения

$$K_1 : k^{\frac{1}{p}}(x, y) = K^{\frac{1}{p}}(x, y, z_1, z_2, \ldots) \cdot k^{\frac{1}{p}}(x, y)$$

в $p$ раз меньше степени расширения

$$K : k(x, y).$$

Пусть $P$ есть простой дивизор поля $K$, $g(x)^p$ — его норма, т. е. общий наибольший делитель всех входящих в $P$ целых элементов. Мы видели, что $g(x)$ есть целый полином.

Рассмотрим дивизор $P$ в поле $K_1$. Это значит, что мы рассмотрим все целые элементы поля $K_1$, $p$-делящиеся на некоторый элемент $u$ поля $K$ (см. теорему 25). Дивизор $P$ может остаться простым и в поле $K_1$. В противном случае элемент $c \cdot u$ ($c$ — $p$ — единица поля $K$) можно представить в виде произведения элементов $u_1$, $u_2$ поля $K_1$:

$$c \cdot u = u_1 \cdot u_2,$$

причём ни $u_1$ ни $u_2$ не $p$-единицы, т. е. их нормы делятся на $g_1(x)$, где $g_1(x)$ — множитель полинома $g(x)$, неприводимый в поле $K^{\frac{1}{p}}$, так что или $g_1(x) = g(x)$, или $[g(x)]^p = g(x)$.

Пусть

$$u_1 = u_1(u^{\frac{1}{p}}, \ v^{\frac{1}{p}}, \ w^{\frac{1}{p}}, \ \ldots ; \ x, \ y, \ z_1, \ z_2, \ \ldots)$$

— тот из всевозможных множителей такого рода, норма которого делится на возможно более низкую степень полинома $g_1(x)$. $p$-я степень элемента $u_1$

$$u_1^p = u(u, \ v, \ w; \ \ldots ; \ x^p, \ y^p, \ z_1^p, \ z_2^p, \ \ldots)$$

есть элемент поля $K$; его норма делится на $g(x)$; вместе с тем, из

$$u^p = u_1^p \cdot u_2^p$$

и теоремы 25 следует, что всякий целый элемент дивизора $P^p$ $p$-делится на $u_1^p$. Отсюда следует, что в поле $K$ дивизор $P^p$ делится на дивизор $P_1^p$, т. е. на дивизор, образованный элементом $u_1^p$. Таким образом дивизоры $P$ и $P_1^p$ поля $K$ не могут быть взаимно простыми; в силу простоты дивизора $P$

$$P = P_1^p,$$

где $P_1$ — дивизор поля $K_1$, образованный элементом $u_1$.

Вместе с этим из определения элемента $u_1$ следует простота дивизора $P_1$ в поле $K_1$.

Итак, при расширении числового поля $k$ до поля $k^{\frac{1}{p}}$ простой дивизор поля $K$ или остаётся простым, или превращается в $p$-ю степень простого дивизора. В первом случае его вес (в силу понижения степени поля $K$) уменьшается в $p$ раз, во втором — в $p^2$ раз.

Повторяя операцию присоединения к числовому полю его $p$-х корней достаточное число раз, мы придём к присоединению 1-го рода, у которого поведение простых дивизоров изучено ранее.

Произведённые рассмотрения позволяют нам доказать теорему 25 для случая конечного числового поля $k$. Пусть $k$ — конечное поле порядка $p^f$, $k(x, y) : k(x)$ — расширение степени $n$, которое мы,

в случае необходимости меняя ролями $x$ и $y$, можем считать расширением 1-го рода. Пусть $P$ — простой дивизор поля $k(x, y)$, имеющий вес $m \cdot \mu$, где $m$ — степень неприводимого полинома $g(x)$, на который делятся нормы всех элементов дивизора $P$, а $\mu$ — степень неприводимого в поле $k(x_1)$ множителя $f^*(x_1, y)$ полинома $f(x, y)$, где $x_1$ — корень полинома $g(x)$. Выберем число $f^*$, взаимно простое с $m$ и $\mu$, для которого пусть

$$f^* > n, \tag{12}$$

и присоединим к числовому полю $k$ корень $\alpha$ неприводимого в рациональном поле характеристики $p$ уравнения

$$\varphi(u) = 0.$$

Это присоединение оставит полиномы $g(x)$ и $f^*(x_1, y)$ неприводимыми. В самом деле, допустим, например, что

$$g(x) = h_1(\alpha, x) \cdot h_2(\alpha, x), \tag{13}$$

где степень $m_1$ полинома $h_1(\alpha, x)$ меньше $m$. Коэффициенты полинома

$$h_1(\alpha_1 x) \cdot h_1(\alpha^p, x) \ldots h_1(\alpha^{p^{f^*-1}}, x) \tag{14}$$

лежат в $k$; он не взаимно прост с $g(x)$; следовательно, он делится на $g(x)$. С другой стороны, коэффициенты полинома $g(x)$ удовлетворяют равенствам

$$a_i^{p^{mu}} = a_i$$

при любом целом $u$. Возводя равенство в (13) в степень $p^{mu}$, где $u$ мы заставим удовлетворять уравнению

$$mu = f^* \cdot v + 1,$$

получим:

$$g(x) = h_1(\alpha^{p^{mu}}, x) \cdot h_2(\alpha^{p^{mu}}, x).$$

Но

$$\alpha^{p^{mu}} = (\alpha^{p^{f^* \cdot v}})^p = \alpha^p,$$

поскольку

$$\alpha^{p^{f^*}} = \alpha.$$

Таким образом

$$g(x) = h_1(\alpha^p, x) \cdot h_2(\alpha^p, x),$$

и вообще

$$g(x) = h_1(\alpha^{p^k}, x) \cdot h_2(\alpha^{p^k}, x) \quad k = 0, 1, \ldots, f^* - 1). \tag{15}$$

Перемножая равенства (15), мы видим, что полином (14) есть делитель полинома $[g(x)]^{f^*}$, откуда следует, что он равен какой-то степени полинома $g(x)$. Но это невозможно, так как степень $m_1 \cdot f^*$ полинома (14) в силу

$$m_1 < m, \quad (f^*, m) = 1$$

не может делиться на степень $m$ полинома $g(x)$.

Таким образом при присоединении $\alpha$ к $k$ полиномы $g(x)$ и $f^*(x_1, y)$ остаются неприводимыми, откуда следует, что дивизор $P$ остаётся простым. Из этого следует, что выбранный в $k(x, y)$ элемент $u(x, y)$, норма которого делится на возможно меньшую степень $g(x)$, удовлетворяет этому условию среди всех полиномов поля $k(\alpha_1\ x, y)$, входящих в дивизор $P$. С другой стороны, число элементов поля $k(\alpha)$ в силу (12) превышает число $n$, в силу чего в нём существуют элементы $t_0, t_1, \ldots, t_n$, для которых определитель (6) § 13 не делится на $g(x)$. Это устраняет единственное препятствие к доказательству теоремы 25.

Для дивизоров в незамкнутом числовом поле $P$ имеет место следующая модификация теоремы 29.

Теорема 29′. *Числитель и знаменатель представления всякого элемента поля $k(x, y)$ в поле $k$ являются дивизорами одинакового порядка* (равного порядку элемента), *если под порядком дивизора разуметь сумму весов его простых множителей.*

## Упражнения к главе II

1. *Гауссово преобразование эллиптических кривых.*
Преобразовать соотношение

$$y^2 = x(1-x)\ (1-\lambda^2 x),$$

полагая

$$\lambda^2 = \frac{4k}{(1+k)^2}, \quad x = \frac{(1+k)^2 t}{(1+kt)^2}, \quad y = \frac{(1+k)\ (1-kt)}{(1+kt)^3}.$$

2. Преобразовать соотношение

$$x^3 + y^3 - 3x - 3y + 4 = 0,$$

полагая

$$z = \frac{x-1}{y-1}, \quad t = y - 1.$$

3. Преобразовать соотношение

$$x^3 + y^3 + 3(x^2 + y^2) + 2(x + y) + 1 = 0,$$

полагая

$$z = x + y, \quad t = xy.$$

Показать, что это преобразование не бирационально.

4. Найти фундаментальный базис поля $k(x, y)$, где

$$y^n = f_1(x) \cdot f_2^2(x) \ldots f_{n-1}^{n-1}(x),$$

где $f_1(x), f_2(x), \ldots, f_{n-1}(x)$ — попарно взаимно простые и лишённые кратных делителей полиномы.

ГЛАВА III

# ИЗМЕРЕНИЕ КЛАССОВ

## § 16. Семейства и классы дивизоров

Будем называть два дивизора $U$ и $V$ *эквивалентными*, если они могут служить числителем и знаменателем представления через дивизоры какого-нибудь элемента поля $k(x, y)$. Будем выражать эквивалентность дивизоров $U$, $V$ символом

$$U \sim V.$$

Из теоремы 29 следует, что эквивалентные дивизоры должны быть одинакового порядка.

Теорема 32. *Из* $U \sim V$ *и* $V \sim W$ *следует*

$$U \sim W.$$

В самом деле, из эквивалентности дивизоров следует существование элементов $z$, $u$ поля $k(x, y)$, представляемых через дивизоры так:

$$z \eqsim \frac{U}{V}, \quad u \eqsim \frac{V}{W},$$

откуда

$$zu \eqsim \frac{U}{V} \cdot \frac{V}{W} = \frac{U}{W},$$

откуда

$$U \sim W.$$

Будем говорить, что эквивалентные друг другу дивизоры составляют *класс дивизоров*. Порядок каждого из дивизоров класса будем называть *порядком класса*.

Частное двух эквивалентных дивизоров определяет элемент поля $k(x, y)$ лишь с точностью до постоянного множителя. Поскольку в дальнейшем нам понадобится однозначное сопоставление этих частных с элементами поля, зададимся задачей нормировать постоянные множители. Это можно произвести при помощи самых разнообразных приёмов. Например, можно потребовать, чтобы элемент поля обращался в единицу в какой-нибудь фиксированной точке. Надо только выбирать эту точку таким образом, чтобы

в дальнейших рассуждениях она не понадобилась нам в качестве нуля или бесконечности какого-нибудь элемента поля $k(x, y)$. Если нам придётся рассматривать элемент поля, принимающий в фиксированной точке значение $\lambda$, то мы будем обозначать его символом

$$\lambda \cdot \frac{U}{V}.$$

Можно ввести понятие суммы эквивалентных дивизоров. Если

$$\frac{U}{V} \sim z,$$

то элемеиту

$$\lambda z + \mu$$

будет соответствовать дивизор

$$\lambda \cdot \frac{U}{V} + \mu,$$

который мы будем записывать в форме

$$\frac{\lambda U + \mu V}{V}.$$

Числитель этого символа может считаться дивизором: он является числителем элемента $\lambda z + \mu$. Если при этом мы хотим соблюсти правила нашего нормирования, то этот дивизор должен быть записан так:

$$U_1 = \frac{\lambda U + \mu V}{\lambda + \mu}.$$

Более практично записывать наш дивизор в форме $\lambda U + \mu V$, но всегда полагать сумму коэффициентов $\lambda$, $\mu$ равной единице:

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

Можно, и притом вполне определённым образом, подобрать коэффициенты $\lambda$, $\mu$ так, чтобы дивизор $\lambda U + \mu V$ разделился на любой заданный простой дивизор $P$. Для этого, обозначая значение элемента $z$ в точке $P$ через $z_0$, мы должны решить систему уравнений

$$\lambda z_0 + \mu = 0, \quad \lambda + \mu = 1. \tag{1}$$

Случай $z_0 = \infty$ соответствует делимости дивизора $V$ на $P$, так что в этом случае решением является

$$\lambda = 0, \quad \mu = 1.$$

Если $z_0 = 1$, то система (1) приводит к противоречию. Это, однако, только показывает, что нормирование $\lambda + \mu = 1$ здесь невозможно, решением же задачи (без нормирования) будет

$$\lambda = -\mu.$$

Эквивалентные дивизоры могут и не быть взаимно простыми. Из

$$UW \sim VW$$

следует

$$U \sim V,$$

и обратно.

Если задано некоторое конечное число эквивалентных дивизоров

$$U_1,\ U_2,\ \ldots,\ U_k, \tag{2}$$

то совокупность дивизоров

$$\lambda_1 U_1 + \lambda_2 U_2 + \ldots + \lambda_k U_k, \tag{3}$$

где $\lambda_1, \lambda_2, \ldots, \lambda_k$ — константы, называется *линейным семейством* дивизоров. Если разделим выражение (3) на один из дивизоров этого семейства, например на $U_1$, то получим линейное семейство

$$\lambda_1 + \lambda_2 z_2 + \ldots + \lambda_k z_k \tag{4}$$

элементов поля $k(x, y)$, где

$$z_i = \frac{U_i}{U_1} \qquad (i = 2, 3, \ldots, k).$$

Если выражение (4) не обращается тождественно в нуль ни при каких отличных от нуля значениях $\lambda_i$, будем говорить, что дивизоры (2) *линейно независимы*. Во всяком линейном семействе дивизоров всегда можно выделить систему линейно независимых дивизоров. Их число, которое, очевидно, не зависит от выбора независимых дивизоров, носит название *измерения* семейства дивизоров.

Докажем, что всякое семейство дивизоров имеет величину измерения, ограниченную заданием какого-либо дивизора семейства (или хотя бы его порядка). Для этого установим между порядком дивизоров семейства и измерением этого семейства неравенство. Пусть

$$\mathfrak{A} = (U_1,\ U_2, \ldots,\ U_k)$$

есть семейство дивизоров порядка $m$, имеющее измерение $k$:

$$\text{Изм}\ \mathfrak{A} = k, \quad \text{Пор}\ \mathfrak{A} = m.$$

Выберем произвольно простой дивизор $P$, на который пусть не делится один из дивизоров семейства, например $U_1$, и подберём константы $\lambda_2, \lambda_3, \ldots, \lambda_k$ так, чтобы дивизоры

$$U_2 - \lambda_2 U_1,\quad U_3 - \lambda_3 U_1,\quad \ldots,\quad U_k - \lambda_k U_1 \tag{5}$$

делились на $P$. Все эти дивизоры линейно независимы, так как всякая зависимость между ними повлекла бы за собой зависимость между дивизорами первоначального семейства $\mathfrak{A}$. Сокращая все дивизоры семейства (5) на $P$, а также на другие общие множители,

если таковые окажутся, мы придём к новому семейству дивизоров, которое будет иметь измерение $k-1$ и порядок $\leqslant m-1$. Продолжая переходить к новым семействам, у которых измерения постепенно уменьшаются с каждым шагом точно на единицу, а порядки — по крайней мере на единицу, мы, наконец, придём к семейству порядка $\leqslant 1$ и измерения $k-m+1$. Но семейства порядка 1 имеют измерения $\leqslant 2$, так как в семействах измерения $\geqslant 3$ мы можем произвольно фиксировать два простых множителя, в то время как дивизор порядка 1 содержит всего один простой множитель.

Таким образом

$$k-m+1\leqslant 2,$$

откуда

$$k\leqslant m+1. \tag{6}$$

Этим мы установили предварительное ограничение для измерений семейств дивизоров. Впоследствии мы дадим для измерений более точную оценку.

Пусть нам задан дивизор $U_1$ порядка $m$. Зададимся целью найти все эквивалентные с ним дивизоры. Если эквивалентных с $U_1$ дивизоров нет вовсе, мы будем называть дивизор $U_1$ *изолированным* и говорить, что *измерение класса* $(U_1)$ равно 1. Это также означает, что все эквивалентные с $U_1$ дивизоры имеют вид $\lambda U_1$.

Если существует эквивалентный с $U_1$ и линейно независимый от $U_1$ (т. е. не представимый в форме $\lambda U_1$) дивизор $U_2$, то с $U_1$ будут эквивалентны также все дивизоры

$$\lambda_1 U_1+\lambda_2 U_2, \tag{7}$$

образующие семейство

$$(U_1,\ U_2). \tag{8}$$

Если дивизорами вида (7) исчерпываются все эквивалентные с $U_1$ дивизоры, мы будем говорить, что семейство (8) является *классом* и что класс $(U_1)$ имеет измерение 2. Если же дивизорами вида (7) класс $(U_1)$ не исчерпывается, мы сможем найти дивизор $U_3$, эквивалентный с дивизором $U_1$ и линейно независимый от $U_1$, $U_2$ [т. е. не представимый в форме (7)]. Тогда с дивизором $U_1$ будут эквивалентны все дивизоры

$$\lambda_1 U_1+\lambda_2 U_2+\lambda_3 U_3,$$

образующие семейство

$$(U_1,\ U_2,\ U_3)$$

измерения 3. Продолжая такого рода расширение семейства дивизоров, мы в конце концов придём к семейству, исчерпывающему все дивизоры, эквивалентные с $U_1$. Будем называть такое семейство *классом дивизоров* $(U_1)$. Так как для каждого из семейств, получа-

емых в результате описанного процесса, измерение подчинено ограничению (6), то после конечного числа шагов мы непременно придём к классу, причём:

Измерение класса всегда конечно и может превышать его порядок самое большее на единицу.

Понятие измерения классов тесно связано с важным вопросом о существовании элементов поля $k(x, y)$ с заданными нулями (или бесконечностями). Именно, для того чтобы существовал непостоянный элемент поля $k(x, y)$, имеющий знаменателем заданный дивизор $U$ (или его делитель), необходимо и достаточно, чтобы измерение класса $(U)$ было $\geqslant 2$.

Если все дивизоры класса имеют какой-нибудь дивизор общим делителем, то класс называется *несобственным*. В этом случае, сократив все делители класса на общий делитель, мы придём к другому классу, имеющему то же измерение, но меньший порядок.

Теорема 33. *Общий делитель несобственного класса всегда является изолированным дивизором.*

Доказательство. Пусть $M$ есть общий наибольший делитель всех дивизоров класса $\mathfrak{A}$, так что

$$\mathfrak{A} = M \cdot \mathfrak{A}',$$

где $\mathfrak{A}'$ — уже собственный класс. Пусть $U_1, U_2, \ldots, U_s$ будет полная система линейно независимых дивизоров класса $\mathfrak{A}$. Допустим, что существует дивизор $M'$, эквивалентный дивизору $M$. Тогда дивизоры

$$M'U_1,\ M'U_2, \ldots$$

будут эквивалентны дивизорам класса $\mathfrak{A}$, линейно независимы и, следовательно, составляют полную систему линейно независимых дивизоров класса $\mathfrak{A}$. Таким образом все дивизоры класса $\mathfrak{A}$ делятся на $M'$. Это, однако, невозможно, так как $M'$ отличен от $M$, т. е. содержит хотя бы один простой дивизор, не входящий в $M$. Все дивизоры класса должны делиться на этот простой дивизор $p$, а это противоречит тому, что общий наибольший делитель всех дивизоров класса $\mathfrak{A}$ есть $M$.

В заключение заметим, что в геометрической теории алгебраических функций (алгебраической геометрии) рассматривается понятие, по существу совпадающее с понятием класса дивизоров, но носящее другое название. Именно, там дивизору соответствует *группа точек*, отсекаемая кривой

$$\varphi(x, y) = 0 \tag{9}$$

на основной кривой

$$f(x, y) = 0 \tag{10}$$

[соответствующей нашему соотношению, определяющему поле $k(x, y)$]. Линейному семейству точек соответствует *линейная серия* групп, отсекаемая на кривой (10) линейным семейством кривых

$$\lambda_1\varphi_1(x, y) + \lambda_2\varphi_2(x, y) + \ldots + \lambda_s\varphi_s(x, y) = 0.$$

Классу дивизоров соответствует *полная серия групп* (série complète). При этом у геометров принято считать измерением число, на единицу меньшее — число отношений $\frac{\lambda_2}{\lambda_1}, \frac{\lambda_3}{\lambda_1}, \ldots, \frac{\lambda_s}{\lambda_1}$ между коэффициентами.

## § 17. Определение производных

Для дальнейших исследований классов дивизоров необходимо ввести понятие *производной*. Введение этого понятия, в некотором смысле аналогичного понятию производной в анализе, должно быть произведено иначе, так как, определяя поле $k$, мы не делаем никаких предположений о величине его элементов и тем менее об их непрерывном изменении.

Если $u$, $v$ — элементы поля $k(x, y)$, то под производной «от $u$ по $v$» (обозначаемой через $\frac{du}{dv}$) мы будем разуметь новый элемент поля $k(x, y)$, значение которого в каждой точке $P$ (будем обозначать значения в ней элементов $u$, $v$, ... через $u_0$, $v_0$, ...) равно

$$\left(\frac{du}{dv}\right)_0 = \left(\frac{u - u_0}{v - v_0}\right)_0. \tag{1}$$

Чтобы сделать это определение правомерным, необходимо:

1) доказать, что элементы поля $k(x, y)$ вполне определяются своими значениями во всех точках поля $k(x, y)$;

2) доказать существование элемента поля $k(x, y)$, который бы принимал значения (во всех точках поля), указанные формулой (1).

Для решения первого вопроса предположим, что два элемента $u$, $v$ из $k(x, y)$ принимают во всех точках поля одни и те же значения. Тогда разность $u - v$ принимает значение нуль для всех точек поля. Но в том случае, когда числовое поле $k$ содержит бесчисленное множество элементов, это невозможно, так как мы видели, что отличные от нуля элементы поля $k(x, y)$ обращаются в нуль лишь в конечном числе точек. Если же $k$ есть конечное поле, то в $k(x, y)$ могуть существовать неравные нулю элементы, которые обращаются в нуль во всех точках, в которых элементы $x$, $y$ принимают значения из $k$. Например, если поле $k$ состоит из $p^n$ элементов, то элемент $x^{p^n} - x$ обращается в нуль при всех значениях $x \subset k$. Таким образом выражение для производной, которое мы сейчас найдём, в случае конечного поля $k$ не является единственным, которое бы удовлетворяло условию (1). Однако оно будет удовлетворять условию (1) также при всевозможных расширениях числового поля $k$,

что особенно важно ввиду того, что для получения всевозможных точек поля мы должны расширять поле.

В дальнейшем мы для простоты рассуждений будем предполагать, что рассматриваемые простые дивизоры имеют вес 1, т. е. что они соответствуют точкам поля, в которых элементы поля $k(x, y)$ имеют значения из $k$. Это безусловно имеет место в том случае, если $k$ алгебраически замкнуто. В противном случае мы должны расширять поле $k$ до того, чтобы рассматриваемые простые дивизоры в расширенном поле распадались на простые множители веса 1. Далее, установив справедливость равенства в расширенном поле, мы тем самым докажем его справедливость в первоначальном поле.

Можно было бы рассуждать иначе, подобно тому как мы это делали в § 15: взяв от элемента арифметическую норму, мы бы могли установить её делимость на неприводимый полином, соответствующий рассматриваемому простому дивизору высшего веса.

Перейдём ко второму вопросу. Сначала рассмотрим случай, когда $u$ есть полином от $v$:

$$u = f(v).$$

Полагая $v = v_0 + h$, мы перепишем формулу (1) так:

$$\left(\frac{du}{dv}\right)_0 = \left(\frac{f(v_0+h) - f(v_0)}{h}\right)_0. \tag{2}$$

Вместе с тем, рассматривая $f(v+h)$ как полином относительно $h$, разлагая его по степеням $h$ и обозначая через $f'(v)$ коэффициент при первой степени $h$, мы получим после подстановки в правую часть формулы (2), если примем во внимание, что

$$h_0 = (v - v_0)_0 = v_0 - v_0 = 0,$$

следующее:

$$\left(\frac{du}{dv}\right)_0 = \left(\frac{f(v_0) + hf'(v_0) + \ldots + h^n A_n(v_0) - f(v_0)}{h}\right)_0 = \\ = [f'(v_0) + \ldots + h^{n-1} A_n(v_0)]_0 = f'(v_0).$$

Это показывает, что производная $\frac{du}{dv}$ есть полином $f'(v)$, т. е. элемент поля $k(v)$. В частности, если

$$u = v^n,$$

то

$$\frac{du}{dv} = n \cdot v^{n-1}. \tag{3}$$

Далее, из формулы (2) вытекает, что из

$$u = u_1 + u_2$$

следует

$$\frac{du}{dv} = \frac{du_1}{dv_1} + \frac{du_2}{dv_2}. \tag{4}$$

Формулы (3) и (4) дают нам общеизвестное простое правило нахождения производных от полиномов.

Итак, производная от полинома $f(v)$ есть полином $f'(v)$. Назовём производную от $f'(v)$ *второй производной*, $f''(v)$, затем введём понятие третьей производной и т. д.

Напишем разложение полинома $f(v+h)$ по степеням $h$:

$$(5)\quad f(v+h)=A_0(v)+A_1(v)\cdot h+A_2(v)\cdot h^2+\ldots+A_n(v)\cdot h^n.$$

Полагая $h=0$, получим:

$$A_0(v)=f(v).$$

Далее, беря от обеих частей производную (при постоянном $v$) и руководясь правилами (4) и (5), получим:

$$(6)\quad f'(v+h)=A_1(v)+A_2(v)\cdot 2h+A_3(v)\cdot 3h^2+\ldots+A_n(v)\cdot n\cdot h^{n-1}.$$

Положим $h=0$:

$$A_1(v)=f'(v).$$

Опять берём производную от (6) и продолжаем процесс. Тогда

$$(7)\qquad A_k(v)=\frac{f^{(k)}(v)}{k!}\qquad (k=0,\ 1,\ 2,\ \ldots,\ n).$$

Подставляя в (5), мы придём к *формуле Тейлора*

$$(8)\quad f(v+h)=f(v)+h\cdot f'(v)+\frac{h^2}{2!}f''(v)+\ldots+\frac{h^n}{n!}f^{(n)}(v).$$

Можно аналогичным образом получить разложение полинома от нескольких переменных. Не останавливаясь на этом подробно, определим *частные производные* от полинома $f(x, y)$, $\frac{\partial f}{\partial x}$ и $\frac{\partial f}{\partial y}$ как коэффициенты при первых степенях соответственно $h$ и $k$ разложения $f(x+h, y+k)$ по степеням $h$ и $k$:

$$(9)\quad f(x+h, y+k)=f(x, y)+h\cdot\frac{\partial f(x, y)}{\partial x}+k\frac{\partial f(x, y)}{\partial y}+\ldots$$

Можно вывести, рассуждая аналогично предыдущему, формулу Тейлора для переменных

$$(10)\qquad f(x+h,\ y+k)=\sum_{\substack{0\leqslant\mu\leqslant m\\ 0\leqslant\nu\leqslant n}}\frac{h^\mu k^\nu}{\mu!\nu!}\cdot\frac{\partial^{\mu+\nu}f(x, y)}{\partial x^\mu\cdot\partial y^\nu},$$

где $\frac{\partial^{\mu+\nu}f(x, y)}{\partial x^\mu\cdot\partial y^\nu}$ — частная производная от $f(x, y)$, взятая $\mu$ раз по $x$ и $\nu$ раз по $y$ (можно показать, что операции нахождения производной по $x$ и по $y$ перестановочны).

Пусть элементы $x$, $y$ поля $f(x, y)$ связаны соотношением

$$f(x, y) = 0, \tag{11}$$

причём пусть в точке $P$ элементы $x$, $y$ принимают, соответственно, конечные значения $x_0$, $y_0$. Перепишем формулу (9) так:

$$f(x, y) = f(x_0, y_0) + (x - x_0)\left(\frac{\partial f}{\partial y}\right)_0 + (y - y_0)\left(\frac{\partial f}{\partial y}\right)_0 + \dots \tag{12}$$

Здесь должно иметь место (11), а также

$$f(x_0, y_0) = 0. \tag{13}$$

Из двух отношений

$$\frac{y - y_0}{x - x_0}, \quad \frac{x - x_0}{y - y_0}$$

по крайней мере одно принимает в точке $P$ конечное значение. Пусть это будет $\frac{y - y_0}{x - x_0}$. Разделим соотношение (12) на $x - x_0$ и примем во внимание (11) и (13):

$$\left(\frac{\partial f}{\partial x}\right)_0 + \frac{y - y_0}{x - x_0} \cdot \left(\frac{\partial f}{\partial y}\right)_0 + \sum_{\substack{0 \leqslant \mu \leqslant m \\ 0 \leqslant \nu \leqslant n \\ \mu + \nu \geqslant 2}} A_{\mu,\nu}(x_0, y_0)(x - x_0)^{\mu - 1}(y - y_0)^{\nu} = 0.$$

Теперь, совершая в этом равенстве подстановку $x = x_0$, $y = y_0$ (т. е. беря значения его членов в точке $P$) и учитывая, что при $\mu + \nu \geqslant 2$ члены $(x - x_0)^{\mu - 1}(y - y_0)^{\nu}$ в точке $P$ обращаются в нуль, получим:

$$\left(\frac{\partial f}{\partial x}\right)_0 + \left(\frac{y - y_0}{x - x_0}\right)_0 \cdot \left(\frac{\partial f}{\partial y}\right)_0 = 0. \tag{14}$$

Из этой формулы вытекает, что элемент

$$-\frac{\partial f}{\partial x} : \frac{\partial f}{\partial y} = -f_x : f_y \text{ *)}$$

поля $k(x, y)$ принимает в точке $P$ значение

$$\left(\frac{y - y_0}{x - x_0}\right)_0.$$

Принимая во внимание определение производной, т. е. формулу (1), мы приходим к заключению, что

$$\frac{dy}{dx} = -\frac{f_x}{f_y}. \tag{15}$$

Таким образом мы решили в самом общем случае и второй вопрос.

*) В дальнейшем мы вместо $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$ часто будем употреблять обозначения $f_x$, $f_y$.

Отметим в заключение формулу, полезную для приложений. Из очевидной формулы

$$\left(\frac{u-u_0}{v-v_0}\right)_0 \cdot \left(\frac{v-v_0}{w-w_0}\right)_0 = \left(\frac{u-u_0}{w-w_0}\right)_0$$

мы в силу (1) имеем:

$$\frac{du}{dv} \cdot \frac{dv}{dw} = \frac{du}{dw}. \tag{16}$$

Найдём производную $\frac{du}{dv}$, если $u = \frac{1}{v^k}$. Соотношение

$$f(u, v) = u \cdot v^k - 1 = 0$$

даёт

$$\frac{\partial f}{\partial v} = v^k, \quad \frac{\partial f}{\partial v} = k \cdot u \cdot v^{k-1},$$

откуда

$$\frac{du}{dv} = -k \cdot \frac{u}{v^k} \cdot v^{k-1} = -\frac{k}{v^{k+1}}.$$

Из этого мы делаем вывод, что формула (3) справедлива и для отрицательных значений показателя $n$.

## § 18. Представление производных через дивизоры

Пусть

$$x \approx \frac{X_1}{X}, \quad y \approx \frac{Y_1}{Y} \tag{1}$$

— представления элементов $x$, $y$ у поля $k(x, y)$ через дивизоры. Сначала рассмотрим случай конечных значений $x_0$, $y_0$ элементов $x$, $y$ в точке $P$. Пусть $x - x_0$ и $y - y_0$ делятся точно соответственно на $P^\alpha$ и $P^\beta$. Возьмём элемент $z$, делящийся точно на первую степень $P$. Тогда можно положить

$$x - x_0 = z^\alpha \cdot u, \quad y - y_0 = z^\beta \cdot v, \tag{2}$$

где

$$u_0 \neq \infty, \quad u_0 \neq 0; \quad v_0 \neq \infty, \quad v_0 \neq 0.$$

Вместе с тем значения производных $\frac{du}{dz}$, $\frac{dv}{dz}$ в точке $P$ равны значениям в этой точке выражений

$$\frac{u-u_0}{z}, \quad \frac{v-v_0}{z}.$$

Но в последних знаменатель делится точно на первую степень $P$, а числители — по крайней мере на первую степень $P$, в силу чего

$$\left(\frac{du}{dz}\right)_0 \neq \infty; \quad \left(\frac{dv}{dz}\right)_0 \neq \infty. \tag{3}$$

Руководясь правилами нахождения производной, указанными в предыдущем параграфе, мы получим из формул (2):

$$\frac{dx}{dz} = \alpha \cdot z^{\alpha-1} \cdot u + z^{\alpha} \cdot \frac{du}{dz},$$

$$\frac{dy}{dz} = \beta \cdot z^{\beta-1} \cdot v + z^{\beta} \cdot \frac{dv}{dz}.$$

В правых частях этих формул первые члены точно делятся, соответственно, на $P^{\alpha-1}$ и $P^{\beta-1}$, если мы исключим случай, когда поле $k$ имеет характеристику $p$, а показатель $\alpha$ (или $\beta$) делится на $p$. В этом случае первый член этих формул обращается в нуль. Вторые же члены этих формул, в силу (3), делятся по крайней мере на $P^{\alpha}$ и соответственно на $P^{\beta}$. Отсюда следует, что, за исключением упомянутого случая, $\frac{dx}{dz}$, $\frac{dy}{dz}$ точно делятся, соответственно, на $P^{\alpha-1}$ и на $P^{\beta-1}$.

Пользуясь формулой (16) § 17, будем иметь

$$\frac{dy}{dx} = \frac{dy}{dz} : \frac{dx}{dz},$$

откуда следует, что в представлении $\frac{dy}{dx}$ через дивизоры простой дивизор $P$ входит в степени

$$P^{(\beta-1)-(\alpha-1)}.$$

Особого рассмотрения требует случай бесконечного значения $x_0$ или $y_0$. Пусть, например, $x_0 = \infty$ и пусть простой дивизор $P$ входит в знаменатель $X$ представления элемента $x$ точно в $\alpha$-й степени. Тогда, оставляя за $z$, $u$ их прежние значения, мы будем иметь

$$x = z^{-\alpha} \cdot u, \quad \frac{dx}{dz} = -\alpha \cdot z^{-\alpha-1} \cdot u + z^{-\alpha} \cdot \frac{du}{dz},$$

откуда следует, что в знаменатель представления $\frac{dx}{dz}$ через дивизоры простой дивизор $P$ входит в $(\alpha+1)$-й степени. Таким образом, если ввести обозначения

$$(4) \qquad z_x = \prod P^{\alpha-1}, \quad z_y = \prod P^{\beta-1},$$

где все произведения распространены на все простые дивизоры, для которых показатель $\alpha$ (или соответственно $\beta$) превышает единицу, то нетрудно видеть, что всякий простой дивизор входит в представление производной $\frac{dy}{dx}$ в той же (положительной или отрицательной) степени, в какой он входит в дробный дивизор

$$\frac{Z_y}{Y^2} : \frac{Z_x}{X^2}.$$

Если мы убедимся, что произведения в формулах (4) конечны, то сможем заключить, что производная $\frac{dy}{dx}$ представляется через дивизоры так:

$$\frac{dy}{dx} \simeq \frac{Z_y}{Y^2} : \frac{Z_x}{X^2}. \tag{5}$$

Таким образом нам остаётся доказать, что число простых дивизоров, для которых значение $\alpha - 1$ (это число мы будем называть *мерой критичности* простого дивизора) больше нуля, конечно. Отбросив простые дивизоры, в которых $x$ или $y$ принимают бесконечное значение (их число конечно, поскольку они входят в дивизоры $X$ или $Y$), докажем, что остальные критические простые дивизоры являются делителями частной производной

$$f_y(x, y) = \frac{\partial f(x, y)}{\partial y}.$$

Допустим противное: пусть $x - x_0$ делится на $P^\alpha$, $\alpha > 1$, и пусть

$$f_y(x_0, y_0) \neq 0. \tag{6}$$

Тогда из формулы (14) § 17 следует, что $y - y_0$ делится по крайней мере на $P^\alpha$, т. е. что

$$\beta \geqslant \alpha.$$

Пусть $z$ — элемент поля $k(x, y)$, делящийся точно на первую степень $P$. Выразим его через $x, y$, причём в виде частного от деления полинома от $x, y$ на полином только от $x$:

$$z = \frac{j(x, y)}{h(x)}. \tag{7}$$

Из теоремы 1 следует, что такое представление всегда возможно.

Расположим числитель по степеням $x - x_0$ и $y - y_0$. Далее, разлагая по степеням $x - x_0$ и $y - y_0$ уравнение

$$f(x, y) = 0,$$

мы из (6) заключаем, что в этом разложении коэффициент при первой степени $y - y_0$ отличен от нуля и $y - y_0$ может быть выражено в виде полинома от $x - x_0$, $y - y_0$, члены которого содержат или $x - x_0$, или более высокие степени $y - y_0$. Подставим это выражение для $y - y_0$ в тот член числителя $j(x, y)$ выражения (7), который содержит самую низкую степень $y - y_0$. Если после этого все члены $j(x, y)$ будут содержать множитель $x - x_0$, выделим его и продолжим процесс, который прекратится после того, как полученный полином будет иметь отличный от нуля свободный член. Это непременно рано или поздно произойдёт, так как в противном случае мы бы пришли к полиному, делящемуся на сколь угодно

высокую степень простого дивизора $P$. Выделим и в знаменателе наивысшую степень $x - x_0$, так что получим

$$z = \frac{(x-x_0)^a \cdot j_1(x, y)}{(x-x_0)^b \cdot h_1(x)},$$

где

$$j_1(x_0, y_0) \neq 0, \quad h_1(x_0) \neq 0.$$

Таким образом элемент $z$ точно делится на $P^{\alpha(a-b)}$ и в силу нашего условия мы должны иметь:

$$\alpha(a-b) = 1.$$

Однако, если $\alpha > 1$, это невозможно ни при каких целых $a$, $b$.

Итак, если $x - x_0$ делится на $P^\alpha$, $\alpha > 1$, то $P$ есть делитель или элемента $f_y(x, y)$, или одного из дивизоров $X$, $Y$. Число таких простых дивизоров конечно, так что справедливость формулы (5) установлена.

В ходе доказательства нам было необходимо предположить, что производная $f_y(x, y)$ не обращается в нуль тождественно, что вполне возможно, если поле $k$ имеет характеристику $p$, и притом в выражении $f(x, y)$ входят только степени $y$, кратные $p$. В этом случае все простые дивизоры критичны, и все эти рассуждения не имеют силы. В том случае, когда поле $k$ имеет характеристику $p$, а в соотношении между элементами $x$, $y$ примитивной пары поля $k(x, y)$ элементы $x$, $y$ входят только в степенях $x^{p^r}$, $y^{p^s}$, нам придётся довольствоваться выражениями для производных от элементов поля $k(x^{p^r}, y^{p^s})$.

## § 19. Класс дифференциалов

Обратимся к представлению (5) § 18 производной $\frac{dy}{dx}$ через дивизоры. Правая часть этой формулы представляет собой частное двух дивизоров

$$\frac{Z_y}{Y^2}, \quad \frac{Z_x}{X^2},$$

из которых первый зависит только от $y$, а второй только от $x$. Это позволяет считать эти дивизоры представлениями *дифференциалов* $dy$, $dx$:

$$dx \eqsim \frac{Z_x}{X^2}. \tag{1}$$

Формула (5) § 18 показывает, что выражения (1), составленные для всевозможных элементов поля $k(x, y)$, эквивалентны друг с другом и таким образом образуют класс, который мы будем называть *классом дифференциалов* и обозначать через $\mathfrak{W}$. Класс $\mathfrak{W}$ играет фундаментальную роль во всей теории.

Порядок класса $\mathfrak{W}$ равен

$$\sum(\alpha-1)-2n_x, \tag{2}$$

где $\alpha-1$ есть мера критичности каждого простого дивизора относительно элемента $x$, а $n_x$ — порядок элемента $x$. Это выражение не зависит от выбора в поле $k(x, y)$ элемента $x$, т. е. является инвариантом поля $k(x, y)$. Введём обозначение

$$w_x=\sum(\alpha-1). \tag{3}$$

Ниже мы убедимся, что это число совпадает с введённым в § 12 *порядком критичности* $w_x$ элемента $x$. В § 12 мы видели, что $w_x$ — всегда чётное число. Далее, вводя обозначение

$$p=\frac{1}{2}w_x-n_x+1, \tag{4}$$

мы получим для порядка класса выражение

$$\text{Пор}\,\mathfrak{W}=2p-2. \tag{5}$$

Число $p$ является основным инвариантом теории алгебраических функций, независимо от того, как построена эта теория: теоретико-функционально, геометрически или арифметически. Это число встречается ещё в работах Абеля (N. — H. Abel, 1802—1829). Впервые в явном виде его ввёл Риман (B. Riemann, 1824—1866), который назвал его *родом* (Geschlecht); он определил $2p$ как порядок связности введённой им римановой поверхности. Вейерштрасс (K. Weierstrass, 1815—1897) ввёл это число независимо от Римана и назвал его *рангом*. Во Франции это число называют *жанром*, и этого термина мы и будем придерживаться ввиду того, что его употребление не грозит никакими недоразумениями, так как никакое другое понятие не носит название жанра.

Вслед за Риманом большинство математиков обозначает жанр буквой $p$. В самое последнее время буквы $p$ стали избегать, чтобы избежать смешения с характеристикой $p$ числового поля, и заменять её буквой $g$. Я предпочитаю пользоваться буквой $p$, введённой Вейерштрассом.

Когда мы говорим об измерении класса дивизоров, то должны иметь в виду число линейно независимых *целых* дивизоров, входящих в этот класс: в противном случае в каждом классе можно было бы найти сколько угодно линейно независимых дробных дивизоров. Но класс $\mathfrak{W}$ задан дробным дивизором. Поэтому нашей ближайшей задачей является нахождение числа линейно независимых целых дивизоров, лежащих в классе $\mathfrak{W}$.

Примем во внимание, что не все дивизоры класса $\mathfrak{W}$ соответствуют дифференциалам элементов поля $k(x, y)$. В самом деле, пусть задан элемент

$$z=\varphi(x, y)$$

поля $k(x, y)$, а также дифференциал $dx$ и пусть

$$z \approx \frac{U}{V}, \quad dx \approx \frac{Z_x}{X^2}.$$

Тогда

$$z \cdot dx \approx \frac{U \cdot Z_x}{V \cdot X^2}. \tag{6}$$

Здесь дивизор, стоящий в правой части, соответствует не дифференциалу какого-нибудь элемента поля $k(x, y)$, а дифференциалу интеграла

$$\int z \cdot dx = \int \varphi(x, y) \cdot dx. \tag{7}$$

Такого рода интегралы дали первый толчок к построению теории алгебраических функций. Они носят название *абелевых интегралов* в честь Абеля, который впервые предпринял их систематическое исследование.

Замечательно, что аналогия дивизоров класса $\mathfrak{W}$ с соответствующими им абелевыми интегралами имеет весьма глубокий характер: именно, оказывается, что знаменатель дивизора указывает, в каких точках соответствующий ему интеграл перестаёт иметь смысл, т. е. принимает бесконечное значение. В самом деле, если $P(x_0, y_0)$ есть точка, в которой ни $z$ ни $x$ не принимают бесконечных значений (т. е. простой дивизор $P$ не входит ни в $V$ ни в $X$), то дивизор (6) не содержит в знаменателе $P$; с другой стороны, в точке $P$ интеграл (7) конечен. Если в точке $P$ элемент $z$ принимает бесконечное значение (т. е. если простой дивизор $P$ входит в $V$), то дивизор (6) не содержит в знаменателе $P$ в том и только в том случае, если $P$ содержится также в $Z_x$, причём по крайней мере в той же степени (дивизоры $U$ и $V$ мы предполагаем взаимно простыми). Другими словами, это имеет место в случае, когда $V$ содержит $P$ не выше чем в $(\alpha - 1)$-й степени. Интеграл же (7) имеет смысл для точки $P$, в которой $x$ принимает конечное значение $x_0$, в том и только в том случае, если подинтегральная функция $z$ при приближении $x$ к значению $x_0$ стремится к бесконечности медленее, чем

$$\frac{1}{x - x_0}.$$

Это возможно только тогда, если $x - x_0$ делится на $P^\alpha$, $\alpha > 1$, причём в этом случае $z$ имеет право стремиться при $x \to x_0$ к бесконечности не быстрее, чем

$$(x - x_0)^{-\frac{\alpha - 1}{\alpha}};$$

это имеет место в том и только в том случае, если $V$ содержит $P$ не выше, чем в $(\alpha - 1)$-й степени.

Пусть теперь $x$ в точке $P$ обращается в бесконечность и пусть простой дивизор $P$ входит в $X$ в $\alpha$-й степени. Тогда $P$ не входит в дивизор (6) (после сокращения) тогда и только тогда, если $P$ входит в $U$ по крайней мере в $(\alpha+1)$-й степени (вспомним, что $P$ входит в $Z_\infty$ в $(\alpha-1)$-й степени). С другой стороны, интеграл (7) имеет при $x\to\infty$ смысл тогда и только тогда, если при $x\to\infty$ функция $z$ обращается в нуль быстрее, чем $\frac{1}{x}$, т. е. в нашем случае по крайней мере так же быстро, как

$$\left(\frac{1}{x}\right)^{\frac{\alpha+1}{\alpha}}.$$

Это означает, что $U$ содержит $P$ по крайней мере в $(\alpha+1)$-й степени.

Таким образом интеграл (7) остаётся всюду конечным в том и только в том случае, если соответствующий ему дивизор (6) есть целый дивизор. Интегралы поля $k(x, y)$, остающиеся всюду конечными, носят название *интегралов 1-го рода*. Из приведённых рассуждений вытекает

Теорема 34. *Число линейно независимых интегралов 1-го рода равно измерению класса дифференциалов* $\mathfrak{W}$.

## § 20. Измерение класса дифференциалов

Теорема 35. *Если элемент $z$ поля $k(x, y)$ делится на все простые дивизоры, входящие в числитель элемента $x-c$, то его след $S(z)$ относительно $x$ делится на $x-c$.*

Доказательство. В силу условия теоремы значения элемента $z$ во всех точках, в которых $x=c$, равны нулю. Отсюда следует, что уравнение

$$(1)\qquad z^n+b_1(x)\cdot z^{n-1}+\ldots+b_{n-1}(x)\cdot z+b_n(x)=0,$$

которому удовлетворяет $z$, при $x=0$ обращается в численное уравнение, все корни которого равны нулю, т. е. в $z^n=0$, откуда

$$b_i(c)=0 \qquad (i=1,\ 2,\ \ldots,\ n).$$

В частности,

$$S(z)=-b_1(x)$$

обращается при $x=c$ в нуль, откуда следует, что выражение $S(z)$ содержит в числителе множитель $x-c$, что требовалось доказать.

Имеет место также следующая теорема, в известном смысле обратная к теореме 35:

Теорема 36. *Пусть* $[\omega_1, \omega_2, \ldots, \omega_n]$ — *фундаментальный базис кольца* $\Omega$. *Если для элемента* $z$ *имеет место*

$$S(z \cdot \omega_i) \equiv 0 \ [\mathrm{mod}\,(x-c)] \qquad (i = 1, 2, \ldots, n), \tag{2}$$

*то* $z$ *делится на все простые дивизоры, входящие в* $x - c$.

Доказательство. Допустим противное: пусть $z$, например, не делится на простой дивизор $P_1$, где

$$P_1^{e_1} P_2^{e_2} \ldots P_s^{e_s}$$

есть числитель представления $x - c$ через дивизоры. Пусть $u$ есть целый элемент поля $k(x, y)$, делящийся на достаточно высокие степени простых дивизоров $P_2, P_3, \ldots, P_s$ (это требование связано с тем, что не исключена возможность, что представление элемента $z$ через дивизоры содержит $P_2, P_3, \ldots, P_s$ в знаменателе), но не делящийся на $P_1$. Тогда произведение $z \cdot u$ будет принимать в точках $P_2, P_3, \ldots, P_s$ значение нуль, а в точке $P_1$ — отличное от нуля значение, конечное или бесконечное. Если это бесконечное значение, то заставим $u$ делиться на такую степень простого дивизора $P_1$, чтобы произведение $z \cdot u$ и в точке $P_1$ не обращалось ни в нуль, ни в бесконечность.

Составим уравнение (с коэффициентами, рационально зависящими от $x$), которому удовлетворяет $z \cdot u$, и положим в его коэффициентах $x = c$. Это уравнение будет иметь только один отличный от нуля корень (возможно, высшей кратности), который определяет значение элемента $zu$ в точке $P_1$. Поэтому след $S(zu)$, равный взятому с обратным знаком коэффициенту при $(zu)^{n-1}$, не может при $x = c$ обращаться в нуль, откуда

$$S(zu) \not\equiv 0 \quad [\mathrm{mod}\,(x-c)]. \tag{3}$$

Представим $zu$ через базис $[\omega_1, \omega_2, \ldots, \omega_n]$:

$$zu = g_1\omega_1 + g_2\omega_2 + \ldots + g_n\omega_n,$$

где $g_i$ — рациональные функции от $x$, входящие в кольцо $\Omega_{x=c}$, т. е. не содержащие в знаменателях множителя $x - c$. Умножая сравнение (2) на $g_i$ и суммируя по $i$, получим

$$S(zu) \equiv 0 \ [\mathrm{mod}\,(x-c)],$$

что противоречит формуле (3). Теорема доказана.

*Примечание.* Доказательство справедливо также для полей характеристики $p$, за исключением случая, когда уравнение, которому удовлетворяет $zu$, при $x = c$ имеет ненулевой корень, кратность которого есть число, кратное $p$. Этого нельзя избежать в том случае, когда показатель $e_1$ делится на $p$.

Следствие. *Если элемент* $x - c$ *не делится на простые множители дивизора* $Z_x$, *то из* (2) *следует, что* $z$ *делится на* $x - c$.

В самом деле, в этом случае числитель представления элемента $x-c$ через дивизоры содержит простые дивизоры только в первых степенях. Поэтому делимость элемента $z$ на $P_1P_2\ldots P_s$ влечёт за собой его делимость на $x-c$.

**Теорема 37.** *Пусть опять* $[\omega_1, \omega_2, \ldots, \omega_n]$ *есть фундаментальный базис кольца* $\Omega$. *Чтобы элемент* $z$ *поля* $k(x, y)$ *при представлении через дивизоры содержал в знаменателе, кроме простых множителей дивизора* $X$ *в любых степенях, где*

$$x \equiv \frac{X_1}{X},$$

*только дивизор* $Z_x$ *или его делитель, необходимо и достаточно, чтобы все элементы*

$$S(z\omega_i) \qquad (i = 1, 2, \ldots, n)$$

*были полиномами от* $x$.

Доказательство. Пусть $c_1, c_2, \ldots, c_m$ — те из значений элемента $x$, принимаемых в точках, соответствующих простым множителям дивизора $Z_x$, в которых $x$ принимает конечные значения. Если $z$ удовлетворяет условиям теоремы, то произведение

$$v = z \cdot g(x) = z(x-c_1)(x-c_2)\ldots(x-c_m)$$

имеет в качестве представления дивизор, числитель которого делится на каждый из простых дивизоров $P$, входящих в $Z_x$, но не входящих в $X$ по крайней мере в $\alpha$-й степени, а знаменатель — не выше чем в $(\alpha-1)$-й степени, и после сокращения в числителе будет содержать $P$. Отсюда в силу теоремы 35 след $S(v)$ делится на каждый из множителей $x-c_1, x-c_2, \ldots, x-c_m$, т. е. на $g(x)$. То же имеет место относительно следов

$$S(v\omega_i) \qquad (i = 1, 2, \ldots, n).$$

Но

$$S(v\omega_i) = S(zg(x)\omega_i) = g(x) \cdot S(z\omega_i).$$

Отсюда следует, что функции $S(z\omega_i)$ не содержат в своих знаменателях множителей $x-c_1$, $x-c_2, \ldots, x-c_m$. Множители же типа $x-c$, где $c$ отлично от $c_1, c_2, \ldots, c_m$, тоже не могут содержаться в знаменателях выражений $S(v\omega_i)$, поскольку $v\omega_i$ представляются через дивизоры, в знаменателях которых содержатся только простые множители дивизора $X$. Таким образом функции $S(z\omega_i)$ являются полиномами от $x$, что требовалось доказать.

Обратно, пусть $S(z\omega_i)$ являются полиномами от $x$. Тогда из следствия к теореме 36 вытекает, что $z$ не содержит в знаменателе простых дивизоров, не входящих в $g(x)$. В самом деле, если бы существовал такого рода простой дивизор, который бы являлся

делителем линейного полинома $x-c$, то из сделанного предположения следовало бы

$$S[z(x-c)\omega_i] \equiv 0 \,[\mathrm{mod}\,(x-c)] \qquad (i=1, 2, \ldots, n),$$

и тогда в силу следствия $z(x-c)$ делилось бы на $x-c$.

Пусть теперь $P$ — простой дивизор, входящий в $x-c$ в $\alpha$-й и, следовательно, в $Z_x$ в $(\alpha-1)$-й степени. Из того, что $S(z\omega_i)$ являются полиномами, следует, что $S[zg(x)\omega_i]$ делятся на $g(x)$. Применяя теорему 36, мы убеждаемся, что $zg(x)$ делится на $P$. Но так как $g(x)$ точно делится на $P^\alpha$, то отсюда следует, что в представлении элемента $z$ через дивизоры простой дивизор $P$ входит в знаменателе не выше, чем в $(\alpha-1)$-й степени, т. е. не в более высокой степени, чем он входит в $Z_x$. Теорема доказана.

Поставим себе задачу найти все линейно независимые целые дивизоры класса дифференциалов $\mathfrak{W}$. Пусть $W$ — произвольный целый дивизор этого класса. Деля его на дивизор

$$\frac{Z_x}{X^2} \sim dx,$$

мы получим дивизор

$$u \sim \frac{WX^2}{Z_x}, \tag{4}$$

представляющий некоторый элемент $u$ поля $k(x, y)$, играющий роль подинтегральной функции интеграла 1-го рода. Элементы типа (4) могут быть охарактеризованы двумя следующими условиями:

1) $u$ содержит в знаменателе только простые множители дивизора $Z_x$, притом не в более высокой степени, чем $Z_x$.

2) $u$ содержит *в числителе* все простые дивизоры, входящие в $X$ (т. е. соответствующие точкам, в которых $x$ обращается в бесконечность). При этом если $X$ точно делится на $P^\varkappa$, то $u$ должно делиться по крайней мере на

$$P^{2\alpha-(\alpha-1)} = P^{\alpha+1}.$$

Другими словами, произведение $ux$ должно делиться на $P$.

Сначала найдём все элементы $u$, удовлетворяющие только условию 1). Из теоремы 37 следует, что это условие равносильно требованию, чтобы все элементы

$$S(u\omega_i) \qquad (i=1, 2, \ldots, n)$$

были полиномами от $x$. Это условие очень просто выражается, если мы введём так называемый *дополнительный базис*

$$[\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n],$$

определяемый при помощи равенств

$$S(\varepsilon_i\omega_j) = \delta_{ij} \qquad (i, j=1, 2, \ldots, n), \tag{5}$$

где $\delta_{ij}=0$ при $i\neq j$, а $\delta_{ii}=1$. Найдём явное выражение для дополнительного базиса. Пусть

$$\varepsilon_i = e_{i1}\omega_1 + e_{i2}\omega_2 + \ldots + e_{in}\omega_n \qquad (i=1, 2, \ldots, n),$$

где $e_{ij}$ — элементы поля $k(x)$. Умножая это равенство на $\omega_j$ $(j=1, 2, \ldots, n)$ и после этого применяя к нему оператор $S(\ldots)$, мы в силу (5) получим

$$e_{i1}S(\omega_1\omega_j) + e_{i2}S(\omega_2\omega_j) + \ldots + e_{in}S(\omega_n\omega_j) = \delta_{ij},$$

откуда при фиксированном $i$ можно определить $e_{i1}, e_{i2}, \ldots, e_{in}$. Определитель этой системы линейных уравнений есть дискриминант кольца $\Omega$, так что эти рассуждения имеют силу только в том случае, если этот дискриминант отличен от нуля, т. е. если $k(x, y):k(x)$ есть расширение 1-го рода.

Пусть

$$u = h_1\varepsilon_1 + h_2\varepsilon_2 + \ldots + h_n(\varepsilon_n) \tag{6}$$

есть выражение элемента $u$ через дополнительный базис. Умножая (6) на $\omega_i$ и применяя оператор $S(\ldots)$, мы в силу (5) будем иметь:

$$S(u\omega_i) = h_i \qquad (i=1, 2, \ldots, n). \tag{7}$$

Таким образом условие 1) равносильно требованию, чтобы все коэффициенты представления элемента $u$ через дополнительный базис были полиномами от $x$.

Обратимся теперь к условию 2). Это условие можно ещё формулировать так:

2′) $ux$ должно обращаться в нуль во всех точках, в которых $x$ обращается в бесконечность.

Выберем в качестве фундаментального базиса нормальный базис

$$[\lambda_1, \lambda_2, \ldots, \lambda_n]$$

и пусть дополнительным к нему базисом будет

$$[\mu_1, \mu_2, \ldots, \mu_n].$$

Если

$$u = h_1\varepsilon_1 + h_2\varepsilon_2 + \ldots + h_n\varepsilon_n, \tag{8}$$

то в силу (7)

$$h_i = S(u\lambda_i) \qquad (i=1, 2, \ldots, n). \tag{9}$$

Перейдём к базису

$$[\lambda_1', \lambda_2', \ldots, \lambda_n'], \tag{10}$$

где независимой переменной должна считаться

$$x_1 = \frac{1}{x}$$

и где

$$\lambda_i' = \lambda_i \cdot x^{-r_i} \qquad (i = 1, 2, \ldots, n).$$

Равенства (9) можно переписать так:

$$h_i x^{-(r_i-1)} = S(ux_i\lambda_i') \qquad (i = 1, 2, \ldots, n).$$

С другой стороны, условие 2') можно формулировать ещё так:

2'') Элемент $ux$ должен делиться на все простые дивизоры, входящие в числитель $X$ элемента

$$x_1 \cong \frac{X}{X_1}.$$

Применяя теорему 36 к кольцу $\mathfrak{Q}_1$ целых относительно $x_1$ элементов поля $k(x, y)$, для которого (10) служит фундаментальным базисом, мы видим, что для соблюдения условия 2'') необходимо и достаточно, чтобы элементы

$$h_i x^{-(r_i-1)} \qquad (i = 1, 2, \ldots, n),$$

рассматриваемые как функции от $x_1$, делились на $x_1$.

Другими словами, полиномы $h_i = h_i(x)$ должны быть более низкой степени, чем $x^{r_i-1}$, т. е. не выше $(r_i - 2)$-й степени. Но так как при $r_i \geqslant 2$ полином $(r_i - 2)$-й степени имеет $r_i - 1$ коэффициентов, то общее выражение (8) для элементов $u$, удовлетворяющих условиям 1) и 2'), содержит всего

$$(r_s - 1) + (r_{s+1} - 1) + \ldots + (r_n - 1)$$

линейно входящих произвольных коэффициентов, где

$$r_{s-1} = 1, \quad r_s \geqslant 2.$$

Мы можем переписать это выражение так:

$$(r_2 - 1) + (r_3 - 1) + \ldots + (r_n - 1), \tag{11}$$

так как $r_i \geqslant 1$ при $i > 1$. Это число, таким образом, равно измерению класса $\mathfrak{W}$.

В § 12 мы обозначили число

$$r_1 + r_2 + \ldots + r_n,$$

через $\frac{1}{2} w_x$. Пользуясь этим обозначением, мы можем представить выражение (11) так:

$$\frac{1}{2} w_x - n_x + 1.$$

Сравнивая это выражение с формулой (4) § 19, мы видим, что оно совпадает с выражением для жанра $\rho$ поля $k(x, y)$. Отличие состоит только в том, что в §§ 12 и 19 мы определили число $w_x$ по-разному.

Докажем, что оба эти числа совпадают. Для этого определим, в какой степени входит в дискриминант кольца $\Omega$ множитель $x-c$, делящийся на простой дивизор $P$, который мы предположим критическим, т. е. входящим в дивизор $Z_x$. Из условия 1) и формулы (6) следует, что дополнительный базис

$$[\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n] \tag{12}$$

является базисом для всех элементов поля $k(x, y)$, представления которых через дивизоры содержат в знаменателях, кроме делителей дивизора $X$, ещё дивизор $Z_x$ или его делитель. Построим элемент $z$, точно делящийся на $Z_x$ и, кроме того, содержащий в числителе и знаменателе своего представления простые дивизоры, не входящие в $Z_x$. Тогда все элементы базиса

$$\left[\frac{\omega_1}{z}, \frac{\omega_2}{z}, \ldots, \frac{\omega_n}{z}\right] \tag{13}$$

выражаются через базис (12) с коэффициентами из кольца $\Omega_{x=c}$, и обратно. Отсюда следует, что определитель подстановки $C$, выражающей базис (13) через базис (12), не содержит множителя $x-c$ ни в числителе, ни в знаменателе. С другой стороны, выразим элементы базиса

$$[\omega_1, \omega_2, \ldots, \omega_n] \tag{14}$$

через базис (13):

$$\begin{aligned}
\omega_1 &= b_{11}\frac{\omega_1}{z} + b_{12}\frac{\omega_2}{z} + \ldots + b_{1n}\frac{\omega_n}{z},\\
\omega_2 &= b_{21}\frac{\omega_1}{z} + b_{22}\frac{\omega_2}{z} + \ldots + b_{2n}\frac{\omega_n}{z},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\omega_n &= b_{n1}\frac{\omega_1}{z} + b_{n2}\frac{\omega_2}{z} + \ldots + b_{nn}\frac{\omega_n}{z}.
\end{aligned}$$

После исключения $\omega_1, \omega_2, \ldots, \omega_n$ мы получим уравнение

$$\begin{vmatrix}
b_{11}-z, & b_{12}, & \ldots, & b_{1n}\\
b_{21}, & b_{22}-z, & \ldots, & b_{2n}\\
\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots\\
b_{n1}, & b_{n2}, & \ldots, & b_{nn}-z
\end{vmatrix} = 0,$$

откуда следует, что

$$|B| = \begin{vmatrix}
b_{11}, & b_{12}, & \ldots, & b_{1n}\\
b_{21}, & b_{22}, & \ldots, & b_{2n}\\
\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots\\
b_{n1}, & b_{n2}, & \ldots, & b_{nn}
\end{vmatrix} = N(z).$$

Но норма $N(z)$, в силу определения элемента $z$, делится точно на

$$(x-c)^{(\alpha_1-1)+(\alpha_2-1)+\ldots+(\alpha_s-1)},$$

где

$$x-c \equiv \frac{P_1^{\alpha_1}\cdot P_2^{\alpha_2}\ldots P_s^{\alpha_s}}{X}.$$

Пользуясь формулой (16) § 6, получим:

$$\Delta[\omega_1,\omega_2,\ldots,\omega_n]=|B|^2\cdot\Delta\left[\frac{\omega_1}{z},\frac{\omega_2}{z},\ldots,\frac{\omega_n}{z}\right]= \tag{15}$$

$$=|B|^2\cdot|C|^2\cdot\Delta|\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n|.$$

Теперь выразим дополнительный базис (12) через фундаментальный базис (14). Мы имели

$$\varepsilon_i=e_{i1}\omega_1+e_{i2}\omega_2+\ldots+e_{in}\omega_n \qquad (i=1,2,\ldots,n), \tag{15'}$$

где

$$e_{i1}S(\omega_1\omega_j)+e_{i2}S(\omega_2\omega_j)+\ldots+e_{in}S(\omega_n\omega_j)= \tag{15''}$$

$$=\delta_{ij}\,(i,\ j=1,2,\ldots,n),$$

откуда

$$|\varepsilon|\cdot\Delta[\omega_1,\omega_2,\ldots,\omega_n]=\begin{vmatrix} e_{11}, & e_{12}, & \ldots, & e_{1n}\\ e_{21}, & e_{22}, & \ldots, & e_{2n}\\ \ldots & \ldots & \ldots & \ldots\\ e_{n1}, & e_{n2}, & \ldots, & e_{nn}\end{vmatrix}\times$$

$$\times\begin{vmatrix} S(\omega_1^2), & S(\omega_1\omega_2), & \ldots, & S(\omega_1\omega_n)\\ S(\omega_2\omega_1), & S(\omega_2^2), & \ldots, & S(\omega_2\omega_n)\\ \ldots & \ldots & \ldots & \ldots\\ S(\omega_n\omega_1), & S(\omega_n\omega_2), & \ldots, & S(\omega_n^2)\end{vmatrix}=\begin{vmatrix} 1, & 0, & \ldots, & 0\\ 0, & 1, & \ldots, & 0\\ \ldots & \ldots & \ldots & \ldots\\ 0, & 0, & \ldots, & 1\end{vmatrix}=1.$$

Но так как

$$\Delta[\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n]=|\varepsilon|^2\cdot\Delta[\omega_1,\omega_2,\ldots,\omega_n],$$

то

$$\Delta[\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n]=\frac{1}{\Delta[\omega_1,\omega_2,\ldots,\omega_n]}. \tag{16}$$

Подставляя этот результат в формулу (15), получим

$$\Delta[\omega_1,\omega_2,\ldots,\omega_n]=\pm|B|\cdot|C|=\pm N(z)\cdot|C|,$$

откуда следует, что

$$\Delta[\omega_1,\omega_2,\ldots,\omega_n] \tag{17}$$

точно делится на

$$(x-c)^{(\alpha_1-1)+(\alpha_2-1)+\ldots+(\alpha_s-1)}.$$

Применим это рассуждение к каждому элементу $x-c$, простые дивизоры которого входят в $Z_x$. Мы убедимся, что дискриминант (17) делится на полином, степень которого равна числу простых дивизоров, входящих в $Z_x$ и соответствующих точкам, в которых элемент $x$ принимает конечные значения (другими словами, тех, которые не входят в дивизор $X$). Других делителей полином (17) иметь не может. В самом деле, пусть $x-c$ делится только на первые степени простых дивизоров. Тогда $z=1$, $N(z)=1$, откуда следует, что (17) есть единица кольца $\Omega_{x=c}$.

Подобным же образом, сделав преобразование

$$x=\frac{1}{x_1},$$

мы увидим, что

$$\Delta[\lambda_1', \lambda_2', \ldots, \lambda_n'] \tag{18}$$

точно делится на

$$x_1^{(\gamma_1-1)+(\gamma_2-1)+\cdots+(\gamma_s-1)},$$

где

$$X=P_1'^{\gamma_1}\cdot P_2'^{\gamma_2}, \ldots, P_s'^{\gamma_s}.$$

Это показывает, что порядок дивизора $Z_x$, т. е. $w_x$, равен сумме степени $\delta$ полинома (17) и числа $\delta_0$ нулевых корней полинома (18) относительно $x_1$. Сопоставляя этот результат с формулой (14) § 12, мы получим:

$$w_x=2(r_1+r_2+\ldots+r_n). \tag{19}$$

Отсюда, пользуясь выражением (11) для величины измерения класса $\mathfrak{W}$ и принимая во внимание, что $r_1=0$, будем иметь

$$\text{Изм } \mathfrak{W}=\frac{w_x}{2}-n_x+1,$$

или в силу формулы (4) § 19:

$$\text{Изм } \mathfrak{W}=p. \tag{20}$$

Вместе с тем формула (5) § 19 даёт для порядка класса $\mathfrak{W}$ выражение

$$\text{Пор } \mathfrak{W}=2p-2. \tag{21}$$

Итак:

Теорема 38. *Класс дифференциалов $\mathfrak{W}$ имеет порядок $2p-2$ и измерение $p$.*

Класс $\mathfrak{W}$ замечателен тем, что он не зависит от выбора переменных. Он играет фундаментальную роль при подсчётах измерений других классов (теорема Римана-Роха).

При аналитическом и географическом изложениях теории алгебраических функций теорема о числе линейно независимых интегралов

первого рода доказывается с большим трудом: в аналитическом изложении её доказательство опирается на проблему Дирихле на многолистных поверхностях (метод Неймана), а в геометрическом изложении вопрос приводится к нахождению числа линейно независимых кривых

$$\varphi(x, y) = 0 \tag{22}$$

$(n-3)$-й степени, которые должны проходить через все особые точки кривой

$$f(x, y) = 0. \tag{23}$$

Однако если кривая (23) имеет особые точки высших порядков, то точное определение «прохождения» через них кривой (22) встречает большие трудности. Обычно преобразовывают кривую (23) в другую, имеющую только простые особые точки. Нахождение такого рода преобразования тоже достаточно сложно. После производства такого преобразования все интегралы 1-го рода могут быть выражены в форме

$$\int \frac{\varphi(x, y)}{f_y(x, y)}\, dx.$$

## § 21. Зависимость жанра от числового поля

В предыдущих исследованиях (кроме § 15) мы поступали так, как если бы числовое поле $k$ было алгебраически замкнутым. Говоря точнее, мы при изучении отдельных дивизоров и классов присоединяли к полю $k$ иррациональности, которые были необходимы для полного разложения дивизоров на простые дивизоры, соответствующие точкам, т. е. имеющие вес 1. Возникает вопрос, в какой мере такое присоединение оставляет неизменными свойства поля $k(x, y)$. Именно, ясно, что не всякий класс дивизоров, определённых в расширенном числовом поле $k_1$, существует в первоначальном поле $k(x, y)$. Но если в классе, определённом в поле $k_1(x, y)$, существует дивизор, лежащий в поле $k(x, y)$, то можем ли мы заключить, что измерение этого класса не зависит от того, рассматривается ли он в поле $k(x, y)$ или в поле $k_1(x, y)$? Этот вопрос будет решён окончательно лишь после того, как мы познакомимся с теоремой Римана-Роха. Здесь же мы ограничимся решением этого вопроса для класса дифференциалов $\mathfrak{W}$. В предыдущем параграфе, в котором мы не пользовались замкнутостью поля $k$, мы нашли, что измерение класса $\mathfrak{W}$ равно

$$\rho = (r_2 - 1) + (r_3 - 1) + \ldots + (r_n - 1), \tag{1}$$

где $r_i$ есть целый показатель $i$-го члена $\lambda_i$ нормального базиса. Вспомним, что $\lambda_i$ есть элемент поля $k(x, y)$ [или $k_1(x, y)$] возможно меньшего порядка, не представимый в форме

$$c_1\lambda_1 + c_2\lambda_2 + \ldots + c_{i-1}\lambda_{i-1}.$$

A priori не исключена возможность того, что элемент $\lambda_i$ показателя $r_i$, найденный в поле $k_1(x, y)$, не лежит в поле $k(x, y)$, и $i$-й

член нормального базиса для поля $k(x, y)$ уже будет иметь более высокий порядок. Это будет свидетельствовать о том, что с расширением числового поля жанр будет *понижаться*.

С другой стороны, вспомним, что нормальный базис является фундаментальным базисом кольца $\Omega$. Наложим на поле $k$ ограничение, состоящее в том, что мы предположим, что при расширении поля $k$ степень $n$ не изменяется. Это значит, что определяющее поле $k(x, y)$ неприводимое уравнение не сделается приводимым при расширениях поля $k$, т. е., как принято говорить, *абсолютно неприводимо*. Тогда при расширении поля $k$ с расширением числового поля и сопутствующем ему понижении жанра уменьшится и величина

$$w_\varpi = 2\rho - 2 + 2n,$$

которая, как мы убедились в § 12, равна $\delta + \delta_0$ степени дискриминанта кольца $\Omega$ и числа нулевых корней дискриминанта кольца $\Omega_1$. Но можно подобрать такое дробное линейное преобразование

$$x \longrightarrow \frac{ax + b}{cx + d},$$

чтобы число $\delta_0$ обратилось в нуль. Тогда при понижении жанра снизится и степень дискриминанта фундаментального базиса, откуда будет следовать, что фундаментальный базис для числового поля $k$ уже не является фундаментальным базисом при расширенном числовом поле. Исследуем, возможно ли это. Рассмотрим сначала случай полей характеристики нуль.

Вернёмся к рассуждениям § 11. Пусть существует целый элемент

$$w = \frac{\omega_1}{h(x)} + b_2(x)\,\omega_2 + \ldots + b_n(x) \cdot \omega_n,$$

где полином $h(x)$ и дробные функции $b_2(x), \ldots, b_n(x)$ содержат коэффициенты расширенного числового поля $k_1$ *).

Пусть элемент $\xi$ поля $k_1$ есть корень неприводимого в поле $k$ уравнения

$$\varphi(t) = 0.$$

Назовём сумму всех корней этого уравнения *арифметическим следом* от $\xi$ и будем обозначать её символом

$$S_\tau(\xi) \subset k.$$

Аналогично определим арифметический след от элемента поля $k_1(x)$.

Пусть

$$h(0) = \alpha.$$

Тогда

$$S_\tau(\alpha w) = S_\tau\left[\frac{\alpha}{h(x)}\right]\omega_1 + S_\tau[\alpha b_2(x)]\,\omega_2 + \ldots + S_\tau[\alpha b_n(x)]\omega_n$$

*) Выбор элемента базиса (в данном случае $\omega_1$) не играет никакой роли.

есть целая функция от $x$, и в то же время коэффициенты входящих сюда элементов поля $k_1(x)$ лежат в $k$. Коэффициент

$$S_\tau\left[\frac{\alpha}{h(x)}\right]$$

не обращается в нуль, так как при $x=0$ он обращается в сумму единиц. Он не может быть полиномом от $x$, так как после приведения к общему знаменателю степень его числителя ниже, чем степень знаменателя.

Это рассуждение показывает: если $[\omega_1, \omega_2, \ldots, \omega_n]$ не есть фундаментальный базис при числовом поле $k_1$, то он не может быть фундаментальным базисом и при первоначальном числовом поле $k$. Это показывает, что при том ограничении, которое мы наложили на поле $k$, *жанр поля $k(x, y)$ не может снижаться ни при каких расширениях числового поля.*

Видоизменяя эти рассуждения, легко убедиться в справедливости выводов для случая, когда $k(x, y) : k(x)$ есть расширение 1-го рода. В самом деле, в этом случае мы повторим те же рассуждения, но только в роли $\alpha$ будем брать не $h(0)$, а испытаем в этой роли все целые элементы поля $k_1$. Докажем, что в этом случае коэффициенты

$$S_\tau\left[\frac{\alpha}{h(x)}\right]$$

не могут все быть равны нулю. Если бы для всех целых $\alpha \subset k^1$ имело место

$$S_\tau\left[\frac{\alpha}{h(x)}\right]=0,$$

то, беря в роли $\alpha$ последовательно все коэффициенты полинома $h(x)$, умноженные на каждый элемент фундаментального базиса поля $k_1 : k$, мы бы получили

$$S_\tau(\beta)=0$$

при всех целых $\beta \subset k_1$. Отсюда, в частности,

$$S_\tau(\omega_i\omega_j)=0,$$

если $[\omega_1, \omega_2, \ldots, \omega_r)$ — фундаментальный базис поля $k_1 : k$. Но в этом случае дискриминант расширения $k_1 : k$ равен нулю, откуда следует, что $k_1 : k$ есть расширение 2-го рода.

Если $k(x, y) : k(x)$ есть расширение 2-го рода, наши рассуждения теряют силу, уже хотя бы потому, что тогда дискриминант фундаментального базиса равен нулю. Мы уже упоминали, что в этом случае мы должны в роли класса $\mathfrak{B}$ взять класс дифференциалов поля $k(x^{p^r}, y^{p^s})$, где

$$\xi = x^{p^r}, \quad \eta = y^{p^s}$$

связаны соотношением, в котором $\xi$ и $\eta$ явно входят в степенях, не все показатели которых делятся на $p$. Заметим, что поле $k(x,y)$ изоморфно с полем $k(\xi,\eta)$, если мы присоединим к числовому полю $k$ $p^r$-е и $p^s$-е корни из его элементов.

Интересен вопрос, что произойдёт с жанром поля $k(x,y)$, если заменим связанные с ним равенства сравнениями по простому модулю $p$. Можно ожидать, что при этом жанр не будет оставаться неизменным. Не разбирая этого вопроса, докажем, что существует лишь конечное число простых чисел $p$ такого рода, что абсолютно неприводимому уравнению

$$f(x,y)=0 \tag{2}$$

с целыми рациональными коэффициентами будет соответствовать приводимое сравнение

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

Чтобы убедиться в этом, будем считать коэффициенты полинома $f(x,y)$ неопределёнными переменными и определим те соотношения, которым они должны удовлетворять для того, чтобы $f(x,y)$ разлагался на множители. Для этого зададимся степенями множителей, на которые должен разлагаться $f(x,y)$:

$$f(x,y)=g(x,y)\cdot h(x,y), \tag{4}$$

и будем считать коэффициенты полиномов $g(x,y)$ и $h(x,y)$ тоже переменными параметрами $u_{\mu,\nu}$, $v_{\mu,\nu}$. Из тождества (4) мы получим выражение коэффициентов $a_{\mu,\nu}$ полинома $f(x,y)$ в виде однородно квадратичных полиномов относительно $u_{\mu,\nu}$, $v_{\mu,\nu}$. Исключив из этих выражений параметры $u_{\mu,\nu}$, $v_{\mu,\nu}$, мы получим несколько соотношений между $a_{\mu,\nu}$, которые должны существовать, так как в противном случае при любых $a_{\mu,\nu}$ их упомянутое представление и, значит, разложение (4) было бы возможно, что противоречит абсолютной неприводимости полинома $f(x,y)$. Пусть

$$\Phi_i(a_{11},\ldots,a_{nn})=0 \qquad (i=1,2,\ldots,s) \tag{5}$$

будут эти соотношения, соблюдение которых необходимо и достаточно для того, чтобы полином $f(x,y)$ разлагался на множители заданных степеней. Для полинома $f(x,y)$, который у нас задан численно, хотя бы одно из соотношений (5) не должно удовлетворяться. Подставив в левые части (5) значения $a_{\mu,\nu}$, которые мы предполагаем целыми рациональными или целыми алгебраическими числами, мы получим целые числа $\Phi_i$. Чтобы сравнение (3) разлагалось указанным образом, необходимо и достаточно, чтобы простое число $p$ было общим делителем всех $\Phi_i$. Таких простых общих делителей, очевидно, конечное число. Меняя предположения относительно степеней полиномов $g(x,y)$, $h(x,y)$, мы получим конечное число систем типа (5). Чтобы сравнение (3) было приводимо вообще, необходимо

и достаточно, чтобы $p$ было делителем всех $\Phi_i$, соответствующих какой-либо из конечного числа систем (5). Таких простых чисел — конечное число.

Теория классов дивизоров в незамкнутых числовых полях, и в первую очередь в поле рациональных чисел, в последние годы стала привлекать внимание математиков потому, что она тесно связана с вопросом о рациональных решениях неопределённого уравнения (2) (в предположении, что его коэффициенты рациональны), которое является самым общим неопределённым уравнением с двумя переменными. В настоящее время общих результатов по этому вопросу почти не существует. Можно указать только следующие важные работы:

1) Работу Морделла (L. J. Mordell) [73] об уравнениях типа (2), для которого жанр $\rho = 1$ (так называемые эллиптические кривые). Известно, что эллиптические кривые допускают параметрическое представление

$$x = g(u), \quad y = h(x),$$

где правые части представляют собой эллиптические функции, которые однозначны, трансцендентны и двояко периодичны. Для них имеет место *теорема сложения*

$$g(u+v) = R[g(u),\ h(u),\ g(v),\ h(v)],$$
$$h(u+v) = S[g(u),\ h(u),\ g(v),\ h(v)],$$

где $R(\ldots)$ и $S(\ldots)$ — некоторые рациональные функции от четырёх аргументов. Предположим, что их коэффициенты рациональны. Пусть $u$ и $v$ взяты так, что соответствующие им значения $x, y$ рациональны. Тогда из теоремы сложения следует, что значения

$$g(u+v), \quad h(u+v)$$

тоже рациональны. Таким образом из двух пар чисел $x$, $y$, удовлетворяющих уравнению (2), можно получить бесчисленное множество пар рациональных решений этого уравнения.

Морделл доказал, что уравнение (2) имеет лишь конечное число таких «основных» рациональных решений, что все остальные рациональные решения уравнения (2) смогут быть получены из основных при помощи теоремы сложения.

2) Работу Вейля (A. Weil) [108], в которой обобщён результат Морделла на случай произвольного жанра $\rho \geqslant 1$. Обобщая понятие рациональной точки, Вейль рассмотрел «рациональные системы $\rho$ точек», т. е. дивизоры веса $\rho$, лежащие в поле рациональных чисел (или в фиксированном поле алгебраических чисел конечной степени). Он доказал существование конечного числа «основных» рациональных систем, из которых могут быть получены все рациональные системы при помощи теоремы сложения, которая имеет место также для высших трансцендентных функций ($\vartheta$-функций), связанных с уравнением (2) жанра $\rho > 1$.

3) Работу Зигеля (C. Siegel) [98], который доказал, что при $\rho \geqslant 1$ уравнение (2) имеет лишь конечное число целых рациональных решений.

В своей цитированной работе Вейль высказывает гипотезу, что при $\rho > 1$ уравнение (2) имеет лишь конечное число рациональных решений. При этом он говорит, что для решения этого вопроса в настоящее время мы не имеем достаточно разработанной теории.

Заслуживает также изучения случай, когда $k$ есть поле вещественных чисел. В этом направлении известен следующий результат Гарнака (A. Harnack) [42]:

Если соотношение (2) приводит к полю $k(x, y)$ жанра $\rho$, то кривая (2) на вещественной плоскости состоит не более чем из $\rho + 1$ непрерывных кусков.

Отсюда понятно название *уникурсальной кривой*, присвоенное кривой жанра нуль.

Гильберт (D. Hilbert) [53] и И. Г. Петровский [81] получили в этом направлении некоторые дальнейшие результаты.

## Упражнения к главе III

1. Пусть $k(x, y)$ — поле, заданное соотношением

$$y^2 - f(x) = 0,$$

где $f(x)$ — полином степени $n$, лишённый кратных корней. Такое поле называется *гиперэллиптическим*. Исследуя дискриминант кольца $\Omega$ в поле $k(x)$, доказать, что жанр поля $k(x, y)$ равен $\frac{n-1}{2}$, если $n$ — нечётное число, и равен $\frac{n-2}{2}$, если $n$ — чётное число. Найти $\rho$ линейно независимых интегралов 1-го рода.

2. Пусть поле $k(x, y)$ задано соотношением

$$y^3 - f(x) \cdot [g(x)]^2 = 0,$$

где $f(x)$, $g(x)$ — полиномы степеней $m$, $n$, взаимно простые и лишённые кратных корней. Доказать, что в этом поле все интегралы 1-го рода могут быть представлены в форме

$$\int \frac{\varphi(x)\,dx}{\sqrt[3]{f(x) \cdot [g(x)]^2}} + \int \frac{\psi(x)\,dx}{\sqrt[3]{[f(x)]^2 \cdot g(x)}},$$

где $\varphi(x)$, $\psi(x)$ — полиномы. Определить границы допустимых степеней этих полиномов и при их помощи определить жанр поля $k(x, y)$.

3. Определить жанр поля $k(x, y)$, заданного соотношением

$$x^n + y^n = 1.$$

ГЛАВА IV

# ТЕОРЕМА РИМАНА-РОХА И ЕЁ ПРИЛОЖЕНИЯ

## § 22. Теорема Римана-Роха

Условимся называть *специальным классом* (или классом 1-го рода) класс $\mathfrak{A}$ дивизоров, в котором содержится хотя бы один дивизор $A$, являющийся делителем какого-нибудь дивизора из класса дифференциалов $\mathfrak{W}$. В этом случае любой другой дивизор из класса обладает тем же свойством. В самом деле, если класс $\mathfrak{W}$ содержит дивизор $A \cdot B$,

где $$A \subset \mathfrak{A},$$

и если $A'$ — любой другой дивизор класса $\mathfrak{A}$, то дивизор $A'B$ тоже лежит в классе $\mathfrak{W}$.

Чтобы узнать, является ли $\mathfrak{A}$ специальным классом, возьмём в нём дивизор

$$A = P_1 \cdot P_2 \ldots P_k$$

и определим в классе $\mathfrak{W}$ все дивизоры, делящиеся на $P_1$; все эти дивизоры могут быть представлены в форме

$$P_1 \cdot V,$$

где дивизоры $V$ образуют класс $\mathfrak{W}_1$ измерения $\geqslant p-1$ (см. § 16). Далее, найдём в классе $\mathfrak{W}_1$ дивизоры, делящиеся на $P_2$; они имеют вид $P_2V$, где $V$ пробегает все дивизоры нового класса $\mathfrak{W}_2$, имеющего измерение $\geqslant p-2$. Таким путём мы получим систему классов

(1) $$\mathfrak{W}_1, \mathfrak{W}_2, \ldots, \mathfrak{W}_k,$$

порядки которых соответственно равны

$$2p-3,\ 2p-4,\ \ldots,\ 2p-k-2,$$

а измерения — не меньшие, чем, соответственно, числа

$$p-1,\ p-2,\ \ldots,\ p-k.$$

Если при этом измерение класса $\mathfrak{W}_k$ (и, следовательно, всех предыдущих классов) окажется положительным, то это будет означать, что

в классе $\mathfrak{W}_k$ будет содержаться целый дивизор $V$, откуда будет следовать, что в классе $\mathfrak{W}$ содержится дивизор

$$P_1 \cdot P_2 \ldots P_k V = A \cdot V.$$

Это и будет признаком того, что $\mathfrak{A}$ есть специальный класс.

Может, однако, случиться, что процесс образования классов прервётся ещё ранее $\mathfrak{W}_k$. Именно, класс $\mathfrak{W}_i (i < k)$ окажется измерения 1; тогда он будет содержать один единственный дивизор. Если при этом окажется, что последний делится на дивизор

$$P_{i+1} \cdot P_{i+2} \ldots P_k, \tag{2}$$

то класс $\mathfrak{A}$ всё-таки будет специальным; но если этот дивизор не делится на дивизор (2), то это будет признаком того, что $\mathfrak{W}$ не содержит дивизора, делящегося на $A$, так что класс $\mathfrak{A}$ будет неспециальным (или классом второго рода).

ТЕОРЕМА 39. *Если* Пор $\mathfrak{A} \leqslant p-1$, *то* $\mathfrak{A}$ *есть специальный класс.*

В самом деле, задерживая в классе $\mathfrak{W}$ $p-1$ точек (произвольных) $P_1, P_2, \ldots, P_{p-1}$, т. е. отыскивая в классе $\mathfrak{W}$ дивизоры, делящиеся на

$$P_1 \cdot P_2 \ldots P_{p-1},$$

мы придём к классу $\mathfrak{W}_{p-1}$ измерения

$$\geqslant p-(p-1) = 1.$$

ТЕОРЕМА 40. *Если* Пор $\mathfrak{A} > 2p-2$, *то* $\mathfrak{A}$ *есть неспециальный класс.*

В самом деле, в этом случае

$$\text{Пор } \mathfrak{A} > \text{Пор } \mathfrak{W},$$

а потому класс $\mathfrak{W}$ не может содержать дивизора, делящегося на какой-нибудь дивизор класса $\mathfrak{A}$.

В этом рассуждении не существенно, что в качестве $\mathfrak{W}$ мы взяли класс дифференциалов. Пусть даны два произвольных класса $\mathfrak{A}$, $\mathfrak{B}$, причём

$$\text{Пор } \mathfrak{A} > \text{Пор } \mathfrak{B}.$$

В том случае, если в классе $\mathfrak{A}$ содержатся дивизоры, делящиеся на какой-нибудь дивизор класса $\mathfrak{B}$, будем говорить, что *класс* $\mathfrak{A}$ *делится на класс* $\mathfrak{B}$.

Если класс $\mathfrak{A}$ делится на класс $\mathfrak{B}$, введём понятие их частного $\frac{\mathfrak{A}}{\mathfrak{B}}$. Для этого выделим в «делителе» $\mathfrak{B}$ какой-нибудь дивизор $B$ и найдём в классе $\mathfrak{A}$ все дивизоры, делящиеся на $B$. Пусть они образуют семейство

$$B\mathfrak{C},$$

где $\mathfrak{C}$ есть новый класс дивизоров. Класс $\mathfrak{C}$ не зависит от выбора дивизора $B$ внутри класса $\mathfrak{B}$. В самом деле, возьмём из класса $\mathfrak{B}$ какой-нибудь другой дивизор, например $B'$, где

$$B' \sim B, \tag{3}$$

и пусть $C$ будет какой-нибудь дивизор класса $\mathfrak{C}$:

$$C \subset \mathfrak{C}.$$

Тогда

$$BC \subset \mathfrak{A}.$$

Но из (3) следует

$$B'C \sim BC,$$

откуда вытекает, что каждый дивизор класса $\mathfrak{C}$ будет получен, если мы будем отыскивать все дивизоры класса $\mathfrak{A}$, делящиеся не на $B$, а на $B'$. Построенный таким образом класс $\mathfrak{C}$, который однозначно определяется заданием классов $\mathfrak{A}$ и $\mathfrak{B}$, мы будем называть *частным классов* $\mathfrak{A}$ и $\mathfrak{B}$ и обозначать символом

$$\frac{\mathfrak{A}}{\mathfrak{B}}.$$

Для порядка и измерения класса $\frac{\mathfrak{A}}{\mathfrak{B}}$ имеют место следующие легко выводимые соотношения:

$$\text{Пор } \frac{\mathfrak{A}}{\mathfrak{B}} = \text{Пор } \mathfrak{A} - \text{Пор } \mathfrak{B}, \tag{4}$$

$$\text{Изм } \frac{\mathfrak{A}}{\mathfrak{B}} \geqslant \text{Изм } \mathfrak{A} - \text{Пор } \mathfrak{B}. \tag{5}$$

Теорема Римана-Роха устанавливает связь между измерением произвольного класса $\mathfrak{A}$ и частного

$$\frac{\mathfrak{W}}{\mathfrak{A}},$$

которое носит название класса, *дополнительного* к $\mathfrak{A}$. В частности, если $\mathfrak{A}$ есть неспециальный класс, класс $\frac{\mathfrak{W}}{\mathfrak{A}}$ не содержит целых дивизоров, тогда мы будем полагать:

$$\text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}} = 0.$$

Возьмём произвольный *собственный* класс $\mathfrak{A}$ порядка

$$n = \text{Пор } \mathfrak{A}$$

и измерения

$$\text{Изм } \mathfrak{A} \geqslant 2.$$

Возьмём в нём два произвольных взаимно простых дивизора $A$, $A'$ и выберем в качестве «независимой переменной» элемент

$$x \asymp \frac{A'}{A}.$$

Далее, возьмём в том же классе $\mathfrak{A}$ совершенно произвольный дивизор $A''$ и введём обозначение

$$z \asymp \frac{A''}{A}.$$

В силу теоремы 31 $z$ есть целый элемент относительно $x$. С другой стороны,

$$z : x \asymp \frac{A''}{A'},$$

а это показывает в силу той же теоремы 31, что $z : x$ есть целый элемент относительно элемента

$$x_1 = \frac{1}{x} \asymp \frac{A}{A'}.$$

Отсюда следует, что (целый) показатель элемента $z$ относительно $x$ не превышает единицы.

Обратно, если $z$ есть какой-нибудь целый относительно $x$ элемент показателя $\leqslant 1$, то его можно представить в виде

$$z \asymp \frac{V}{A^k},$$

где $k$ есть достаточно большой показатель. Отсюда

$$z : x \asymp \frac{V}{A^{k-1} \cdot A'}.$$

Но так как в силу условия элемент $z : x$ должен быть целым относительно $x_1$, т. е. содержать в знаменателе только простые дивизоры, входящие в $A'$, в то время как дивизор $A$ взаимно прост с $A'$, то дивизор $V$ должен делиться на $A^{k-1}$. Пусть

$$V = A^{k-1} \cdot A'',$$

где $A''$ — целый дивизор. Тогда

$$z \asymp \frac{A''}{A}.$$

Таким образом класс $\mathfrak{A}$ содержит столько линейно независимых дивизоров, сколько существует линейно независимых целых относительно $x$ элементов показателя $\leqslant 1$.

Пусть

$$[\lambda_1, \lambda_2, \ldots, \lambda_n]$$

есть нормальный базис кольца $\mathfrak{Q}$, у которого

$$r_s \leqslant 1, \quad r_{s+1} > 1.$$

Тогда любой элемент поля $k(x, y)$, целый относительно $x$ и имеющий показатель $\leqslant 1$, может быть представлен в форме

$$z = c_1(x)\lambda_1 + c_2(x)\cdot\lambda_2 + \ldots + c_s(x)\cdot\lambda_s,$$

где $c_i(x)$ — полиномы, или ещё так:

$$z = c_1\lambda_1 + c_2\lambda_2 + \ldots + c_s\lambda_s + x\cdot u,$$

где $c_1, c_2, \ldots, c_s$ — константы, а $u$ — некоторый целый относительно $x$ элемент. Но, поскольку $z$, $\lambda_1, \ldots, \lambda_s$ имеют показатель $\leqslant 1$, это же имеет место относительно $x\cdot u$, откуда следует, что $u$ имеет показатель $\leqslant 0$, т. е. есть константа. Итак,

$$z = c_1\lambda_1 + c_2\lambda_2 + \ldots + c_s\lambda_s + c_0 x,$$

так что

$$\text{Изм } A = s + 1. \tag{6}$$

Здесь $s \leqslant n$. В случае, когда $s = n$, все $r_i$ должны быть $\leqslant 1$, откуда

$$\rho = (r_2 - 1) + (r_3 - 1) + \ldots + (r_n - 1) = 0.$$

В этом случае измерение класса $\mathfrak{A}$ равно $n + 1$, а потому, задерживая в нём $n - 1$ точек, мы придём к классу порядка

$$n - (n - 1) = 1$$

и измерения

$$z \geqslant (n + 1) - (n - 1) = 2.$$

Это означает, что в поле $k(x, y)$ существует элемент $t$ порядка 1. Тогда все элементы поля $k(x, y)$ будут связаны с элементом $t$ соотношениями, в которых они входят в первой степени (см. теорему 29), т. е. будут рационально выражаться через $t$. Итак, в случае $\rho = 0$ поле $k(x, y)$ изоморфно с полем рациональных функций одной переменной.

Пусть для какого-нибудь $i$ имеет место

$$r_i > 2.$$

Тогда элементы

$$h_i(x)\cdot\mu_i,$$

где $\mu_i$ — $l$-й элемент дополнительного базиса, а $h_i(x)$ — полином степени $\leqslant r_i - 2$, представляются через дивизоры вида

$$\frac{W\cdot A^z}{z_x},$$

где

$$W \subset \mathfrak{B}$$

[см. § 20, формулу (6)]. В частности, пусть

$$\mu_i \asymp \frac{W_1 A^2}{z_x}, \quad \mu_i x \asymp \frac{W_2 A^2}{z_x},$$

где

$$W_1 \subset \mathfrak{W}, \quad W_2 \subset \mathfrak{W}.$$

Отсюда

$$x \asymp \frac{A'}{A} \asymp \frac{W_2}{W_1}.$$

Но так как $A$ и $A'$ взаимно просты, то отсюда следует, что $W_1$ делится на $A$, а $W_2$ делится на $A'$, так что класс $\mathfrak{A}$ есть специальный класс.

Предположим, что $\mathfrak{A}$ неспециальный класс. Тогда, в силу только что сказанного, для всех $i$ мы имеем:

$$r_i \leqslant 2.$$

Пусть

$$r_2 = r_3 = \ldots = r_s = 1, \quad r_{s+1} = r_{s+2} = \ldots = r_n = 2.$$

Тогда

$$\rho = (r_2 - 1) + \ldots + (r_s - 1) + (r_{s+1} - 1) + \ldots + (r_n - 1) = n - s$$

Сопоставляя полученную формулу с формулой (6), получим:

(7) $$\text{Изм } \mathfrak{A} = \text{Пор } \mathfrak{A} - \rho + 1.$$

Это — важный частный случай теоремы Римана-Роха для неспециальных классов. Риману был известен только этот частный случай.

Пусть теперь $\mathfrak{A}$ — специальный класс. Вычислим измерение класса $\frac{\mathfrak{W}}{\mathfrak{A}}$, т. е. число линейно независимых дивизоров класса $\mathfrak{W}$, делящихся на какой-нибудь дивизор класса $\mathfrak{A}$, например на $A$. Чтобы дивизор $W_1$ класса $\mathfrak{W}$ делился на $A$, необходимо и достаточно, чтобы оба элемента

$$w \asymp \frac{W_1 \cdot A^2}{z_x}, \quad wx \asymp \frac{W_1 A \cdot A'}{z_x}$$

были подинтегральными функциями интегралов 1-го рода; другими словами, чтобы $w$ и $wx$ выражались через дополнительный базис:

$$w = h_1 \mu_1 + h_2 \mu_2 + \ldots + h_n \mu_n,$$
$$wx = x h_1 \mu_1 + x h_2 \mu_2 + \ldots + x h_n \mu_n,$$

где $h_i$ и $x h_i$ — полиномы не выше $(r_i - 2)$-й степени. Значит, степень полинома $h_i$ не должна превышать $r_i - 3$. Отсюда следует, что измерение класса $\frac{\mathfrak{W}}{\mathfrak{A}}$ выражается так:

(8) $$\text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}} = (r_{s+1} - 2) + (r_{s+2} - 2) + \ldots + (r_n - 2).$$

С другой стороны, в силу

$$r_2 = r_3 = \ldots = r_s = 1$$

жанр $\rho$ может быть выражен так:

$$\rho = (r_{s+1} - 1) + (r_{s+2} - 1) + \ldots + (r_n - 1). \tag{9}$$

Вычитая из формулы (9) формулу (8), получим:

$$\rho - \text{Изм}\,\frac{\mathfrak{W}}{\mathfrak{A}} = n - s.$$

Сопоставляя это с формулой (6), будем иметь:

$$\boxed{\text{Изм}\,\mathfrak{A} = \text{Изм}\,\frac{\mathfrak{W}}{\mathfrak{A}} + \text{Пор}\,\mathfrak{A} - \rho + 1.} \tag{10}$$

Эта зависимость и составляет содержание теоремы Римана-Роха, которую можно формулировать словами так:

Теорема 41 (Римана-Роха). *Измерение класса менее его порядка на разность числа* $\rho - 1$ *и измерения дополнительного класса.*

Эта зависимость имеет место и для неспециальных классов, поскольку для них

$$\text{Изм}\,\frac{\mathfrak{W}}{\mathfrak{A}} = 0.$$

Подставляя это значение в формулу (10), мы приведём к ранее выведенной формуле (7).

Небольшое преобразование приводит формулу (10) к виду, более удобному для запоминания, хотя и не столь удобному для вычислений.

Если для двух классов $\mathfrak{A}$, $\mathfrak{B}$ имеет место

$$\mathfrak{A} \cdot \mathfrak{B} = \mathfrak{W},$$

так что

$$\text{Пор}\,\mathfrak{A} + \text{Пор}\,\mathfrak{B} = 2\rho - 2,$$

то из формулы (10) легко получается

$$\text{Изм}\,\mathfrak{A} - \frac{1}{2}\,\text{Пор}\,\mathfrak{A} = \text{Изм}\,\mathfrak{B} - \frac{1}{2}\,\text{Пор}\,\mathfrak{B}. \tag{11}$$

## § 23. Продолжение: случай несобственных классов

Формула (10) предыдущего параграфа получена нами для собственных классов. Докажем её справедливость для несобственных классов.

Сначала рассмотрим случай, когда $\mathfrak{A}$ есть несобственный специальный класс. Пусть

$$\mathfrak{A} = M \cdot \mathfrak{A}',$$

где $M$ — общий наибольший делитель дивизоров класса $\mathfrak{A}$, так что $\mathfrak{A}'$ является уже собственным классом. Если порядок дивизора $M$ равен $m$, то

$$\text{Пор } \mathfrak{A}' = \text{Пор } \mathfrak{A} - m, \tag{1}$$

$$\text{Изм } \mathfrak{A}' = \text{Изм } \mathfrak{A}. \tag{2}$$

Пусть $\mathfrak{B}$, $\mathfrak{B}'$ — классы, дополнительные к классам $\mathfrak{A}$, $\mathfrak{A}'$, так что

$$\mathfrak{A}\mathfrak{B} = \mathfrak{W}, \quad \mathfrak{A}'\mathfrak{B}' = \mathfrak{W}.$$

Класс $\mathfrak{B}'$ является классом, содержащим семейство $M\mathfrak{B}$, так что

$$\text{Изм } \mathfrak{B} \geqslant \text{Изм } \mathfrak{B}' - m. \tag{3}$$

Применяя к классам $\mathfrak{A}'$, $\mathfrak{B}'$ теорему Римана-Роха в форме (11) § 22 (мы имеем на это право, поскольку $\mathfrak{A}'$ есть собственный класс), мы в силу (3) будем иметь:

$$\text{Изм } \mathfrak{A}' - \frac{\text{Пор } \mathfrak{A} - m}{2} =$$

$$= \text{Изм } \mathfrak{B}' - \frac{\text{Пор } \mathfrak{B} + m}{2} \leqslant \text{Изм } \mathfrak{B} + m - \frac{\text{Пор } \mathfrak{B} + m}{2},$$

откуда в силу (2) получим:

$$\text{Изм } \mathfrak{A} - \frac{1}{2} \text{ Пор } \mathfrak{A} \leqslant \text{Изм } \mathfrak{B} - \frac{1}{2} \text{ Пор } \mathfrak{B}.$$

Меняя ролями $\mathfrak{A}$ и $\mathfrak{B}$, будем иметь, независимо от того, собственный ли класс $\mathfrak{B}$ или несобственный:

$$\text{Изм } \mathfrak{B} - \frac{1}{2} \text{ Пор } \mathfrak{B} \leqslant \text{Изм } \mathfrak{A} - \frac{1}{2} \text{ Пор } \mathfrak{A}.$$

Сопоставляя оба неравенства, получим

$$\text{Изм } \mathfrak{A} - \frac{1}{2} \text{ Пор } \mathfrak{A} = \text{Изм } \mathfrak{B} - \frac{1}{2} \text{ Пор } \mathfrak{B}, \tag{4}$$

а это и есть теорема Римана-Роха в форме (11) § 22.

Пусть теперь $\mathfrak{A}$ — несобственный, неспециальный класс и пусть попрежнему

$$\mathfrak{A} = M \cdot \mathfrak{A}',$$

где $\mathfrak{A}'$ — собственный класс. Попрежнему имеют место формулы (1), (2) и (3).

Найдём собственный класс, в котором $\mathfrak{A}$ является делителем (т. е. на который делится $\mathfrak{A}$). Для этого возьмём в классе $\mathfrak{A}$ дивизор $A$ и построим элемент $u$ поля $k(x, y)$, делящийся на $A$. Представляя

$u$ через дробный дивизор, у которого числитель и знаменатель взаимно просты:

$$u \equiv \frac{V_1}{V_2},$$

мы в силу выбора элемента $u$ заключаем, что $V_1$ делится на $A$, а $V_2$ взаимно прост с $A$. Обозначая через $\mathfrak{A}'$ класс, в котором лежат дивизоры $V_1$ и $V_2$, мы видим, что класс $\mathfrak{A}''$ собственный и делится на классс $\mathfrak{A}$. Он, очевидно, не специален, в силу чего

$$\text{Изм } \mathfrak{A}'' = \text{Пор } \mathfrak{A}'' - p + 1.$$

Пусть

$$\text{Пор } \mathfrak{A}'' = \text{Пор } \mathfrak{A} + q.$$

Тогда

$$\text{Изм } A \geqslant \text{Изм } \mathfrak{A}'' - q,$$

откуда

$$\text{Изм. } \mathfrak{A} \geqslant \text{Пор } \mathfrak{A} - p + 1. \tag{5}$$

С другой стороны, для класса $\mathfrak{A}'$ имеет место

$$\text{Изм } \mathfrak{A}' = \text{Изм } \mathfrak{A} = \text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}'} + (\text{Пор } \mathfrak{A} - m) - p + 1. \tag{6}$$

Сопоставляя с неравенством (5), получим:

$$\text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}'} \geqslant m,$$

откуда следует, что класс $\mathfrak{A}'$ специален.

Если бы имело место

$$\text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}'} > m,$$

то внутри класса $\frac{\mathfrak{W}}{\mathfrak{A}'}$ можно было бы найти дивизор, делящийся на $M$. Но тогда в классе $\mathfrak{W}$ существовал бы дивизор, делящийся на $MA' = A$; это, однако, противоречит предположению, что класс $\mathfrak{A}$ не специален. Таким образом

$$\text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}'} = m$$

подставляя это значение в формулу (6), будем иметь

$$\text{Изм } \mathfrak{A} = \text{Пор } \mathfrak{A} - p + 1, \tag{7}$$

и таким образом теорема Римана-Роха имеет место и для несобственных классов.

Исследуем несколько частных случаев.

1) Пусть $\mathfrak{A}$ есть неспециальный класс, состоящий из изолированного дивизора, т. е. имеющий измерение 1. Формула (7) даёт:

$$\text{Пор } \mathfrak{A} = \text{Изм } \mathfrak{A} + (p - 1) = 1 + (p - 1) = p.$$

Итак:

Неспециальные изолированные дивизоры имеют порядок $p$.

2) Рассмотрим класс $(P\mathfrak{W})$, в котором лежит семейство

$$P\mathfrak{W},$$

где $P$ — простой дивизор, а $\mathfrak{W}$ — класс дифференциалов. Этот класс, имея порядок $2p-1$, в силу теоремы 40 не специален. Применяя к нему формулу (7), получим

$$\text{Изм } (P\mathfrak{W}) = \text{Пор } (P\mathfrak{W}) - p + 1 = p,$$

откуда

$$\text{Изм } (P\mathfrak{W}) = \text{Изм } \mathfrak{W}. \tag{8}$$

Эта формула показывает, что класс $(P\mathfrak{W})$ есть несобственный класс, все дивизоры которого делятся на $P$. Другими словами, класс $(P\mathfrak{W})$ совпадает с семейством $P\mathfrak{W}$.

3) Имеет место также предложение, в известном смысле обратное только что полученному.

Если общий делитель дивизоров несобственного неспециального класса $\mathfrak{A}$ есть простой дивизор $P$, так что

$$\mathfrak{A} = P \cdot \mathfrak{A}',$$

то $\mathfrak{A}'$ есть специальный класс (т. е. $\mathfrak{A}'$ есть или $\mathfrak{W}$, или делитель $\mathfrak{W}$).

В самом деле,

$$\text{Изм } \mathfrak{A} = \text{Пор } \mathfrak{A} - p + 1.$$

Но

$$\text{Изм } \mathfrak{A} = \text{Изм } \mathfrak{A}', \quad \text{Пор } \mathfrak{A} = \text{Пор } \mathfrak{A}' + 1,$$

откуда

$$\text{Изм } \mathfrak{A}' = \text{Пор } \mathfrak{A}' - p + 2.$$

Сопоставляя с формулой (10) § 22, получим:

$$\text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}'} = 1.$$

Отсюда следует, что $\mathfrak{A}'$ есть специальный класс.

4) Теорема Римана-Роха позволяет решить следующий вопрос.

Какое число совершенно произвольных точек достаточно взять для того, чтобы они составляли полную систему точек, в которых какой-нибудь элемент поля $k(x, y)$ обращается в нуль (или в бесконечность), причём эти нули предполагаются некратными?

Пусть такое число есть $k$ и пусть

$$A = P_1 P_2 \dots P_k$$

будет произвольный дивизор порядка $k$, который пусть лежит в некотором классе $\mathfrak{A}$. Чтобы существовал элемент поля $k(x, y)$,

удовлетворяющий поставленному требованию, необходимо и достаточно, чтобы

$$\text{Изм } \mathfrak{A} \geqslant 2. \tag{9}$$

Вместе с тем теорема Римана-Роха даёт

$$\text{Изм } \mathfrak{A} = \text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}} + \text{Пор } \mathfrak{A} - p + 1,$$

откуда

$$\text{Изм } \mathfrak{A} \geqslant k - p + 1.$$

Условие (9) всегда будет выполнено, если мы положим:

$$k = p + 1.$$

Отсюда следует

Теорема 42. *Существует элемент поля $k(x, y)$ жанра $p$ с $p+1$ произвольно заданными нулями.*

Конечно, мы при этом не гарантированы, что часть из этих заданных нулей действительно не будет нулями. Это произойдёт в том случае, если $\mathfrak{A}$ окажется несобственным классом.

С другой стороны, в поле жанра $p$ всегда существуют элементы порядка $p$ (или ниже). Для их получения найдём в классе $\mathfrak{W}$ все дивизоры, делящиеся на произвольно выбранный дивизор $A$ порядка $p-2$. Сокращая эти дивизоры на $A$, мы придём к классу $\mathfrak{W}_{p-2}$ порядка $(2p-2)-(p-2)=p$ и измерения $\geqslant p-(p-2)=2$. Частное двух произвольных дивизоров этого класса и даёт искомый элемент поля.

## § 24. Теорема Нётера о пробелах

В поле рациональных функций одной переменной $x$ любые два дивизора одного и того же порядка эквивалентны. Достаточно доказать это для двух простых дивизоров. Если

$$x \approx \frac{P'}{P}$$

и если в какой-нибудь точке $P_1$ элемент $x$ принимает значение $x_1$, а в другой точке $P_2$ — значение $x_2$, то

$$\frac{P_1}{P_2} \approx \frac{x - x_1}{x - x_2}.$$

В полях жанра $p > 0$ дело обстоит сложнее. В них не всегда существуют элементы, имеющие в знаменателе (или в числителе) заданный дивизор. Более того: если мы зададим себе вопрос, каков наименьший порядок элемента поля $k(x, y)$ при данном $p$, то для разных полей с одним и тем же значением $p$ мы будем получать разные ответы. Поэтому большую ценность представляет нижеследующая

общая теорема о «пробелах», предложенная Максом Нётером (Max Noether):

Теорема 43 (М. Нётера). *Задана неограниченная система простых дивизоров*

$$P_1,\ P_2,\ P_3,\ \ldots,$$

*которые не все должны быть различны. Поставим вопросы о существовании элементов поля* $k(x, y)$, *имеющих бесконечности только в одной из следующих систем точек*:

$$1)\ |\overline{P_1}|;$$

$$2)\ P_1,\ |\overline{P_2}|;$$

$$3)\ P_1,\ P_2,\ |\overline{P_3}|;$$

$$\ldots\ldots,\ \ldots,$$

где особо отмечены точки, которые обязательно должны входить в систему бесконечностей искомых элементов, в то время как остальные точки, входящие в систему, лишь имеют право входить в систему бесконечностей искомого элемента.

*Тогда на вопросы о существовании элементов, которые мы ставим для каждой из заданных систем в отдельности, мы получим отрицательные ответы ровно* $\rho$ *раз.*

*Примечание.* Если в какой-нибудь из этих систем:

$$k)\ P_1,\ P_2,\ \ldots,\ P_{k-1},\ |\overline{P_k}|,$$

точка $P_k$ совпадает с некоторым числом, $\alpha$, остальных точек системы, то мы будем требовать, чтобы в искомом элементе точка $P_k$ была бесконечностью $\alpha$-го порядка.

Доказательство. Рассмотрим $k$-ю систему точек:

$$k)\ P_1,\ P_2,\ \ldots,\ P_{k-1},\ |\overline{P_k}|,$$

где мы выберем

$$k > 2\rho - 2,$$

так что класс $\mathfrak{A}_k$, в котором лежит дивизор

$$P_1 \cdot P_2 \ldots P_{k-1} \cdot P_k,$$

не специален, и теорема Римана-Роха даёт

$$\text{Изм}\,\mathfrak{A}_k = k - \rho + 1. \tag{1}$$

На поставленный вопрос отрицательный ответ получится в том и только в том случае, если простой дивизор $P_k$ будет общим делителем всех дивизоров класса $\mathfrak{A}_k$. Находя в классе $\mathfrak{A}_k$ все дивизоры, делящиеся на $P_k$, и сокращая их на $P_k$, обозначим полученный класс

через $\mathfrak{A}_{k-1}$. Мы видим, что отрицательный ответ на наш вопрос относительно $k$-й системы получится тогда и только тогда, когда

$$\text{Изм}\,\mathfrak{A}_k = \text{Изм}\,\mathfrak{A}_{k-1},$$

т. е. если

$$(\text{Пор}\,\mathfrak{A}_k - \text{Изм}\,\mathfrak{A}_k) = (\text{Пор}\,\mathfrak{A}_{k-1} - \text{Изм}\,\mathfrak{A}_{k-1}) + 1.$$

В случае же положительного ответа на этот вопрос мы будем иметь

$$\text{Изм}\,\mathfrak{A}_k = \text{Изм}\,\mathfrak{A}_{k-1} + 1,$$

откуда

$$(\text{Пор}\,\mathfrak{A}_k - \text{Изм}\,\mathfrak{A}_k) = (\text{Пор}\,\mathfrak{A}_{k-1} - \text{Изм}\,\mathfrak{A}_{k-1}).$$

Таким образом, придавая числу $k$ последовательно значения

$$k,\ k-1,\ \ldots,\ 3,\ 2, \tag{2}$$

мы будем получать отрицательный ответ для $\nu$-й системы всякий раз, когда значение функции

$$\text{Пор}\,\mathfrak{A}_\nu - \text{Изм}\,\mathfrak{A}_\nu \tag{3}$$

с понижением $\nu$ на единицу тоже уменьшится на единицу. Но при $\nu = k$ в силу (1) мы имеем

$$\text{Пор}\,\mathfrak{A}_k - \text{Изм}\,\mathfrak{A}_k = \rho - 1,$$

а при $\nu = 1$

$$\text{Пор}\,\mathfrak{A}_1 = 1, \quad \text{Изм}\,\mathfrak{A}_1 = 1$$

(мы исключаем случай $\rho = 0$), откуда

$$\text{Пор}\,\mathfrak{A}_1 - \text{Изм}\,\mathfrak{A}_1 = 0.$$

Из этого вытекает, что при пробегании значком $\nu$ значений (2) функция (3) ровно $\rho - 1$ раз испытает приращение, и таким образом на наш вопрос для 2-й, 3-й, ..., $k$-й систем мы получим ровно $\rho - 1$ раз отрицательные ответы. Сюда надо ещё присоединить 1-ю систему, которая при $\rho > 0$ даёт отрицательный ответ. Итак, мы получим всего $\rho$ отрицательных ответов. Заметим, что мы не ограничили сверху числа $k$, так что этот результат имеет место для сколь угодно большого $k$. Теорема доказана.

Случай $\rho = 0$ не даёт исключения, поскольку, как мы видели, при $\rho = 0$ мы не получим ни одного отрицательного ответа.

Интересен вопрос, в каких местах системы точек дают отрицательные ответы. Следует ожидать, что первые по порядку системы будут давать отрицательные ответы чаще. Однако общих правил здесь не существует, так как поля разных типов, имеющие один и тот же жанр, могут давать самые разнообразные ответы на этот вопрос. Мы убедимся в этом ниже.

В особом положении находятся так называемые *гиперэллиптические поля*, т. е. поля, содержащие элементы 2-го порядка. Пусть $k(x, y)$ — гиперэллиптическое поле и пусть $x$ — один из его элементов 2-го порядка. Всякий другой элемент этого поля удовлетворяет уравнению 2-й степени, коэффициенты которого являются рациональными функциями от $x$. Решая одно из таких уравнений, связывающих $x$ с элементом, составляющим вместе с $x$ примитивную пару поля $k(x, y)$, мы получим для одного из элементов поля, который тоже составляет с $x$ примитивную пару, выражение в виде квадратного корня из рациональной функции от $x$. Вынося за знак квадратного корня знаменатель, мы преобразуем последнюю в полином. Можно сделать степень этого полинома (который мы можем предположить лишённым кратных корней) чётной, подвергая его в случае надобности преобразованию

$$x = \frac{1}{x_1}.$$

Это позволяет нам считать гиперэллиптическое поле порождённым примитивной парой $x$, $z$, связанной уравнением

$$z^2 - (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_{2k}) = 0.$$

Каждому значению $x = \alpha_i$ соответствует точка $P_i$, причём $x - \alpha_i$ делится на 2-ю степень простого дивизора $P_i$, а $z$ — на первую степень простого дивизора $P_i$. Таким образом

$$Z_x = P_1 \cdot P_2 \ldots P_{2k},$$

откуда

$$w_x = 2k, \quad p = \frac{w_x}{2} - n_x + 1 = k - 1.$$

Рассмотрим такую неограниченную систему точек:

(4) $$P_1', P_2'; \quad P_1', P_2''; \quad P_1'', P_2''; \quad \ldots,$$

причём мы предположим, что дивизор

$$P_1' \cdot P_2'$$

лежит в классе, измерение которого равно 2.

Чтобы выяснить, на каких местах системы (4) мы будем получать «пробелы», т. е. отрицательные ответы на вопрос о существовании элементов с заданными бесконечностями, учтём, что на чётных местах последовательности (4) пробелов не может быть, так как, если положить

$$\frac{P_1'P_2'}{P_1''P_2''} \asymp x - c,$$

то элементы $(x-c)^2$, $(x-c)^3$, ... дают положительные ответы для 4-го, 6-го, ... мест этой последовательности. С другой стороны, если для какого-нибудь нечётного, скажем $(2\alpha+1)$-го, места ответ положителен и ему соответствует элемент $u$, то элементы

$$ux,\ ux^2,\ \ldots$$

дают положительные ответы для всех дальнейших нечётных мест. Таким образом пробелы (их число равно $\rho = k-1$) будут лежать на первых $\rho$ нечётных местах последовательности (4):

$$1,\ 3,\ 5,\ \ldots,\ 2\rho-1.$$

Здесь первым $s$-местам последовательности (4) соответствует ровно $\left[\frac{s+1}{2}\right]$ пробелов.

Ниже мы убедимся, что на первых $s$-местах любой последовательности точек любого поля $k(x, y)$ жанра $\rho$ $(s \leqslant 2\rho-1)$ встречается по крайней мере $\left[\frac{s+1}{2}\right]$ пробелов (теорема Клиффорда).

Вопрос о расположении пробелов был подробно изучен Вейерштрассом (Weierstrass) и Гурвицем (A. Hurwitz) для того частного случая, когда все точки $P_1$, $P_2$, ... заданной последовательности совпадают.

## § 25. Точки Вейерштрасса

Ещё до Нётера его теорема была открыта Вейерштрассом для того частного случая, когда все точки $P_1$, $P_2$, $P_3$, ... заданной последовательности совпадают. Теорема Нётера исторически была лишь обобщением результатов Вейерштрасса, которые представляют интерес с другой точки зрения: они позволили найти точки специальной природы, являющиеся инвариантами поля $k(x, y)$ и дающие возможность вскрыть его глубокие и важные свойства. Результаты Вейерштрасса в этом направлении были продолжены Гурвицем.

У Вейерштрасса его теорема (впоследствии обобщённая Нётером) имела такой вид:

Теорема 44 (Вейерштрасса). *Зададимся вопросами о существовании в поле $k(x, y)$ элементов, имеющих в качестве бесконечности только одну точку $P$, но в различных кратностях: первой, второй, третьей и т. д. Тогда из всех ответов на эти вопросы мы получим ровно $\rho$ отрицательных, которые притом все будут получаться не далее, чем на $(2\rho-1)$-м месте.*

В случае Вейерштрасса очень легко решить вопрос, на каких местах могут находиться отрицательные ответы. Для этого можно воспользоваться следующим очевидным фактом.

Если в поле $k(x, y)$ существуют элементы, имеющие бесконечностью только $P$, притом точно в $\alpha$-й и в $\beta$-й кратностях, то

произведение этих элементов имеет $P$ единственной бесконечностью, притом точно в $(\alpha+\beta)$-й кратности.

Отсюда следует:

Если в последовательности

$$P,\ P^2,\ P^3,\ \ldots \tag{1}$$

на $\alpha$-м и на $\beta$-м местах даются положительные ответы (т. е. если в них нет «пробелов»), то это же имеет место и для $(\alpha+\beta)$-го места.

Назовём *аддитивным модулем* бесконечную систему целых положительных чисел такого рода, что если два каких-нибудь числа $\alpha$ и $\beta$ входят в систему, то их сумма $\alpha+\beta$ тоже войдёт в систему. Тогда система показателей в последовательности (1), для которых ответы положительны, образует аддитивный модуль.

Нетрудно сделать полный обзор всех возможных аддитивных модулей. Для этого обозначим через $n$ наименьшее число, входящее в исследуемый модуль. Разобьём все числа натурального ряда на прогрессии с разностью $n$. Прежде всего, в модуль входят все члены прогрессии

$$n,\ 2n,\ 3n,\ \ldots$$

Далее, если в модуль входит какое-нибудь число $m$, то в него войдут также все числа

$$m,\ m+n,\ m+2n,\ \ldots$$

Поэтому нам достаточно отметить в каждой прогрессии

$$k+nx \qquad (0<k<n)$$

наименьшее число

$$k+\mu_k\cdot n \qquad (0<k<n),$$

входящее в модуль. Могло бы случиться, что в модуль вовсе не входят члены некоторых прогрессий, и тогда бы следовало положить $\mu_k=\infty$. Однако в этом случае в модуль не войдёт бесконечное множество чисел; в исследуемых нами модулях этого не случится, так как в модули не должно входить ровно $\rho$ чисел.

Таким образом все числа, входящие в модуль, могут быть расположены в виде следующей таблицы:

$$\begin{array}{c}
n,\ 2n,\ 3n,\ \ldots \\
1+\mu_1 n,\ 1+(\mu_1+1)n,\ 1+(\mu_1+2)n,\ \ldots \\
2+\mu_2 n,\ 2+(\mu_2+1)n,\ 2+(\mu_2+2)n,\ \ldots \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
(n-1)+\mu_{n-1}n,\ (n-1)+(\mu_{n-1}+1)n,\ (n-1)+(\mu_{n-1}+2)n,\ \ldots
\end{array}$$

Между числами $\mu_i$ $(i=1,\ 2,\ \ldots,\ n-1)$ имеют место следующие неравенства:

1°. $\mu_i+\mu_k\geqslant\mu_{i+k}$ $\qquad (i+k<n)$.

2°. $\mu_i+\mu_k\geqslant\mu_{i+k-n}-1$ $\qquad (i+k>n)$.

В самом деле, в модуль, наряду с числами

$$i+\mu_i n, \quad k+\mu_k n,$$

должна входить их сумма

$$(i+k)+(\mu_i+\mu_k)\,n.$$

Если $i+k<n$, то эта сумма входит в прогрессию

$$i+k+\mu_{i+k}\cdot n,$$

откуда получается неравенство 1°. Если же $i+k>n$, то можно переписать эту сумму так:

$$(i+k-n)+(\mu_i+\mu_k+1)\,n.$$

Это число должно входить в прогрессию

$$(i+k-n)+\mu_{i+k-n}\cdot n, \quad (i+k-n)+(\mu_{i+k-n}+1)\,n, \ldots,$$

откуда вытекает неравенство 2°.

Легко убедиться, что условия 1° и 2° также достаточны для того, чтобы система образовала аддитивный модуль.

Выразим жанр $\rho$ через числа $n, \mu_i$. В каждой из выделенных нами прогрессий в модуль не входят $\mu_i$ чисел, так что теорема о пробелах даёт:

$$\rho=\mu_1+\mu_2+\ldots+\mu_{n-1}. \tag{2}$$

Самым замечательным результатом теории точек Вейерштрасса является следующий:

Теорема 45. *Во всяком поле $k(x, y)$ число точек Вейерштрасса конечно, а при $\rho>1$ оно притом отлично от нуля.*

При этом под *точкой Вейерштрасса* мы будем разуметь такую точку $P$, что в последовательности (1) отрицательные ответы даются не на $\rho$ первых местах.

Пусть

$$0<\sigma_1<\sigma_2<\ldots<\sigma_\rho\leqslant 2\rho-1$$

будут номера мест, которым в ряду (1) соответствуют отрицательные ответы (пробелы). Тогда при значениях

$$\alpha=\sigma_i \qquad (i=1, 2, \ldots, \rho) \tag{3}$$

имеет место

$$\text{Изм}\,(P^\alpha)=\text{Изм}\,(P^{\alpha-1}),$$

где под $(P^\alpha)$ мы разумеем класс, в котором лежит дивизор $P^\alpha$. Отсюда в силу теоремы Римана-Роха мы будем иметь:

$$\text{Изм}\left(\frac{\mathfrak{W}}{(P^\alpha)}\right)=\text{Изм}\left(\frac{\mathfrak{W}}{(P^{\alpha-1})}\right)-1.$$

Другими словами, значения (3) являются теми значениями значка $\alpha$, для которых существуют дивизоры класса $\mathfrak{W}$, делящиеся точно на $P^{\alpha-1}$. Итак, в нашем случае существуют дивизоры класса $\mathfrak{W}$, делящиеся точно на

$$P^{\sigma_1-1},\ P^{\sigma_2-1},\ \ldots,\ P^{\sigma_\rho-1}.$$

Легко видеть, что эти дивизоры линейно независимы.
Пусть это будут

$$W_1 = P^{\sigma_1-1}V_1,\quad W_2 = P^{\sigma_2-1}V_2,\quad \ldots,\quad W_\rho = P^{\sigma_\rho-1}V_\rho,$$

где дивизоры

$$V_1,\ V_2,\ \ldots,\ V_\rho$$

уже не делятся на $P$.

Дальнейшие рассуждения справедливы только в случае, когда числовое поле $k$ имеет характеристику нуль.

Введём понятие высших производных от элементов поля $k(x, y)$. Под второй производной $\frac{d^2y}{dx^2}$ мы будем разуметь производную от элемента $\frac{dy}{dx}$ (см. § 17) по элементу $x$. Точно так же введём высшие производные

$$\frac{d^3y}{dx^3},\ \frac{d^4y}{dx^4},\ \ldots$$

Найдём формулы, связывающие высшие производные по различным элементам. Для первой производной мы уже имели формулу (16) § 17. Для дальнейшего нам понадобится следующее обобщение формулы (15) § 17:

Если элементы $u, v, \ldots, w$ связаны зависимостью

$$F(u, v, \ldots, w) = 0, \tag{4}$$

то имеет место

$$\frac{\partial F}{\partial u}\cdot\frac{du}{dt} + \frac{\partial F}{\partial v}\cdot\frac{dv}{dt} + \ldots + \frac{\partial F}{\partial w}\cdot\frac{dw}{dt} = 0. \tag{5}$$

Вывод этого соотношения есть дословный пересказ рассуждений § 17. В частности, полагая

$$F = W - u\cdot v,$$

получим из формулы (5):

$$w = u\cdot v,\quad \frac{dw}{dt} = u\frac{dv}{dt} + v\frac{du}{dt} \tag{6}$$

(формула для производной от произведения).

Перепишем формулу (16) § 17 так:

$$\frac{dy}{dt} = \frac{dy}{dx} \cdot \frac{dx}{dt}. \tag{7}$$

Беря производную от этого соотношения по элементу $t$, мы в силу (6) получим:

$$\frac{d^2y}{dt^2} = \frac{d^2y}{dx^2} \cdot \left(\frac{dx}{dt}\right)^2 + \frac{dy}{dt} \cdot \frac{d^2x}{dt^2}. \tag{8}$$

Опять возьмём производную по элементу $t$:

$$\frac{d^3y}{dt^3} = \frac{d^3y}{dx^3} \cdot \left(\frac{dx}{dt}\right)^3 + 3\frac{d^2y}{dx^2} \cdot \frac{dx}{dt} \cdot \frac{d^2x}{dt} + \frac{dy}{dx} \cdot \frac{d^3x}{dt^3}, \tag{9}$$

и т. д. Заметим, что в выражении $\frac{d^ky}{dt^k}$ при всяком $k$ коэффициентом при $\frac{d^ky}{dx^k}$ будет $\left(\frac{dx}{dt}\right)^k$.

Рассмотрим определитель

$$\Delta_x = \begin{vmatrix} u_1', & u_2', & \dots, & u_\rho' \\ u_1'', & u_2'', & \dots, & u_\rho'' \\ \dots & \dots & \dots & \dots \\ u_1^{(\rho)}, & u_2^{(\rho)}, & \dots, & u_\rho^{(\rho)} \end{vmatrix}, \tag{10}$$

где

$$u_1, u_2, \dots, u_\rho \tag{11}$$

есть система линейно независимых интегралов 1-го рода, а штрихами (или цифрой в скобках наверху) мы обозначаем порядок производной по $x$. Заметим, что в выражение определителя (10) входят только элементы поля $k(x, y)$, каковыми являются производные от $u_t$.

Заменяя в выражении (10) производные по $x$ производными по другому элементу, $t$, и применяя для этого формулы (8), (9), ..., мы получим соотношение

$$\Delta_t = \Delta_x \cdot \left(\frac{dx}{dt}\right)^{\frac{\rho(\rho+1)}{2}}. \tag{12}$$

Поставим себе задачу определить степень, в которой входит какой-нибудь простой дивизор $P$ в числитель представления $\Delta_t$ через дивизоры. Выберем в качестве $t$ такой элемент поля $k(x, y)$, что разность $t - t_0$ делится точно на первую степень $P$, если $t_0$ — значение элемента $t$ в точке $P$. Пусть $x - x_0$ делится точно на $k$-ю степень $P$, так что

$$x - x_0 = (t - t_0)^k \cdot u, \tag{13}$$

где $u_0 \not\equiv 0$, $u_0 \not\equiv \infty$. Отсюда

$$(14) \qquad \frac{dx}{dt} = (t-t_0)^{k-1}\left[k \cdot u + (t-t_0)\frac{du}{dt}\right] = (t-t_0)^{k-1} \cdot u_1,$$

где $\left(\frac{du}{dt}\right)_0 - \left(\frac{u-u_0}{t-t_0}\right)_0 \not\equiv \infty$, так что

$$(u_1)_0 = k \cdot u_0.$$

Продолжая процесс, получим

$$(15) \qquad \frac{d^\nu x}{dt^\nu} = (t-t_0)^{k-\nu} \cdot u_\nu \qquad (\nu = 1, 2, \ldots, k),$$

где

$$(16) \qquad (u_\nu)_0 = k(k-1)\ldots(k-\nu+1) \cdot u_0 \qquad (\nu = 1, 2, \ldots, k).$$

Предположим для общности, что $P$ есть точка Вейерштрасса, которой соответствуют показатели $\sigma_1, \sigma_2, \ldots, \sigma_\rho$. В частности, если $P$ есть обыкновенная точка, мы будем иметь:

$$\sigma_1 = 1, \quad \sigma_2 = 2, \quad \ldots, \quad \sigma_\rho = \rho.$$

Введём в рассмотрение число

$$(17) \qquad \tau = \sigma_1 + \sigma_2 + \ldots + \sigma_\rho - \frac{\rho(\rho+1)}{2},$$

которое мы будем называть *весом* точки $P$. Чтобы точка $P$ была точкой Вейерштрасса, необходимо и достаточно, чтобы его вес был больше нуля.

Если мы подвергнем интегралы (11) линейной подстановке с постоянными коэффициентами, то легко видеть, что определитель $\Delta_t$ умножится на определитель этой подстановки, т. е. на постоянное число, и его представление через дивизоры останется тем же. Подвергнем интегралы (11) такой подстановке, чтобы целые дивизоры, представляющие дифференциалы

$$du_1, \; du_2, \; \ldots, \; du_\rho,$$

соответственно делились точно на

$$P^{\sigma_1-1}, \; P^{\sigma_2-1}, \; \ldots, \; P^{\sigma_\rho-1}.$$

Но в силу нашего условия относительно делимости $t-t_0$ точно на первую степень $P$ производные

$$\frac{du_i}{dt} \equiv \frac{W_i T^2}{Z_t} \qquad (i = 1, 2, \ldots, \rho),$$

где $t \equiv \frac{T'}{T}$, делятся точно на $P^{\sigma_i-1}$. Пусть

$$\frac{du_i}{dt} = (t-t_0)^{\sigma_i-1} v_i \qquad (i = 1, 2, \ldots, \rho),$$

где $(v_i)_0 \neq 0$. Тогда в силу (14) и (15)

$$\frac{d^\nu u_i}{dt^\nu} = (t-t_0)^{\sigma_i-\nu}\cdot v_i^{(\nu)} \qquad (i=1, 2, \ldots, \rho), \tag{18}$$

где

$$(v_i^{(\nu)})_0 = (\sigma_i-1)(\sigma_i-2)\ldots(\sigma_i-\nu+1)\cdot(v_i)_0.$$

Подставляя выражение (18) в определитель $\Delta_t$, будем иметь:

$$\Delta_t = \begin{vmatrix} (t-t_0)^{\sigma_1-1}\cdot v_1, & (t-t_0)^{\sigma_2-1}\cdot v_2, \ldots, & (t-t_0)^{\sigma_\rho-1}\cdot v_\rho, \\ A_1^1(t-t_0)^{\sigma_1-2}\cdot v_1^{(2)}, & A_2^1(t-t_0)^{\sigma_2-2}\cdot v_2^{(2)}, \ldots & \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ A_1^{\rho-1}(t-t_0)^{\sigma_1-\rho}v_1^{(\rho)}, \vdots & & \end{vmatrix} =$$

$$= (t-t_0)^{(\sigma_1-1)+(\sigma_2-2)+\ldots+(\sigma_\rho-\rho)} \times$$

$$\times \begin{vmatrix} v_1, & v_2, \ldots, & v_\rho \\ (\sigma_1-1)\cdot v_1^{(2)}, & (\sigma_2-1)v_2^{(2)}, \ldots & (\sigma_\rho-1)v_\rho^{(2)} \\ \ldots\ldots\ldots\ldots\ldots\ldots & & \end{vmatrix},$$

где $A_i^k = (\sigma_i-1)(\sigma_i-2)\ldots(\sigma_i-k+1)$.

Стоящий множителем в правой части определитель в точке $P$ имеет значение

$$v_1 v_2 \ldots v_\rho \begin{vmatrix} 1, & 1, \ldots, & 1 \\ \ldots\ldots\ldots & & \\ \sigma_1, & \sigma_2, \ldots, & \sigma_\rho, \\ \sigma_1^{\rho-1}, & \sigma_2^{\rho-1}, \ldots, & \sigma_\rho^{\rho-1} \end{vmatrix} \neq 0.$$

Таким образом $\Delta_t$ делится на простой дивизор $P$ в степени

$$(\sigma_1-1)+(\sigma_2-2)+\ldots+(\sigma_\rho-\rho) = \sigma_1+\sigma_2+\ldots+\sigma_\rho-\frac{\rho(\rho+1)}{2} = \tau.$$

Из этого следует, что при нашем подборе элемента $t$ элемент $\Delta_t$ делится на простой дивизор $P$ ровно в степени $\tau$. Определим, на какую степень $P$ должен делиться $\Delta_x$, если $x$ — фиксированный элемент поля $k(x, y)$, в то время как $t$ подбирается для каждой точки так, что $t_0$ конечно и $t-t_0$ делится точно на первую степень. Для этого мы будем пользоваться формулой (12).

Пусть $x_0$ конечно и пусть $x-x_0$ делится точно на $P^\alpha$. Тогда $Z_x$, а также $\frac{dx}{dt}$ делятся точно на $P^{\alpha-1}$. Из формулы (12) следует, что $\Delta_x$ делится точно на

$$P^{\tau-(\alpha-1)\cdot\frac{\rho(\rho+1)}{2}}.$$

Если $x_0 = \infty$ и $\frac{1}{x}$ делится на $P^{\alpha}$, $Z_x$ делится на $P^{\alpha-1}$, то $\frac{dx}{dt}$ делится точно на $P^{-(\alpha+1)+p(\alpha-1)-2\alpha}$ так, что $\Delta_x$ делится точно на

$$P^{-(\alpha-1)\frac{p(p+1)}{2}+2\alpha\cdot\frac{p(p+1)}{2}}.$$

Таким образом $\Delta_x$ представляется через дробный дивизор, числитель которого есть

$$\Pi P_{\nu}^{\tau_{\nu}} \cdot X^{p(p+1)},$$

где произведение распространяется на все точки Вейерштрасса, а знаменатель

$$Z_x^{\frac{p(p+1)}{2}}.$$

Числитель и знаменатель дробного дивизора, представляющего элемент поля, должны быть дивизорами одинакового порядка. Отсюда прежде всего ясно, что число точек Вейерштрасса конечно. Равенство обоих порядков даёт:

$$\sum_{\nu}\tau_{\nu}+p(p+1)\cdot n = w_x\cdot\frac{p(p+1)}{2}.$$

Принимая во внимание, что

$$\frac{w_x}{2}-n=p-1,$$

получим окончательно:

$$\sum_{\nu}\tau_{\nu}=(p-1)p(p+1). \tag{19}$$

Правая часть при $p>1$ больше нуля, в силу чего точки Вейерштрасса обязательно существуют. Таким образом теорема 45 доказана.

Исследования Вейерштрасса были продолжены Гурвицем. Наиболее важный результат последнего состоит в нахождении верхней границы для веса $\tau$, что определяет минимальное число различных точек Вейерштрасса для каждого поля $k(x, y)$ жанра $p$. Для получения своего результата Гурвиц располагает таблицу *дефектных* показателей (т. е. показателей, дающих отрицательные ответы) в следующем виде:

$$\begin{gathered}1,\ 1+n,\ \ldots,\ 1+(\mu_1-1)n,\\ 2,\ 2+n,\ \ldots,\ 2+(\mu_2-1)n,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ n-1,\ (n-1)+n,\ \ldots,\ (n-1)+(\mu_{n-1}+1)n,\end{gathered} \tag{20}$$

где $n$ попрежнему обозначает наименьший из показателей, которым соответствует положительный ответ.

В силу теоремы Нётера число этих показателей равно $\rho$, откуда

$$\sum_{i=1}^{n-1} \mu_i = \rho. \tag{21}$$

С другой стороны, показатели (20) являются расположенными в другом порядке показателями $\sigma_1, \sigma_2, \ldots, \sigma_\rho$, а потому их сумма, за вычетом $\frac{\rho(\rho+1)}{2}$, равна весу $\tau$ точки $P$. Таким образом

$$\tau = \frac{1}{2}\sum_{i=1}^{n-1} \{2i + (\mu_i - 1)n\}\mu_i - \frac{\rho(\rho+1)}{2}.$$

Заменим в этой формуле числа $\mu_i$ числами $r_i$, где

$$r_i = i + (\mu_i - 1)n,$$

т. е. последними членами в отдельных строках таблицы (20). Для них имеет место

$$r_i \leqslant 2\rho - 1. \tag{22}$$

Подставляя в выражение для $\tau$, будем иметь:

$$\tau = \frac{1}{2}\sum_{i=1}^{n-1}(i + r_i)(r_i + n - i) - \frac{\rho(\rho+1)}{2} =$$

$$= \frac{1}{2n}\sum_{i=1}^{n-1} r_i^2 + \frac{1}{2}\sum_{i=1}^{n-1} r_i + \frac{1}{2n}\sum_{i=1}^{n-1} i(n-i) - \frac{\rho(\rho+1)}{2}.$$

Из (21) мы получим:

$$\sum_{i=1}^{n-1} r_i = \sum_{i=1}^{n-1} \{i + (\mu_i - 1)n\} = n\rho - \frac{n(n-1)}{2}. \tag{23}$$

Преобразуем выражение для $\tau$:

$$\tau = \frac{1}{2n}\sum_{i=1}^{n-1} r_i^2 + \frac{1}{2}\left\{n\rho - \frac{n(n-1)}{2}\right\} +$$

$$+ \frac{1}{4}n(n-1) - \frac{1}{12}(n-1)(2n-1) - \frac{\rho(\rho+1)}{2} =$$

$$= \frac{1}{2n}\sum_{i=1}^{n-1} r_i^2 + \frac{1}{2}n\rho - \frac{1}{12}(n-1)(2n-1) - \frac{1}{2}\rho(\rho+1).$$

Оценим сумму $\sum_{i=1}^{n-1} r_i^2$, пользуясь формулами (22) и (23):

$$\frac{1}{2n}\sum_{i=1}^{n-1} r_i^2 = \frac{1}{2n}\sum_{i=1}^{n-1} r_i \cdot r_i \leqslant \frac{2\rho-1}{2n}\sum_{i=1}^{n-1} r_i = \frac{\rho(2\rho-1)}{2} - \frac{(n-1)(2\rho-1)}{4},$$

откуда

$$\tau \leqslant \frac{1}{2}\rho(2\rho-1) - \frac{1}{2}\rho(\rho+1) + \frac{1}{2}n\rho - \frac{1}{4}(n-1)(2\rho-1) -$$
$$- \frac{1}{12}(n-1)(2n-1) = \frac{1}{2}(2\rho^2-\rho-\rho^2-\rho+\rho) + \frac{1}{4}(n-1) -$$
$$- \frac{1}{12}(n-1)(2n-1) = \frac{\rho(\rho-1)}{2} - \frac{1}{6}(n-1)(n-2).$$

Отсюда следует

$$\tau \leqslant \frac{\rho(\rho-1)}{2}, \tag{24}$$

причём равенство может иметь место только при $n=2$, т. е. в случае гиперэллиптического поля.

Сопоставляя (24) с формулой (19), в силу которой сумма весов, соответствующих всем точкам Вейерштрасса поля, равна $(\rho-1)\rho(\rho+1)$, мы приходим к

Теореме 46 (Гурвица). *Число различных точек Вейерштрасса в поле $k(x, y)$ жанра $\rho$ по крайней мере равно*

$$2(\rho+1), \tag{25}$$

*причём в негиперэллиптических полях их число непременно превышает* $2(\rho+1)$.

Рассмотрим случай гиперэллиптического поля. Пусть поле $k(x,y)$ задано соотношением

$$y^2 - (x-a_1)(x-a_2)\ldots(x-a_{2\rho+2}) = 0, \tag{26}$$

где все $a_1, a_2, \ldots, a_{2\rho+2}$ отличны друг от друга. Элемент $x$ имеет порядок 2. Элементы

$$x - a_i \qquad (i = 1, 2, \ldots, a_{2\rho+2})$$

обращаются в нуль в одной точке $P_i(x=a_i, y=0)$ второй кратности, так что

$$x - a_i \sim \frac{P_i^2}{P_\infty \cdot P_\infty'}. \tag{27}$$

Точки $P_\infty$, $P'_\infty$, в которых $x$ и $y$ обращаются в бесконечность, различны, так как уравнение (26) можно переписать так:

$$\left(\frac{y}{x^{\rho+1}}\right)^2-\left(1-\frac{a_1}{x}\right)\left(1-\frac{a_2}{x}\right)\ldots\left(1-\frac{a_{2\rho+2}}{x}\right)=0,$$

откуда видно, что при $\frac{1}{x}=0$ элемент

$$\frac{y}{x^{\rho+1}}$$

принимает значения $+1$ и $-1$.

Из представления (27) следует, что в последовательности

$$P_i,\ P_i^2,\ P_i^3,\ \ldots$$

степень $p_i^2$ даёт положительный ответ и точно так же все чётные степени. Это показывает, что $P_i$ есть точка Вейерштрасса, для которой

$$\sigma_1=1,\ \sigma_2=3,\ \ldots,\ \sigma_\rho=2_{\rho-1},$$

так что её вес равен

$$\tau_i=\sigma_1+\sigma_2+\ldots+\sigma_\rho-\frac{\rho(\rho+1)}{2}=$$
$$=1+3+\ldots+(2\rho-1)-\frac{\rho(\rho+1)}{2}=\frac{\rho(\rho-1)}{2},$$

т. е. как раз максимальному возможному значению [см. (24)]. Сумма весов для всех точек $P_1$, $P_2$, ..., $P_{2\rho+2}$ равна:

$$\sum_{i=1}^{2\rho+2}\tau_i=\frac{\rho(\rho-1)}{2}\cdot(2\rho+2)=(\rho-1)\rho(\rho+1).$$

Сличая этот результат с формулой (19), мы заключаем, что поле $k(x, y)$, кроме точек $P_1$, $P_2$, ..., $P_{2\rho+2}$, других точек Вейерштрасса не имеет.

Сделаем для веса $\tau$ оценку снизу. Для этого, положив

$$r_i=i+(\mu_i-1)n,$$

получим:

$$\sum_{i=1}^{n-1}r_i^2=\sum_{i=1}^{n-1}\{(\mu_i-1)n+i\}^2= \tag{28}$$
$$=(n^2\sum_{i=1}^{n-1}(\mu_i-1)^2+2n\sum_{i=1}^{n-1}i(\mu_i-1)+\sum_{i=1}^{n-1}i^2.$$

Из (21) следует:

$$\sum_{i=1}^{n-1}(\mu_i-1)=\rho-(n-1). \tag{29}$$

Найдём наименьшее значение, принимаемое суммой

$$\sum_{i=1}^{n-1}(\mu_i-1)^2 \tag{30}$$

при условии (29), если будем предполагать, что переменные $\mu_i$ изменяются непрерывно. Из элементарных соображений вытекает, что сумма (30) принимает минимум, если мы придадим переменным $\mu_i-1$ равные друг другу значения, которые в силу (29) равны

$$\frac{\rho}{n-1}-1.$$

Отсюда следует, что

$$\sum_{i=1}^{n-1}(\mu_i-1)^2 \geqslant (n-1)\left(\frac{\rho}{n-1}-1\right)^2=\frac{\rho^2}{n-1}-2\rho+(n-1).$$

Подставляя в (28), где мы отбросим вторую сумму, получим:

$$\sum_{i=1}^{n-1} r_i^2 \geqslant \frac{n^2}{n-1}\rho^2-2n^2\rho+n^2(n-1)+\frac{n(n-1)(2n-1)}{6}.$$

Подставляя в выражение для $\tau$, будем иметь

$$\tau \geqslant \frac{n}{2(n-1)}\cdot\rho^2-n\rho+\frac{n(n-1)}{2}+\frac{(n-1)(2n-1)}{12}+$$
$$+\frac{1}{2}n\rho-\frac{1}{2}(n-1)(2n-1)-\frac{\rho(\rho+1)}{2},$$

т. е.

$$\tau \geqslant \frac{1}{2(n-1)}\cdot\rho^2-\frac{n+1}{2}\rho+\frac{n(n-1)}{2}. \tag{31}$$

Эта оценка существенно зависит от числа $n$. При больших значениях $n$ она даёт мало. Например, при $n=\rho$ (в этом случае $\tau=1$) в правой части формулы (31) получается отрицательная величина. Но, например, при $n=2$, т. е. в случае гиперэллиптического поля, формула (31) даёт:

$$\tau \geqslant \frac{(\rho-1)(\rho-2)}{2}.$$

Как мы уже убедились, эта оценка является точной.

## § 26. Теорема Клиффорда и её обобщение

Мы уже упоминали, что если дана произвольная последовательность точек

$$P_1,\ P_2,\ P_3,\ \ldots, \tag{1}$$

то мы знаем очень мало о том, на каких местах находятся её «дефектные» номера. Однако известно, что, идя от начала последо-

вательности, мы будем по порядку номеров чаще встречать дефектные, чем недефектные номера. Это правило, конечно, справедливо до тех пор, пока мы находимся в пределах «специальной» части последовательности.

Формулируем это правило точнее. Рассмотрим последовательность классов

$$(P_1),\ (P_1P_2),\ \ldots,\ (P_1 \cdot P_2 \ldots P_k). \tag{2}$$

Мы знаем, что $i$ есть дефектный номер последовательности (1) тогда и только тогда, если

$$\text{Изм}\,(P_1 \cdot P_2 \ldots P_i) = \text{Изм}\,(P_1P_2 \ldots P_{i-1});$$

в противном же случае мы имеем

$$\text{Изм}\,(P_1P_2 \ldots P_i) = \text{Изм}\,(P_1P_2 \ldots P_{i-1}) + 1.$$

Таким образом, если среди $k$ первых номеров имеется $\varkappa$ дефектных, то, идя вдоль системы классов (2), мы на $\varkappa - 1$ местах не получим роста измерения, так что

$$\text{Изм}\,(P_1P_2 \ldots P_k) = k - \varkappa + 1.$$

Теорема Клиффорда состоит в утверждении, что дефектных номеров не меньше, чем недефектных:

$$\varkappa \geqslant k - \varkappa; \tag{3}$$

Клиффорд выражал её, пользуясь числами, выражающими порядок и измерение класса

$$\mathfrak{A} = (P_1P_2 \ldots P_k).$$

Эти числа выражаются через $k$ и $\varkappa$ так:

$$\text{Пор}\,\mathfrak{A} = k, \quad \text{Изм}\,\mathfrak{A} = k - \varkappa + 1,$$

откуда

$$k = \text{Пор}\,\mathfrak{A}, \quad \varkappa = \text{Пор}\,\mathfrak{A} - \text{Изм}\,\mathfrak{A} + 1.$$

Подставляя в (3), мы получим утверждение Клиффорда в таком виде:

$$2 \cdot \text{Пор}\,\mathfrak{A} - 2\,\text{Изм}\,\mathfrak{A} + 2 \geqslant \text{Пор}\,\mathfrak{A},$$

т. е.

$$\text{Пор}\,\mathfrak{A} \geqslant 2 \cdot \text{Изм}\,\mathfrak{A} - 2. \tag{4}$$

Но Клиффорд доказал больше: он установил, что в соотношении (4) знак равенства может иметь место только в конце специальной части последовательности (2), т. е. только в том случае, когда

$$\mathfrak{A} = \mathfrak{W}, \quad \text{Изм}\,\mathfrak{A} = \rho, \quad \text{Пор}\,\mathfrak{A} = 2\rho - 2.$$

Другими словами, если мы имеем специальный класс $\mathfrak{A}$, у которого порядок и измерение связаны соотношением

$$\text{Пор}\,\mathfrak{A} = 2 \cdot \text{Изм}\,\mathfrak{A} - 2, \tag{5}$$

то $\mathfrak{A}$ есть класс дифференциалов $\mathfrak{W}$, откуда

$$\rho = \text{Изм}\,\mathfrak{A}.$$

Утверждение Клиффорда даёт возможность получить верхнюю границу для жаира $\rho$ поля $k(x, y)$, если в нём известен класс $\mathfrak{A}$ дивизоров, удовлетворяющий соотношению (5). При этом не требуется, чтобы класс был специальным: в самом деле, если класс $\mathfrak{A}$ не специален, то ограничение для жанра вытекает сразу из теоремы Римана-Роха

$$\rho = \text{Пор}\,\mathfrak{A} - \text{Изм}\,\mathfrak{A} + 1; \tag{6}$$

при существовании соотношения (5) это приводит к значению

$$\rho = \text{Изм}\,\mathfrak{A} - 1.$$

Второе утверждение Клиффорда допускает исключение: если $k(x, y)$ есть гиперэллиптическое поле, причём

$$\text{Изм}\,(P_1P_2) = 2,$$

то, беря в роли (1) такую последовательность:

$$P_1,\ P_2;\quad P_1,\ P_2;\quad P_1,\ P_2;\quad \ldots,$$

мы получим следующие значения для измерений построенных с её помощью классов (2):

$$1,\ 2;\quad 2,\ 3;\quad 3,\ 4;\quad \ldots,$$

так что равенство (5) будет выполняться на каждом чётном месте. В дальнейшем мы увидим, что это исключение теоремы Клиффорда единственное, и во всех остальных случаях теорема Клиффорда справедлива.

Теорему Клиффорда можно обобщить, задавшись следующей проблемой:

Даны измерение и порядок некоторого класса $\mathfrak{A}$ в поле $k(x, y)$. В каком случае мы можем определить жанр поля $k(x, y)$ или по крайней мере указать для него верхнюю границу?

Если класс $\mathfrak{A}$ не специален, то жанр поля $k(x, y)$ сразу определится из формулы (6). В случае же специального класса надо попрежнему исключить гиперэллиптическое поле. Тогда, введя обозначения

$$\text{Изм}\ \mathfrak{A} = n,\quad \text{Пор}\,\mathfrak{A} = m,\quad r = m - 2n + 2,$$

мы при условии выполнения неравенства

$$2n - r - 4 > 0 \tag{7}$$

получим для жанра $p$ следующее ограничение:

$$p \leqslant n + 2r + \left[\frac{2r(r+1)}{2n-r-4}\right], \tag{8}$$

где, как в теории чисел, под символом $[a]$ мы будем разуметь наименьшее целое число, не превышающее $a$ («entier»).

Если $r = 0$, мы получим отсюда теорему Клиффорда:

Теорема 47 (Клиффорда). *Между измерением и порядком специального класса* $\mathfrak{A}$ *существует неравенство*

$$\text{Пор}\,\mathfrak{A} \geqslant 2 \cdot \text{Изм}\,\mathfrak{A} - 2. \tag{9}$$

Доказательство. Допустим противное: пусть класс $\mathfrak{A}$ имеет измерение $n$ и порядок $m$, причём

$$m < 2n - 2. \tag{10}$$

Не нарушая общности, предположим, что класс $\mathfrak{A}$ собственный: в противном случае мы бы сократили его на общий дивизор, что уменьшило бы его порядок и оставило бы неизменным его измерение, так что неравенство (10) не нарушилось бы.

Возьмём произвольную не-вейерштрассову точку $P$ и закрепим в классе $\mathfrak{A}$ $(n-1)$-ю степень простого дивизора $P$. Тогда в классе $\mathfrak{A}$ определится по крайней мере один дивизор вида

$$P^{n-1} \cdot P_1 P_2 \ldots P_{m-n+1}.$$

В силу (10) мы имеем

$$n - 1 > m - n + 1,$$

так что, закрепляя в классе $\mathfrak{A}$ точки $P_1, P_2, \ldots, P_{m-n+1}$, мы получим класс

$$(P^{n-1}),$$

измерение которого подчинено неравенству

$$\text{Изм}\,(P^{n-1}) \geqslant n - (m - n + 1) \geqslant n - (n-2) = 2,$$

так что в поле $k(x, y)$ существует элемент, в представлении которого через дивизоры знаменатель состоит из дивизора $P^{n-1}$. Это, однако, противоречит тому, что $P$ не есть точка Вейерштрасса. В самом деле, мы предположили, что класс $\mathfrak{A}$ специален, откуда

$$\text{Изм}\,\mathfrak{A} \leqslant \text{Изм}\,\mathfrak{B},$$

т. е.

$$n \leqslant p,$$

так что

$$\text{Изм}\,(P^{p-1}) \geqslant 2.$$

Получившееся противоречие доказывает теорему.

В дальнейшем нам понадобится следующая простая

Лемма. *Если*

$$\text{Изм } \mathfrak{A} = n,$$

*то мы можем найти в классе* $\mathfrak{A}$ *такой дивизор*

$$Q \cdot P_1 P_2 \dots P_{n-1}, \tag{11}$$

*чтобы имело место*

$$\text{Изм } (Q) = 1.$$

Доказательство. Выберем в качестве $P_1$ простой дивизор, не входящий в общий делитель класса $\mathfrak{A}$. Тогда, находя в классе $\mathfrak{A}$ все дивизоры, делящиеся на $P_1$, и сокращая их на $P_1$ («закрепив» $P_1$), мы придём к классу $\mathfrak{A}_1$ измерения $n-1$. Закрепим в нём точку $P_2$, которой соответствует простой дивизор, не входящий в общий делитель класса $\mathfrak{A}_1$. Получим класс $\mathfrak{A}_2$ измерения $n-2$. Продолжая процесс, мы, наконец, придём к классу $\mathfrak{A}_{n-1}$ измерения 1. Если он порождается дивизором $Q$, то в классе $\mathfrak{A}$ лежит дивизор (11), ч. т. д.

Теорема 48. *Пусть измерение* $n$ *и порядок* $m$ *специального класса* $\mathfrak{A}$ *поля* $k(x, y)$ *связаны соотношением*

$$m = 2n-2+r, \quad r \geqslant 0, \tag{12}$$

*причём*

$$2n - r - 4 > 0. \tag{13}$$

*Кроме того, пусть класс* $\mathfrak{A}$ *содержит такой дивизор*

$$A = P_1 P_2 \dots P_{n-2} P_{n-1} Q, \tag{14}$$

*что класс* $(P_1 Q)$ *имеет измерение* 2 *и является собственным. Тогда жанр* $p$ *поля* $k(x, y)$ *удовлетворяет неравенству*

$$p \leqslant n + 2r + \left[\frac{3r(r+1)}{2n-r-1}\right]. \tag{15}$$

Доказательство. В силу предыдущей леммы в классе $\mathfrak{A}$ можно найти такой дивизор (14), что Изм $(Q) = 1$. Тогда

$$\text{Изм } (P_1 Q) = 2, \text{Изм } (P_1 P_2 Q) = 3, \dots, \text{ Изм } (P_1 P_2 \dots P_{n-1} Q) = n. \tag{16}$$

В силу нашего предположения класс $(P_1 Q)$ собственный. Кроме того, из рассуждения при доказательстве предыдущей леммы следует, что каждую из точек $P_1, P_2, \dots, P_{n-1}$ можно выбирать произвольно, избегая лишь конечного числа значений. Выберем эти точки так, чтобы

$$\text{Изм } (P_1 P_2 \dots P_{n-1}) = 1. \tag{17}$$

Для этого достаточно выбрать $P_1$ произвольно; $P_2$ так, чтобы $P_2$ не был общим делителем класса $\left(\frac{\mathfrak{A}}{P_1}\right)$; $P_3$ так, чтобы $P_3$ не был общим

делителем класса $\left(\frac{\mathfrak{W}}{P_1P_2}\right)$, и т. д. Тогда

$$\text{Изм}\left(\frac{\mathfrak{W}}{P_1P_2\ldots P_{n-1}}\right)=p-n+1,$$

и теорема Римана-Роха даёт:

$$\text{Изм}\,(P_1P_2\ldots P_{n-1})=$$
$$=\text{Пор}\,(P_1P_2\ldots P_{n-1})-p+1+\text{Изм}\left(\frac{\mathfrak{W}}{P_1P_2\ldots P_{n-1}}\right)=$$
$$=(n-1)-p+1+(p-n+1)=1.$$

Введём обозначение

$$Q=P_1'P_2'\ldots P_{m-n+1}'$$

и применим теорему Нётера к последовательности точек, состоящую из периодически повторяющейся последовательности

$$P_1',P_2',\ldots,P_{m-n+1}';\quad P_1,P_2,\ldots,P_{n-1}.$$

На отрезке

$$P_1',\ P_2',\ \ldots,\ P_{m-n+1}'$$

первого периода мы в силу

$$\text{Изм}\,(Q)=1$$

получим $m-n+1$ пробелов. На остальной части первого периода мы в силу (16) не получим ни одного пробела.

Рассмотрим отрезок

$$P_1',\ P_2',\ \ldots,\ P_{m-n+1}',\ P_1$$

второго периода. На отрезке

$$P_2,\ \ldots,\ P_{n-1},\ P_1',\ \ldots,\ P_{m-n+1}',\ P_1 \tag{18}$$

в силу

$$\text{Изм}\,(P_2)=1,$$
$$\text{Изм}\,(P_2\ \ldots\ P_{n-1}\cdot P_1'\ \ldots\ P_{m-n+1}',\ P_1)=\text{Изм}\,\mathfrak{A}=n$$

встречается ровно $n-1$ непробелов. В силу (17) эти непробелы не встречаются на первых $n-2$ местах. Пусть дивизор

$$P_2\ \ldots\ P_{n-1}\ P_1'\ \ldots\ P_\alpha' \qquad (\alpha=1,\ 2,\ \ldots,\ m-n+2) \tag{19}$$

дает непробел. Это значит, что в поле $k(x,\ y)$ существует элемент, представляемый дивизором со знаменателем (19), причём $P_\alpha$ не сокращается с числителем. С другой стороны, в силу того, что класс $(QP_1)$ собственный, в поле $k(x,\ y)$ существует элемент,

представляемый дивизором со знаменателем $QP_1$, причём ни один из простых дивизоров знаменателя не сокращается с числителем. Беря произведение обоих элементов, мы убедимся, что отрезку

$$P_1', \ldots, P_{m-n+1}', P_1, P_2, \ldots, P_{n-1}, P_1', \ldots, P_\alpha'$$

соответствует непробел. Таким образом на отрезке

$$P_1', \ldots, P_{m-n+1}', P_1$$

второго периода встречается по крайней мере $n-1$ непробелов и, следовательно,

$$\leqslant (m-n+2)-(n-1) = r+1$$

пробелов.

Отрезок

$$P_2, \ldots, P_{n-1}$$

второго периода в силу (16) и того, что класс $\mathfrak{A}$ собственный, не даёт пробелов. Таким образом в рассматриваемой периодической последовательности точек первый период даёт $m-n+1$ пробелов, а каждый из последующих периодов не более $r+1$ пробелов.

Пусть в нашей последовательности все пробелы закончатся после $k$ полных периодов, так что $k$-й период пусть содержит хотя бы один пробел, а $(k+1)$-й вовсе не содержит пробелов. Из теоремы Нётера следует:

$$(m-n+1)+(k-1)(r+1) \geqslant \rho. \tag{20}$$

Кроме того, поскольку пробелы могут встречаться не далее, чем на $(2\rho-1)$-м месте, и в то же время в начале $k$-го периода непременно встретится хотя бы один пробел, мы имеем:

$$(k-1)\cdot m+1 \leqslant 2\rho-1. \tag{21}$$

Подставляя в (20) значение $k-1$:

$$k-1 \leqslant \frac{2\rho-2}{m},$$

получим

$$m(m-n+1)+(2\rho-2)(r+1) \geqslant m\rho,$$

откуда, подставляя

$$m = 2n+(r-2),$$

будем иметь

$$\rho \leqslant \frac{(2n+r-2)(n+r-1)-2r-2}{2n-(r+4)},$$

или

$$\rho \leqslant n+2r+\frac{3r(r+1)}{2n-r-4},$$

откуда и вытекает формула (15).

Особо отметим случай $r = 0$, в котором неравенство (15) принимает вид

$$\rho \leqslant n.$$

Отсюда следует:

$$m = 2n - 2 \geqslant 2\rho - 2.$$

Если при этом класс $\mathfrak{A}$ специален, то он должен совпадать с $\mathfrak{W}$. Итак:

Следствие. Если измерение и порядок специального класса $\mathfrak{A}$ связаны соотношением

$$\text{Пор}\,\mathfrak{A} = 2 \cdot \text{Изм}\,\mathfrak{A} - 2$$

и если $\mathfrak{A}$ содержит собственный класс порядка $m - n + 1$ и измерения 2, то $\mathfrak{A}$ есть класс дифференциалов.

*Примечание.* В ходе доказательства мы предположим, что $\mathfrak{A}$ есть собственный класс. Это предположение не ведёт к существенным ограничениям, так как в противном случае, сокращая класс $\mathfrak{A}$ на общий делитель, мы придём к собственному классу $\mathfrak{A}'$, тоже специальному, у которого измерение останется тем же, а порядок и, следовательно, число $r$ уменьшатся. Ограничение для $\rho$, наложенное при помощи формулы (15) для класса $\mathfrak{A}'$, более жёстко, чем то, которое мы бы получили, применяя формулу (15) непосредственно к классу $\mathfrak{A}$.

Перейдём к исследованию случаев, когда сделанное нами предположение не выполняется. В этих случаях, выбрав совершенно произвольно точки $P_1, P_2, \ldots, P_{n-1}$ и определяя в классе $\mathfrak{A}$ дивизор $QP_1P_2 \ldots P_{n-1}$, мы получим классы

$$(22) \qquad (QP_i) \qquad (i = 1, 2, \ldots, n-1).$$

из которых ни один не является собственным.

Пусть класс $(QP_1)$ имеет общим делителем точку $P_1'$; она не может быть общим делителем всех классов (22), так как в противном случае она была бы общим делителем всех дивизоров линейных семейств

$$(23) \qquad (QP_i)\,\frac{P_1P_2 \ldots P_{n-1}}{P_i} \qquad (i = 1, 2, \ldots, n-1).$$

Но линейными комбинациями этих дивизоров исчерпываются все дивизоры класса $\mathfrak{A}$. В самом деле, пусть в классе $(QP_i)$ содержится дивизор $R_i$, не делящийся на $P_i\,(i = 1, 2, \ldots, n-1)$. Тогда в семействах (23) можно выделить $n$ дивизоров

$$(24) \quad QP_1 \ldots P_{n-1}, \quad R_1 \cdot \frac{P_1 \ldots P_{n-1}}{P_1}, \; R_2 \cdot \frac{P_1 \ldots P_{n-1}}{P_2}, \; \ldots$$

$$\ldots, \; R_{n-1}\frac{P_1 \ldots P_{n-1}}{P_{n-1}},$$

лежащих в классе $\mathfrak{A}$. Они линейно независимы, так как, предположив между ними линейную зависимость

$$A_0QP_1 \dots P_{n-1} + \sum_{i=1}^{n-1} A_iR_i\frac{P_1 \dots P_{n-1}}{P_i} = 0,$$

мы из делимости всех слагаемых, кроме $R_i\frac{P_1 \dots P_{n-1}}{P_i}$, на $P_i$ заключаем, что

$$A_i = 0 \qquad (i = 1, 2, \dots, n-1).$$

Если бы $P_1'$ был общим делителем всех классов $(QP_i)$, то и $Q$ и все $R_i$ и, значит, все дивизоры (24) делились бы на $P_1'$. Следовательно, $P_1'$ был бы общим делителем класса $\mathfrak{A}$.

Пусть $A_1, A_2, \dots, A_n$ представляет собой систему линейно независимых дивизоров класса $\mathfrak{A}$ и пусть их частным соответствуют элементы поля $k(x, y)$:

$$\frac{A_2}{A_1} \asymp z_2, \quad \frac{A_3}{A_1} \asymp z_3, \quad \dots, \quad \frac{A_n}{A_1} \asymp z_n.$$

Специализируем $A_1, A_2, A_3$ так, чтобы они делились на простые дивизоры $P_3, \dots, P_{n-1}$, выбранные так, чтобы при их закреплении в классе $\mathfrak{A}$ получался класс измерения 3. Сократив семейство $(A_1, A_2, A_3)$ на $P_3 \dots P_{n-1}$, получим класс измерения 3. Соответствующее ему поле $k(z_2, z_3)$ порождается элементами $z_2, z_3$, которые пусть связаны уравнением

$$g(z_2, z_3) = 0. \tag{25}$$

Выберем точку $P_1$, на которую пусть не делится $A_1$ и которая пусть не соответствует особой точке кривой (25). Пусть $\zeta_2, \zeta_3$ будут значения элементов $z_2, z_3$ в точке $P_1$. Имеем:

$$z_2 - \zeta_2 \asymp \frac{A_2 - \zeta_2 A_1}{A_1}, \quad z_3 - \zeta_3 \asymp \frac{A_3 - \zeta_3 A_1}{A_1}.$$

Очевидно, что семейство $(A_2 - \zeta_2 A_1, A_3 - \zeta_3 A_1)$ по сокращении приводится к классу измерения 2, который получается из класса $\mathfrak{A}$ после закрепления точек $P_1, P_3, \dots, P_{n-1}$. В силу нашего предположения его общий наибольший делитель содержит простые дивизоры, отличные от $P_1, P_3, \dots, P_{n-1}$ и, в силу доказанного относительно точек $P_1$ и $P_2$, отличные от простых дивизоров, входящих одновременно в $A_1, A_2, A_3$. Допустим, что

$$k(z_2, z_3) = k(x, y).$$

$z_2 - \zeta_2$ и $z_3 - \zeta_3$ имеют общими делителями, кроме $P_1$, ещё другие дивизоры. Но тогда в силу теоремы 54 (см. ниже) точка $(\zeta_2, \zeta_3)$

есть особая точка кривой (25), что мы исключили. Таким образом $k(z_2, z_3)$ есть истинное подполе поля $k(x, y)$.

Более того: оказывается, что всё поле $k(z_2, z_3, \ldots, z_n)$ является истинным подполем поля $k(x, y)$. Для строгого доказательства этого факта понадобилось бы применение довольно тонких соображений теории Галуа, а потому мы ограничимся приведением интуитивного геометрического доказательства. Будем считать $z_2, z_3, \ldots, z_n$ координатами $(-1)$-мерного пространства. Считая их функциями от $x, y$, связанных алгебраическим уравнением, мы получим в этом пространстве кривую $L$. Предполагая, что

$$k(z_2, z_3, \ldots, z_n) = k(x, y),$$

мы должны считать кривую $L$ *простой*. Это означает, что различным точкам поля $k(x, y)$ будут соответствовать в общем случае (т. е. за исключением особых точек) различные точки кривой $L$. Закрепив на $L$ $n-1$ обыкновенных точек $P_1, P_2, \ldots, P_{n-1}$, мы определим проходящее через них $(n-2)$-мерное плоское многообразие, пересекающее кривую $L$ в дальнейших точках $P'_1, P'_2, \ldots, P'_{m-n+1}$. Выражаясь языком, к которому мы привыкли, элемент

$$\lambda_1 + \lambda_2 z_2 + \ldots + \lambda_n z_n,$$

где $\lambda_1, \lambda_2, \ldots, \lambda_n$ подобраны (с точностью до постоянного множителя) так, чтобы он обращался в нуль в точках $P_1, P_2, \ldots, P_{n-1}$, будет обращаться в нуль ещё в точках $P'_1, P'_2, \ldots, P'_{m-n+1}$.

Если мы предоставим точке $P_2$ свободно двигаться вдоль кривой $L$, то наше плоское многообразие опишет пучок многообразий, точки пересечения которых с $L$ опишут двумерное семейство дивизоров класса $\mathfrak{A}$ с закреплёнными точками $P_1, P_3, \ldots, P_{n-1}$. Согласно предположению, кроме точек $P_1, P_3, \ldots, P_{n-1}$, в этом семействе остаются неподвижными ещё некоторые точки. Это означает, что пучок наших плоских многообразий пересекает кривую $L$, кроме точек $P_1, P_3, \ldots, P_{n-1}$, ещё в нескольких неподвижных точках, одна из которых пусть будет $P'_1$. Поскольку они неподвижны, они должны лежать на всех наших плоских многообразиях, пересечение которых образует $(n-3)$-мерное плоское многообразие, однозначно определяемое точками $P_1, P_3, \ldots, P_{n-1}$. Будем называть такие многообразия *гиперпрямыми*.

Для большей наглядности дальнейшего доказательства предварительно проведём его для случая $n = 4$, который соответствует трёхмерному пространству. Здесь роль $(n-2)$-мерных плоских многообразий играют плоскости, проходящие через точки $P_1, P_2, P_3$, а роль гиперпрямых — прямые $P_1P_3$. Дано, что прямая $P_1P_3$, где $P_1$ и $P_3$ — произвольные точки кривой $L$, всегда проходит ещё через одну точку кривой $L$, которую мы будем обозначать через $P'_1$. Если

мы закрепим точку $P_1$ и заставим точку $P_3$ пробегать кривую $L$, то получим конус $K(P_1)=K_1$, каждая образующая которого, кроме вершины $P_1$, должна пересекать кривую $L$ ещё по крайней мере в двух точках. Докажем, что тогда кривая $L$ лежит в неподвижной плоскости. Доказательство было бы гораздо проще провести в том случае, если бы точки $P_1$, $P_3$, $P_1'$ пробегали три различные кривые $L_1$, $L_3$, $L_1'$. Чтобы притти к этому случаю, возьмём в качестве $L_1$ и $L_3$ произвольные малые отрезки кривой $L$, не имеющие общих точек, а в качестве $L_1'$ — отрезок, который пробегает точка $P_1'$ пересечения прямой $P_1P_3$ с кривой $L$, когда $P_1$ пробегает $L_1$, а $P_3 — L_3$. При этом выберем $L_1$ и $L_3$ настолько малыми, чтобы $L_1'$ не имела общих точек ни с $L_1$ ни с $L_3$. Фиксируем точку $P_1$ и заставим $P_3$ пробегать кривую $L_3$. Прямые $P_1P_3$ опишут конус $K_1$, на котором будет лежать часть $L_{11}'$ кривой $L_1'$. Переместим точку $P_1$ в положение $P_{12}$ на кривой $L_1$. Получим другой конус $K_2$, пересекающийся с $L_1'$ по отрезку $L_{12}'$. Перемещение сделаем настолько малым, чтобы отрезки $L_{11}'$ и $L_{12}'$ имели общую часть, которую мы обозначим через $L_{13}'$. Конусы $K_1$ и $K_2$, если они различны, пересекаются по кривой $L_3$ и, кроме того, как алгебраические поверхности могут иметь общими лишь конечное число образующих, которые в свою очередь могут пересекаться с $L_{13}'$ лишь в конечном числе точек. Но, поскольку $L_{13}'$ целиком лежит на обоих конусах, последние должны совпадать (точнее выражаясь, должны быть частями одного общего конуса); с другой стороны, единственным типом конуса, имеющего неопределённую вершину, является плоскость. Поскольку вершины совпадающих конусов $K_1$ и $K_2$ различны, оба они представляют собой плоскость. Беря на кривой $L$ всевозможные отрезки, мы убедимся, что вся кривая лежит на неподвижной плоскости.

Проведём аналогичное доказательство для $(n-1)$-мерного пространства. Выделим на кривой $L$ достаточно малые и не имеющие общих частей отрезки $L_1$ и $L_3$. Заставляя точку $P_1$ пробегать отрезок $L_1$, а точки $P_3, \ldots, P_{n-1}$ — независимо друг от друга отрезок $L_3$ и проводя через $P_1, P_3, \ldots, P_{n-1}$ гиперпрямые, мы, согласно условию, каждый раз будем получать по крайней мере ещё одно пересечение гиперпрямой с кривой $L$; обозначим одно из них через $P_1'$, и пусть оно описывает на кривой $L$ отрезок $L_1'$. Отрезки $L_1$ и $L_3$ пусть будут настолько малы, чтобы $L_1'$ не имел общих частей ни с $L_1$, ни с $L_3$. Фиксируем точку $P_1$. Тогда наши гиперпрямые опишут неплоское $(n-2)$-мерное многообразие (гиперконус) $K_1$, а точка $P_1'$ — лежащий на $L_1'$ отрезок $L_{11}'$. Сдвигая точку $P_1$ в положение $P_{12}$, мы точно таким же образом получим гиперконус $K_2$ и отрезок $L_{12}'$. Сдвиг $P_1$ в $P_{12}$ будем предполагать настолько малым, чтобы отрезки $L_{11}'$ $L_{12}'$ имели общую часть. Гиперконусы $K_1$ и $K_2$,

если они различны, могут иметь пересечением только направляющую $L_3$ и конечное число образующих гиперпрямых, которые отсекут на $L_1'$ конечное число точек. Так как, с другой стороны, они должны отсекать на $L_1'$ общую часть отрезков $L_{11}'$ и $L_{12}'$, то гиперконусы $K_1$ и $K_2$ должны иметь общую $(n-2)$-мерную часть. Но поскольку они имеют разные вершины $P_1$ и $P_{12}$, они должны содержать наименьшее плоское многообразие, проведённое через $P_1$ и $P_{12}$. Производя достаточное число сдвигов вершины $P_1$, мы придём к $(n-2)$-мерному плоскому многообразию, проходящему через каждый из получаемых гиперконусов. Но тогда каждый из них совпадёт с этим плоским многообразием. Таким образом отрезки кривой $L$ лежат на $(n-2)$-мерном плоском многообразии, ч. т. д. Аналитически это выражается так: элементы $z_2, z_3, \ldots, z_n$ связаны линейным соотношением

$$c_1 + c_2 z_2 + c_3 z_3 + \ldots + c_n z_n = 0 \tag{26}$$

с постоянными $c_1, c_2, c_3, \ldots, c_n$.

Проведённое рассуждение справедливо и для комплексных значений $z_2, z_3, \ldots, z_n$, поскольку условие их вещественности нигде не было использовано.

Соотношение (26) показывает, что не все дивизоры $A_1, A_2, \ldots, A_n$ линейно независимы, т. е. что измерение класса $\mathfrak{A}$ меньше $n$. Так как это противоречит нашему предположению, то наше предположение, что поле $k(z_2, z_3, \ldots, z_n)$ совпадает с $k(x, y)$, неверно: $k(z_2, z_3, \ldots, z_n)$ есть истинное подполе поля $k(x, y)$.

Представим через дивизоры элементы $z_2, z_3, \ldots, z_n$ внутри поля $k(z_2, z_3, \ldots, z_n)$. Ниже (в § 35) мы убедимся, что простой дивизор поля $k(z_2, z_3, \ldots z_n)$ представляется как произведение одного и того же числа, $k$, простых дивизоров поля $k(x, y)$. Таким образом классу $\mathfrak{A}$ в поле $k(z_2, z_3, \ldots, z_n)$ будет соответствовать класс $\mathfrak{A}'$, измерение которого останется тем же, а порядок уменьшится в $k$ раз:

$$n' = n, \quad m' = \frac{m}{k}.$$

При этом в силу доказанного класс $\mathfrak{A}'$ будет удовлетворять сделанному нами предположению, так как иначе образованное элементами $z_2, z_3, \ldots, z_n$ поле не могло бы совпадать с $k(z_2, z_3, \ldots, z_n)$.

Число $r'$ для класса $\mathfrak{A}'$ равно

$$r' = m' - 2n' + 2 = \frac{m - 2k(n-1)}{k}.$$

Но так как $k \geqslant 2$, то если мы учтём предположение (13), то получим:

$$r' \leqslant \frac{m-4n+4}{k} = \frac{2n-2+r-4n+4}{k} = \frac{-2n+r+2}{k} < -\frac{2}{k} < 0,$$

откуда в силу теоремы Клиффорда следует, что класс $\mathfrak{A}'$ не специален. Применяя к нему теорему Римана-Роха, получим для жанра $p'$

поля $k(z_2, z_3, \ldots, z_n)$ величину

$$\rho' = \text{Пор}\,\mathfrak{A}' - \text{Изм}\,\mathfrak{A}' + 1 = \frac{m - k(n-1)}{k} \leqslant \frac{m - 2(n-1)}{k} = \frac{r}{k}.$$

В частности, если принять $r = 0$, как это сделано у Клиффорда, то

$$\rho' = 0,$$

т. е. поле $k(z_2, z_3, \ldots, z_n)$ уникурсально. Отсюда также следует

$$k = 2.$$

Обращаясь опять к § 35, мы выведем отсюда, что относительный порядок поля $k(x, y)$ над $k(z_2, z_3, \ldots, z_n)$ равен 2. Но так как поле $k(z_2, z_3, \ldots, z_n)$ уникурсально, то отсюда следует, что $k(x, y)$ есть гиперэллиптическое поле. В этом состоит известное дополнение к теореме Клиффорда (например, см. [97], стр. 133).

Изложение обобщения теоремы Клиффорда, опубликованное в моей статье [103], содержит погрешности. Одна из основных идей изложенного здесь доказательства геометрической теоремы принадлежит А. П. Нордену, сообщившему мне её устно.

## § 27. Теорема Римана-Роха при произвольном числовом поле

В § 21 мы убедились, что при оговорённом там ограничении фундаментальный базис кольца $\mathfrak{Q}$ остаётся фундаментальным базисом после присоединения к полю $k(x, y)$ любого числового поля. Из этого мы вывели следствие, что показатели $r_1, r_2, \ldots, r_n$ элементов нормального базиса $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ тоже при этом останутся неизменными.

Пусть теперь $\mathfrak{A}$ будет произвольный класс дивизоров в поле $k(x, y)$ измерения $\geqslant 2$, $A$, $A'$, $A''$ — входящие в него целые дивизоры. Введём для элемента $\frac{A'}{A}$ обозначение $x$:

$$x \equiv \frac{A'}{A},$$

и построим, исходя от элемента $x$ как независимой переменной, нормальный базис. В § 22 мы видели, что

$$\text{Изм}\,\mathfrak{A} = s + 1, \tag{1}$$

где элементы $\lambda_1, \lambda_2, \ldots, \lambda_s$ имеют показателей $\leqslant 1$, в то время как $\lambda_{s+1}$ имеет показатель $> 1$.

Присоединим к $k(x, y)$ произвольное числовое поле $k_1$. Тогда в поле $k_1(x, y)$ базис $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ тоже будет нормальным, так что для класса $\mathfrak{A}$, рассматриваемого в поле $k_1(x, y)$, число $s$ будет иметь прежнее значение. Формула (1) показывает, что измерение класса $\mathfrak{A}$ в поле $k_1(x, y)$ останется тем же.

В частности, несобственный класс в поле $k(x, y)$ не может сделаться собственным в поле $k_1(x, y)$. В самом деле, пусть в поле $k(x, y)$ имеет место

$$\mathfrak{A} = M \cdot \mathfrak{A}_1,$$

где $\mathfrak{A}_1$ — уже собственный класс, и пусть в поле $k_1(x, y)$ $\mathfrak{A}$ содержит дивизор $A_1$, не делящийся на $M$. Тогда класс $\mathfrak{A}$ в поле $k_1(x, y)$ будет иметь большее измерение, чем в поле $k(x, y)$, что противоречит ранее доказанному.

Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — дополнительные друг к другу классы, содержащиеся в $k(x, y)$. Поскольку их порядки и измерения одни и те же в полях $k(x, y)$ и $k_1(x, y)$, а также равны друг другу жанры обоих полей, теорема Римана-Роха, справедливая для поля $k_1(x, y)$ (которое можно считать алгебраически замкнутым), имеет также место для поля $k(x, y)$, ч. т. д.

Доказанное справедливо только для расширений 1-го рода. Поэтому доказательство теоремы Римана-Роха должно быть проведено иначе в том случае, когда поле $k(x, y)$ имеет характеристику $p$ и притом некоторые из образующих его элементов входят в уравнения, связывающие их с другими элементами поля, в степенях, кратных $p$. Здесь мы должны отдельно рассмотреть два случая:

1) В поле $k(x, y)$ не существует пар элементов, входящих в связывающие их неприводимые уравнения в степенях, кратных $p$. Заметим, что если $k$ есть совершенное поле, то этот случай является единственно возможным. В самом деле, в § 8 мы убедились, что при совершенном поле $k$ полином $f(x^p, y^p)$ есть $p$-я степень некоторого полинома и поэтому не может быть неприводимым.

Пусть для поля $k(x, y)$ уравнение

$$f(x, y) = 0,$$

связывающее элементы $x$ и $y$, содержит $y$ в степенях, не кратных $p$. Это означает, что $k(x, y) : k(x)$ есть расширение 1-го рода. Тогда дискриминант поля $k(x, y)$ отличен от нуля, так что мы имеем возможность построить для него дополнительный базис и определить при его помощи класс дифференциалов. При проведении доказательства теоремы Римана-Роха все рассуждения останутся в силе, если заданный класс $\mathfrak{A}$ содержит по крайней мере два таких целых дивизора $A_1$, $A_2$, что, положив

$$x = \frac{A_1}{A_2},$$

мы придём к расширению $k(x, y) : k(x)$ 1-го рода. Такого рода класс может быть охарактеризован тем, что не все входящие в него целые дивизоры при надлежащем расширении числового поля $k$ могут быть представлены как $p$-е степени некоторых дивизоров, умноженные на общий делитель класса. Поэтому воспроизведём для этого

случая другое доказательство теоремы Римана-Роха, которое было предложено Гензелем и Ландсбергом ([51], стр. 301—304) и приспособлено для полей характеристики $p$ Шмидтом [93].

Выделим в классе $\mathfrak{A}$ произвольный дивизор $A$. Тогда измерение класса $\mathfrak{A}$ будет равно числу линейно независимых элементов поля $k(x, y)$, представляемых дивизорами, в знаменателях которых стоит только $A$. Выберем в качестве $x \asymp \frac{X_1}{X}$ элемент, знаменатель которого $X$ есть дивизор, не содержащий кратных множителей и взаимно простой с $A$. Построим нормальный базис относительно $x$ для кольца $\Omega$, состоящего из элементов, в знаменателях которых стоят первые степени $A$ и любые степени $X$. Пусть этот базис есть

$$[\lambda_1, \lambda_2, \ldots, \lambda_n] \tag{2}$$

и пусть

$$e_1 \leqslant e_2 \leqslant \ldots \leqslant e_n$$

— показатели его элементов, которые в данном случае могут быть и отрицательными. При этом показатель $e_i$ элемента $\lambda_i$ указывает, в какой степени $X$ входит в знаменатель его представления; если же $e_i < 0$, то $X$ входит в числитель представления $\lambda_i$ в $(-e_i)$-й степени.

Пусть

$$e_s \leqslant 0, \quad e_{s+1} > 0.$$

Тогда все элементы, представляемые дивизорами, имеющими в знаменателях только $A$, могут быть представлены в форме

$$c_1(x) \cdot \lambda_1 + c_2(x) \cdot \lambda_2 + \ldots + c_s(x) \cdot \lambda_s,$$

где $c_i(x)$ — полином не выше $(-e_i)$-й степени, который содержит $1 - e_i$ произвольных коэффициентов. Отсюда следует, что

$$\text{Изм}\,\mathfrak{A} = (1 - e_1) + (1 - e_2) + \ldots + (1 - e_s). \tag{3}$$

Рассмотрим базис

$$[\mu_1, \mu_2, \ldots, \mu_n], \tag{4}$$

дополнительный к базису (2). Модифицируя рассуждения § 20, мы убедимся, что (4) является базисом для элементов, содержащих в знаменателях только $Z_\infty$ и степени $X$, а в числителе непременно $A$.

Определим показатели элементов базиса (4). Для этого учтём, что в силу определения (3) § 12 показатель следа $S(\alpha)$ не превышает показателя элемента $\alpha$. Далее, из формул (15′) и (15″) § 20 мы получим

$$\mu_i = e_{i1}\lambda_1 + e_{i2}\lambda_2 + \ldots + e_{in}\lambda_n, \tag{5}$$

где

$$e_{ik} = \frac{\Delta_{ik}[\lambda_1, \lambda_2, \ldots, \lambda_n]}{\Delta[\lambda_1, \lambda_2, \ldots, \lambda_n]}, \tag{6}$$

$$\Delta[\lambda_1, \lambda_2, \ldots, \lambda_n] = \begin{vmatrix} S(\lambda_1^2), & S(\lambda_1\lambda_2), \ldots, S(\lambda_1\lambda_n) \\ S(\lambda_2\lambda_1), & S(\lambda_2^2), \ldots, S(\lambda_2\lambda_n) \\ \ldots\ldots\ldots\ldots\ldots \\ S(\lambda_n\lambda_1), & S(\lambda_n\lambda_2), \ldots, S(\lambda_n^2) \end{vmatrix}, \tag{7}$$

а $\Delta_{ik}[\lambda_1, \lambda_2, \ldots, \lambda_n]$ является минором этого определителя. Из формулы (14) § 12 следует, что степень (т. е. показатель) $\Delta[\lambda_1, \lambda_2, \ldots, \lambda_n]$ равна:

$$2(e_1 + e_2 + \ldots + e_n)$$

(здесь надо учесть, что в силу выбора дивизора $X$ имеет место $\delta_0 = 0$). С другой стороны, показатель элемента $S(\lambda_1\lambda_k)$ не превышает $e_i + e_k$, откуда следует, что показатель минора $\Delta_{ik}[\lambda_1, \lambda_2, \ldots, \lambda_n]$ не превышает

$$2(e_1 + e_2 + \ldots + e_n) - (e_i + e_k).$$

Из формулы (6) следует, что показатель элемента $e_{ik}$ не превышает

$$-(e_i + e_k).$$

Наконец, формула (5) показывает, что показатель элемента $\mu_i$ не превышает

$$-e_i.$$

Но из формулы (16) § 20 следует, что показатель определителя

$$\Delta[\mu_1, \mu_2, \ldots, \mu_n]$$

равен $-2(e_1 + e_2 + \ldots + e_n)$, что возможно лишь в том случае, если показатель $\mu_i$ в точности равен $-e_i$. Итак, показатели элементов базиса (4) равны соответственно

$$-e_1, \quad -e_2, \quad \ldots, \quad -e_n.$$

Измерение дополнительного класса

$$\mathfrak{W}/\mathfrak{A}$$

равно числу целых дивизоров, эквивалентных дивизору

$$\frac{Z_\infty}{X^2A}.$$

Другими словами, оно равно числу линейно независимых элементов, делящихся на $X^2A$ и содержащих в знаменателях только $Z_\infty$. Мы видели, что такие элементы представляются в форме

$$c_1(x) \cdot \mu_1 + c_2(x)\mu_2 + \ldots + c_n(x)\mu_n,$$

где $c_i(x)$ — полиномы, причём показатели таких элементов не должны превышать — 2.

Пусть

$$e_{s+1} = e_{s+2} = \ldots = e_t = 1, \quad e_{t+1} \geqslant 2.$$

Тогда нашему условию будут удовлетворять элементы

$$c_{t+1}(x)\,\mu_{t+1} + \ldots + c_n(x)\,\mu_n,$$

где $c_i(x)$ — полиномы, степень которых не превышает $e_i - 2$. Такие полиномы содержат $e_i - 1$ коэффициентов, в силу чего

$$\text{Изм } \mathfrak{B}/\mathfrak{A} = (e_{t+1} - 1) + \ldots + (e_n - 1);$$

эту формулу можно переписать так:

$$\text{Изм } \mathfrak{B}/\mathfrak{A} = (e_{s+1} - 1) + \ldots + (e_n - 1). \tag{8}$$

Вычитая из (7) (8), получим:

$$\text{Изм } \mathfrak{A} - \text{Изм } \mathfrak{B}/\mathfrak{A} = -(e_1 - 1) - (e_2 - 1) - \ldots - (e_n - 1) = \\ = -(e_1 + e_2 + \ldots + e_n) + n. \tag{9}$$

В § 20 мы видели, что степень $w_x$ дискриминанта фундаментального базиса равна:

$$2(r_1 + r_2 + \ldots + r_n)$$

[формула (19)]. В настоящем случае базис (2) есть не фундаментальный базис, а базис идеала $\frac{1}{A}$. В конце § 13 мы видели, что дискриминант базиса простого идеала равен дискриминанту поля, умноженному на квадрат линейного полинома от $x$. Распространяя эти рассуждения на наш случай и сравнивая степени дискриминантов, мы придём к формуле

$$2(e_1 + e_2 + \ldots + e_n) = w_x - 2. \text{ Пор } A. \tag{10}$$

Подставляя в формулу (9) и вспоминая, что

$$p = \frac{1}{2} w_x - n + 1,$$

мы придём к теореме Римана-Роха.

2) Этот приём ни к чему не приводит в том случае, когда в поле $k(x, y)$ существуют элементы, связанные неприводимыми уравнениями, в которых эти элементы входят в степенях, кратных $p$. В этом случае может и не существовать примитивной пары элементов, порождающей поле $k(x, y)$, так что мы сохраним обозначение $k(x, y)$ лишь как символ. Мы будем лишь предполагать, что число элементов,

порождающих поле $k(x, y)$, конечно. Тогда, расширяя числовое поле $k$ до $k^{\frac{1}{p}}$, мы сделаем некоторые из уравнений, связывающих порождающие поле элементы, приводимыми, так что степень поля $k(x, y) : k(x)$ уменьшится. Если при этом поле $k(x, y)$ останется полем типа 2), расширим числовое поле до $k^{\frac{1}{p^2}}$, и т. д. В силу конечности степени поля $k(x, y) : k(x)$ очевидно, что этот процесс приведёт к полю типа 1). Пусть $K = k(x, y)$ и $K_s = k^{\frac{1}{p^s}}(x, y)$ является полем типа 1). Тогда между классами полей $K$ и $K_s$ будет иметь место взаимно однозначное соответствие

$$\mathfrak{A} \longleftrightarrow \mathfrak{A}_s, \quad \mathfrak{B} \longleftrightarrow \mathfrak{B}_s, \quad \ldots$$

В частности, в поле $K$ класс дифференциалов $\mathfrak{W}$ не поддаётся непосредственному определению, так как все соотношения между дифференциалами элементов этого поля являются тождествами. Поэтому под классом $\mathfrak{W}$ мы будем разуметь класс, соответствующий классу дифференциалов $\mathfrak{W}_s$ поля $K_s$.

Наряду с полями $K$ и $K_s$ введём в рассмотрение промежуточные поля

$$K_1 = k^{\frac{1}{p}}(x, y), \quad \ldots, \quad K_{s-1} = k^{\frac{1}{p^{s-1}}}(x, y).$$

Между простыми дивизорами $P_\nu$, $P_{\nu+1}$ соседних полей $K_\nu$, $K_{\nu+1}$ ($\nu = 0, 1, \ldots, s-1$) будет иметь место соответствие

$$P_\nu \longleftrightarrow P_{\nu+1};$$

однако поскольку степень поля $K_{\nu+1}$ в $p$ раз ниже степени поля $K_\nu$, вес дивизора $P_{\nu+1}$ в $p$ раз меньше, чем вес дивизора $P_\nu$, причём норма дивизора $P_\nu$ есть $p$-я степень нормы дивизора $P_{\nu+1}$ (обе являются неприводимыми полиномами в своём числовом поле).

Отсюда следует, что порядок любого дивизора $A_\nu$ поля $K_\nu$ в $p$ раз превышает порядок соответствующего дивизора $A_{\nu+1}$ поля $K_{\nu+1}$, в силу чего

$$\text{Пор } \mathfrak{A}_\nu = p \cdot \text{Пор } \mathfrak{A}_{\nu+1}. \tag{11}$$

Для вывода теоремы Римана-Роха необходимо ещё установить зависимость между измерениями классов $\mathfrak{A}_\nu$ и $\mathfrak{A}_{\nu+1}$, которая по всей вероятности, такова:

$$\text{Изм } \mathfrak{A}_\nu - 1 = p\,(\text{Изм } \mathfrak{A}_{\nu+1} - 1). \tag{12}$$

В настоящее время я не располагаю полным выводом этой зависимости, в силу чего я ограничусь её проверкой на простейшем примере,

Пусть в классе $\mathfrak{A}$ содержатся дивизоры $A$, $A'$, $A''$, ...; пусть элементы

$$x \equiv \frac{A'}{A}, \quad y \equiv \frac{A''}{A}$$

составляют примитивную пару рассматриваемого поля $K$ и связаны зависимостью

$$x^{np} + y^{np} - w = 0, \tag{13}$$

где $p$ — характеристика поля $K$, $w$ — элемент числового поля $k$, из которого пусть не извлекается корень $p$-й степени. В поле $k^{\frac{1}{p}}$ тогда будет содержаться элемент

$$v = w^{\frac{1}{p}},$$

так что в поле $k^{\frac{1}{p}}$ левая часть уравнения (13) есть $p$-я степень полинома

$$x^n + y^n - v.$$

Пусть в поле $K_1 = k^{\frac{1}{p}}(x, y)$ классу $\mathfrak{A}$ соответствует класс $\mathfrak{A}_1$. Мы знаем [см. (6) § 22], что

$$\text{Изм } \mathfrak{A}_1 = s_1 + 1,$$

где $s_1$ — число элементов нормального базиса поля $K_1 : k^{\frac{1}{p}}(x)$, показатели которых не превышают единицы. Поскольку нормальным базисом является $[1, y, y^2, \ldots, y^{n-1}]$ и показатель элемента $y$ есть 1, мы имеем:

$$s_1 = 2.$$

С другой стороны,

$$\text{Изм } \mathfrak{A} = s + 1,$$

где $s$ является аналогичным числом для поля $K$. Но в нём элемент $x^n + y^n$ имеет показатель нуль, в силу чего в качестве элементов нормального базиса поля $K : k(x)$ можно взять

$$(x^n + y^n)^\mu \cdot y^\nu \qquad (\mu = 0, 1, \ldots, p-1; \ \nu = 0, 1, \ldots, n-1).$$

Из этих элементов показатели $\leqslant 1$ имеют те, у которых $\nu = 0$ или $\nu = 1$, в силу чего

$$s = 2 \cdot p = p \cdot s_1,$$

так что

$$\text{Изм } \mathfrak{A} - 1 = p\,(\text{Изм } \mathfrak{A}_1 - 1).$$

Считая соотношение (12) выведенным, мы обычным способом придём к теореме Римана-Роха

$$(14)\qquad \text{Изм } \mathfrak{A}_s - \frac{1}{2}\cdot \text{Пор } \mathfrak{A}_s = \text{Изм } \mathfrak{W}_s/\mathfrak{A}_s - \frac{1}{2}\cdot \text{Пор}\cdot \mathfrak{W}_s/\mathfrak{A}_s.$$

Соотношения (11) и (12) дадут:

$$(15)\qquad \text{Пор } \mathfrak{A} = p^s\cdot \text{Пор } \mathfrak{A}_s,\ \text{Пор } \mathfrak{W}/\mathfrak{A} = p^s\cdot \text{Пор } \mathfrak{W}_s/\mathfrak{A}_s,$$

$$(16)\qquad \text{Изм } \mathfrak{A}-1 = p^s\cdot(\text{Изм } \mathfrak{A}_s-1),\ \text{Изм } \mathfrak{W}/\mathfrak{A}-1 = p^s(\text{Изм } \mathfrak{W}_s/\mathfrak{A}_s-1);$$

из соотношения (14) мы получим равенство

$$(17)\qquad \text{Изм } \mathfrak{A} - \frac{1}{2}\cdot \text{Пор } \mathfrak{A} = \text{Изм } \mathfrak{W}/\mathfrak{A} - \frac{1}{2}\ \text{Пор } \mathfrak{W}/\mathfrak{A},$$

которое представляет теорему Римана-Роха для поля $K$.

Если $\rho_s$ есть жанр поля $K_s$, т. е. измерение класса $\mathfrak{W}_s$, то измерение $\rho$ класса $\mathfrak{W}$ найдётся по формулам (16):

$$(18)\qquad \rho - 1 = p^s\cdot(\rho_s - 1).$$

Применяя формулы (15) и (18), мы получим:

$$\text{Пор } \mathfrak{W} = p^s\cdot(2\rho_s - 2) = 2\rho - 2.$$

Шмидт (94) вывел для общего поля $K$ формулу (17), но не указал связи между жанрами полей $K$ и $K_s$.

ГЛАВА V

# СТРУКТУРА ПОЛЕЙ АЛГЕБРАИЧЕСКИХ ФУНКЦИЙ

## § 28. Понятие группы преобразований

Не излагая основ общей теории групп, с которой можно познакомиться по многим руководствам, ограничимся определением *группы преобразований*.

Задано множество $\mathfrak{M}$ объектов, которые мы будем обозначать через $M_1$, $M_2$, $M_3$, ... и назовём *элементами* множества. Под *преобразованием* мы будем разуметь сопоставление каждого элемента множества $\mathfrak{M}$ с определённым элементом того же множества. Таким образом понятие преобразования есть частный вид понятия функции в смысле Дирихле (G. Lejeune-Dirichlet), который под функцией понимал сопоставление объектов множества с определёнными объектами, вообще говоря, другого множества.

*Пример* 1. Пусть множество $\mathfrak{M}$ состоит из конечного числа объектов, которые мы занумеруем цифрами 1, 2, ..., $n$. Сопоставление каждой цифре $i$ цифры $\alpha_i$ той же последовательности является преобразованием; его принято называть *подстановкой* и записывать в виде

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}.$$

Если цифры $\alpha_1$, $\alpha_2$, ..., $\alpha_n$ ни разу не повторяются, мы будем называть подстановку обратимой. В дальнейшем мы будем иметь дело только с обратимыми подстановками.

*Пример* 2. Множество $\mathfrak{M}$ состоит из всех вещественных чисел и числа $\infty$. Сопоставление каждому числу $x$ числа

$$\frac{ax+b}{cx+d},$$

где $a$, $b$, $c$, $d$ — вещественные числа, причём

$$ad - bc \neq 0$$

есть преобразование; оно называется *дробной линейной подстановкой*.

Под *произведением* $AB$ двух преобразований $A$, $B$ мы будем разуметь следующее. Пусть преобразование $B$ переводит каждый

элемент $M$ множества $\mathfrak{M}$ в элемент $M'$ того же множества, а преобразование $A$ переводит элемент $M'$ в элемент $M''$. Тогда преобразованием $AB$ мы будем называть преобразование, переводящее каждый элемент $M$ в $M''$.

Введём обозначения, заимствованные из теории функций: пусть преобразование $B$ переводит $M$ в $f(M)$ и пусть преобразование $A$ переводит $M$ в $g(M)$:

$$A \mid \quad M \to g(M), \tag{1}$$

$$B \mid \quad M \to f(M). \tag{2}$$

Тогда преобразование $AB$ будет переводить $M$ в $g\{f(M)\}$:

$$AB \mid \quad M \to g\{f(M)\}.$$

Операция умножения преобразований подчиняется *ассоциативному закону*. Это означает, что

$$A(BC) = (AB)C. \tag{3}$$

В справедливости его можно убедиться следующим образом. Пусть наряду с (1) и (2) имеет место

$$C \mid \quad M \to h(M). \tag{4}$$

Тогда

$$BC \mid \quad M \to f\{h(M)\},$$

откуда

$$A(BC) \mid M \to g[f\{h(M)\}],$$

а с другой стороны,

$$(AB)C \mid \quad M \to g[f\{h(M)\}].$$

Таким образом оба преобразования $A(BC)$ и $(AB)C$ переводят каждый элемент $M$ множества $\mathfrak{M}$ в один и тот же элемент. Это и значит, что оба преобразования совпадают, ч. т. д.

Заметим, что коммутативный (перестановочный) закон, вообще говоря, не имеет места, т. е.

$$AB \neq BA. \tag{5}$$

Можно убедиться в этом на простом примере. Пусть

$$A \mid \quad x \to x + 1,$$

$$B \mid \quad x \to 2x + 1.$$

Тогда

$$AB \mid \quad x \to (2x + 1) + 1 = 2x + 2,$$

$$BA \mid \quad x \to 2(x + 1) + 1 = 2x + 3.$$

Эти преобразования, очевидно, отличны друг от друга.

Будем теперь рассматривать отдельные преобразования множества $\mathfrak{M}$ как особые объекты. Множество $G$ преобразований, обладающее тем свойством, что из

$$A \subset G, \quad B \subset G$$

всегда вытекает

$$AB \subset G$$

(другими словами, всякое произведение преобразований, входящих в $G$, тоже входит в $G$), называется *ассоциативной системой* преобразований.

*Пример.* Множество преобразований

$$A \mid \quad x \to ax + b, \tag{6}$$

где $a$, $b$ — целые рациональные числа, как нетрудно убедиться, составляет ассоциативную систему. Другую ассоциативную систему мы получим, если наложим на коэффициенты $a$ дополнительное требование быть нечётными. Вторая из этих систем является подмножеством первой или, как мы будем говорить, её *подсистемой*.

Множество же преобразований (6), в которых оба числа $a$ и $b$ нечётны, уже не составляет ассоциативной системы. В самом деле, пусть (6) и

$$B \mid \quad x \to a'x + b' \tag{7}$$

будут такого рода преобразования. Тогда

$$AB \mid \quad x \to aa'x + (ab' + b).$$

Но если $a$, $b'$, $b$ нечётны, то коэффициент $ab' + b$ должен быть чётным, так что преобразование $AB$ не входит в систему.

В дальнейшем мы будем постоянно пользоваться более узким понятием, чем ассоциативные системы — понятием *группы*. Для этого мы должны ввести два новых понятия: *единичного* (тождественного) преобразования и *обратного* преобразования.

Единичным называется преобразование, переводящее каждый элемент множества $\mathfrak{M}$ в самого себя. Будем обозначать его через $\mathfrak{E}$:

$$\mathfrak{E} \mid \quad M \to M.$$

Если $A$ есть произвольное преобразование рассматриваемой системы, то имеют место очевидные соотношения

$$A\mathfrak{E} = A, \tag{8}$$

$$\mathfrak{E}A = A. \tag{9}$$

Эти соотношения формулируются словами так: преобразование $\mathfrak{E}$ является *правой единицей* и оно же является *левой единицей* системы.

Пусть дано преобразование $A$, переводящее каждый элемент $M$ множества $\mathfrak{M}$ в элемент $M'$. Будем называть *обратным* преобразование (будем обозначать символом $A^{-1}$), дающее при умножении на $A$ единичное преобразование

$$A \cdot A^{-1} = \mathfrak{E}. \tag{10}$$

Преобразование $A^{-1}$, если оно существует, переводит элемент $M'$ (в который преобразование $A$ перевело $M$) обратно в $M$. Для того чтобы обратное к $A$ преобразование существовало, необходимо и достаточно, чтобы

1) при пробегании элементом $M$ множества $\mathfrak{M}$ элемент $M'$ также пробегал всё множество $\mathfrak{M}$ без пропусков;

2) различным $M$ соответствовали различные $M'$.

При несоблюдении первого условия преобразование $A^{-1}$ остаётся вообще неопределённым, так как тогда в множестве $\mathfrak{M}$ будут содержаться элементы $M'$, в которые преобразование $A$ не будет переводить никаких элементов; тогда $A^{-1}$ не может переводить такой элемент $M'$ ни в какой элемент. При несоблюдении же второго условия преобразование $A^{-1}$ не может быть определённым (однозначным), поскольку оно должно переводить один и тот же элемент в несколько различных элементов.

В том случае, если $\mathfrak{M}$ — конечное множество, каждое из условий 1) и 2) является следствием другого. Если они соблюдены, т. е. если все $\alpha_1, \alpha_2, \ldots, \alpha_n$ различны, где

$$A = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix},$$

то

$$A^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

При этом подстановку $A^{-1}$ можно записать так, чтобы в верхней строке цифры стояли в первоначальном порядке: 1, 2, ..., $n$. Для этого надо переставить цифры верхней строки в упомянутом порядке, а под каждой из них подписывать ту цифру, в какую она переводится.

*Пример.* Пусть

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Тогда

$$A^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Однако если $\mathfrak{M}$ есть бесконечное множество, то условия 1) и 2) независимы друг от друга. Приводимый ниже пример показывает,

что одно из этих условий может быть соблюдено без соблюдения другого.

*Пример.* Пусть

$$A \mid \quad x \to x^2.$$

Если множество $\mathfrak{M}$ элементов $x$ состоит из натуральных чисел, то условие 1) не соблюдается, так как натуральный ряд не исчерпывается квадратами, условие же 2) соблюдено.

Пусть теперь множество $\mathfrak{M}$ состоит из всех комплексных чисел. Тогда условие 1) будет соблюдено, условие же 2) — нет.

Наряду с (10) имеет также место

$$A^{-1} \cdot A = \mathfrak{E}. \tag{11}$$

Это может быть формулировано словами так: правый обратный элемент в то же время является левым обратным элементом.

Отметим важную формулу

$$(AB)^{-1} = B^{-1} \cdot A^{-1}. \tag{12}$$

В её справедливости можно убедиться, умножая $AB$ на $B^{-1} \cdot A^{-1}$:

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = A\mathfrak{E}A^{-1} = AA^{-1} = \mathfrak{E}.$$

Ассоциативная система называется *группой*, если 1) она содержит единичное преобразование, 2) наряду с каждым преобразованием $A$ она содержит также обратное преобразование $A^{-1}$.

*Пример* 1. Пусть $\mathfrak{M}$ состоит из $n$ цифр 1, 2, ..., $n$. Совокупность подстановок, переводящих 1, 2, ..., $n$ в каждое из $n!$ различных расположений этих цифр, составляет группу, которая называется *симметрической группой* из $n$ элементов и обозначается символом $\gamma_n$.

*Пример* 2. Совокупность дробных линейных подстановок

$$x \to \frac{ax+b}{cx+d}, \tag{13}$$

где $a$, $b$, $c$, $d$ пробегают всевозможные вещественные значения, для которых

$$ad - bc \neq 0 \tag{14}$$

составляет, как нетрудно убедиться, группу. Такая же совокупность, где $a$, $b$, $c$, $d$ пробегают всевозможные целые значения с соблюдением (14), составляет другую группу, входящую, как часть, в первую и потому называемую её *подгруппой* (или *делителем*). Подчиняя $a$, $b$, $c$, $d$ новому ограничению

$$ad - bc = 1,$$

мы получим новую подгруппу второй (и тем более первой) группы.

*Пример* 3. Элементы любого поля составляют группу относительно операции сложения. Те же элементы, за исключением элемента нуль, составляют группу относительно операции умножения. Обе группы коммутативны.

## § 29. Подгруппы, смежные классы, нормальные делители

Пусть $G$ — какая-нибудь группа, $\mathfrak{H}$ — её подгруппа, т. е. часть совокупности $G$, элементы которой тоже составляют группу. Пусть $A$ — какое-нибудь преобразование группы $G$. Если мы умножим слева каждое преобразование группы $\mathfrak{H}$ на $A$, то получим совокупность некоторых элементов группы $G$, которую мы будем обозначать символом

$$A\mathfrak{H}$$

и называть *смежным классом* группы $G$ по подгруппе $\mathfrak{H}$. Имеет место

Теорема 49. *Два смежных класса*

$$A\mathfrak{H},\quad B\mathfrak{H}$$

*или целиком совпадают, или не содержат общих элементов.*

Доказательство. Пусть $A\mathfrak{H}$ и $B\mathfrak{H}$ содержат общий элемент $C$:

$$C\subset A\mathfrak{H},\quad C\subset B\mathfrak{H}.$$

Это означает, что элемент $C$ может быть представлен так:

$$C=AH,\quad C=BH',$$

где под $H$, $H'$, $H''$, ... мы разумеем преобразования, входящие в группу $\mathfrak{H}$. Отсюда получим:

$$B=AHH'^{-1}=AH''.$$

Таким образом

$$B\mathfrak{H}=AH''\mathfrak{H}=A\mathfrak{H},$$

так как умножение $\mathfrak{H}$ на элемент $H''\subset\mathfrak{H}$ даёт $\mathfrak{H}$. Оба смежных класса $A\mathfrak{H}$ и $B\mathfrak{H}$ совпадают, ч. т. д.

Совокупность всех смежных классов группы $G$ по $\mathfrak{H}$, очевидно, содержит все элементы группы $G$. Отсюда для конечных групп можно получить важные следствия.

Назовём *порядком* конечной группы $G$ (Пор $G$) число различных преобразований, которые она содержит. Далее, назовём *индексом* подгруппы $\mathfrak{H}$ относительно $G$ и обозначим символом

$$(G:\mathfrak{H})$$

число смежных классов группы $G$ по подгруппе $\mathfrak{H}$.

Пусть $(G:\mathfrak{H}) = \nu$. Это значит, что существует всего $\nu$ смежных классов

$$\mathfrak{H},\ A_2\mathfrak{H},\ \ldots,\ A_\nu\mathfrak{H},$$

и всякий элемент группы $G$ входит в один и только один из этих смежных классов. Отсюда следует:

$$\text{Пор } G = \text{Пор } \mathfrak{H} \cdot (G:\mathfrak{H}). \tag{1}$$

Из этой формулы вытекают как простые следствия две следующие важные теоремы:

Теорема 50 (Лагранжа). *Порядок всякой подгруппы есть делитель порядка группы.*

Теорема 51. *Если группа $G$ содержит конечную группу $\mathfrak{H}$ и если индекс $(G:\mathfrak{H})$ конечен, то сама группа $G$ конечна.*

*Примечание.* Может случиться, что и группа $G$ и её подгруппа $\mathfrak{H}$ бесконечны, а индекс $(G:\mathfrak{H})$ конечен. В виде примера рассмотрим совокупность целых чисел, положительных и отрицательных, как группу относительно сложения. Лучше представить себе её как группу преобразований вида

$$A \mid \quad x \to x + a, \tag{2}$$

где $x$ пробегает совокупность целых чисел, а $a$ — какое-нибудь целое число. Если дано другое преобразование

$$B \mid \quad x \to x + b, \tag{3}$$

то

$$AB = BA \mid x \to x + (a + b).$$

Группа этих преобразований, называемая *группой параллельных переносов*, обладает свойством коммутативности $(AB = BA)$; группы, обладающие этим свойством, носят название *коммутативных* или *абелевых*.

В качестве подгруппы $\mathfrak{H}$ рассмотрим совокупность преобразований вида (2), коэффициенты которых $a$ делятся на фиксированное целое число $n$:

$$H \mid x \to x + n \cdot h.$$

Чтобы образовать смежные классы, выделим $n$ преобразований

$$A_k \mid x \to x + k \qquad (k = 0, 1, \ldots, n-1).$$

Смежный класс $A_k\mathfrak{H}$ состоит из преобразований

$$A_k H \mid x \to x + (nh + k),$$

где $h$ пробегает всевозможные целые значения.

Всякий элемент $A$ группы $G$ входит в один из смежных классов

$$\mathfrak{H},\ A_1\mathfrak{H},\ A,\ \mathfrak{H},\ \ldots,\ A_{n-1}\mathfrak{H}.$$

Чтобы узнать, в какой именно, надо разделить коэффициент $a$ на $n$, и остаток от деления и укажет номер смежного класса. Таким образом индекс $(G:\mathfrak{H})=n$, т. е. конечен.

Группа, состоящая из всевозможных положительных и отрицательных степеней одного и того же преобразования $A$, носит название *циклической группы*. При этом под степенью $A^n\,(n>0)$ мы будем разуметь

$$\overbrace{A\cdot A\ldots A}^{n\ \text{раз}},$$

а под $A^{-n}\,(n>0)$ — $n$-ю степень обратного элемента $A^{-1}$. Кроме того, под $A^0$ мы разумеем $\mathfrak{E}$.

Ясно, что циклическая группа абелева.

Если преобразование $A$ является элементом какой-нибудь конечной группы $G$, то элементы

$$A,\ A^2,\ A^3,\ \ldots$$

не могут быть различны. Пусть

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

Отсюда

$$A^p=\mathfrak{E}. \tag{4}$$

Назовём наименьший положительный показатель $p$, при котором имеет место (3), *порядком* (или *периодом*) преобразования $A$. Вместе с тем $p$ есть порядок циклической группы, образованной степенями преобразования $A$:

$$A^0=\mathfrak{E},\ A,\ A^2,\ \ldots,\ A^{p-1}.$$

Из теоремы 50 вытекает

Теорема 52. *Порядок элемента конечной группы есть делитель порядка группы.*

Будем говорить, что мы производим *преобразование* $S$ над элементами группы $G$, если мы заменяем каждый её элемент $A$ элементом $SAS^{-1}$:

$$A\to SAS^{-1}.$$

Если мы подвергаем преобразованию $S$ все элементы подгруппы $\mathfrak{H}$, то получающаяся при этом совокупность

$$S\mathfrak{E}S^{-1}=\mathfrak{E},\ SHS^{-1},\ SH'S^{-1},\ SH''S^{-1},\ \ldots,$$

обозначаемая символом $S\mathfrak{H}S^{-1}$, тоже составляет группу, так как из

$$H\cdot H'=H''$$

следует

$$SHS^{-1}\cdot SH'S^{-1}=SH''S^{-1}$$

и, кроме того, в силу (12)

$$(SHS^{-1})^{-1} = SH^{-1}S^{-1}.$$

Группа $S\mathfrak{H}S^{-1}$ называется *сопряжённой* с $\mathfrak{H}$ *подгруппой*.

Существуют подгруппы, совпадающие со своими сопряжёнными подгруппами. Такие подгруппы носят название *нормальных делителей* (или *инвариантных подгрупп*).

*Пример* 1. Симметрическая группа $\gamma_3$ трёх символов 1, 2, 3 состоит из шести подстановок:

$$\mathfrak{E} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad A = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \quad B = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad C = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$

$$D = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \quad F = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

Она имеет подгруппу

$$\mathfrak{E},\ A,$$

которая не является её нормальным делителем, так как её сопряжёнными подгруппами являются

$$\mathfrak{E},\ B;\quad \mathfrak{E},\ C.$$

Кроме того, группа $\gamma_3$ имеет подгруппу

$$\mathfrak{E},\ D,\ F,$$

которая является нормальным делителем группы $\gamma_3$. В самом деле, нетрудно убедиться, что

$$ADA^{-1} = F,\quad AFA^{-1} = D,\quad BDB^{-1} = F,\quad BFB^{-1} = D,\quad \ldots$$

*Пример* 2. Группа $G$ преобразований

$$S \mid x \to ax + b,$$

где $a$, $b$ пробегают всевозможные вещественные значения, причём $a \neq 0$, имеет подгруппу $\mathfrak{H}$:

$$H \mid x \to x + k.$$

Группа $\mathfrak{H}$ есть нормальный делитель группы $G$. В самом деле,

$$SHS^{-1} = (x \to ax + b)(x \to x + k)\left(x \to \frac{x-b}{a}\right) =$$

$$= (x \to ax + ak + b)\left(x \to \frac{x-b}{a}\right) = (x \to x + ak).$$

Это преобразование лежит в $\mathfrak{H}$, поскольку коэффициент при $x$ в правой части равен единице. Кроме того, если $H$ пробегает всю группу $\mathfrak{H}$, т. е. если $k$ пробегает все вещественные значения, то $SHS^{-1}$ тоже

пробегает всю группу $\mathfrak{H}$, поскольку $ak$ пробегает все вещественные значения вместе с $k$.

Преобразование группы при помощи $S$ можно представить как преобразование множества $\mathfrak{M}$ при помощи того же $S$. Пусть преобразование $A$ группы $G$ переводит элемент $M$ в $M'$. Какое преобразование переведёт $S(M)$ в $S(M')$? Применяя к $S(M)$ преобразование $SAS^{-1}$, будем иметь:

$$SAS^{-1}(S(M)) = SA(M) = S(M').$$

Итак:

*Если элементы $M$ множества $\mathfrak{M}$ подвергаются преобразованиям группы $G$ и $S$ — обратимое преобразование, то элементы $S(M)$ подвергнутся преобразованиям группы $SGS^{-1}$.*

## § 30. Автоморфизм и гомоморфизм. Факторгруппы

Пусть заданы две группы $\mathfrak{G}$ и $\mathfrak{g}$, природа элементов в которых нас не интересует. Это могут быть преобразования отличных друг от друга множеств, могут быть даже заданы абстрактно, т. е. при помощи символов, обозначающих элементы, с указанием, какой символ будет получаться в результате перемножения заданных символов. Пусть каждому элементу $A$, $B$, $C$, ... группы $\mathfrak{G}$ мы можем сопоставить определённый элемент группы $\mathfrak{g}$:

$$A \to a,\ B \to b,\ C \to c,\ \ldots$$

и пусть при этом всякий раз, когда

$$AB = C,$$

мы будем иметь также

$$ab = c.$$

В частности,

$$A^{-1} \to a^{-1}.$$

Такое соответствие носит название *гомоморфизма* и обозначается символом

$$\mathfrak{G} \to \mathfrak{g}. \tag{1}$$

Если такое соответствие возможно установить между двумя заданными группами $\mathfrak{G}$ и $\mathfrak{g}$ (может быть, не единственным образом), то говорят, что группа $\mathfrak{g}$ *гомоморфна* группе $\mathfrak{G}$.

Гомоморфизм не является обратимым понятием: из (1) вовсе не следует $\mathfrak{g} \to \mathfrak{G}$. Может случиться, что различным элементам группы $\mathfrak{G}$ будет соответствовать один и тот же элемент группы $\mathfrak{g}$. Если же между обеими группами можно установить такое соответствие, при котором различным элементам группы $\mathfrak{G}$ будут соответствовать различные элементы группы $\mathfrak{g}$, и притом этим соответствием будут охвачены все элементы группы $\mathfrak{g}$, то соответствие делается взаимным.

В этом случае оно называется *изоморфизмом* и обозначается символом

$$\mathfrak{G} \longleftrightarrow \mathfrak{g}, \quad \mathfrak{g} \longleftrightarrow \mathfrak{G}. \tag{2}$$

Группы, между которыми можно установить изоморфизм, называются *изоморфными группами*. С точки зрения абстрактной теории групп изоморфные группы не считаются различными. Свойства группы, не связанные с характером преобразований, составляющих группу, и называемые структурными свойствами группы, сохраняются для всех изоморфных групп. Выразимся точнее:

Всякое свойство группы, сохраняющееся для всех изоморфных с нею групп, называется её *структурным свойством*.

К числу структурных свойств групп принадлежат следующие свойства (предлагаем читателю убедиться в этом самостоятельно):

1) свойство группы быть абелевой,
2) порядок конечной группы,
3) число различных подгрупп,
4) число различных нормальных делителей.

Обратимся теперь к детальному исследованию гомоморфизма. Пусть между группами $\mathfrak{G}$, $\mathfrak{g}$ установлено соответствие (1), причём пусть различным элементам $A$, $B$ группы $\mathfrak{G}$ соответствует один и тот же элемент $a$ группы $\mathfrak{g}$:

$$A \to a, \quad B \to a.$$

Тогда элементу $AB^{-1} = C$, отличному от $\mathfrak{E}$, будет соответствовать единичный элемент $e$ группы $\mathfrak{g}$:

$$C \to e.$$

Обозначим через $\mathfrak{H}$ совокупность элементов группы $\mathfrak{G}$, которым в группе $\mathfrak{g}$ соответствует $e$. Тогда

1. $\mathfrak{H}$ есть группа. В самом деле, пусть $A \subset \mathfrak{H}$, $B \subset \mathfrak{H}$. Отсюда $A \to e$, $B \to e$, откуда следует $AB \to e$, в силу чего $AB \subset \mathfrak{H}$. Кроме того, из $A \subset \mathfrak{H}$ следует $A \to e$, откуда $A^{-1} \to e$ и $A^{-1} \subset \mathfrak{H}$.

2. $\mathfrak{H}$ есть нормальный делитель группы $\mathfrak{G}$. В самом деле, пусть $S \subset \mathfrak{G}$, $S \subset a$. Если $H \subset \mathfrak{H}$, то $H \to e$, откуда $SHS^{-1} \to a \cdot e \cdot a^{-1} = e$, в силу чего $SHS^{-1} \subset \mathfrak{H}$.

3. Чтобы два элемента $A$, $B$ группы $\mathfrak{G}$ соответствовали одному и тому же элементу группы $\mathfrak{g}$, необходимо и достаточно, чтобы они лежали в одном и том же смежном классе разложения $\mathfrak{G}$ по $\mathfrak{H}$. В самом деле, пусть $A \to a$, $B \to a$. Тогда $AB^{-1} \to e$, т. е. $AB^{-1} \subset \mathfrak{H}$, откуда $A \subset B\mathfrak{H}$, и отсюда $A\mathfrak{H} = B\mathfrak{H}$. Обратно, пусть $A\mathfrak{H} = B\mathfrak{H}$. Тогда, если $A \to a$, то из $B = AH$, где $H \subset \mathfrak{H}$, следует $B \to ae = a$.

Эти теоремы описывают гомоморфизм самого общего типа. В самом деле, пусть $\mathfrak{H}$ есть произвольный нормальный делитель группы $\mathfrak{G}$. Рассмотрим совокупность всех смежных классов $A\mathfrak{H}$ группы $\mathfrak{G}$ по подгруппе $\mathfrak{H}$ и поставим в соответствие с каждым из них символ $a$. Установим для символов $a$, $b$, ... такое правило умножения. Пусть

$A\mathfrak{H} \to a$, $B\mathfrak{H} \to b$. Произведение любых двух элементов из $A\mathfrak{H}$ и из $B\mathfrak{H}$ лежит в одном и том же смежном классе $AB\mathfrak{H}$. В самом деле, возьмём два произвольных элемента $AH$, $BH'$ из смежных классов $A\mathfrak{H}$, $B\mathfrak{H}$. В силу нормальности делителя $\mathfrak{H}$ имеем

$$B^{-1}HB = H'' \subset \mathfrak{H},$$

откуда

$$HB = BH''$$

и таким образом

$$AH \cdot BH' = A(HB)H' = ABH''H' = ABH''' \subset AB\mathfrak{H}.$$

Будем считать произведением $ab$ тот символ $c$, которым мы обозначили смежный класс $AB\mathfrak{H}$. Этот закон умножения определяет группу $\mathfrak{g}$, элементами которой служат символы $a, b, c, \ldots$ Группа $\mathfrak{g}$ гомоморфна группе $\mathfrak{G}$. Она носит название *факторгруппы* $\mathfrak{G}$ по нормальному делителю $\mathfrak{H}$ и обозначается символом

$$\mathfrak{G}/\mathfrak{H}. \tag{3}$$

Если подгруппа $\mathfrak{H}$ имеет конечный индекс относительно $\mathfrak{G}$, то порядок факторгруппы (3) равен этому индексу. В силу построения имеет место

$$\mathfrak{G} \to \mathfrak{G}/\mathfrak{H}.$$

В заключение докажем, что всякой абстрактно заданной группе соответствует изоморфная с ней группа преобразований; в частности, если заданная группа конечна, она изоморфна с некоторой группой подстановок. Этот факт, давно известный для случая конечных групп, был формулирован в общем случае Вейлем (H. Weyl).

Для доказательства возьмём в качестве множества $\mathfrak{M}$ элементы $\mathfrak{E}$, $A, B, C, \ldots$ самой заданной группы $\mathfrak{G}$. Будем сопоставлять с элементом $X$ группы $\mathfrak{G}$ преобразование, переводящее каждый элемент $A$ в $XA$:

$$X \mid A \to XA. \tag{4}$$

Докажем, что это соответствие имеет характер гомоморфизма. Если, наряду с (4), имеет место

$$Y \mid A \to YA, \tag{5}$$

то произведению $XY$ будет соответствовать преобразование

$$XY \mid A \to (XY)A. \tag{6}$$

Введём для преобразований (4), (5), (6) функциональное обозначение

$$XA = f_X(A), \quad YA = f_Y(A), \quad (XY)A = f_{XY}(A).$$

В силу ассоциативного закона будем иметь:

$$f_{XY}(A) = (XY)\,A = X(YA) = X \cdot f_Y(A) = f_X\{f_Y(A)\}.$$

Это равенство показывает, что преобразования, поставленные в соответствии с элементами $X$, $Y$, $XY$ группы $\mathfrak{G}$ таковы, что произведению $X \cdot Y$ элементов группы $\mathfrak{G}$ соответствует произведение преобразований $f_X(A)$, $f_Y(A)$. Это и есть гомоморфизм.

Чтобы убедиться в изоморфизме этого соответствия, исследуем, каким элементам $X$ группы $\mathfrak{G}$ соответствует тождественное преобразование. Это будет тогда, если

$$X \cdot A = A,$$

откуда

$$X = \mathfrak{E}.$$

Таким образом наше соответствие есть изоморфизм.

*Пример гомоморфизма.* Пусть $\mathfrak{G}$ есть симметрическая группа подстановок между 4 символами $x_1$, $x_2$, $x_3$, $x_4$. Применяя их к функциям

$$z_1 = x_1x_2 + x_3x_4, \quad z_2 = x_1x_3 + x_2x_4, \quad z_3 = x_1x_4 + x_2x_3,$$

мы поставим в соответствие с подстановками группы $\mathfrak{G}$ подстановки между 3 символами $z_1$, $z_2$, $z_3$. Это соответствие, очевидно, имеет характер гомоморфизма. Исследуем, каким подстановкам группы $\mathfrak{G}$ соответствует единичная подстановка между $z_1$, $z_2$, $z_3$. Если такая подстановка оставляет $x_1$ на месте, то, оставляя на месте

$$z_1 = x_1x_2 + x_3x_4,$$

она должна оставлять на месте $x_2$ и точно так же $x_3$ и $x_4$. Таким образом, это тождественная подстановка.

Если такая подстановка переводит $x_1$ в $x_2$, то, оставляя $z_1$ на месте, она должна перевести $x_2$ в $x_1$. Далее, оставляя на месте

$$z_2 = x_1x_3 + x_2x_4,$$

она должна перевести $x_3$ в $x_4$, а $x_4$ в $x_3$. Это будет подстановка

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \end{pmatrix}.$$

Продолжая рассуждение, мы убедимся, что группа $\mathfrak{H}$, которой в нашем гомоморфизме соответствует единичная подстановка, состоит из следующих 4 подстановок:

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_4 & x_1 & x_2 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_4 & x_3 & x_2 & x_1 \end{pmatrix}.$$

Но $\operatorname{Пор}\mathfrak{G}=24$, $\operatorname{Пор}\mathfrak{H}=4$, откуда

$$(\mathfrak{G}:\mathfrak{H})=6,$$

т. е. группа $\mathfrak{g}$ подстановок между $z_1$, $z_2$, $z_3$ имеет порядок 6, т. е. максимальный порядок, какой только может иметь группа подстановок 3 символов. Таким образом $\mathfrak{g}$ есть симметрическая группа между $z_1$, $z_2$, $z_3$.

## § 31. Группа преобразований в себя

Назовём *преобразованием в себя* (или *автоморфным преобразованием*) всякое бирациональное преобразование

$$x=\varphi(u,\ v),\quad y=\psi(u,\ v), \tag{1}$$

которое переводит соотношение

$$f(x,\ y)=0 \tag{2}$$

в соотношение той же формы

$$f(u,\ v)=0. \tag{3}$$

Нетрудно видеть, что произведение двух преобразований в себя есть также преобразование в себя и преобразование, обратное к преобразованию в себя, есть преобразование в себя. Таким образом совокупность преобразований каждого поля $k(x,\ y)$ в себя составляет группу.

Имеет место

Теорема 53. *Если* $p>1$, *то группа преобразований в себя поля* $k(x,\ y)$ *конечна.*

Доказательство. Предварительно докажем, что для негиперэллиптического поля $k(x,\ y)$ всякое преобразование в себя, оставляющее все точки Вейерштрасса на месте, есть тождественное преобразование. Допустим противное: пусть существует нетождественное преобразование в себя $S$, оставляющее все точки Вейерштрасса на месте, и пусть оно переводит обыкновенную (т. е. невейерштрассову) точку $P$ в отличную от $P$ точку $P_1$. Найдём в $k(x,\ y)$ элемент, в представление которого через дивизоры в знаменателе стоит только $P^{p+1}$ (так как точка $P$ невейерштрассова, то $p+1$ не принадлежит к дефектным показателям последовательности

$$(P,\ P^2,\ P^3,\ \ldots).$$

Пусть

$$x\equiv\frac{Q}{P^{p+1}}.$$

Пусть рассматриваемое преобразование переводит $x$ в элемент

$$z\equiv\frac{Q_1}{P_1^{p+1}}.$$

Представление через дивизоры разности $x - z$ содержит в знаменателе $P^{p+1} \cdot P_1^{p+1}$, а потому эта разность есть элемент порядка $2p + 2$. Но, согласно условию, наше преобразование оставляет все точки Вейерштрасса на месте. Это значит, что в каждой такой точке значение элемента после преобразования останется тем же. Отсюда следует, что в каждой точке Вейерштрасса разность $x - z$ обращается в нуль. Но так как, в силу теоремы 46, в негиперэллиптических полях число точек Вейерштрасса превышает $2p + 2$, то в числителе представления элемента $z - x$ через дивизоры содержится более чем $2p + 2$ простых дивизоров, в то время как знаменатель содержит только $2p + 2$. Это возможно только в случае $z = x$.

*Примечание.* Мы должны разъяснить, как это преобразование в себя переводит элементы и точки поля $k(x, y)$ друг в друга. Будем записывать преобразование (1) в форме

$$x \to \varphi(x, y), \quad y \to \psi(x, y), \tag{4}$$

и тогда, сопоставляя (2) и (3), мы можем сказать, что преобразование (4) не нарушает соотношения (2). Будем говорить, что преобразование (1) переводит друг в друга все элементы поля $k(x, y)$: именно, оно переводит каждый элемент

$$F(x, y) \tag{5}$$

в элемент

$$F(\varphi(x, y), \quad \psi(x, y)). \tag{6}$$

Ясно, что преобразование (1) не нарушает соотношений, существующих между отдельными элементами поля.

Пусть точка $P$ определяется значениями $x = a$, $y = b$. Будем говорить, что преобразование (1) переводит её в точку $P_1$, определяемую значениями

$$\varphi(x, y) = a, \quad \psi(x, y) = b. \tag{7}$$

Поскольку $S$ есть обратимое преобразование, $\varphi(x, y)$, $\psi(x, y)$ есть тоже примитивная пара поля $k(x, y)$, а потому значения (7) вполне определяют точку $P_1$.

Если элемент (5) обращается в нуль в точке $P$, то элемент (6) обращается в нуль в точке $P_1$. С другой стороны, преобразование (1) сохраняет порядки элементов, а потому нули (и бесконечности) элемента (6) исчерпываются точками, в которые переводятся нули и бесконечности элемента (5). Другими словами, преобразование (1) переводит, наряду с элементами поля $k(x, y)$, их представления через дивизоры.

Если $P$ есть точка Вейерштрасса, то это значит, что существует элемент

$$z \asymp \frac{Q}{P^m} \qquad (m \leqslant p).$$

Если преобразование (1) переводит $z$ в $z_1$, $P$ в $P_1$ и $Q$ в $Q_1$, то

$$z_1 \equiv \frac{Q_1}{P_1^m} \qquad (m \leqslant \rho),$$

а это показывает, что $P_1$ есть точка Вейерштрасса. Таким образом всякое преобразование в себя переводит точку Вейерштрасса в точку Вейерштрасса.

Пусть теперь $k$ $(x, y)$ будет гиперэллиптическое поле, определяемое соотношением

$$y^2 - f(x) = 0, \tag{8}$$

где $f(x)$ — полином. Тогда существует преобразование в себя

$$x \to x, \quad y \to -y, \tag{9}$$

оставляющее все точки Вейерштрасса на местах. Это преобразование будет переводить каждую точку

$$P(x = x_0, \ y = -y_0)$$

в точку

$$P_1(x = x_0, \ y = -y_0).$$

Пусть (1) есть преобразование в себя, оставляющее на местах все точки Вейерштрасса гиперэллиптического поля $k(x, y)$, и пусть оно переводит элемент

$$\xi = \frac{1}{x - x_0} \equiv \frac{Q}{PP_1}$$

в элемент

$$\xi' \equiv \frac{Q'}{P'P_1'}.$$

Элемент $\xi - \xi'$ может иметь в знаменателе своего представления только 4 простых дивизора $P$, $P_1$, $P'$, $P_1'$, в силу чего его порядок не превышает 4. Вместе с тем он должен обращаться в нуль во всех точках Вейерштрасса, которых всего $2\rho + 2$ (см. § 25), т. е. при $\rho > 1$ больше четырёх. Это возможно только в случае тождества

$$\xi = \xi'.$$

Но отсюда следует

$$P \cdot P_1 = P' \cdot P_1',$$

откуда или

$$P = P', \quad P_1 = P_1',$$

или

$$P = P_1', \quad P_1 = P'.$$

В качестве $P$ мы можем взять любую точку. В первом случае мы имеем тождественное преобразование; во втором — преобразование (9).

Таким образом в случае гиперэллиптического поля существуют два преобразования в себя, оставляющие все точки Вейерштрасса на местах.

Чтобы доказать конечность числа всех преобразований в себя поля $k(x, y)$, учтём, что каждое из них переводит точку Вейерштрасса в точку Вейерштрасса. Пусть $\mathfrak{G}$ — группа всех преобразований поля $k(x, y)$ жанра $\rho > 1$ в себя; будем обозначать эти преобразования символами

$$u_1, \ u_2, \ u_3, \ \ldots \tag{10}$$

Пусть этим преобразованиям соответствуют подстановки

$$\Sigma_1, \ \Sigma_2, \ \Sigma_3, \ \ldots, \tag{11}$$

которые эти преобразования производят среди точек Вейерштрасса поля. Это соответствие имеет характер гомоморфизма. Обозначая группу подстановок через $\gamma$, имеем:

$$\mathfrak{G} \to \gamma.$$

Для этого гомоморфизма роль нормального делителя $\mathfrak{H}$ играет группа преобразований в себя, оставляющих все точки Вейерштрасса на местах. Мы показали, что

$\operatorname{Пор} \mathfrak{H} = 1$, если $k(x, y)$ негиперэллиптическое поле,
$\operatorname{Пор} \mathfrak{H} = 2$, если $k(x, y)$ гиперэллиптическое поле.

С другой стороны, индекс $(\mathfrak{G} : \mathfrak{H})$ равен порядку группы $\gamma$, которая как группа подстановок среди конечного числа точек Вейерштрасса, конечна. Тогда из теоремы 51 следует конечность группы $\mathfrak{G}$, ч. т. д.

Пользуясь другими соображениями, Гурвиц доказал, что порядок группы преобразований в себя поля $k(x, y)$ не превышает числа

$$84(\rho - 1).$$

Исследуем группы преобразований в себя полей жанра $\rho = 0$ и $\rho = 1$.

В случае $\rho = 0$ поле $k(x, y)$ является полем рациональных функций от некоторого примитивного элемента $\xi$:

$$k(x, y) = k(\xi).$$

Каждое преобразование в себя переводит $\xi$ в другой, тоже примитивный, элемент $\xi'$ поля $k(\xi)$ (см. § 7, следствие 1 из теоремы (11)):

$$\xi' = \frac{\alpha\xi + \beta}{\gamma\xi + \delta},$$

где $\alpha$, $\beta$, $\gamma$, $\delta$ — константы, причём

$$\alpha\delta - \beta\gamma \neq 0.$$

Это преобразование переводит всякий элемент

$$\eta = F(\xi)$$

поля $k(\xi)$ в элемент

$$\eta' = F\left(\frac{\alpha\xi + \beta}{\gamma\xi + \delta}\right).$$

Таким образом в случае $\rho = 0$ существует *континуум* (конечно, только в том случае, если числовое поле $k$ имеет мощность континуума) преобразований в себя, зависящий от трёх существенных параметров

$$\frac{\alpha}{\delta}, \quad \frac{\beta}{\delta}, \quad \frac{\gamma}{\delta}.$$

В случае $\rho = 1$ (*эллиптическое поле*) тоже существует бесчисленное множество преобразований в себя. При $\rho = 1$ точек Вейерштрасса нет, так как тогда

$$(\rho - 1)\rho(\rho + 1) = 0.$$

Более того, в любой последовательности точек «пробел» должен быть на первом месте, так как если бы там не было пробела, мы бы имели элемент поля $k(x, y)$ 1-го порядка, что возможно только при $\rho = 0$. Поэтому измерение всякого класса порядка 2 равно двум. В этом мы можем убедиться также из теоремы Римана-Роха:

$$\text{Изм}\,\mathfrak{Q} = \text{Пор}\,\mathfrak{Q} - \rho + 1 + \text{Изм}\frac{\mathfrak{W}}{\mathfrak{Q}} = 2 - 1 + 1 = 2,$$

так как при $\rho = 1$ класс $\mathfrak{W}$ содержит только константы, в силу чего

$$\text{Изм}\frac{\mathfrak{W}}{\mathfrak{Q}} = 0.$$

Возьмём произвольный класс $\mathfrak{Q}$ порядка 2. Он имеет измерение 2. Частное его любых двух дивизоров даёт представление некоторого элемента поля $k(x, y)$, имеющего порядок 2. Меняя дивизоры внутри класса, мы тем самым будем совершать над только что построенным элементом дробные линейные преобразования.

Каждому такому классу, т. е. определённому при его помощи элементу, соответствует дивизор критичности порядка

$$w = 2(n + \rho - 1) = 2(2 + 1 - 1) = 4.$$

Каждый из простых дивизоров, входящих множителями в дивизор критичности, входит в класс $\mathfrak{Q}$ в квадрате. Взяв частное от двух из этих квадратов

$$z = \frac{P_1^2}{P_2^2},$$

мы получим особого рода элемент 2-го порядка.

Возьмём другой класс 2-го порядка, $\mathfrak{Q}'$, и аналогично найдём в нём особый элемент

$$z' \equiv \frac{P_1'^2}{P_2'^2}.$$

Между $z$ и $z'$ имеет место соотношение, квадратное относительно обоих элементов:

$$(az^2 + bz + c)\,z'^2 + (a'z^2 + b'z + c')\,z' + (a''z^2 + b''z + c'') = 0.$$

В точке $P_1$ мы имеем $z = 0$, откуда

$$cz'^2 + c'z' + c'' = 0.$$

Поскольку каждый элемент в определённой точке имеет одно определённое значение, оба корня этого квадратного уравнения должны совпадать. Подставляя также значения, соответствующие точкам $P_2$, $P_1'$, $P_2'$, мы убедимся, что каждое из четырёх квадратных уравнений

$$cz'^2 + c'z' + c'' = 0, \quad az'^2 + a'z' + a'' = 0,$$
$$a''z^2 + b''z + c'' = 0, \qquad az^2 + bz + c = 0$$

имеет кратные корни. Этим условиям мы удовлетворим в самом общем виде, если положим

$$c = \lambda^2, \quad c' = 2\lambda\mu, \quad c'' = \mu^2, \quad b'' = 2\rho\mu,$$
$$a'' = \rho^2, \quad a' = 2\rho\nu, \quad a^2 = \nu^2, \quad b = 2\lambda\nu,$$

и соотношение между $z$ и $z'$ перепишется так:

$$(\nu^2z^2 + 2\lambda\nu z + \lambda^2)\,z'^2 + (2\rho\nu z^2 + b'z + 2\lambda\mu)\,z' + \\ + (\rho^2z^2 + 2\rho\mu z + \mu^2) = 0. \tag{12}$$

Постоянные $\lambda$ и $\delta$ не могут быть равны нулю. В самом деле, из $\lambda = 0$ следовало бы

$$\nu^2z^2z'^2 + (2\rho\nu + b'z)\,z' + (\rho z^2 + 2\rho\mu z + \mu^2) = 0,$$

так что точке, в которой $z = 0$, соответствовало бы значение $z' = \infty$. Отсюда следовало бы совпадение точек $P_1$ и $P_2'$, т. е. совпадение классов

$$\mathfrak{Q} = (P_1^2), \quad \mathfrak{Q}' = (P_2'^2),$$

в то время как мы условились, что классы $\mathfrak{Q}$ и $\mathfrak{Q}'$ различны. Подобным же образом докажем, что $\rho \neq 0$.

Подставляя в соотношение (12)

$$z' = \frac{\rho}{\lambda} \cdot z_1,$$

получим

$$(\nu^2z^2+2\rho\nu z+\lambda^2)\rho^2z_1^2+(2\rho\nu z^2+b'z+2\lambda\mu)\lambda\rho z+(\rho^2+2\rho\mu z+\mu^2)\lambda^2=0$$

или

$$\lambda^2\nu^2\rho^2z^2z_1^2+2\lambda\nu\rho^2zz_1(z+z_1)+\lambda^2\rho^2(z^2+z_1^2)+ \\ +\lambda\rho b'zz_1+2\lambda^2\mu\rho(z+z_1)+\mu^2\lambda^2=0. \tag{13}$$

Это соотношение симметрично относительно $z$ и $z_1$. Оно не может давать, как решение относительно $z_1$, рациональную функцию от $z$, потому что тогда в силу симметричности уравнения элемент $z$ тоже рационально бы выражался через $z_1$, а это бы означало, что $z_1$ есть дробная рациональная функция от $z$. Но тогда оба класса $\mathfrak{Q}$ и $\mathfrak{Q}'$ совпадали бы, что мы исключили.

Итак, уравнение (13) неприводимо. Отсюда следует, что поле $k(z, z_1)$ совпадает с полем $k(x, y)$, так как значению элемента 2-го порядка $z$ соответствуют два различных значения элемента $z_1$. Вместо $z_1$ мы можем взять радикал

$$u=\sqrt{(2\rho\nu z^2+b'z+2\lambda\mu)^2-4(\nu z^2+2\lambda\nu z+\lambda^2)(\rho^2z^2+2\rho\mu z+\mu^2)}. \tag{14}$$

Точно так же

$$k(x, y)=k(z_1, u_1),$$

где

$$u_1=\sqrt{(2\rho\nu z_1^2+b'z_1+2\lambda\mu)^2-4(\nu z_1^2+2\lambda\nu z_1+\lambda^2)(\rho^2z_1^2+2\rho\mu z_1+\mu^2)}. \tag{15}$$

В силу

$$k(z, u)=k(z_1, u_1)=k(x, y)$$

пару $z_1$, $u_1$ можно выразить через $z$, $u$ и обратно:

$$z_1=\varphi(z, u), \quad u_1=\psi(z, u). \tag{16}$$

Преобразование (16) является преобразованием в себя, так как соотношение (14), связывающее $z$, $u$, имеет те же коэффициенты, что и соотношение (15), связывающее $z_1$, $u_1$. Совокупность этих преобразований образует однопараметрический континуум. В самом деле, при заданном $z$ каждому классу $\mathfrak{Q}'$ соответствует одно значение $z_1$ (вернее, 6 значений $z_1$, связанных дробными линейными соотношениями; мы должны взять одно из них). Но каждый класс 2-го порядка можно однозначно сопоставить с точкой поля. В самом деле, предварительно фиксируем общую для всех классов точку $P$ (совершенно произвольно). Тогда каждой переменной точке соответствует класс $(PP')$. Обратно, в каждом классе можно найти один и только один дивизор, делящийся на $P$. Если это $PP'$, то каждому классу соответствует точка $P'$.

## § 32. Особые точки

В геометрической теории алгебраических функций особой точкой алгебраической кривой

(1) $$f(x, y) = 0$$

называется точка, в которой угловой коэффициент касательной $\frac{dy}{dx}$ не может быть определён из уравнения

(2) $$\frac{\partial f}{\partial x} + \frac{dy}{dx} \cdot \frac{\partial f}{\partial y} = 0,$$

поскольку в этой точке обе частные производные, $\frac{\partial f}{\partial x}$ и $\frac{\partial f}{\partial y}$, обращаются в нуль. Исходя из этого определения, дадим вкратце классификацию особых точек и в первую очередь дадим определение кратности особой точки.

Найдём представление частных производных через дивизоры. Для этого найдём степень, в которой в $f_y = \frac{\partial f}{\partial y}$ входит какой-нибудь простой дивизор $P$, если в $Z_x$ он входит в степени $\alpha - 1$, а в $Z_y$ — в степени $\beta - 1$. Сначала предположим, что $x$ и $y$ принимают в точке $P$ конечные значения $x_0$, $y_0$. Известно, что $x - x_0$ точно делится на $P^\alpha$, а $y - y_0$ на $P^\beta$. В этом случае уравнение

$$f(x_0, y) = 0$$

имеет $y - y_0$ в качестве корня $\alpha$-й кратности (см. следствие к теореме 29). Это значит, что имеет место

(3) $$f(x_0, y) = (y - y_0)^\alpha \cdot \varphi(y),$$

где $\varphi(y)$ — полином, причём $\varphi(y_0) \neq 0$. Найдём производную от (3):

$$\frac{\partial f(x_0, y)}{\partial y} = \alpha (y - y_0)^{\alpha - 1} \cdot \varphi(y) + (y - y_0)^\alpha \cdot \varphi'(y).$$

С другой стороны,

$$\frac{\partial f(x, y)}{\partial y} = \frac{\partial f(x_0, y)}{\partial y} + (x - x_0) \cdot \frac{\partial^2 f(x_0, y)}{\partial x \, \partial y} + \ldots$$

Сопоставляя обе формулы, мы видим, что $f_y(x, y)$ во всяком случае делится на меньшую из степеней простого дивизора $P$, на которую делятся $(y - y_0)^{\alpha - 1}$ и $x - x_0$, т. е. на меньшую из

$$P^{\beta(\alpha - 1)}, \; P^\alpha.$$

Эта степень во всяком случае не меньше, чем $P^{\alpha - 1}$.

Если в точке $P$ элемент $x$ принимает значение $\infty$, то из тождества

$$f(x, y) = x^m F\left(\frac{1}{x}, y\right),$$

где $F$ — полином (будем предполагать, что $f$ содержит $x$ в $m$-й, а $y$ в $n$-й степени), мы получим

$$f_y(x, y) = x^m F_y\left(\frac{1}{x}, y\right),$$

откуда видно, что $f_y$ содержит в знаменателе простой дивизор $P$ не выше, чем в степени

$$m\alpha - (\alpha - 1).$$

Если в точке $P$ элемент $y$ принимает значение $\infty$, то из подобного же тождества

$$f(x, y) = y^n \cdot F_1\left(x, \frac{1}{y}\right)$$

получим

$$f_y(x, y) = n \cdot y^{n-1} F_1\left(x, \frac{1}{y}\right) - y^{n-2} \frac{\partial F_1\left(x, \frac{1}{y}\right)}{\partial \frac{1}{y}},$$

откуда в силу $F_1\left(x, \frac{1}{y}\right) = 0$:

$$f_y(x, y) = -y^{n-2} \frac{\partial F_1\left(x, \frac{1}{y}\right)}{\partial \frac{1}{y}}.$$

Эта формула показывает, что $f_y(x, y)$ содержит $P$ в знаменателе не выше, чем в степени

$$(n-2)\beta - (\alpha - 1).$$

Если, наконец, в точке $P$ и $x$ и $y$ обращаются в $\infty$, то из тождества

$$f(x, y) = x^m y^n F_2\left(\frac{1}{x}, \frac{1}{y}\right)$$

мы будем иметь:

$$f_y(x, y) = n x^m y^{n-1} F_2\left(\frac{1}{x}, \frac{1}{y}\right) - x^m y^{n-2} \cdot \frac{\partial F_2\left(\frac{1}{x}, \frac{1}{y}\right)}{\partial \frac{1}{y}}.$$

Это в силу

$$F_2\left(\frac{1}{x}, \frac{1}{y}\right) = 0$$

показывает, что $f_y(x, y)$ содержит в знаменателе $P$ не выше, чем в степени

$$m\alpha + (n-2)\beta - (\alpha - 1).$$

Отсюда мы легко можем заключить, что $f_y(x, y)$ представляется через дивизоры так:

$$f_y(x, y) \equiv \frac{Z_x \cdot D}{X^{m} \cdot Y^{n-2}}, \tag{4}$$

где $D$ — некоторый целый дивизор. Принимая во внимание полученную в § 18 формулу (5)

$$\frac{dy}{dx} \equiv \frac{Z_y \cdot X^2}{Z_x \cdot Y^2}, \tag{5}$$

мы при помощи формул (2) и (4) получим:

$$f_x(x, y) \equiv \frac{Z_y \cdot D}{X^{m-2} \cdot Y^{n}}. \tag{6}$$

Сравнивая формулы (4) и (6), мы видим, что одна получается из другой перестановкой $x$ и $y$.

Дивизор $D$ носит название *дивизора особых точек*. Он вполне определяется заданием примитивной пары элементов $x$, $y$. Однако особые точки не обладают инвариантностью в том смысле, как точки Вейерштрасса: при замене примитивной пары $x$, $y$ другой парой дивизор $D$ меняется.

Из формул (4) и (6) не вытекает, что обе частные производные одновременно обращаются в нуль только в тех точках, которым соответствуют простые дивизоры, входящие в $D$; можно было бы ещё предположить, что дивизоры $Z_x$, $Z_y$ имеют общие делители, не входящие в $D$. Это, однако, невозможно, так как всякий простой дивизор, входящий в $Z_x$ и в $Z_y$, непременно входит и в $D$. В самом деле, в этом случае $\alpha \geqslant 2$, $\beta \geqslant 2$; с другой стороны, мы видели, что $f_y(x, y)$ во всяком случае делится на $P^{\gamma}$, где $\gamma$ — меньшее из чисел $\beta(\alpha - 1)$ и $\alpha$, т. е. в нашем случае по крайней мере на $P^{\alpha}$. Но так как $Z_x$ точно делится на $P^{\alpha-1}$, то другой множитель элемента $f_y(x, y)$, дивизор $D$, непременно должен делиться на $P$. Точно так же докажем, что $f_x(x, y)$ делится на $P$ в степени, не меньшей, чем меньшее из чисел $\alpha(\beta - 1)$ и $\beta$: при $\alpha \geqslant 2$, $\beta \geqslant 2$ это число не менее $\beta$, в то время как $Z_y$ точно делится на $P^{\beta-1}$. Аналогичный подсчёт можно произвести в случае, когда в особых точках $x$ или $y$ обращается в бесконечность.

Порядок каждой особой точки принято определять по-разному. Для алгебры проще всего определить его как степень, в которой $P$ входит в $D$. Сумма этих порядков, т. е. порядок дивизора $D$, может считаться числом особых точек (с учётом их кратностей). Вводя для него обозначение $2d$ (это всегда чётное число), мы можем вычислить

его, если применим к формуле (4) теорему о равенстве порядков эквивалентных дивизоров

$$\text{Пор } Z_w + \text{Пор } D = \text{Пор } X^m + \text{Пор } Y^{n-2},$$

откуда

$$2d = -w_w + mn + m(n-2).$$

Но так как

$$w_w = 2p - 2 + 2n,$$

то

$$d = (m-1)(n-1) - p. \tag{7}$$

Для особых точек характерно то, что одной и той же системе значений $x = x_0$, $y = y_0$ может соответствовать несколько точек. В самом деле, разложение полинома $f(x, y)$ по степеням $x - x_0$ и $y - y_0$ в силу

$$f_x(x_0, y_0) = 0, \quad f_y(x_0, y_0) = 0$$

начинается по крайней мере со второй степени, и таким образом значению $x = x_0$ соответствует кратный корень $y_0$ уравнения

$$f(x_0, y) = 0.$$

С другой стороны, значению $x = x_0$ соответствует $n$ точек. Чтобы узнать, скольким из них соответствует система значений $x = x_0$, $y = y_0$, введём новый элемент $t$, получаемый из формулы

$$y - y_0 = t(x - x_0). \tag{8}$$

Сокращая после этой подстановки уравнение (1) на возможно более высокую степень $x - x_0$ и полагая после этого $x = x_0$, мы получим уравнение относительно $t$, корни которого дадут значения $t$, которым соответствуют значения $x = x_0$, $y = y_0$. Если некоторые из них различны, то это явно будет указывать на то, что системе значений $x = x_0$, $y = y_0$ соответствует несколько различных точек.

Подстановка (8) является простым и довольно грубым способом нахождения точек, соответствующих одной и той же системе значений $x$ и $y$. Она имеет весьма простое геометрическое толкование и потому часто употребляется в геометрии. В самом деле, представим себе кривую, заданную уравнением (1). Считая $t$ постоянным, мы можем толковать (8) как уравнение секущей, проведённой через точку $(x_0, y_0)$ с угловым коэффициентом $t$. Пусть после подстановки (8) мы получили из левой части уравнения (1)

$$f(x, y) = (x - x_0)^k \varphi_k(t) + (x - x_0)^{k+1} \cdot \varphi_{k+1}(t) + \dots \tag{9}$$

Тогда значения $f$, удовлетворяющие уравнению

$$\varphi_k(t) = 0, \tag{10}$$

дают угловые коэффициенты касательных к различным ветвям кривой (1), проходящим через точку $(x_0, y_0)$. В самом деле, зададимся целью провести к кривой (1) секущую, проходящую через точку $(x_0, y_0)$ и ещё через весьма близкую к ней точку $(x_1, y_1)$ кривой (1). Для получения углового коэффициента $t$ мы должны подставить в (9) значение $x = x_1$ и, сократив на $(x - x_1)^k$, приравнять нулю:

$$\varphi_k(t) + (x_1 - x_0)\,\varphi_{k+1}(t) + \ldots = 0.$$

При приближении $x_1 - x_0$ к нулю мы получим уравнение (10) $k$-й степени. Оно показывает, что через точку $(x_0, y_0)$ можно провести к кривой $k$ касательных. Простейшим является случай, когда уравнение (10) не имеет кратных корней. В этом случае особую точку кривой (1) называют *особой точкой $k$-й кратности с раздельными касательными*. Ясно, что ей соответствует $k$ различных точек поля $k(x, y)$.

Однако кратному корню уравнения (10) может соответствовать и несколько различных точек поля $k(x, y)$. Существование различных точек, для которых $x = x_0, y = y_0$, характеризуется существованием элемента и поля $k(x, y)$, принимающего в этих точках различные значения. Но элемент $t$, получаемый из уравнения (10), может и не быть элементом такого рода.

Задача нахождения элементов, принимающих в разных точках поля $k(x, y)$ различные значения, называется задачей разрешения особых точек. Переходя к новой примитивной паре, мы можем избавиться от данной особой точки или, как говорят, *разрешить* её. Но при этом мы не гарантированы, что преобразованная кривая не будет иметь никаких других особых точек. Известно, что не в всяком поле $k(x, y)$ существует пара элементов, соотношение между которыми даёт кривую без особых точек. Однако путём нескольких преобразований типа (10) можно прийти к кривой, имеющей только особые точки с раздельными касательными.

Мы не будем доказывать этого предложения, поскольку в следующем параграфе мы выведем более общий результат Кронекера (L. Kronecker): можно всегда преобразовать кривую так, чтобы она имела только двойные точки. Здесь же ограничимся доказательством нескольких общих теорем.

Теорема 54. *Чтобы точка $(x_0, y_0)$ была особой точкой кривой* (1), *необходимо и достаточно, чтобы в числителях представлений элементов $x - x_0$ и $y - y_0$ существовал общий делитель выше первого порядка.*

Доказательство. Условие необходимо. В самом деле, если $x - x_0$ и $y - y_0$ имеют общим делителем только простой дивизор $P$, который при этом входит в один из этих элементов (или в оба) в первой степени, то пусть, например, это будет $x - x_0$. Докажем, что

$$f_y(x_0, y_0) \neq 0.$$

Это вытекает из следствия к теореме 29, согласно которому в данном случае уравнение

$$f(x_0, y) = 0$$

имеет $v = y_0$ в качестве простого корня, откуда

$$f_y(x_0, y_0) \neq 0,$$

так что $(x_0, y_0)$ не является особой точкой кривой (1).

Условие достаточно. В самом деле, если оба элемента $x - x_0$ и $y - y_0$ делятся на простые дивизоры $P$ и $P'$ (всё равно, одинаковые или различные), из того следствия к теореме 29 вытекает, что уравнение

$$f(x_0, y) = 0$$

имеет корень $y = y_0$ по крайней мере 2-й кратности, а уравнение

$$f(x, y_0) = 0$$

— корень $x = x_0$ по крайней мере 2-й кратности. Отсюда следует

$$f_x(x_0, y_0) = 0, \qquad f_y(x_0, y_0),$$

а это означает, что $(x_0, y_0)$ есть особая точка кривой (1).

*Примечание.* Случай, когда одно из значений или оба эти значения обращаются в бесконечность, исследуется путём подстановки

$$x = \frac{1}{x_1}, \quad v = \frac{1}{y_1}$$

и рассмотрения точки (0, 0) кривой

$$F(x_1, y_1) = 0.$$

Рассмотрим случай, когда $(x_0, y_0)$ есть особая точка кривой (1) с раздельными касательными. Это имеет место тогда, и только тогда, когда все корни полинома $\varphi_k(t)$ из формулы (9) просты. Перепишем формулу (9) так:

$$f(x, y + tx - tx_0) = (x - x_0)^k \varphi_k(t) + (x - x_0)^{k+1} \varphi_{k+1}(t) + \dots,$$

и берём производную от обеих частей по $t$:

$$(x - x_0) f_y(x, y) = (x - x_0)^k \varphi_k'(t) + (x - x_0)^{k+1} \varphi_{k+1}(t) + \dots$$

Пусть в точке $P$ $t = t_0$ и пусть дивизор $D$ точно делится на $P^\delta$. Тогда в силу (4) левая часть точно делится на $P$ в степени

$$(2\alpha - 1) + \delta,$$

правая же, в силу того, что $\varphi_k'(t_0) \neq 0$, делится на $P$ в степени $k \cdot \alpha$. Отсюда

$$\delta = (k - 2)\alpha + 1. \tag{11}$$

Меняя ролями $x$ и $y$, мы получим

$$\delta = (k-2)\beta + 1,$$

если условимся считать, что уравнение (10) не имеет ни нулевых, ни бесконечных корней, чего можно всегда достичь путём линейного преобразования $x$ и $y$. Отсюда

$$\alpha = \beta.$$

Пусть $P_1, P_2, \ldots, P_s$ будут те простые дивизоры, на которые одновременно делятся $x - x_0$, $y - y_0$. Иначе говоря, пусть точке кривой (1) соответствуют точки $P_1, P_2, \ldots, P_s$ поля $k(x, y)$. Применяя следствие теоремы 29 к элементам $x$ и $y$, мы из (9) заключаем, что

$$k = \sum_{i=1}^{s} \alpha_i = \sum_{i=1}^{s} \beta_i.$$

С другой стороны, если мы преобразуем кривую (1) к переменным $x_1 t$, то формула (9), которую надо разделить на $(x - x_0)$, показывает, что $f_t \not\equiv 0$ для каждой из точек $P_1, P_2, \ldots, P_s$, в силу чего $x$ должно делиться на первые степени простых дивизоров $P_1, P_2, \ldots, P_s$, откуда

$$\alpha_i = 1, \quad \beta_i = 1, \quad k = s,$$

и формула (11) даёт:

$$\delta = s - 1,$$

так что $D$ точно делится на

$$(P_1 \cdot P_2 \ldots P_s)^{s-1}. \tag{12}$$

Обратно, если дивизор особых точек делится точно на дивизор (12), где $P_1, P_2, \ldots, P_s$ — все точки поля $k(x, y)$, для которых $x = x_0$, $y = y_0$, то $(x_0, y_0)$ есть особая точка с раздельными касательными. В самом деле, в противном случае или не все $\alpha_i = 1$, или $\varphi_k(t)$ имеет кратные корни; в обоих случаях

$$\delta > s - 1.$$

Теорема 55. *Чтобы $(x_0, y_0)$ была особой точкой кривой (1) с раздельными касательными, необходимо и достаточно, чтобы дивизор $D$ особых точек точно делился на дивизор (12), где $P_1, P_2, \ldots, P_s$ — совокупность точек поля $k(x, y)$, для которых $x = x_0$, $y = y_0$.*

Если, в частности, $s = 2$, то мы приходим к случаю *двойной точки*. Соответствующие ей простые дивизоры входят в $D$ в первых степенях, откуда

Теорема 56. *Чтобы кривая (1) имела только двойные особые точки, необходимо и достаточно, чтобы её дивизор особых точек не содержал простых делителей выше, чем в первых степенях.*

## § 33. Теорема Кронекера

Особые точки алгебраических кривых имеют весьма интересную связь с чисто алгебраическим вопросом о существовании степенных фундаментальных базисов в поле $k(x, y)$. Для выяснения этой связи сначала предположим, что $y$ есть целая функция от $x$, т. е. что соотношение между ними имеет вид

$$f(x, y) = y^n + a_1(x) \cdot y^{n-1} + \ldots + a_n(x) = 0, \tag{1}$$

где $a_i(x)$ — полиномы. Рассмотрим степенной базис

$$[1, y, y^2, \ldots, y^{n-1}]. \tag{2}$$

Если он не фундаментальный, то существует целый элемент

$$z = \frac{c_0(x) + c_1(x)\, y + \ldots + c_{n-1}(x)\, y^{n-1}}{d(x)}, \tag{3}$$

где $c_i(x)$ — полиномы, не имеющие общих делителей, а $d(x)$ — полином, содержащий $x$. Если $x - x_0$ есть один из линейных множителей полинома $d(x)$, то элемент

$$\frac{c_0(x_0) + c_1(x_0)\, y + \ldots + c_{n-1}(x_0)\, y^{n-1}}{x - x_0}$$

тоже является целым. Разложим числитель на множители:

$$\frac{c_{n-1}(x_0)(y - b_1)(y - b_2)\ldots(y - b_{n-1})}{x - x_0}.$$

Этот элемент как целый не содержит в знаменателе своего представления простых дивизоров, соответствующих конечным точкам. Поэтому его числитель делится на все $n$ простых дивизоров, на которые делится $x - x_0$. Из этого следует, что хотя бы один из его $n - 1$ множителей

$$y - b_1, \quad y - b_2, \quad \ldots, \quad y - b_{n-1}$$

делится по крайней мере на два из этих простых дивизоров. Если это, например, $y - b_1$, то в силу теоремы 54 $(x_0, b_1)$ есть особая точка кривой (1).

Обратно, пусть $(x_0, y_0)$ есть особая точка кривой (1). Тогда в силу теоремы 54 элементы $x - x_0$ и $y - y_0$ делятся на дивизор $P \cdot P'$, где $P$ и $P'$ — простые дивизоры, совпадающие или различные. Целый элемент $z$, делящийся на первую степень $P$ и более не делящийся на простые делители элемента $x - x_0$, не может быть представлен через базис (2) в форме

$$c_0(x) + c_1(x)\, y + \ldots + c_{n-1}(x)\, y^{n-1}, \tag{4}$$

где $c_i(x)$ — полиномы. В самом деле, всякое выражение вида (4) может быть переписано так:

$$b_0(x)+b_1(x)(y-y_0)+\ldots+b_{n-1}(x)(y-y_0)^{n-1}. \tag{5}$$

Все члены этого выражения, кроме первого, делятся на $PP'$; в силу условия и $b_0(x)$ должен делиться на $P$ и, следовательно, на $x-x_0$. Но тогда выражение (5) делится на $PP'$, вопреки предположению, что $z$ делится на $P$ и более ни на один простой делитель элемента $x-x_0$. Таким образом:

Теорема 57. *Чтобы кривая* (1) *не имела конечных особых точек, необходимо и достаточно, чтобы степенной базис* (2) *был фундаментальным.*

Эта связь может быть выражена точнее, если мы примем во внимание выражение для дискриминанта степенного базиса. Именно, имеет место

$$\Delta[1, y, y^2, \ldots, y^{n-1}] = (-1)^{\frac{n(n-1)}{2}} \cdot N(f_y). \tag{6}$$

Мы не станем выводить этой формулы, приводимой во всех курсах алгебры. С другой стороны, если мы обратимся к формуле (17) § 20, то увидим, что дискриминант фундаментального базиса может быть представлен так:

$$\Delta[\omega_1, \omega_2, \ldots, \omega_n] = \Pi(x-c)^{\alpha-1}. \tag{7}$$

С другой стороны,

$$Z_x = \Pi P^{\alpha-1}. \tag{8}$$

Отсюда, пренебрегая бесконечными простыми дивизорами и учитывая, что

$$N(P) = (x-c),$$

если $x-c$ делится на $P$, мы из (7) и (8) имеем:

$$\Delta[\omega_1, \omega_2, \ldots, \omega_n] = N(Z_x). \tag{9}$$

Беря норму от обеих частей формулы (4) § 32, получим, учитывая (6) и (9),

$$\Delta[1, y, \ldots, y^{n-1}] = N(D) \cdot \Delta[\omega_1, \omega_2, \ldots, \omega_n]. \tag{10}$$

Эта формула даёт новое доказательство теоремы 57. Но, кроме того, она по известным дискриминантам позволяет делать заключения относительно характера особых точек кривой (1). Именно, из теоремы 56 мы заключаем, что кривая (1) имеет только двойные особые точки в том и только в том случае, если дивизор $D$ содержит только по два простых дивизора, на которые делится один и тот же элемент вида $x-c$; другими словами, если полином $N(D)$ имеет корни не выше 2-й кратности.

Пусть $[\omega_1, \omega_2, \ldots, \omega_n]$ — фундаментальный базис. Рассмотрим линейную функцию

$$u = t_1\omega_1 + t_2\omega_2 + \ldots + t_n\omega_n, \tag{11}$$

где $t_1, t_2, \ldots, t_n$ — независимые переменные, и базис

$$[1, u, u^2, \ldots, u^{n-1}],$$

элементы которого выражаются через фундаментальный базис при помощи коэффициентов, которые являются полиномами от $x$, $t_1$, $t_2, \ldots, t_n$. Определитель $|U|$ этой подстановки тоже есть полином от этих переменных. Сопоставляя (10) с формулой (16), мы получим:

$$|U|^2 = N(D).$$

Итак, чтобы кривая (1) имела только двойные точки, необходимо и достаточно, чтобы $|U|$ не имел кратных корней.

Будем рассматривать $|U|$ как полином от $t_1, t_2, \ldots, t_n$, коэффициенты которого суть полиномы от $x$. Докажем, что $|U|$ не содержит множителей, зависящих только от $x$. Допустим противное: пусть $|U|$ содержит множитель $x - c$, не зависящий от выбора $t_1, t_2, \ldots, t_n$. Обозначая элементы матрицы $U$ через $u_{ik}$, будем иметь:

$$\begin{cases} 1 = u_{11}\omega_1 + u_{12}\omega_2 + \ldots + u_{1n}\omega_n, \\ u = u_{21}\omega_1 + \omega_{22}\omega_2 + \ldots + u_{2n}\omega_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u^{n-1} = u_{n1}\omega_1 + \omega_{n2}\omega_2 + \ldots + u_{nn}\omega_n. \end{cases} \tag{12}$$

Пусть

$$x - c \equiv \frac{P_1^{e_1} \cdot P_2^{e_2} \ldots P_s^{e_s}}{X},$$

где $P_1, P_2, \ldots, P_s$ — различные простые дивизоры. Придадим $t_1, t_2, \ldots, t_n$ значения таких полиномов от $x$, чтобы

$$u - c_1, \quad u - c_2, \quad \ldots, \quad u - c_s,$$

где $c_1, c_2, \ldots, c_s$ отличные друг от друга константы, соответственно делились на $P_1, P_2, \ldots, P_s$, но не на $P_1^2, P_2^2, \ldots, P_s^2$. Этого можно достичь, обозначая через $u_1, u_2, \ldots, u_s$ целые элементы, делящиеся соответственно на $P_1, P_2, \ldots, P_s$, но более ни на какие делители $x - c$, и полагая

$$w = u_1 \cdot u_2 \ldots u_s,$$

$$u = \sum_{i=1}^{s} b_i \cdot \frac{w^2}{u_i^2} + wa,$$

где константы $b_i$ подобраны так, чтобы все произведения

$$b_i\left(\frac{w^2}{u_i^2}\right)p_i \qquad (i=1, 2, \ldots, s)$$

были отличны друг от друга, а константа $a$ так, чтобы частные $\frac{u-u_{p^i}}{u_i}$ не обращались в нуль в точке $P_i$ $(i=1, 2, \ldots, s)$.

Из делимости определителя системы (12) на $x-c$ следует возможность подобрать такие полиномы от $x$:

$$c_0, c_1, \ldots, c_{n-1},$$

не все делящиеся на $x-c$, чтобы имело место

$$c_0+c_1u+\ldots+c_{n-1}u^{n-1}\equiv 0 \pmod{x-c}. \tag{13}$$

Можно считать $c_0, c_1, \ldots, c_{n-1}$ константами и представить сравнение (13) в таком виде:

$$(u-q_1)(u-q_2)\ldots(u-q_r)\equiv 0 \pmod{x-c}, \quad r\leqslant n-1. \tag{14}$$

Это сравнение, однако, невозможно, так как, чтобы $u-q_i$ делился на один из простых дивизоров $P_1, P_2, \ldots, P_s$, необходимо, чтобы $q_i$ совпадало с одной из констант $c_1, c_2, \ldots, c_s$, и тогда $u-q_i$ будет делиться только на один из простых дивизоров, притом в первой степени, произведение же $r\leqslant n-1$ таких множителей не сможет делиться на $n$ простых делителей элемента $x-c$. Наше утверждение доказано.

Кроме того, нам необходимо доказать, что $|U|$ не содержит квадратичных множителей, хотя бы и зависящих от $t_1, t_2, \ldots, t_n$. Поскольку мы доказали несуществование независимых от $t_1, t_2, \ldots, t_n$ множителей, для этого нам достаточно убедиться, что дискриминант

$$\Delta[1, u, u^2, \ldots, u^{n-1}] \tag{15}$$

не содержит множителей выше, чем во второй степени. Оказывается, что этот дискриминант разлагается на линейные относительно $t_1, t_2, \ldots, t_n$ множители. Именно, в курсах алгебры доказывается, что этот дискриминант равен квадрату определителя Вандермонда

$$\begin{vmatrix} 1, & u_1, & \ldots, & u_1^{n-1} \\ 1, & u_2, & \ldots, & u_2^{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & u_n, & \ldots, & u_n^{n-1} \end{vmatrix}, \tag{16}$$

где $u_1, u_2, \ldots, u_n$ — сопряжённые с $u$ корни уравнения $n$-й степени с коэффициентами из $k(x; t_1, t_2, \ldots, t_n)$ и вместе с тем в силу (11)

однородные линейные функции от $t_1, t_2, \ldots, t_n$. В свою очередь определитель (16) может быть представлен в виде произведения

$$\prod_{i>k}(u_i - u_k). \tag{17}$$

Таким образом вопрос приводится к исключению возможности пропорциональности множителей выражения (17) как линейных функций от $t_1, t_2, \ldots, t_n$:

$$u_i - u_k = \varkappa\,(u_\lambda - u_\mu), \tag{18}$$

где $\varkappa$ не зависит от $t_1, t_2, \ldots, t_n$.

Чтобы доказать невозможность соотношения (18), мы тремя различными способами специализируем переменные $t_1, t_2, \ldots, t_n$, беря вместо них некоторые полиномы от $x$: первый раз так, чтобы $u_i, u_k, u_\lambda, u_\mu$ превратились в величины, сопряжённые с некоторым целым элементом $z$, образующим с $x$ примитивную пару поля $k(x, y)$; второй раз — с $z^2$ и третий раз — с $z^3$. Получим:

$$(z_i - z_k) = \varkappa\,(z_\lambda - z_\mu), \tag{19}$$

$$(z_i^2 - z_k^2) = \varkappa\,(z_\lambda^2 - z_\mu^2), \tag{20}$$

$$(z_i^3 - z_k^3) = \varkappa\,(z_\lambda^3 - z_\mu^3). \tag{21}$$

Деля (20) и (21) на (19), будем иметь:

$$z_i + z_k = z_\lambda + z_\mu, \tag{22}$$

$$z_i^2 + z_i z_k + z_k^2 = z_\lambda^2 + z_\lambda z_\mu + z_\mu^2. \tag{23}$$

Возводя (22) в квадрат и вычитая (23), получим:

$$z_i z_k = z_\lambda z_\mu. \tag{24}$$

Из уравнений (22) и (24) следует или

$$z_i = z_\lambda, \quad z_k = z_\mu, \tag{25}$$

или

$$z_i = z_\mu, \quad z_k = z_\lambda. \tag{26}$$

Каждая из полученных систем равенств противоречит тому, что $z$ составляет с $x$ примитивную пару поля $k(x, y)$ и потому есть корень неприводимого уравнения $n$-й степени, не имеющего кратных корней.

В силу доказанного определитель $|U|$, рассматриваемый как полином от $x$:

$$|U| = \varphi(x),$$

взаимно прост со своей производной $\varphi'(x)$. Применяя к ним алгоритм Эвклида по букве $x_1$ мы найдём полиномы $A_1(x)$, $B_1(x)$,

дающие:

$$\varphi(x)\cdot A_1(x)+\varphi'(x)\cdot B_1(x)=1. \tag{27}$$

Коэффициенты полиномов $A_1(x)$, $B_1(x)$ являются дробными рациональными функциями от $t_1, t_2, \ldots, t_n$. Выделяя в них общий знаменатель $\psi(t_1, t_2, \ldots, t_n)$ и вводя обозначения

$$A_1(x)=\frac{A(x)}{\psi},\quad B_1(x)=\frac{B(x)}{\psi},$$

мы преобразуем равенство (27) к виду

$$\varphi(x)\cdot A(x)+\varphi'(x)\cdot B(x)=\psi(t_1, t_2, \ldots, t_n), \tag{28}$$

в котором все входящие функции суть полиномы от всех своих переменных. Поэтому, если мы возьмём для $t_1, t_2, \ldots, t_n$ постоянные значения, не обращающие $\psi$ в нуль:

$$\psi(t_1, t_2, \ldots, t_n)\neq 0, \tag{29}$$

то $|U|=\varphi(x)$ не будут иметь кратных корней, а потому соотношение между $x$ и $u$ даёт кривую, имеющую на конечном расстоянии только двойные особые точки.

При таком решении задачи кривая непременно будет иметь на бесконечности особую точку высшей кратности. В самом деле, если $y$ есть целая функция от $x$ и если

$$x\approx\frac{X_1}{X},\quad y\approx\frac{Y_1}{Y},$$

то $Y$ делится только на те простые дивизоры, которые входят в $X$. Поэтому соотношение между элементами

$$x_1=\frac{1}{x}\approx\frac{X}{X_1},\quad y_1=\frac{1}{y}\approx\frac{Y}{Y_1}$$

даёт кривую, для которой $x_1=0$, $y_1=0$ есть особая точка высшей кратности. Таким образом для доказательства теоремы Кронекера необходимо модифицировать только что изложенный приём.

Возьмём примитивную пару $x$, $y$ поля $k(x, y)$; пусть порядок элемента $x$ будет $n$.. Составим дискриминант $D(x)$ уравнения (1) и найдём все значения $y$, соответствующие его корням. Пусть $y=b$ есть отличное от этих значений и в остальном произвольное значение элемента $y$ и пусть ему соответствуют значения элемента $x$.

$$x=a_1,\quad x=a_2,\quad \ldots,\quad x=a_k. \tag{30}$$

Тогда каждому из значений (30) будут соответствовать по $n$ различных значений $y$, в силу чего они не будут давать особых точек кривой (1).

Преобразуем элемент $y$, взяв вместо него

$$\frac{1}{y-b}.$$

Тогда каждому из значений (30) будут соответствовать по $n$ различных значений $y$, из которых по одному значению будут равны $\infty$. Других бесконечных значений элемент $y$ иметь не будет. Точно таким же образом преобразуем элемент $x$.

Рассмотрим в поле $k(x)$ кольцо $\mathfrak{Q}$, элементы которого пусть будут рациональные функции от $x$, содержащие в знаменателях только степени функций

$$x-a_1, \quad x-a_2, \quad \ldots, \quad x-a_k. \tag{31}$$

При помощи этого кольца построим кольцо $\mathfrak{Q}_1$ внутри поля $k(x, y)$ (см. § 10). Поскольку элемент $y$ обращается в бесконечность только в точках (30), он входит в кольцо $\mathfrak{Q}_1$.

Построим для кольца $\mathfrak{Q}_1$ фундаментальный базис

$$[\omega_1, \omega_2, \ldots, \omega_n]. \tag{32}$$

Для этого, исходя от базиса

$$[1, y, \ldots, y^{n-1}],$$

будем при его построении избегать делений на функции (31). В силу выбора кольца $\mathfrak{Q}_1$ мы имеем на это право. Далее, пользуясь этим базисом, построим при помощи формулы (11) элемент $u$. Соотношение между $x$ и $u$ даёт кривую, которая в силу доказанного выше не имеет особых точек, кроме точек (30) и $x=\infty$. Для этого нужно в качестве $t_1, t_2, \ldots, t_n$ выбрать константы, подчинённые неравенству (29).

Что касается значений (30), то каждое из них соответствует $n$ различным точкам поля $k(x, y)$, из которых только в одной $y=\infty$. Следовательно, это же имеет место для элемента $u$ при неопределённых $t_1, t_2, \ldots, t_n$. Подчиним их неравенствам, выражающим несовпадение значений элемента $u$ в различных точках, соответствующих каждому значению $x=a_i$. Эти неравенства совместимы с неравенством (29).

Наконец, рассмотрим значение $x=\infty$. Во всех точках, соответствующих этому значенню, значения элемента $y$ конечны и различны. Вместе с тем, беря фундаментальный базис кольца $\mathfrak{Q}_1$ в форме, описанной в § 11, мы без нарушения общности можем считать, что его второй член есть $y$. В самом деле, в противном случае он бы имел вид

$$\omega_2=\frac{b_0(x)+y}{d_2(x)},$$

где $d_2(x)$ — полином, не делящийся на полиномы (31); тогда мы могли бы взять $\omega_2$ в роли $y$. Таким образом среди членов базиса будут принимающие при $x=\infty$ конечные и различные вначения, другие же могут принимать нулевые значения. Поэтому условия несовпадения значений элемента (11) при $x=\infty$ будут иметь вид нера-

венств между $t_1, t_2, \ldots, t_n$, не противоречащих ранее добытым неравенствам, и мы приходим к

Теорема 58 (Кронекера). *Всякая алгебраическая кривая может быть бирационально преобразована в кривую, имеющую только двойные особые точки.*

В теории алгебраических кривых часто, наряду с плоскими кривыми, рассматриваются пространственные кривые, задаваемые в пространстве любого числа измерений. В трёхмерном пространстве координаты $x$, $y$, $z$ кривой являются элементами поля $k(x, y)$ и потому могут быть представлены через дивизоры

$$x \asymp \frac{X_1}{X}, \quad y \asymp \frac{Y_1}{Y}, \quad z \asymp \frac{Z_1}{Z}.$$

По аналогии с теорией плоских кривых $(x_0, y_0, z_0)$ является особой точкой кривой в том и только в том случае, если элементы $x - x_0$, $y - y_0$, $z - z_0$ имеют общим делителем дивизоры выше первого порядка. В этом и только в этом случае проекция кривой на любую плоскость будет иметь в $(x_0, y_0, z_0)$ особую точку.

Рассмотрим проекции кривой на координатные плоскости $XY$ и $XZ$. Для каждой из этих плоских кривых составим полиномы

$$|U| = \varphi(x, t_1, t_2, \ldots, t_n), \quad |U'| = \Phi(x, u_1, \ldots, u_n),$$

обращение которых в нуль происходит в особых точках преобразованных проекций. Поскольку значения $t_1, t_2, \ldots, t_n$ и $u_1, u_2, \ldots, u_n$ не зависят друг от друга, можно найти такие полиномы $V(x)$, $W(x)$, $\Psi(t_1, \ldots, t_n; u_1, \ldots, u_n)$, что

$$\varphi(x)\, V(x) + \Phi(x)\, W(x) = \Psi(t_1, \ldots, t_n; u_1, \ldots, u_n).$$

Если придать $t_1, \ldots, t_n; u_1, \ldots, u_n$ такие постоянные значения, чтобы $\Psi \neq 0$, полиномы $\varphi(x)$ и $\Phi(x)$ не будут одновременно обращаться в нуль, и обе проекции кривой после преобразования не будут иметь общих особых точек. Отсюда следует, что пространственная кривая после преобразования не будет иметь особых точек, и мы приходим к теореме

Теорема 59. *Всякая алгебраическая кривая в трёхмерном пространстве может быть бирационально преобразована в кривую, вовсе не имеющую особых точек.*

## § 34. Число параметров поля алгебраических функций

Одним из принципиально важнейших вопросов теории алгебраических функций является вопрос, сколько независимых параметров должно быть задано, чтобы определить поле $k(x, y)$ жанра $\rho$. Пусть поле $k(x, y)$ задано уравнением

$$f(x, y) = 0, \tag{1}$$

коэффициенты которого мы будем считать переменными. Чтобы жанр поля был равен $\rho$, надо подчинить эти коэффициенты некоторым условиям, сводящимся к тому, чтобы кривая (1) имела число особых точек $2d$, связанное со степенями $m$, $n$ уравнения (1) относительно $x$, $y$ и жанром $\rho$ зависимостью

$$d = (m-1)(n-1) - \rho \tag{2}$$

[см. § 32, формулу (71)]. Число коэффициентов, остающихся независимыми, в общем случае превышает число параметров поля, так как можно, оставляя поле неизменным, подвергнуть уравнение (1) бирациональному преобразованию и таким образом изменить не только значения коэффициентов, но и степени $m$, $n$.

Вопрос о числе параметров поля $k(x, y)$ впервые был решён Риманом, который называл параметры *модулями*; этот термин употребляется многими математиками до сих пор.

Чтобы яснее представить себе идею вывода, дадим сначала не строгий, но простой вывод, близкий к выводу Римана. Мы видели, что в каждом поле жанра $\rho$ существует элемент порядка $\leqslant \rho$. Он может быть представлен в виде частного дивизоров порядка $\leqslant \rho$, порождающих класс $\mathfrak{A}$, который, как мы уже видели, специален. Другими словами, этот элемент может быть представлен в виде частного двух дивизоров класса $\mathfrak{B}$, имеющих $\rho - 2$ общих простых дивизоров. Ещё лучше представить себе этот элемент в виде частного двух подинтегральных функций интегралов 1-го рода, обращающихся в нуль в $\rho - 2$ общих точках. Обе функции представим себе выраженными через коэффициенты уравнения (1). Теперь подчиним эти коэффициенты условию того, чтобы обе подинтегральные функции имели ещё один общий нуль. Это условие нетрудно выразить, пользуясь теорией исключения. Тогда порядок нашего элемента будет уже не $\rho$, а $\rho - 1$. Далее, поставим условие того, чтобы подинтегральные функции имели ещё один нуль, $\rho$-й. Этим мы наложим на коэффициенты второе условие и придём к элементу $(\rho - 2)$-го порядка. Продолжая процесс, мы после наложения на коэффициенты $\rho - 2$ условий придём к элементу 2-го поля, т. е. к гиперэллиптическому полю. В последнем можно найти элементы, удовлетворяющие уравнению

$$u^2 = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_{2\rho+2}),$$

где $\alpha_1, \alpha_2, \ldots, \alpha_{2\rho+2}$ можно рассматривать как независимые параметры поля. Однако не все они существенны: подвергая $z$ дробному линейному преобразованию

$$z = \frac{az' + c}{cz' + d},$$

мы можем *трём* из них придать заданные значения.

Таким образом гиперэллиптическое поле имеет

$$(2\rho + 2) - 3 = 2\rho - 1$$

существенных параметров. Общее же поле, из которого гиперэллиптическое поле получено наложением $\rho - 2$ условий, имеет

$$(2\rho - 1) + (\rho - 2) = 3\rho - 3 \tag{3}$$

существенных параметров.

Этот вывод нельзя считать строгим: во-первых, мы не доказывали, что при наложении условий мы не понижаем жанра поля. Это вытекает из факта существования гиперэллиптических полей любого жанра. Во-вторых, не доказывается, что накладываемые условия независимы друг от друга.

Приведём строгий вывод утверждения Римана. Для этого предварительно приведём уравнение (1) к нормальной форме, т. е. к уравнению такого типа, что существует или одна пара, или во всяком случае лишь конечное число примитивных пар поля $k(x, y)$, связанных уравнениями нормального типа.

Возьмём какую-нибудь точку Вейерштрасса $P_\infty$ поля $k(x, y)$ (при $\rho > 1$ их всего конечное число). Пусть $n$ — наименьший показатель, для которого

$$\text{Изм}\,(P_\infty^n) > 1.$$

Тогда, очевидно,

$$\text{Изм}\,(P_\infty^n) = 2.$$

Далее, пусть $r$ будет наименьшее взаимно простое с $n$ число, для которого имеет место

$$\text{Изм}\,(P_\infty^{n+r}) > \text{Изм}\,(P_\infty^{n+r-1}),$$

и пусть

$$\text{Изм}\,(P_\infty^{n+r}) = h + 1.$$

Тогда в поле $k(x, y)$ будет существовать элемент $x$, представляемый через дивизоры так:

$$x \approx \frac{X_1}{P_\infty^n},$$

и элемент $y$, представляемый через дивизоры так:

$$y \approx \frac{Y_1}{P_\infty^{n+r}},$$

причём дивизоры $X_1$ и $Y_1$ не будут делиться на $P_\infty$.

Дивизор $X_1$ определяется таким путём не вполне: в качестве $X_1$ мы можем взять любой дивизор семейства

$$\lambda X_1 + \mu P_\infty^n \qquad (\lambda \neq 0).$$

Нормируем его так, чтобы он делился на простой дивизор $P_0$, где $P_0$ — какая-нибудь другая точка Вейерштрасса. Это определит элемент $x$ с точностью до мультипликативной постоянной. В качестве дивизора $Y_1$ тоже можно выбрать произвольный дивизор класса $(P_\infty^{n+r})$, если только он не делится на $P_\infty$. Выберем его так, чтобы он делился на возможно более высокую степень, $P_0^e$, простого дивизора $P_0$. Этим элемент $y$ тоже будет определён с точностью до мультипликативной постоянной. Таким образом

$$x \asymp \frac{P_0 L}{P_\infty^n}, \quad y \asymp \frac{P_0^e \cdot M}{P_\infty^{n+r}}. \tag{4}$$

Мы поставили условием взаимную простоту $n$ и $r$ для того, чтобы быть уверенными, что $x$, $y$ являются примитивной парой. В самом деле, если $x$, $y$ не составляют примитивной пары, то связывающее их уравнение является $\nu$-й степенью неприводимого уравнения. Но оно $(n+r)$-й степени относительно $x$ и $n$-й относительно $y$, так что при $(n, r) = 1$ это невозможно.

Пусть это уравнение имеет вид

$$F(x, y) = y^n + a_1(x) y^{n-1} + a_2(x) y^{n-2} + \ldots + a_n(x) = 0. \tag{5}$$

В силу представления (4) $y$ есть целый элемент от $x$, а потому коэффициенты $c_i(x)$ являются полиномами от $x$. Определим степени этих полиномов. Проще всего выполнить это, расширив поле $k(x, y)$, т. е. присоединив к нему элемент $\xi$, связанный с $x$ соотношением

$$\xi^n = x. \tag{6}$$

Тогда уравнение (5) примет вид

$$F(\xi^n, y) = y^n + a_1(\xi^n) y^{n-1} + \ldots + a_n(\xi^n) = 0.$$

Посмотрим, каковы будут представления элементов $\xi$, $y$ в расширенном поле. Каждый из простых дивизоров поля $k(x, y)$ внутри поля $k(\xi, y)$ распадается в произведения $n$ простых дивизоров, причём взаимно простые дивизоры останутся взаимно простыми. Поэтому мы можем считать, что в поле $k(\xi, y)$ имеют место представления (4), где $P_0$, $P_\infty$ являются уже не простыми дивизорами, а произведениями $n$ простых дивизоров. Таким образом в силу (4) и (6) будем иметь

$$\xi \asymp \frac{\Pi_0 \cdot \Lambda_0}{P_\infty}, \tag{7}$$

где

$$\Pi_0^n = P_0, \quad \Lambda_0^n = L.$$

Воспользуемся введённым в § 12 понятием показателя $y$ относительно $\xi$: это есть наименьший показатель $\varkappa$, при котором элемент

$$z = y : \xi^{\varkappa}$$

есть элемент кольца $\Omega_1$ целых относительно $\frac{1}{\xi}$ элементов. Из (4) и (7) следует, что

$$\varkappa = n + r.$$

В силу этого коэффициенты соотношения между $\xi$ и $z$

$$z^n + a_1(\xi^n) \cdot \xi^{-(n+r)} \cdot z^{n-1} + a_2(\xi^n) \cdot \xi^{-2(n+r)} \cdot z^{n-2} + \ldots$$
$$\ldots + a_n(\xi^n)\, \xi^{-n(n+r)} = 0$$

должны быть полиномами относительно $\frac{1}{\xi}$, в силу чего степени полиномов $a_i(\xi^n)$ не должны превышать $i(n+r)$. Отсюда следует

$$\text{степень } a_i(x) \leqslant \left[\frac{i(n+r)}{n}\right], \tag{8}$$

где $[M]$ — символ наибольшего целого числа, не превышающего $M$ («entier»).

В частности, коэффициент $a_n(x)$ имеет *точно* степень $n+r$, так как иначе степень уравнения (5) относительно $x$ была бы меньше $n+r$, что противоречит представлению (4).

Неравенства (8) дают возможность подсчитать число независимых коэффициентов в уравнении (5). Оно равно:

$$\sigma = \left\{\left[\frac{n+r}{n}\right] + 1\right\} + \left\{\left[\frac{2(n+r)}{n}\right] + 1\right\} + \ldots$$
$$\ldots + \left\{\left[\frac{(n-1)(n+r)}{n}\right] + 1\right\} + (n+r+1).$$

Для упрощения этого выражения соединим каждый его ($i$-й) член с $(n-i)$-м и учтём, что $n+r$ взаимно просто с $n$, а потому $\left[\frac{i(n+r)}{n}\right]$ и $\left[\frac{(n-i)(n+r)}{n}\right]$ — непременно дробные числа. Но так как

$$\frac{i(n+r)}{n} + \frac{(n-i)(n+r)}{n} = n + r,$$

то отсюда

$$\left[\frac{i(n+r)}{n}\right] + \left[\frac{(n-i)(n+r)}{n}\right] = n + r - 1.$$

Таким образом

$$\sigma = \frac{(n+r+1)(n-1)}{2} + (n+r+1) = \frac{(n+r+1)(n+1)}{2}. \tag{9}$$

Это всегда целое число, так как $n+r$ и $n$ в силу своей взаимной простоты не могут быть одновременно чётными.

Докажем, что при таком выборе степеней у коэффициентов $a_i(x)$ мы всегда получим в знаменателях представлений элементов $x$, $y$ степени только одного простого дивизора. Мы видели, что при соблюдении условий (8)

$$z = y : \xi^{n+r}$$

есть целый элемент кольца $\Omega_1$ и его норма взаимно проста с $\frac{1}{\xi}$, в силу чего при представлении через дивизоры числитель дивизора $\frac{1}{x}$ не содержится ни в числителе, ни в знаменателе элемента $z$. Если $u$, $v$ — целые положительные числа, удовлетворяющие равенству

$$(n+r)u - nv = 1,$$

то элемент

$$y^u : x^v = z^u \cdot \xi^{(n+r)u - nv} = z^u \cdot \xi$$

есть также элемент кольца $\Omega_1$, а его $n$-я степень

$$\{ y^u : x^v \}^n = z^{nu} \cdot x$$

при представлении через дивизоры будет содержать в знаменателе точно первую степень знаменателя представления элемента $x$. Таким образом в поле $k(x, y)$ существует элемент, $n$-я степень которого содержит в представлении через дивизоры точно первую степень знаменателя представления элемента $x$, который имеет порядок $n$. Это возможно только в том случае, если этот знаменатель есть $n$-я степень некоторого дивизора, который должен быть простым. Обозначая его через $P_\infty$, получим:

$$x = \frac{X_1}{P_\infty^n}.$$

Из того, что $y$ есть целый элемент кольца $\Omega$, следует, что в знаменателе представления $y$ содержится только степень $P_\infty$:

$$y = \frac{Y_1}{P_\infty^{n+r}}.$$

Далее, чтобы $x$ делился на $P_0$, а $y$ делился на $P_0^e$, мы должны наложить на коэффициенты уравнения (5) ещё $h+1$ условий, так что получим всего

$$\sigma - h - 1$$

независимых коэффициентов. Нормируя множители при $x$ и $y$, мы останемся с

$$\sigma - h - 3$$

параметрами.

Наконец, для того чтобы жанр поля $k(x, y)$ был равен заданному числу $\rho$, нужно подчинить коэффициенты новым условиям,

благодаря которым кривая (5) приобретёт надлежащее число особых точек. Чтобы определить число этих условий, подсчитаем, в какой степени простой дивизор $P_\infty$ входит в знаменатель представления элемента $F_y(x, y)$. Имеем:

$$F_y(x, y) = ny^{n-1} + (n-1)\,a_1(x)y^{n-2} + \ldots$$
$$\ldots + (n-i)\,a_i(x)\,y^{n-i-1} + \ldots + a_{n-1}(x).$$

В знаменателе представления члена

$$(n-i)\cdot a_i(x)\cdot y^{n-i-1} \qquad (i = 1, 2, \ldots, n-1)$$

простой дивизор $P_\infty$ входит в степени, не превышающей числа

$$\left[\frac{i(n+r)}{n}\right]\cdot n + (n-i-1)(n+r) < \frac{i(n+r)}{n}\cdot n +$$
$$+ (n-i-1)(n+r) = (n-1)(n+r),$$

в то время как в знаменателе представления члена с $y^{n-1}$ простой дивизор $P_\infty$ входит точно в степени

$$(n-1)(n+r).$$

Поэтому после приведения представления элемента $F_y$ к одночленной форме никаких сокращений на $P_\infty$ произойти не может, и в знаменателе этого представления $P_\infty$ входит точно в степени $(n-1)(n+r)$.

Перепишем представление (4) § 32 элемента $F_y$ через дивизоры в такой форме:

$$F_y(x, y) \asymp \frac{D'Z'}{P_\infty^{(n-1)(n+2)}}, \tag{10}$$

где под $D'$, $Z'$ мы будем разуметь дивизоры $D$, $Z_x$, лишённые делителей, являющихся степенями $P_\infty$. Из того, что $P_\infty$ входит в $X$ в степени $n$, следует, что

$$Z_x = P_\infty^{n-1}\cdot Z'.$$

Сравним порядки числителя и знаменателя в представлении (10):

$$\text{Пор}\,(D'Z') = (n-1)(n+r),$$

откуда

$$\text{Пор}\,Z_x = (n-1)(n+r) + (n-1) - \text{Пор}\,D',$$

или, обозначая $\text{Пор}\,D'$ через $2d'$ и вспоминая, что

$$\text{Пор}\,Z_x = 2p - 2 + 2n,$$

получим:

$$d' = \frac{1}{2}(n-1)(n+r-1) - p. \tag{11}$$

Наложим на коэффициенты уравнения (5) условия того, чтобы имело место (11). Заставим кривую (5) иметь $d'$ двойных точек. Каждая такая точка в силу (12) § 32 при $s=2$ увеличивает порядок $2d'$ дивизора $D'$ на 2. Вместе с тем требование, чтобы кривая (5) имела двойную точку, даёт одно равенство; чтобы получить его, надо написать условие того, чтобы результанты 1-го и 2-го, а также 1-го и 3-го из элементов

$$F(x, y), \quad F_x(x, y), \quad F_y(x, y)$$

имели общий корень. Таким образом у нас останется

$$\sigma - h - 3 - d' \tag{12}$$

независимых параметров. Это и есть искомое число параметров поля $k(x, y)$. Здесь

$$\sigma = \frac{1}{2}(n+r+1)(n+1),$$

$$d' = \frac{1}{2}(n+r-1)(n-1) - \rho,$$

$$h+1 = \text{Изм}\,(P_\infty^{n+r}).$$

Пользуясь теоремой Римана-Роха, получим:

$$h = n + r - \rho + \text{Изм}\,\frac{\mathfrak{W}}{(P_\infty^{n+r})}.$$

Подставляя в (12), получим для искомого числа параметров следующее выражение:

$$n + 2\rho - 3 - \text{Изм}\,\frac{\mathfrak{W}}{(P_\infty^{n+r})}. \tag{13}$$

Поскольку $n \leqslant \rho$, число (13) не может превышать числа $3\rho - 3$. С другой стороны, если поле $k(x, y)$ содержит только простейшие точки Вейерштрасса с системой пробелов

$$1, 2, \ldots, (\rho-1), (\rho+1),$$

до принять:

$$n = \rho, \quad \text{Изм}\,\frac{\mathfrak{W}}{(P_\infty^{n+r})} = 0,$$

и выражение (13) превращается в следующее:

$$3\rho - 3,$$

т. е. приобретает максимальное возможное значение. Таким образом, если системы всех параметров заполняют $(3\rho-3)$-мерное пространство, то точки этого пространства, соответствующие особенным полям, у которых $n<\rho$, заполнят многообразия меньшего числа измерений.

В частности, для гиперэллиптических полей

$$n=2, \quad n+r=2p+1, \quad \text{Изм}\frac{\mathfrak{W}}{(P_\infty^{n+r})}=0,$$

в силу чего формула (13) даёт:

(14) $$2p-1.$$

Мы уже получали это выражение, излагая первый способ вывода результата Римана.

## § 35. Подполя

Рассмотрим взаимоотношения между элементами и точками полей алгебраических функций и их подполей. Пусть $k(x, y)$ есть поле алгебраических функций с коэффициентами из числового поля $k$, которое мы будем считать алгебраически замкнутым. Пусть $k_1$ будет подполе поля $k(x, y)$ и пусть оно содержит поле $k$. Возьмём внутри $k_1$ элемент, не входящий в $k$, и подберём к нему как элементу поля $k(x, y)$ элемент, составляющий с ним примитивную пару. Не нарушая общности, можно обозначать первый из этих элемеитов через $x$, а второй через $y$; другими словами, мы предположим, что $x$ входит в $k_1$. Пусть $z$ есть элемент поля $k_1$, составляющий с $x$ примитивную пару этого поля. Таким образом

$$k_1=k(x, z).$$

Пусть

(1) $$f(x, y)=0$$

есть неприводимое уравнение, связывающее $x$ и $y$, и пусть его степень есть $n$. Далее, пусть

(2) $$z=\varphi(x, y),$$

где правая часть есть рациональная функция от $x$ и полином от $y$. Чтобы получить уравнение, связывающее $x$ и $z$, можно поступать так, как мы указывали в § 4 (преобразоварие Чирнгаузена). Можно прийти к тому же результату, пользуясь теорией симметрических функций, излагаемой во всех курсах алгебры. Именно, оставляя $x$ неопределённым, мы обозначим через

(3) $$y_1, y_2, \ldots, y_n$$

корни уравнения (1). Далее, вводя обозначения

(4) $$z_i=\varphi(x, y_i) \qquad (i=1, 2, \ldots, n),$$
$$F(x, z)=(z-z_1)(z-z_2)\ldots(z-z_n),$$

мы убедимся, что коэффициенты при различных степенях $z$ в полиноме $F(x, z)$ как симметрические функции от (3) рационально выражаются через коэффициенты уравнения (1), т. е. являются рациональными функциями от $x$. Если все элементы (4) различны, то уравнение

$$F(x, z) = 0 \tag{5}$$

неприводимо. В этом случае $k(x, z) = k(x, y)$. Если же элементы (4) частично или полностью совпадают друг с другом, то уравнение (5) имеет кратные корни. Более того:

Теорема 60. *Левая часть уравнения* (5) *есть степень неприводимого полинома.*

Доказательство. Допустим противное. Тогда $F(x, z)$ располагается в произведение взаимно простых полиномов

$$F(x, z) = G(x \cdot z) \cdot H(x, z), \tag{6}$$

причём можно найти такие полиномы $U(x, z)$, $V(x, z)$ от $z$, рационально зависящие от $x$, что

$$G(x, z) \cdot U(x, z) + H(x, z) \cdot V(x, z) = 1. \tag{7}$$

Вместе с тем подстановка (2) переводит $F(x, z)$, а также $G(x, z)$ и $H(x, z)$ в полиномы от $y$, имеющие с $f(x, y)$ общие корни и потому в силу неприводимости $f(x, y)$ делящиеся на $f(x, y)$. Таким образом, подставляя в (7) вместо $z$ полином $\varphi(x, y)$, мы в левой части получим полином от $y$, делящийся на $f(x, y)$, а в правой части единицу. Противоречие доказывает теорему.

Пусть

$$F(x, z) = \{h(x, z)\}^r, \tag{8}$$

где $h(x, z)$ — неприводимый полином. Число $r$ есть не что иное, как степень алгебраического расширения $k(x, y) : k(x, z)$. Поле $k(x, z)$ определяется соотношением

$$h(x, z) = 0; \tag{9}$$

степень этого уравнения относительно $z$ есть $n_1$, где

$$n = r \cdot n_1. \tag{10}$$

Отсюда следует, что порядок элемента $x$ как элемента поля $k(x, z)$ в $r$ раз меньше, чем его порядок как элемента поля $k(x, y)$. Поскольку в качестве $x$ мы могли бы взять всякий непостоянный элемент поля $k(x, z)$ и $r$ не зависит от этого выбора, мы заключаем, что порядок всякого элемента поля $k(x, z)$ увеличивается в $r$ раз, если его рассматривать внутри поля $k(x, y)$. Другими словами, этот элемент представляется в $k(x, y)$ в виде частного от произведений в $r$ раз большего числа простых дивизоров, чем в поле $k(x, z)$.

Выясним взаимоотношение между простыми дивизорами (точками) в обоих полях более детально. Точка $\pi$ поля $k(x, z)$ есть совокупность значений, которые принимают элементы этого поля, причём две точки считаются различными в том и только в том случае, если в поле $k(x, z)$ существует хотя бы один элемент, принимающий в этих точках различные значения. Отсюда следует, что всякой точке $P$ поля $k(x, y)$ соответствует одна определённая точка $\pi$ поля $k(x, z)$. Однако различным точкам $P$, $P'$ поля $k(x, y)$ может соответствовать одна и та же точка $\pi$ поля $k(x, z)$. Пусть $y$ есть тот элемент поля $k(x, y)$, который в точках $P$, $P'$ принимает различные значения. Элементы $x$ и $z$, как лежащие в $k(x, z)$, принимают в $P$ и $P'$ одинаковые значения. Обращаясь к формуле (2), мы из теоремы 60 заключаем, что $n$ значениям $y$, соответствующим одному и тому же значению $x$, соответствует $n_1$ различных значений элемента $z$, причём каждому значению $z$ соответствует $r$ значений $y$. Это значит, что каждой точке поля $k(x, z)$ соответствует $r$ различных точек поля $k(x, y)$, причём задание одной точки поля $k(x, y)$ вполне определяет точку поля $k(x, z)$ и тем самым $r-1$ остальных точек поля $k(x, y)$.

Пусть $P_1, P_2, \ldots, P_r$ будут точки поля $k(x, y)$, которым соответствует одна и та же точка $\pi$ поля $k(x, z)$. Рассмотрим определяемые этими точками простые дивизоры в обоих полях. Пусть $u$ есть элемент поля $k(x, z)$ и пусть он как элемент поля $k(x, y)$ делится на $P_1$, т. е. обращается в точке $P_1$ в нуль. Поскольку все элементы поля $k(x, z)$ принимают в каждой из точек $P_1, P_2, \ldots, P_r$ одно и то же значение, элемент $u$ делится на каждый из простых дивизоров $P_1, P_2, \ldots, P_r$, а потому и на их произведение. В силу этого простой дивизор $\cdot\pi$ поля $k(x, z)$ в поле $k(x, y)$ разлагается в произведение $r$ простых дивизоров:

$$\pi = P_1 \cdot P_2 \ldots P_r. \tag{11}$$

Мы разобрали случай, когда все простые дивизоры, на которые делится дивизор $\pi$, простой внутри поля $k(x, z)$, различны. Рассмотрим общий случай. Пусть $\pi$ есть дивизор, простой внутри поля $k(x, z)$, и пусть внутри поля $k(x, y)$ он разлагается в произведение простых дивизоров следующим образом:

$$\pi = P_1^{\eta_1} \cdot P_2^{\eta_2} \ldots P_k^{\eta_k}. \tag{12}$$

Возьмём от обеих частей норму, как от дивизора поля $k(x, y)$. Правая часть даёт в качестве нормы полином от $x$ степени

$$\eta_1 + \eta_2 + \ldots + \eta_k.$$

Для нахождения же нормы от левой части обратим внимание на то, что норма от $t-u$, где $t$ — неопределённая переменная, а $u$ — элемент поля $k(x, y)$, есть левая часть уравнения $n$-й степени, кото-

рому удовлетворяет $u$. В частности, если $u$ лежит в поле $k(x, z)$, то эта норма есть $r$-я степень полинома $n$-й степени, который имеет корнем $u$. Другими словами, норма от элемента поля $k(x, z)$, но внутри поля $k(x, y)$ равна $r$-й степени этого элемента внутри поля $k(x, z)$. Вспоминая, что норма простого дивизора $\pi$ есть $x - c$, где $c$ — значение элемента $x$ в точке $\pi$, и что $N(u)$ делится точно на первую степень $x - c$, если $u$ делится точно на первую степень $\pi$, мы видим, что норма простого дивизора $\pi$ поля $k(x, z)$ есть $r$-я степень линейного относительно $x$ полинома. Таким образом

$$\eta_1 + \eta_2 + \ldots + \eta_k = r. \tag{13}$$

В частности, если все $\eta_i = 1$, мы придём к разложению (11).

Найдём зависимость между жанрами обоих полей. Для этого рассмотрим дивизор $Z_x$, являющийся произведением (в соответствующих степенях) критических простых дивизоров поля $k(x, y)$. Его порядок равен

$$w_x = 2p - 2 + 2n.$$

Рассмотрим произвольный простой дивизор $P_\mu$, входящий в $Z_x$. Пусть он входит в простой дивизор $\pi_\mu$ поля $k(x, z)$ в степени $\eta_\nu$ и пусть $\pi_\mu$ входит в $x - c$ в степени $e_\mu$. Тогда $P_{\mu,\nu}$ войдёт в $x - c$ в степени $e_\mu \eta_\nu$, так что

$$Z_x = \prod_{\mu,\nu} P_{\mu,\nu}^{e_\mu \eta_\nu - 1}. \tag{14}$$

Перепишем эту формулу так:

$$Z_x = \prod_{\mu,\nu} P_{\mu,\nu}^{(e_\mu - 1)\eta_\nu} \cdot \prod_{\mu,\nu} P_{\mu,\nu}^{\eta_\nu - 1}.$$

В первом произведении правой части выполним умножение сначала по значку $\nu$, принимая во внимание, что

$$\prod_{\nu} P_{\mu,\nu}^{\eta_\nu} = \pi_\mu.$$

Получим:

$$Z_x = \prod_{\mu} \pi_\mu^{e_\mu - 1} \cdot \prod_{\mu,\nu} P_{\mu,\nu}^{\eta_\nu - 1}. \tag{15}$$

Первый множитель правой части есть не что иное, как дивизор критичности поля $k(x, z)$; обозначим его через $\zeta_x$. Второй множитель правой части можно назвать *дивизором относительной критичности* поля $k(x, y) : k(x, z)$; в настоящий момент для нас важно лишь то, что его порядок не отрицателен; пусть этот порядок будет равен $\tilde{w}$. Сравним порядки обеих частей формулы (15). Тогда, при-

нимая во внимание, что порядок дивизора $\pi_\mu$ внутри $k(x, y)$ равен $r$, и обозначая порядок дивизора $\zeta_\alpha$ внутри $k(x, z)$ через $w'_x$, получим:

$$w_x = r \cdot w'_x + \tilde{w}. \tag{16}$$

Обозначая через $\rho_1$ жанр поля $k(x, z)$, будем иметь

$$2\rho - 2 + 2n = r(2\rho_1 - 2 + 2n_1) + \tilde{w},$$

откуда в силу (10):

$$2\rho - 2 = r(2\rho_1 - 2) + \tilde{w}. \tag{17}$$

Это соотношение позволяет сделать весьма важные выводы. Именно, из неравенств

$$\rho \geqslant 0, \quad \rho_1 \geqslant 0, \quad r \geqslant 2, \quad \tilde{w} \geqslant 0$$

мы получим

$$2\rho - 2 \geqslant 2(2\rho_1 - 2),$$

т. е.

$$\rho_1 \leqslant \frac{\rho + 1}{2}. \tag{18}$$

Если $\rho = 0$, то $\rho_1 \leqslant \frac{1}{2}$, т. е. $\rho_1 = 0$.

Это составляет содержание теоремы Люрота, для которой мы таким образом получаем новое доказательство.

Если $\rho = 1$, то $\rho_1 \leqslant 1$. Это показывает, что подполями эллиптического поля могут быть только рациональные и эллиптические поля. Здесь существование рациональных подполей тривиально. Более детальное исследование дало бы возможность установить существование бесчисленного миожества эллиптических подполей.

Наконец, если $\rho > 1$, то $\rho_1 < \rho$, и мы приходим к

Теореме 61. *В поле алгебраических функций жанра* $\rho$ *жанр всякого подполя меньше* $\rho$, *за исключением случаев* $\rho = 0$ и $\rho = 1$, *когда он может быть равен* $\rho$.

Установим понятия *некритичных* (unverzweigt) расширений, абсолютных и относительных.

Под *некритичным расширением* над $k(x)$ мы будем разуметь поле $k(x, y) : k(x)$, не содержащее критических простых дивизоров. Это свойство характеризуется равенством $w_x = 0$. В силу

$$w_x = 2\rho - 2 + 2n_x, \qquad p \geqslant 0,$$

оно возможно только при

$$\rho = 0, \quad n_x = 1,$$

а в этом случае $k(x, y)$ совпадает с полем $k(x)$, т. е. никакого расширения нет. Таким образом абсолютно некритичных расширений не существует.

Под относительно некритичным расширением $k(x,y):k(x,z)$ мы будем разуметь поле $k(x,y)$, не содержащее *относительно критических простых дивизоров*, т. е. простых дивизоров, содержащихся в простых дивизорах поля $k(x,z)$ выше, чем в первой степени. Это свойство характеризуется равенством $\tilde{w}=0$, которое может иметь место для многих полей. Например, если оба поля $k(x,y)$ и $k(x,z)$ эллиптические, то, как показывает равенство (17), расширение $k(x,y):k(x,z)$ некритично.

Эти факты имеют также место в теории алгебраических чисел, где они получаются далеко не так просто и приводят к весьма глубокой теории *полей классов* (Klassenkörper). Например, несуществование абсолютных некритичных расширений соответствует знаменитой теореме Минковского: «дискриминант поля не может быть равен единице», которая была с трудом доказана методами геометрии чисел.

Эти первоначальные соображения далеко недостаточны для решения задачи перечисления всех подполей поля алгебраических функций, задачи, которая, насколько я знаю, никем не ставилась. Эта задача является аналогом основной задачи теории Галуа в поле алгебраических чисел. Повидимому, она весьма трудна.

## § 36. Результаты Гурвица в теории групп преобразований в себя

Гурвиц, опираясь на теорию подполей, изложенную в предыдущем параграфе, получил для порядка группы преобразований в себя поля алгебраических функций жанра $\rho>1$ верхнюю границу. Его соображения настолько красивы и открываемые ими перспективы настолько широки, что я решил воспроизвести часть его исследований.

Пусть $k(x,y)$ — поле алгебраических функций жанра $\rho>1$. Мы уже доказали, что число преобразований в себя этого поля конечно (см. теорему 53). Пусть

$$S=\mathfrak{E},\ S_2,\ \ldots,\ S_r$$

— эти преобразования и пусть они переводят элемент $y$ соответственно в

$$\varphi_1(x,y)=y,\quad \varphi_2(x,y),\ldots,\quad \varphi_r(x,y).$$

Элементарные симметрические функции от этих элементов, т. е. коэффициенты полинома

$$(1)\qquad \prod_{i=1}^{r}\{t-\varphi_i(x,y)\}=F(t)=t^r+A_1\cdot t^{r-1}+\ldots+A_r,$$

являются *инвариантами* группы преобразований в себя, т. е. элементами, не изменяющимися при производстве над ними преобразо-

ваний в себя. Это следует из того, что каждое преобразование $S_i$ переводит элементы $\varphi_i(x, y)$ друг в друга и притом не может перевести два различных из этих элементов в один и тот же. Поэтому произведение (1) выражений

$$t - \varphi_i(x, y)$$

при произвольном $t$ переводится в себя.

Все инварианты

$$A_1, A_2, \ldots, A_r$$

не могут быть одновременно постоянными, так как тогда были бы постоянны корни полинома $F(t)$ и, в частности, $y$. С другой стороны, сумма и произведение двух инвариантов являются тоже инвариантами, в силу чего совокупность инвариантов поля $k(x, y)$ составляет поле, отличное от поля $k$. Пусть это будет поле $k(x, z)$ и пусть его жанр будет $\rho_1$. Далее, пусть $y$ будет элемент, составляющий вместе с $x$ примитивную пару поля $k(x, y)$.

Составим для элемента $y$ полином $F(t)$. Его коэффициенты являются инвариантами и, следовательно, элементами поля $k(x, z)$. Этот полином неприводим в поле $k(x, z)$. В самом деле, все элементы $\varphi_i(x, y)$ $(i = 2, 3, \ldots, r)$ отличны от $\varphi_1(x, y) = y$, так как равенство

$$y = \varphi_i(x, y)$$

означало бы, что преобразование $S_i$ не меняет элемента $y$. Но так как $x, y$ есть примитивная пара поля $k(x, y)$, то любой элемент из $k(x, y)$ рационально выражается через $x, y$ и в силу нашего предположения инвариантен относительно преобразования $S_i$. Это означает, что $S_i$ есть тождественное преобразование, чего мы не предполагаем.

Допустим, что полином $F(t)$ приводим в поле $k(x, z)$; пусть $H(t)$ будет тот его неприводимый множитель, который имеет корнем $y$, и пусть

$$F(t) = H(t) \cdot R(t).$$

Полином $R(t)$ не имеет $y$ корнем и, следовательно, взаимно прост с $H(t)$. Пусть $\varphi_k(x, y)$ будет корень полинома $R(t)$ и, следовательно, не будет корнем полинома $H(t)$. Тогда

$$H(y) = 0, \tag{2}$$

$$H\{\varphi_k(x, y)\} \neq 0. \tag{3}$$

В отношении (2) выразим коэффициенты через $x$, $z$ и подвергнем его преобразованию $S_k$. Поскольку $S_k$ есть преобразование в себя, это соотношение должно сохраняться. При этом коэффициенты как функции от $x$, $z$ останутся неизменными, и мы получим

$$H\{\varphi_k(x, y)\} = 0,$$

что стоит в противоречии с (3). Поэтому полином $F(t)$ неприводим.

Таким образом всякий элемент поля $k(x, y)$ может быть представлен через базис $[1, y, \ldots, y^{r-1}]$ с коэффициентами из поля $k(x, z)$, т. е. $r$ есть относительная степень поля $k(x, y) : k(x, z)$. Это позволяет нам воспользоваться формулой (17) § 35

$$2\rho - 2 = r(2\rho_1 - 2) + \tilde{w}, \tag{4}$$

где

$$\tilde{w} = \sum_{\mu=1}^{a} \sum_{\nu=1}^{k_\mu} (\eta_\nu - 1), \tag{5}$$

$$\sum_{\nu=1}^{k_\mu} \eta_\nu = r. \tag{6}$$

Воспользуемся тем, что корни полинома $F(t)$ рационально выражаются через один в поле $k(x)$. Согласно выработанной в теории Галуа терминологии, уравнение

$$F(t) = 0$$

*нормально*. Мы докажем, что в этом случае все простые дивизоры поля $k(x, y)$, на которые делится простой дивизор поля $k(x, z)$, входят в него в одной и той же степени; другими словами, что при данном $\mu$ все $\eta_\nu$ равны друг другу. Пусть $u$ будет элемент поля $k(x, y)$, делящийся точно на первую степень простого дивизора $P$ и более не делящийся на простые делители того простого дивизора $\pi$ поля $k(x, z)$, на который делится $P$; $u$ есть корень уравнения

$$\Phi(t) = t^r + B_1 \cdot t^{r-1} + \ldots + B_r = 0$$

$r$-й степени. Другие его корни,

$$u_2, u_3, \ldots, u_r, \tag{7}$$

являются элементами поля $k(x, y)$, в которые переходит $u$ после преобразований

$$S_2, S_3, \ldots, S_r.$$

Каждый из этих корней делится точно на первую степень одного из простых дивизоров $P_1 = P, P_2, \ldots, P_k$, где

$$P_1^{\eta_1} \cdot P_2^{\eta_2} \ldots P_k^{\eta_k} = \pi.$$

Коэффициент $B_r$ делится точно на первую степень простого дивизора $\pi$ поля $k(x, z)$.

Пусть

$$S_1 = \mathfrak{E}, S_2, \ldots, S_q \tag{8}$$

будут преобразования, не меняющие простого дивизора $P_1$. Это значит, что $u_1, u_2, \ldots, u_\eta$ и только эти корни (7) делятся на простой дивизор $P_1$. Совокупность преобразований (8) составляет группу, которая является подгруппой группы всех преобразований в себя. Обозначим её через $\mathfrak{H}$. Пусть

$$T_2, T_3, \ldots, T_k$$

будут какие-нибудь преобразования в себя, переводящие $P_1$ соответственно в

$$P_2, P_3, \ldots, P_k.$$

Тогда смежные классы

$$T_2\mathfrak{H}, T_3\mathfrak{H}, \ldots, T_k\mathfrak{H}$$

будут состоять из преобразований, переводящих $P_1$ соответственно в $P_2, P_3, \ldots, P_k$. Всякое преобразование смежного класса $T_i\mathfrak{H}$ переведёт $u_1$ в один из корней (7), который делится на $P_i$. Таким образом среди корней (7) будет точно $\eta$ таких, которые делятся на $P_i (i = 1, 2, \ldots, k)$. Из соотношения

$$u_1 \cdot u_2 \ldots u_k = (-1)^r B_r$$

мы заключаем, что $B_r$, а с ним и $\pi$ точно делятся на $P_i^\eta$ $(i = 1, 2, \ldots, k)$, так что

$$\pi = (P_1 \cdot P_2 \ldots P_k)^\eta, \tag{9}$$

$$\eta \cdot k = r, \tag{10}$$

ч. т. д.

Пользуясь полученным результатом, преобразуем внутреннюю сумму формулы (5):

$$\sum_{\nu=1}^{k_\mu} (\eta_\nu - 1) = r - k_\mu = r - \frac{r}{\eta_{|\mu}}.$$

Подставляя в формулу (4), которую мы предварительно разделим на $r$, получим

$$\frac{2\rho - 2}{r} = 2\rho_1 - 2 + a - \frac{1}{\eta_1} - \frac{1}{\eta_2} - \ldots - \frac{1}{\eta_a}, \tag{11}$$

где $a$ — число различных простых дивизоров поля $k(x, z)$, делящихся на высшие степени простых дивизоров поля $k(x, y)$.

Соотношение (11) позволяет получить для числа $r$ верхнюю границу. Сделаем относительно $\rho_1$ несколько предположений:

1) $\rho_1 \geqslant 2$. Тогда

$$r \leqslant \rho - 1. \tag{12}$$

2) $\rho_1 = 1$. Тогда в силу

$$1 - \frac{1}{\eta_i} \geqslant \frac{1}{2}$$

имеем

$$\frac{2\rho - 2}{r} \geqslant \frac{1}{2},$$

откуда

$$r \leqslant 4(\rho - 1). \tag{13}$$

3) $\rho_1 = 0$. Тогда

$$\frac{2\rho - 2}{r} = a - 2 - \frac{1}{\eta_1} - \frac{1}{\eta_2} - \ldots - \frac{1}{\eta_a}. \tag{14}$$

Если бы имело место $a \leqslant 2$, то правая часть (14) имела бы отрицательное значение, что при $\rho > 1$ невозможно. Поэтому $a \geqslant 3$.

A) Пусть $a \geqslant 5$. Тогда

$$\frac{2\rho - 2}{r} \geqslant \frac{5}{2} - 2 = \frac{1}{2},$$

откуда опять имеет место (13).

B) Пусть $a = 4$. Тогда случай $\eta_i = 2$ $(i = 1, 2, 3, 4)$ приводит к невозможному равенству

$$\frac{2\rho - 2}{r} = 0.$$

Поэтому по крайней мере один из $\eta_i \geqslant 3$, в силу чего

$$\frac{2\rho - 2}{r} \geqslant 2 - \frac{1}{3} - \frac{1}{2} - \frac{1}{2} - \frac{1}{2} = \frac{1}{6},$$

откуда

$$r \leqslant 12(\rho - 1). \tag{15}$$

C) Пусть $a = 3$. Тогда из положительности правой части формулы (14) мы выводим

$$\frac{1}{\eta_1} + \frac{1}{\eta_2} + \frac{1}{\eta_3} < 1, \tag{16}$$

откуда следует, что по крайней мере одна из дробей $\frac{1}{\eta_1}$, $\frac{1}{\eta_2}$, $\frac{1}{\eta_3}$ меньше трети. Пусть $\eta_1 \geqslant \eta_2 \geqslant \eta_3$. Тогда можно сделать следующие предположения:

C1) $$\eta_1 \geqslant \eta_2 \geqslant \eta_3 \geqslant 4.$$

Тогда формула (14) даёт

$$\frac{2\rho - 2}{r} \geqslant 1 - \frac{1}{4} - \frac{1}{4} - \frac{1}{4} = \frac{1}{4},$$

откуда

(17) $$r \leqslant 8(\rho - 1).$$

C2) $$\eta_1 \geqslant \eta_2 \geqslant 4, \qquad \eta_3 = 3,$$

и формула (14) даёт

$$\frac{2\rho - 2}{r} \geqslant 1 - \frac{1}{4} - \frac{1}{4} - \frac{1}{3} = \frac{1}{6},$$

откуда

(18) $$r \leqslant 12(\rho - 1).$$

C3) $$\eta_1 \geqslant 4, \quad \eta_2 = \eta_3 = 3,$$

и формула (14) даёт

$$\frac{2\rho - 2}{r} \geqslant 1 - \frac{1}{4} - \frac{1}{3} - \frac{1}{3} = \frac{1}{12},$$

откуда

(19) $$r \leqslant 24(\rho - 1).$$

Если $\eta_3 = 2$, то из (16) получим

$$\frac{1}{\eta_1} + \frac{1}{\eta_2} < \frac{1}{2},$$

в силу чего

$$\frac{1}{\eta_1} < \frac{1}{4}, \quad \eta_1 \geqslant 5, \quad \eta_2 \geqslant 3.$$

C4) Если

$$\eta_1 \geqslant 7,$$

то формула (14) даёт

$$\frac{2\rho - 2}{r} \geqslant 1 - \frac{1}{7} - \frac{1}{3} - \frac{1}{2} = \frac{1}{42},$$

откуда

(20) $$r \leqslant 84(\rho - 1).$$

C5) Если $\eta_1 = 6$, то из (16) получим

$$\frac{1}{\eta_2} < \frac{1}{3}, \quad \eta_2 \geqslant 4,$$

и формула (14) даёт

$$\frac{2\rho - 2}{r} \geqslant 1 - \frac{1}{6} - \frac{1}{4} - \frac{1}{2} = \frac{1}{2},$$

откуда

(21) $$r \leqslant 24\ (\rho - 1).$$

Таким образом во всех случаях имеет место (20), и мы приходим к

Теорема 62 (Гурвица). *Порядок группы преобразований в себя поля* $k(x, y)$ *жанра* $\rho$ *не превышает числа* $84(\rho - 1)$.

## Упражнения к главе V

1. Доказать, что всякое подмножество $\mathfrak{M}$ элементов ковечной группы, образующее ассоциативную систему, т. е. обладающее тем свойством, что из

$$a \subset \mathfrak{M}, \quad b \subset \mathfrak{M}$$

следует $ab \subset \mathfrak{M}$, образует группу.

2. *Знакопеременная группа.* Доказать, что совокупность подстановок симметрической группы, не меняющих значения произведения разностей

$$\prod_{\lambda > \mu} (x_\lambda - x_\mu),$$

образует подгруппу снмметрической группы индекса 2.

3. Группа подстановок над множеством $x_1, x_2, \ldots, x_n$ называется *транзитивной*, если она содержит подстановки, переводящие любой элемент $x_i$ в любой другой $x_k$. Доказать, что группа транзитивна, если она содержит подстановкн, переводящне $x_1$ в любой элемент $x_i$.

4. Дана группа $\mathfrak{G}$ подстановок над множеством $x_1, x_2, \ldots, x_n$. Совокупность подстановок группы $\mathfrak{G}$, оставляющнх $x_1$ на месте, называется её *стационарной подгруппой*. Доказать, что стацнонарвая подгруппа транзнтивной группы нмеет нндекс $n$.

5. Совокупность дробных линейных преобразованнй

$$x \longrightarrow \frac{a'x + b'y + c'}{ax + by + c}, \quad y \longrightarrow \frac{a''x + b''y + c''}{a_0x + b_0y + c_0}$$

составляет ассоциативную систему тогда и только тогда, еслн

$$\frac{a}{a_0} = \frac{b}{b_0} = \frac{c}{c_0}.$$

При какнх ограннчениях для коэффициентов эта совокупность составляет группу?

6. Элементамн ассоцнативной системы являются матрицы, т. е. системы нз $n^2$ чисел:

$$A = \begin{Vmatrix} a_{11}, a_{12}, \ldots, a_{1n} \\ a_{21}, a_{22}, \ldots, a_{2n} \\ \cdots\cdots\cdots \\ a_{n1}, a_{n2}, \ldots, a_{nn} \end{Vmatrix}, \quad B = \begin{Vmatrix} b_{11}, b_{12}, \ldots, b_{1n} \\ b_{21}, b_{22}, \ldots, b_{2n} \\ \cdots\cdots\cdots \\ b_{n1}, b_{n2}, \ldots, b_{nn} \end{Vmatrix}, \quad \ldots$$

Закон умножения определяется равенствами

$$AB = C = \begin{Vmatrix} c_{11}, c_{12}, \ldots, c_{1n} \\ c_{21}, c_{22}, \ldots, c_{2n} \\ \cdots\cdots\cdots \\ c_{n1}, c_{n2}, \ldots, c_{nn} \end{Vmatrix},$$

где

$$c_{ik} = a_{i1}b_{1k} + a_{i2}a_{2k} + \ldots + a_{in}b_{nk} \qquad (i, k = 1, 2, \ldots, n).$$

Доказать, что

а) умножение матриц подчиняется ассоциативному закону;

b) совокупность матриц, определитель которых $|A| \neq 0$, образует группу;

c) совокупность матриц, определнтели которых $|A| = 1$, образует подгруппу и притом нормальный делитель определённой в b) группы.

7. *Транспонированной* к матрице $A$ называется матрица

$$A' = \begin{Vmatrix} a_{11}, a_{21}, \ldots, a_{n1} \\ a_{12}, a_{22}, \ldots, a_{n2} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_{1n}, a_{2n}, \ldots, a_{nn} \end{Vmatrix}.$$

Доказать, что из $AB = C$ следует $B'A' = C'$.

8. *Ортогональной* называется матрица $A$ из вещественных чисел, удовлетворяющая соотношению

$$A \cdot A' = \mathfrak{E},$$

где $\mathfrak{E}$ есть единичная матрица:

$$\mathfrak{E} = \begin{Vmatrix} 1\ 0\ \ldots\ 0 \\ 0\ 1\ \ldots\ 0 \\ \cdot\ \cdot\ \cdot\ \cdot \\ 0\ 0\ \ldots\ 1 \end{Vmatrix}.$$

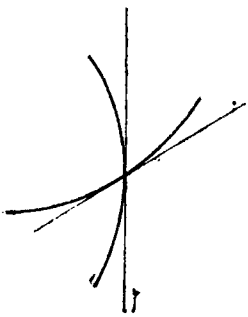
Доказать, что совокупность ортогональных матриц образует группу.

9. *Унитарной* называется матрица $A$ из комплексных чисел, удовлетворяющая соотношению

$$\bar{A} \cdot A' = \mathfrak{E},$$

где $\bar{A}$ — матрица, составленная из сопряжённо-комплексных чисел к числам, составляющим матрицу $A$. Доказать, что совокупность унитарных матриц образует группу.

10. Доказать, что поле алгебраических функций, допускающее преобразование в себя с периодом $n$, может быть задано соотношением типа $f(x, y^n) = 0$. (*Указание.* Для нахождения элемента $y$, переходящего при преобразовании в $e^{\frac{2\pi i}{n}} \cdot y$, применить приём, аналогичный приёму Лагранжа для решения в радикалах циклических уравнений.) (Шварц).



Черт 1.

11. Доказать, что поле алгебраических функций жанра $\rho > 1$ допускает только такие преобразования в себя, период которых не превышает $10(\rho - 1)$ (Гурвиц).

12. Пусть в особой точке, которую мы без нарушения общности можем считать началом координат, не все 2-е производные обращаются в нуль. Полагая $y = t \cdot x$, получим

$$f(x, y) = x^2 \cdot \varphi_2(t) + x^3 \cdot \varphi_3(t) + \ldots,$$

где $\varphi_k(t)$ — полиномы $k$-й степени. Доказать следующее:

a) Если корни полинома $\varphi_2(t)$ неравны, то (0,0) есть двойная точка с раздельными касательными (черт. 1).

b) Если полином $\varphi_2(t)$ имеет кратный корень, который не является корнем полинома $\varphi_3(t)$, то (0, 0) есть точка возврата 1-го рода (черт. 2).

c) Если полином $\varphi_2(t)$ имеет кратный корень $a$, который является также корнем полинома $\varphi_3(t)$, и притом, полагая $t - a = ux$, мы получим при $x = 0$ для $u$ два неравных значения, то точка (0, 0) есть точка самокасания (черт. 3).

d) Если оба корня для $u$ при $x = 0$ равны, то точка (0,0) в общем случае есть точка возврата 2-го рода (черт. 4).

Черт. 2.

Черт. 3.

Черт. 4.

13. Каково число параметров, которое может содержать поле $k(x, y)$, если определяющее его соотношение может быть приведено к виду кривой, лишённой особых точек? Исходя из формулы (7) § 32

$$d = (m-1)(n-1) - \rho,$$

показать, что в том случае, если $\rho$ есть простое число, $k(x, y)$ есть гиперэллиптическое поле, т. е. зависит от $2\rho - 1$ параметров. Исследовать вопрос для того случая, когда $\rho$ разлагается в произведение двух простых чисел.

14. *Число особых точек в проективном смысле.* Рассмотрим общую кривую $n$-го порядка. Определяемый ею элемент $y$ есть целая функция от $x$, так что имеет место представление

$$x \approx \frac{U'}{U}, \quad y \approx \frac{U''}{U},$$

где $U$, $U'$, $U''$ — попарно взаимно простые дивизоры $n$-го порядка, причём предположим, что все простые делители дивизора $U$ различны. Тогда дивизор $D$ особых точек содержит $U$ точно в $(n-1)$-й степени (см. теорему 55). Полагая

$$D = U^{n-1} \cdot D_0,$$

мы получим для порядка $d_0$ дивизора $D_0$ выражение

$$d_0 = \frac{(n-1)(n-2)}{2} - \rho.$$

15. *Главная кривая.* Элементы поля $k(x, y)$, представляемые отношениями $\rho$ линейно независимых дивизоров класса дифференциалов $\mathfrak{B}$:

$$z_1 \approx \frac{W_1}{W_0}, \quad z_2 \approx \frac{W_2}{W_0}, \quad \ldots, \quad z_{\rho-1} \approx \frac{W_{\rho-1}}{W_0},$$

образуют в $(\rho-1)$-мерном пространстве кривую, называемую *главной кривой*. Доказать, что в том случае, если $k(x, y)$ не есть гиперэллиптическое поле, главная кривая не имеет особых точек (т. е. что общий делитель числителей $W_1, W_2, \ldots, W_{\rho-1}$ не может быть дивизором выше 1-го порядка).

Если $k(x, y)$ — гиперэллиптическое поле, то элементы $z_i$ лежат в подполе $k(x)$, а потому всякая точка главной кривой есть двойная точка.

---

# ГЛАВА VI

# ПРИМЕНЕНИЯ ТЕОРИИ АНАЛИТИЧЕСКИХ ФУНКЦИЙ

## § 37. Сведения из общей теории аналитических функций

Начиная с настоящей главы, мы покидаем почву арифметической теории алгебраических функций и изложим те отделы теории, которые существенным образом опираются на общую теорию аналитических функций. Здесь мы должны предположить у читателя знание основ теории аналитических функций (функций комплексной переменной).

В настоящем параграфе мы напомним читателю основные факты, которыми в дальнейшем будем пользоваться. С их выводами можно познакомиться по любому курсу теории аналитических функций.

Аналитической функцией $f(z)$ комплексной переменной $z = x = iy$ называется функция вида

$$f(z) = u(x, y) + iv(x, y), \tag{1}$$

где вещественные функции $u$, $v$ и двух вещественных переменных $x$, $y$ предполагаются дифференцируемыми внутри некоторой области $K$ плоскости комплексной переменной $z$ и удовлетворяющими внутри $K$ дифференциальным уравнениям

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \qquad \frac{\partial u}{\partial y} = \frac{\partial v}{\partial x}, \tag{2}$$

носящим название *уравнений Коши-Римана.*

Под плоскостью комплексной переменной $z = x + iy$ мы разумеем плоскость с выбранной в ней прямоугольной системой координат, причём составляющие $x$, $y$ комплексной переменной $z$ принимаются за координаты точки в этой плоскости, так что между значениями переменной $z$ и точками плоскости устанавливается взаимно однозначное соответствие.

I. Аналитическая функция $f(z)$ имеет в каждой точке области $K$ производную, т. е. предел

$$\lim_{\Delta z \to 0} \frac{\Delta f}{\Delta z} = f'(z),$$

значение которого не зависит от характера стремления к нулю составляющих $\Delta x$, $\Delta y$ приращения $\Delta z = \Delta x + i\Delta y$.

II. Каждой точке плоскости переменной $z = x + iy$ аналитическая функция $w = f(z) = u + iv$ приводит в соответствие точку плоскости переменной $w$, т. е. осуществляет *отображение* одной плоскости на другую: каждой линии плоскости $z$ соответствует линия плоскости $w$, и т. д. Это отображение *конформно*: если две линии в плоскости $z$ пересекаются под углом $\theta$, то в плоскости $w$ им соответствуют две линии, пересекающиеся под тем же углом $\theta$. При этом направлению угла (например, против часовой стрелки) в плоскости $z$ соответствует то же направление угла в плоскости $w$ (конформное отображение 1-го рода).

III. *Теорема Коши. Спрямляемой* называется кривая, для которой длина дуги имеет определённое конечное значение. Если замкнутая спрямляемая кривая $C$ ограничивает область, целиком лежащую в $K$, то криволинейный интеграл

$$\int_C f(z)\,dz = \int_C (u\,dx - v\,dy) + i\int_C (v\,dx + u\,dy) = 0 \tag{3}$$

равен нулю. Здесь существенно требование, чтобы функция $f(z)$ внутри области, ограниченной кривой $C$, удовлетворяла перечисленным условиям, или, как принято говорить, была *регулярной*.

Для наших целей достаточно, если мы в роли спрямляемых кривых постоянно будем брать ломаные из конечного числа звеньев, а также дуги окружностей.

Справедливость формулы (3) является следствием *формулы Грина*

$$\int_C \{P(x, y)\,dx + Q(x, y)\,dy\} = \int\int \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right) dx\,dy \tag{4}$$

и соотношений (2). Двойной интеграл в правой части распространён на область, ограниченную кривой $C$. При этом в дальнейшем мы будем предполагать, что криволинейный интеграл по замкнутому контуру берётся в таком направлении, чтобы при обходе внутренность контура оставалась слева.

IV. *Формула Коши.* Если относительно $C$ сделаны те же предположения, что и в III, и если точка $a$ лежит внутри $C$, то

$$f(a) = \frac{1}{2\pi i}\int \frac{f(z)\,dz}{z - a}. \tag{5}$$

Может показаться, что формула (5) противоречит формуле (3), в которой мы положим

$$f_1(z) = \frac{f(z)}{z - a}.$$

Разъяснение этого противоречия заключается в том, что $f_1(z)$ не везде внутри $C$ регулярна; именно, в точке $a$ она обращается в бесконечность.

V. *Ряд Тейлора.* Если точка $a$ взята внутри области $K$ [в дальнейшем будем говорить: внутри области регулярности функции $f(z)$], то в этой точке могут быть определены значения всех высших производных функций $f(z)$:

$$f^{(n)}(a)=\frac{n!}{2\pi i}\int\limits_C \frac{f(z)\cdot dz}{(z-a)^{n+1}} \qquad (n=1,\ 2,\ 3,\ \ldots), \tag{6}$$

где $C$ — любой спрямляемый контур, целиком лежащий внутри $K$ и содержащий внутри себя точку $z=a$. При этом функция $f(z)$ разлагается в ряд

$$f(z)=f(a)+\frac{f'(a)}{1}(z-a)+\frac{f''(a)}{2!}(z-a)^2+\ldots \\ \ldots+\frac{f^{(n)}(a)}{n!}(z-a)^n+\ldots, \tag{7}$$

который сходится для всех точек $z$, лежащих внутри круга с центром в точке $z=a$, и расходится для точек $z$, лежащих вне этого круга. В силу этого указанный круг называется *кругом сходимости.* С одной стороны, внутри круга сходимости функция $f(z)$ регулярна; с другой стороны, на его границе непременно имеется хотя бы одна точка, в которой функция $f(z)$ перестаёт быть регулярной.

VI. *Ряд Лорана* (Laurent). Пусть функция $f(z)$ однозначна и регулярна внутри кольца, ограниченного двумя окружностями $C$ и $c$ радиусов $R$ и $r$ $(R>r)$ с центром в точке $z=a$. Тогда $f(z)$ разлагается в сходящийся внутри кольца ряд, расположенный как по положительным, так и по отрицательным степеням $z-a$:

$$f(z)=a_0+a_1(z-a)+a_2(z-a)^2+\ldots \\ \ldots+\frac{b_1}{z-a}+\frac{b_2}{(z-a)^2}+\ldots, \tag{8}$$

где коэффициенты имеют следующие выражения:

$$a_n=\frac{1}{2\pi i}\int\limits_C \frac{f(z)\,dz}{(z-a)^{n+1}} \qquad (n=1,\ 2,\ 3,\ \ldots), \tag{9}$$

$$b_n=\frac{1}{2\pi i}\int\limits_C f(z)\,(z-a)^{n-1}\,dz \qquad (n=1,\ 2,\ 3,\ \ldots). \tag{10}$$

Поскольку $f(z)$ внутри круга $c$ не регулярна, не следует считать, что

$$a_n=\frac{f^{(n)}(a)}{n!} \qquad \text{[см. (6)]}.$$

Особый интерес представляет случай, когда $f(z)$ регулярна везде внутри $C$, за исключением точки $z=a$. В этом случае говорят, что $f(z)$ имеет в точке $z=a$ *изолированную особую точку*. Часть ряда (8), содержащая отрицательные степени $z-a$, называется *главной частью* функции $f(z)$ в точке $z=a$. Если она равна нулю, $f(z)$ регулярна в точке $z=a$; если она состоит из конечного числа членов, говорят, что точка $z=a$ является *полюсом* функции $f(z)$, притом $m$-й кратности, если

$$b_m \neq 0, \quad b_n = 0 \qquad (n = m+1,\ m+2,\ \ldots).$$

Если $f(z)$ имеет в точке $z=a$ полюс $m$-й кратности, то произведение

$$(z-a)^m f(z)$$

регулярно в точке $z=a$. Если $z$ приближается к $a$, то $f(z)$ стремится к бесконечности.

Если главная часть функции $f(z)$ для точки $z=a$ состоит из бесконечного числа членов, то точка $z=a$ носит название *существенно особой точки* функции $f(z)$. Если $z=a$ есть существенно особая точка функции $f(z)$, то, в отличие от полюса, при приближении $z$ к $a$ функция $f(z)$ не стремится к бесконечности, а принимает значения, сколь угодно близкие к произвольно заданному числу (теорема Вейерштрасса). Мы не будем в дальнейшем иметь дела с существенно особыми точками, поскольку ни рациональные, ни алгебраические функции их не имеют.

VII. *Критические особые точки.* Так называются особые точки аналитической функции, в любой окрестности которых функция не однозначна. Примером критической точки может служить точка $z=a$ для функции

$$w = \sqrt[n]{z-a}.$$

Если положить

$$z-a = \rho \cdot e^{i\theta},$$

то

$$w = \sqrt[n]{\rho} \cdot e^{i\frac{\theta}{n}}.$$

Если заставить точку $z$ пробежать окружность радиуса $\rho$ вокруг $z=a$, т. е., сохраняя $\rho$ постоянным, заставить аргумент $\theta$ пробежать непрерывный ряд значений от 0 до $2\pi$, то функция $w$ не вернётся к своему первоначальному значению, а приобретёт множитель

$$\varepsilon = e^{\frac{2\pi i}{n}}, \quad \varepsilon^n = 1.$$

Только после $n$-кратного пробега $z$ вокруг точки $a$ мы вернёмся к исходному значению функции $w$. Более общим примером критиче-

ской точки является случай сходящегося ряда, расположенного по целым степеням $(z-a)^{\frac{1}{n}}$. Такого рода критические точки характерны для алгебраических функций, и мы подробнее изучим их в § 38.

Примером другого рода критических точек является точка $z=a$, для функции

$$w=\ln(z-a).$$

Полагая

$$z-a=\rho e^{i\theta},$$

мы будем иметь

$$w=\ln\rho+i\theta.$$

Если попрежнему заставить $z$ пробежать окружность вокруг точки $a$, то функция $w$ приобретёт аддитивное приращение $2\pi i$. Сколько бы раз мы ни пробежали окружность, мы никогда не вернёмся к исходному значению $w$. Такие критические точки называются *логарифмическими* в отличие от рассмотренных ранее *алгебраических критических точек*.

VIII. *Теорема Лиувилля.* Если функция регулярна для всех значений $z$, не исключая и значения $z=\infty$, то она равна постоянной.

При этом под поведением функции $f(z)$ в точке $z=\infty$ надо разуметь поведение функции $f\left(\frac{1}{z_1}\right)$ в точке $z_1=0$, совершенно так же, как мы уже имели это в арифметической теории.

Из теоремы Лиувилля вытекают важные следствия, позволяющие определять класс функции по характеру её особых точек, как мы сейчас в этом убедимся.

IX. *Рациональные функции.* Всякая рациональная функция в любой точке или регулярна, или имеет полюс. В этом легко убедиться при помощи разложения рациональных функций на частные дроби, применяемого обычно в интегральном исчислении. В частности, полином имеет полюс только в точке $z=\infty$.

Обратно, пользуясь теоремой Лиувилля, легко доказать, что функция, не имеющая других особых точек, кроме полюсов, непременно является рациональной функцией. Прежде всего доказывается, что в таком случае число полюсов функции конечно: иначе точка сгущения полюсов была бы особой точкой, но не полюсом. Далее, вычитая из функции главные части, соответствующие всем её полюсам (включая и $z=\infty$), мы придём ко всюду регулярной функции, которая в силу теоремы Лиувилля равна постоянной.

X. *Алгебраические функции.* Алгебраической функцией называется функция $w$, связанная с независимой переменной $z$ алгебраическим уравнением

$$f(z,\ w)=0. \tag{11}$$

Если степень этого уравнения относительно $w$ есть $n$, то каждому значению $z$ соответствует $n$ значений $w$; функция $w$, таким образом,

неоднозначна. Если значения $z_0$, $w_0$ удовлетворяют уравнению (11), и притом

$$\frac{\partial f(z_0, w_0)}{\partial w} \neq 0, \tag{12}$$

то, дифференцируя уравнение (11) любое число раз в предположении, что $w$ есть функция от $z$, мы получим значения производных всех порядков от $w$ по $z$ в точке $(z_0, w_0)$; пользуясь формулой (7), мы получим разложение $w$ в ряд по целым степеням $z - z_0$, который будет сходиться внутри окружности, проходящей через ближайшую особую точку функции $w$, т. е. или её полюс, или точку, в которой

$$\frac{\partial f(z_0, w_0)}{\partial w} = 0. \tag{13}$$

Но так как последние точки обращают в нуль дискриминант уравнения (11), который является полиномом от $z$, то общее число особых точек функции $w$ конечно. В § 38 мы увидим, что в точке, для которой имеет место (13), функция $w$ разлагается в ряд по *дробным* степеням $z - z_0$, т. е. является алгебраической критической точкой.

Таким образом особые точки алгебраических функций могут быть только или полюсами, или алгебраическими критическими точками. Обратно, ниже мы убедимся, что всякая функция, имеющая особые точки только типа полюсов и алгебраических критических точек, непременно является алгебраической функцией.

XI. *Единственность определения аналитической функции.* Известно, что две аналитические функции, значения которых совпадают в какой-нибудь области или даже вдоль кривой, лежащей внутри области регулярности обеих функций, то они совпадают во всей области, в которой эти функции могут быть определены.

XII. *Аналитическое продолжение.* Упомянутое свойство позволяет расширить область $K$, в которой функция $f(z)$ была первоначально определена. Выбрав внутри $K$ круг $C_1$ с центром в точке $z = a_1$, мы можем получить ряд Тейлора как для его центра, так и для всякой его внутренней точки. Пусть одна из таких точек будет $z = a_2$. Для неё ряд Тейлора будет сходиться внутри некоторой окружности $C_2$ с центром в точке $a_2$. В силу свойства круга сходимости, упомянутого в V, круг $C_2$ во всяком случае содержит внутри себя наибольший круг, содержащийся в $C_1$, но может в некоторых случаях выйти за пределы $C_1$. Поступая с кругом $C_2$ так, как мы поступили с $C_1$, и продолжая процесс, мы расширим область определения функции $f(z)$ до пределов возможного. При этом у нас могут возникнуть следующие затруднения:

1) Может оказаться, что за пределы какой-нибудь области продолжить функцию невозможно. В этом случае границу области называют *естественной границей* функции $f(z)$. Построить пример функции с естественной границей нетрудно; так, для функции

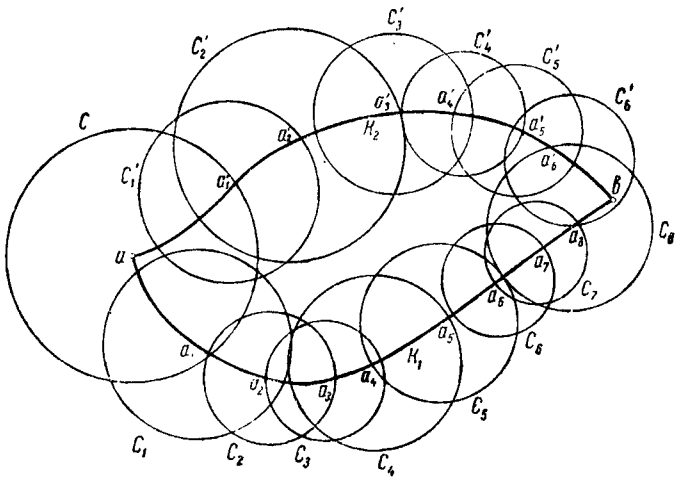
$$1 + z + z^{2^2} + z^{3^2} + z^{4^2} + \ldots + z^{n^2} + \ldots,$$

единичный круг

$$|z| = 1$$

является естественной границей. Однако для изучаемых нами алгебраических функций естественных границ не существует.

2) Может оказаться, что аналитическое продолжение функции приводит к различным значениям для одного и того же значения независимой переменной. Выразимся точнее: пусть нам задано разложение функции $f(z)$ в степенной ряд вблизи точки $z = a$, т. е. в ряд




Черт. 5.

по степеням $z - a$, сходящийся внутри круга $C$ с центром в точке $a$ (черт. 5). Требуется найти значение функции $f(z)$ в точке $z = b$, лежащей вне круга $C$. Для этого соединим точки $a$ и $b$ какой-нибудь спрямляемой кривой $K_1$, причём пусть $K_1$ пересекается с $C$ в регулярной точке функции $f(z)$. Построим разложение $f(z)$ в ряд по степеням $z - a_1$, где $a_1$ — какая-нибудь точка, лежащая на $K_1$, но внутри $C$. Пусть этот ряд сходится внутри круга $C_1$, выходящего за пределы круга $C$. Возьмём вдоль кривой $K_1$ точку $a_2$, лежащую внутри круга $C_1$, построим для неё круг сходимости $C_2$ ряда Тейлора и будем продолжать процесс. Если при этом кривая $K_1$ не проходит через особые точки функции $f(z)$, то каждый из получающихся кругов $C_i$ имеет радиус, не меньший, чем ближайшее расстояние $\delta$ особых точек функции $f(z)$ до точек кривой $K_1$. С другой стороны, если мы, например, условимся брать точку $a_{i+1}$ на расстоянии половины радиуса круга $C_i$ от точки $a_i$, то, полагая отрезок дуги $K_1$ между $a$ и $b$ равным $s$, мы после числа шагов процесса, не превышающего

$$\frac{2s}{\delta},$$

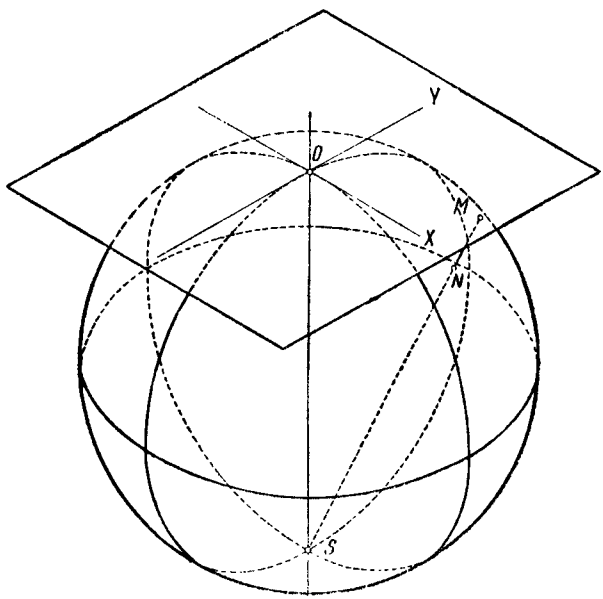
дойдём до точки $b$ и найдём в ней значение функции $f(z)$.

Пусть мы определили $f(b)$, совершая процесс аналитического продолжения с одной стороны вдоль $K_1$, а с другой стороны вдоль другой спрямляемой кривой $K_2$, соединяющей точки $a$ и $b$. В общем случае оба значения $f(b)$ не будут совпадать, и теория алгебраических функций будет давать примеры таких случаев. Однако если кривые $K_1$ и $K_2$ ограничивают некоторую область $K$, то, пользуясь теоремой единственности (см. XI), можно доказать:

Если при аналитическом продолжении функции $f(z)$ вдоль кривых $K_1$ и $K_2$ мы придём к её различным значениям в точке $z=b$, то внутри области $K$ непременно существуют критические точки, в любой окрестности которых функция $f(z)$ не однозначна.

В § 38 мы увидим, что критические точки алгебраических функций всегда являются алгебраическими.

XIII. *Сфера Неймана* (C. Neumann). Изображение значений комплексной переменной на плоскости имеет то неудобство, что значе-




Черт. 6.

нию $z=\infty$, которое в теории алгебраических функций принципиально не отличается от конечных значений $z$, на плоскости не соответствует никакой точки. Ввиду этого Нейман предложил особым образом проектировать точки плоскости на сферу. Для этого он строит сферу произвольного радиуса, касательную к плоскости комплексной переменной $z$ в точке $O$ (0,0) (черт. 6). Затем он обозначает через

$S$ (южный полюс) точку сферы, лежащую на том же диаметре, что и точка $O$. Чтобы построить проекцию произвольной точки $M$ плоскости на сферу, соединим $M$ с $S$ и будем считать искомой проекцией пересечение $N$ прямой $MS$ со сферой. Точка $N$ определяется единственным образом, так как другая точка пересечения прямой и сферы есть $S$.

Обратно, чтобы найти точку плоскости, соотвествующую произвольной точке $N$ сферы (отличной от точки $S$ продолжим хорду $NS$ до её пересечения $M$ с плоскостью и будем считать, что, точке $N$ сферы соответствует точка $M$ плоскости.

Если $M$ неограниченно удаляется от $O$, то соответствующая ей точка $N$ неограниченно приближается к $S$. Советую читателю в виде упражнения установить зависимость между расстояниями $OM$ и $SN$.

Таким образом внешней части круга весьма большого радиуса проведённого на плоскости с центром в точке $O$, соответствует на сфере внутренняя часть круга весьма малого радиуса, содержащего внутри себя точку $S$, т. е. окрестность точки $S$. Это позволяет нам считать точку $S$ соответствующей значению $z = \infty$.

Отметим разницу в толковании бесконечно удаленных точек в теории аналитических функций и в аналитической (собственно говоря, проективной) геометрии, где каждому направлению в плоскости приводится в соответствие своя бесконечно удалённая точка, так что все бесконечные точки образуют бесконечную прямую, которая как бы опоясывает плоскость.

## § 38. Диаграмма Ньютона

В предыдущем параграфе мы видели, что алгебраическая функция $w$, определённая уравнением

1) $$f(z, w) = 0,$$

разлагается в сходящийся ряд по целым степеням $z - z_0$, если $z_0$ не есть корень дискриминанта $D(z)$ уравнения (1). Рассмотрим наиболее общий случай, т. е. не будем делать никаких предположений относительно $z_0$. Предположим только, что левая часть уравнения (1) при переменных $z$, $w$ не разлагается на кратные множители, т. е. что дискриминант $D(z)$ не равен тождественно нулю.

Не нарушая общности, можно предположить, что $z_0 = 0$; иначе в роли $z$ мы могли бы взять разность $z - z_0$.

Обобщая дальнейшее исследование, предположим, что коэффициенты $a_k(z)$ являются степеиными рядами от $z^{\frac{1}{q}}$, где $q$ — любое натуральное число.

Пусть

(2) $$f(z, w) = a_0(z) + a_1(z)\, w + \ldots + a_{n-1}(z)\, w^{n-1} + a_n(z)\, w^n,$$

где

$$(3)\quad a_k(z)=c_{k0}z^{\rho_k}+c_{k1}z^{\rho_k+\frac{1}{q}}+\dots \qquad (c_{k0}\neq 0;\ k=0,\ 1,\dots,n).$$

Станем искать функцию $w$ в форме ряда

$$(4)\quad w=\alpha z^{\varepsilon}+\alpha' z^{\varepsilon'}+\dots \qquad (\varepsilon<\varepsilon'<\varepsilon''<\dots,\ \alpha\neq 0),$$

где будем считать показатели $\varepsilon,\ \varepsilon',\ \varepsilon'',\dots$, вообще говоря, дробными числами. Чтобы найти возможные значения для $\varepsilon$ и $\alpha$, учтём, что, подставляя (4) в (2), мы должны получить тождественный нуль. В частности, должен обратиться в нуль коэффициент при низшей степени $z$. Пока $\varepsilon$ остаётся неопределённым, мы не можем точно сказать, какие из получаемых членов будут низшими; единственное, что мы знаем, это то, что низшие члены содержатся среди следующих:

$$(5)\quad c_{00}z^{\rho_0};\ c_{10}\alpha z^{\rho_1+\varepsilon};\ c_{20}\alpha^2 z^{\rho_2+2\varepsilon};\ \dots;\ c_{n0}\alpha^n z^{\rho_n+n\varepsilon}.$$

Ни один из коэффициентов в этих членах не равен нулю; поэтому, чтобы низшие члены в $f(z,\ \alpha z^{\varepsilon}+\dots)$ обратились в нуль, необходимо подобрать $\varepsilon$ так, чтобы по крайней мере два из показателей

$$(6)\quad \rho_0,\ \rho_1+\varepsilon,\ \rho_2+2\varepsilon,\ \dots,\ \rho_n+n\varepsilon$$

были равны друг другу, а остальные были больше; после этого нетрудно подобрать $\alpha$ так, чтобы сумма коэффициентов членов (5), имеющих равные показатели, была равна нулю. Вопрос решается конечным числом действий: $\varepsilon$ должен быть корнем одного из линейных уравнений

$$(7)\quad \rho_i+i\varepsilon=\rho_j+j\varepsilon \qquad (i\neq j;\ i,j=0,\ 1,\dots,\ n-1),$$

причём из этих корней только те дают решение задачи, подстановка которых в остальные выражения (6) даёт не меньшие значения, чем $\rho_i+i\varepsilon$.

Для быстрого и удобного нахождения этих значений $\varepsilon$ существует геометрический приём, ведущий начало от Ньютона и носящий название *диаграммы Ньютона*, или *многоугольника Ньютона*, или *параллелограмма Ньютона*. Он состоит в следующем. Нанесём на координатной сетке точки с координатами

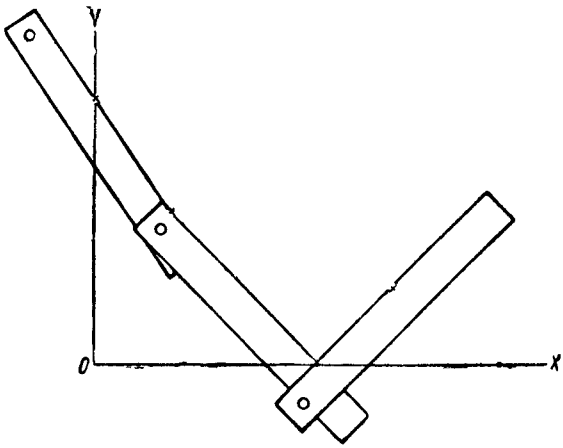
$$(8)\quad (0,\rho_0),\ (1,\rho_1),\ (2,\rho_2),\ \dots,\ (n,\rho_n)$$

и проведём через каждую из этих точек параллельные прямые с угловым коэффициентом $\varepsilon$ (здесь под угловым коэффициентом мы разумеем тангенс угла между данной прямой и *отрицательным* направлением оси $X$). Каждая из этих прямых пересечёт ось $Y$ на высоте

$$\rho_k+k\varepsilon \qquad (k=0,\ 1,\ \dots,\ n).$$

Таким образом требуется, чтобы по крайней мере две нижние из этих прямых совпали, а остальные лежали выше.

Отсюда вытекает такой графический способ нахождения значений $\varepsilon$ (черт. 7). Приставим к точке $(0, \rho_0)$ линейку вертикально вниз и станем вращать её против часовой стрелки до тех пор, пока она впервые попадёт на другую из нанесённых точек, например, на $(k, \rho_k)$. Положение линейки определит одно из искомых значений $\varepsilon$. Затем станем вращать линейку в том же направлении вокруг точки $(k, \rho_k)$ до первого совпадения с дальнейшей точкой, например, с $(l, \rho_l)$. Продолжая процесс, мы получим всевозможные значения $\varepsilon$.



Черт. 7.

Получаемая на чертеже выпуклая ломаная носит название *диаграммы Ньютона*. Каждому из её отрезков соответствует столько различных или совпадающих значений коэффициента $\alpha$, сколько единиц содержит длина её проекции на ось $X$. В самом деле, если крайние точки отрезка суть $(i, \rho_i)$ и $(j, \rho_j)$, то для того, чтобы в выражении $f(z, \alpha z^\varepsilon + \ldots)$ самые низшие члены сокращались, нужно, чтобы имело место

$$c_{i0}\alpha^i + c_{i+1,0}\alpha^{i+1} + \ldots + c_{j,0}\alpha^j = 0,$$

т. е.

$$c_{i0} + c_{i+1,0}\alpha + \ldots + c_{j,0}\alpha^{j-i} = 0.$$

Это уравнение относительно $\alpha$ имеет $j - i$ корней, ч. т. д.

С другой стороны, длина проекции всей ломаной равна $n$. Отсюда следует, что мы получим все $n$ (различных или частично совпадающих) значений начального члена $\alpha z^\varepsilon$ для разложения функции $w$.

Для получения следующего члена разложения надо произвести в уравнении (1) подстановку

$$w = \alpha z^\varepsilon + w_1$$

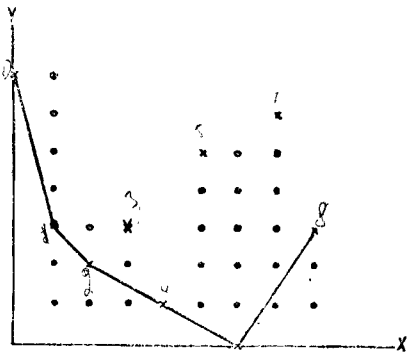
и, пользуясь тем же приёмом, найти низший член разложения для $w_1$, и т. д. Получаемые значения $\varepsilon$, $\varepsilon'$, ..., суть, вообще говоря, дробные числа.

*Пример* (Юнг):

$$(9)\quad 2z^7 - z^8 - z^8w + (4z^2 + z^3)w^2 + (z^3 - z^4)w^8 - 4zw^4 + \\ + 7z^5w^5 + (1 - z^2)w^6 + 5z^6w^7 + z^8w^8 = 0.$$

Для этого уравнения диаграмма Ньютона изображена на черт. 8. Из этого чертежа мы получаем для $\varepsilon$ следующие значения:

$$\varepsilon_1 = 4, \quad \varepsilon_2 = 1,$$
$$\varepsilon_3 = \frac{1}{2}, \quad \varepsilon_4 = -\frac{3}{2}.$$



Черт. 8.

Для определения коэффициента $\alpha$ получаем следующие уравнения:

A) $\varepsilon_1 = 4, \quad 2 - \alpha = 0,$

B) $\varepsilon_2 = 1, \quad -1 + 4\alpha = 0,$

C) $\varepsilon_3 = \frac{1}{2}, \quad 4 - 4\alpha^2 + \alpha^4 = 0,$

D) $\varepsilon_4 = -\frac{3}{2}, \quad 1 + \alpha^2 = 0.$

Таким образом мы получим для $w$ следующие 8 разложений:

$$2z^4 + \ldots, \ \frac{1}{4}z + \ldots, \ \sqrt{2}\cdot z^{\frac{1}{2}} + \ldots, \ \sqrt{2}\cdot z^{\frac{1}{2}} + \ldots,$$
$$-\sqrt{2}\cdot z^{\frac{1}{2}} + \ldots, \ -\sqrt{2}\cdot z^{\frac{1}{2}} + \ldots,$$
$$-iz^{-\frac{3}{2}} + \ldots, \ -iz^{-\frac{3}{2}} + \ldots$$

Начальные члены для 3-го и 4-го, а также для 5-го и 6-го разложений совпадают. Найдём для них вторые члены. Для этого мы должны положить

$$w = \pm\sqrt{2}\cdot z^{\frac{1}{2}} + w_1.$$

Подставляя в (9), получим уравнение для $w_1$, которое даёт для $\varepsilon_1$ значение $\frac{3}{4}$, а для $\alpha_1$ значения $\pm\frac{\sqrt[4]{2}}{4}, \pm i\frac{\sqrt[4]{2}}{4}$, так что 3-е, 4-е, 5-е и 6-е разложения функции $w$ будут таковы:

$$w_{3,4} = \sqrt{2}\cdot z^{\frac{1}{2}} \pm \frac{\sqrt[4]{2}}{2} z^{\frac{3}{4}} + \ldots,$$
$$w_{5,6} = -\sqrt{2}\cdot z^{\frac{1}{2}} \pm \frac{i\sqrt[4]{2}}{4} z^{\frac{3}{4}} + \ldots$$

Таким образом мы получили 8 различных разложений функции $w$. Чтобы быть уверенным, что такое разложение всегда приводит к сходящемуся ряду, необходимо доказать несколько теорем.

Теорема 63. *Получаемое методом диаграммы Ньютона разложение*

$$w = \alpha z^{\varepsilon} + \alpha' z^{\varepsilon'} + \alpha'' z^{\varepsilon''} + \dots \tag{9'}$$

*расположено по возрастающим степеням* $z$:

$$\varepsilon < \varepsilon' < \varepsilon'' < \dots$$

Доказательство. Ограничимся выводом неравенства $\varepsilon < \varepsilon'$, так как дальнейшие показатели получаются тем же путём. Кроме того, ниже мы убедимся, что достаточно ограничиться изучением только одного разложения. Выберем в качестве изучаемого разложения то, в котором показатель $\varepsilon$ наибольший. В этом случае соответствующий ему отрезок ломаной — ближайший к оси $Y$. Из черт. 7 нетрудно видеть, что

$$\varepsilon = \operatorname{Max}\left(\frac{\rho_0 - \rho_1}{1}, \frac{\rho_0 - \rho_2}{2}, \dots, \frac{\rho_0 - \rho_n}{n}\right). \tag{10}$$

Отметим важный для дальнейшего побочный факт: если максимум правой части (10) достигается на $k$-м члене, т. е. если $\varepsilon = \frac{\rho_0 - \rho_k}{k}$, то $\varepsilon$ есть дробь, знаменатель которой равен или $k$, или делителю $k$.

Будем временно считать коэффициент $\alpha$ переменным. Напишем $f(z, \alpha z^{\varepsilon})$ в таком виде:

$$f(z, \alpha z^{\varepsilon}) = \varphi(\alpha) \cdot z^{s} + \varphi_1(\alpha) \cdot z^{s_1} + \dots, \tag{11}$$

где $s < s_1 < \dots$ Мы уже знаем, что в качестве $\alpha$ мы должны брать один из корней полинома $\varphi(\alpha)$. Пусть это будет $\alpha = \alpha_0$; предположим для общности, что $\alpha_0$ есть $k$-кратный корень полинома $\varphi(\alpha)$.

Чтобы получить уравнение для $w_1$, где

$$w = \alpha_0 z^{\varepsilon} + w_1,$$

напишем

$$f(z, \alpha z^{\varepsilon} + w_1) = \tag{12}$$
$$= A_0(z) + A_1(z) w_1 + \dots + A_{n-1}(z) w_1^{n-1} + A_n(z) \cdot w_1^n,$$

где

$$A_k(z) = \frac{1}{k!}\left(\frac{\partial^k f(z, \alpha z^{\varepsilon})}{\partial w^k}\right)_{\alpha = \alpha_0} \qquad (k = 0, 1, \dots, n),$$

или также

$$A_k(z) = \frac{1}{k!}\left(\frac{\partial^k f(z, \alpha z^{\varepsilon})}{\partial \alpha^k}\right)_{\alpha = \alpha_0} \cdot z^{-k\varepsilon} \qquad (k = 0, 1, \dots, n). \tag{13}$$

Обозначим через $R_0, R_1, \ldots, R_n$ порядки, с которыми обращаются в нуль при $z=0$ функции

$$A_0(z),\ A_1(z),\ \ldots,\ A_n(z).$$

Из (11), (13) и $\varphi(\alpha_0)=0$ следует, что

$$R_0 \geqslant s_1 > s.$$

Дифференцируя (11) по $\alpha$ $k$ раз, получим

$$\frac{\partial^k f(z, \alpha z^\varepsilon)}{\partial \alpha^k} = \varphi^{(k)}(\alpha)\cdot z^s + \varphi_1^{(k)}(\alpha)\cdot z^{s_1} + \ldots,$$

откуда в силу (13) и $\varphi^{(k)}(\alpha_0)\neq 0$ следует, что $A_k(z)$ при $z=0$ обращается в нуль точно $(s-k\varepsilon)$-й кратности, так что в силу определения $R_k$

$$R_k = s - k\varepsilon, \tag{14}$$

откуда

$$\frac{R_0-R_k}{k} \geqslant \frac{s_1-s+k\varepsilon}{k} = \varepsilon + \frac{s_1-s}{k} > \varepsilon.$$

Но $A_k(z)$ суть коэффициенты уравнения (12), которому удовлетворяет $w_1$, в силу чего

$$\varepsilon' = \operatorname{Max}\left(\frac{R_0-R_1}{1}, \frac{R_0-R_2}{2}, \ldots, \frac{R_0-R_n}{n}\right) \geqslant \frac{R_0-R_k}{k} > \varepsilon,$$

ч. т. д.

Отметим следующий факт, вытекающий из хода настоящего доказательства: степень уравнения, из которого определяется коэффициент $\alpha'$ при члене $\alpha' z^{\varepsilon'}$, не превышает порядка кратности корня $\alpha_0$ полинома $\varphi(\alpha)$. В самом деле, степень этого уравнения равна наибольшему индексу $u$, при котором

$$\frac{R_0-R_u}{u} = \varepsilon'.$$

Но при любом $u > k$ имеем:

$$\frac{R_0-R_u}{u} \leqslant \frac{R_0-s+u\varepsilon}{u} = \frac{R_0-s}{u} + \varepsilon < \frac{R_0-s}{k} + \varepsilon = \frac{R_0-(s-k\varepsilon)}{k} = \frac{R_0-R_k}{k} \leqslant \varepsilon'. \tag{15}$$

Здесь мы воспользовались неравенством

$$R_u \geqslant s - u\varepsilon.$$

Оно выводится так же, как равенство (14). Однако здесь не исключена возможность $\varphi^{(u)}(\alpha_0)=0$.

Из (15) следует

$$u \leqslant k.$$

Отсюда следует:

Знаменатель дроби $\varepsilon'$ может быть больше знаменателя дроби $\varepsilon$ в число раз, не превышающее кратности корня $\alpha_0$ полинома $\varphi(\alpha)$.

Если теперь мы составим полиномы

$$\varphi(\alpha),\ \varphi_1(\alpha),\ \varphi_2(\alpha),\ \ldots,$$

корнями которых являются коэффициенты

$$\alpha_0,\ \alpha_0',\ \alpha_0'',\ \ldots$$

разложения (9), то степень каждого последующего полинома не превышает порядка кратности одного корня в предыдущем полиноме. Отсюда следует, что степени этих полиномов всё время убывают, за исключением единственной возможности, когда, начиная с какого-нибудь места, каждый полином есть какая-нибудь (одна и та же) степень линейной функции:

$$\varphi_\mu(\alpha) = (\alpha - \alpha_0^{(\mu)})^\nu,\quad \varphi_{\mu+1}(\alpha) = (\alpha - \alpha_0^{(\mu+1)})^\nu,\ \ldots$$

Если при этом $\nu > 1$, то мы будем получать $\nu$ одинаковых разложений, сколь далеко они ни были бы продолжены. При этом даже в случае $\nu > 1$ мы в показателях $\varepsilon^{(\mu)}$, $\varepsilon^{(\mu+1)}$,... не будем получать растущих знаменателей. В самом деле,

$$\varphi_\mu(\alpha) = (\alpha - \alpha_0^{(\mu)})^\nu = \alpha^\nu - \binom{\nu}{1}\alpha^{\nu-1}\alpha_0^{(\mu)} + \ldots + (\alpha_0^{(\mu)})^\nu.$$

Здесь ни один член не равен нулю. Это значит, что на отрезке ломаной, который соответствует показателю $\varepsilon^{(\mu)}$, нанесённые точки $(i, \rho_i^{(\mu)})$ лежат на расстояниях, проекции которых на ось $X$ равны единице. Так как, с другой стороны, разность ординат соседних точек является числом, кратным $\varepsilon^{(\mu-1)}$, то и угловой коэффициент отрезка есть число, кратное $\varepsilon^{(\mu-1)}$. Таким образом

Теорема 64. *В разложении*

$$w = az^\varepsilon + a'z^{\varepsilon'} + a''z^{\varepsilon''} + \ldots$$

*показатели* $\varepsilon$, $\varepsilon'$, $\varepsilon''$, ... *являются дробями, у которых общий знаменатель есть конечное число.*

Пусть этот общий знаменатель есть $a_1$ и пусть

$$\varepsilon = \frac{b}{a_1},\quad \varepsilon' = \frac{b'}{a_1},\quad \varepsilon'' = \frac{b''}{a_1},\quad \ldots$$

Вводя обозначение

$$z = \xi^{a_1},$$

мы получим для $w$ ряд, расположенный по целым степеням $\xi$:

$$w = a\xi^b + a'\xi^{b'} + a''\xi^{b''} + \ldots$$

Введём символ сравнения

$$u(\xi) \equiv v(\xi) \pmod{\xi^M},$$

обозначающий, что частное $\frac{u(\xi)-v(\xi)}{\xi^M}$ содержит лишь неотрицательные степени $\xi$. Тогда, обозначая через $w_1$ отрезок ряда для $w$:

$$w_1 = \alpha \cdot \xi^b + \alpha' \xi^{b'} + \ldots + \alpha^{(\mu)} \xi^{b^{(\mu)}},$$

где $\mu$ — достаточно большое число, мы в силу способа получения членов разложения функции $w$ будем иметь

$$f(\xi^{a_1}, w_1) \equiv 0 \pmod{\xi^{\mu}},$$

откуда, пользуясь теоремой Безу для сравнений, получим для произвольного $\eta$

$$f(\xi^{a_1}, \eta) \equiv (\eta - w_1) f_1(\xi, \eta) \pmod{\xi^M},$$

где $M$ безгранично растёт с ростом $\mu$, а $f_1(\xi, \eta)$ — новый полином. Построив диаграмму Ньютона для полинома $f_1(\xi, \eta)$, мы получим описанным способом разложение $w_2$ для его корня.

Для $w_2$ также имеют место теоремы 63 и 64. Продолжая разложение, мы в конце концов получим

$$(16) \quad f(t^a, \eta) \equiv a_n(t^a)(\eta - w_1)(\eta - w_2) \ldots (\eta - w_n) \pmod{t^N},$$

где $a$ — некоторое новое целое число,

$$z = t^a,$$

$w_1, w_2, \ldots, w_n$ — конечные ряды, расположенные по отрицательным и положительным степеням $t$, которые мы можем по произволу сделать сколь угодно высокой степени, и при этом $N$ тоже будет безгранично расти. Из (16) следует, что не существует рядов, отличных от $w_1, w_2, \ldots, w_n$, которые бы удовлетворяли соотношению (1).

Остаётся доказать сходимость бесконечных рядов, получаемых при безграничном возрастании $N$. Для этого обратим внимание на то, что $w$ является функцией от $t$, аналитической (регулярной) в каждой точке, достаточно близкой к точке $t = 0$, так как производная $\frac{\partial f(t^a, w)}{\partial w}$ в достаточно малой окрестности точки $t = 0$, но не в ней, не обращается в нуль. Далее, поскольку при обходе вокруг точки $t = 0$ функция $w$ не меняет своего значения (об этом см. ниже), то её можно разложить в ряд Лорана по степеням $t$, причём в точке $t = 0$ она может иметь только полюс (так как существует такое $k$, что произведение $t^k \cdot w$ остаётся конечным при $t = 0$).

Ряд Лорана сходится; с другой стороны, он совпадает с построенным нами рядом, так как аналитическая функция всегда разлагается в степенной ряд единственным образом. Переходя опять к переменной $z = t^a$, имеем:

**Теорема 65.** *Получаемые методом диаграммы Ньютона ряды по дробным степеням $z$ сходятся в достаточно малой окрестности точки $z = 0$.*

При доказательстве этой теоремы у нас осталось ещё неисследованным поведение функции $w$ при обходе вокруг точки $z = 0$. Положим

$$z = \rho e^{i\theta},$$

где $\rho > 0$ и достаточно мало, и заставим $\theta$ пробежать все значения от 0 до $2\pi$. При этом в качестве начального значения $w$ возьмём один из корней, $w_1$, уравнения

$$f(\rho, w) = 0. \tag{17}$$

Тогда в силу непрерывности всё время будет соблюдаться (1), так что при $\theta = 2\pi$ мы придём к значению $w_2$, тоже удовлетворяющему уравнению (17). Но так как это уравнение имеет всего $n$ корней, то после некоторого конечного числа $a_1$ таких обходов мы придём к прежнему значению $w_1$. Если теперь мы положим $z = \xi^{a_1}$, то $a_1$ обходам переменной $z$ вокруг точки $z = 0$ будет соответствовать один обход переменной $\xi$ вокруг точки $\xi = 0$, откуда следует однозначность функции $w(\xi)$ при обходе вокруг точки $\xi = 0$, ч. т. д.

Если $a_1 < n$, то, начиная обход со значения $w$, отличного от значений

$$w_1, w_2, \ldots, w_{a_1},$$

мы опять после конечного числа обходов вокруг точки $z = 0$ придём к прежнему значению $w$. Таким образом мы разобьём все значения

$$w_1, w_2, \ldots, w_n$$

на несколько систем, называемых *циклами*. Число $a_1$ мы будем называть порядком соответствующего (в данном случае первого) цикла. Мы видим, что при обходе вокруг критической точки значения $w$ претерпевают подстановку, состоящую из циклов порядков $a_1, a_2, \ldots$ Нетрудно видеть, что число $a_1$ есть общий знаменатель показателей одного из разложений функции $w(z)$ по дробным степеням $z$. В самом деле, пусть

$$w_1 = \alpha \cdot z^{\frac{b}{a_1}} + \alpha' \cdot z^{\frac{b'}{a_1}} + \alpha'' \cdot z^{\frac{b''}{a_1}} + \ldots \tag{18}$$

Тогда после $k$ ($k=0, 1, \ldots, a_1-1$) обходов вокруг точки $z=0$ мы будем приходить к значениям $w(z)$, получаемым из разложений

$$w_{k+1}=\alpha\omega^{bk}z^{\frac{b}{a_1}}+\alpha'\omega^{b'k}z^{\frac{b'}{a_1}}+\alpha''\omega^{b''k}z^{\frac{b''}{a_1}}+\ldots \tag{19}$$

$$(k=0, 1, \ldots, a_1-1),$$

где

$$\omega=e^{\frac{2\pi i}{a_1}}.$$

Все эти разложения различны, если $a_1$ есть общий знаменатель показателей

$$\varepsilon=\frac{b}{a_1},\quad \varepsilon'=\frac{b'}{a_1},\quad \varepsilon''=\frac{b''}{a_1},\ldots,$$

т. е. если числители $b$, $b'$, $b''$, ... не имеют общего множителя. После $(k+1)$-го обхода мы вернёмся к исходному разложению. Таким образом:

Теорема 66. *Если показатели в разложении n-значной алгебраической функции $w(z)$ в окрестности критической точки имеют знаменатели $a_1, a_2, \ldots$ ($a_1+a_2+\ldots=n$), то при обходе вокруг этой критической точки значения $w(z)$ претерпевают подстановку, состоящую из циклов порядков $a_1, a_2, \ldots$*

Ниже мы увидим, что определяемые таким образом подстановки составляют *группу монодромии* алгебраической функции, обладающей многими свойствами, присущими *группе Галуа*.

## § 39. Эффективное нахождение фундаментального базиса

Разложения, полученные в § 38, дают возможность весьма легко находить элементы фундаментального базиса, существование которого мы доказали в §§ 11, 12. В основу излагаемого способа будет поставлена

Теорема 67. *Чтобы алгебраическая функция $w(z)$ была целой, необходимо и достаточно, чтобы все её разложения в окрестностях всех точек $z=a$ не содержали отрицательных степеней $z-a$.*

Доказательство. Если в окрестности точки $z=a$ хотя бы одно из разложений функции $w(z)$ содержит отрицательные степени $z-a$, то это значит, что один из корней уравнения

$$f(z, w)=0 \tag{1}$$

при $z=a$ обращается в бесконечность. Если мы представим $z$ и $w$ через простые дивизоры, то в этом случае простой дивизор, стоящий в числителе представления $z-a$ и потому не стоящий в его знаменателе, будет содержаться в знаменателе представления $w$. $w$ не может быть целой функцией.

Если же $w$ разлагается вблизи всех точек, в которых $z$ конечно, по положительным степеням $z-a$, то это значит, что при всех конечных значениях $z$ функция $w(z)$ остаётся конечной. Отсюда следует, что знаменатель представления $w$ содержит только те простые дивизоры, которые входят в знаменатель представления $z$. Значит, $w$ есть целая функция от $z$.

Пусть $w$ есть целая функция от $z$, образующая вместе с $z$ примитивную пару поля $k(z, w)$. Пусть $D(z)$ есть дискриминант базиса

$$[1, w, w^2, \ldots, w^{n-1}].$$

Мы видели, что элементы фундаментального базиса имеют вид

$$\frac{c_{k_0}(z)+c_{k_1}(z)\cdot w+\ldots+w^k}{d_k(z)} \qquad (k=0, 1, \ldots, n-1), \tag{2}$$

где $d_k(z)$ являются делителями полинома $D(z)$.

Пусть

$$z-a_1,\ z-a_2,\ \ldots,\ z-a_s$$

— совокупность линейных делителей полинома $D(z)$. Станем искать целые функции в форме

$$\frac{c_{k0}(z)+c_{k1}(z)\,w+\ldots+w^k}{(z-a_\nu)^{\mu}} \qquad (k=0, 1, \ldots, n-1), \tag{3}$$

где $\mu$ — возможно более высокий показатель. Для этого найдём разложения функций $1, w, w^2, \ldots, w^{n-1}$ по степеням $z-a_\nu$ и станем искать такие линейные комбинации этих функций, все разложения которых начинались бы с возможно более высоких степеней $z-a_\nu$.

Этого мы будем достигать при помощи следующего алгоритма. Пусть все разложения функции $w$, а с ней и $w^2, \ldots, w^{n-1}$ распадаются на $k$ циклов и каждому циклу пусть соответствуют общие знаменатели показателей

$$b_1, b_2, \ldots, b_k,$$

так что

$$b_1+b_2+\ldots+b_k=n.$$

Каждому элементу базиса мы будем сопоставлять $k$ чисел $\mu_1, \mu_2, \ldots, \mu_k$, $\mu_i$ есть наиболее низкий из показателей при $z-a_\nu$ в его разложениях $i$-го цикла. Таким образом $\mu_i$ есть дробь со знаменателем $b_i$ (может быть, сократимая).

В силу целости всех элементов базиса все числа $\mu_i$ не отрицательны. Если для какого-нибудь элемента все $\mu_i \geqslant 1$, то, деля его на $z-a_\nu$, мы получим целый элемент, у которого все $\mu_i$ будут на единицу ниже. Таким образом мы можем привести базис к такому виду, что среди показателей $\mu_i$ каждого его элемента хотя бы один был меньше единицы. Если не для каждого цикла в базисе имеется элемент

с числом $\mu < 1$, то для какого-нибудь ($i$-го) цикла таких элементов будет больше чем $b_i$. Но так как значения $\mu_i < 1$ могут быть только

$$0, \frac{1}{b_i}, \frac{2}{b_i}, \ldots, \frac{b_i - 1}{b_i}, \tag{4}$$

то в базисе будет два элемента с одним и тем же $\mu_i$. Мы заменим один из них их линейной комбинацией так, чтобы в ней член $(z - a_\nu)^{\mu_i}$ исчез, и тогда для неё значение $\mu_i$ повысится. После этого мы начнём пересмотр значений $\mu_i$ сначала, причём опять, если в каком-нибудь из полученных элементов все $\mu_i \geqslant 1$, мы разделим его на $z - a_\nu$. Этот процесс должен закончиться, так как, с одной стороны, значения $\mu_i$ не могут безгранично расти, а с другой стороны, каждое деление на $z - a_\nu$ понижает степень дискриминанта базиса.

Таким образом после конечного числа шагов мы придём к базису, в котором для какого-то ($i$-го) цикла имеется $b_i$ элементов с числами $\mu_i$, совпадающими с системой (4). Пусть $i = 1$ и пусть

$$w_1, w_2, \ldots, wb_1$$

будут элементы базиса, для которых значения $\mu_1$ равны числам (4). Прибавляя к остальным элементам базиса комбинации элементов $w_1, w_2, \ldots, w_{b_1}$, умноженные на соответственные степени $z - a_\nu$, мы можем добиться того, чтобы значения $\mu_1$ для остальных элементов базиса были сколь угодно велики.

Далее рассмотрим все элементы базиса, кроме $w_1, w_2, \ldots, w_{b_1}$ и в них обратим внимание на все циклы, кроме первого. Продолжая процесс, мы разделим все элементы базиса на $k$ категорий с числом элемеитов $b_1, b_2, \ldots, b_k$ в каждой так, что для элементов $i$-й категории значения $\mu_i$ будут равны числам (4). Значения же для элементов категорий, отличных от $i$-й, можно сделать $\geqslant 1$ и, более того, сколь угодно большими.

Полученный таким образом базис является фундаментальным для кольца $\Omega_{z=a_\nu}$. В самом деле, допустим противное: пусть целый элемент $u$ поля $k(z, w)$ представляется через наш базис $w_1, w_2, \ldots, w_n$ с коэффициентами, содержащими в знаменателях $z - a_\nu$. Пусть

$$u = c_1(z)\, w_1 + c_2(z)\, w_2 + \ldots + c_n(z)\, w_n, \tag{5}$$

где пусть $c_i(z)$ есть рациональная функция, содержащая в знаменателе $z - a_\nu$ и потому при разложении по степеням $x - a_\nu$ имеющая члены с отрицательными степенями. Пусть $w_i$ соответствует $i$-му циклу и пусть его $i$-е разложение начинается с члена $(z - a_\nu)^{\frac{j}{b_i}}$ $(0 \leqslant j < b_i)$. Тогда $i$-е разложение произведения

$$c_i(z)\, w_i$$

начинается с отрицательных степеней $z - a_\nu$. Другие же члены выражения (5) имеют $i$-е разложения, в которых не может быть членов,

подобных с этими членами; те, которые не соответствуют $i$-му циклу, имеют $i$-е разложения с положительными степенями $z-a_\nu$; соответствующие же $i$-му циклу имеют разложения, содержащие отрицательные степени, у показателей которых дробные части отличны от $\frac{j}{b_i}$. Таким образом $i$-е разложение левой части формулы (5) содержит лишь положительные степени $z-a_\nu$, а правой части — непременно отрицательные степени $z-a_\nu$. Противоречие доказывает наше утверждение.

Последовательно преобразуя базис относительно множителей $z-a_1$, $z-a_2$ ..., $z-a_s$, мы получим фундаментальный базис кольца $\Omega$. Это следует из того, что описанный процесс лишит базис всех множителей дискриминанта $D(z)$, которые не входят в дискриминант фундаментального базиса.

*Пример* (Юнг):

$$f(z, w) = w^3 - 3zw + 2z^2 = 0.$$

Дискриминант этого уравнения, кубического относительно $w$, может быть получен из известной формулы

$$D(z) = z^4 - z^3 = z^3(z-1).$$

Множитель $z-1$ входит в первой степени и потому не может пропасть при переходе к фундаментальному базису. Остаётся исследовать только множитель $z$.

Разложения по степеням $z$ образуют два цикла:

$$\text{I цикл}\begin{cases} w = \pm\sqrt{3}\cdot z^{\frac{1}{2}} - \frac{z}{3} \mp \frac{z^{\frac{3}{2}}}{6\sqrt{3}} + \dots, \\ w^2 = 3z \mp \frac{2}{\sqrt{3}} z^{3/2} - \frac{2}{9} z^2 + \dots, \end{cases}$$

$$\text{II цикл}\begin{cases} w = \frac{2}{3} z + \frac{8}{11} z^2 + \frac{32}{729} z^3 + \dots, \\ w^2 = \frac{4}{9} z^2 + \frac{32}{243} z^3 + \frac{448}{6561} z^4 + \dots \end{cases}$$

Отсюда сразу видно, что $\frac{w^2}{z}$ есть целая функция:

$$\text{I цикл}\ \left\{ \frac{w^2}{z} = 3 \mp \frac{2}{3} z^{\frac{1}{2}} - \frac{2}{9} z + \dots, \right.$$

$$\text{II цикл}\ \left\{ \frac{w^2}{z} = \frac{4}{9} z + \frac{32}{243} z^2 + \frac{448}{6561} z^3 + \dots \right.$$

Базис $\left[1, w, \frac{w^2}{z}\right]$ является фундаментальным, так как его дискриминант равен $z(z-1)$, и его степень не может быть уменьшена, по-

сколько он лишён квадратных множителей. Числа $\mu_i$ для его элементов таковы:

$$(0, 0), \quad \left(\frac{1}{2}, 1\right), \quad (0, 1).$$

Отсюда следует, что его элемент 1 принадлежит II циклу, а остальные первому. Мы можем повысить $\mu_i$ для чужих циклов, что для некоторых целей бывает полезно. Так, элемент

$$1 - \frac{1}{3}\frac{w^2}{z} - \frac{2}{3}w$$

имеет $\mu_1 = 1$, $\mu_2 = 0$; его следует взять в базисе вместо 1.

Для многих целей теории алгебраических функций, в частности для нахождения интегралов 1-го рода, важно уметь найти нормальный базис, а также дополнительный к нему базис. Эта задача значительно облегчается, если известен какой-нибудь фундаментальный базис, так как известна форма, в которой следует искать элементы кольца $\Omega$. В этом случае прежде всего нужно разложить все элементы базиса в окрестности $z = \infty$. Для этого можно совершить преобразование $z = \frac{1}{z_1}$; но проще воспользоваться теми же точками, которые были нанесены для построения диаграммы разложения по степеням $z$ или $z - a_\nu$, и построить ломаную, лежащую выше этих точек. Для этого нужно приставить линейку к оси ординат, направленную *вверх*, и вращать её около *высшей* из отмеченных точек *по часовой стрелке*.

Полученные разложения дают возможность найти дробные, а с ними и целые показатели элементов базиса: дробный показатель есть не что иное, как наибольшее из чисел $\mu_i$, соответствующих всем разложениям элемента по *убывающим* степеням $z$.

Чтобы построить нормальный базис, надо взять элемент фундаментального базиса, имеющий наивысший показатель (это будет $r_n$), и вычесть его кратность из остальных элементов базиса с тем, чтобы их порядки максимально снизились; затем среди остальных элементов базиса выбрать элемент наименьшего порядка и проделать с ним то же самое, и т. д.

*Пример.* Вернёмся к предыдущему примеру и найдём разложения $w$ по убывающим степеням $z$. Они образуют один единственный цикл

$$w = -\sqrt[3]{2} \cdot z^{2/3} - \frac{1}{\sqrt[3]{2}} z^{1/3} + \dots,$$

$$w^2 = \sqrt[4]{4} \cdot z^{4/3} + 2z + \dots$$

Остальные разложения цикла получаются из этого разложения известным образом [см. формулы (18) и (19) § 38]. Поскольку показатели элементов 1, $w$, $w^2$ все различны

$$r_1 = 0, \quad r_2 = 1, \quad r_3 = 2, \tag{6}$$

эти элементы образуют нормальный базис.

Из (6) легко получить жанр $\rho$ поля $k(z, w)$:

$$\rho = (r_2 - 1) + (r_3 - 1) = 1.$$

Рассмотрим задачу нахождения интегралов 1-го рода. В § 20 мы видели, что она приводится к нахождению базиса, дополнительного к нормальному. Существует несколько способов решения этой задачи, из которых мы укажем следующие:

1) Пусть

$$[\lambda_1, \lambda_2, \ldots, \lambda_n]$$

есть нормальный базис. Дополнительный базис

$$[\mu_1, \mu_2, \ldots, \mu_n]$$

определяется равенствами

$$S(\lambda_j \mu_j) = \delta_{ij} \qquad (i, j = 1, 2, \ldots, n).$$

Если мы выразим дополнительный базис через нормальный:

$$(7) \qquad \mu_j = e_{1j}\lambda_1 + e_{2j}\lambda_2 + \ldots + e_{nj}\lambda_n \qquad (j = 1, 2, \ldots, n),$$

то рациональные функции $e_{ij}(z)$ определятся из систем линейных уравнений

$$e_{1j}S(\lambda_1\lambda_i) + e_{2j}S(\lambda_2\lambda_i) + \ldots + e_{nj}S(\lambda_n\lambda_i) = \delta_{ij} \qquad (i = 1, 2, \ldots, n),$$

если $j$ придавать значения 1, 2, ..., $n$. Подинтегральные функции интегралов 1-го рода выразятся в форме

$$(8) \qquad h_1(z) \cdot \mu_1 + h_2(z) \cdot \mu_2 + \ldots + h_n(z) \cdot \mu_n,$$

где $h_i(z)$ — полиномы не выше $(r_i - 2)$-й степени.

Неудобство этого способа состоит в его технической громоздкости; в частности, много труда отнимает вычисление следов $S(\lambda_i\lambda_j)$.

2) Базис, дополнительный к фундаментальному, может быть охарактеризован тем, что его элементы обращаются при конечных $z$ в бесконечность ниже 1-го порядка. Пользуясь этим, можно сразу найти элементы дополнительного базиса при помощи того же приёма, которым мы находим фундаментальный базис. Разница будет состоять в том, что здесь показатели $\mu_i$ должны удовлетворять не $\mu_i \geqslant 0$, а неравенствам

$$(9) \qquad \mu_i > -1,$$

в силу чего роль показателей (4) будут играть следующие числа:

$$(10) \qquad -\frac{b_i - 1}{b_i}, \quad -\frac{b_i - 2}{b_i}, \quad \ldots, \quad -\frac{1}{b_i}, \quad 0.$$

После нахождения дополнительного базиса его следует привести к нормальному виду, т. е. расположить его элементы по порядкам обращения в нуль при $z = \infty$, делая при помощи линейных комбинаций эти порядки возможно большими. После этого искомые подинтегральные функции опять выразятся в форме (8).

3) Из формулы (4) § 32

$$f_w(z, w) \equiv \frac{Z_x \cdot D}{X^m \cdot Y^{n-2}}$$

видно, что элементы дополнительного базиса могут быть представлены в форме

$$\frac{\varphi(z, w)}{f_w(z, w)},$$

где $\varphi(z, w)$ — целый элемент, притом делящийся на дивизор $D$ двойных точек. Имеет место замечательный факт:

Теорема 68. *Если в числителе представления целого элемента $\varphi(z, w)$ через дивизоры содержится дивизор $D$, то $\varphi(z, w)$ представляется в виде полинома от $z$, $w$.*

Доказательство. Представим $\varphi(z, w)$ через базис $[1, w, \ldots, w^{m-1}]$:

$$\varphi(z, w) = r_0(z) + r_1(z)\, w + \ldots + r_{n-1}(z)\, w^{n-1}.$$

Требуется доказать, что $r_i(z)$ являются полиномами от $z$. Для этого введём новую независимую переменную $u$ и обозначим через

$$w_1, w_2, \ldots, w_n$$

корни уравнения

$$f(z, w) = 0,$$

считая $z$ произвольным, но фиксированным числом. Вводя обозначение

$$\varphi(z, u) = r_0(z) + r_1(z) \cdot u + \ldots + r_{n-1}(z)\, u^{n-1},$$
$$\varphi(z, w_i) = \varphi_i \qquad (i = 1, 2, \ldots, n)$$

и пользуясь интерполяционной формулой Лагранжа, получим:

$$\varphi(z, u) = \sum_{i=1}^{n} \frac{\varphi(z, w_i)}{f_w(z, w_i)} \cdot \frac{f(z, u)}{u - w_i} = S\left(\frac{\varphi(z, w)}{f_w(z, w)} \cdot \frac{f(z, u)}{u - w}\right).$$

Стоящий под знаком $S(\ldots)$ элемент поля $k(z, w, u)$ состоит из двух множителей, из которых первый, в силу нашего предположения, представляется дивизором, в знаменателе которого содержится $Z_w$, а также знаменателем представлений элементов $z$ и $w$; второй множитель есть целый элемент поля $k(z, w, u)$. Отсюда в силу теоремы 37 следует, что $\varphi(z, u)$ при любом $u$ является полиномом от $z$, ч. т. д.

Пусть

$$z \equiv \frac{X_1}{X}, \quad w \equiv \frac{Y_1}{Y}.$$

Тогда, если $\varphi(z, w)$ — полином степеней $\mu$, $\nu$ относительно $z$, $w$, то

$$\varphi(z, w) \sim \frac{D \cdot H}{X^{\mu} \cdot Y^{\nu}},$$

где $H$ — некоторый целый дизизор. Отсюда

$$(11) \quad \begin{cases} \dfrac{\varphi(z, w)}{f_w(z, w)} \sim \dfrac{X^{m-\mu} \cdot Y^{n-\nu-2}}{Z_z}, \\ \dfrac{\varphi(z, w)dz}{f_w(z, w)} \sim X^{m-\mu-2} \cdot Y^{n-\nu-2}. \end{cases}$$

Таким образом:

Теорема 69. *Чтобы*

$$\frac{\varphi(z, w)\, dz}{f_w(z, w)}$$

*был дифференциалом 1-го рода, достаточно, чтобы $\varphi(z,w)$ был полиномом степени $\leqslant m-2$ относительно $z$ и $\leqslant n-2$ относительно $w$, который как элемент поля $k(z,w)$ делился бы на $D$. Если ни $w$ не цел относительно $z$, ни $z$ относительно $w$, то это условие и необходимо.*

Полиномы $\varphi(z, w)$, удовлетворяющие условиям теоремы 69, носят название *присоединённых* (adjungiert) полиномов и играют большую роль в геометрической теории алгебраических функций. Ими удобно пользоваться в частном случае, когда $f(z, w)$ есть полином $n$-й степени относительно обеих переменных, а все особые точки соответствующей ему кривой являются двойными. Тогда, как можно доказать, присоединённый полином есть наиболее общий полином степени $\leqslant n-3$, обращающийся в нуль во всех особых точках кривой $f(z, w) = 0$.

## Упражнения к главе VI

1. Существует ещё один способ нахождения дополнительных базисов, требующий применения теории симметрических функций. Пусть

$$[\omega_1, \omega_2, \ldots, \omega_n]$$

— фундаментальный базис и пусть

$$\omega_i^{(1)}, \quad \omega_i^{(2)}, \quad \ldots, \quad \omega_i^{(n)} \qquad (i = 1, 2, \ldots, n)$$

— корни уравнения $F_i(x, \omega) = 0$, которому удовлетворяет $\omega_i = \omega_i^{(1)}$. Составим матрицу, обратную к матрице

$$\begin{Vmatrix} \omega_1^{(1)}, & \omega_2^{(1)}, & \ldots, & \omega_n^{(1)} \\ \omega_1^{(2)}, & \omega_2^{(2)}, & \ldots, & \omega_n^{(2)} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \omega_1^{(n)}, & \omega_2^{(n)}, & \ldots, & \omega_n^{(n)} \end{Vmatrix},$$

и транспонируем её. Тогда первая строка полученной матрицы даёт дополнительный базис. Доказать это.

2. Доказать: если разложения элемента $w$ вблизи $z = a$ распадаются на $k$ циклов, состоящих из $b_1, b_2, \ldots, b_k$ разложений, то числитель представления элемента $z - a$ через дивизоры содержит $k$ различных простых дивизоров, входящих в степенях $b_1, b_2, \ldots, b_k$.

3. Пользуясь диаграммой Ньютона, исследовать типы особых точек алгебраических кривых упражнения 12 к главе V.

4. *Теорема Дюма* (Dumas). Зная диаграммы Ньютона для уравнений

$$f(z, w) = 0, \quad g(z, w) = 0,$$

построить диаграмму Ньютона для уравнения

$$f(z, w) \cdot g(z, w) = 0.$$

Для этого нужно считать отрезки обеих ломаных векторами и построить при помощи всех этих векторов выпуклую ломаную, что приводит к одной единственной диаграмме.

5. Доказать: если $f(z)$ и имеет на всей плоскости только полюсы и логарифмические точки, т. е. такие точки $z = a_\nu$, что в их окрестности разность

$$f(z) - A_\nu \cdot \ln(z - a_\nu)$$

регулярна или имеет полюс, то $f(z)$ может быть представлена как неопределённый интеграл от рациональной функции.

ГЛАВА VII

# РИМАНОВА ПОВЕРХНОСТЬ

## § 40. Построение римановой поверхности

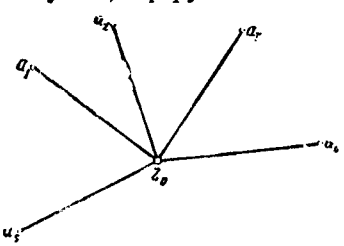
Дано алгебраическое уравнение

$$f(z, w) = 0 \tag{1}$$

степени $n$ относительно $w$. Как мы видели, оно определяет $n$-значную аналитическую функцию $w(z)$. Возьмём значение $z = z_0$ такого рода, чтобы все корни уравнения (1) при $z = z_0$ были различны, и в остальном произвольное. Пусть это будут

$$w_1, w_2, \ldots, w_n. \tag{2}$$

Возьмём один из них, например $w = w_1$. Возьмём плоскость или, что лучше, сферу Неймана комплексной переменной $z$ (см. § 37, XIII) и будем относить к каждой её точке $z$ значение, которое мы найдём путём аналитического продолжения (см. § 37, XII), исходя из значения $w = w_1$ в точке $z = z_0$. Однако такое определение в общем случае приведёт к неоднозначному результату, поскольку функция $w(z)$ имеет критические точки, вблизи которых она неоднозначна. Чтобы избежать такой неоднозначности, отметим на сфере корни дискриминанта $D(z)$ уравнения (1) и соединим их отрезками прямых с точкой $z = z_0$. При этом наложим на точку $z = z_0$ дополнительное требование, состоящее в том, что эти отрезки не должны налегать один на другой (черт. 9). Если мы мысленно представим себе вдоль этих отрезков разрезы, то они не нарушат *связности* сферы; это значит, что любую точку сферы можно соединить с $z_0$ кривой (и даже ломаной), не пересекающей ни одного из проведённых разрезов.



Черт. 9.

Вместе с тем, если мы условимся понимать под значением $w(z)$ в каждой точке $z$, не лежащей ни на одном из наших разрезов, то значение, которое получено из $w(z_0) = w_1$ путём аналитического продолжения вдоль пути, не пересекающего ни одного из наших

разрезов, то это определение $w(z)$ будет однозначно. В самом деле, если мы проведём два такого рода пути, то их совокупность образует замкнутую кривую, не содержащую внутри себя критических точек $a_1$, $a_2$, $a_3$, ... С другой стороны, если при аналитическом продолжении функции вдоль замкнутой кривой мы не возвращаемся к исходному значению, то внутри площади, ограниченной этой кривой, непременно содержатся критические точки (см. § 37, XII, конец).

Что касается точек, лежащих на разрезах, то мы можем определить на них значения функции $w(z)$, если будем приближаться к ним с той или другой стороны (*берега*) разреза. Таким путём мы получим для одной и той же точки два значения, которые в общем случае не будут совпадать, а будут различными корнями уравнения (1), соответствующими одному и тому же значению $z$. Если бы оказалось, что на всех разрезах оба значения функции совпадают, то это бы означало, что функция $w(z)$ была бы однозначна на всей сфере и, следовательно, не имела бы на ней критических точек, а потому в силу § 37, IX, была бы рациональной функцией от $z$, так что левая часть уравнения (1) имела бы рациональный множитель, линейный относительно $w$.

Возьмём $n$ сфер, проведём на каждой описанную систему разрезов и отнесём каждой точке $z$ $i$-й сферы значение $w(z)$, полученное путём аналитического продолжения функции $w(z)$, исходя из значения $w = w_i$ при $z = z_0$ ($i = 1, 2, \ldots, n$). Таким путём мы получим для каждого значения $z$ $n$ значений $w$. Если точка $z$ не критическая, то все они будут различны, так как в противном случае, совершая аналитическое продолжение в обратном порядке вдоль пути, не проходящего через разрезы, мы придём от одного и того же значения $w$ в точке $z$ к двум различным значениям $w$ в точке $z = z_0$, что невозможно. Из этого следует, что значения функции $w(z)$ для одного и того же значения $z$ на всех $n$ сферах исчерпают все корни уравнения (1) для этого значения $z$.

Возьмём точку $z = z_1$, лежащую на одном из наших разрезов. Обозначим через

$$\overset{+}{w}_1,\ \overset{+}{w}_2,\ \ldots,\ \overset{+}{w}_n \tag{3}$$

значения $w(z_1)$ на 1-й, 2-й, ..., $n$-й сферах, определённые с одного и того же берега, и через

$$\overset{-}{w}_1,\ \overset{-}{w}_2,\ \ldots,\ \overset{-}{w}_n \tag{4}$$

те же значения, определённые с противоположного берега. Как совокупность (3), так и совокупность (4) исчерпывают все корни уравнения (1) при $z = z_1$, а потому обе совокупности совпадают, так что

$$\overset{+}{w}_1 = \overset{-}{w}_{a_1},\quad \overset{+}{w}_2 = \overset{-}{w}_{a_2},\quad \ldots,\quad \overset{+}{w}_n = \overset{-}{w}_{a_n},$$

где

$$S=\begin{pmatrix}1 & 2 & \dots & n\\ \alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix} \tag{5}$$

есть некоторая подстановка над цифрами 1, 2, ..., $n$. Эта подстановка одна и та же вдоль разреза. В самом деле, если мы будем продвигаться вдоль одного берега разреза, то значение $\overset{+}{w}_i$ будет меняться непрерывно, и точно так же будет непрерывно меняться значение $\overset{-}{w}_{\alpha_i}$. Но так как в точке $z=z_1$ имеет место

$$\overset{+}{w}_i=\overset{-}{w}_{\alpha_i}, \tag{6}$$

причём вдоль всего разреза, за исключением одного конца, все значения (3), а также все значения (4) различны, то (5) должно иметь место вдоль всего разреза.

Чтобы определить подстановку (5), совершаемую при переходе через $\nu$-й разрез, обратимся к тем точкам разреза, которые находятся вблизи его конца, т. е. в окрестности критической точки $z=a_\nu$. Мы видели [см. § 38, (18) и (19)], что все разложения функции $w(z)$ вблизи критической точки $z=a_\nu$ разбиваются на несколько циклов порядков $b_1, b_2, \dots, b_k$, где

$$b_1+b_2+\dots+b_k=n.$$

При этом разложения $\mu$-го цикла являются рядами по целым степеням $(z-a_\nu)^{\frac{1}{b_\mu}}$:

$$w_{\mu,0}=\psi\left[(z-a_\nu)^{\frac{1}{b_\mu}}\right],\quad w_{\mu,1}=\psi\left[\varepsilon_\mu\cdot(z-a_\nu)^{\frac{1}{b_\mu}}\right],\quad \dots, \tag{7}$$

$$w_{\mu,\,b_\mu-1}=\psi\left[\varepsilon_\mu^{b_\mu-1}\cdot(z-a_\nu)^{\frac{1}{b_\mu}}\right],$$

$$\varepsilon_\mu=e^{\frac{2\pi i}{b_\mu}}\qquad(\mu=1,2,\dots,k).$$

Пусть $z=z_2$ есть значение $z$ вблизи точки $z=a_\nu$. Положим

$$z_2-a_\nu=\rho\cdot e^{i\theta_2}$$

и станем, не изменяя значения $\rho$, непрерывно увеличивать $\theta$ от $\theta_2$ до $\theta_2+2\pi$. Тогда точка $z$ опишет окружность радиуса $\rho$ с центром в $a_\nu$. Из формул (7) следует, что $w_{\mu0}$ перейдёт в $w_{\mu1}$, $w_{\mu1}$ в $w_{\mu2}$, ... ..., $w_{\mu,\,b_\mu-1}$ в $w_{\mu0}$.

Будем обозначать символом $+$ ($-$) тот берег $\nu$-го разреза, который соответствует значению $\theta=\theta_2$ ($\theta=\theta_2+2\pi$). Это означает, что, продвигаясь вдоль разреза от $z=z_0$ до $z=a_\nu$, мы будем иметь берег $+$ с правой стороны, а берег $-$ с левой. Тогда

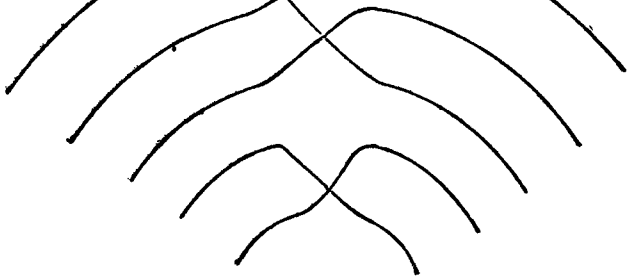
$$\overset{-}{w}_{\mu0}=\overset{+}{w}_{\mu1},\quad \overset{-}{w}_{\mu1}=\overset{+}{w}_{\mu2},\quad \dots,\quad \overset{-}{w}_{\mu,\,b_\mu-1}=\overset{+}{w}_{\mu0}. \tag{8}$$

Заменяя нумерацию, введённую в формулах (7), нумерацией формул (3) и (4), мы получим искомую подстановку $S = S_v$.

Пусть $a_1, a_2, \ldots, a_v$ будет полная система критических точек функции $w(z)$, занумерованных так, что, вращая луч, проведённый из точки $z = z_0$, против часовой стрелки, мы будем последовательно совмещать его с 1-м, 2-м, ..., $v$-м разрезом. Тогда, совершая одновременно на всех сферах обход против часовой стрелки, вокруг точки $z = z_0$, мы при переходе через $\nu$-й разрез заставим значения функции $w(z)$ испытать подстановку $S_\nu$ ($\nu = 1, 2, \ldots, v$). Поэтому, если мы совершим полный обход вокруг точки $z = z_0$, то значения функции $w(z)$ претерпят подстановку $S_1 \cdot S_2 \ldots S_v$. Но, поскольку $z = z_0$ есть некритическая точка функции $w(z)$, при обходе вокруг $z = z_0$ значения функции должны вернуться к исходным, т. е. испытают тождественную подстановку, а потому

$$S_1 \cdot S_2 \ldots S_v = \mathcal{E}. \tag{9}$$

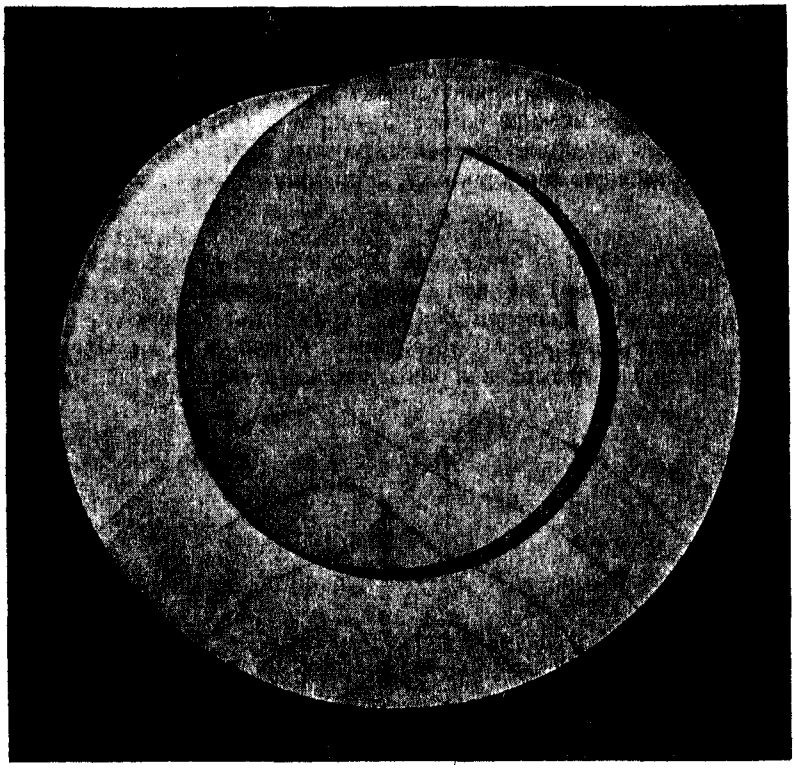
Для получения из $n$ отдельных сфер единой поверхности отождествим в каждом ($v$-м) разрезе берег $+$ $i$-й сферы с берегом $-$ $\alpha_i$-й сферы, поскольку значения $w(z)$ вдоль этих берегов совпадают. Вместо абстрактного «отождествления» Риман и его последователи (Нейман и др.) вкладывали в него вполне материальный наглядный



Черт. 10.

смысл. Они представляли себе $n$ сфер концентрически вложенными одна в другую, причём одинаковым значениям $z$ должны были соответствовать точки, расположенные на общем радиусе. Поэтому и разрезы должны были лежать на общих конусах с вершиной в центре сфер. Затем края разрезов склеивались (сферы мыслились сделанными из гибкой и растяжимой плёнки), $i$-ый край $+$ склеивался с $\alpha_i$-м краем $-$, сообразно с подстановкой $S$, которую должны были претерпевать значения функции $w(z)$ при переходе через разрез. При этом плёнка, из которой сделаны сферы, предполагалась проницаемой, так как при склеивании листы сфер должны были пересекаться друг с другом (на черт. 10 изображён разрез поверхности,

перпендикулярный к системе склеенных листов сфер), если при переходе через разрез значения $w(z)$ претерпевают подстановку $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$; однако при этом точки двух листов, находящиеся на пересечении этих листов, должны считаться различными. Если



Черт. 11.

угодно, можно представить себе склеивание сфер произведённым в 4-мерном пространстве.

Полученная система из $n$ склеенных сфер получила название *римановой поверхности*. Она замечательна тем, что каждой её точке соответствует одно определённое значение функции $w(z)$, причём значения $w(z)$ для различных точек поверхности получаются одно из другого при помощи аналитического продолжения вдоль путей, расположенных на римановой поверхности; результат аналитического продолжения не зависит от формы пути.

Вблизи критических точек риманова поверхность образует несколько систем переплетающихся друг с другом листов, сообразно с числом циклов, которые образуют разложения вблизи этих критических точек. Нейман назвал каждую такую систему словом Kalotte. На черт. 11 изображён образец такой системы, высеченный из римановой поверхности конусом с вершиной в центре сфер и с осью, проходящей через критическую точку.

Каждой точке римановой поверхности можно взаимно однозначно сопоставить определённую нами в § 13 точку поля $k(z, w)$; это делает понятным термин «точка абсолютной римановой поверхности», введённый Дедекиндом и Вебером и употребляемый как синоним термина «точка поля».

## § 41. Группа монодромии

Представим себе новую сферу, концентрическую со сферами, образующими риманову поверхность, и помещённую снаружи. Будем сопоставлять с каждой её точкой значение переменной $z$, а $n$ пересечений проведённого к ней радиуса с листами римановой поверхности со значениями функции $w(z)$, определёнными на этих листах. Будем называть эту сферу *следовой сферой*.

С каждым замкнутым путём на следовой сфере (если он не проходит через критические точки) будем сопоставлять подстановку, которую претерпят значения функции $w(z)$, если мы заставим точку $z$ описать этот путь. Для наглядности представим себе иглу, закреплённую одним концом в центре сферы и свободно принимающую положение любого радиуса сферы. В каждом своём положении она протыкает следовую сферу в одной точке и риманову поверхность в соответствующих ей точках (материал, из которого сделаны сферы, предполагается не оставляющим дыр после прохождения по нему иглы). Пусть игла продета сквозь $n$ бусинок, каждая из которых скользит по листу римановой поверхности, и пусть эти бусинки могут свободно проходить одна сквозь другую Тогда при прохождении иглой замкнутой кривой, начерченной на следовой сфере, бусинки претерпят подстановку, ту самую, которую при этом претерпевают значения функции $w(z)$.

В частности, если игла опишет малую окружность вокруг $\nu$-й критической точки $z = a_\nu$, бусинки претерпят подстановку $S_\nu$, которая определяется при помощи циклов разложений $w(z)$ вблизи точки $z = a_\nu$.

Будем называть, следуя Жордану (C. Jordan), *группой монодромии* совокупность подстановок, которые претерпевают бусинки при прохождении иглой всевозможных замкнутых путей, начинающихся и кончающихся в фиксированной точке $z = z_0$ следовой сферы. Эта совокупность образует группу, так как, если путям $\Sigma$, $\Sigma'$ соответствуют подстановки $S$, $S'$, то пути $\Sigma + \Sigma'$, состоящему в последо-

вательном прохождении путей $\Sigma$ и $\Sigma'$ (сложение путей не коммутативно!), соответствует подстановка $S \cdot S'$.

Будем называть *композитом* подстановок (1)

$$S_1, S_2, \ldots, S_\nu \tag{1}$$

наименьшую группу, содержащую эти подстановки. В теории групп доказывается, что всякая подстановка, входящая в композит, может быть представлена как конечное произведение подстановок (1). Мы не будем останавливаться на доказательстве этого факта.

Имеет место

Теорема 70. *Группа монодромии есть композит подстановок* (1).

Доказательство. Прежде всего заметим, что каждая из подстановок (1) входит в группу монодромии, так как она соответствует пути, состоящему из прямолинейного отрезка, соединяющего точку $z = z_0$ с точкой окрестности точки $z = a_\nu$, обхода вокруг этой точки и того же прямолинейного отрезка, путь по которому идёт в обратном направлении, до точки $z = z_0$. В силу этого и композит подстановок (1) содержится в группе монодромии.

Обратно, пусть $S$ будет произвольная подстановка группы монодромии и пусть ей соответствует на следовой сфере замкнутая кривая $\Sigma$, не проходящая через критические точки. Если она пересекается сама с собой, заменим её суммой нескольких замкнутых кривых, каждая из которых не пересекается сама с собой. Если такой контур не проходит через точку $z = z_0$, то, соединив любую его точку с $z_0$ прямолинейным отрезком и заставляя иглу пройти вдоль отрезка от $z_0$ до контура, затем вдоль контура и, наконец, вдоль того же отрезка до $z_0$ в обратном направлении, мы разобьём контур на сумму контуров, не пересекающих самих себя.

Если какой-нибудь слагаемый контур, не пересекающий сам себя, содержит внутри себя несколько критических точек, то точно таким же образом разобьём его на сумму контуров, содержащих внутри себя по одной критической точке. Пусть такого рода контур содержит внутри себя только одну критическую точку $a_\nu$. Если обход вдоль него должен совершаться в положительном (отрицательном) направлении*), то при обходе вдоль него иглы её бусинки претерпевают подстановку $S_\nu (S_\nu^{-1})$. Это показывает, что при обходе иглы вдоль заданного контура её бусинки претерпевают подстановку, выражаемую в виде произведения подстановок (1), т. е. входящую в композит подстановок (1), ч. т. д.

Группа монодромии является группой Галуа поля $k(z, w)$, если в качестве области рациональности мы возьмём поле $k(z)$ рациональ-

*) Как и раньше, мы будем считать положительным направлением обхода по замкнутому контуру то его направление, при обходе вдоль которого внутренняя площадь, ограниченная контуром, остаётся слева.

ных функций от $z$ с любыми комплексными коэффициентами. Нижеследующие теоремы убедят в этом знающего теорию Галуа, а незнающий получит в них понятие о теории Галуа, приспособленное к этим специальным полям.

Будем называть всякое соотношение вида

$$\Phi(z, w_1, w_2, \ldots, w_n) = 0, \tag{2}$$

в котором левая часть есть полином от своих аргументов, *рациональным соотношением* между корнями уравнения

$$f(z, w) = 0. \tag{3}$$

Будем говорить, что подстановка

$$S = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \end{pmatrix}$$

*не нарушает* соотношение (2), если также имеет место

$$\Phi(z, w_{\alpha_1}, w_{\alpha_2}, \ldots, w_{\alpha_n}) = 0. \tag{4}$$

Тогда имеет место

Теорема 71. *Подстановки $S$ группы монодромии не нарушают рациональных соотношений между корнями уравнения* (3).

Доказательство Будем рассматривать левую часть соотношения (2) как аналитическую функцию от точки следовой сферы. Поскольку она равна нулю в некоторой области, она должна быть равна нулю при всевозможных аналитических продолжениях. В частности, выберем в качестве пути для продолжения замкнутую кривую, соответствующую подстановке $S$. После его прохождения левая часть (2) обращается в левую часть (4), которая таким образом равна нулю, ч. т. д.

Теорема 72. *Функция $\Psi(z, w_1, w_2, \ldots, w_n)$, рациональная относительно своих аргументов и инвариантная при всех подстановках группы монодромии, рациональна относительно $z$.*

Доказательство. Рассматривая $\Psi$ как аналитическую функцию от точки $z$ следовой сферы, мы из предположенного свойства заключаем, что она однозначна. Она не имеет других особых точек, кроме полюсов, а потому в силу § 37, IX, есть рациональная функция от $z$, ч. т. д.

Будем называть *транзитивной* группу подстановок, содержащую подстановки, переводящие любую заданную цифру, $i$, в любую другую, $j$. Чтобы убедиться в транзитивности группы, достаточно проверить, что она переводит цифру 1 в любую другую цифру. В самом деле, если $S_i$ переводит 1 в $i$, а $S_j$ переводит 1 в $j$, $S_j S_i^{-1}$ переводит $i$ в $j$.

**Теорема 73.** *Чтобы уравнение* (3) *было неприводимо, необходимо и достаточно, чтобы его группа монодромии была транзитивна.*

Доказательство. Пусть (3) приводимо, но не имеет кратных корней. Пусть

$$f(z, w) = g(z, w) \cdot h(z, w).$$

Пусть $w_1$ будет один из корней первого множителя и $w_2$ — второго. Тогда

$$g(z, w_2) \neq 0.$$

Но в силу теоремы 71 соотношение

$$g(z, w_1) = 0$$

сохраняется при всех подстановках группы монодромии. Из этого следует, что группа монодромии не содержит подстановки, переводящей $w_1$ в $w_2$, т. е. что она интранзитивна.

Обратно, пусть группа монодромии уравнения (3) интранзитивна и пусть она переводит $w_1$ в

$$w_1, w_2, \ldots, w_k \qquad (k < n).$$

Тогда коэффициенты полинома

$$g(z, w) = (w - w_1)(w - w_2)\ldots(w - w_n)$$

инвариантны относительно подстановок группы монодромии и потому в силу теоремы 72 являются рациональными функциями от $z$. Полином $f(z, w)$ делится на полином $g(z, w)$ более низкой степени, в силу чего он приводим.

Из этой теоремы следует, что риманова поверхиость неприводимого уравнения *связна*: каковы бы ни были две её точки, существует соединяющая их непрерывная кривая, лежащая целиком на поверхности. Отсюда также следует доказанный ранее факт, что всякое неприводимое уравнение непременно имеет критические точки. В самом деле, если бы критических точек не было, то все подстановки (1) были бы тождественными и группа монодромии была бы единичной группой, а тогда уравнение (3) в силу теоремы 73 не могло бы быть неприводимым.

## § 42. Элементарные сведения из топологии

Существенное различие между сферой (или плоскостью) и римановой поверхностью состоит в том, что всякая спрямляемая замкнутая кривая (*прорез*), проведённая на сфере, делит её на две части такого рода, что две точки, лежащие в различиых частях, не могут быть соединены путём, не пересекающим прореза. Мы будем счи-

тать известным этот факт, доказываемый в больших курсах анализа и топологии.

Это свойство сферы (и плоскости) не имеет места для других поверхностей. Примером может служить *тор* (полое кольцо), полученный вращением окружности вокруг оси, не пересекающей её. Прорез вдоль одного из положений окружности (*меридиональный*) оставляет поверхность связной.

Будем рассматривать поверхности, обладающие следующими свойствами:

I. Они должны быть *триангулируемы*, т. е. допускать разбиение на конечное число треугольников (или конечных кусков поверхности, которые могут быть непрерывно и взаимно однозначно отображены на треугольники).

II. Они должны быть *ориентируемы* (или *двусторонними*). Это значит, что после триангуляции мы можем установить такое направление обхода вдоль границы каждого треугольника, что эти направления у соседних треугольников вдоль их общей границы всегда будут противоположны.

В каждой поверхности мы будем предполагать конечное число *границ*, т. е. связных линий такого рода, что точки поверхности лежат по одиу их сторону. Так, треугольник имеет одну границу; плоское кольцо — две.

Сначала мы будем рассматривать поверхности, имеющие хотя бы одну границу. Поверхности, не имеющие границ, будем называть *замкнутыми*.

Будем называть *разрезом* (Querschnitt) спрямляемую кривую, концы которой лежат на границах поверхности. *Прорезом* (Rückerschnitt) будем называть спрямляемую замкнутую кривую, не имеющую ни самопересечений, ни пересечений с границами поверхности. *Проколом* будем называть прорез в виде небольшой окружности с последующим изъятием вырезанного круга. Прокол всегда увеличивает число границ на единицу.

Часть поверхности, отображаемая на треугольник (или на круг), называется *односвязной*. Она обладает следующим почти очевидиым свойством, доказательство которого мы опустим:

III. Всякий разрез, проведённый на односвязной поверхности, делит её на две части.

Если поверхность после проведения на ней $P$ разрезов разбивается на $K$ односвязных кусков, то Риман называет число

$$P-K+2 \tag{1}$$

*порядком связности* поверхности. Чтобы сделать это определение законным, он доказывает следующую теорему:

Теорема 74. *Если мы проведём на одной и той же поверхности две системы разрезов, состоящих соответственно из $P$ и*

*$P'$ разрезов и разбивающих поверхность соответственно на $K$ и $K'$ односвязных кусков, то*

$$P - K + 2 = P' - K' + 2. \tag{2}$$

Доказательство. Наложим обе системы разрезов одна на другую, причём предположим, что

1) пересечения первой системы разрезов не совпадают с пересечениями второй системы разрезов;

2) каждое пересечение первой системы пересекается с каждым пересечением второй системы лишь в конечном числе точек. Этим условиям мы всегда сможем удовлетворить при помощи бесконечно малой деформацин одной из систем разрезов.

Пусть первая система в целом пересекается со второй системой в $S$ точках. Будем считать первую систему разрезов уже проведённой. После этого поверхность будет состоять из $K$ односвязных кусков. Когда мы на неё наложим вторую систему разрезов, то она будет состоять уже не из $P'$ разрезов, а из $P' + S$ разрезов, поскольку каждая точка пересечения обеих систем увеличивает число разрезов на единицу. Но, так как каждый разрез, проведённый по односвязной поверхности, делит её на две, после проведения второй системы разрезов мы получим всего

$$K + P' + S$$

односвязных кусков.

Меняя ролями первую и вторую системы разрезов, мы придём к

$$K' + P + S$$

односвязным кускам. Но так как оба числа получаются в результате проведения на поверхности одной и той же системы разрезов, то они должны быть равны

$$K + P' + S = K' + P + S,$$

откуда вытекает соотношение (2), ч. т. д.

В частности, односвязная поверхность имеет порядок связности 1, поскольку для неё может быть положено $P = 0$, $K = 1$ (для получения этого результата Римана вводят в определение порядка связности слагаемое 2).

Порядок связности может быть определён по такому же правилу для несвязной поверхности, т. е. для системы нескольких связных поверхностей. Для них он может иметь и отрицательные значения.

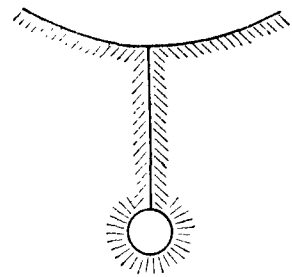
Теорема 74 *показывает, что порядок связности поверхности есть величина, характеризующая внутренние свойства поверхности. Из неё, как простые следствия, вытекают следующие теоремы:*

Теорема 75. *Разрез, проведённый на поверхности, уменьшает порядок её связности на единицу.*

В самом деле, если после проведения этого разреза $P$ новых разрезов приведут поверхность к $K$ односвязным кускам, то в первоначальной поверхности для этого же потребуется $P+1$ разрезов.

Теорема 76. *Прокол повышает порядок связности поверхности на единицу.*

Это следует из того, что разрез, соединяющий прокол с другой границей, аннулирует прокол (черт. 12).

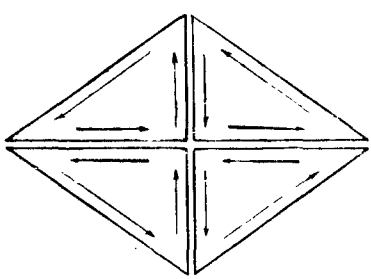


Черт. 12.

Теорема 77. *Прорез не меняет порядка связности.* Это следует из того, что прорез может рассматриваться как прокол с последующим разрезом, соединяющим точки границы, образованной проколом.

Определение порядка связности, сделанное Риманом, предполагает, что поверхность имеет границы, поскольку разрез можно провести только по поверхности, имеющей границы. Для определения порядка связности замкнутой поверхности сделаем на ней прокол. Пусть порядок связности полученной поверхности (которая уже имеет границу) есть $C$. Тогда введём как определение порядка связности первоначальной поверхности, что *её порядок связности равен* $C-1$ *).

Это определение сохраняет в силе теоремы 76 и 77 и для замкнутых поверхностей.



Черт. 13.

В частности, нетрудно доказать, что для сферы порядок связности равен нулю; для тора он равен двум.

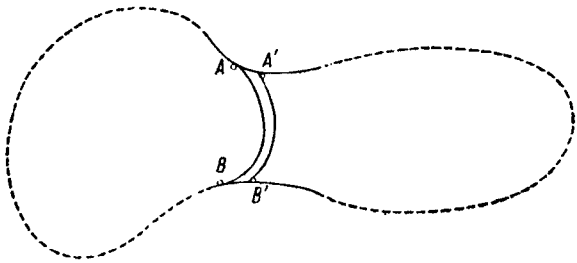
Обратимся к рассмотрению числа границ поверхности.

Теорема 78. *Каждый прорез, проведённый по ориентируемой поверхности, увеличивает число её границ на два.*

Доказательство. Триангулируем поверхность так, чтобы треугольники расположились вдоль прореза, и установим для каждого треугольника направление обхода. Если мы установим по прорезу тоже определение обхода, то в каждой точке прореза к нему будут примыкать два треугольника, в одном из которых направление обхода будет совпадать с направлением обхода на прорезе, а в другом будет ему противоположно. Если мы будем продвигаться вдоль определённого берега прореза (т. е. без перехода через прорез), то из черт. 13 видно, что направления обхода треугольников будут всё время или

*) Это определение порядка связности замкнутой поверхности не общепринято.

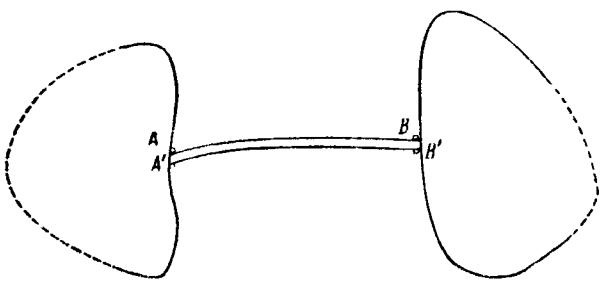
совпадать с направлением обхода прореза, или направлены противоположно ему. В первом случае будем называть берег левым, во втором — правым. Таким образом при обходе вдоль всего берега он всё время остаётся левым (или правым), так что каждый из берегов образует отдельную границу прорезанной поверхности.




Черт. 14.

Теорема 79. *Разрез или увеличивает на единицу, или уменьшает на единицу число границ поверхности.*

Доказательство. Если разрез соединяет две точки одной и той же границы, то вместе с частью границы один его берег составит новую границу, а другой его берег вместе с оставшейся частью границы составит вторую новую границу (черт. 14). Таким образом число границ возрастёт на единицу. Если же разрез соединяет точки двух различных границ, то последовательный обход первой границы, правого берега разреза, второй границы и левого берега разреза




Черт. 15.

показывает, что разрез превратил обе границы в одну, так что число границ уменьшилось на единицу (черт. 15).

Из того, что этот обход соединяет точки, лежащие на противоположных берегах разреза, не переходя через разрез, следует.

Теорема 80. *Разрез, соединяющий две различные границы, не нарушает связности поверхности.*

Каждый проведённый разрез меняет чётность как порядка связности (теорема 75), так и числа границ поверхности. С другой сто-

роны, если после проведения $P$ разрезов поверхность превращается в $K$ односвязных кусков, то порядок связности полученной системы кусков равен

$$0 - K + 2,$$

а число её границ равно $K$. Эти числа имеют одинаковую чётность, а потому вообще имеет место

Теорема 81. *Порядок связности и число границ одной и той же поверхности имеют одну и ту же чётность. В частности, порядок связности замкнутой поверхности есть чётное число.*

Среди систем разрезов, приводящих поверхность к системе односвязных кусков, существует система разрезов, приводящая поверхность к одному куску и носящая название *римана канонического сечения*. Она играет большую роль в теории абелевых интегралов.

Ограничимся рассмотрением замкнутой поверхности, что, впрочем, не является существенным ограничением. Пусть её порядок связности равен $2p$ (см. теорему 81). Сделаем в ней прокол, после чего её порядок связности будет $2p+1$ (см. теорему 76). При $p>0$ эта поверхность не односвязна. Вместе с тем

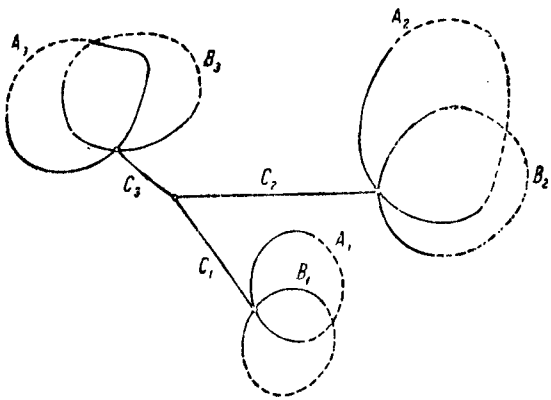
Теорема 82. *Если поверхность имеет одну границу и такова, что любой проведённый на ней разрез разбивает её на две части, то она односвязна.*

Доказательство. Триангулируем поверхность. Если она состоит из одного треугольника, справедливость теоремы очевидна. Предположим, что она доказана для $n-1$ или меньшего числа треугольников, и докажем её для $n$ треугольников. Возьмём один из треугольников, имеющих часть границы в качестве стороны, и проведём разрез вдоль остальных двух сторон. Пусть этот разрез не пересекается с границей. Согласно предположению, он разобьёт поверхность на две части, из которых одна, очевидно, односвязна, а другая, как состоящая из $n-1$ треугольников и вместе с тем, как легко доказать, разбивающаяся всяким разрезом на две части, тоже односвязна. Поэтому для исходной поверхности можно принять $P=1$, $K=2$, откуда её порядок связности равен $1-2+2=1$.

Если выбранный нами треугольник вершиной примыкает к границе, то разрез вдоль двух его сторон составляет два разреза поверхности, которые делят поверхность на три части, каждая из которых, как мы аналогично докажем, односвязна. Поэтому мы можем положить для исходной поверхности $P=2$, $K=3$, так что её порядок связности равен $2-3+2=1$. В обоих случаях поверхность односвязна.

Вернёмся к каноническому сечению. В силу теоремы 82 существует разрез, не разбивающий поверхности. Поскольку прокол является единственной границей поверхности, разрез должен начинаться и кончаться у прокола. Обозначим этот разрез буквой $A_1$. Его левый

и правый берега образуют две границы рассечённой поверхности. Обозначим через $B_1$ разрез, соединяющий точки, лежащие друг против друга на обоих берегах разреза $A_1$. В силу теоремы 80 он не разбивает поверхности. Полученная поверхность будет иметь одну границу и порядок связности $2p-1$. При $p>1$ она опять не односвязна, в силу чего на ней существует разрез $A_2$, не разбивающий поверхности. Его начало и конец всегда можно взять исходящими из общей точки границы. Он опять превратит поверхность в поверхность с двумя границами. Соединим разрезом $B_2$ две точки, лежащие друг против друга на обоих берегах разреза. Продолжая проводить такого рода разрезы, мы после $2p$ разрезов



Черт. 16.

$$A_1,\ B_1;\quad A_2,\ B_2;\ \ldots\ \ldots;\quad A_p,\ B_p$$

придём к поверхности с одной границей, имеющей порядок связности 1, т. е. односвязной.

Для удобства обозрения канонической системы разрезов сделаем предварительный прокол в форме $p$-конечной звезды и каждую пару разрезов $A_i$, $B_i$ $(i=1, 2, \ldots, p)$ будем начинать и кончать в $i$-м конце этой звезды (черт. 16). Обозначим лучи звезды буквами $C_1, C_2, \ldots, C_p$. Тогда обход всей границы поверхности будет происходить по следующим (через $\overset{+}{A}_i$, $\overset{-}{A}_i$ будем обозначать левый и правый берега разреза $A_i$) разрезам:

$$\overset{+}{C}_1,\ \overset{+}{A}_1,\ \overset{+}{B}_1,\ \overset{-}{A}_1,\ \overset{-}{B}_1;\quad \overset{-}{C}_2,\ \overset{+}{C}_2;\ \overset{+}{A}_2,\ \ldots;\quad \overset{+}{C}_p;\ \overset{+}{A}_p,\ \overset{+}{B}_p,\ \overset{-}{A}_p,\ \overset{-}{B}_p,\ \overset{-}{C}_p.$$

## § 43. Порядок связности римановой поверхности

При определении порядка связности римановой поверхности мы встретим затруднение, которое заключается в том, что часть поверхности, которую мы в § 41 назвали Kalotte, не подходит под тип разобранных нами кусков поверхности и даже не умещается в трёхмерном пространстве.

Чтобы преодолеть это затруднение, учтём, что риманова поверхность в теории алгебраических функций играет вспомогательную роль. Дело в том, что на поверхности, на которой проведена кано-

ническая система разрезов, имеет место теорема Коши, так как всякий замкнутый контур (прорез) на такой поверхности делит её на две части, из которых внутренняя допускает триангуляцию. Поэтому важно знать, из скольких разрезов состоит каноническое сечение. В связи с этим мы должны будем считать, что «Kalotte» односвязна, если для неё будет доказана теорема Коши.

Рассмотрим «Kalotte», склеенную из $m$ листов. На ней однозначна функция

$$w = \varphi\left(z^{\frac{1}{m}}\right).$$

Подстановка

$$z = t^m$$

переводит «Kalotte» во внутреннюю часть круга, на котором однозначна функция

$$w = \varphi(t).$$

Интеграл

$$\int \psi\left(z^{\frac{1}{m}}\right) dz$$

переходит при этом в интеграл

$$\int \psi(t)\, m t^{m-1} dt,$$

для которого внутри упомянутого круга справедлива теорема Коши. Это даёт нам право считать «Kalotte» односвязным куском поверхности.

Определим порядок связности римановой поверхности, склеенной из $n$ сфер, на которых нанесены критические точки

$$P_1,\ P_2,\ \ldots,\ P_k$$

соответственно кратностей

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k.$$

Здесь мы считаем, что в каждой точке $P_k$ циклически переходят друг в друга $\alpha_i$ листов, причём считаем эти точки отдельно, независимо от того, принимает ли для некоторых из них переменная $z$ одинаковые значения или нет. Значение $z = \infty$ рассматривается наряду с другими. Для числа

$$\sum_{i=1}^{k} (\alpha_i - 1) = \sum_{i=1}^{k} \alpha_i - k,$$

как обычно, вводится обозначение $w$. Все точки $P_i$ соединены отрезками с обыкновенной точкой $P_0 (z = z_0)$ следовой сферы, и склеивание листов произведено по этим отрезкам.

Обозначим искомый порядок связности через $C$. Сделаем проколы в $n$ точках, соответствующих точке $P_0$ следовой сферы; порядок связности полученной поверхности в силу теоремы 76 равен $C+n$. Далее, сделаем прорезы вокруг точек $P_1, P_2, \ldots, P_k$. Порядок связности от этого не изменится, но от поверхности отделится $k$ «Kalotten».

В полученной поверхности сделаем разрезы вдоль отрезков, соединяющих точки со следом $P_0$ с точками $P_i$. Число этих разрезов, $P$, равно сумме чисел листов, соединённых в каждом цикле:

$$P=\sum_{i=1}^{k}\alpha_i.$$

После этого все сферы сделаются разделёнными, причём каждая сфера будет снабжена одним звездообразным проколом с центром в $P_0$, так что будет односвязна. Сюда же мы должны присчитать $k$ односвязных «Kalotten», выделенных ранее. Таким образом

$$K=n+k,$$

и для искомого порядка связности мы получим

$$C+n=P-K+2=\sum_{i=1}^{K}\alpha_i-n-k+2=$$

$$=\sum_{i=1}^{K}(\alpha_i-1)-n+2=w-n+2,$$

откуда

$$C=w-2n+2=2\rho, \tag{1}$$

и мы приходим к теореме:

Теорема 83. *Порядок связности римановой поверхности, построенной для алгебраических функций жанра $\rho$, равен удвоенному жанру.*

Если мы при определении поля $k(z, w)$ возьмём другую примитивную пару элементов, то в полученной для неё римановой поверхности может быть другое число листов и другое число критических точек. Однако порядок связности обеих поверхностей будет один и тот же. Это связано с тем, что точки обеих римановых поверхностей могут быть приведены во взаимно однозначное и непрерывное соответствие, получаемое при помощи бирационального соотношения между обеими примитивными парами.

## § 44. Число замкнутых вещественных ветвей кривой

В виде приложения теории римановых поверхностей выведем результаты Гариака (A. Harnack) относительно максимального числа отдельных замкнутых и не пересекающих друг друга замкнутых ветвей, которые может образовать алгебраическая кривая жанра $\rho$.

Предварительно докажем вспомогательную теорему из топологии.

Теорема 84. *На ориентируемой замкнутой поверхности порядка связности $2p$ можно провести не более $p$ не пересекающих друг друга прорезов, которые бы не разбивали поверхности на части.*

Доказательство. Пусть на этой поверхности проведено $k$ таких прорезов. В силу теоремы 78 эта поверхность будет иметь $2k$ границ и в то же время в силу теоремы 77 останется порядка связности $2p$. Из того, что разрез, соединяющий две различные границы, не нарушает связности поверхности (теорема 80), следует, что на поверхности можно ещё пронести $2k-1$ разрезов, не нарушающих её связности. Полученная поверхность будет иметь одну границу и вместе с тем в силу теоремы 75 будет иметь порядок связности $2p-2k+1$. Если поверхность Римана такова, что любой проведённый на ней разрез нарушает её связность, то она в силу теоремы 82 односвязна; в противном случае мы можем провести на ней ещё несколько разрезов, которые в конце концов сделают её односвязной поверхностью. В обоих случаях

$$2p-2k+1 \geqslant 1,$$

откуда

$$k \leqslant p,$$

ч. т. д.

Рассмотрим алгебраическое уравнение

$$f(x, y)=0 \tag{1}$$

жанра $p$ с вещественными коэффициентами. Пусть удовлетворяющие ему системы вещественных значений переменных $x$, $y$ образуют $s$ связных множеств, не пересекающих друг друга. Каждое из них отобразится на римановой поверхности на связную замкнутую линию, причём ни одна из этих $s$ линий не пересекается с другой. На следовой сфере все эти линии спроектируются на вещественную ось. Обозначим эти линии через

$$L_1, L_2, \ldots, L_s. \tag{2}$$

Рассмотрим отображение $T$ римановой поверхности самой на себя, состоящее в сопоставлении каждой её точки $(x, y)$ с точкой $(\bar{x}, \bar{y})$, в которой значения переменных $x$, $y$ комплексно сопряжены. Отметим следующие свойства отображения $T$:

1) оно непрерывно на всей римановой поверхности;

2) оно оставляет на месте все точки, лежащие на линиях (2);

3) оно переводит точку левого берега кривой $L_\nu$ $(\nu=1, 2, \ldots, s)$ в точку правого берега, и обратно.

Первые два утверждения очевидны. Для доказательства последнего заметим, что принадлежность точки $(\xi+i\eta, y)$ к левому (пра-

вому) берегу кривой может быть охарактеризована тем, что $\eta > 0$ ($\eta < 0$) и $|\eta|$ весьма мало.

Проведём вдоль каждой из линий (2) римановой поверхности прорезы, кроме одной из них, например $L_s$. Докажем, что эти прорезы не нарушают связности римановой поверхности. Допустим противное: пусть эти прорезы разбивают поверхность на несколько кусков. Тогда линия $L_s$ должна целиком лежать на одном из этих кусков, $K$. Поскольку преобразование $T$ оставляет все точки линии $L_s$ на месте, оно в силу непрерывности переводит $K$ в себя. Пусть границами куска $K$ являются берега прорезов $L_1, L_2, \ldots, L_t$. Тогда, поскольку преобразование $T$ переводит один из берегов этих линий в другой, $K$ должно содержать оба берега каждой из линий $L_1, L_2, \ldots, L_t$. Однако это невозможно. В самом деле, пусть при последовательном проведении прорезов $L_1, L_2, \ldots, L_{r-1}$ ($r \leqslant t$) риманова поверхность остаётся связной, а прорез $L_r$ нарушает её связность. Тогда берега прореза $L_r$ должны принадлежать различным кускам. Итак разрезы $L_1, L_2, \ldots, L_t$ не нарушают связности поверхности. Так каждый из кусков, на которые разбивается поверхность после проведения дальнейших прорезов $L_{t+1}, \ldots, L_s$, должен иметь в качестве границ некоторые из берегов прорезов $L_{t+1}, \ldots, L_s$, что противоречит предположению. Итак, прорезы

$$L_1, L_2, \ldots, L_{s-1}$$

не нарушают связности римановой поверхности, откуда в силу теоремы 84 следует

$$s - 1 \leqslant \rho,$$

и таким образом:

Теорема 85 (Гарнака). *Неприводимая алгебраическая кривая жанра $\rho$ не может состоять более чем из $\rho + 1$ связных ветвей, не пересекающих друг друга.*

*Примечание.* При доказательстве мы считали связной ветвью кривой совокупность точек, которая отображается на римановой поверхности в виде связной кривой. Если эта кривая не проходит через точки, в которых переменные $x$, $y$ принимают бесконечные значения, то она действительно изображается на плоскости в виде связной вещественной кривой. В противном случае она может состоять из нескольких ветвей. Простейшим примером может служить гипербола, уравнение которой

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

имеет жанр $\rho = 0$ и которая состоит из двух ветвей. На римановой поверхности обе эти ветви сливаются в одну.

Теорема 85 оправдывает название *уникурсальных* для кривых жанра $\rho = 0$, поскольку они состоят из одной ветви.

Граница, данная в теореме 85, для числа связных ветвей является точной. Для доказательства рассмотрим гиперэллиптическую кривую

$$y^2 - (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_{2p+2}) = 0 \tag{3}$$

жанра $p$, где предположим $\alpha_1, \alpha_2, \dots, \alpha_{2p+2}$ вещественными. Пусть

$$\alpha_1 < \alpha_2 < \dots < \alpha_{2p+1} < \alpha_{2p+2}.$$

Тогда вещественным значениям $x$ соответствуют вещественные значения $y$ тогда и только тогда, если значения $x$ лежат в одном из следующих интервалов:

$$(-\infty, \alpha_1), (\alpha_2, \alpha_3), (\alpha_4, \alpha_5), \dots, (\alpha_{2p}, \alpha_{2p+1}), (\alpha_{2p+2}, +\infty).$$

Каждому из этих интервалов соответствует одна связная вещественная ветвь кривой (3). При этом первая и последняя ветви на римановой поверхности сливаются в одну связную кривую.

Гильберт (D. Hilbert) и И. Г. Петровский получили дополнительные результаты относительно вещественных ветвей кривой жанра $p$.

Представляет большой интерес получение теоремы Гарнака чисто алгебраическим путём, без помощи римановых поверхностей или геометрических соображений. Насколько мне известно, это до сих пор не было сделано.

## Упражнении к главе VII

1. Построить римановы поверхности для эллиптического поля и для гиперэллиптического поля жанра $p = 2$, производя прорезы между парами критических точек (следовательно, не соединяя критические точки с обыкновенными точками). Определить порядки связности полученных поверхностей.

*Указание.* Можно изобразить двулистную поверхность на обыкновенной плоскости, если условиться проводить линии на верхнем и соответственно нижнем листе различными чертами (например сплошной линией и пунктиром). При переходе линий через места склейки листов надо менять пунктир на сплошную линию и обратно.

2. Провести в построенных римановых поверхностях системы канонических сечений.

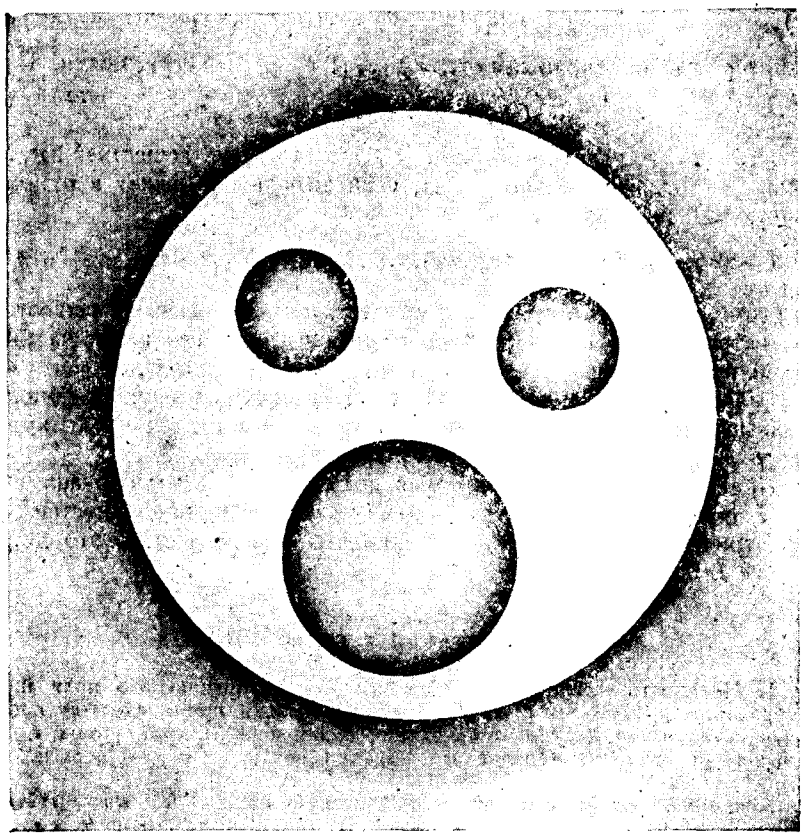
3. В поверхности тора провести прокол и два разреза так, чтобы поверхность после разгиба превратилась в прямоугольник.

4. Показать, что плоский кусок поверхности с $p$-границами (одной внешней и остальными внутренними; черт. 17) имеет порядок связности $p$.

5. Показать, что поверхность, ограничивающая шар с $p$-ручками, имеет порядок связности $2p$.

6. *Лист Мёбиуса* (Möbius). Вырежем из бумаги прямоугольник $ABCD$ с длинными сторонами $AB$, $CD$ и короткими $BC$, $DA$ и склеим стороны $BC$ и $DA$ так, чтобы точка $A$ совпала с $C$, а $B$ — с $D$. Доказать, что полученная поверхность не ориентируема (с одной стороны — триангуляцией; с другой стороны — путём попытки выкрасить обе стороны поверхности в разные цвета). Во что превратится поверхность, если провести на ней прорез параллельно длинным сторонам?

7. *Проективная плоскость.* Если в обыкновенной плоскости отождествить бесконечно удалённые точки на обоих концах каждой прямой и на



Черт. 17.

параллельных прямых, то получится так называемая *проективная* плоскость. Разбив её на 4 треугольника, показать, что она неориентируема.

8. Доказать, что всякая риманова поверхность ориентируема.

# ГЛАВА VIII

# АБЕЛЕВЫ ИНТЕГРАЛЫ

## § 45. Классификация абелевых интегралов

Пусть поле $k(z, w)$ задано соотношением

$$f(z, w) = 0. \tag{1}$$

Всякий интеграл вида

$$\int \varphi(z, w)\, dz, \tag{2}$$

где $\varphi(z, w)$ — рациональная функция, называется *абелевым интегралом*. Абелевы интегралы задаются как криволинейные интегралы от аналитических функций комплексной переменной спрямляемыми кривыми, проведёнными на римановой поверхности, вдоль которых должно быть произведено интегрирование. Задание верхнего и нижнего пределов интегрирования не вполне определяет значение абелева интеграла. Как мы увидим ниже, изменение пути интегрирования придаёт к значению абелева интеграла целочисленные кратности некоторых постоянных, называемых *периодами абелевых интегралов*.

В основу теории абелевых интегралов положена следующая классификация:

1) *Интегралом 1-го рода* называется абелев интеграл, остающийся конечным при всевозможных значениях верхнего предела интегрирования, который мы обычно будем считать основным аргументом абелева интеграла, в то время как нижний предел мы будем считать фиксированным. Мы уже убедились (см. § 19), что дифференциалы абелевых интегралов 1-го рода выражаются целыми дивизорами. Далее, мы видели, что всякий интеграл 1-го рода в поле жанра $\rho$ выражается как линейная комбинация от $\rho$ независимых интегралов 1-го рода (см. § 20).

2) *Интегралом 2-го рода* называется абелев интеграл, имеющий, как функция от верхнего предела, только полюсы. Чтобы абелев интеграл был интегралом 2-го рода с полюсами в точках $P_1$, $P_2$, ..., $P_k$, необходимо, чтобы представление соответствующего ему дифференциала через дивизоры содержало в знаменателе только

простые дивизоры $P_1, P_2, \ldots, P_k$, притом каждый не менее чем во второй степени. В самом деле, если

$$\varphi(z, w)\,dz \approx \frac{R}{Q}, \tag{2'}$$

где $Q$ делится точно на $P^\nu$, а $R$ не делится на $P$, то, выбрав в качестве независимой переменной $t$, которая делится точно на $P$ в 1-й степени, мы преобразуем интеграл к виду

$$\int \psi(t, u) \cdot dt,$$

где

$$dt \approx \frac{Z_t}{T^2},$$

причём ни $Z_t$, ни $T^2$ не делятся на $P$. Из (2') следует, что представление

$$\psi(t, u) \approx \frac{R}{Q} \cdot \frac{T^2}{Z_t}$$

тоже содержит в знаменателе $P$ точно в $\nu$-й степени, а $\psi(t, u)$ в окрестности точки $P$ допускает разложение

$$\psi(t, u) = \frac{a_{-\nu}}{t^\nu} + \frac{a_{-\nu+1}}{t^{\nu-1}} + \ldots \tag{3}$$

Отсюда следует, что рассматриваемый интеграл в точке $P$ обращается в бесконечность $(\nu-1)$-го порядка, если $\nu > 1$, и имеет логарифмическую бесконечность, если $\nu = 1$. Таким образом, чтобы интеграл имел полюсы только в точках $P_1, P_2, \ldots, P_k$ и не имел логарифмических бесконечностей, необходимо (но не достаточно), чтобы дивизор $Q$ был произведением степеней простых дивизоров $P_1, P_2, \ldots, P_k$:

$$Q = P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_k^{\alpha_k} \qquad (\alpha_i \geqslant 2).$$

*Элементарным абелевым интегралом 2-го рода* называется интеграл 2-го рода, имеющий полюс только в одной точке $P$ и имеющий вблизи неё главную часть $\frac{1}{(z-a)^{\nu-1}}$. Соответствующий ему дифференциал представляется через дивизоры так:

$$\frac{R}{P^\nu}, \quad \nu \geqslant 2.$$

Докажем, что для каждого $\nu \geqslant 2$ и каждой точки $P$ действительно существует элементарный интеграл 2-го рода. Для этого учтём, что дивизор $R$ лежит в классе $(P^\nu \cdot \mathfrak{W})$, который не специален, а потому в силу теоремы Римана-Роха

$$\text{Изм}\,(P^\nu \cdot \mathfrak{W}) = 2p - 2 + \nu - p + 1 = p - 1 + \nu$$

Отсюда следует, что при $\nu = 1$ измерение класса $(P \cdot \mathfrak{W})$ равно измерению $\mathfrak{W}$, т. е. что этот класс несобственный, а потому интегралов с единственной логарифмической бесконечностью не существует. С другой стороны, при $\nu \geqslant 2$ дивизор $R$ может быть представлен, притом единственным образом, в виде

$$R = c_0 R_0 + c_1 P \cdot R_1 + c_2 P^2 \cdot R_2 + \ldots + c_{\nu-2} \cdot P^{\nu-2} \cdot R_{\nu-2} + P^{\nu} \cdot W,$$

где $R_0, R_1, \ldots, R_{\nu-2}$ — фиксированные не делящиеся на $P$ дивизоры соответственно классов

$$(P^{\nu}\mathfrak{W}), \quad (P^{\nu-1}\mathfrak{W}), \quad \ldots, \quad (P^2 \cdot \mathfrak{W}),$$

а $W$ — некоторый дивизор класса $\mathfrak{W}$. Отсюда

$$\frac{R}{P^{\nu}} = c_0 \frac{R_0}{P^{\nu}} + c_1 \frac{R_1}{P^{\nu-1}} + \ldots + c_{\nu-2} \frac{R_{\nu-2}}{P^2} + W,$$

откуда и следует наше утверждение.

Заметим, что все элементарные интегралы 2-го рода не имеют логарифмических бесконечностей; другими словами, в разложении (3) их подинтегральных функций члены с $\frac{1}{t}$ отсутствуют: $a_{-1} = 0$. Коэффициент $a_{-1}$ носит название *вычета* (résidu) функции $\psi(t, u)$*) в точке $P$. Ясно, что $2\pi i \cdot a_{-1}$ равно интегралу по достаточно малому замкнутому контуру, окружающему точку $P$.

Наше утверждение является простым следствием

**Теорема 86.** *Для всякого абелева интеграла сумма всех вычетов, распространённая на все точки римановой поверхности, равна нулю.*

Доказательство. Прежде всего заметим, что точек, для которых вычет данного абелева интеграла отличен от нуля, всего конечное число, так что рассматриваемая сумма конечна. Выразим каждый вычет, в силу только что сказанного, через интеграл, причём сгруппируем точки так, чтобы в каждой группе находилось $n$ точек, лежащих одна над другой на $n$ листах римановой поверхности, которым соответствует одна и та же точка следовой сферы. При этом и окружающие эти точки контуры выберем так, чтобы они соответствовали одному и тому же контуру, окружающему точку следовой сферы.

Чтобы исключить возможность того, что точки с неравными нулю вычетами будут критическими, выберем независимую переменную $t$ так, чтобы для неё они не были критическими. При этом вычет интеграла не изменяется, что следует из его выражения через интеграл.

---

*) В дальнейшем будем считать $a_{-1}$ вычетом *интеграла* $\int \psi(t, u)\, dt$, так как при замене переменных $\psi(t, u)$ интеграл остаётся неизменным.

Сумма вычетов, соответствующих каждой группе точек, выразится так:

$$\int \{\psi(t, u_1) + \psi(t, u_2) + \ldots + \psi(t, u_n)\}\, dt,$$

где $u_1, u_2, \ldots, u_n$ — значения функции $u$ в лежащих друг под другом точках римановой поверхности. Подинтегральная функция равна следу от функции $\psi(t, u)$,

$$S\{\psi(t, u)\},$$

т. е. рациональной функции $R(t)$ от $t$ одной и той же для всех групп точек. Таким образом теорема будет доказана, если её доказать для рациональных функций.

Пусть $R(t)$ имеет полюсы в точках $a_1, a_2, \ldots, a_k$, так что её можно разложить на частные дроби следующим образом:

$$R(t) = H(t) + \sum_{\nu=1}^{k} \left\{ \frac{A_{k_\nu}^{(\nu)}}{(t-a_\nu)^{k_\nu}} + \ldots + \frac{A_1^{(\nu)}}{t-a_\nu} \right\},$$

где $H(t)$ — полином. Вычет в каждой точке $t = a_\nu$ равен $A_1^{(\nu)}$, так что сумма всех вычетов, распространённая на все конечные точки, равна

$$\sum_{\nu=1}^{k} A_1^{(\nu)}. \tag{4}$$

Чтобы получить вычет для точки $t = \infty$, сделаем преобразование $t = \frac{1}{u}$, $dt = -\frac{du}{u^2}$, в силу чего нам придётся найти вычет от функции

$$-R\left(\frac{1}{u}\right)\cdot\frac{1}{u^2} = \tag{5}$$

$$= -H\left(\frac{1}{u}\right)\cdot\frac{1}{u^2} - \sum_{\nu=1}^{k} \left\{ \frac{A_{k_\nu}^{(\nu)} u^{k_\nu - 2}}{(1-a_\nu u)^{k_\nu}} + \ldots + \frac{A_1^{(\nu)}}{u(1-a_\nu u)} \right\}$$

для $u = 0$. Найдём вычет от каждого слагаемого правой части. Первое слагаемое не содержит члена с $\frac{1}{u}$, а потому вычет от него равен нулю. Слагаемое

$$\frac{A_\mu^{(\nu)} u^{\mu-2}}{(1-a_\nu u)^\mu}$$

при $\mu \geqslant 2$ не обращается в бесконечность в точке $u = 0$, а потому вычет от него равен нулю (случай $a_\nu = 0$ не исключается). Наконец слагаемое

$$-\frac{A_1^{(\nu)}}{u(1-a_\nu u)}$$

имеет в точке $u=0$ вычет $-A_1^{(\nu)}$, так как его произведение на $u$ принимает в точке $u=0$ значение $-A_1^{(\nu)}$. Таким образом вычет функции (5) в точке $u=0$ равен

$$-\sum_{\nu=1}^{k} A_1^{(\nu)}.$$

Складывая его с выражением (4), мы получаем нуль, ч. т. д.

Таким образом интеграл, обращающийся в бесконечность только в одной точке, не имеет в ней логарифмической бесконечности и потому является абелевым интегралом 2-го рода.

3) *Интегралом 3-го рода* называется абелев интеграл, имеющий и логарифмические особенности. Мы уже убедились, что не существует абелевых интегралов 3-го рода с одной единственной особой точкой. Поэтому *элементарным интегралом 3-го рода* мы должны считать интеграл, имеющий логарифмические бесконечности в двух заданных точках $P_1$ и $P_2$. Соответствующий ему дифференциал содержит в знаменателе произведение $P_1 \cdot P_2$. Из того, что

$$\text{Изм } (P_1P_2 \cdot \mathfrak{W}) = p+1,$$

следует, что элементарный интеграл 3-го рода существует при произвольно заданных точках $P_1$ и $P_2$. В силу теоремы 86 вычеты этого интеграла, соответствующие точкам $P_1$ и $P_2$, имеют противоположные значения.

Имеет место

Теорема 87. *Всякий абелев интеграл линейно выражается через элементарные интеграла 2-го и 3-го рода, а также интегралы 1-го рода.*

Доказательство. Пусть дифференциал заданного абелева интеграла выражается через дивизоры так:

$$\varphi(z, w) \cdot dz = \frac{U}{V},$$

где $V$ пусть точно делится на $P^m$:

$$V = P^m \cdot V_1,$$

где $P$ — простой дивизор и $V_1$ не делится на $P$.

Обозначим через $\mathfrak{A} = (V \cdot \mathfrak{W})$ класс, в котором лежит дивизор $U$. Найдём в классе $\mathfrak{A}$ дивизоры, делящиеся на $V_1$. Они непременно существуют, если

$$t = \text{Пор } V > 1.$$

В самом деле,

$$\text{Пор } \mathfrak{A} = \text{Пор } V + \text{Пор } \mathfrak{W} = t + 2p - 2,$$
$$\text{Изм } \mathfrak{A} = \text{Пор } \mathfrak{A} - p + 1 = t + p - 1,$$

в то время как измерение класса $\left(\frac{\mathfrak{A}}{V_1}\right) = (P^m \cdot \mathfrak{B})$, который тоже не специален, равно $m + \rho - 1$.

Класс $\left(\frac{\mathfrak{A}}{V_1}\right)$ не может быть при $m > 1$ несобственным, так как, закрепив в нём один простой дивизор, мы получим опять неспециальный класс, у которого и порядок и измерение будут меньше на единицу.

Пусть $T_1$ — какой-нибудь дивизор класса $\left(\frac{\mathfrak{A}}{V_1}\right)$, не делящийся на $P$. Представим класс $\mathfrak{A}$ через следующий базис:

$$(6) \qquad (V_1 \cdot T_1,\ V_1 \cdot T_2,\ \ldots,\ V_1 \cdot T_{m-\rho+1},\ \theta_1 \cdot \theta_2,\ \ldots,\ \theta_{t-m}).$$

Нормируем его, добавляя кратности $V_1 T_1$ так, чтобы последние $t - m$ дивизоров делились на $P$. Тогда вид базиса указывает, что каждый дивизор класса $\mathfrak{A}$, и в частности $U$, может быть представлен в виде суммы дивизора, делящегося на $V_1$, и дивизора, делящегося на $P$:

$$U = \lambda \cdot V_1 \cdot T + \mu P \theta,$$

откуда

$$\frac{U}{V} = \lambda \cdot \frac{T}{P^m} + \mu \frac{\theta}{P^{m-1} \cdot V_1}.$$

Таким образом, выделив в дифференциале $\frac{U}{V}$ элементарный дифференциал 2-го рода, мы снизили порядок его знаменателя.

Таким путём мы приведём дифференциал $\frac{U}{V}$ к такому, в знаменателе которого простые дивизоры будут входить в первых степенях. Обозначим его опять через $\frac{U}{V}$, и пусть $V = P \cdot V_1$, где $V_1$ не делится на $P$. Выберем произвольный простой дивизор $P_0$, и пусть $\mathfrak{A}$ будет класс, в котором лежит дивизор $P_0 U$. Поскольку порядок дивизора $\frac{P_0 U}{V_1}$ равен $2p$, его класс должен быть собственным, и мы, применяя к классу $\mathfrak{A}$ предыдущие рассуждения, представим его дивизоры, в частности дивизор $P_0 U$, в виде суммы дивизора, делящегося на $V_1$, и дивизора, делящегося на $PP_0$:

$$P_0 U = \lambda V_1 T + \mu P P_0 \theta,$$

откуда

$$\frac{U}{V} = \lambda \frac{T}{P_0 P} + \mu \frac{\theta}{V_1}.$$

Для этого мы должны найти среди дивизоров базиса (6) один дивизор, $V_1 T_1$, не делящийся на $P_0$, и другой дивизор, $V_1 T_2$, не делящийся на $P$, и нормировать при их помощи последние дивизоры базиса, $\theta_i$, так, чтобы они делились на $PP_0$.

Такой процесс расщепит дифференциал $\frac{U}{V}$ на сумму элементарных дифференциалов 2-го и 3-го рода, причём в знаменателях последних один из простых дивизоров может быть выбран по нашему произволу.

## § 46. Периоды абелевых интегралов

Абелевы интегралы как функции от верхнего предела не могут быть однозначными на всей римановой поверхности. В самом деле, будем называть сопряжёнными с данным абелевым интегралом те интегралы, которые имеют ту же подинтегральную функцию и пути интегрирования которых являются проекциями данного пути интегрирования на другой лист римановой поверхности (мы будем избегать прохождения путей интегрирования через критические точки). Тогда элементарные симметрические функции от сопряжённых интегралов будут однозначными функциями от точки на следовой сфере и, поскольку они не имеют других особенных точек, кроме полюсов, они должны быть рациональными функциями от $z$. Отсюда следует, что данный интеграл является алгебраической функцией от $z$. Таким образом, если какой-нибудь абелев интеграл однозначен на римановой поверхности, то отсюда следует, что его можно проинтегрировать в конечном виде.

В частности, интеграл 1-го рода может быть однозначной функцией от верхнего предела только тогда, когда он равен нулю. В самом деле, все элементарные симметрические функции от сопряжённых с ним интегралов будут тогда функциями $z$, не имеющими вообще никаких особенных точек, и в силу теоремы Лиувилля должны быть константами. Отсюда следует, что и заданный интеграл равен константе. Но поскольку для значения верхнего предела, равного нижнему пределу, его значение равно нулю, он равен нулю тождественно.

С другой стороны, всякий абелев интеграл 1-го или 2-го рода есть однозначная функция от верхнего предела, пробегающего точки римановой поверхности, на которой проведены разрезы канонического сечения. Чтобы доказать это, достаточно убедиться, что абелев интеграл, взятый по замкнутому пути, лежащему внутри рассечённой римановой поверхности, равен нулю. Чтобы убедиться в последнем, учтём, что рассечённая риманова поверхность односвязна и, следовательно, что всякий проведённый по ней замкнутый путь разделяет её на внешнюю и внутреннюю области. Триангулируя последнюю, притом так, чтобы каждый из треугольников лежал только на одном листе, мы применим к каждому из них теорему Коши, которая таким образом будет доказана для всего контура, ч. т. д.

Из этого следует, что абелевы интегралы 1-го и 2-го рода теряют однозначность при переходе через разрезы канонического сечения. Дело обстоит так. Если мы возьмём нижний предел интеграла где-

нибудь на рассечённой римановой поверхности и определим значения интеграла как интеграла вдоль пути, не переходящего через каноническое сечение, то он будет однозначно определён как функция от верхнего предела. Но на разрезах сечения значение интеграла будет зависеть от того, с какой стороны мы будем приближаться к разрезу. Обозначим этот интеграл через

$$V(P) = \int_{P_0}^{P} \varphi(z, w)\, dz. \tag{1}$$

Пусть $\overset{+}{P}_1$, $\overset{-}{P}_1$; $\overset{+}{P}_2$, $\overset{-}{P}_2$ — две пары точек, лежащих друг против друга на разных берегах сечения $A_\nu$ (черт. 18).

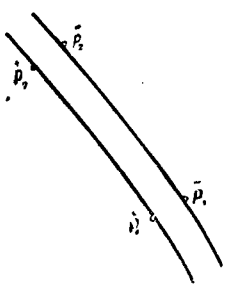
Имеем:

$$V\cdot(\overset{+}{P}_2) - V(\overset{+}{P}_1) = \int_{\overset{+}{P}_1}^{\overset{+}{P}_2} \varphi(z, w)\, dz,$$

$$V\cdot(\overset{-}{P}_2) - V(\overset{-}{P}_1) = \int_{\overset{-}{P}_1}^{\overset{-}{P}_2} \varphi(z, w)\, dz.$$

Поскольку значения функции $\varphi(z, w)$ в соответственных точках разреза на разных берегах совпадают (мы считаем толщину разреза бесконечно малой), интегралы в правых частях обоих равенств равны друг другу, откуда

$$V(\overset{+}{P}_2) - V(\overset{+}{P}_1) = V(\overset{-}{P}_2) - V(\overset{-}{P}_1).$$



Черт. 18.

Из этого равенства следует:

$$V(\overset{+}{P}_1) - V(\overset{-}{P}_1) = V(\overset{+}{P}_2) - V(\overset{-}{P}_2). \tag{2}$$

Это равенство можно формулировать словами так:

При переходе через один из разрезов канонического сечения абелев интеграл получает приращение, величина которого не зависит от того, в какой точке разреза мы совершили переход.

Это приращение абелева интеграла носит название *периода*. Таким образом всякий абелев интеграл имеет $2\rho$ периодов, соответствующих $2\rho$ разрезам

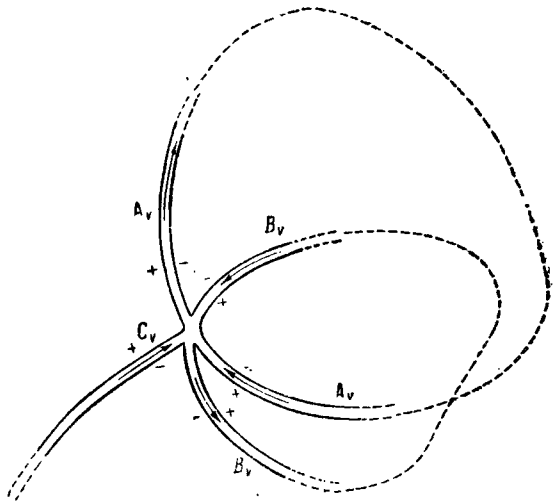
$$A_1, B_1; A_2, B_2; \ldots; A_\rho, B_\rho,$$

из которых состоит каноническое сечение (см. конец § 42).

Чтобы определить соотношение между периодами, необходимо уточнить взаимное расположение разрезов сечения и направлений обхода по ним. Условимся считать *положительным* направлением вдоль каждого берега сечения то, при обходе вдоль которого область остаётся с *левой* стороны. Далее, присвоим каждому разрезу $A_\nu$, $B_\nu$ или $C_\nu$ определённое направление, причём выбор подчиним следующим требованиям, учитывая, что в случае нужды мы имеем право менять ролями разрезы $A_\nu$ и $B_\nu$, имеющие один и тот же номер:

1) Положительным направлением вдоль $C_\nu$ будем считать продвижение от центра звезды вдоль её $\nu$-го луча.

2) При обходе вокруг конца $\nu$-го луча звезды *по* часовой стрелке мы вслед за отрицательным направлением разреза $C_\nu$ будем последовательно встречать: положительное направление $A_\nu$, отрицательное направление $B_\nu$, отрицательное направление $A_\nu$ и, наконец, положительное направление $B_\nu$ (черт. 19).




Черт. 19.

Будем называть *левым берегом* разреза и обозначать значком $+$ сверху тот берег, направление которого *совпадает* с направлением разреза. Тогда положительный обход сечения будет производиться вдоль таких берегов:

$$\overset{+}{C}_\nu,\ \overset{+}{A}_\nu,\ \overset{+}{B}_\nu,\ \overset{-}{A}_\nu,\ \overset{-}{B}_\nu,\ \overset{-}{C}_\nu. \tag{3}$$

3) Лучи звезды нумеруются в порядке обхода вокруг её центра по часовой стрелке.

Тогда положительный обход сечения будет производиться в порядке возрастания номеров разрезов.

Введём для периодов интеграла $w(p)$ следующие обозначения:

$$a_\nu = w(\overset{+}{P})_{A_\nu} - w(\overset{-}{P})_{A_\nu},$$

где индекс $A_\nu$ выражает, что точки $\overset{+}{P}$ и $\overset{-}{P}$ лежат на берегах сечения $A_\nu$.

Точно так же

$$b_\nu = w(\overset{+}{P})_{B_\nu} - w(\overset{-}{P})_{B_\nu},$$

$$c_\nu = w(\overset{+}{P})_{C_\nu} - w(\overset{-}{P})_{C_\nu}.$$

Имеет место

ТЕОРЕМА 88. $c_\nu = 0 \quad (\nu = 1,2,\ldots,\rho)$.

В самом деле, проведём вокруг $\nu$-го конца звезды весьма малую окружность. Совершая по ней обход против часовой стрелки, мы заставим интеграл $w(P)$ претерпеть при переходах через разрезы (начиная с $C_\nu$) следующие приращения:

$$-c_\nu + b_\nu - a_\nu - b_\nu + a_\nu,$$

и вернуться к исходному положению, откуда

$$c_\nu = 0, \tag{4}$$

ч. т. д.

Пусть

$$w(P) = \int_{P_0}^{P} \varphi(r, w)\, dz.$$

Тогда из черт. 19 видно, что

$$\int_{A_\nu} \varphi(z, w)\, dz = w(\overset{+}{P})_{B_\nu} - w(\overset{-}{P})_{B_\nu} = b_\nu, \tag{5}$$

а также

$$\int_{B_\nu} \varphi(z, w)\, dz = w(\overset{-}{P})_{A_\nu} - w(\overset{+}{P})_{A_\nu} = -a_\nu. \tag{6}$$

Между периодами абелевых интегралов существуют соотношения. Для их вывода мы будем применять формулу Коши к контуру, состоящему из всего канонического сечения, причём областью, лежащей внутри этого контура, является вся риманова поверхность.

Пусть

$$w_1(P), \quad w_2(P), \quad \ldots, \quad w_\rho(P) \tag{7}$$

есть система линейно независимых интегралов 1-го рода и пусть

$$w_\nu(P) = u_\nu(P) + iv_\nu(P) \qquad (\nu = 1, 2, \ldots, \rho),$$

где $u_\nu(P)$, $v_\nu(P)$ — гармонические функции, удовлетворяющие уравнениям Коши-Римана

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial u}{\partial x}. \tag{8}$$

Введём для периодов интегралов $w_\nu(P)$ обозначения

$$a_\mu^{(\nu)} = \alpha_\mu^{(\nu)} + i\dot{\alpha}_\mu^{(\nu)}, \quad b_\mu^{(\nu)} = \beta_\mu^{(\nu)} + i\dot{\beta}_\mu^{(\nu)}. \tag{9}$$

I. Выведем для периодов произвольного интеграла 1-го рода $w(P)$ важное неравенство. Для этого в формуле Грина

$$\int (P\,dx + Q\,dy) = \iint \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right) dx\,dy$$

положим

$$P = u\frac{\partial v}{\partial x}, \quad Q = u\frac{\partial v}{\partial y}$$

Тогда, пользуясь уравнениями (8), получим:

$$\int u\,dv = \iint \left\{\left(\frac{\partial u}{\partial x}\right)^2 + \left(\frac{\partial u}{\partial y}\right)^2\right\} dx\,dy.$$

Правая часть положительна; она может быть равна нулю только тогда, когда

$$\frac{\partial u}{\partial x} = 0, \quad \frac{\partial u}{\partial y} = 0$$

всюду на римановой поверхности. Пользуясь (8), мы видим, что в этом случае $w(P) = \text{const}$. Итак:

$$\int u \cdot dv > 0. \tag{10}$$

Разбивая сечение на разрезы, мы приведём это неравенство к виду

$$\sum_{\nu=1}^{p} \left\{ \int_{A_\nu} u(\overset{+}{P})\,dv - \int_{A_\nu} u(\overset{-}{P})\,dv + \int_{B_\nu} u(\overset{+}{P})\,dv - \int_{B_\nu} u(\overset{-}{P})\,dv + \right.$$
$$\left. + \int_{C_\nu} u(\overset{+}{P})\,dv - \int_{C_\nu} u(\overset{-}{P})\,dv \right\} > 0.$$

Объединяя в этом неравенстве 1-й интеграл со 2-м, 3-й с 4-м и 5-й с 6-м и вспоминая определение периодов, а также пользуясь теоремой 88, получим:

$$\sum_{\nu=1}^{p} \left\{ \alpha_\nu \int_{A_\nu} dv + \beta_\nu \int_{B_\nu} dv \right\} > 0.$$

Наконец, пользуясь формулами (5) и (6), будем иметь:

$$\sum_{\nu=1}^{p} (\alpha_\nu \dot{\beta}_\nu - \beta_\nu \dot{\alpha}_\nu) > 0, \tag{11}$$

Это неравенство играет большую роль в теории периодов абелевых интегралов. Прежде всего из него вытекает, что не существует интегралов 1-го рода, для которых все периоды $a_\mu$ обращались бы в нуль или для которых все периоды $b_\mu$ обращались бы в нуль. Полагая

$$w(P) = \xi_1 w_1(P) + \xi_2 w_2(P) + \ldots + \xi_\rho w_\rho(P), \tag{12}$$

где $\xi_1, \xi_2, \ldots, \xi_\rho$ — произвольные константы, мы в силу

$$\begin{aligned} a_\mu &= \xi_1 a_\mu^{(1)} + \xi_2 a_\mu^{(2)} + \ldots + \xi_\rho a_\mu^{(\rho)}, \\ b_\mu &= \xi_1 b_\mu^{(1)} + \xi_2 b_\mu^{(2)} + \ldots + \xi_\rho b_\mu^{(\rho)} \end{aligned} \tag{13}$$

убеждаемся в несуществовании решений системы линейных уравнений

$$a_\mu^{(1)}\xi_1 + a_\mu^{(2)}\xi_2 + \ldots + a_\mu^{(\rho)}\xi_\rho = 0$$

относительно $\xi_1, \xi_2, \ldots, \xi_\rho$. Другими словами,

$$\begin{vmatrix} a_1^{(1)}, & a_1^{(2)}, & \ldots, & a_1^{(\rho)} \\ a_2^{(1)}, & a_2^{(2)}, & \ldots, & a_2^{(\rho)} \\ \ldots & \ldots & \ldots & \ldots \\ a_\rho^{(1)}, & a_\rho^{(2)}, & \ldots, & a_\rho^{(\rho)} \end{vmatrix} \neq 0.$$

Решая каждую из неоднородных систем

$$a_\mu^{(1)}\xi_1^{(\nu)} + a_\mu^{(2)}\xi_2^{(\nu)} + \ldots + a_\mu^{(\rho)} \cdot \xi_\rho^{(\nu)} = \delta_\mu^{(\nu)} \qquad (\mu = 1, 2, \ldots, \nu),$$

где $\delta_\mu^\nu$ — символ Кронекера, так что

$$\delta_\mu^{(\nu)} = 0 \quad (\mu \neq \nu), \qquad \delta_\nu^{(\nu)} = 1,$$

и обозначая интегралы

$$\xi_1^{(\nu)} w_1(P) + \xi_2^{(\nu)} w_2(P) + \ldots + \xi_\rho^{(\nu)} w_\rho(P) \qquad (\nu = 1, 2, \ldots, \rho)$$

опять через $w_1(P)$, $w_2(P)$, $\ldots$, $w_\rho(P)$, мы приходим к системе *нормированных интегралов 1-го рода*, для которых система периодов даётся следующей таблицей:

| | $A_1$ | $A_2 \ldots A_\rho$ | $B_1$ | $B_2 \ldots B_\rho$ |
|---|---|---|---|---|
| $w_1$ | 1 | $0 \ldots 0$ | $\tau_{11}$ | $\tau_{12} \ldots \tau_{1\rho}$ |
| $w_2$ | 0 | $1 \ldots 0$ | $\tau_{21}$ | $\tau_{22} \ldots \tau_{2\rho}$ |
| $\vdots$ | | | | |
| | $\ldots$ | $\ldots \ldots$ | $\ldots$ | $\ldots \ldots$ |
| $w_\rho$ | 0 | $0 \ldots 1$ | $\tau_{\rho 1}$ | $\tau_{\rho 2} \ldots \tau_{\rho\rho}$ |

Из формулы (11) вытекает второе важное следствие.

Беря в качестве системы $w_1(P)$, $w_2(P), \ldots, w_\rho(P)$ систему нормированных интегралов 1-го рода, вводя обозначения

$$\tau_{\mu\nu} = \sigma_{\mu\nu} + i\dot{\sigma}_{\mu\nu}$$

и задавая интеграл $w(P)$ формулой (12), где под $\xi_1, \xi_2, \ldots, \xi_\rho$ мы будем разуметь вещественные параметры, так что

$$a_\mu = \alpha_\mu + i\dot{\alpha}_\mu = \sum_{\nu=1}^{\rho} \xi_\nu \delta_\mu^{(\nu)} = \xi_\mu,$$

$$b_\mu = \beta_\mu + i\dot{\beta}_\mu = \sum_{\nu=1}^{\rho} \xi_\nu \tau_{\nu\mu} = \sum_{\nu=1}^{\rho} \xi_\nu (\sigma_{\nu\mu} + i\dot{\sigma}_{\nu\mu}),$$

мы представим неравенство (11) так:

$$\sum_{\mu,\nu=1}^{\rho} \dot{\sigma}_{\nu\mu} \xi_\mu \xi_\nu > 0. \tag{14}$$

В силу произвольности $\xi_\mu$, $\xi_\nu$ отсюда вытекает, что левая часть неравенства (14) представляет собой положительную квадратичную форму. Впрочем, для этого утверждения мы должны ещё доказать, что

$$\dot{\sigma}_{\nu\mu} = \dot{\sigma}_{\mu\nu},$$

чем мы сейчас и займёмся. Неравенство (14) играет большую роль в теории $\vartheta$-функций.

II. Функция $w_\mu(P) \cdot \dfrac{dw_\sigma(P)}{dz}$ регулярна внутри рассечённой римановой поверхности. Применяя к ней теорему Коши, получим

$$\sum_{\nu=1}^{\rho} \left\{ \int_{A_\nu} w_\mu(\overset{+}{P})\, dw_\sigma(P) - \int_{A_\nu} w_\mu(\overset{-}{P})\, dw_\sigma(P) + \right.$$

$$+ \int_{B_\nu} w_\mu(\overset{+}{P})\, dw_\sigma(P) - \int_{B_\nu} w_\mu(\overset{-}{P})\, dw_\sigma(P) +$$

$$\left. + \int_{C_\nu} w_\mu(\overset{+}{P})\, dw_\sigma(P) - \int_{C_\nu} w_\mu(\overset{-}{P})\, dw_\sigma(P) \right\} = 0,$$

т. е.

$$\sum_{\nu=1}^{\rho} \left\{ a_\nu^{(\mu)} \int_{A_\nu} dw_\sigma(P) - b_\nu^{(\mu)} \int_{B_\nu} dw_\sigma(P) \right\} = 0,$$

откуда в силу формул (5) и (6)

$$\sum_{\nu=1}^{\rho}\left(a_\nu^{(\mu)}b_\nu^{(\sigma)}-b_\nu^{(\mu)}a_\nu^{(\sigma)}\right)=0. \tag{15}$$

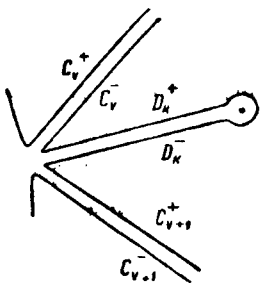
В случае нормированных интегралов формула (15) принимает такой вид:

$$\tau_{\sigma\mu}=\tau_{\mu\sigma}. \tag{16}$$

В частности, левая часть неравенства (14) действительно представляет собой квадратичную форму.

Добавляя ко всякому абелевому интегралу 2-го или 3-го рода надлежащим образом выбранную линейную комбинацию интегралов 1-го рода с постоянными коэффициентами, мы можем нормировать его так, чтобы его периоды вдоль разрезов $A_1, A_2, \ldots, A_\rho$ были равны нулю. Будем в этом случае называть интеграл *нормированным*. В дальнейшем мы будем, главным образом, рассматривать нормированные интегралы.

При определении периодов абелевых интегралов 3-го рода мы встретимся с затруднением, происходящим вследствие того, что эти интегралы имеют логарифмические бесконечности и потому неоднозначны на рассечённой римановой поверхности. Чтобы обойти это затруднение, окружим каждую точку, в которой интеграл имеет логарифмическую бесконечность (см. точку $M_k$ на черт. 20), и соединим её прямолинейным разрезом $D_k$ с центром звезды. После этого интеграл будет однозначен на рассечённой таким образом поверхности и будет дополнительно иметь периоды вдоль линий $D_k$:



Черт. 20.

$$u(\overset{+}{P})-u(\overset{-}{P}),$$

где $\overset{+}{P}$, $\overset{-}{P}$ — точки, лежащие друг против друга на разных берегах разреза $D_k$. Нетрудно убедиться, что такой период равен произведению $2\pi i$ на вычет интеграла в точке $M_k$.

Метод получения соотношений между периодами состоит в следующем. Пусть $X(P)$, $Y(P)$ будут два абелевых интеграла с системами периодов

$$a_1, a_2, \ldots, a_\rho; \quad b_1, b_2, \ldots, b_\rho;$$
$$a_1', a_2', \ldots, a_\rho'; \quad b_1', b_2', \ldots, b_\rho'.$$

Рассмотрим интеграл

$$\int X(P)\,dY(P). \tag{17}$$

Рассуждая, как при получении формулы (15), мы получим для него значение

$$(18)\qquad \sum_{\nu=1}^{p}(a_\nu b'_\nu - a'_\nu b_\nu) + \sum_k 2\pi i \xi_k\,[Y(M_k) - Y(P_0)],$$

где $\xi_k$ представляет собой вычет интеграла $X(P)$ в точке $M_k$. С другой стороны, интеграл (17) равен сумме своих вычетов (во всей рассечённой римановой поверхности), умноженной на $2\pi i$. Будем брать в качестве $X(P)$ и $Y(P)$ элементарные абелевы интегралы всевозможных типов.

III. Пусть

$$(19)\qquad X(P) = t_{P_1}^{(\nu)}(P)$$

есть нормированный элементарный абелев интеграл 2-го рода $\nu$-го порядка, разложение которого для точки имеет главную часть $\frac{1}{(z-a)^\nu}$, а

$$(20)\qquad Y(P) = w_\mu(P) = \int_{P_0}^{P} \varphi_\mu(z, w)\,dz.$$

Интеграл (17) равен $2\pi i$, умноженному на его вычет в точке $a$; последний же равен

$$\frac{1}{(\nu-1)!}\left(\frac{d^{\nu-1}\varphi_\mu(z, w)}{dz^{\nu-1}}\right)_P.$$

Выражение же (18) равно

$$-b_\mu,$$

где $b_\mu$ — период интеграла (19) на разрезе $B_\nu$. Итак,

$$(21)\qquad b_\mu = \frac{2\pi i}{(\nu-1)!}\left(\frac{d^{\nu-1}\varphi_\mu(z, w)}{dz^{\nu-1}}\right)_P.$$

IV. Пусть

$$(22)\qquad Y(P) = \omega_{P_1, P_2}(P)$$

есть нормированный элементарный интеграл 3-го рода с бесконечностями в $P_1$ и $P_2$ и вычетами в них $+1, -1$, а $X(P)$ имеет значение (20). Тогда интеграл (17) равен $2\pi i w_\mu(P_1) - 2\pi i w_\mu(P_2)$, а выражение (18) $-b_\mu$, где $b_\mu$ есть период интеграла (22) на разрезе $B_\nu$. Итак,

$$(23)\qquad b_\mu = 2\pi i w_\mu(P_1) - 2\pi i w_\mu(P_2) = 2\pi i \int_{P_2}^{P_1} dw_\mu(P).$$

V. Пусть

$$X(P) = t_{P_1}(P), \quad Y(P) = t_{P_2}(P)$$

— два нормированных элементарных интеграла 2-го рода с главными частями вида $\frac{1}{z-a}$. Тогда интеграл (17) равен $2\pi i$, умноженному на сумму вычетов этого интеграла в точках $P_1$ и $P_2$. Но вблизи точки $P_1$

$$t_{P_1}(P)=\frac{1}{z-a_1}+\ldots, \quad \frac{dt_{P_3}(P)}{dz}=\frac{dt_{P_3}(P_1)}{dz}+\ldots,$$

так что вычет в точке $P_1$ равен

$$\frac{dt_{P_3}(P_1)}{dz}.$$

Вблизи же точки $P_2$

$$t_{P_1}(t)=t_{P_1}(P_2)+(z-a_2)\frac{dt_{P_1}(P_2)}{dz}+\ldots,$$

$$\frac{dt_{P_3}(P)}{dz}=-\frac{1}{(z-a_2)^2}+\ldots,$$

так что вычет в точке $P_2$ равен

$$-\frac{dt_{P_1}(P_2)}{dz}.$$

С другой стороны, выражение (18) равно нулю, откуда

$$\frac{dt_{P_3}(P_2)}{dz}=\frac{dt_{P_3}(P_1)}{dz} \tag{24}$$

(теорема о перестановке аргумента с параметром для подинтегральных функций интегралов 2-го рода).

VI. Пусть

$$X(P)=t_{P_1}(P), \quad Y(P)=\omega_{P_3P_3}(P).$$

Интеграл (17) имеет вычеты в точках $P_1$, $P_2$ и $P_3$. Вблизи $P_1$

$$t_{P_1}(P)=\frac{1}{z-a_1}+\ldots, \quad \frac{d\omega_{P_3P_3}(P)}{dz}=\frac{d\omega_{P_3P_3}(P_1)}{dz}+\ldots,$$

так что вычет в точке $P_1$ равен

$$\frac{d\omega_{P_3P_3}(P_1)}{dz}.$$

Вблизи $P_2$ и $P_3$ соответственно

$$t_{P_1}(P)=t_{P_1}(P_2)+\ldots, \quad \frac{d\omega_{P_3P_3}(P)}{dz}=\frac{1}{z-a_2}+\ldots,$$

$$t_{P_1}(P)=t_{P_1}(P_3)+\ldots, \quad \frac{d\omega_{P_3P_3}(P)}{dz}=-\frac{1}{z-a_3}+\ldots,$$

так что вычеты в точках $P_2$ и $P_3$ равны

$$t_{P_1}(P_2), \quad -t_{P_1}(P_3).$$

С другой стороны, выражение (18) равно нулю, так что

$$\frac{d\omega_{P_3P_2}(P_1)}{dz} = t_{P_1}(P_3) - t_{P_1}(P_2) = \int_{P_2}^{P_3} dt_{P_1}(P). \tag{25}$$

VII. Пусть

$$X(P) = \omega_{P_1P_2}(P), \quad Y(P) = \omega_{P_3P_4}(P).$$

Сделаем на поверхности дополнительные разрезы $l_1$, $l_2$, $l_3$, $l_4$, соединяющие $P_0$ с $P_1$, $P_2$, $P_3$, $P_4$. Поскольку вычет $X(P)$ в точке $P_1$ есть $+1$, разность его значений в точках левого и правого берегов разреза $l_1$ равна $2\pi i$, а потому

$$\int_{l_1} X\,dY = 2\pi i \int_{P_0}^{P_1} dY = 2\pi i \{\omega_{P_3P_4}(P_1) - \omega_{P_3P_4}(P_0)\}. \tag{26}$$

Точно так же вдоль разреза $l_2$

$$\int_{l_2} X\,dY = -2\pi i \int_{P_0}^{P_2} dY = -2\pi i \{\omega_{P_3P_4}(P_2) - \omega_{P_3P_4}(P_0)\}. \tag{27}$$

Для исследования интеграла вдоль разрезов $l_3$ и $l_4$ возьмём его предварительно по частям:

$$\int_{l_3} X\,dY = \omega_{P_1P_2}(\bar{P}_0)\,\omega_{P_3P_4}(\bar{P}_0) - \omega_{P_1P_2}(\overset{+}{P}_0)\,\omega_{P_3P_4}(\overset{+}{P}_0) - \int_{l_3} Y \cdot dX; \tag{28}$$

$$\int_{l_4} X\,dY = \omega_{P_1P_2}(\bar{P}_0)\,\omega_{P_3P_4}(\bar{P}_0) - \omega_{P_1P_2}(\overset{+}{P}_0)\,\omega_{P_3P_4}(\overset{+}{P}_0) - \int_{l_4} Y \cdot dX. \tag{29}$$

Но в силу

$$\omega_{P_1P_2}(\bar{P}_0) = \omega_{P_1P_2}(\overset{+}{P}_0), \quad \omega_{P_3P_4}(\bar{P}) = \omega_{P_3P_4}(\overset{+}{P}) \pm 2\pi i,$$

где для $l_3$ надо взять один знак, а для $l_4$ другой, члены вне интегралов в (28) и (29) при суммировании взаимно уничтожаются, а интеграл — $\int Y\,dX$ вычисляется подобно (27). Учитывая, что интеграл (17) вдоль рассечённой поверхности равен нулю, мы получим окончательно:

$$\omega_{P_0P_4}(P_1) - \omega_{P_3P_4}(P_2) = \omega_{P_1P_2}(P_3) - \omega_{P_1P_2}(P_4), \tag{30}$$

или

$$\int_{P_1}^{P_2} d\omega_{P_3P_4}(P) = \int_{P_3}^{P_4} d\omega_{P_1P_2}(P) \tag{31}$$

(теорема о перестановке аргумента с параметром для элементарных абелевых интегралов 3-го рода).

Вейерштрасс (K. Weierstrass) получил теоремы о перестановке аргумента с параметром алгебраическим путём, изучая разложения в степенные ряды.

## § 47. Теорема Абеля

Принято считать начало теории алгебраических функций с большого мемуара Абеля, в котором центральное место занимает следующая теорема:

Теорема 89 (Абеля). *Пусть поле* $k(z, w)$ *задано уравнением*

$$f(z, w) = 0. \tag{1}$$

*Сумма интегралов*

$$\int \varphi(z, w)\, dz, \tag{2}$$

*где* $\varphi(z, w)$ *есть рациональная функция, нижние и верхние пределы составляют полные системы точек, в которых какой-нибудь элемент и поля* $k(z, w)$ *принимает одни и те же значения, равна рационально-логарифмической функции от коэффициентов функции* $\varphi(z, w)$.

Доказательство. Не нарушая общности, мы можем принять в качестве $u$ элемент $z$, в случае нужды произведя в интегралах замену переменных. Далее, пусть $z$ принимает в точках нижних и верхних пределов соответственно значения $a$ и $b$. Мы имеем, таким образом, сумму $n$ интегралов, у которых и верхние и нижние пределы лежат на римановой поверхности друг под другом. Если теперь мы, оставляя один из путей интегрирования неизменным, деформируем остальные пути так, чтобы они оказались лежащими на разных листах поверхности друг под другом, то в результате этой деформации каждый из слагаемых интегралов получит приращение, равное сумме целочисленных кратностей периодов интеграла (2). С другой стороны, после этой деформации путей рассматриваемая сумма интегралов может быть представлена так:

$$\int_a^b \left\{ \varphi + (z, w_1) + \varphi(z, w_2) + \ldots + \varphi(z, w_n) \right\} dz,$$

где $w_1, w_2, \ldots, w_n$ — совокупность корней уравнения (1) при одном и том же значении $z$, лежащем на пути интегрирования. Подинтегральная функция представляет собой след функции $\varphi(z, w)$, т. е. является рациональной функцией от $z$, так что интеграл может быть представлен в виде рационально-логарифмической функции от $z$. Подставив вместо $z$ в её выражение верхний предел $b$ и нижний предел $a$, мы получим для рассматриваемой суммы интегралов выражение, требуемое в условии теоремы 89, сложенное с целочисленной линейной комбинацией от периодов интеграла (2). Теорема доказана.

Особый интерес представляет случай, когда интеграл (2) является интегралом 1-го рода. Тогда след

$$S\{\varphi(z, w)\} \tag{3}$$

в силу теорем § 20 есть полином от $z$. Но так как преобразование

$$z = \frac{1}{z_1},$$

которое оставляет дифференциал 1-го рода дифференциалом 1-го рода, переводит $\varphi(z, w)$ в подинтегральную функцию 1-го рода, умноженную на

$$\frac{dz_1}{dz} = -\frac{1}{z^2},$$

то выражение (3) равно полиному от $z_1$, умноженному на $\frac{1}{z^2}$. Оба эти условия совместимы только в случае

$$S\{\varphi(z, w)\} = 0. \tag{4}$$

Здесь оператор $S(\ldots)$ взят относительно элемента $z$ Как мы уже упоминали, если мы заменим $z$ другим элементом, $t$, то подинтегральной функцией в преобразованном интеграле будет функция

$$\varphi(z, w) \cdot \frac{dz}{dt},$$

и таким образом формула (4), написанная относительно переменной $t$, будет иметь вид

$$S_t\left\{\varphi(z, w) \cdot \frac{dz}{dt}\right\} = 0. \tag{5}$$

Формуле (5) можно дать иное истолкование. Пусть $c$ — какое-нибудь совершенно произвольное значение элемента $t$ и пусть это значение принимается в точках

$$P_1, P_2, \ldots, P_m,$$

где $m$ — порядок элемента $t$. Пусть

$$u_1(P), u_2(P), \ldots, u_\rho(P) \tag{6}$$

будет система линейно независимых подинтегральных функций 1-го рода, взятых относительно переменной $z$. Далее, пусть

$$\frac{dz}{dt} = \psi(P).$$

Левая часть равенства (5) для точки $P(z, w)$ есть коэффициент при $u^{m-1}$ с обратным знаком в уравнении, корнем которого является

$$u = \varphi(P) \cdot \psi(P).$$

Если положить в этом уравнении $t = c$, то левая часть (5) обратится в сумму корней этого уравнения, т. е. в сумму значений функции $\varphi(P)$, $\psi(P)$, взятых для точек $P_1, P_2, \ldots, P_m$. Беря в роли $\varphi(P)$ последовательно все функции (6), мы получим из (5) ряд следующих равенств:

$$(7) \quad u_i'(P_1) \cdot \psi(P_1) + u_i'(P_2) \cdot \psi(P_2) + \ldots + u_i'(P_m) \cdot \psi(P_m) = 0 \quad (i = 1, 2, \ldots, \rho).$$

Если рассматривать эти равенства как систему линейных уравнений относительно $\psi(P_\nu)$, то можно утверждать, что эта система имеет отличные от нуля решения. Каковы же требования, налагаемые на точки $P_1, P_2, \ldots, P_m$ для того, чтобы это условие выполнялось? Только существование элемента $t$ поля $k(z, w)$, который бы принимал в этих точках, и только в этих точках, значение $c$. Другими словами, чтобы система (7) имела отличные от нуля решения, необходимо, чтобы измерение класса $\mathfrak{A}$, в котором лежит дивизор

$$(8) \qquad Q = P_1 \cdot P_2 \ldots P_m,$$

было больше единицы. Таким образом мы приходим к следующему аналитическому условию справедливости неравенства

$$\text{Изм } \mathfrak{A} > 1:$$

Теорема 90. *Чтобы класс* $\mathfrak{A}$, *в котором лежит дивизор* (8), *имел измерение больше единицы, необходимо, чтобы ранг матрицы*

$$(9) \qquad \left\| \begin{array}{cccc} u_1'(P_1), & u_1'(P_2), & \ldots, & u_1'(P_m) \\ u_2'(P_1), & u_2'(P_2), & \ldots, & u_2'(P_m) \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ u_\rho'(P_1), & u_\rho'(P_2), & \ldots, & u_\rho'(P_m) \end{array} \right\|,$$

где $u_1', u_2', \ldots, u_\rho'$ — система линейно независимых подинтегральных функций 1-го рода, был меньше $m$.

Это условие является также и достаточным. В самом деле, если ранг матрицы (9) меньше $m$, то матрица (9) имеет менее чем $m$ независимых *строк*. Это означает существование по крайней мере $p - m + 1$ линейно независимых функций типа

$$\lambda_1 u_1'(P) + \lambda_2 u_2'(P) + \ldots + \lambda_p u_p'(P),$$

которые бы обращались в нуль при

$$P = P_1,\ P_2,\ \ldots,\ P_m.$$

Но так как

$$u_i' \approx \frac{W_i X^2}{Z_x},$$

причём общий множитель $\frac{X^2}{Z_x}$ при замене переменных заменяется другим множителем, вообще говоря, взаимно простым с $\frac{X^2}{Z_x}$, то это условие равносильно условию существования $p - m + 1$ линейно независимых дивизоров

$$\lambda_1 W_1 + \lambda_2 W_2 + \ldots + \lambda_p W_p,$$

делящихся на дивизор $P_1 P_2 \ldots P_m$. Другими словами, должно иметь место

$$\text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}} \geqslant p - m + 1.$$

Отсюда в силу теоремы Римана-Роха

$$\text{Изм } \mathfrak{A} = \text{Изм } \frac{\mathfrak{W}}{\mathfrak{A}} + \text{Пор } \mathfrak{A} - p + 1 \geqslant p - m + 1 + m - p + 1 = 2,$$

что требовалось доказать. Таким образом:

Теорема 91. *Чтобы измерение класса* $\mathfrak{A}$ *было* $\geqslant 2$, *необходимо и достаточно, чтобы ранг матрицы* (9), *где* $P_1 \cdot P_2 \ldots P_m$ — *произвольный дивизор класса* $\mathfrak{A}$, *был меньше* $m$.

Заметим, что вывод этой теоремы является чисто алгебраическим, так как опирается не на теорему Абеля в её трансцендентной формулировке, а на её алгебраический эквивалент, выражаемый формулой (4). Вообще, говоря о теореме Абеля, можно оставаться в рамках арифметической теории, если под теоремой Абеля разуметь факт возможности представления элемента

$$S_t\left[\varphi(z, w)\frac{dz}{dt}\right]$$

в виде рациональной функции через элемент $t$.

В дальнейшем нам будет полезна теорема Абеля для интегралов 1-го рода в следующей (трансцендентной) формулировке:

Теорема 92. *Пусть*

$$u_\nu\left(\frac{P'}{P}\right)=\int_P^{P'} du_\nu \quad (\nu=1, 2, \ldots, \rho) \tag{10}$$

*будет система линейно независимых интегралов* 1-*го рода. Чтобы в поле* $k(z, w)$ *существовал элемент, представляемый через дивизоры так*:

$$\frac{P_1'P_2'\ldots P_m'}{P_1P_2\ldots P_m}, \tag{11}$$

*необходимо и достаточно, чтобы имели место сравнения*

$$u_\nu\left(\frac{P_1'}{P_1}\right)+u_\nu\left(\frac{P_2'}{P_2}\right)+\ldots+u_\nu\left(\frac{P_m'}{P_m}\right)\equiv 0 \quad (\nu=1, 2, \ldots, \rho) \tag{12}$$

*по модулю периодов.*

Доказательство. Не нарушая общности, мы можем предположить интегралы $u_\nu\left(\frac{P'}{P}\right)$ нормированными. Рассмотрим выражение

$$e^{\omega_{P_1', P_1}(P)+\omega_{P_2', P_2}(P)+\ldots+\omega_{P_m', P_m}(P)}, \tag{13}$$

где $\omega_{P_\nu', P_\nu}(P)$ — нормированный элементарный интеграл 3-го рода. Выражение (13) однозначно на рассечённой римановой поверхности и имеет на ней простые нули $P_1', P_2', \ldots, P_m'$ и простые полюсы $P_1, P_2, \ldots, P_m$. При переходе через разрезы $A_\nu$ его значение в силу нормировки не меняется, а при переходе через $B_\nu$ оно приобретает множитель

$$e^{2\pi i\left\{u_\nu\left(\frac{P_1'}{P_1}\right)+u_\nu\left(\frac{P_2'}{P_2}\right)+\cdots+u_\nu\left(\frac{P_m'}{P_m}\right)\right\}}$$

[см. § 46, IV, формулу (23)]. Если существует элемент поля $k(z, w)$, представляемый через дивизоры в форме (11), то из формулы (4) после интегрирования вытекает (12). С другой стороны, если имеют место формулы (12), то мы всегда можем изменить пути интегрирования (проведя их так, чтобы они не пересекали разрезов $A_\nu$, $B_\nu$) таким образом, чтобы уравнения (12) превратились в точные равенства. Тогда выражение (13) будет однозначно на нерассечённой римановой поверхности и имеет на ней только полюсы, а потому является функцией поля $k(z, w)$. Вместе с тем она представляется через дивизоры в форме (11), ч. т. д.

## Упражнения к главе VIII

1. Вывести соотношения для периодов интегралов 1-го рода, не предположенных нормированными, и доказать инвариантиость этих соотношений относительно линейных преобразований, производимых над интегралами.

2. Пусть $P_1$, $P_2$ — две произвольные точки римановой поверхности. Если $\omega_{P_1, P_2}(P)$ есть нормированный элементарный интеграл 3-го рода, функция

$$e_{P_1P_2}(P) = e^{\omega_{P_1, P_2}(P)}$$

называется *элементарной функцией*. Она имеет нуль в точке $P_1$ и полюс в точке $P_2$. Можно выразить любую алгебраическую функцию от $z$, $w$ в виде произведения элементарных функций. С другой стороны, произведение элементарных функций есть алгебраическая функция тогда и только тогда, когда оно однозначно на римановой поверхности. Пользуясь этим, доказать теорему Нётера о пробелах.

3. Пользуясь методом предыдущей задачи и теоремой Абеля, доказать теорему Римана-Роха.

ГЛАВА IX

# КЛАССИЧЕСКИЕ ПРОБЛЕМЫ В ТЕОРИИ АЛГЕБРАИЧЕСКИХ ФУНКЦИЙ

В этой главе мы сделаем краткий обзор основных классических проблем, возникших в связи с развитием теории алгебраических функций и частично разрешённых. Эти проблемы были в центре внимания лучших математиков прошлого столетия; в настоящее время ими занимаются мало. Не имея возможности изложить эти проблемы во всех деталях, я буду ссылаться на источники, по которым читатель сможет познакомиться с ними подробно.

## § 48. $\vartheta$-функция

$\vartheta$-функцией от $\rho$ переменных $u_1, u_2, \ldots, u_\rho$ называется целая трансцендентная функция, определяемая при помощи $\rho$-кратного ряда

$$(1)\qquad \vartheta(u_1, u_2, \ldots, u_\rho) = \sum_{m_1, m_2, \ldots, m_\rho = -\infty \ldots +\infty} e^{\pi i \sum_{\mu,\nu}^{1\ldots\rho} a_{\mu\nu} m_\mu m_\nu + 2\pi i \sum_{\mu=1}^{\rho} m_\mu u_\mu},$$

в котором $\frac{\rho(\rho+1)}{2}$ комплексных величин $a_{\mu\nu}$ $(a_{\mu\nu} = a_{\nu\mu})$ являются параметрами $\vartheta$-функции.

Теорема 93. *Если квадратичная форма*

$$(2)\qquad \sum_{\mu,\nu}^{1\ldots\rho} \beta_{\mu\nu}\xi_\mu\xi_\nu,$$

где

$$(3)\qquad a_{\mu\nu} = \alpha_{\mu\nu} + i\beta_{\mu\nu},$$

*— положительно определённая, то ряд* (1) *сходится при всевозможных значениях* $u_\mu$ *и потому представляет целую аналитическую функцию от аргументов* $u_1, u_2, \ldots, u_\rho$.

Доказательство. Достаточно доказать, что ряд (1) сходится абсолютно. Полагая

$$u_\mu = u'_\mu + iu''_\mu,$$

будем иметь

$$\left| e^{\pi i \sum\limits_{\mu,\nu}^{1\ldots\rho} \alpha_{\mu\nu} m_\mu m_\nu + 2\pi i \sum\limits_{\mu=1}^{\rho} m_\mu u_\mu} \right| = e^{-\pi \sum\limits_{\mu,\nu}^{1\ldots\rho} \beta_{\mu\nu} m_\mu m_\nu - 2\pi \sum\limits_{\mu=1}^{\rho} m_\mu u''_\mu},$$

а потому для сходимости ряда (1) достаточно, чтобы сходился ряд

$$\sum_{m_1,\ldots,m_\rho}^{-\infty\ldots+\infty} e^{-\pi \sum\limits_{\mu,\nu}^{1\ldots\rho} \beta_{\mu\nu} m_\mu m_\nu - 2\pi \sum\limits_{\mu=1}^{\rho} m_\mu u''_\mu}. \tag{4}$$

С другой стороны, в силу условия форма (2) не принимает ни отрицательных, ни нулевых значений при отличных от

$$\xi_1 = \xi_2 = \ldots = \xi_\rho = 0$$

вещественных значениях аргументов. Из этого следует, что на ограниченном многообразии

$$\xi_1^2 + \xi_2^2 + \ldots + \xi_\rho^2 = 1 \tag{5}$$

значения формы (2) имеют положительный минимум. Пусть это будет $k > 0$. Тогда на многообразии (5) имеет место

$$\sum_{\mu,\nu}^{1\ldots\rho} \beta_{\mu\nu} \xi_\mu \xi_\nu \leqslant k$$

или

$$\sum_{\mu,\nu}^{1\ldots\rho} \beta_{\mu\nu} \xi_\mu \xi_\nu \leqslant k \sum_{\mu=1}^{\rho} \xi_\mu^2.$$

Последнее неравенство в силу однородности имеет место для всех вещественных значений аргументов. Таким образом ряд (4) сходится, если сходится ряд

$$\sum_{m_1,\ldots,m_\rho}^{-\infty\ldots+\infty} e^{-\pi k \sum\limits_{\mu=1}^{\rho} m_\mu^2 - 2\pi \sum\limits_{\mu=1}^{\rho} m_\mu u''_\mu} = \prod_{\mu=1}^{\rho} \left( \sum_{m=-\infty}^{+\infty} e^{-\pi k m^2 - 2\pi m u''_\mu} \right).$$

Но к каждому из рядов, стоящих под знаком конечного произведения, можно применить известный критерий сходимости Даламбера

$$e^{-\pi k (m+1)^2 - 2\pi (m+1) u''_\mu} : e^{-\pi k m^2 - 2\pi m u''_\mu} = e^{-2\pi k m - \pi k - 2\pi v''_\mu}.$$

Последнее выражение при достаточно большом $m > 0$ меньше единицы, в силу чего часть ряда, соответствующая членам с $m > 0$, сходится. Для части ряда с $m < 0$ произведём подстановку $m = -m'$ и составим аналогичное выражение. Таким образом сходимость ряда (1) доказана.

$\vartheta$-функция обладает свойством $2\rho$-кратной квазипериодичности. Именно, с одной стороны, она не изменяется, если придать к её аргументам произвольные целые числа:

$$(6)\qquad \vartheta(u_1, \ldots, u_\nu + 1, \ldots, u_\rho) = \vartheta(u_1, \ldots, u_\nu, \ldots, u_\rho) \qquad (\nu = 1, 2, \ldots, \rho).$$

С другой стороны, если одновременно придать к её аргументам числа

$$a_{1\sigma}, a_{2\sigma}, \ldots, a_{\rho\sigma} \qquad (\sigma = 1, 2, \ldots, \rho),$$

то из преобразования

$$\sum_{\mu,\nu} a_{\mu\nu} m_\mu m_\nu + 2\sum_\mu m_\mu (u_\mu + a_{\mu\sigma}) =$$
$$= \sum_{\mu,\nu} a_{\mu\nu} (m_\mu + \delta_\mu^\sigma)(m_\nu + \delta_\nu^\sigma) - a_{\sigma\sigma} + 2\sum_\mu (m_\mu + \delta_\mu^\sigma) u_\mu - 2u_\sigma$$

и из того, что $m_\sigma + 1$ пробегает вместе с $m_\sigma$ все значения от $-\infty$ до $+\infty$, мы легко получим:

$$(7)\quad \vartheta(u_1 + a_{1\sigma}, u_2 + a_{2\sigma}, \ldots, u_\rho + a_{\rho\sigma}) = e^{-\pi i a_{\sigma\sigma} - 2\pi i u_\sigma} \vartheta(u_1, u_2, \ldots, u_\rho).$$

Наряду с $\vartheta$-функцией типа (1) рассматриваются *$\vartheta$-функции с характеристиками*. Они получаются из (1), если вместо $m_\mu$ мы будем брать $m_\mu + h_\mu$, а вместо $u_\mu$ брать $u_\mu + g_\mu$, где

$$h_1, h_2, \ldots, h_\rho; \quad g_1, g_2, \ldots, g_\rho$$

— система величин, принимающих значения 0 или $\frac{1}{2}$ и называемых *характеристиками* $\vartheta$-функции:

$$(8)\quad \vartheta\begin{bmatrix} h_1, \ldots, h_\rho \\ g_1, \ldots, g_\rho \end{bmatrix}(u_1, \ldots, u_\rho) = \sum_{m_1, \ldots, m_\rho}^{-\infty \ldots +\infty} e^{\pi i \sum_{\mu,\nu} a_{\mu\nu}(m_\mu + h_\mu) \times} \times (m_\nu + h_\nu) + 2\pi i \sum_\mu (m_\mu + h_\mu)(u_\mu + g_\mu).$$

Для них свойства квазипериодичности выражаются несколько более сложными формулами

$$(9)\quad \vartheta\begin{bmatrix} h \\ g \end{bmatrix}(u_1, \ldots, u_\nu + 1, \ldots, u_\rho) = e^{2h_\nu \pi i} \vartheta\begin{bmatrix} h \\ g \end{bmatrix}(u_1, \ldots, u_\rho),$$

$$(10)\quad \vartheta\begin{bmatrix} h \\ g \end{bmatrix}(u_1 + a_{1\sigma}, \ldots, u_\rho + a_{\rho\sigma}) =$$
$$= e^{-\pi i a_{\sigma\sigma} - 2\pi i u_\sigma - 2g_\sigma \pi i} \vartheta\begin{bmatrix} h \\ g \end{bmatrix}(u_1, \ldots, u_\rho).$$

Полагая в частности все $h_\nu$, $g_\nu$ равными нулю, мы придём к ϑ-функции (1). Всего существует $2^\rho$ различных ϑ-функций типа (7).

Перемножая ϑ-функции типа (7), мы будем получать *ϑ-функции высших порядков*, между которыми имеют место линейные зависимости. Деля две ϑ-функции одного и того же порядка друг на друга, мы в силу (9) и (10) будем получать функции, квадраты которых обладают свойством 2ρ-кратной периодичности. Они играют большую роль в проблеме обращения абелевых интегралов, с которой мы познакомимся ниже.

Теории ϑ-функций посвящена большая монография Крацера (A. Krazer), к которой мы отошлём читателя.

## § 49. Римановы ϑ-функции

Пусть

(1) $$u_1(P),\ u_2(P),\ \ldots,\ u_\rho(P)$$

есть система интегралов 1-го рода, построенная для поля $k(z, w)$ жанра ρ, причём пусть $u_\nu(z)$ имеет вдоль разрезов $A_1, A_2, \ldots, A_\rho$ римановой поверхности периоды

(2) $$0,\ 0,\ \ldots,\ 1,\ \ldots,\ 0 \qquad (1 \text{ на } \nu\text{-м месте}),$$

а вдоль разрезов $B_1, B_2, \ldots, B_\rho$ — периоды

(3) $$a_{1\nu},\ a_{2\nu},\ \ldots,\ a_{\rho\nu}.$$

В силу (16) § 46 имеет место

$$a_{\mu\nu} = a_{\nu\mu},$$

а в силу (14) § 46 мнимая часть квадратичной формы

$$\sum_{\mu,\ \nu} a_{\mu\nu}\xi_\mu\xi_\nu$$

положительна. Эти свойства позволяют построить ϑ-функцию (1), пользуясь периодами $a_{\mu\nu}$ как параметрами (см. § 48).

Если в построенную таким образом ϑ-функцию подставить вместо аргументов $u_1, u_2, \ldots, u_\rho$ интегралы (1), то получится *риманова ϑ-функция*

(4) $$\vartheta(u_\nu(P) - e_\nu)$$

(где $e_1, e_2, \ldots, e_\rho$ — произвольные константы), которая однозначна на рассечённой римановой поверхности, не изменяется при переходе точки $P$ через разрезы $A_\nu$, а при переходе через разрезы $B_\nu$ приобретает множители

(5) $$e^{-\pi i a_{\nu\nu} - 2\pi i u_\nu(P) + 2\pi i e_\nu}$$

[см. (4) § 48]. Подобным же образом можно построить римановы $\vartheta$-функции с характеристиками. Составляя при помощи их римановы функции высших порядков (т. е. перемножая $\vartheta$-функции первого порядка и складывая произведения одинаковых порядков и с одинаковыми суммами характеристик), а затем деля одну на другую две $\vartheta$-функции одинакового порядка и с одинаковой суммой характеристик, мы получим функцию, у которой множители (5), приобретаемые при переходе аргумента через разрезы $B_\nu$, равны единице. Другими словами, мы получим функцию, однозначную на *нерассечённой* римановой поверхности и могущую иметь на ней только полюсы. Применяя к ней рассуждение, приведённое в начале § 46, мы увидим, что построенная нами функция является функцией (элементом) поля $k(z, w)$.

Определим число нулей римановой $\vartheta$-функции на всей римановой поверхности. В силу теории логарифмических вычетов оно равно интегралу

$$\frac{1}{2\pi i}\int d\log\vartheta(u_\mu(P)-e_\mu), \tag{6}$$

распространённому по границе всей римановой поверхности. Таковой является её каноническое сечение. Оно состоит из двойного прохождения вдоль каждого из разрезов $A_\nu$, $B_\nu$: в положительном направлении по правому берегу: $\overset{+}{A}_\nu$, $\overset{+}{B}_\nu$ и в отрицательном по левому: $\overline{A}_\nu$, $\overline{B}_\nu$. Отсюда интеграл (6) равен

$$\sum_{\nu=1}^{p}\frac{1}{2\pi i}\int d\log\vartheta(u_\mu(\overset{+}{P})-e_\mu)-\sum_{\nu=1}^{p}\frac{1}{2\pi i}\int d\log\vartheta(u_\mu(\overline{P})-e_\mu)+$$
$$+\sum_{\nu=1}^{p}\int d\log\vartheta(u_\mu(\overset{+}{P})-e_\mu)-\sum_{\nu=1}^{p}\int d\log\vartheta(u_\mu(\overline{P})-e_\mu)=$$
$$=\sum_{\nu=1}^{p}\frac{1}{2\pi i}\int_{A_\nu} d\log\frac{\vartheta(u_\mu(\overset{+}{P})-e_\mu)}{\vartheta(u_\mu(\overline{P})-e_\mu)}+\sum_{\nu=1}^{p}\int_{B} d\log\frac{\vartheta(u_\mu(\overset{+}{P})-e_\mu)}{\vartheta(u_\mu(\overline{P})-e_\mu)},$$

а это выражение в силу (5) равно:

$$\sum_{\nu=1}^{p}\frac{1}{2\pi i}\int_{B_\nu} d(-\pi i a_{\nu\nu}-2\pi i u_\nu(P)+2\pi i e_\nu)=-\sum_{\nu=1}^{p}\int_{B_\nu} du_\nu(P).$$

Но в силу формулы (6) § 46 каждый интеграл под знаком суммы равен $-a_{\nu\nu}$, т. е. взятому с обратным знаком периоду интеграла $u_\nu(P)$ вдоль разреза $A_\nu$. В силу нормировки интеграла $u_\nu(P)$ $a_{\nu\nu}=1$, откуда следует, что выражение (6) равно $p$, и мы приходим к

Теорема 94. *Римана функция $\vartheta(u_\mu(P)-e_\mu)$ имеет на всей римановой поверхности всего $p$ нулей* (учитывая их кратности).

Обозначим эти нули через $P_1, P_2, \ldots, P_p$. Для проблемы обращения абелевых интегралов фундаментальную роль играют суммы

$$\sigma_i = u_i(P_1) + u_i(P_2) + \ldots + u_i(P_p). \tag{7}$$

Поскольку каждый интеграл $u_i(P)$ определяется с точностью до кратностей периодов, это имеет место также относительно сумм $\sigma_i$.

Из теории вычетов для $\sigma_i$ получается следующее выражение:

$$\sigma_i = \frac{1}{2\pi i}\int u_i(P)\, d\log\vartheta(u_\mu(P) - e_\mu), \tag{8}$$

где интеграл попрежнему распространён на все разрезы $A_\nu$, $B_\nu$ канонического сечения. Подобно предыдущему, будем иметь (см. черт. 19):

$$\sigma_i = \frac{1}{2\pi i}\sum_{\nu=1}^{p}\left\{\int_{A_\nu^{P_\alpha}}^{P_\delta} u_i(\overset{+}{P})\, d\log\vartheta(u_\mu(\overset{+}{P}) - e_\mu) - \right. \tag{9}$$

$$- \int_{P_\beta}^{P_\gamma} u_i(\overline{P})\, d\log\vartheta(u_\mu(\overline{P}) - e_\mu) + \int_{B_\nu^{P_\delta}}^{P_\gamma} u_i(\overset{+}{P})\, d\log\vartheta(u_\mu(\overset{+}{P}) - e_\mu) -$$

$$\left. - \int_{B_\nu^{P_\beta}}^{P_\alpha} u_i(\overline{P})\, d\log\vartheta(u_\mu(\overline{P}) - e_\mu)\right\}.$$

Первые два члена под знаком суммы в силу

$$u_i(\overset{+}{P}) = u_i(\overline{P}) + \delta_{i\nu}$$

дают:

$$\delta_{i\nu}\int_{A_\nu} d\log\vartheta(u_\mu(\overset{+}{P}) - e_\mu) + \int_{A_\nu} u_i(\overline{P})\, d\log\frac{\vartheta(u_\mu(\overset{+}{P}) - e)_\mu}{\vartheta(u_\mu(\overline{P}) - e)_\mu}. \tag{10}$$

Первый из этих интегралов в силу рассуждений, применённых для вывода формулы (5) § 46, равен:

$$(\delta_{i\nu}\log\vartheta(u_\mu(P_\delta) - b_\mu) - \delta_{i\nu}\log\vartheta(u_\mu(P_\alpha) - b_\mu).$$

Поскольку функция $\log w$ при данном $w$ определяется с точностью до кратности $2\pi i$, это выражение в силу формулы (5) равно

$$\delta_{i\nu}(-\pi i a_{\nu\nu} - 2\pi i u_\nu(P_\alpha) + 2\pi i e_\nu + 2\pi i m_\nu), \tag{11}$$

где $m_\nu$ — некоторое целое число.

Второй интеграл выражения (10) в силу периодичности равен нулю. Вторые два члена под знаком суммы в формуле (9) в силу

$$u_i(\overset{+}{P}) = u_i(\overset{-}{P}) + a_{i\nu}$$

дают:

$$(12)\quad a_{i\nu}\int_{B_\nu} d\log\vartheta(u_\mu(\overset{+}{P}) - e_\mu) + \int_{B_\nu} u_i(\overset{-}{P})\cdot d\log\frac{\vartheta(u_\mu(\overset{+}{P}) - e_\mu)}{\vartheta(u_\mu(\overset{-}{P}) - e_\mu)}.$$

Здесь первый из интегралов равен

$$(13)\qquad 2\pi i a_{i\nu} m'_\nu,$$

где $m'_\nu$ — некоторое целое число, а второй в силу рассуждений при выводе (6) § 46 и формулы (5) даёт:

$$(14)\qquad -2\pi i\int_{B_\nu} u_i(\overset{-}{P})\cdot du_\nu(P).$$

Подставляя (11), (13) и (14) в формулу (9), будем иметь:

$$(15)\quad \sum_{\nu=1}^{p} u_i(P_\nu) = e_i - \frac{1}{2}a_{ii} + m_i + \\ + \sum_{\nu=1}^{p} a_{i\nu} m'_\nu - u_i(\overset{+}{P}_{0i}) - \sum_{\nu=1}^{p}\int_{B_\nu} u_i(\overset{-}{P})\,du_\nu(P).$$

Для уничтожения неопределённого члена $u_i(\overset{+}{P}_{0i})$ преобразуем в последней сумме член с $\nu = i$:

$$-\int_{B_\nu} u_i(\overset{-}{P})\,du_i(P) = -\frac{1}{2}\Big\{u_i(P_\beta) - u_i(P_\alpha)\Big\}\Big\{u_i(P_\beta) + u_i(P_\alpha)\Big\}.$$

Первый множитель в фигурных скобках равен $-1$, второй равен $2u_i(P_\alpha)+1$, в силу чего

$$-\int_{B_\nu} u_i(\overset{-}{P})\,du_i(P) = u_i(P_\alpha) + \frac{1}{2}.$$

Но точка $P_\alpha$ есть не что иное, как $\overset{+}{P}_{0i}$ в выражении (15), в силу чего формула (15) перепишется так:

$$\sum_{\nu=1}^{p} u_i(P_\nu) = e_i + \frac{1}{2} - \frac{1}{2}a_{ii} - \sum_{\substack{\nu=1\\ \nu\neq i}}^{p}\int_{B_\nu} u_i(\overset{-}{P})\,du_\nu(P) + m_i + \sum_{\nu=1}^{p} a_{i\nu} m'_\nu.$$

Вводя знак сравнения ($\equiv$) по модулю периодов, а также обозначение

$$k_i = -\frac{1}{2} + \frac{1}{2}a_{ii} + \sum_{\substack{\nu=1 \\ \nu \neq i}}^{\rho} \int_{B_\nu} u_i(P)\, du_\nu(P) \tag{16}$$

(заметим, что величины $k_i$ зависят только от канонического сечения, но не от $e_i$, не от положения нулей $P_1, P_2, \ldots, P_\rho$), мы можем представить полученную формулу в таком виде:

$$\sum_{\nu=1}^{\rho} u_i(P_\nu) \equiv e_i - k_i \qquad (i = 1, 2, \ldots, \rho). \tag{17}$$

Эта формула играет фундаментальную роль в теории обращения абелевых интегралов.

Соотношения (17) получаются в том случае, если константы $e_i$ подобраны так, что функция (4) не обращается тождественно в нуль. Однако существуют значения $e_i$, при которых функция (4) тождественно обращается в нуль. Для доказательства предварительно докажем лемму:

Лемма. *Если*

$$e_i = \sum_{\nu=1}^{\rho} u_i(P_\nu) + k_i \qquad (i = 1, 2, \ldots, \rho),$$

*где* $P_1, P_2, \ldots, P_\rho$ — *произвольная система точек, то функция* (4) *имеет нулями* $P_1, P_2, \ldots, P_\rho$.

Доказательство. Предварительно докажем лемму для случая, когда

$$\text{Изм}\,(P_1 \cdot P_2 \ldots P_\rho) = 1.$$

Пусть функция (4) не обращается тождественно в нуль и пусть $P_1', P_2', \ldots, P_\rho'$ — её нули. Сопоставим заданные выражения для $e_i$ с формулой (17):

$$\sum_{\nu=1}^{\rho} u_i(P_\nu) \equiv \sum_{\nu=1}^{\rho} u_i(P_\nu') \qquad (i = 1, 2, \ldots, \rho),$$

откуда в силу теоремы 92 следует, что дивизоры $P_1P_2 \ldots P_\rho$ и $P_1'P_2' \ldots P_\rho'$ эквивалентны. Но в силу нашего предположения это может иметь место только при совпадении обоих дивизоров, откуда и следует справедливость утверждения.

Пусть теперь

$$\text{Изм}\,(P_1P_2 \ldots P_\rho) > 1.$$

Из теоремы Римана-Роха следует

$$\text{Изм}\,\frac{\mathfrak{W}}{(P_1P_2 \ldots P_\rho)} = \text{Изм}\,(P_1P_2 \ldots P_\rho) - 1,$$

и таким образом наше предположение имеет место тогда и только тогда, когда класс $(P_1P_2 \dots P_\rho)$ специален. Докажем, что точки $P_1, P_2, \dots, P_\rho$ могут сколь угодно мало быть сдвинуты так, чтобы в их новом положении Изм $(P_1'P_2' \dots P_\rho') = 1$. Для этого надо последовательно закреплять в классе $\mathfrak{W}$ простые дивизоры $P_1', P_2', \dots, P_\rho'$ так, чтобы $P_\nu'$ были весьма близки к $P_\nu$ и в то же время ни одна из них не входила в соответственный класс $\frac{\mathfrak{W}}{(P_1'P_2' \dots P_{\nu-1}')}$ $(\nu = 1, 2, \dots, \rho)$.

Вводя обозначение

$$e_i' = \sum_{\nu=1}^{\rho} u_i(P_\nu) + k_i \qquad (i = 1, 2, \dots, \rho),$$

мы в силу доказанного будем иметь:

$$\vartheta(u_i(P_\nu') - e_i') = 0 \qquad (\nu = 1, 2, \dots, \rho).$$

Неограниченно приближая $P_1', P_2', \dots, P_\rho'$ соответственно к $P_1, P_2, \dots, P_\rho$, мы в силу непрерывности левой части в пределе получим

$$\vartheta(u_i(P_\nu) - e_i) = 0 \qquad (\nu = 1, 2, \dots, \rho),$$

ч. т. д.

Теорема 95. *Если класс $(P_1P_2 \dots P_\rho)$ имеет измерение $> 1$, то функция*

$$\vartheta\left(u_\nu(P) - \sum_{\mu=1}^{\rho} u_\nu(P_\mu) - k_\nu\right) \tag{18}$$

*обращается в нуль тождественно относительно $P$.*

Доказательство. В силу леммы функция (4) имеет в качестве нулей $P_1, P_2, \dots, P_\rho$. Пусть класс $(P_1P_2 \dots P_\rho)$ содержит другой дивизор, $P_1', P_2', \dots, P_\rho'$. Тогда в силу теоремы 92

$$\sum_{\mu=1}^{\rho} u_\nu(P_\mu) \equiv \sum_{\mu=1}^{\rho} u_\nu(P_\mu') \qquad (\nu = 1, 2, \dots, \rho),$$

вследствие чего функция (18) только множителем (который притом нигде не обращается в нуль) отличается от функции

$$\vartheta\left(u_\nu(P) - \sum_{\mu=1}^{\rho} u_\nu(P_\mu') - k_\nu\right)$$

и потому имеет нулями также точки $P_1', P_2', \dots, P_\rho'$. Но так как функция (4) или тождественно обращается в нуль, или имеет ровно $\rho$ нулей, то в данном случае она тождественно равна нулю, ч. т. д.

Теорема 95′. *Для любых* $\rho-1$ *точек* $P_1, P_2, \ldots, P_{\rho-1}$ *имеет место*:

$$\vartheta(u_\nu(P_1)+u_\nu(P_2)+\ldots+u_\nu(P_{\rho-1})+k_\nu)=0. \tag{19}$$

Доказательство. Докажем, что систему $P_1, P_2, \ldots, P_{\rho-1}$ можно дополнить точкой $P_\rho$ так, чтобы Изм $(P_1P_2\ldots P_{\rho-1}P_\rho)=1$. Это очевидно, если Изм $(P_1P_2\ldots P_{\rho-1})>1$. Если же Изм $(P_1P_2\ldots P_{\rho-1})=1$, то найдём в классе $\mathfrak{W}$ делящийся на $P_1P_2\ldots P_{\rho-1}$ дивизор

$$W=P_1P_2\ldots P_{\rho-1}\cdot P_1'\cdot P_2'\ldots P_{\rho-1}'.$$

Тогда каждый из классов $(P_1P_2\ldots P_{\rho-1}P_i')$ $(i=1, 2, \ldots, \rho-1)$ специален и потому в силу теоремы Римана-Роха имеет измерение $>1$.

Полагая в доказанном тождестве

$$\vartheta\Big(u_\nu(P)-\sum_{\mu=1}^{\rho}u_\nu(P_\mu)-k_\nu\Big)=0$$

$P=P_\rho=P_i'$ и принимая во внимание, что функция $\vartheta(u_1, u_2, \ldots, u_\rho)$ чётная, мы получим тождество (19). Теоремы 94—95 обратимы:

Теорема 96. (Обратная теореме 95.) *Если*

$$\vartheta(u_\mu(P)-e_\mu) \tag{20}$$

*тождественно относительно* $P$, *то существуют точки* $P_1, P_2, \ldots, P_\rho'$, *для которых*

$$e_\mu\equiv\sum_{\mu=1}^{\rho}u_\mu(P_\nu)+k_\mu \qquad (\mu=1, 2, \ldots, \rho), \tag{21}$$

*причём*

$$\text{Изм}\ (P_1\cdot P_2\ldots P_\rho)>1.$$

Предварительно докажем лемму:

Лемма. *Как бы ни была задана система значений* $d_1, d_2, \ldots, d_\rho$, *можно найти такую систему значений* $c_1, c_2, \ldots, c_\rho$, *чтобы имело место*

$$\vartheta(c)\not\equiv 0, \quad \vartheta(c+d)\not\equiv 0. \tag{22}$$

Доказательство. Аналитическая функция $\vartheta(u)$ не равна нулю тождественно, а потому всегда можно найти систему значений $c_1, c_2, \ldots, c_\rho$, для которой $\vartheta(c)\neq 0$. Далее, в силу непрерывности фуикции $\vartheta(u)$ точку $C(c_1, c_2, \ldots, c_\rho)$ можно окружить окрестностью $G$, для точек которой имеет место $\vartheta(u)\neq 0$.

Рассмотрим функцию $\vartheta(u+d)$, где $u$ заставим пробегать всю окрестность $G$ точки $C$. Если бы всё время имело место $\vartheta(u+d)=0$, то это бы означало, что аналитическая функция обращалась в нуль в целой окрестности и потому должна была бы быть равной нулю

везде, что невозможно. Поэтому в окрестности $G$ существует точка $C'$, для которой $\vartheta(c'+d)\neq 0$ и, как мы видели, $\vartheta(c')\neq 0$, ч. т. д.

Приступим к доказательству теоремы 96. Пусть имеет место (20). Положим

$$d_\mu = -\sum_{\sigma=1}^{\rho-1} u_\mu(P_\sigma) - e_\mu - k_\mu \qquad (\mu = 1, 2, \ldots, \rho), \tag{23}$$

где $P_1, P_2, \ldots, P_\rho$ — система произвольных точек, и подберём значения $c_1, c_2, \ldots, c_\rho$ так, чтобы имело место (22). Функция

$$\vartheta(u(P) - c)$$

не равна нулю тождественно относительно $P$, так как, совмещая $P$ с нижним пределом интегралов $u(P)$, который мы будем считать общим для всех $u_\mu(P)$, мы получим:

$$\vartheta(-c) = \vartheta(c) \neq 0.$$

Поэтому в силу теоремы 93 она будет иметь $\rho$ нулей $P_1', P_2', \ldots, P_\rho'$, для которых будет иметь место соотношение (17):

$$c_\mu \equiv \sum_{\sigma=1}^{\rho} u_\mu(P_\sigma') + k_\mu \qquad (\mu = 1, 2, \ldots, \rho). \tag{24}$$

Складывая (23) и (24), получим:

$$c_\mu + d_\mu \equiv \sum_{\sigma=1}^{\rho} u_\mu(P_\sigma') - \sum_{\sigma=1}^{\rho-1} u_\mu(P_\sigma) - e_\mu \qquad (\mu = 1, 2, \ldots, \rho).$$

Отсюда и из $\vartheta(c+d)\neq 0$ следует, что функция

$$\vartheta\left(\sum_{\sigma=1}^{\rho} u_\mu(P_\sigma') - \sum_{\sigma=1}^{\rho-1} u_\mu(P_\sigma) - e_\mu\right) \tag{25}$$

при переменных $P_\sigma$, $P_\sigma'$ не обращается тождественно в нуль.

Рассмотрим функции

$$\vartheta\left(\sum_{\sigma=0}^{\rho} u_\mu(P_\sigma') - \sum_{\sigma=1}^{s} u_\mu(P_\sigma) - e_\mu\right) \tag{26}$$

от $2s+1$ переменных точек $P'$, $P_1', \ldots, P_s'$; $P_1, \ldots, P_s$, давая $s$ последовательно значения $1, 2, \ldots, \rho-1$. Пусть $s$ будет наименьший значок, при котором (26) не равна тождественно нулю ($s \leqslant \rho-1$), поскольку, полагая $s = \rho-1$, мы получим неравную нулю фуикцию (25). Фиксируем значения $P_1', \ldots, P_s'$; $P_1, \ldots, P_s$, при которых функция (26) не равна нулю тождественно относительно $P'$. Она будет иметь $\rho$ нулей, среди которых будут $P_1, P_2, \ldots, P_s$, так как, полагая

$$P' = P_\nu \qquad (\nu = 1, 2, \ldots, s),$$

мы придём к функции типа (26), но где в роли $s$ будет $s-1$; по предположению, эта функция равна нулю.

Обозначим остальные нули функции (26) через

$$P''_{s+1},\ P''_{s+2},\ \ldots,\ P''_{\rho}.$$

В силу (17) имеет место

$$\sum_{\sigma=1}^{s} u_\mu(P_\sigma)+\sum_{\sigma=s+1}^{\rho} u_\mu(P''_\sigma)\equiv -\sum_{\sigma=1}^{\rho} u_\mu(P'_\sigma)+\sum_{\sigma=1}^{s} u_\mu(P_\sigma)+e_\mu-k_\mu,$$

откуда

$$(27)\qquad e_\mu\equiv\sum_{\sigma=1}^{s} u_\mu(P'_\sigma)+\sum_{\sigma=s+1}^{\rho} u_\mu(P''_\sigma)+k_\mu\qquad(\mu=1,2,\ldots,\rho).$$

Итак, при тождественном обращении в нуль функции $\vartheta(u(P)-e)$ систему значений $e_\mu$ можно представить в форме (27), причём в роли точек $P_1, P_2, \ldots, P_\rho$ можно взять $P'_1, \ldots, P'_s; P''_{s+1}, \ldots, P''_\rho$. Остаётся доказать, что

$$\text{Изм}\ (P'_1\ldots P'_s\cdot P''_{s+1}\ldots P''_\rho)>1.$$

Для этого обратим внимание на то, что точки $P'_1, \ldots, P'_s$ определяются значениями $c_\mu$, которые выбраны нами произвольно, лишь с соблюдением условий (22). Выбирая другую систему значений $c_\mu$ (например, достаточно мало сдвигая старые значения $c_\mu$), мы придём к точкам $\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_s$, которые в силу (24) не могут совпадать с точками $P'_1, P'_2, \ldots, P'_s$, и для них будем иметь

$$(28)\qquad e_\mu\equiv\sum_{\sigma=1}^{s} u_\mu(\overline{P}_\sigma)+\sum_{\sigma=s+1}^{\rho} u_\mu(\overline{P}_\sigma)\qquad(\mu=1,2,\ldots,\rho),$$

где $\overline{P}_{s+1}, \ldots, \overline{P}_\rho$ — аналогично полученная новая система точек. Вычитая (28) из (27) и учитывая, что

$$u_\mu(P')-u_\mu(\overline{P})=\int_{\overline{P}}^{P'} du_\mu(P),$$

будем иметь:

$$\sum_{\sigma=1}^{s}\int_{\overline{P}_\sigma}^{P'_\sigma} du_\mu(P)+\sum_{\sigma=s+1}^{\rho}\int_{\overline{P}_\sigma}^{P''_\sigma} du_\mu(P)\equiv 0\qquad(\mu=1,2,\ldots,\rho).$$

Отсюда в силу теоремы 92 вытекает, что дивизоры $P'_1\ldots P'_s\cdot P''_{s+1}\ldots P''_\rho$ и $\overline{P}_1\ldots\overline{P}_s\cdot\overline{P}_{s+1}\overline{P}_\rho$ эквивалентны. Вместе с тем они могут быть

сделаны различными. В самом деле, для этого достаточно изменить значения $c_\mu$ так, чтобы хоть одно было отлично от сумм каждых $s$ из величин

$$u_\mu(P_1'), \ldots, u_\mu(P_s'); \quad u_\mu(P_{s+1}''), \ldots, u_\mu(P_\rho'').$$

Существование же двух различных эквивалентных дивизоров доказывает, что измерение класса $(P_1' \ldots P_s' P_{s+1}'' \ldots P_\rho')$ больше единицы. Можно было бы доказать, что оно точно равно $s+1$. Теорема доказана.

Теорема 97. (Обратная теореме 95.) *Если для какой-нибудь системы чисел* $e_1, e_2, \ldots, e_\rho$ *имеет место*

$$\vartheta(e) = 0, \tag{29}$$

*то имеет место*:

$$e_\mu \equiv \sum_{\nu=1}^{\rho-1} u_\mu(P_\nu) + k_\mu \qquad (\mu = 1, 2, \ldots, \rho). \tag{30}$$

Доказательство. В силу чётности функции $\vartheta(u)$ из (29) следует:

$$\vartheta(-e) = 0.$$

Это означает, что функция

$$\vartheta(u(P) - e), \tag{31}$$

если она не тождественно обращается в нуль, имеет в качестве одного из своих нулей общий нижний предел $P_0$ интегралов $u_\mu(P)$, для которого, следовательно, $u_\mu(P_0) = 0$. Обозначая остальные нули функции (31) через $P_1, P_2, \ldots, P_{\rho-1}$, мы из формулы (17) получим

$$e_\mu \equiv \sum_{\nu=1}^{\rho-1} u_\mu(P_\nu) + k_\mu,$$

что требовалось доказать.

Если же функция (31) тождественно равна нулю, то в силу теоремы 96 будет иметь место

$$e_\mu \equiv \sum_{\nu=1}^{\rho} u_\mu(P_\nu) + k_\mu \qquad (\mu = 1, 2, \ldots, \rho), \tag{32}$$

причём

$$\text{Изм}\,(P_1 \cdot P_2 \ldots P_\rho) > 1.$$

Выберем в классе $(P_1 \cdot P_2 \ldots P_\rho)$ дивизор $P_1' P_2' \ldots P_{\rho-1}' P_0$, делящийся на $P_0$. В силу $u_\mu(P_0) = 0$ и теоремы 92 будем иметь:

$$\sum_{\nu=1}^{\rho-1} u_\mu(P_\nu') \equiv \sum_{\nu=1}^{\rho} u_\mu(P_\nu).$$

Подставляя в формулу (32), получим

$$e_\mu \equiv \sum_{\nu=1}^{\rho-1} u_\mu(P_\nu') + k_\mu \qquad (\mu = 1, 2, \ldots, \rho), \tag{33}$$

и теорема доказана в самом общем случае.

## § 50. Проблема обращения абелевых интегралов

Если $u(P)$ — эллиптический интеграл 1-го рода, то его обращение однозначно. Это означает, что точка $P$ является однозначной функцией от значения $u$, связанного с $P$ равенством

$$u = u(P).$$

Именно, значения элементов $z$, $w$ поля $k(z, w)$ в точке $P$ являются *эллиптическими функциями* от $u$, одиозначными и двоякопериодическими. Для доказательства однозначности этих функций примем во внимание *теорему монодромии*, состоящую в том, что аналитическая функция однозначна, если она однозначна в окрестности всякой точки плоскости комплексной переменной. Будем исходить из соотношения

$$u = \int_{z_0}^{z} \frac{dz}{\sqrt{(z-\alpha)(z-\beta)(z-\gamma)(z-\delta)}}.$$

В окрестности любого конечного значения $z = z_1$, кроме значений $\alpha$, $\beta$, $\gamma$, $\delta$, правая часть разлагается в ряд по положительным степеням $z - z_1$, причём в силу

$$\left(\frac{du}{dz}\right)_{z=z_1} = \frac{1}{\sqrt{(z_1-\alpha)(z_1-\beta)(z_1-\gamma)(z_1-\delta)}} \neq 0$$

коэффициент при $z - z_1$ в первой степени отличен от нуля. Поэтому, обращая этот ряд, мы получим разложение $z - z_1$ в ряд по целым положительным степеням от $u - u_1$, где $u_1$ — значение $u$ при $z = z_1$, в окрестности одной из точек $\alpha$, $\beta$, $\gamma$, $\delta$, например $\alpha$, $\frac{du}{dz}$ разлагается так:

$$\frac{du}{dz} = a_0(z-\alpha)^{-\frac{1}{2}} + a_1(z-\alpha)^{\frac{1}{2}} + \ldots,$$

откуда

$$u - u_\alpha = 2a_0(z-\alpha)^{\frac{1}{2}} + \frac{2}{3}a_1(z-\alpha)^{\frac{3}{2}} + \ldots$$

Обращая этот ряд, мы получим для $(z-\alpha)$ [и даже для $(z-\alpha)^{\frac{1}{2}}$] ряд по целым положительным степеням от $u - u_\alpha$.

В окрестности $z=\infty$ мы имеем:

$$u=-\int_{z_0}^{z'}\frac{dz'}{\sqrt{(1-\alpha z')(1-\beta z')(1-\gamma z')(1-\delta z')}},\quad z'=\frac{1}{z}.$$

Правая часть разлагается в ряд по целым положительным степеням с неравным нулю коэффициентом при $z'$ в первой степени. Отсюда следует, что $z'$ разлагается в ряд по целым степеням $u-u_\infty$.

Однако это доказательство недостаточно, так как мы не доказали, что при неограниченном изменении переменной $z$ переменная $u$ будет пробегать все комплексные значения. Это может быть выведено из теоремы (96) и формулы (17), в которых мы положим $\rho=1$.

Далее, мы убедимся в однозначной зависимости функции

$$w=\sqrt{(z-\alpha)(z-\beta)(z-\gamma)(z-\delta)}$$

от $u$. Действительно,

$$w=\frac{dz}{du};$$

дифференцируя ряды, полученные для $z$ во всевозможных окрестностях переменной $u$, мы убедимся, что $w$ разлагается тоже в ряды по целым степеням $u-u_1$, каково бы ни было $u_1$. После этого однозначность вытекает из теоремы монодромии.

Этот факт не допускает непосредственного обобщения на интегралы 1-го рода жанра $\rho>1$. В самом деле, при $\rho>1$ дифференциал 1-го рода, как видно из его представления через дивизоры, имеет нули. Если

$$\varphi\ (z,\ w)\ dz\equiv W,$$

то

$$\varphi\ (z,\ w)\equiv\frac{W\cdot N_z^2}{Z_z},$$

где

$$z\equiv\frac{M_z}{N_z}.$$

Пусть простой дивизор $P$ входит в $W$ в $\beta$-й степени, в $Z_z$ в $(\alpha-1)$-й степени, а в $N_z$ вовсе не входит (последнего мы всегда можем добиться заменой переменной). Тогда, если в точке $P$ $z=z_0$, то $P$ входит в $z-z_0$ в $\alpha$-й степени. Отсюда следует, что в $\varphi(z,\ w)$ дивизор $P$ входит в $(\beta-\alpha+1)$-й степени, а потому $\varphi(z,\ w)$ разлагается в ряд по степеням $z-z_0$ так:

$$\varphi(z,w)=a\ (z-z_0)^{\frac{\beta-\alpha+1}{\alpha}}+b\ (z-z_0)^{\frac{\beta-\alpha+1}{\alpha}}+\ldots,$$

где $a=0$. Отсюда

$$u=\int \varphi(z, w)\,dz=$$

$$=u_0+\frac{\alpha}{\beta+1}\cdot a(z-z_0)^{\frac{\beta+1}{\alpha}}+\frac{\alpha}{\beta+2}\cdot b(z-z_0)^{\frac{\beta+2}{\alpha}}+\ldots$$

Заметим, что здесь $\beta>0$, $\alpha\geqslant 1$. Из этого разложения получается такое разложение $z-z_0$ по степеням $u-u_0$:

$$z-z_0=\left(\frac{\beta+1}{\alpha a}\right)^{\frac{\alpha}{\beta+1}}\cdot(u-u_0)^{\frac{\alpha}{\beta+1}}+\ldots$$

Если теперь $w-w_0$ *точно* делится на $P$ в первой степени [такие элементы непременно существуют в поле $k(z, w)$], то имеет место такое разложение:

$$w-w_0=c\cdot(u-u_0)^{\frac{1}{\beta+1}}+\ldots$$

При этом в силу $\beta>0$ число $\frac{1}{\beta+1}$ непременно дробное, в силу чего $w$ не может быть однозначной функцией от $u$.

Якоби (C. G. Jacobi) [58] видоизменил постановку проблемы обращения. Он рассмотрел систему уравнений

$$(1)\qquad e_\mu\equiv u_\mu(P_1)+u_\mu(P_2)+\ldots+u_\mu(P_\rho)\qquad(\mu=1, 2, \ldots, \rho),$$

в которых считал $P_1, P_2, \ldots, P_\rho$ функциями от $e_1, e_2, \ldots, e_\rho$. Оказалось, что заданием значений $e_1, e_2, \ldots, e_\rho$ точки $P_1, P_2, \ldots, P_\rho$ почти всюду определяются однозначно. Именно, определяются однозначно тогда и только тогда, если функция

$$(2)\qquad \vartheta(u(P)-e-k)$$

не обращается в нуль тождественно относительно $P$. В самом деле, из формулы (17) § 49 следует, что системе (1) можно удовлетворить, полагая в качестве $P_1, P_2, \ldots, P_\rho$ нули функции (2). Это решение единственное. В самом деле, если бы, наряду с (1), имело место

$$e_\mu\equiv u_\mu(P_1')+u_\mu(P_2')+\ldots+u_\mu(P_\rho')\qquad(\mu=1, 2, \ldots, \rho),$$

то из теоремы 92 мы бы заключили, что дивизоры $P_1P_2\ldots P_\rho$ и $P_1'\cdot P_2'\ldots P_\rho'$ эквивалентны, откуда в силу теоремы 94 следовало бы, что функция (2) тождественно равна нулю.

Если функция (2) обращается в нуль тождественно относительно $P$, то, применяя теорему 96 к значениям $e_\mu+k_\mu$ в роли $e_\mu$, мы убедимся, что системе (1) тоже можно удовлетворить, хотя и не однозначно. Отсюда следует, что всю совокупность точек $P_1, P_2, \ldots, P_\rho$ можно считать однозначно зависящей от значений $e_1, e_2, \ldots, e_\rho$. Чтобы

убедиться в этом, рассмотрим $2\rho$-мерное пространство, в котором декартовыми координатами будут служить вещественные и мнимые части величин $e_\mu$ ($\mu = 1, 2, \ldots, \rho$). Каждой системе значений $e_1, e_2, \ldots, e_\rho$ будет соответствовать точка этого пространства, и обратно. При этом каждой точке пространства соответствует одна и только одна система точек $P_1, P_2, \ldots, P_\rho$. Исключение представляют только те точки пространства, которым соответствуют системы точек такого рода, что

$$\text{Изм}\,(P_1 \cdot P_2 \ldots P_\rho) > 1.$$

Тогда каждому дивизору класса $(P_1 \cdot P_2 \ldots P_\rho)$ будет соответствовать одна и та же система значений $e_1, e_2, \ldots, e_\rho$. Если мы выберем в этом классе дивизор $P_1' \cdot P_2' \ldots P_{\rho-1}' \cdot P_0$ так, чтобы он делился на дивизор $P_0$, где $P_0$ — общая нижняя граница интегралов $u_\mu(P)$, то получим для значений $e_1, e_2, \ldots, e_\rho$ представление

$$e_\mu \equiv k_\mu + u_\mu(P_1') + u_\mu(P_2') + \ldots + u_\mu(P_{\rho-1}') \qquad (\mu = 1, 2, \ldots, \rho).$$

Если мы теперь заставим $P_1', P_2', \ldots, P_{\rho-1}'$ пробегать всевозможные значения на римановой поверхности, то координаты $e_1, e_2, \ldots, e_\rho$ исключительных точек опишут в $2\rho$-мерном пространстве многообразие измерения $\leqslant 2\rho - 2$. Исключив точки этого многообразия из нашего пространства, мы придём, как нетрудно понять, к пространству, которое останется *связным*. Это означает, что две любые точки пространства можно соединить непрерывной линией, не проходящей через исключительное многообразие. Системы точек $P_1, P_2, \ldots, P_\rho$ являются однозначными непрерывными функциями точек пространства.

Чтобы найти для этих функций аналитические выражения, произвольно выберем в поле $k(z, w)$ элемент

$$z = z(P).$$

Из доказанного следует, что заданием значений $e_1, e_2, \ldots, e_\rho$ однозначно определяется совокупность значений

$$z(P_1),\ z(P_2),\ \ldots,\ z(P_\rho). \tag{3}$$

Отсюда вытекает, что симметрические функции от величин (3) являются однозначными аналитическими функциями $\rho$ аргументов $e_1, e_2, \ldots, e_\rho$. Такие функции носят название *абелевых функций*. Нахождение для них аналитических выражений и составляет проблему обращения абелевых интегралов *в расширенном смысле*. Оказывается, что абелевы функции допускают представление в виде частных от $\vartheta$-функций от аргументов $e_1, e_2, \ldots, e_\rho$. Исключительным точкам соответствуют значения аргументов, обращающие в нуль и числитель, и знаменатель этих выражений.

Для решения проблемы обращения Риман (B. Riemann) [89] наметил два различных пути. Первый из них состоит в выражении

через $\vartheta$-функции элементов поля $k(z, w)$, имеющих нулями 2-го порядка заданные точки $P_1, P_2, \ldots, P_\rho$ римановой поверхности. Второй, разработанный Клебшем и Горданом [30], основан на представлении элементов поля при помощи интегралов 3-го рода.

Остановимся на описании первого из этих методов. Предварительно остановимся более подробно на введённых нами в § 48 $\vartheta$-функциях с характеристиками. Вводя обозначения

$$h_\mu = \frac{\varepsilon_\mu}{2}, \quad g_\mu = \frac{\varepsilon'_\mu}{2} \qquad (\mu = 1, 2, \ldots, \rho), \tag{4}$$

где, следовательно, $\varepsilon_\mu$ и $\varepsilon'_\mu$ могут принимать значения 0 и 1, мы представим $\vartheta$-функцию в виде следующего ряда:

$$\vartheta\begin{bmatrix}\varepsilon\\ \varepsilon'\end{bmatrix}(u) = \vartheta_\varepsilon(u) = \tag{5}$$

$$= \sum_{m_1, \ldots, m_\rho}^{-\infty \ldots +\infty} e^{\sum_{\mu=1}^{\rho}\sum_{\nu=1}^{\rho} \alpha_{\mu\nu}\left(m_\mu + \frac{\varepsilon_\mu}{2}\right)\left(m_\nu + \frac{\varepsilon_\nu}{2}\right) + 2\pi i \sum_{\mu=1}^{\rho}\left(m_\mu + \frac{\varepsilon_\mu}{2}\right)\left(u_\mu + \frac{\varepsilon'_\mu}{2}\right)}.$$

Из (6) и (7) § 48 вытекает:

$$\vartheta_\varepsilon(u_\mu + \delta_{\mu\sigma}) = (-1)^{\varepsilon_\sigma}\vartheta_\varepsilon(u), \tag{6}$$

$$\vartheta_\varepsilon(u_\mu + a_{\mu\sigma}) = (-1)^{\varepsilon_\sigma} \cdot e^{-\pi i a_{\sigma\sigma} - 2\pi i u_\sigma}\vartheta_\varepsilon(u). \tag{7}$$

Кроме того, непосредственной выкладкой можно убедиться в справедливости следующих формул:

$$\vartheta_\varepsilon(u_\mu) = \vartheta\left(u_\mu + \frac{\varepsilon_\mu}{2} + \sum_{\nu=1}^{\sigma} a_{\mu\nu}\frac{\varepsilon'_\nu}{2}\right) \cdot e^{\sum_{\mu,\nu}^{1 \ldots \rho} a_{\mu_\nu}\frac{\varepsilon_\mu \varepsilon_\nu}{4} + \pi i \sum_{\mu=1}^{\rho} \varepsilon_\mu\left(u_\mu + \frac{\varepsilon'_\mu}{2}\right)}. \tag{8}$$

Из этих формул видно, что $\vartheta_\varepsilon(u_\mu)$ лишь несущественным множителем отличается от $\vartheta(u_\mu)$, у которой к аргументам прибавлена половина периода. Это позволяет нам непосредственно применять к $\vartheta_\varepsilon(U_\mu)$ теорию нулей римановых $\vartheta$-функций, прикладывая к аргументам соответствующие половины периодов.

Далее,

$$\vartheta_\varepsilon(-u_\mu) = (-1)^{\sum_{\mu=1}^{\rho}\varepsilon_\mu\varepsilon'_\mu} \cdot \vartheta_\varepsilon(u_\mu). \tag{9}$$

Из этой формулы следует, что функция $\vartheta_\varepsilon(u_\mu)$ будет чётной или нечётной в зависимости от чётности или нечётности выражения

$$\sum_{\mu=1}^{\rho} \varepsilon_\mu\varepsilon'_\mu. \tag{10}$$

Сообразно с этим, и самые характеристики $\begin{bmatrix}\varepsilon\\ \varepsilon'\end{bmatrix}$ называются чётными или нечётными.

Обозначим через $g_\rho$ и $u_\rho$ число чётных и нечётных характеристик от $\rho$ аргументов и вычислим их величины. Прежде всего

$$g_1 = 3, \quad u_1 = 1,$$

так как из 4 характеристик от одного аргумента

$$\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix} \tag{11}$$

первые три чётные, а четвёртая нечётная.

Возьмём одну из характеристик от $\rho - 1$ аргументов и припишем к ней один из столбцов (11) для образования характеристики от $\rho$ аргументов. Тогда, если она была чётная (нечётная), то, приписав к ней один из первых трёх столбцов (11), мы сделаем её чётной (нечётной); приписав же к ней четвёртый столбец $\begin{bmatrix}1\\1\end{bmatrix}$, мы сделаем её нечётной (чётной). Притом это наиболее общий способ получения всех различных характеристик от $\rho$ аргументов. Отсюда вытекают следующие рекуррентные формулы:

$$g_\rho = 3 \cdot g_{\rho-1} + u_{\rho-1}, \quad u_\rho = g_{\rho-1} + 3u_{\rho-1}. \tag{12}$$

Вычитая эти формулы одну из другой, получим

$$g_\rho - u_\rho = 2(g_{\rho-1} - u_{\rho-1}),$$

откуда в силу $g_1 - u_1 = 2$ будем иметь:

$$g_\rho - u_\rho = 2^\rho.$$

Сопоставляя эту формулу с

$$g_\rho + u_\rho = 2^{2\rho},$$

получим окончательно:

$$g_\rho = 2^{\rho-1}(2^\rho + 1), \quad u_\rho = 2^{\rho-1}(2^\rho - 1). \tag{13}$$

Перейдём к исследованию римановых функций с характеристиками. Возьмём две различные характеристики $\begin{bmatrix}\varepsilon\\ \varepsilon'\end{bmatrix}$ и $\begin{bmatrix}\eta\\ \eta'\end{bmatrix}$ и введём для половин периодов следующие сокращённые обозначения:

$$\frac{\varepsilon_\mu}{2} + \sum_{\nu=1}^{\rho} a_{\mu\nu}\frac{\varepsilon'_\nu}{2} = \frac{1}{2}(\varepsilon\varepsilon')_\mu, \quad \frac{\eta_\mu}{2} + \sum_{\nu=1}^{\rho} a_{\mu\nu}\frac{\eta'_\nu}{2} = \frac{1}{2}(\eta\eta')_\mu.$$

Тогда, если функции

$$\vartheta_\varepsilon(u_\mu(P)), \quad \vartheta_\eta(u_\mu(P)) \tag{14}$$

не обращаются тождественно в нуль, то их нулевые точки $P_1$, $P_2$, ..., $P_\rho$ и $P_1'$, $P_2'$, ..., $P_\rho'$ в силу формулы (8) этого параграфа и формулы (8) § 49 удовлетворяют следующим соотношениям:

$$\sum_{\nu=1}^{\rho} u_\mu(P_\nu) \equiv \frac{1}{2}(\varepsilon\varepsilon')_\mu - k_\mu, \tag{15}$$

$$\sum_{\nu=1}^{\rho} u_\mu(P_\nu') \equiv \frac{1}{2}(\eta\eta')_\mu - k_\mu. \tag{16}$$

Умножая их на 2 и вычитая одно из другого, получим в силу $(\varepsilon\varepsilon_\mu) \equiv 0$

$$2\sum_{\nu=1}^{\rho} u_\mu(P_\nu) \equiv 2\sum_{\nu=1}^{\rho} u_\mu(P_\nu') \qquad (\mu = 1, 2, \ldots, \rho),$$

откуда в силу теоремы 92 следует, что существует элемент поля $k(z, w)$, имеющий (только) $P_1, P_2, \ldots, P_\rho$ двойными нулями и (только) $P_1', P_2', \ldots, P_\rho'$ двойными полюсами. Этот элемент может быть найден чисто алгебраическим путём. Особенно просто это производится в том случае, если обе характеристики $\left[\begin{smallmatrix}\varepsilon\\ \varepsilon'\end{smallmatrix}\right]$ и $\left[\begin{smallmatrix}\eta\\ \eta'\end{smallmatrix}\right]$ нечётные. Тогда, приняв $P = P_0$, где $P_0$ — общий нижний предел интегралов $u_\mu(P)$, будем иметь

$$\vartheta_\varepsilon(u_\mu(P_0)) = \vartheta_\varepsilon(0) = 0, \quad \vartheta_\eta(u_\mu(P_0)) = \vartheta_\eta(0) = 0,$$

откуда следует, что в каждую из систем $P_1, \ldots, P_\rho$ и $P_1', \ldots, P_\rho'$ нулей обеих $\vartheta$-функций входит $P_0$. С другой стороны, выбирая произвольно $\rho - 1$ точек $P_1'', P_2'', \ldots, P_{\rho-1}''$ и составляя выражения

$$e_\mu = \sum_{\nu=1}^{\rho-1} u_\mu(P_\nu'') + k_\mu \qquad (\mu = 1, 2, \ldots, \rho),$$

мы в силу теоремы 95 получим $\vartheta(e_\mu) = 0$, откуда $\vartheta(-e_\mu) = 0$. Из последнего равенства в силу теоремы 97 следует существование таких точек $P_\rho'', P_{\rho+1}'', \ldots, P_{2\rho-2}''$, что

$$-e_\mu \equiv \sum_{\nu=\rho}^{2\rho-2} u_\mu(P_\nu'') + k_\mu \qquad (\mu = 1, 2, \ldots, \rho).$$

Отсюда

$$\sum_{\nu=1}^{2\rho-2} u_\mu(P_\nu'') + 2k_\mu \equiv 0 \qquad (\mu = 1, 2, \ldots, \rho). \tag{17}$$

Сопоставляя с (15), мы в силу $(\varepsilon\varepsilon')_\mu \equiv 0$ будем иметь:

$$\sum_{\nu=1}^{2\rho-2} u_\mu(P''_\nu) \equiv 2 \sum_{\nu=1}^{\rho} u_\mu(P_\nu) \quad (\mu = 1, 2, \ldots, \rho).$$

Отсюда в силу теоремы 92 следует эквивалентность дивизоров $P''_1 P''_2 \ldots P''_{2\rho-2}$ и $P_1^2 \cdot P_2^2 \ldots P_{\rho-1}^2$ (если принять, что $P_\rho = P_0$). Но из произвольности выбора точек $P''_1, P''_2, \ldots, P''_{\rho-1}$ в дивизоре $P''_1 \cdot P''_2 \ldots P''_{2\rho-2}$ следует

$$\text{Изм } P_1^2 P_2^2 \ldots P_{\rho-1}^2 = \text{Изм } P''_1 P''_2 \ldots P''_{2\rho-2} \geqslant \rho,$$

откуда в силу теоремы Римана-Роха:

$$\text{Изм } \frac{\mathfrak{W}}{P_1^2 P_2^2 \ldots P_{\rho-1}^2} = \text{Изм } P_1^2 \ldots P_{\rho-1}^2 - \text{Пор } P_1^2 \ldots P_{\rho-1}^2 + \rho - 1 \geqslant \rho - (2\rho - 2) + \rho - 1 = 1,$$

а это неравенство показывает, что класс $(P_1^2 \cdot P_2^2 \ldots P_{\rho-1}^2)$ специальный, т. е. совпадает с классом дифференциалов $\mathfrak{W}$. Таким образом в классе $\mathfrak{W}$ существуют дивизоры, все простые множители которых входят в квадратах. Для практического нахождения таких дивизоров удобно воспользоваться присоединёнными полиномами (см. § 39), т. е. полиномами $\varphi(z, w)$ степени $\leqslant m-2$ относительно $z$ и $\leqslant n-2$ относительно $w$, которые как элементы поля $k(z, w)$ делились бы на дивизор двойных точек $D$. Известно, что существует ровно $\rho$ линейно независимых присоединённых полиномов. Выбирая какую-нибудь систему $\varphi_1, \varphi_2, \ldots, \varphi_\rho$ присоединённых полиномов и полагая

$$\varphi(z, w) = c_1\varphi_1 + c_2\varphi_2 + \ldots + c_\rho\varphi_\rho,$$

где $c_1, c_2, \ldots, c_\rho$ — система пока неопределённых констант, подберём последние так, чтобы наш полином как элемент поля $k(z, w)$ содержал каждый простой дивизор по крайней мере в квадрате. Для этого составим норму от $\varphi(z, w)$:

$$N(c_1\varphi_1 + c_2\varphi_2 + \ldots + c_\rho\varphi_\rho) = \Phi(z) \cdot N(D).$$

Множитель $N(D)$ не зависит от $c_1, c_2, \ldots, c_\rho$, множитель же $\Phi(z)$ будет степени $2\rho - 2$ от $z$, поскольку каждому «переменному» простому множителю элемента $\varphi(z, w)$ соответствует линейный множитель полинома $\Phi(z)$. Для нашего условия необходимо, чтобы $\Phi(z)$ и его производная $\Phi'(z)$ имели общий наибольший делитель степени $\geqslant \rho - 1$. Производя над $\Phi(z)$ и $\Phi'(z)$ алгоритм Эвклида при неопределённых коэффициентах $c_1, c_2, \ldots, c_\rho$, приравняем нулю все коэффициенты в первом из остатков, степень которого $< \rho - 1$. Получится $\rho - 1$ уравнений относительно однородно входящих $\rho$ пере-

менных $c_1, c_2, \ldots, c_\rho$, которые в общем случае будут найдены с точностью до общего множителя. Заметим, что справедливость сравнения (17) не зависит от существования неравных тождественно нулю функций $\vartheta_\varepsilon(u_\mu(P))$ с нечётной характеристикой $[{}^{\varepsilon}_{\varepsilon'}]$. Это сравнение показывает, что выражение

$$\sum_{\nu=1}^{2\rho-2} u_\mu(P''_\nu),$$

где дивизор $P''_1, P''_2, \ldots, P''_{2\rho-2}$ лежит в классе $\mathfrak{W}$, сравнимо с $-2k_\mu$ (очевидно, что для дивизоров, лежащих в одном и том же классе, оно должно быть сравнимо с одной и той же величиной в силу теоремы 92).

Докажем обратное: пусть в классе $\mathfrak{W}$ мы нашли дивизор типа $P_1^2 P_2^2 \ldots P_{\rho-1}^2$. Тогда в силу сделанного замечания

$$\sum_{\nu=1}^{\rho-1} 2 \cdot u_\mu(P_\nu) + 2k_\mu \equiv 0 \qquad (\mu = 1, 2, \ldots, \rho),$$

откуда следует

$$\sum_{\nu=1}^{\rho-1} u_\mu(P_\nu) + k_\mu \equiv \frac{1}{2}(\varepsilon\varepsilon')_\mu \qquad (\mu = 1, 2, \ldots, \rho), \tag{18}$$

где $\frac{1}{2}(\varepsilon\varepsilon')$ — какой-то полупериод. Отсюда в силу формулы (8) и теоремы 95 имеет место

$$\vartheta_\varepsilon(0) = 0. \tag{19}$$

Таким образом, среди нулей функции $\vartheta_\varepsilon(u_\mu(P))$, если она не обращается в нуль тождественно, должен быть $P_0$. Обозначая остальные через $P''_1, P''_2, \ldots, P''_{\rho-1}$, будем иметь:

$$\sum_{\nu=1}^{\rho-1} u_\mu(P''_\nu) + k_\mu \equiv \frac{1}{2}(\varepsilon\varepsilon') \qquad (\mu = 1, 2, \ldots, \rho).$$

Сопоставляя с (18), мы приходим или к совпадению обеих систем $P_1, P_2, \ldots, P_{\rho-1}$ и $P''_1, P''_2, \ldots, P''_{\rho-1}$ или к эквивалентности дивизоров $P_1 P_2 \ldots P_{\rho-1}$ и $P''_1 P''_2 \ldots P''_{\rho-1}$, откуда

$$\text{Изм}\,(P_1 P_2 \ldots P_{\rho-1}) > 1,$$

и таким образом функция $\vartheta_\varepsilon(u_\mu(P))$ в силу теоремы 94 тождественно равна нулю.

Заметим, что при нечётной характеристике $\begin{bmatrix}\varepsilon\\ \varepsilon'\end{bmatrix}$ всегда имеет место (19). Если же характеристика $\begin{bmatrix}\varepsilon\\ \varepsilon'\end{bmatrix}$ чётная, то для некоторых полей $k(z, w)$ частного вида (в частности, гиперэллиптических) (19) также имеет место. Однако в этом случае всегда $\vartheta_\varepsilon(u_\mu(P))$ тождественно обращается в нуль. Это доказал Риман [89]; здесь мы не имеем возможности воспроизвести его доказательства. Вебер [105'] исследовал поля с исчезающими $\vartheta$-функциями для некоторых чётных характеристик.

Пусть $\begin{bmatrix}\varepsilon\\ \varepsilon'\end{bmatrix}$ и $\begin{bmatrix}\eta\\ \eta'\end{bmatrix}$ — две нечётные характеристики, причём пусть функции $\vartheta_\varepsilon(u_\mu(P))$ и $\vartheta_\eta(u_\mu(P))$ не обращаются тождественно в нуль. Частное

$$\vartheta_\varepsilon(u_\mu(P)):\vartheta_\eta(u_\mu(P)) \tag{20}$$

однозначно на рассечённой римановой поверхности, имеет простые нули в точках $P_1, P_2, \ldots, P_{p-1}$ и простые полюсы в точках $P_1', P_2', \ldots, P_{p-1}'$. Далее, из формул (6) и (7) следует, что при переходе через разрез $A$ оно приобретает множитель

$$(-1)^{\varepsilon_\nu-\eta_\nu},$$

а при переходе через разрез $B_\nu$ — множитель

$$(-1)^{\varepsilon_\nu'-\eta_\nu'}.$$

Отсюда следует, что квадрат частного (20) однозначен на нерассечённой римановой поверхности и имеет на ней только полюсы. Следовательно, он равен некоторому элементу поля $k(z, w)$. Нетрудно видеть, что те же нули и полюсы имеет частное

$$\varphi_\varepsilon(z, w):\varphi_\eta(z, w),$$

где $\varphi_\varepsilon$, $\varphi_\eta$ — найденные нами для характеристик $\begin{bmatrix}\varepsilon\\ \varepsilon'\end{bmatrix}$ и $\begin{bmatrix}\eta\\ \eta'\end{bmatrix}$ присоединённые полиномы. Таким образом

$$\frac{\vartheta_\varepsilon(u_\mu(P))}{\vartheta_\eta(u_\mu(P))} = A\cdot\sqrt{\frac{\varphi_\varepsilon(z, w)}{\varphi_\eta(z, w)}}, \tag{21}$$

где $A$ — константа.

Аналогичные рассуждения можно провести и для случая чётных характеристик. Здесь только $\vartheta$-функция не имеет известного нуля, так что для неё приходится подбирать полином $\psi_\varepsilon(z, w)$, имеющий $p$ нулей 2-го порядка. Выбор такого полинома здесь зависит от одного непрерывного параметра — произвольного выбора одной из точек.

Рассмотрим функцию

$$Q(P_1, P_2, \ldots, P_\rho) = \frac{\vartheta_\varepsilon\left(\sum_{\nu=0}^{\rho} u_\mu(P_\mu) - \sum_{\nu=1}^{\rho} u_\mu(\Pi_\nu)\right)}{\vartheta_\eta\left(\sum_{\nu=0}^{\rho} u_\mu(P_\nu) - \sum_{\nu=1}^{\rho} u_\mu(\Pi_\nu)\right)}, \tag{22}$$

где точки $P, P_1, \ldots, P_\rho$ будем считать независимыми переменными. Тогда, если обозначить через $\Pi_1^{(\varepsilon)}, \Pi_2^{(\varepsilon)}, \ldots, \Pi_\rho^{(\varepsilon)}$ и $\Pi_1^{(\eta)}, \Pi_2^{(\eta)}, \ldots, \Pi_\rho^{(\eta)}$ нули функций $\vartheta_\varepsilon(u_\mu(P))$ и $\vartheta_\eta(u_\mu(P))$, то нули $\Pi_1', \Pi_2', \ldots, \Pi_\rho'$ и бесконечности $\Pi_1'', \Pi_2'', \ldots, \Pi_\rho''$ функции (22) от $P$ будут связаны следующими соотношениями:

$$\sum_{\nu=1}^{\rho} [u_\mu(\Pi_\nu') - u_\mu(\Pi_\nu^{(\varepsilon)})] + \sum_{\nu=1}^{\rho} [u_\mu(P_\nu) - u_\mu(\Pi_\nu)] \equiv 0, \tag{23}$$

$$\sum_{\nu=1}^{\rho} [u_\mu(\Pi_\nu'') - u_\mu(\Pi_\nu^{(\eta)})] + \sum_{\nu=1}^{\rho} [u_\mu(P_\nu) - u_\mu(\Pi_\nu)] \equiv 0 \tag{24}$$

$$(\mu = 1, 2, \ldots, \rho),$$

в справедливости которых мы легко убедимся, применяя ко всем системам точек формулу (17) § 49. Как функция от $P$, функция (22), как мы видели, равна квадратному корню из элемента поля $k(z, w)$: Именно, на разрезах $A_\nu$, $B_\nu$ она приобретает множители

$$(-1)^{\varepsilon_\nu - \eta_\nu}, \quad (-1)^{\varepsilon_\nu' - \eta_\nu'}.$$

Точно такие же множители приобретает функция

$$S = \sqrt{\frac{\psi_\varepsilon(z, w)}{\psi_\eta(z, w)}}, \tag{25}$$

так что их частное есть элемент поля $k(z, w)$.

С другой стороны, точки $P, P_1, \ldots, P_\rho$ входят в выражение (22) симметрично. Поэтому, вводя обозначение

$$S_k = \sqrt{\frac{\psi_\varepsilon(z_k, w_k)}{\psi_\eta(z_k, w_k)}}, \qquad (k = 1, 2, \ldots, \rho), \tag{26}$$

где $z_k$, $w_k$ — независимые от $z$, $w$ переменные, связанные тем же соотношением, как $z$, $w$, и определяя функцию $R$ равенством

$$Q = S \cdot S_1 \cdot S_2 \ldots S_\rho \cdot R, \tag{27}$$

мы убедимся, что $R$ есть рациональная функция от пар $z$, $w$; $z_1$, $w_1$; $\ldots$; $z_\rho$, $w_\rho$, которые притом входят в неё симметрично. Как функция от $P$ (т. е. от $z$, $w$) $R$ обращается в нуль в нулях

функции $Q$, т. е. в $\Pi_1', \Pi_2', \ldots, \Pi_\rho'$, и в полюсах функции $S$, т. е. в $\Pi_1^{(\eta)}, \Pi_2^{(\eta)}, \ldots, \Pi_\rho^{(\eta)}$, и имеет полюсы в $\Pi_1'', \Pi_2'', \ldots, \Pi_\rho''$ и в $\Pi_1^{(\varepsilon)}, \Pi_2^{(\varepsilon)}, \Pi_\rho^{(\varepsilon)}$. Системы $\Pi_1', \Pi_2', \ldots, \Pi_\rho'$ и $\Pi_1'', \Pi_2'', \ldots, \Pi_\rho''$ не заданы явно, а косвенно определяются при помощи сравнений (28) и (24). Именно, сравнения (23) в силу теоремы 92 показывают, что дивизор $\Pi_1'\Pi_2' \ldots \Pi_\rho' \cdot P_1 \cdot P_2 \ldots P_\rho$ лежит в том же классе, что и $\Pi_1^{(\varepsilon)} \cdot \Pi_2^{(\varepsilon)} \ldots \Pi_\rho^{(\varepsilon)} \times \Pi_1 \cdot \Pi_2 \ldots \Pi_\rho$, точки которого известны. Его порядок равен $2\rho$, его измерение равно

$$2\rho - (\rho - 1) = \rho + 1,$$

а потому дивизор $\Pi_1' \cdot \Pi_2' \ldots \Pi_\rho' \cdot P_1 \cdot P_2 \ldots P_\rho$ рационально определится его делимостью на простые дивизоры $P_1, P_2, \ldots, P_\rho$. Найдём элемент

$$T_\varepsilon(P) \equiv \frac{\Pi_1'\Pi_2' \ldots \Pi_\rho' \cdot P_1 \cdot P_2 \ldots P_\rho}{\Pi_1^{(\varepsilon)} \cdot \Pi_2^{(\varepsilon)} \ldots \Pi_\rho^{(\varepsilon)} \cdot \Pi_1 \cdot \Pi_2 \ldots \Pi_\rho}$$

и точно так же элемент

$$T_\eta(P) \equiv \frac{\Pi_1'' \cdot \Pi_2'' \ldots \Pi_\rho'' \cdot P_1 \cdot P_2 \ldots P_\rho}{\Pi_1^{(\eta)} \cdot \Pi_2^{(\eta)} \ldots \Pi_\rho^{(\eta)} \cdot \Pi_1 \cdot \Pi_2 \ldots \Pi_\rho}.$$

Деля один элемент на другой, получим элемент, имеющий те же нули и полюсы, что и $R$:

$$T_\varepsilon(P) : T_\eta(P) \equiv \frac{\Pi_1' \cdot \Pi_2' \ldots \Pi_\rho' \cdot \Pi_1^{(\eta)} \cdot \Pi_2^{(\eta)} \ldots \Pi_\rho^{(\eta)}}{\Pi_1'' \cdot \Pi_2'' \ldots \Pi_\rho'' \cdot \Pi_1^{(\varepsilon)}, \Pi_2^{(\varepsilon)}, \ldots, \Pi_\rho^{(\varepsilon)}}, \tag{28}$$

и в силу этого отличающийся от $R$ независимым от $P$ множителем, который может, однако, зависеть от $P_1, P_2, \ldots, P_\rho$. Последней зависимости можно избежать, если нормировать выражение (28) так, чтобы все точки $P_1, P_2, \ldots, P_\rho$ входили в него симметрично. Возможность такого нормирования вытекает из того, что правую часть (28) можно представить в форме

$$e^{\sum_{\nu=1}^{\rho} \omega_{\Pi_\nu', \Pi''}(P) + \sum_{\nu=1}^{\rho} \omega_{\Pi_\nu^{(\eta)}, \Pi_\nu^{(\varepsilon)}}(P)},$$

где $\omega_{\Pi', \Pi''}(P)$ — нормированные элементарные интегралы 3-го рода, а затем применить теорему о перестановке аргумента с параметром (см. § 46, VII).

Таким образом мы приходим к формуле

$$\frac{\vartheta_\varepsilon\left(\sum_{\nu=0}^{\rho} u_\mu(P_\nu) - \sum_{\nu=1}^{\rho} u_\mu(\Pi_\nu)\right)}{\vartheta_\eta\left(\sum_{\nu=0}^{\rho} u_\mu(P_\nu) - \sum_{\nu=1}^{\rho} u_\mu(\Pi_\nu)\right)} = C_{\varepsilon\eta} \cdot \sqrt{\prod_{\nu=1}^{\rho} \frac{\psi_\varepsilon(z, \omega)}{\psi_\eta(z, \omega)}} \cdot \frac{T_\varepsilon(P)}{T_\eta(P)}, \tag{29}$$

в которой левая часть есть функция от

$$u_\mu = \sum_{\nu=0}^{\rho} u_\mu(P_\nu) - \sum_{\nu=1}^{\rho} u_\mu(\Pi_\nu), \tag{30}$$

а правая рационально зависит от пар $z$, $w$; $z_1$, $w_1$; ...; $z_\rho$, $w_\rho$, связанных уравнениями

$$f(z_k, w_k) = 0 \qquad (k = 0, 1, \ldots, \rho). \tag{31}$$

Полагая $P = P_0$, в силу чего $u_\mu(P_0) = 0$ и $z = z_0$, $w = w_0$ обращаются в постоянные, а затем, составляя равенства для $\rho$ различных пар характеристик $\left[\frac{\varepsilon}{\varepsilon'}\right], \left[\frac{\eta}{\eta'}\right]$, мы получим систему алгебраических уравнений (29) и (31) относительно $2\rho$ неизвестных $z_\nu$, $w_\nu$ ($\nu = 1, 2, \ldots, \rho$), из которых последние определяются как алгебраические функции от

$$\frac{\vartheta_\varepsilon(u_\mu)}{\vartheta_\eta(u_\mu)}.$$

В заключение остановимся на определении полиномов $\varphi_\varepsilon(z, w)$, носящих название *касательных функций* (Berührungs funktionen) для двух примеров.

*Пример* 1. Пусть гиперэллиптическое поле задано переменными $z$, $w$, связанными уравнением

$$w^2 = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_{2\rho+2}).$$

Для этого поля интегралы 1-го рода имеют вид

$$\frac{c_0 + c_1 z + \ldots + c_{\rho-1} z^{\rho-1}}{w},$$

так что

$$\varphi(z, w) = c_0 + c_1 z + \ldots + c_{\rho-1} z^{\rho-1}.$$

Для получения касательных функций надо подобрать постоянные $c_0$, $c_1$, ..., $c_{\rho-1}$ так, чтобы $\varphi(z, w)$ обращались в нули 2-й кратности в своих нулевых точках. Таковыми являются:

1) Полиномы $(z - \beta_1)(z - \beta_2) \ldots (z - \beta_{\rho-1})$, где $\beta_1, \beta_2, \ldots, \beta_{\rho-1}$ — всевозможные системы из $\rho - 1$ значений, взятых из $\alpha_1, \alpha_2, \ldots, \alpha_{2\rho+2}$; их всего

$$C_{2\rho+2}^{\rho-1} \frac{(2\rho+2)(2\rho+1)\ldots(\rho+4)}{1 \cdot 2 \ldots (\rho-1)}.$$

2) Полиномы $(z - \beta_1)(z - \beta_2) \ldots (z - \beta_{\rho-3})(z - c)^2$, где $c$ — произвольная величина.

3) Полиномы $(z - \beta_1)(z - \beta_2) \ldots (z - \beta_{\rho-5})(z - c)^2(z - c_1)^2$, где $c$ и $c_1$ — произвольные величины.

. . . . . .

. . . . . .

Из этих выражений мы видим, что здесь многие из касательных полиномов содержат произвольные константы, а потому соответствующие им римановы $\vartheta$-функции с характеристиками тождественно обращаются в нуль.

*Пример* 2. Кривая 4-го порядка

$$f(z, w) = 0 \tag{32}$$

без особых точек даёт начало полю $k(z, w)$ жанра $p = 3$. Для него интегралы 1-го рода могут быть представлены в виде

$$\frac{a + bz + cw}{f_w(z, w)},$$

где $a$, $b$, $c$ — константы. Касательные полиномы

$$\varphi(z, w) = a + bz + cw \tag{33}$$

должны обращаться в нуль 2-й кратности в двух точках [поскольку $2p - 2 = 4$ и прямая $\varphi(z, w) = 0$ пересекает кривую (32) в четырёх точках]. Таким образом, чтобы $\varphi(z, w)$ был касательным полиномом, необходимо и достаточно, чтобы прямая $\varphi(z, w) = 0$ *касалась* кривой (32) в двух точках. Из геометрии известно, что кривая 4-го порядка без особых точек имеет 28 касательных. Это число как раз равно числу $u_3$ нечётных характеристик для 3 аргументов:

$$u_3 = 2^{3-1} \cdot (2^3 - 1) = 28$$

[см. ниже, § 52, формулы (23) — (26)]. В этом случае существует лишь конечное число касательных полиномов.

## § 51. Задача, обратная проблеме обращения абелевых интегралов. Поверхности переноса

Мы видели, что, решая проблему обращения абелевых интегралов, мы приходим к $\vartheta$-функциям. Возникает вопрос: можем ли мы, исходя от заданной $\vartheta$-функции от $p$ аргументов, притти обратно к полю алгебраических функций жанра $p$? Простой подсчёт параметров показывает, что в общем случае это невозможно. В самом деле, выражение $\vartheta$-функции содержит параметры $a_{\mu\nu}$, число которых равно

$$\frac{p(p+1)}{2},$$

в то время как число параметров, определяющих поле жанра $p$, равно

$$3p - 3$$

(см. § 34). Таким образом для того, чтобы заданная $\vartheta$-функция приводила к полю жанра $p$, необходимо, чтобы её параметры удов-

летворяли условиям.

$$(1)\qquad \frac{\rho(\rho+1)}{2}-(3\rho-3)=\frac{(\rho-2)(\rho-3)}{2}$$

При $\rho=2$ и $\rho=3$ это число обращается в нуль, так что обратная задача в этих случаях возможна без всяких ограничений. И действительно, Гёпель [40] и Розенгайн [90] построили теорию для $\rho=2$, исходя от $\vartheta$-функций. Подобную же задачу решил Шоттки (F. Schottky) [95] для $\rho=3$.

Виртингер (W. Wirtinger) [112] исследовал вопрос о поле алгебраических функций, к которому приводят общие $\vartheta$-функции от $\rho$ аргументов. Он построил в пространстве $2^\rho-1$ измерений многообразие $\rho$ измерений, описываемое $\vartheta$-функциями 2-го порядка, и показал, что одномерное плоское сечение этого многообразия имеет жанр

$$\pi=\rho'\cdot 2^{\rho-2}(\rho-1)+1.$$

Шоттки [96] нашёл условие, которому должны подчиняться параметры $\vartheta$-функции от 4 аргументов для того, чтобы она приводила к полю жанра 1. Его вывод носит частный характер. Он основан на том, что отношение двух римановых $\vartheta$-функций с нечётными характеристиками

$$\frac{\vartheta_\varepsilon(u_\mu(P)-u_\mu(P_0))}{\vartheta_\eta(u_\mu(P)-u_\mu(P_0))}$$

есть симметричная функция от $P$ и $P_0$ и вместе с тем распадается в произведение двух функций, из которых одна зависит только от $P$, а другая только от $P_0$:

$$\frac{\vartheta_\varepsilon(u_\mu(P)-u_\mu(P_0))}{\vartheta_\eta(u_\mu(P)-u_\mu(P_0))}=\frac{\Phi_\varepsilon(P)\cdot\Phi_\varepsilon(P_0)}{\Phi_\eta(P)\cdot\Phi_\eta(P_0)}.$$

Этот факт может быть выведен из формулы (29) § 50. Пользуясь им, Шоттки показывает, что система однородных квадратичных соотношений между $\vartheta$-функциями с нечётными характеристиками, выводимая в общей теории $\vartheta$-функций (здесь она не приведена), может удовлетворяться произведениями типа $\Phi_\varepsilon(P)\cdot\Phi_\varepsilon(P_0)$ только в том случае, если нулевые значения $\vartheta$-функций с чётными характеристиками связаны некоторым соотношением, которое для общих $\vartheta$-функций не имеет места. Не давая вывода этого соотношения, ограничимся указанием его внешнего вида. При $\rho=4$ существует всего $8\cdot 17=136$ $\vartheta$-функций с чётными характеристиками. Из них, пользуясь теорией так называемых сизигетических групп, можно выделить 3 системы по 8 $\vartheta$-функций. Обозначая произведение каждых из восьми функций через $R_1$, $R_2$, $R_3$, а их нулевые значения через $r_1$, $r_2$, $r_3$, Шоттки приходит к соотношению

$$(2)\qquad r_1^2+r_2^2+r_3^2-2r_1r_2-2r_2r_3-2r_3r_1=0,$$

которому можно придать форму

$$\sqrt{r_1} \pm \sqrt{r_2} \pm \sqrt{r_3} = 0.$$

Это выражение трансцендентно относительно периодов $a_{\mu\nu}$. Шоттки только показал его необходимость. Его достаточность вытекает, хотя и без должной строгости, из того, что при $\rho = 4$ выражение (1) принимает значение, равное 1, из чего следует, что между $a_{\mu\nu}$ может существовать только одно соотношение. Во всяком случае метод Шоттки не даёт возможности, исходя из $\vartheta$-функций с периодами, удовлетворяющими соотношению (2), построить соответствующее им поле алгебраических функций. Тем более не видно, как распространить этот метод на случай более высоких значений жанра.

Пуанкаре (H. Poincaré) [83] исследовал ту же задачу, но его постановка задачи носит общий характер и может быть применена к $\vartheta$-функции от любого числа аргументов. Кроме того, из его исследований вытекает принципиальная возможность построения из данной $\vartheta$-функции соответствующего ей поля алгебраических функций.

Пуанкаре исходит из уравнения

$$\vartheta(u_1, u_2, \ldots, u_\rho) = 0, \tag{3}$$

определяющего в $\rho$-мерном пространстве некоторую гиперповерхность. Из теоремы 97 следует, что координаты этой гиперповерхности допускают следующее параметрическое представление:

$$u_\mu = u_\mu(P_1) + u_\mu(P_2) + \ldots + u_\mu(P_{\rho-1}) + k_\mu \quad (\mu = 1, 2, \ldots, \rho), \tag{4}$$

где $P_1, P_2, \ldots, P_{\rho-1}$ являются независимыми параметрами. Такого рода гиперповерхности носят название *гиперповерхностей переноса*, поскольку они могут быть образованы при помощи параллельного переноса кривых

$$x_\mu = u_\mu(P) \qquad (\mu = 1, 2, \ldots, \rho)$$

в пространстве. Более того, гиперповерхность (3) допускает два существенно различных параметрических решения типа (4). В самом деле, в силу чётности $\vartheta$-функций, наряду с (3), имеет место также

$$\vartheta(-u_1, -u_2, \ldots, -u_\rho) = 0,$$

откуда в силу теоремы 97 следует, что и величины $-u_\mu$ допускают представление типа (4), и таким образом

$$u_\mu \equiv -u_\mu(P_\rho) - u_\mu(P_{\rho+1}) - \ldots - u_\mu(P_{2\rho-2}) - k_\mu \quad (\mu = 1, 2, \ldots, \rho), \tag{5}$$

где $P_\rho, P_{\rho+1}, \ldots, P_{2\rho-2}$ — новые параметры. Таким образом задача

сводится к нахождению условий того, чтобы уравнение (3) представляло гиперповерхность двойного переноса.

Сам Пуанкаре ограничивается решением задачи для того случая, когда периоды $a_{\mu\nu}$ образуют матрицу

$$\|a_{\mu\nu}\|, \tag{6}$$

бесконечно мало отличающуюся от диагональной.

Если матрица (6) имеет характер диагональной матрицы, т. е. если $a_{\mu\nu}=0\,(\mu\neq\nu)$, то $\vartheta$-функция распадается в произведение четырёх эллиптических $\theta$-функций:

$$\vartheta(u_1, u_2, u_3, u_4)=$$

$$=\sum_{m_1, m_2, m_3, m_4}^{-\infty\ldots+\infty} e^{\pi i\sum_{\mu=1}^{4} a_{\mu\mu}\cdot m_\mu^2+2\pi i\sum_{\mu=1}^{4} m_\mu u_\mu}=\theta_1(u_1)\cdot\theta_2(u_2)\cdot\theta_3(u_3)\cdot\theta_4(u_4),$$

где

$$\theta_\nu(u_\nu)=\sum_{m_\nu=-\infty}^{+\infty} e^{\pi i a_{\nu\nu}m_\nu^2+2\pi i m_\nu u_\nu}\qquad(\nu=1,\ 2,\ 3,\ 4).$$

Обозначив нули этих функций (константы) соответственно через $\alpha_1$, $\alpha_2$, $\alpha_3$, $\alpha_4$, Пуанкаре делает различные гипотезы относительно характера близости периодов $a_{\mu\nu}\,(\mu\neq\nu)$ к нулю, а корней уравнения (3) к $a_\nu$. Все они, кроме одной, приводят к гиперповерхностям переноса. Последняя гипотеза, которая только одна и представляет для нас интерес, следующая. Пусть

$$u_\nu=\alpha_\nu+t\cdot\xi_\nu,\quad a_{\mu\nu}=t^2\cdot\gamma_{\mu\nu}\qquad(\mu,\ \nu=1,\ 2,\ 3,\ 4;\ \ \mu\neq\nu),$$

где $t$ — параметр, принимающий весьма малые значения. Разложим функцию $\vartheta\,(u_1, u_2, u_3, u_4)$ по степеням $t$. Предварительно сделаем подстановку

$$u_\nu\to\frac{u_\nu}{2\pi i},\quad \alpha_\nu\to\frac{\alpha_\nu}{2\pi i},\quad a_{\mu\nu}\to\frac{a_{\mu\nu}}{2\pi i},$$

которая приведёт $\vartheta$-функцию к виду

$$(7)\ \vartheta(u_1, u_2, u_3, u_4)=\sum_{m_1, m_2, m_3, m_4}^{-\infty\ldots+\infty} e^{\frac{1}{2}\cdot\sum_{\mu,\nu}\alpha_{\mu\nu}m_\mu m_\nu+\sum_\nu m_\nu u_\nu}=$$

$$=\sum_{m_1, m_2, m_3, m_4}^{-\infty\ldots+\infty} e^{\frac{1}{2}\sum_\nu a_{\nu\nu}\cdot m_\nu^2+\sum_\nu m_\nu\cdot\alpha_\nu}\cdot\varrho^{\,t\cdot\sum_\nu m_\nu\xi_\nu+\frac{t^2}{2}\sum_{\mu\neq\nu}\gamma_{\mu\nu}\cdot m_\mu\cdot m_\nu}.$$

Разложим по степеням $t$ второй множитель под знаком суммы. Временно введём обозначения

$$\sum_{\nu} m_\nu \cdot \xi_\nu = A; \quad \sum_{\mu \neq \nu} \gamma_{\mu\nu} \cdot m_\mu \cdot m_\nu = B, \tag{8}$$

$$\begin{aligned} e^{A \cdot t + \frac{1}{2} \cdot Bt^2} &= 1 + \left(At + \frac{1}{2} Bt^2\right) + \frac{1}{2}\left(A^2t^2 + ABt^3 + \frac{1}{4} A^2t^4\right) + \\ &+ \frac{1}{6}(A^3t^3 + 3A^2Bt^4 + \ldots) + \frac{1}{24}(A^4t^4 + \ldots) + \ldots = \\ &= 1 + A \cdot t + \frac{1}{2}(A^2 + B)\, t^2 + \frac{1}{6}(A^3 + 3AB)\, t^3 + \\ &+ \frac{1}{24}(A^4 + 12A^2B + 3B^2)\, t^4 + \ldots \end{aligned} \tag{9}$$

После этого подставим в (7) выражение (9), куда вставим (8), разлагая полиномы по степеням $m_\nu$. Принимая во внимание, что члены, не содержащие хотя бы одного значка $m_1$, $m_2$, $m_3$, $m_4$, после внешней суммации (7) в силу $\theta_\nu(\alpha_\nu) = 0$ обратятся в нуль, будем учитывать только члены с $m_1$, $m_2$, $m_3$, $m_4$. Вводя обозначения

$$\theta'_\nu(\alpha_\nu) = \sum_{m_1, m_2, m_3, m_4}^{-\infty \ldots +\infty} e^{\frac{1}{2} \cdot a_{\nu\nu} \cdot m_\nu^2 + m_\nu \cdot \alpha_\nu} \cdot m_\nu,$$

будем иметь

$$\begin{aligned} \vartheta(u_1, u_2, u_3, u_4) = \\ = t^4 \cdot \theta'_1(\alpha_1) \cdot \theta'_2(\alpha_2) \cdot \theta'_3(\alpha_3) \cdot \theta'_4(\alpha_4) \{ \xi_1\xi_2\xi_3\xi_4 + \\ + \sum_{(\alpha\beta\gamma\delta)} \gamma_{\alpha\beta} \cdot \xi_\gamma \cdot \xi_\delta + \sum_{(\alpha\beta\gamma\delta)} \gamma_{\alpha\beta}\gamma_{\gamma\delta} \} + \ldots, \end{aligned} \tag{10}$$

где $(\alpha\beta\gamma\delta)$ пробегает те перестановки цифр 1, 2, 3, 4, которые дают различные члены. Поскольку уравнение (3) должно представлять гиперповерхность переноса при всяком малом значении $t$, в частности и уравнение

$$\xi_1\xi_2\xi_3\xi_4 + \sum_{(\alpha\beta\gamma\delta)} \gamma_{\alpha\beta} \cdot \xi_\gamma \cdot \xi_\delta + \sum_{(\alpha\beta\gamma\delta)} \gamma_{\alpha\beta} \cdot \gamma_{\gamma\delta} = 0 \tag{11}$$

должно давать гиперповерхность переноса.

Аналогичным образом полученная поверхность в случае $p = 3$, т. е.

$$\xi_1\xi_2\xi_3 + \gamma_{23} \cdot \xi_1 + \gamma_{31} \cdot \xi_2 + \gamma_{12} \cdot \xi_3 = 0, \tag{12}$$

всегда является поверхностью переноса. В самом деле, если мы положим

$$\begin{cases} \xi_1 = P_1\left(\dfrac{1}{u} + \dfrac{1}{v}\right), \\ \xi_2 = P_2\left(\dfrac{1}{u-\varepsilon} + \dfrac{1}{v-\varepsilon} + \dfrac{3}{2\varepsilon}\right), \\ \xi_3 = P_3\left(\dfrac{1}{u+\varepsilon} + \dfrac{1}{v+\varepsilon} - \dfrac{3}{2\varepsilon}\right), \end{cases} \tag{13}$$

где

$$(14)\quad P_1=\frac{2\sqrt{\gamma_{23}}}{\varepsilon\sqrt{\gamma_{31}\cdot\gamma_{12}}},\quad P_2=\frac{\sqrt{\gamma_{31}}}{2\varepsilon\sqrt{\gamma_{23}\cdot\gamma_{12}}},\quad P_3=\frac{\sqrt{\gamma_{12}}}{2\varepsilon\sqrt{\gamma_{23}\cdot\gamma_{31}}},$$

то (12) удовлетворится тождественно. Производя над $u$ и $v$ одно и то же дробное линейное преобразование, мы можем перевести значения $0$, $\varepsilon$, $-\varepsilon$, при которых соответственно $\xi_1$, $\xi_2$, $\xi_3$ обращаются в бесконечность, в три произвольных числа $a_1$, $a_2$, $a_3$, и после этого преобразования в выражении для $\xi_1$, $\xi_2$, $\xi_3$ перед дробями $\frac{1}{u-a_1}$, $\frac{1}{u-a_2}$, $\frac{1}{u-a_3}$ будут стоять соответственно коэффициенты

$$(15)\quad \begin{cases} A_1=\dfrac{(\alpha_2-\alpha_3)(\alpha_1-\alpha_2)}{\alpha_3-\alpha_1}\cdot\sqrt{\dfrac{\gamma_{23}}{\gamma_{31}\cdot\gamma_{12}}}, \\ A_2=\dfrac{(\alpha_3-\alpha_1)(\alpha_2-\alpha_3)}{\alpha_1-\alpha_2}\sqrt{\dfrac{\gamma_{31}}{\gamma_{12}\cdot\gamma_{23}}}, \\ A_3=\dfrac{(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)}{\alpha_2-\alpha_3}\cdot\sqrt{\dfrac{\gamma_{12}}{\gamma_{23}\cdot\gamma_{31}}}. \end{cases}$$

Обратимся к гиперповерхности (11). Предположим, что она является гиперповерхностью переноса, т. е. что её координаты $\xi_1$, $\xi_2$, $\xi_3$, $\xi_4$ допускают параметрическое представление вида

$$(16)\quad \begin{cases} \xi_1=\varphi_1(u)+\varphi_2(v)+\varphi_3(w), \\ \xi_2=\varphi_4(u)+\varphi_5(v)+\varphi_6(w), \\ \xi_3=\varphi_7(u)+\varphi_8(v)+\varphi_9(w), \\ \xi_4=\varphi_{10}(u)+\varphi_{11}(v)+\varphi_{12}(w). \end{cases}$$

Далее, предположим, что существует значение $w=a_4$, обращающее в $\infty$ $\varphi_{12}(w)$, но не функции $\varphi_3(w)$, $\varphi_6(w)$, $\varphi_9(w)$. После подстановки $w=a_4$ мы получим $\xi_4=\infty$, и уравнение (11) примет вид

$$\xi_1\xi_2\xi_3+\gamma_{23}\xi_1+\gamma_{31}\xi_2+\gamma_{12}\xi_3=0,$$

т. е. вид (12). Мы видели, что это уравнение допускает параметрическое представление типа

$$(17)\qquad \xi_\nu=\frac{A_\nu}{u-a_\nu}+\frac{A_\nu}{v-a_\nu}+B_\nu\qquad(\nu=1,\ 2,\ 3),$$

где $A_\nu$ даны формулами (15). Вместе с тем можно убедиться (например, методами следующего параграфа), что координаты поверхности (12) допускают представление как поверхности переноса только в форме (17), так что, подставляя в (16) $W=a_4$, мы получим

$$\varphi_1(u)=\frac{A_1}{u-a_1}+\text{const.},\quad \varphi_2(v)=\frac{A_1}{v-a_1}+\text{const.},\qquad \text{и т. д.},$$

и первые три формулы (16) перепишутся так:

$$\xi_\nu = \frac{A_\nu}{u - a_\nu} + \frac{A_\nu}{v - a_\nu} + \text{const.} \qquad (\nu = 1, 2, 3).$$

Далее, оставляя $W$ переменным и полагая $v = a_3$, мы из тех же соображений убедимся, что и функции $\varphi_8$, $\varphi_9$, $\varphi_{10}$, $\varphi_{11}$, $\varphi_{12}$ имеют такую же форму, т. е. что для гиперповерхности (11)

$$(18) \qquad \xi_\nu = \frac{A_\nu}{u - a_\nu} + \frac{A_\nu}{v - a_\nu} + \frac{A_\nu}{w - a_\nu} + B_\nu \qquad (\nu = 1, 2, 3, 4).$$

Чтобы найти выражение для $A_1$, положим $w = a_4$. Тогда из формул (15) следует:

$$A_1 = \frac{(a_2 - a_3)(a_1 - a_2)}{a_3 - a_1} \cdot \sqrt{\frac{\gamma_{23}}{\gamma_{31} \cdot \gamma_{12}}}.$$

Полагая же $v = a_3$, мы аналогично получим:

$$A_1 = \frac{(a_2 - a_4)(a_1 - a_2)}{a_4 - a_1} \cdot \sqrt{\frac{\gamma_{24}}{\gamma_{41} \cdot \gamma_{12}}}.$$

Сопоставляя обе формулы, будем иметь:

$$(19) \qquad \frac{(a_2 - a_3)(a_1 - a_4)}{(a_1 - a_3)(a_2 - a_4)} = \sqrt{\frac{\gamma_{13} \cdot \gamma_{24}}{\gamma_{23} \cdot \gamma_{14}}}.$$

Здесь, конечно, мы должны подразумевать перед радикалом двойной знак.

Приравнивая друг другу значения других $A_\nu$, мы придём к формулам, получаемым из (19) перестановкой значков 1, 2, 3, 4:

$$(20) \qquad \frac{(a_3 - a_4)(a_1 - a_2)}{(a_2 - a_4)(a_1 - a_3)} = \sqrt{\frac{\gamma_{13} \cdot \gamma_{24}}{\gamma_{12} \cdot \gamma_{34}}},$$

$$(21) \qquad \frac{(a_2 - a_3)(a_1 - a_4)}{(a_1 - a_2)(a_3 - a_4)} = \sqrt{\frac{\gamma_{12} \cdot \gamma_{34}}{\gamma_{23} \cdot \gamma_{14}}}.$$

Но между левыми частями (19) и (20) имеет место соотношение

$$\frac{(a_2 - a_3)(a_1 - a_4)}{(a_1 - a_3)(a_2 - a_4)} + \frac{(a_1 - a_2)(a_3 - a_4)}{(a_1 - a_3)(a_2 - a_4)} = 1,$$

откуда

$$(22) \qquad \pm \frac{1}{\sqrt{\gamma_{23}\gamma_{14}}} \pm \frac{1}{\sqrt{\gamma_{12}\gamma_{34}}} \pm \frac{1}{\sqrt{\gamma_{13}\gamma_{24}}} = 0,$$

или в силу $a_{\mu\nu} = t^2 \cdot \gamma_{\mu\nu}$

$$(23) \qquad \pm \frac{1}{\sqrt{a_{23} \cdot a_{14}}} \pm \frac{1}{\sqrt{a_{12} \cdot a_{34}}} \pm \frac{1}{\sqrt{a_{13} \cdot a_{24}}} = 0$$

для малых значений $a_{\mu\nu}$. Сравни [83], стр. 292 (12 bis).

Это исследование Пуанкаре может показаться имеющим частный характер. Однако положенный в его основу принцип приобретает решающий и самый общий характер при решении поставленной проблемы, если мы сопоставим его с исследованиями Ли (S. Lie) [70,71] и его последователей. Ли доказал, что поверхности в трёхмерном пространстве, допускающие два различных параметрических представления как поверхности переноса, допускают представление своих координат через суммы абелевых интегралов жанра $\rho = 3$, и впоследствии обобщил этот результат на случай $\rho = 4$. Пуанкаре [84] дал эскиз доказательства для произвольного $\rho$. Чеботарёв [102] провёл полное доказательство для произвольного $\rho$, а также наметил способ узнавать, является ли поверхность, заданная уравнением, поверхностью переноса. Этот способ даёт возможность, исходя от заданной $\vartheta$-функции от $\rho$ аргументов, найти условия того, чтобы ей соответствовали абелевы интегралы жанра $\rho$, и в том случае, если эти условия соблюдаются, построить поле алгебраических функций жанра $\rho$, приводящее к этим абелевым интегралам и к заданной $\vartheta$-функции. При этом нужно оговориться, что до сих пор только указан путь к решению этих задач, а проведение по этому пути вычислений тормозится в силу необычайно сложных формул, к которым приводит теория гиперповерхностей переноса, а также сложности соотношений между $\vartheta$-функциями. Теории гиперповерхностей переноса будет посвящён следующий параграф.

## § 51′. Общая теория гиперповерхностей переноса

Пусть в $(n+1)$-мерном пространстве задана гиперповерхность

$$z = f(x_1, x_2, \ldots, x_n), \tag{1}$$

где $f$ — функция, дифференцируемая по всем аргументам по крайней мере 4 раза. Если эта гиперповерхность является гиперповерхностью переноса, то её координаты допускают такое параметрическое представление:

$$x_\mu = \varphi_{\mu 1}(u_1) + \varphi_{\mu 2}(u_2) + \ldots + \varphi_{\mu n}(u_n) \qquad (\mu = 1, 2, \ldots, n), \tag{2}$$

$$z = \varphi_1(u_1) + \varphi_2(u_2) + \ldots + \varphi_n(u_n), \tag{3}$$

причём мы в дальнейшем будем прлдполагать, что функции $\varphi_{\mu\nu}(u_\nu)$ дифференцируемы по крайней мере 2 раза. В этом случае дифференцируем по $u_1$ соотношение (1), считая, что $x_\mu$ и $z$ заданы формулами (2) и (3). Вводя обозначения

$$\frac{\partial x_\mu}{\partial u_1} = \vartheta_\mu, \quad \frac{\partial z}{\partial u_1} = \zeta \qquad (\mu = 1, 2, \ldots, n),$$

$$P_\mu = \frac{\partial f}{\partial x_\mu}, \quad r_{\mu\nu} = \frac{\partial^2 f}{\partial x_\mu \cdot \partial x_\nu} \qquad (\mu, \nu = 1, 2, \ldots, n),$$

получим:

$$\zeta = p_1\theta_1 + p_2\theta_2 + \ldots + p_n\theta_n. \tag{4}$$

В этом соотношении величины $\zeta$, $\theta_\mu$ являются функциями только от $u_1$. В силу того, что в роли $u_1$ мы можем взять любую функцию от $u_1$, разделим (4) на $\theta_1$ (конечно, если $\theta_1 \not\equiv 0$) и обозначим частные $\frac{\zeta}{\theta_1}$, $\frac{\theta_\mu}{\theta_1}$ вновь через $\zeta$, $\theta_\mu$. Далее, если $\theta_2$ не есть константа, обозначим её через $\tau$ и будем считать $\theta_3, \ldots, \theta_n, \zeta$ функциями от $\tau$. Соотношение (4) примет вид

$$p_1 + p_2\tau + p_3\theta_3 + \ldots + p_n\theta_n - \zeta = 0. \tag{5}$$

Будем теперь считать, что функции $\varphi_{\mu\nu}(u_1)$ являются функциями от $\tau$, и дифференцируем (5) по $u_1$, полагая, что $x_\mu$ и $z$ представляются формулами (2), (3):

$$\sum_{\mu,\nu=1}^{n} r_{\mu\nu}\theta_\mu\theta_\nu + \Big(\sum_{\nu=1}^{n} p_\nu\theta'_\nu - \zeta'_\nu\Big)\psi = 0, \tag{6}$$

где

$$\theta'_1 = 0,\ \theta'_2 = 1,\ \theta'_\mu = \frac{d\theta_\mu}{d\tau},\quad \zeta' = \frac{d\zeta}{d\tau},\quad \psi = \frac{d\tau}{du_1}\qquad (\mu = 3, \ldots, n).$$

Нетрудно составить условия совместности уравнений (1), (5) и (6). Введём обозначения

$$R = \sum_{\nu=1}^{n} p_\nu\theta_\nu,\quad C = \sum_{\mu,\nu=1}^{n} r_{\mu\nu}\theta_\mu\theta_\nu,$$

где будем считать $R$ и $C$ функциями от $x_\nu$ и $\tau$. Значками внизу будем обозначать дифференцирование:

$$R_{x_\nu} = \frac{\partial R}{\partial x_\nu},\quad R_x = \frac{\partial R}{\partial \tau}.$$

Предположим, что $\psi \not\equiv 0$ тождественно [равенство $\psi = 0$, как можно убедиться, означало бы, что (1) есть линейчатая гиперповерхность, и тогда уравнения (5), (6) могут быть удовлетворены без того, чтобы (1) была гиперповерхность переноса]. Уравнения (5) и (6) перепишутся так:

$$R - \zeta = 0, \tag{5'}$$

$$C + R_\tau \cdot \psi = 0. \tag{6'}$$

Будем считать $\tau = \tau(x_1, x_2, \ldots, x_n)$ искомой функцией от $x_\nu$. Дифференцируя (5') по $x_\nu$, получим

$$R_\nu + (R_\tau - \zeta') \cdot \frac{\partial\tau}{\partial x_\nu} = 0 \qquad (\nu = 1, 2, \ldots, n) \tag{7}$$

или

$$\sum_{\nu=1}^{n} R_\nu\, dx_\nu + (R_\tau - \zeta')\, d\tau = 0. \tag{8}$$

Уравнение (6) показывает, что функция $\frac{C}{R_\tau}$ зависит от $\tau$, в силу чего якобиева матрица

$$\left\| \begin{matrix} \left(\frac{C}{R_\tau-\zeta'}\right)_1 + \left(\frac{C}{P_\tau-\zeta'}\right)_\tau \cdot \frac{\partial\tau}{\partial x_1}, & \ldots, & \left(\frac{C}{R_\tau-\zeta'}\right)_n + \left(\frac{C}{R_\tau-\zeta'}\right)_\tau \cdot \frac{\partial\tau}{\partial x_n} \\ \frac{\partial\tau}{\partial x_1}, & \ldots, & \frac{\partial\tau}{\partial x_n} \end{matrix} \right\|,$$

а в силу этого матрица

$$\left\| \begin{matrix} \left(\frac{C}{R_\tau-\zeta'}\right)_1, & \left(\frac{C}{R_\tau-\zeta'}\right)_2, \ldots, & \left(\frac{C}{R_\tau-\zeta'}\right)_n \\ \frac{\partial\tau}{\partial x_1}, & \frac{\partial\tau}{\partial x_2}, \quad \ldots, & \frac{\partial\tau}{\partial x_n} \end{matrix} \right\|$$

имеют ранг $\leqslant 1$. Учитывая формулы (7), мы заключаем отсюда:

$$\begin{vmatrix} C_1\cdot(R_\tau-\zeta') - C\cdot R_{\tau 1}, & R_1, & r_{13}, \ldots, r_{1n} \\ C_2\cdot(R_\tau-\zeta') - C\cdot R_{\tau 2}, & R_2, & r_{23}, \ldots, r_{2n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_n\cdot(R_\tau-\zeta') - C\cdot R_{\tau n}, & R_n, & r_{n3}, \ldots, r_{nn} \end{vmatrix} = 0. \tag{9}$$

Но

$$R_\mu = \sum_{\nu=1}^{n} r_{\mu\nu}\cdot\theta_\nu, \quad R_{\tau\mu} = \sum_{\nu=1}^{n} r_{\mu\nu}\theta'_\nu = r_{\mu 2} + r_{\mu 3}\theta'_3 + \ldots$$
$$\ldots + r_{\mu n}\theta'_n \quad (\mu = 1, 2, \ldots, n).$$

Подставляя в (9), мы после преобразований получим

$$(R_\tau-\zeta')\begin{vmatrix} C_1, r_{11}+r_{12}\cdot\tau, r_{13}, \ldots, r_{1n} \\ C_2, r_{21}+r_{22}\cdot\tau, r_{23}, \ldots, r_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ C_n, r_{n1}+r_{n2}\cdot\tau, r_{n3}, \ldots, r_{nn} \end{vmatrix} + C\cdot\begin{vmatrix} r_{11}, r_{12}, \ldots, r_{1n} \\ r_{21}, r_{22}, \ldots, r_{2n} \\ \ldots\ldots\ldots \\ r_{n1}, r_{n2}, \ldots, r_{nn} \end{vmatrix} = 0, \tag{10}$$

или, обозначая первый из определителей через $M$, а второй через $D$ (функция только от $x_\nu$), будем иметь:

$$(R_\tau-\zeta')\cdot M + C\cdot D = 0. \tag{11}$$

Исключая из (8) и (11) выражение $R_\tau - \zeta' = \sum_{\nu=1}^{n} p_\nu\theta'_\nu - \zeta'$, мы придём к следующему уравнению в полных дифференциалах:

$$M\cdot(R_1\cdot dx_1 + R_2\cdot dx_2 + \ldots + R_n\cdot dx_n) - C\cdot D\cdot d\tau = 0. \tag{12}$$

Все входящие в него выражения являются известными [при заданном уравнении (1)] функциями от $x_\nu$, $\tau$, $\theta_\nu$, а потому, интегрируя (12), мы получим $\tau$, $\theta_\nu$ как функции от $x_\nu$, если только соблюдаются условия интегрируемости этого уравнения. Последние могут быть представлены так:

$$\left(\frac{M}{D}\right)_\mu \cdot R_\nu - \left(\frac{M}{D}\right)_\nu \cdot R_\mu = 0 \qquad (\mu, \nu = 1, 2, \ldots, n). \tag{13}$$

Эти условия выражают в силу (7), что $\frac{M}{D}$ есть функция только от $\tau$.

Кроме того, мы должны получить выражение для $d\theta_\nu$. Для этого при составлении матрицы (9) допишем к матрице из двух столбцов матрицу

$$\begin{Vmatrix} r_{12}, r_{13}, \ldots, r_{1n} \\ r_{22}, r_{23}, \ldots, r_{2n} \\ \cdots\cdots\cdots \\ r_{n2}, r_{n3}, \ldots, r_{nn} \end{Vmatrix},$$

у которой откинем какой-нибудь, например $(k-1)$-й столбец. Тогда, вводя обозначение

$$M^{(k)} = \begin{vmatrix} C_1, r_{11} + r_{1k}\theta_k, r_{12}, \ldots, r_{1n} \\ C_2, r_{21} + r_{2k}\theta_k, r_{22}, \ldots, r_{2n} \\ \cdots\cdots\cdots\cdots\cdots \\ C_n, r_{n1} + r_{nk}\theta_k, r_{n2}, \ldots, r_{nn} \end{vmatrix} \qquad (k = 3, 4, \ldots, n),$$

мы будем иметь

$$(R_\tau - \zeta') \cdot M^{(k)} - C \cdot D \cdot \theta_k' = 0 \; (k = 3, 4, \ldots, n),$$

откуда в силу (11):

$$\frac{d\theta_k}{d\tau} = \frac{M^{(k)}}{M} \qquad (k = 3, 4, \ldots, n). \tag{14}$$

Система уравнений в полных дифференциалах (12), (14) может удовлетворяться тождественно, и тогда её интегрирование введёт в решение произвольные константы. Мы рассмотрим только тот случай, когда в решение константы входить не будут, т. е. когда условия совместимости уравнений (12), (14) определяют все $\tau$, $\theta_\nu$ как функции от $x_\nu$. Если притом эти функции будут удовлетворять системе (12), (14), то они и дадут нам искомый параметр $\tau$ (или $u_1$).

Для нахождения остальных параметров $u_2, \ldots, u_n$ нам надо найти $n$ различных решений

$$\tau^{(1)} = \tau, \; \tau^{(2)}, \ldots, \tau^{(n)}$$

системы (12), (14), которые притом должны быть связаны соотношениями

$$(15)\qquad \sum_{\mu,\nu}^{1\ldots n} r_{\mu\nu}\theta_\mu^{(i)}\theta_\nu^{(k)} = 0 \qquad (i \neq k;\ i,\ k = 1,\ 2,\ \ldots,\ n).$$

Последние получатся, если в отношении

$$\sum_{\mu=1}^{n} p_n\theta_\mu^{(i)} - \zeta^{(i)} = 0$$

считать $x_1, x_2, \ldots, x_n$ представленными формулами (2) и дифференцировать его по $u_k$, учитывая, что $\theta_\mu^{(i)}$, $\zeta^{(i)}$ являются функциями только от $u_i$ и потому от $u_k$ не зависят.

Покажем, что если такие решения $\tau^{(i)}$, $\theta_\nu^{(i)}$ системы (12), (14) существуют, то они действительно приводят к представлению $x_\nu$, $z$ в форме (2), (3). Для упрощения выкладок заменим $x_\nu$, $z$ лежандровой системой координат

$$p_\nu = \frac{\partial f}{\partial x_\nu}, \qquad \vartheta = p_1x_1 + p_2x_2 + \ldots + p_nx_n - z \qquad (\nu = 1,\ 2,\ \ldots,\ n)$$

и будем считать $r_{\mu\nu}$ функциями от $p_\nu$. Дифференцирование уравнения (5′) по $p_i$ даёт

$$(16)\qquad \theta_i + (R_\tau - \zeta')\frac{\partial\tau}{\partial p_i} = 0 \qquad (i = 1,\ 2,\ \ldots,\ n),$$

откуда

$$(17)\qquad (dp_1 + \tau\cdot dp_2 + \theta_3\cdot dp_3 + \ldots + \theta_n\cdot dp_n) + R_\tau\cdot d\tau = 0.$$

Далее, в силу (6′) выражение $\frac{C}{R_\tau - \zeta'}$ есть функция только от $\tau$, в силу чего

$$\frac{\partial\left(\frac{C}{R_\tau - \zeta'}, \tau\right)}{\partial(p_i, p_k)} = 0 \qquad (i, k = 1,\ 2,\ \ldots,\ n),$$

или

$$(R_\tau - \zeta')(C_i\theta_k - C_k\theta_i) - C(\theta_i'\theta_k - \theta_k'\theta_i) = 0 \qquad (i, k = 1,\ 2,\ \ldots,\ n).$$

Вводя обозначение

$$(17')\qquad N^{(i,k)} = C_i\theta_k - C_k\theta_i \qquad (i, k = 1,\ 2,\ \ldots,\ n),$$

мы при $i = 1$ будем иметь:

$$(18)\qquad (R_\tau - \zeta')N^{(1,k)} + C\cdot\theta_k' = 0 \qquad (k = 2,\ 3,\ \ldots,\ n).$$

Исключая $R_\tau - \zeta'$ из (17) и (18), получим

$$(19)\quad N^{(1,k)}(dp_1 + \tau \cdot dp_2 + \theta_3 \cdot dp_3 + \ldots + \theta_n \cdot dp_n) - C \cdot d\theta_k = 0 \qquad (k = 2, 3, \ldots, n)$$

и в частности

$$(20)\quad N^{(1,2)}(dp_1 + \tau \cdot dp_2 + \theta_3 dp_3 + \ldots + \theta_n \cdot dp_n) - C \cdot d\tau = 0.$$

Из (19) и (20) вытекает:

$$(21)\quad \frac{d\theta_k}{d\tau} = \frac{N^{(1,k)}}{N^{(1,2)}} \qquad (k = 2, 3, \ldots, n).$$

Условия интегрируемости уравнения (20) дают:

$$N_\lambda^{(1,2)} \cdot \theta_\mu - N_\mu^{(1,2)} \cdot \theta_\lambda = 0 \qquad (\lambda, \mu = 2, 3, \ldots, n).$$

Эти условия можно представить в виде

$$\frac{\partial (N^{(1,2)}, p_1 + p_2\tau + \ldots + p_n\theta_n)}{\partial (p_\lambda, p_\mu)} = 0.$$

Но так как $\zeta = p_1 + p_2\tau + \ldots + p_n\theta_n$ есть функция только от $\tau$, то и $N^{(1,2)} = N$ есть функция только от $\tau$.

Пусть система (20), (21) имеет решения $\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(n)}$, связанные соотношениями (15), которые можно переписать в форме

$$(22)\quad \sum_{\nu=1}^{n} R_\nu^{(i)} \cdot \theta_\nu^{(k)} = 0 \qquad (i \neq k;\ i, k = 1, 2, \ldots, n).$$

Будем пользоваться матричными обозначениями. Перепишем уравнения (20) так:

$$\frac{d\tau^{(k)}}{N^{(k)}} = \frac{1}{C^{(k)}} \cdot (dp_1 + \tau^{(k)} \cdot dp_2 + \ldots + \theta_n^{(k)} \cdot dp_n) \qquad (k = 1, 2, \ldots, n),$$

или при помощи матриц:

$$(23)\quad \left\| \begin{matrix} \frac{d\tau^{(1)}}{N^{(1)}} \\ \frac{d\tau^{(2)}}{N^{(2)}} \\ \vdots \\ \frac{d\tau^{(n)}}{N^{(n)}} \end{matrix} \right\| = \left\| \begin{matrix} \frac{1}{C^{(1)}}, & \frac{\tau^{(1)}}{C^{(1)}}, & \ldots, & \frac{\theta_n^{(1)}}{C^{(1)}} \\ \frac{1}{C^{(2)}}, & \frac{\tau^{(2)}}{C^{(2)}}, & \ldots, & \frac{\theta_n^{(2)}}{C^{(2)}} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{1}{C^{(n)}}, & \frac{\tau^{(n)}}{C^{(n)}}, & \ldots, & \frac{\theta_n^{(n)}}{C^{(n)}} \end{matrix} \right\| \cdot \left\| \begin{matrix} dp_1 \\ dp_2 \\ \vdots \\ dp_n \end{matrix} \right\|.$$

С другой стороны, соотношения

$$dp_i = \sum_{k=1}^{n} r_{ik} \cdot dx_k \qquad (i = 1, 2, \ldots, n)$$

можно переписать так:

$$\left\|\begin{matrix} dp_1 \\ dp_2 \\ \vdots \\ dp_n \end{matrix}\right\| = \left\|\begin{matrix} r_{11}, & r_{12}, & \ldots, & r_{1n} \\ r_{21}, & r_{22}, & \ldots, & r_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ r_{n1}, & r_{n2}, & \ldots, & r_{nn} \end{matrix}\right\| \cdot \left\|\begin{matrix} dx_1 \\ dx_2 \\ \vdots \\ dx_n \end{matrix}\right\|. \tag{24}$$

Наконец, соотношения (22), к которым мы присоединим ещё

$$C^{(i)} = \sum_{\nu=1}^{n} R_\nu^{(i)} \cdot \theta_\nu^{(i)}, \text{ т. е.}$$

$$\sum_{\nu=1}^{n} \frac{\theta_\nu^{(i)}}{C^{(i)}} \cdot R_\nu^{(i)} = 1 \quad (i = 1, 2, \ldots, n), \tag{25}$$

дают:

$$\left\|\begin{matrix} \frac{1}{C^{(1)}}, & \frac{\tau^{(1)}}{C^{(1)}}, & \ldots, & \frac{\theta_n^{(1)}}{C^{(1)}} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{1}{C^{(n)}}, & \frac{\tau^{(n)}}{C^{(n)}}, & \ldots, & \frac{\theta_n^{(n)}}{C^{(n)}} \end{matrix}\right\| \cdot \left\|\begin{matrix} R_1^{(1)}, & R_1^{(2)}, & \ldots, & R_1^{(n)} \\ \ldots & \ldots & \ldots & \ldots \\ R_n^{(1)}, & R_n^{(2)}, & \ldots, & R_n^{(n)} \end{matrix}\right\| = \left\|\begin{matrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{matrix}\right\|. \tag{26}$$

Здесь мы имеем право переставить множители, так что

$$\left\|\begin{matrix} R_1^{(1)}, & \ldots, & R_1^{(n)} \\ \ldots & \ldots & \ldots \\ R_n^{(1)}, & \ldots, & R_n^{(n)} \end{matrix}\right\| \cdot \left\|\begin{matrix} \frac{1}{C^{(1)}}, & \frac{\tau^{(1)}}{C^{(1)}}, & \ldots, & \frac{\theta_n^{(1)}}{C^{(1)}} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{1}{C^{(n)}}, & \frac{\tau^{(n)}}{C^{(n)}}, & \ldots, & \frac{\theta_n^{(n)}}{C^{(n)}} \end{matrix}\right\| = \left\|\begin{matrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{matrix}\right\|. \tag{27}$$

Но величины $R_\nu^{(i)}$ определяются равенствами

$$R_\nu^{(i)} = r_{\nu 1} + r_{\nu 2} \cdot \tau^{(i)} + r_{\nu 3} \cdot \theta_3^{(i)} + \ldots + r_{\nu n} \cdot \theta_n^{(i)} \tag{28}$$
$$(\nu, i = 1, 2, \ldots, n)$$

или

$$\left\|\begin{matrix} R_1^{(1)}, & \ldots, & R_1^{(n)} \\ \ldots & \ldots & \ldots \\ R_n^{(1)}, & \ldots, & R_n^{(n)} \end{matrix}\right\| = \left\|\begin{matrix} r_{11}, & \ldots, & r_{1n} \\ \ldots & \ldots & \ldots \\ r_{n1}, & \ldots, & r_{nn} \end{matrix}\right\| \cdot \left\|\begin{matrix} 1, & \ldots, & 1 \\ \tau^{(1)}, & \ldots, & \tau^{(n)} \\ \ldots & \ldots & \ldots \\ \theta_n^{(1)}, & \ldots, & \theta_n^{(n)} \end{matrix}\right\|. \tag{29}$$

Из (23) и (24) мы получим в силу (26):

$$\begin{Vmatrix} r_{11}, \ldots, r_{1n} \\ \ldots\ldots \\ r_{n1}, \ldots, r_{nn} \end{Vmatrix} \cdot \begin{Vmatrix} dx_1 \\ \vdots \\ dx_n \end{Vmatrix} = \begin{Vmatrix} R_1^{(1)}, \ldots, R_1^{(n)} \\ \ldots\ldots\ldots \\ R_n^{(1)}, \ldots, R_n^{(n)} \end{Vmatrix} \cdot \begin{Vmatrix} \frac{d\tau^{(1)}}{N^{(1)}} \\ \vdots \\ \frac{d\tau^{(n)}}{N^{(n)}} \end{Vmatrix}.$$

Далее, пользуясь (29) и умножая обе части равенства на

$$\begin{Vmatrix} r_{11}, \ldots, r_{1n} \\ \ldots\ldots \\ r_{n1}, \ldots, r_{nn} \end{Vmatrix}^{-1},$$

получим

$$\begin{Vmatrix} dx_1 \\ \vdots \\ dx_n \end{Vmatrix} = \begin{Vmatrix} 1, & \ldots, 1 \\ \tau^{(1)}, & \ldots, \tau^{(n)} \\ \ldots\ldots & \ldots\ldots \\ \theta_n^{(1)}, & \ldots, \theta_n^{(n)} \end{Vmatrix} \cdot \begin{Vmatrix} \frac{d\tau^{(1)}}{N^{(1)}} \\ \vdots \\ \frac{d\tau^{(n)}}{N^{(n)}} \end{Vmatrix},$$

т. е.

$$(30)\quad dx_\nu = \frac{\theta_\nu^{(1)} \cdot d\tau^{(1)}}{N^{(1)}} + \frac{\theta_\nu^{(2)} \cdot d\tau^{(2)}}{N^{(2)}} + \ldots + \frac{\theta_\nu^{(n)} \cdot d\tau^{(n)}}{N^{(n)}} \quad (\nu = 1, 2, \ldots, n).$$

Из

$$dz = p_1\, dx_1 + p_2\, dx_2 + \ldots + p_n\, dx_n$$

мы, пользуясь тем, что в силу (5′)

$$p_1 + p_2\tau^{(\nu)} + p_3\theta_3^{(\nu)} + \ldots + p_n\theta_n^{(\nu)} = \zeta^{(\nu)} \qquad (\nu = 1, 2, \ldots, n),$$

при помощи (30) получим:

$$(31)\qquad dz = \frac{\zeta^{(1)} \cdot d\tau^{(1)}}{N^{(1)}} + \frac{\zeta^{(2)} \cdot d\tau^{(2)}}{N^{(2)}} + \ldots + \frac{\zeta^{(n)} \cdot d\tau^{(n)}}{N^{(n)}}.$$

Учитывая, что величины $N^{(\nu)}$, $\theta_k^{(\nu)}$, $\zeta^{(\nu)}$ являются функциями только от $\tau^{(\nu)}$, и интегрируя уравнения (30), (31), мы приходим к представлению координат $x_\nu$, $z$ в форме (2), (3). Таким образом при соблюдении поставленных условий гиперповерхность (1) есть действительно гиперповерхность переноса.

Теперь докажем

Теорему 98. Пусть

1) *построенные для гиперповерхности* (1) *уравнения в полных дифференциалах* (20), (21) *имеют условия интегрируемости, определяющие* $\tau$, $\theta_3, \ldots, \theta_n$, $\zeta$ *как функции от* $p_1, p_2, \ldots, p_n$, *удовлетворяющие уравнениям* (20), (21);

2) *между n решениями этих условий интегрируемости имеют место соотношения* (22) (будем говорить тогда, что эти решения составляют *систему*);

3) *существует по крайней мере две системы решений.*

*Тогда координаты гиперповерхности* (1) *допускают представление в виде сумм абелевых интегралов жанра* $\rho \leqslant n+1$. *Если* $\rho = n+1$, *то все эти интегралы* 1*-го рода.*

Доказательство. Будем предполагать у читателя некоторое знакомство с теорией Галуа. Исключая из условий интегрируемости величины $\theta_3, \ldots, \theta_n$, получим уравнение, связывающее $\tau$ с $p_1, p_2, \ldots, p_n$, алгебраическое относительно $\tau$ и в силу 3) имеющее по крайней мере степень $2n$. Выделим множитель левой части этого уравнения, корни которого образуют две *системы*: $\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(n)}$ и $\tau^{(n+1)}, \ldots, \tau^{(2n)}$:

$$\Phi(t) = (t-\tau^{(1)})(t-\tau^{(2)})\ldots(t-\tau^{(n)})(t-\tau^{(n+1)})\ldots(t-\tau^{(2n)}) = \\ = t^{2n} + q_1 t^{2n-1} + \ldots + q_{2n}.$$

Будем считать *областью рациональности* совокупность рациональных функций от $p_\nu$, от величин $q_\mu$ [коэффициентов полинома $\Phi(t)$] и их производных по $p_\nu$. Мы увидим впоследствии, что эта область рациональности состоит только из рациональных функций от $p_\nu$.

Сопоставим уравнение в полных дифференциалах (20) с приравненным нулю дифференциалом полинома $\Phi(t)$:

$$\Phi_1 \cdot dp_1 + \Phi_2 \cdot dp_2 + \ldots + \Phi_n \cdot dp_n + \Phi_\tau \cdot d\tau = 0.$$

Поскольку $p_1, p_2, \ldots, p_n$ — независимые переменные, должно иметь место

(32) $\Phi_1 = \lambda N, \quad \Phi_2 = \lambda N\tau, \quad \Phi_3 = \lambda N\theta_3, \ldots, \quad \Phi_n = \lambda N\theta_n, \quad \Phi_\tau = -\lambda C.$

Эти равенства в общем случае удовлетворяются не тождественно, а на основании $\Phi = 0$.

Из первых двух равенств (32) следует

$$\Phi_1(\tau)\cdot\tau - \Phi_2(\tau) = 0,$$

или тождественно относительно $t$:

(33) $$\Phi_1(t)\cdot t - \Phi_2(t) = \mathcal{E}(t)\cdot\Phi(t),$$

где $\mathcal{E}(t)$ должеи быть линейным полиномом.

Дифференцируя его по $t$, получим

$$\Phi_{1t}(t)\cdot t - \Phi_{2t}(t) + \Phi_1(t) = \mathcal{E}_t(t)\cdot\Phi(t) + \mathcal{E}(t)\cdot\Phi_t(t),$$

откуда в силу $\Phi(\tau) = 0$

(34) $$\Phi_{1\tau}(\tau)\cdot\tau - \Phi_{2\tau}(\tau) + \Phi_1(\tau) = \mathcal{E}(\tau)\cdot\Phi_\tau(\tau).$$

С другой стороны, дифференцируем последнее равенство (32), где будем считать $\lambda$ функцией только от $p_\nu$, по $p_1$ и $p_2$:

$$\Phi_{1\tau} + \Phi_{\tau\tau} \cdot \frac{\partial \tau}{\partial p_1} = -\lambda_1 C - \lambda \left( C_1 + C_\tau \cdot \frac{\partial \tau}{\partial p_1} \right),$$

$$\Phi_{2\tau} + \Phi_{\tau\tau} \cdot \frac{\partial \tau}{\partial p_2} = -\lambda_2 C - \lambda \left( C_2 + C_\tau \cdot \frac{\partial \tau}{\partial p_2} \right).$$

Учитывая, что в силу первых двух равенств (16)

$$\frac{\partial \tau}{\partial p_2} - \frac{\partial \tau}{\partial p_1} \cdot \tau = 0, \tag{35}$$

мы получим, принимая также во внимание, что $C_1\tau - C_2 = N$ [(17′) при $\lambda = 1$, $\mu = 2$]:

$$\Phi_{1\tau} \cdot \tau - \Phi_{2\tau} = -C(\lambda_1 \tau - \lambda_2) - \lambda N. \tag{36}$$

Сопоставим (34), (36) и первое равенство (32):

$$\mathfrak{G}(\tau) = \frac{\lambda_1}{\lambda} \cdot \tau - \frac{\lambda_2}{\lambda}. \tag{37}$$

Нашей ближайшей целью будет доказательство, что равенство (37) есть тождество относительно $\tau$. Группа Галуа уравнения $\Phi(\tau) = 0$ в силу соотношений

$$\sum_{i,\,k} r_{ik} \theta_i^{(\mu)} \theta_k^{(\nu)} = 0 \qquad (\mu \neq \nu;\ \mu, \nu = 1, 2, \ldots, n),$$

$$\sum_{i,\,k} r_{ik} \theta_i^{(\mu)} \theta_k^{(\nu)} = 0 \qquad (\mu \neq \nu;\ \mu, \nu = n+1, n+2, \ldots, 2n)$$

импримитивна, причём системами импримитивности являются

$$1)\ \tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(n)}; \quad 2)\ \tau^{(n+1)}, \tau^{(n+2)}, \ldots, \tau^{(2n)}.$$

Здесь надо учесть, что величины $\theta_3, \ldots, \theta_n$ рационально выражаются через $\tau$, так как из (32) мы имеем:

$$\Phi_\nu = \theta_\nu \cdot \Phi_1 \qquad (\nu = 3, \ldots, n).$$

Возьмём функцию

$$\rho = [\tau^{(1)}]^k + [\tau^{(2)}]^k + \ldots + [\tau^{(n)}]^k - [\tau^{(n+1)}]^k - \ldots - [\tau^{(2n)}]^k, \tag{38}$$

где $k$ подберём так, чтобы она не обращалась в нуль. Функция $\rho$ не изменяется при подстановках группы Галуа, оставляющих системы импримитивности на месте, и меняет знак при подстановках, перемещающих системы импримитивности. Поскольку $\rho$ не меняется при всех подстановках группы Галуа, оставляющих на месте корень $\tau = \tau^{(1)}$, в силу теоремы Лагранжа $\rho$ рационально выражается через $\tau$:

$$\rho = \rho(\tau).$$

Введём при помощи равенства

$$\lambda(\tau) = \rho(\tau) \cdot \mu(\tau) \tag{39}$$

функцию $\mu(\tau)$. Можно считать, что $\rho(\tau)$ и $\mu(\tau)$ являются полиномами от $\tau$ не выше $(2n-1)$-й степени.

В силу условий 3) и представления (30) имеет место:

$$x_1 = \int \frac{d\tau^{(1)}}{N^{(1)}} + \ldots + \int \frac{d\tau^{(n)}}{N^{(n)}} = \int \frac{d\tau^{(n+1)}}{N^{(n+1)}} + \ldots + \int \frac{d\tau^{(2n)}}{N^{(2n)}}.$$

Дифференцируя по $p_1$, получим:

$$\frac{1}{N^{(1)}} \cdot \frac{\partial \tau^{(n)}}{\partial p_1} + \ldots + \frac{1}{N^{(n)}} \cdot \frac{\partial \tau^{(n)}}{\partial p_1} = \frac{1}{N^{(n+1)}} \cdot \frac{\partial \tau^{(n+1)}}{\partial p_1} + \ldots + \frac{1}{N^{(2n)}} \cdot \frac{\partial \tau^{(2n)}}{\partial p_1}. \tag{40}$$

Но из уравнения (20) следует:

$$\frac{\partial \tau^{(\nu)}}{\partial p_1} = \frac{N^{(\nu)}}{C^{(\nu)}} \qquad (\nu = 1, 2, \ldots, 2n).$$

Подставляя в (40), будем иметь:

$$\frac{1}{C^{(1)}} + \ldots + \frac{1}{C^{(n)}} = \frac{1}{C^{(n+1)}} + \ldots + \frac{1}{C^{(2n)}}. \tag{41}$$

Но из последней формулы (32) следует:

$$\frac{1}{C^{(\nu)}} = -\frac{\lambda(\tau^{(\nu)})}{\Phi_\tau(\tau^{(\nu)})} \qquad (\nu = 1, 2, \ldots, 2n).$$

Принимая во внимание (39) и учитывая, что

$$\rho(\tau^{(1)}) = \ldots = \rho(\tau^{(n)}) = -\rho(\tau^{(n+1)}) = \ldots = -\rho(\tau^{(2n)}), \tag{42}$$

мы после подстановки в (41) будем иметь

$$\frac{\mu(\tau^{(1)})}{\Phi_\tau(\tau^{(1)})} + \ldots + \frac{\mu(\tau^{(n)})}{\Phi_\tau(\tau^{(n)})} + \frac{\mu(\tau^{(n+1)})}{\Phi_\tau(\tau^{(n+1)})} + \ldots + \frac{\mu(\tau^{(2n)})}{\Phi_\tau(\tau^{(2n)})} = 0; \tag{43}$$

из этой формулы в силу известного свойства разложения рациональных дробей на частные дроби следует, что степень полинома $\mu(t)$ не превышает $2n-2$.

Берём логарифмическую производную от (39):

$$\begin{cases} \dfrac{\lambda_1(\tau)}{\lambda(\tau)} + \dfrac{\lambda_\tau(\tau)}{\lambda(\tau)} \cdot \dfrac{\partial \tau}{\partial p_1} = \left[\dfrac{\rho_1(\tau)}{\rho(\tau)} + \dfrac{\rho_\tau(\tau)}{\rho(\tau)} \cdot \dfrac{\partial \tau}{\partial p_1}\right] + \left[\dfrac{\mu_1(\tau)}{\mu(\tau)} + \dfrac{\mu_\tau(\tau)}{\mu(\tau)} \cdot \dfrac{\partial \tau}{\partial p_1}\right], \\ \dfrac{\lambda_2(\tau)}{\lambda(\tau)} + \dfrac{\lambda_\tau(\tau)}{\lambda(\tau)} \cdot \dfrac{\partial \tau}{\partial p_2} = \left[\dfrac{\rho_2(\tau)}{\rho(\tau)} + \dfrac{\rho_\tau(\tau)}{\rho(\tau)} \cdot \dfrac{\partial \tau}{\partial p_2}\right] + \left[\dfrac{\mu_2(\tau)}{\mu(\tau)} + \dfrac{\mu_\tau(\tau)}{\mu(\tau)} \cdot \dfrac{\partial \tau}{\partial p_2}\right]. \end{cases} \tag{44}$$

Из (42) следует, что выражения

$$\frac{\rho_1(\tau)}{\rho(\tau)} + \frac{\rho_\tau(\tau)}{\rho(\tau)} \cdot \frac{\partial \tau}{\partial p_1}, \quad \frac{\rho_2(\tau)}{\rho(\tau)} + \frac{\rho_\tau(\tau)}{\rho(\tau)} \cdot \frac{\partial \tau}{\partial p_2}$$

инвариантны от подстановок группы Галуа, а потому являются величинами области рациональности. Обозначая их через $a_1$, $a_2$, мы видим, что уравнения

$$\rho_1(t) - \rho(t) \cdot a_1 = 0, \quad \rho_2(t) - \rho(t) \cdot a_2 = 0,$$

будучи степеней не выше $2n-1$, имеют по $2n$ корней и потому являются тождествами.

Из (44) мы в силу (35) получим:

$$\frac{\lambda_1(\tau)}{\lambda(\tau)} \cdot \tau - \frac{\lambda_2(\tau)}{\lambda(\tau)} = (a_1\tau - a_2) + \frac{\mu_1(\tau)}{\mu(\tau)} \cdot \tau - \frac{\mu_2(\tau)}{\mu(\tau)}.$$

Подставляя в (37), будем иметь:

$$\mathfrak{G}(\tau) \cdot \mu(\tau) = (a_1\tau - a_2) \cdot \mu(\tau) + \mu_1(\tau) \cdot \tau - \mu_2(\tau). \tag{45}$$

Но так как степени полиномов $\mu(t)$, $\mu_1(t)$, $\mu_2(t)$ не превышают $2n-2$, то это уравнение, будучи степени $\leqslant 2n-1$, имеет $2n$ корней и потому является тождеством.

Рассмотрим функцию

$$\psi(t) = \frac{\Phi(t)}{\rho \cdot \mu(t)},$$

где будем считать $\rho$ функцией только от $p_1, p_2, \ldots, p_n$ (квадратным радикалом из величины области рациональности). Имеет место

$$\psi_1(t) \cdot t - \psi_2(t) = \frac{1}{\rho \cdot \mu(t)} \cdot [\Phi_1(t) \cdot t - \Phi_2(t)] - \frac{\Phi(t)}{\rho^2 \cdot \mu(t)} [\rho_1 t - \rho_2] -$$

$$- \frac{\Phi(t)}{\rho\mu^2(t)} [\mu_1(t) \cdot t - \mu_2(t)] =$$

$$= \frac{1}{\rho\mu(t)} \cdot \Phi(t) \cdot \mathfrak{G}(t) - \frac{\Phi(t)}{\rho\mu(t)}(a_1 t - a_2) - \frac{\Phi(t)}{\rho\mu(t)} \left[ \frac{\mu_1(t)}{\mu(t)} t - \frac{\mu_2(t)}{\mu(t)} \right] = 0$$

[в силу (45)]. Но левую часть можно представить как якобиан

$$\frac{\partial(\psi(t),\ p_1 + p_2 t)}{\partial(p_1,\ p_2)} = 0, \tag{46}$$

и таким образом $\psi(t)$ при неопределённом $t$ зависит только от $t$, $p_1 + p_2 t$, $p_3, \ldots, p_n$.

Разложим рациональную дробь $\psi(t)$ по убывающим степеням $t$. Обозначая степень $\mu(t)$ через $g$ ($g \leqslant 2n-2$), мы получим разложение

$$\psi(t) = a^{(2n-g)} \cdot t^{2n-g} + a^{(2n-g-1)} \cdot t^{2n-g-1} + \ldots, \tag{47}$$

сходящееся в некоторой области переменных $p_1, p_2, \ldots, p_n$. Подставляя это разложение в тождество (46), получим:

$$a_1^{(2n-g)} = 0, \quad a_1^{(2n-g-1)} = a_2^{(2n-g)}, \quad \ldots, \quad a_1^{(\nu-1)} = a_2^{(\nu)}, \ldots \tag{48}$$

Из этих соотношений следует, что $a^{(2n-g)}$ вовсе не содержит $p_1$, $a^{(2n-g-1)}$ содержит его лишь в первой степени, $a^{(2n-g-2)}$ во второй, и т. д.

Разложение (46) *рекуррентно*: существуют множители $A_0, A_1, \ldots, A_g$, пропорциональные коэффициентам полинома $\mu(t)$, которые связаны с коэффициентами разложения (47) так:

$$A_0 \cdot a^{(-i)} + A_1 \cdot a^{(i-1)} + \ldots + A_g \cdot a^{(-i-g)} = 0, \tag{49}$$

и справедливы при всех $i > 0$. Значения $A_0, A_1, \ldots, A_\rho$ могут быть определены из уравнений (49) с точностью до общего множителя: например, их можно взять равными минорам матрицы

$$\begin{Vmatrix} a^{(-i)}, & a^{(-i-1)}, \ldots, & a^{(-i-g)} \\ a^{(-i-1)}, & a^{(-i-2)}, \ldots, & a^{(-i-g-1)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a^{(-i-g+1)}, & a^{(-i-g)}, \ldots, & a^{(-i-2g+1)} \end{Vmatrix},$$

и тогда они будут рационально зависеть от $p_1$. Беря вместо $\mu(t)$ пропорциональный ему полином

$$M(t) = A_0 + A_1 t + \ldots + A_g \cdot t^g,$$

мы придём к полиному

$$\overline{\Phi}(t) = M(t) \cdot \psi(t),$$

пропорциональному полиному $\Phi(t)$, коэффициенты которого рационально зависят от $p_1$.

Для доказательства рациональной зависимости $\Phi(t)$ от $p_2$ разложим $\psi(t)$ по *возрастающим* степеням $t$ и станем рассуждать аналогично. Чтобы доказать это для переменной $p_3$, найдём уравнение $2n$-й степени, $\psi_3(t) = 0$, которому удовлетворяет $\theta_3$, пользуясь уравнениями

$$\Phi(\tau) = 0, \quad \Phi_1 \cdot \theta_3 - \Phi_3 = 0$$

(см. § 4, теорема 2). Его коэффициенты, очевидно, рационально зависят от $p_1$ и $p_2$. С другой стороны меняя ролями $\tau$ и $\theta_3$, мы придём к уравнению $2n$-й степени $\overline{\psi}(\theta_3) = 0$, имеющему те же корни, что и $\psi(\theta_3) = 0$, но у которого коэффициенты будут рационально зависеть от $p_1$ и $p_3$. Поскольку старшие коэффициенты обоих уравнений могут быть взяты равными 1, оба уравнения совпадают, и таким образом коэффициенты уравнения $\psi(\theta_3) = 0$ [а также и $\Phi(\tau) = 0$] рационально зависят от $p_1$, $p_2$, $p_3$ и т. д.

Исключая из уравнений

$$\begin{cases} \Phi(\tau) = 0, \quad \Phi_1 \cdot \theta_3 - \Phi_3 = 0, \quad \ldots, \quad \Phi_1 \cdot \theta_n - \Phi_n = 0, \\ \Phi_1 \cdot \zeta - \sum_{\nu=1}^{n} \Phi_\nu \cdot p_\nu = 0 \end{cases} \tag{50}$$

только одну из переменных $p_1, p_2, \ldots, p_n$, мы получим $n-1$ уравнений, в которые ни одна из переменных $p_1, p_2, \ldots, p_n$ не войдёт,

так как в силу нашего предположения $\theta_3, \ldots, \theta_n, \zeta$ должны быть вполне определёнными функциями от $\tau$. Таким образом мы придём к алгебраической кривой $L$ в $n$-мерном пространстве с координатами $\tau, \theta_3, \ldots, \theta_n, \zeta$.

Из

$$N(\tau) = \frac{\Phi_1(\tau)}{\lambda(\tau)} = \left(\frac{\Phi(\tau)}{\lambda(\tau)}\right)_1 = \psi_1(\tau)$$

и того, что $N(\tau)$ есть функция только от $\tau$, следует, что $\psi_1(\tau)$ может быть рационально выражена через $\tau, \theta_3, \ldots, \theta_n, \zeta$:

$$N(\tau) = \varphi(\tau, \theta_3, \ldots, \theta_n, \tau).$$

Подставляя в формулы (30) и (31), будем иметь:

$$(51)\quad x_\nu = \sum_{\mu=1}^{n} \int \frac{\theta_\nu^{(\mu)} \cdot d\tau^{(\mu)}}{\varphi(\tau^{(\mu)}, \ldots, \zeta^{(\mu)})} = -\sum_{\mu=n+1}^{2n} \int \frac{\theta_\nu^{(\mu)} \cdot d\tau^{(\mu)}}{\varphi(\tau^{(\mu)}, \ldots, \zeta^{(\mu)})} \quad (\nu = 1, 2, \ldots, n),$$

$$(52)\quad z = \sum_{\mu=1}^{n} \int \frac{\zeta^{(\mu)} \cdot d\tau^{(\mu)}}{\varphi(\tau^{(\mu)}, \ldots, \zeta^{(\mu)})} = -\sum_{\mu=n+1}^{2n} \int \frac{\zeta^{(\mu)} \cdot d\tau^{(\mu)}}{\varphi(\tau^{(\mu)}, \ldots, \zeta^{(\mu)})}.$$

Эти формулы показывают, что координаты гиперповерхности (1) выражаются как суммы абелевых интегралов.

Найдём жанр кривой $L$. Предварительно определим её порядок. Гиперплоскость

$$p_1 + p_2\tau + \ldots + p_n\theta_n - \zeta = 0$$

пересекает кривую $L$ в $2n$ точках $\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(2n)}$, которые можно найти, подставляя значения $p_1, p_2, \ldots, p_n$ в уравнение $\Phi(\tau) = 0$. Остальные координаты $\theta_3, \ldots, \theta_n$ однозначно получатся из уравнений (50). Таким образом порядок кривой $L$ равен $2n$.

Если перейти к терминологии арифметической теории, то можно сказать, что порядок элемента

$$(53)\qquad p_1 + p_2\tau + p_3\theta_3 + \ldots + p_n\theta_n - \zeta$$

(при постоянных $p_1, p_2, \ldots, p_n$) и, в частности, элементов

$$(54)\qquad \tau, \theta_3, \ldots, \theta_n \zeta$$

равен $2n$. Это показывает, что элементы (54) представляются в виде частных от дивизоров $2n$-го порядка, причём в их знаменателях стоит один и тот же дивизор

$$\tau \asymp \frac{A_2}{A_1}, \quad \theta_3 \asymp \frac{A_3}{A_1}, \quad \ldots, \quad \theta_n \asymp \frac{A_n}{A_1}, \quad \zeta = \frac{A_{n+1}}{A_1}.$$

Эти дивизоры линейно независимы, так как иначе всякая кривая лежала бы в какой-то гиперплоскости, и из формул (51) и (52) следовало бы, что и координаты $x_\nu$, $z$ гиперповерхности (1) лежат в гиперплоскости, что мы исключаем.

Таким образом измерение класса

$$\mathfrak{A} = (A_1, A_2, \ldots, A_{n+1})$$

равно по крайней мере $n+1$. Если класс $\mathfrak{A}$ не специален, то из теоремы Римана-Роха следует:

$$\rho = \text{Пор}\,\mathfrak{A} - \text{Изм}\,\mathfrak{A} + 1 \leqslant 2n - (n+1) + 1 = n. \tag{55}$$

Если же класс $\mathfrak{A}$ специален, то из теоремы Клиффорда (§ 26, теорема 47) вытекает, что $\rho = n+1$ и что класс $\mathfrak{A}$ совпадает с классом $\mathfrak{W}$ дифференциалов поля. Исключение представляет только случай гиперэллиптических полей.

Докажем, что в случае $\rho = n+1$ все интегралы, входящие в формулы (51) и (52), являются интегралами 1-го рода. Допустим противное: пусть интеграл

$$\int \frac{\theta_k \cdot d\tau}{\varphi} \tag{56}$$

обращается в точке $P_0$ в бесконечность. Не нарушая общности, можно предположить, что $A_1$ не делится на $P_0$, так как в противном случае мы могли бы взять в роли $p_1$ другую из переменных $p_\nu$. Подберём значения $p_1, p_2, \ldots, p_n$ так, чтобы элемент (53) делился на $P_0$ точно в первой степени. Это всегда возможно в случае негиперэллиптического поля. В самом деле, в противном случае все линейные комбинации дивизоров класса $\mathfrak{W}$, делящиеся на $P_0$, делились бы на $P_0^2$, а это означало бы, что

$$\text{Изм}\left(\frac{\mathfrak{W}}{P_0^2}\right) = \text{Изм}\left(\frac{\mathfrak{W}}{P_0}\right). \tag{57}$$

Но из теоремы Римана-Роха следует

$$\text{Изм}\left(\frac{\mathfrak{W}}{P_0^2}\right) - \frac{1}{2}\,\text{Пор}\left(\frac{\mathfrak{W}}{P_0^2}\right) = \text{Изм}\,(P_0^2) - \frac{1}{2}\,\text{Пор}\,(P_0^2),$$

и при соблюдении (57) мы бы имели

$$\rho - 1 - \frac{1}{2}(2\rho - 4) = \text{Изм}\,P_0^2 - \frac{1}{2}\cdot 2,$$

т. е.

$$\text{Изм}\,(P_0^2) = 2,$$

а это возможно только в случае гиперэллиптического поля. Кроме того, распорядимся константами $p_1, p_2, \ldots, p_n$ так, чтобы элементы (53) не обращались в нуль ни в какой другой бесконечной точке интеграла (53).

Возьмём выбранный таким образом элемент $z$ за независимую переменную. Можно переписать $k$-ю из формул (51) так:

$$\sum_{\mu=1}^{2n} \int \frac{\theta_k^{\mu} \cdot d\tau^{(\mu)}}{\varphi(\tau^{(\mu)}, \ldots, \zeta^{(\mu)})} = 0. \tag{57'}$$

В силу выбора $z$ верхние пределы входящих в эту сумму интегралов являются нулями функции $z - z_0$, где $z_0$ произвольно, и, соответственно меняя пути интегрирования, мы получим отсюда

$$\sum_{\mu=1}^{2n} \int^{z_0} F(z, w)\, dz \equiv 0,$$

где

$$\int F(x, w)\, dz = \int \frac{\theta_k\, d\tau}{\varphi(\tau, \ldots, \zeta)}. \tag{58}$$

В силу произвольности $z_0$ отсюда следует:

$$S\{F(z, w)\} = 0. \tag{59}$$

Пусть

$$P_0, P_0^{(2)}, \ldots, P_0^{(2n)} \tag{60}$$

будут все точки, в которых $z$ обращается в нуль. Согласно условию, интеграл (58) обращается в бесконечность только в первой из точек (60). Но так как в силу нашего условия $z$ обращается в $P_0$ в нуль 1-й кратности, то $F(z, w)$ в точке $P_0$ обращается в бесконечность не медленнее, чем $\frac{1}{z}$. С другой стороны, в каждой из точек $P_0^{(\nu)}$ $(\nu = 2, 3, \ldots, n)$ $F(z, w)$ обращается в бесконечность не быстрее, чем $z^{-\frac{a_\nu - 1}{a_\nu}}$, где $a_\nu$ — кратность нуля в точке $P_0^{(\nu)}$. Таким образом сумма сопряжённых значений $F(z, w)$, т. е. след $S\{F(z, w)\}$, должна при $z = 0$ обращаться в бесконечность. Это, однако, противоречит равенству (59), и наше утверждение доказано.

В случае $p < n + 1$, когда класс $\mathfrak{A}$ не специален, входящие в формулы (51) и (52) интегралы могут быть интегралами 3-го рода.

В случае гиперэллиптического поля неравенство $p \leqslant n + 1$ может и не иметь места. Всякий гиперэллиптический интеграл может быть представлен в форме

$$\int \frac{M(\xi) + N(\xi)\sqrt{R(\xi)}}{Q(\xi) \cdot \sqrt{R(\xi)}} \cdot d\xi = \int \frac{M(\xi)}{Q(\xi)} \cdot \frac{d\xi}{\sqrt{R(\xi)}} + \int \frac{N(\xi)}{Q(\xi)} \cdot d\xi, \tag{61}$$

где $M(\xi)$, $N(\xi)$, $Q(\xi)$, $R(\xi)$ — полиномы. Первый из интегралов этой суммы может всегда служить для представления (51), (52) координат гиперповерхностей переноса. Для таких интегралов всегда

имеет место теорема Абеля в форме (57′), так как каждому значению $\xi$ соответствуют два противоположных значения интеграла

$$\int \frac{M \cdot d\xi}{Q \cdot \sqrt{R}},$$

которые при суммировании уничтожаются. Однако два различных представления координат в виде сумм (51), (52) в этом случае различны только формально.

Что касается до второго из интегралов суммы (61), то он относится к случаю $\rho = 0$. Примеры (см. ниже, Упражнения) показывают, что такие интегралы могут давать начало гиперповерхностям с двумя системами линий переноса.

*Пример.* Разберём поверхность

$$xyz + x + y + z = 0, \tag{62}$$

рассмотренную в предыдущем параграфе. Имеем

$$z = -\frac{x+y}{xy+1}, \quad p = \frac{y^2-1}{(xy+1)^2}, \quad q = \frac{x^2-1}{(xy+1)^2},$$
$$r = -\frac{2y(y^2-1)}{(xy+1)^3}, \quad s = \frac{2(x+y)}{(xy+1)^3}, \quad t = -\frac{2x(x^2-1)}{(xy+1)^3},$$

так что уравнения (5) и (6) принимают вид

$$(y^2-1) + (x^2-1)\cdot\tau - (xy+1)^2\cdot\zeta = 0, \tag{63}$$

$$-2y(y^2-1) + 4(x+y)\tau - 2x(x^2-1)\tau^2 + \{x^2-1-(xy+1)^2\zeta'\}(xy+1)\psi = 0. \tag{64}$$

Алгебраические поверхности удобнее исследовать алгебраически, и потому мы не будем составлять уравнения в полных дифференциалах, а обратим внимание на то, что уравнения (63), (64) должны удовлетворяться при постоянных значениях $\tau$ и $\zeta$ вдоль линий переноса, в силу чего из них не должны определяться $x, y$. Другими словами, какое значение мы бы ни придали переменной $x$ (или $y$), полученные из (5) и (6) уравнения должны иметь общее решение. Это определит зависимости между $\tau$, $\zeta$, $\zeta'$, $\psi$.

I. Положим $x = \infty$. Уравнения (63) и (64) примут вид

$$\tau - y^2\zeta = 0, \quad -2\tau^2 - y^3\zeta'\psi + y\psi = 0.$$

Чтобы они были совместны, должно быть:

$$\psi = \frac{2\tau^{5/3}\cdot\zeta^{5/3}}{\zeta - \tau\zeta'}.$$

II. Полагая $y = \infty$, получим:

$$\psi = -\frac{2\zeta^{5/3}}{\zeta'}.$$

III. Полагая $x=1$, будем иметь:

$$-(1+\zeta)\zeta+(1-\zeta)^2\cdot\tau-\zeta'\psi=0.$$

Исключая из этих соотношений $\zeta'$ и $\psi$, получим

$$\tau=\frac{\zeta}{(\sqrt{\zeta}+1)^2},$$

или, вводя новые параметры по формулам

$$\tau=\theta^2,\quad \zeta=\xi^2,$$

$$\theta=\frac{\xi}{\xi+1},\qquad \xi=\frac{\theta}{1-\theta}.$$

Подставляя это выражение в уравнение (63), получим:

$$(x^2-1)\theta^4-2(x^2-1)\theta^3+[(x^2-1)+(y^2-1)+(xy+1)^2]\theta^2-2(y^2-1)\theta+(y^2-1)=0.$$

Это уравнение показывает, что для каждой точки поверхности можно найти 4 и только 4 значения $\theta$, откуда видно, что она допускает только 4 системы линий переноса. Значения $\theta$ попарно связаны соотношениями (15)

$$y(y^2-1)-(x+y)(\theta_1^2+\theta_2^2)+x(x^2-1)\theta_1^2\theta_2^2=0,$$

$$y(y^2-1)-(x+y)(\theta_3^2+\theta_4^2)+x(x^2-1)\theta_3^2\theta_4^2=0.$$

Мы видели в § 51, что одна пара систем линий переноса существует. Здесь мы видим, что может существовать и другая, но тогда соответствующие ей значения $\theta_3$, $\theta_4$ получаются из таких же уравнений, что и $\theta_1, \theta_2$, и потому соответствующее им представление координат поверхности должно иметь ту же форму, что и представление (13) § 51, т. е. состоять из дробных линейных функций, и может отличаться только числовыми коэффициентами. Поверхность (12) § 51 переходит в нашу поверхность путём подстановки типа

$$\xi_1=\alpha x,\quad \xi_2=\beta y,\quad \xi_3=\gamma x.$$

Таким образом сделанная нами в § 51 гипотеза полностью доказана. Получить же из полученных нами уравнений представление координат поверхности мы предоставим читателю.

## § 52. Принцип соответствия

Проблема обращения абелевых интегралов дала толчок к возникновению трансцендентного метода, связанного с $\theta$-функциями, который оказался плодотворным в некоторых чисто алгебраических вопросах. К их числу относится так называемый принцип *соответствия*, который был предложен Шалем (Chasles) для кривых жанра нуль,

распространён Кэли (A. Cayley) на кривые любого жанра и впервые доказан Бриллем (A. Brill) [23, 24]. Он состоит в следующем. Пусть между координатами $x_1$, $y_1$ и $x_2$, $y_2$ двух точек алгебраической кривой

$$f(x, y) = 0 \tag{1}$$

жанра $p$ имеет место алгебраическое соотношение

$$\Psi(x_1, y_1; x_2, y_2) = 0, \tag{2}$$

в силу которого точке $(x_1, y_1)$ соответствует $\alpha$ подвижных точек $(x_2, y_2)$, а каждой точке $(x_2, y_2)$ — $\beta$ точек $(x_1, y_1)$. Тогда точки $(x_1, y_1)$ и $(x_2, y_2)$ совпадают в

$$C = \alpha + \beta + 2p\gamma$$

местах на кривой (1), где $\gamma$ — целое число, называемое «весом» (Wertigkeit) соответствия (2).

Гурвиц [55], применив трансцендентный метод, произвёл исчерпывающий обзор всех возможных соответствий, обнаружив существование соответствий с отрицательным весом, а также *особенных соответствий*. Приведём его основные рассуждения.

Пусть заданное соответствие относит каждой точке $P$ поля $k(x, y)$ точки $Q', Q'', \ldots, Q^{(\alpha)}$ того же поля и пусть

$$u_1(P),\ u_2(P),\ \ldots,\ u_p(P)$$

— система нормированных интегралов 1-го рода, периоды которых вдоль сечений $B_\nu$ представляются матрицей

$$\|a_{\mu\nu}\|.$$

Суммы

$$u_\nu(Q') + u_\nu(Q'') + \ldots + u_\nu(Q^{(\alpha)}) \qquad (\nu = 1, 2, \ldots, p) \tag{3}$$

являются однозначными и всюду конечными функциями точки $P$ на рассечённой римановой поверхности. Если точка $P$ совершит замкнутый путь, то точки $Q', Q'', \ldots, Q^{(\alpha)}$ лишь переставятся между собой, и суммы (3) лишь получат постоянные перемещения (периоды). Поэтому суммы (3) тоже являются интегралами 1-го рода, т. е. линейно (с постоянными коэффициентами) выражаются через $u_\nu(P)$:

$$\sum_{\mu=1}^{\alpha} u_\nu(Q^{(\mu)}) = \sum_{\lambda=1}^{p} \pi_{\nu\lambda} \cdot u_\lambda(P) + \pi_\nu \qquad (\nu = 1, 2, \ldots, p). \tag{4}$$

Если $P$ опишет путь вдоль $B_\sigma$, то в силу формулы (6) § 46 правая часть приобретёт приращение $-\pi_{\nu\sigma}$, в то время как левая увеличится на некоторую целую кратность периодов. Таким образом

$$\pi_{\nu\sigma} = h_{\nu\sigma} + \sum_{\mu=1}^{p} g_{\mu\sigma} a_{\nu\mu} \qquad (\nu, \sigma = 1, 2, \ldots, p), \tag{5}$$

где $h_{\nu\sigma}$, $g_{\mu\sigma}$ — некоторые целые числа. Описывая точкой $P$ путь вдоль $A_\sigma$, мы точно так же в силу формулы (5) § 46 получим:

$$(6)\qquad \sum_{\lambda=1}^{\rho} \pi_{\nu\lambda} \cdot a_{\lambda\sigma} = H_{\nu\sigma} + \sum_{\mu=1}^{\rho} G_{\mu\sigma} a_{\nu\mu} \qquad (\nu, \sigma = 1, 2, \ldots, \rho).$$

Исключая из формулы (5) и (6) величины $\pi_{\nu\sigma}$, будем иметь:

$$(7)\qquad \sum_{\lambda=1}^{\rho} h_{\nu\lambda} a_{\lambda\sigma} + \sum_{\lambda,\,\mu}^{1\ldots\rho} g_{\mu\lambda} a_{\nu\mu} a_{\lambda\sigma} = H_{\nu\sigma} + \sum_{\mu=1}^{\rho} G_{\mu\sigma} a_{\nu\mu} \quad (\nu, \sigma = 1, 2, \ldots, \rho).$$

Будем называть соответствие *обыкновенным* (или *весовым*), если для него равенства (7) удовлетворяются тождественно относительно периодов $a_{\nu\sigma}$; в противном случае соответствие будет называться *особым*. В случае обыкновенного соответствия имеет место:

$$H_{\nu\sigma} = 0,\ g_{\mu\nu} = 0 \qquad (\nu, \sigma, \mu = 1, 2, \ldots, \rho),$$

$$h_{\nu\lambda} = 0\ (\nu \neq \lambda);\quad G_{\mu\sigma} = 0\ (\mu \neq \sigma) \quad (\nu, \lambda, \mu, \sigma = 1, 2, \ldots, \rho),$$

$$h_{11} = h_{22} = \ldots = h_{\rho\rho} = G_{11} = G_{22} = \ldots = G_{\rho\rho}.$$

Если обозначить последнее общее целое число через $-\gamma$, то формулы (4) примут вид

$$(8)\qquad \sum_{\mu=1}^{\alpha} u_\nu(Q^{(\mu)}) + \gamma \cdot u_\nu(P) = \pi_\nu \qquad (\nu = 1, 2, \ldots, \rho).$$

Число $\gamma$ и называется *весом* соответствия.

Для соответствий с положительным весом ($\gamma > 0$) Гурвиц определяет алгебраическое соотношение между функциями $P$ и $Q$ при помощи $\vartheta$-функций. Для этого он наряду с переменной точкой $P$ и соответствующими ей точками $Q', Q'', \ldots, Q^{(\alpha)}$ вводит соответствующие друг другу постоянные точки $P_0$; $Q_0', Q_0'', \ldots, Q_0^{(\alpha)}$, а также независимую переменную точку $Q$. Определяются константы $c_1, c_2, \ldots, c_\rho$ так, чтобы функция

$$(9)\qquad \vartheta\,[u_\nu(P) - u_\nu(Q) - c_\nu]$$

обращалась в нуль при $P = Q$ (в силу теоремы 95; для этого надо положить

$$c_\nu = \sum_{\mu=1}^{\rho-1} u_\nu(R^{(\mu)}) - k_\nu \qquad (\nu = 1, 2, \ldots, \rho),$$

где $R', R'', \ldots, R^{(\rho-1)}$ — совершенно произвольные точки; таким образом значения $c_\nu$ не зависят ни от $P$, ни от $Q$). Кроме того, функция (9) обращается в нуль в точках $R', R'', \ldots, R^{(\rho-1)}$, зависящих только от выбора констант $c_\nu$, но не от $Q$. Функция

$$(10)\qquad C(P, Q) = \prod_{\mu=1}^{\alpha} \frac{\vartheta\,[u_\nu(Q) - u_\nu(Q^{(\mu)}) - c_\nu]}{\vartheta\,[u_\nu(Q_0) - u_\nu(Q^{(\mu)}) - c_\nu] \cdot \vartheta\,[u_\nu(Q) - u_\nu(Q_0^{(\mu)}) - c_\nu]}$$

как функция от $Q$ обращается в нуль только в точках $Q = Q^{(\mu)}$ и в бесконечность только в точках $Q = Q_0^{(\mu)}$; в точках же $R', R'', \ldots, R^{(\rho-1)}$ и числитель и знаменатель имеют нули $\alpha$-й кратности. Она зависит от $P$, поскольку от $P$ зависят точки $Q^{(\mu)}$. Далее, функция

$$(11)\quad F(P, Q) = C(P \cdot Q) \cdot \left[\frac{\vartheta\,[u_\nu(Q) - u_\nu(P) - c_\nu]}{\vartheta\,[u_\nu(Q) - u_\nu(P_0) - c_\nu]\,\vartheta\,[u_\nu(Q_0) - u_0(P) - c_\nu]}\right]^\gamma$$

при обходе точкой $Q$ замкнутого контура на римановой поверхности в силу формулы (5) § 49 приобретает множитель:

если замкнутый контур пересекает $A_\nu$, то

$$e^{-\pi i\alpha_\nu a_{\nu\nu} - 2\pi i \sum_{\mu=1}^{\alpha} [u_\nu(Q) - u_\nu(Q^{(\mu)}) - e_\nu] + \pi i \alpha_\nu a_{\nu\nu} + 2\pi i \sum_{\mu=1}^{\alpha} [u_\nu(Q) - u_\nu(Q_0^{(\mu)}) - e_\nu]} \times$$

$$\times\, e^{-\pi i\gamma a_{\nu\nu} - 2\pi i\gamma [u_\nu(Q) - u_\nu(P)] + \pi i\gamma a_{\nu\nu} + 2\pi i [u_\nu(Q) - u_\nu(P_0)]} = (-1)^{2\pi i\alpha_\nu - 2\pi i\gamma_\nu} = 1$$

[последнее в силу (8)];

если замкнутый контур пересекает $A_\nu$, то этот множитель равен 1 в силу того, что $\vartheta$-функции имеют период 1 относительно всякого своего аргумента.

Из этого следует, что функция $F(P, Q)$ однозначна на нерассечённой римановой поверхности, а потому является алгебраической относительно $Q$. Как функция от точки $P$, от которой также однозначно зависит система точек $Q', Q'', \ldots, Q^{(\alpha)}$, она при замкнутых обходах могла бы приобретать множители типа

$$e^{2\pi i \sum_{\nu=1}^{\rho} M_\nu [u_\nu(Q) - u_\nu(Q_0)]},$$

где $M_\nu$ — некоторые целые числа. Но так как такие множители при $M_\nu \neq 0$ содержат $Q$ трансцендентным образом, а функция $F(P, Q)$ алгебраическая относительно $Q$ как до, так и после обхода точкой $P$ коитуров, то необходимо должно быть

$$M_\nu = 0,$$

так что функция $F(P, Q)$ алгебраически зависит и от $P$ и от $Q$.

Теорема 99. *Всякое весовое соответствие веса $\gamma$ двух точек $P, Q$ на римановой поверхности может быть представлено уравнением*

$$(12)\qquad F(P, Q) = 0.$$

*Если мы фиксируем точку $P$* (или $Q$), *то левая часть* (12) *как функция от $Q$* (или *от $P$*) *имеет нули первой кратности в точках $Q', Q'', \ldots, Q^{(\alpha)}$* (*или в каких-либо точках $P', P'', \ldots, P^{(\beta)}$*) *и, кроме того, нуль $\gamma$-й кратности в точке $P$* (*или в точке $Q$*); *в точках же $Q_0', Q_0'', \ldots, Q_0^{(\alpha)}$* (или в $P_0', P_0'', \ldots, P_0^{(\beta)}$) *она имеет простые, а в точке $P_0$* (или в $Q_0$) — *$\gamma$-кратную бесконечность.*

Ясно, что в случае $\gamma < 0$ вместо «$\gamma$-кратный нуль» следует сказать: $(-\gamma)$-кратная бесконечность, и обратно.

Теорема 99 даёт возможность определить все соответствия алгебраически, если задано уравнение (12), определяющее все соответствия. Мы убедимся в этом на примерах, которые будут даны ниже.

Для доказательства принципа соответствия Гурвиц рассматривает функцию

$$F(P) = \left[\frac{F(P, Q)}{\vartheta[u_\nu(Q) - u_\nu(P)]^\gamma}\right]_{Q=P}. \tag{13}$$

Эта функция, в силу теоремы 99, не обращается при $Q = P$ ни в нуль, ни в бесконечность. Если мы заставим обе точки $P$, $Q$ обойти один и тот же замкнутый контур на римановой поверхности, находясь всё время на бесконечно близком расстоянии, то и числитель и знаменатель не претерпят изменений. Поэтому $F(P)$ есть алгебраическая функция от $P$. Она будет обращаться в нуль всякий раз, когда $P$ совпадёт с одной из точек $Q', Q'', \ldots, Q^{(\alpha)}$, определяемых из уравнения (12) при подстановке данного значения $P$. Поэтому число её нулей равно искомому числу $C$ «совпадений», каждое из которых надо считать число раз, равное кратности нуля $P = Q^{(\nu)}$ уравнения (12). С другой стороны, из формул (10), (11) и (13) следует, что функция $F(P)$ имеет простые бесконечности в точках $Q_0', Q_0'', \ldots, Q_0^{(\alpha)}$ и в тех $\beta$ точках $P$, из соответствующих которым точек $Q', Q'', \ldots, Q^{(\alpha)}$ хоть одна совпадёт с $P_0 = Q_0$. Кроме того, она ещё имеет $\gamma$-кратные бесконечности в точках, обращающих в нуль одну из функций

$$\vartheta[u_\nu(P) - u_\nu(P_0) - c_\nu], \quad \vartheta[u_\nu(Q_0) - u_\nu(P) - c_\nu].$$

Их всего $2\rho\gamma$. Но алгебраическая функция имеет столько же нулей, сколько и бесконечностей, откуда

$$\boxed{C = \alpha + \beta + 2\rho\gamma.} \tag{14}$$

Эта формула и выражает принцип соответствия Кэли-Брилля.

Для уяснения способа пользования этим принципом приведём несколько примеров, заимствованных из прекрасной книги Цейтена (H. G. Zeuthen) [115].

*Пример* 1. Пусть поле $k(x, y)$ порождено кривой порядка $n$ и жанра $\rho$, имеющей $d$ особых (двойных) точек и $e$ точек возврата. Пусть $n'$ будет *класс* этой кривой (т. е. число различных касательных, проводимых к ней из точки вне её), $d'$ — число её двойных касательных и $e'$ — число точек перегиба (т. е. стационарных касательных). Рассмотрим соответствие между точками пересечения нашей кривой с прямой, проходящей через постоянную точку $A$ вне кривой. Тогда точке $P$ соответствует $n - 1$ остальных точек пересече-

ния $Q^{(\mu)}$ кривой с прямой $AP$, в силу чего $\alpha = \beta = n - 1$. $F(P, Q)$ есть левая часть уравнения прямой $AP$. Поскольку $AP$ в точке $P$ имеет простой нуль, мы имеем $\gamma = 1$. Точками совпадения являются точки касания касательных, проведённых к кривой из точки $A$ числом $n'$, а также особые точки кривой. Но двойная точка не должна считаться совпадением, так как ей соответствуют две разные точки поля. Точке же возврата соответствует одна точка поля, и её нужно считать совпадением. Таким образом $C = n' + e$, и формула (14) даёт:

$$n' + e = 2(n-1) + 2\rho. \tag{15}$$

*Пример* 2. Кривая та же, что в примере 1. Рассмотрим соответствие между точкой $P$ и остальными точками пересечения $Q^{(\mu)}$ кривой с касательной в точке $P$. Имеем $\alpha = n - 2$. С другой стороны, точке $Q^{(\mu)}$ соответствуют точки касания касательных к кривой, проведённых из точки $Q^{(\mu)}$, исключая касательной в самой точке $Q^{(\mu)}$; эту касательную нужно рассматривать как линию совпадения двух касательных и кривой, проведённых из близкой к $Q^{(\mu)}$ точки; отсюда $\beta = n' - 2$. Поскольку $F(P, Q)$ есть левая часть уравнения касательной к кривой, она в точке $P = Q$ имеет нуль второго порядка, в силу чего $\gamma = 2$. Точками совпадения служат точки перегиба, в которых совпадают не две, а три точки пересечения кривой с секущей, и точки возврата. Таким образом $C = e + e'$, и из формулы (14) следует

$$e + e' = n + n' + 4(\rho - 1). \tag{16}$$

Для получения соответствия с отрицательным весом введём понятие *композиции соответствий*. Пусть соответствие $S_1$ устаиовлено между точками $P$ и $Q$, причём каждой точке $P$ (соответственно $Q$) соответствует $\alpha$ (соответственно $\beta$) точек $Q$ (соответственно $P$). Кроме того, пусть соответствие $S_2$ заставляет каждой точке $R$ (соответственно $Q$) соответствовать $\alpha'$ (соответственно $\beta'$) точек $Q$ (соответственно $R$). Пусть веса этих соответствий будут $\gamma$ и $\gamma'$. Под композицией $S_1 S_2$ этих соответствий мы будем разуметь соответствие между точками $P$ и $R$. Очевидно, что каждой точке $P$ будет соответствовать $\alpha\beta'$ точек $R$, а каждой точке $R$ — $\alpha'\beta$ точек $P$. Кроме того, из равенств (8)

$$\sum_{\mu=1}^{\alpha} u_\nu(Q^{(\mu)}) + \gamma u_\nu(p) = \pi_\nu \qquad (\nu = 1, 2, \ldots, \rho), \tag{17}$$

$$\sum_{\mu=1}^{\beta'} u_\nu(R^{(\mu)}) + \gamma' u_\nu(Q) = \pi'_\nu \qquad (\nu = 1, 2, \ldots, \rho) \tag{18}$$

мы получим:

$$\sum_{\sigma=1}^{\alpha} \sum_{\mu=1}^{\beta'} u_\nu(R^{(\mu,\sigma)}) = \alpha\pi'_\nu - \gamma' \sum_{\sigma=1}^{\alpha} u_\nu(Q^{(\sigma)}) = \alpha\pi'_\nu - \gamma'\pi_\nu + \gamma\gamma' u_\nu(P). \tag{19}$$

Здесь под $R^{(\mu,\sigma)}$ мы разумеем $\mu$-ю из точек $R$, соответствующих точке $Q^{(\sigma)}$. Из (19) мы видим, что вес соответствия $S_1S_2$ равен $-\gamma\gamma'$. В частности, если веса соответствий $S_1$ и $S_2$ положительны, вес соответствия $S_1S_2$ отрицателен.

*Пример* 3. Рассмотрим композицию двух соответствий типа, разобранного в примере 1, причём пусть прямые первого (второго) соответствия проходят через постоянную точку $A(A')$. Другими словами, для получения точек $R$, соответствующих точке $P$, соединим $P$ с $A$ прямой, затем каждую из $n-1$ остальных точек $Q^{(\sigma)}$ пересечения $AP$ с кривой соединим с $A'$, и прямые $AQ^{(\sigma)}$ в пересечении с кривой и дадут искомые точки $R^{(\mu,\sigma)}$. Это соответствие в силу доказанного выше имеет числа

$$\alpha=\beta=(n-1)^2,\quad \gamma=-1,$$

и для числа совпадений мы получим выражение

$$C=2(n-1)^2-2\rho.$$

В этом соответствии совпадения получаются, во-первых, если $P$ попадёт в одну из $n$ точек пересечения прямой $AA'$ с кривой. Чтобы определить кратность такого совпадения, возьмём точку $P$ близко от одного из этих пересечений. Тогда каждая из $n-1$ секущих $A'Q^{(\mu)}$ будет близка к $AA'$, а потому на ней одна из точек пересечения с кривой будет близка к $P$. Таким образом каждая из точек пересечения $AA'$ с кривой даёт $n$-кратное совпадение. Во-вторых, совпадения получатся, если $P$ попадёт в двойную точку или точку возврата кривой. Каждая из этих точек даёт двойное совпадение: двойная точка потому, что ей соответствуют две точки поля; точка же возврата потому, что, взяв точку $P$ близко к точке возврата $P_0$, мы получим второе близкое к ней пересечение $Q'$ с прямой $AP$, причём порядок малости $PQ'$ будет в $\frac{3}{2}$ выше порядка малости $PP_0$; далее, секущая $A'Q'$ пересечёт кривую в другой точке $R$, близкой к $P_0$, и порядок малости $PR$ будет вдвое выше порядка малости $PP_0$.

Таким образом

$$n(n-1)+2d+2e=2(n-1)^2-2\rho,$$

откуда получается известная в алгебраической геометрии формула

$$\rho=\frac{1}{2}(n-1)(n-2)-d-e. \tag{20}$$

Кроме рассмотренной композиции (умножения) соответствий, иногда удобно рассматривать *сложение соответствий*. Если $S$ относит точке $P$ точки $Q^{(\mu)}$, а $S_2$ — той же точке точки $R^{(\nu)}$, то *сумма соответствий* $S_1+S_2$, по определению, относит точке $P$ всю совокупность точек $Q^{(\mu)}$, $R^{(\nu)}$. Если для $S_1$ ($S_2$) числа $\alpha$, $\beta$, $\gamma$ равны $\alpha_1$,

$\beta_1$, $\gamma_1$ ($\alpha_2$, $\beta_2$, $\gamma_2$), то для суммы $S_1 + S_2$ $\alpha = \alpha_1 + \alpha_2$ ($\beta$ мы не будем определять) $\gamma = \gamma_1 + \gamma_2$.

*Пример* 4. Будем относить каждой точке $P$ кривой совокупность точек пересечения с кривой всех касательных, проведённых из $P$, как из внешней точки (т. е. исключая касательную, касающуюся кривой в точке $P$). Последнюю касательную надо считать двойной, так как при приближении $P$ извне к кривой две из касательных из точки $P$ к кривой сливаются в одну. Поэтому из $P$ на кривой можно провести $n'-2$ касательных и каждая пересечёт кривую, кроме $P$ и точек касания $R^{(\nu)}$, ещё в $n-3$ точках $Q^{(\sigma,\nu)}$. С другой стороны, это соответствие взаимное (симметричное), так что для него

$$\alpha = \beta = (n'-2)(n-3).$$

Для определения его веса учтём, что точки $Q^{(\sigma,\nu)}$ являются пересечением заданной кривой с кривой

$$l_1 \cdot l_2 \ldots l_{n-2} = 0, \tag{21}$$

где $l_\nu = 0$ — уравнение $\nu$-й касательной из точки $P$ к заданной кривой. Кривая (21) имеет в $P$ $(n'-2)$-кратную точку. Но кривая (21) имеет ещё в каждой из точек касания $R^{(\nu)}$ двойное пересечение, так что соответствие, относящее $P$ все точки пересечения заданной кривой с (21), следует рассматривать как сумму нашего соответствия с двумя соответствиями, обратными к рассмотренным в примере 2. Таким образом для нашего соответствия

$$\gamma = (n'-2) - 2 \cdot 2 = n' - 6.$$

Отсюда

$$C = 2(n'-2)(n-3) + 2\rho(n'-6).$$

С другой стороны, в нашем соответствии совпадения складываются из: 1) положений точки $P$ в $2d'$ точках касания двойных касательных; 2) положений точки $P$ в точках возврата; поскольку из каждой точки возврата можно провести к кривой $n'-3$ касательных, отличных от касательной в точке возврата, и каждая из этих касательных имеет с точкой возврата двойное пересечение, т. е. совпадение $P$ с точкой $Q^{(\sigma,\nu)}$, в точках возврата произойдёт $(n'-3)$-кратное совпадение. Поэтому

$$2d' + e(n'-3) = 2(n'-2)(n-3) + 2\rho(n'-6). \tag{22}$$

Полученные нами формулы (15), (16), (20) и (22) носят название формул Плюккера (Plücker). Применим их к примеру, рассмотренному в § 50 (пример 2). Для кривой 4-го порядка без особых точек

$$n = 4, \quad d = e = 0.$$

Из формулы (20) имеем:

$$\rho = \frac{1}{2}(4-1)(4-2) = 3. \tag{23}$$

В силу (15) класс кривой равен

$$n' = 2(4-1) + 2\cdot 3 = 12. \tag{24}$$

В силу (16) число точек перегиба равно:

$$e' = 4 + 12 + 4(3-1) = 24. \tag{25}$$

Наконец, в силу (22) число двойных касательных равно:

$$d' = (12-2)(4-3) + 3(12-6) = 28.$$

Особенный интерес представляют исследования Гурвицем особых соответствий. Из формулы (7) следует, что особое соответствие может быть установлено только для полей, периоды которых связаны квадратичными соотношениями с целыми коэффициентами типа (7). Такого рода поля Гурвиц также называет особыми. Гурвиц также показал, что, обратно, для всякого особого поля можно установить особое соответствие. Для этого он, исходя из формул (7), определяет при помощи формул (6) величины $\pi_{\nu\lambda}$. Затем, полагая $\alpha = \rho$, он выбирает величины $\pi_\nu$ так, чтобы равенство

$$\vartheta\left[u_\nu(R) - \sum_{\lambda=1}^{\rho} \pi_{\nu\lambda}\cdot u_\lambda(P) - \pi_k - k_\nu\right] = 0$$

не при всех значениях $P$ имело место тождественно относительно точки $R$. Тогда точки $Q', Q'', \ldots, Q^{(\rho)}$ однозначно определятся из уравнений (4) как решение проблемы обращения.

Соответствия отрицательного веса, а также особые соответствия в общем случае не могут быть представлены одним алгебраическим соотношением типа (12). Гурвиц показывает, что их можно представить *двумя* соотношениями. Для этого он представляет эти соответствия в виде композиции двух соответствий положительного веса.

Вопрос о соответствиях с арифметической точки зрения был в недавнее время рассмотрен Дойрингом (M. Deuring) [33].

## § 53. Приведение абелевых интегралов к интегралам в полях низшего жанра

Одним из вопросов, которые издавна интересовали математиков, в частности русских, является вопрос о выражении абелевых интегралов *в конечном виде*, т. е. при помощи алгебраических функций и их логарифмов. В общем виде вопрос никогда до сих пор не ставился, а получено несколько интересных результатов частного характера. Прежде чем приводить их, докажем несколько предложений относительно формы, в которой можно искать результат. Эти предложения не новы: их можно встретить в трудах Абеля, Лиувилля, Чебышева и др. Но там они формулированы иначе и для нас не всегда убедительно, поскольку в их эпоху ещё не было вполне уточнено понятие многозначной функции.

Будем рассматривать интеграл типа

$$\int u \cdot dx, \tag{1}$$

где $u$ — элемент определённого поля $k(x, y)$.

Пусть интеграл (1) выражается через элементарные функции, т. е. его можно представить как алгебраическую (вообще говоря, иррациональную) функцию от $x, \log w_1, \log w_2, \ldots, \log w_k$, где $w_1, w_2, \ldots, w_k$ являются алгебраическими функциями от $x$:

$$\int u \cdot dx = \Phi(x, \log w_1, \log w_2, \ldots, \log w_k). \tag{2}$$

Оказывается, что в этом случае функцией $\Phi$ служит функция весьма частного вида, как это было в своё время показано Лиувиллем.

I. *Если интеграл* (1) *выражается через элементарные функции, то это выражение может быть представлено в форме*

$$w_0 + a_1 \log w_1 + \ldots + a_k \log w_k, \tag{3}$$

*где* $w_0, w_1, \ldots, w_k$ — *некоторые алгебраические функции от* $x$, *необязательно входящие в поле* $k(x, y)$, *а* $a_1, a_2, \ldots, a_k$ — *константы.*

Доказательство. Предположим, что $x, \log w_1, \log w_2, \ldots, \log w_k$ не связаны никаким рациональным соотношением вида

$$\Psi(x, \log w_1, \log w_2, \ldots, \log w_k) = 0; \tag{4}$$

иначе мы бы могли исключить из выражения (2) одну из функций $\log w_\nu$.

Дифференцируем равенство (2) по $x$:

$$u = \frac{\partial \Phi}{\partial x} + \frac{\partial \Phi}{\partial \log w_1} \cdot \frac{w_1'}{w_1} + \ldots + \frac{\partial \Phi}{\partial \log w_k} \cdot \frac{w_k'}{w_k}. \tag{5}$$

Получается соотношение типа (4). В силу нашего условия оно должно быть тождеством относительно $\log w_1, \log w_2, \ldots, \log w_k$, а потому производная от него по $\log w_\nu$ должна быть равна нулю:

$$\frac{\partial^2 \Phi}{\partial x \cdot \partial \log w_\nu} + \frac{\partial^2 \Phi}{\partial \log w_1 \cdot \partial \log w_\nu} \cdot \frac{w_1'}{w_1} + \ldots + \frac{\partial^2 \Phi}{\partial \log w_k \cdot \partial \log w_\nu} \cdot \frac{w_k'}{w_k} = 0$$
$$(\nu = 1, 2, \ldots, k).$$

Но это выражение есть полная производная по $x$ от функции $\frac{\partial \Phi}{\partial \log w_\nu}$, которая в силу этого равна постоянной

$$\frac{\partial \Phi}{\partial \log w_\nu} = a_\nu \qquad (\nu = 1, 2, \ldots, k). \tag{6}$$

При этом соотношения (6) являются тождествами относительно $\log w_\nu$ и, следовательно, $x$; в противном случае они опять приводили бы к соотношениям типа (4).

Отсюда следует, что в выражении Ф аргументы $\log w_\nu$ входят линейно с постоянными коэффициентами $a_\nu$, т. е. что Ф имеет форму (3).

II. *Можно нормировать выражения* (3) *так, чтобы* $w_0, w_1, \ldots, w_k$ *были функциями поля* $k(x, y)$.

Доказательство. Пусть $x$, $w_0, \ldots, w_k, y$ порождают поле $k(x, z)$. Пусть

$$F(x, y; z) = 0 \tag{7}$$

будет неприводимое в поле $k(x, y)$ уравнение, которому удовлетворяет $z$, и пусть $z_1, z_2, \ldots, z_h$ будут его корни, соответствующие определённым значениям $x, y$ (здесь удобно представить себе их расположенными на разных листах римановой поверхности). Пусть $y$ выражается через $x, z$ так:

$$y = \varphi(x, z).$$

В силу неприводимости уравнения (7) в поле $k(x, y)$ полином $\varphi(x, z) - y$ как функция от $z$ делится на $F(x, y, z)$, а потому

$$y = \varphi(x, z_1) = \varphi(x, z_2) = \ldots = \varphi(x, z_h).$$

Таким образом, наряду с

$$\int u \cdot dx = w_0 + a_1 \cdot \log w_1 + \ldots + a_k \cdot \log w_k, \tag{8}$$

мы будем также иметь

$$\int u \cdot dx = w_0^{(\mu)} + a_1 \cdot \log w_1^{(\mu)} + \ldots + a_k \cdot \log w_k^{(\mu)} \quad (\mu = 1, 2, \ldots, h), \tag{9}$$

где под $w_\nu^{(\mu)}$ мы разумеем функцию, сопряжённую с $w_\nu$: если

$$w_\nu = \psi_\nu(x, z),$$

то

$$w_\nu^{(\mu)} = \psi_\nu(x, z^{(\mu)}) \qquad (\mu = 1, 2, \ldots, h).$$

Суммируя равенства (9), получим:

$$\int u \cdot dx = \frac{1}{h} \cdot \sum_{\mu=1}^{h} w_0^{(\mu)} + \frac{a_1}{h} \cdot \log \prod_{\mu=1}^{h} w_1^{(\mu)} + \ldots + \frac{a_k}{h} \cdot \log \prod_{\mu=1}^{h} w_k^{(\mu)}.$$

Но сумма $\sum_{\mu=1}^{h} w_0^{(\mu)}$ и произведения $\prod_{\mu=1}^{h} w_\nu^{(\mu)}$, как симметрические функции от корней уравнения (7), являются элементами поля $k(x, y)$, и таким образом полученное равенство даёт искомое представление интеграла через элементы поля $k(x, y)$, ч. т. д.

III. *Можно нормировать выражение* (3) *так, чтобы коэффициенты* $a_1, a_2, \ldots, a_k$ *не были связаны линейными соотношениями*

$$a_1 m_1 + a_2 m_2 + \ldots + a_k m_k = 0 \tag{10}$$

*с целыми рациональными* $m_1, m_2, \ldots, m_k$.

Доказательство. Пусть имеет место (10), причём, например, пусть $m_1 \neq 0$. Тогда выражение (3) может быть представлено так:

$$w_0 + \frac{a_2}{m_1} \cdot \log \frac{w_2^{m_1}}{w_1^{m_2}} + \ldots + \frac{a_k}{m_1} \cdot \log \frac{w_k^{m_1}}{w_1^{m_k}}.$$

Вводя для элементов $\dfrac{w_\nu^{m_1}}{w_1^{m_\nu}}$ новые символы, уменьшим на единицу число членов в выражении (3). Продолжая процесс, мы в конце концов придём к выражению типа (3), для которого соотношений (10) уже не будет существовать.

IV. *Если интеграл* (1) *представлен в нормированной форме* (3), *то всякая точка, обращающая в нуль или в бесконечность одну* (*или несколько*) *из функций* $w_1, \ldots, w_k$, *является логарифмической точкой интеграла* (1).

Доказательство. Пусть, например, $w_1$ обращается в нуль в точке $P$. Выберем в качестве $x$ новый элемент поля $k(x, y)$, обращающийся в нуль в точке $P$, но более ни в одной другой точке, в которой обращается в нуль элемент $w_1$. Произведя в (8) замену переменных и затем переходя к сопряжённым относительно $x$ значениям элементов поля $k(x, y)$ и суммируя получаемые таким образом из (9) равенства, будем иметь:

$$\sum_{\mu=1}^{n} \int u^{(\mu)} \cdot dx = \sum_{\mu=1}^{n} w_0^{(\mu)} + a_1 \log \prod_{\mu=1}^{n} w_1^{(\mu)} + \ldots + a_k \log \prod_{\mu=1}^{n} w_k^{(\mu)}. \tag{11}$$

В силу сделанного относительно $x$ предположения $\prod_{\mu=1}^{n} w_1^{(\mu)}$ представляется в форме

$$x^{m_1} \cdot \varphi(x), \quad \varphi(0) \neq 0, \quad \varphi(0) \neq \infty,$$

где $m_1$ — целое положительное число. Аналогично представляются и остальные выражения $\prod_{\mu=1}^{n} w_\nu^{(\mu)}$, но только $m_\nu$ при $\nu \geqslant 2$ может принимать нулевые и отрицательные значения. Отсюда следует, что (11) можно представить в таком виде:

$$\sum_{\mu=1}^{n} \int u^{(\mu)} \cdot dx =$$

$$= \sum_{\mu=1}^{n} w_0^{(\mu)} + (a_1 m_1 + a_2 m_2 + \ldots + a_k m_k) \cdot \log x + \sum_{\nu=1}^{k} a_\nu \log \varphi_\nu(x), \tag{12}$$

Коэффициент при $\log x$ в правой части в силу III отличен от нуля, так что правая часть равенства (12) имеет в точке $x = 0$ логарифмическую бесконечность. С другой стороны, если бы $\int u \cdot dx$ не имел логарифмической бесконечности в точке $x = 0$, то ни один из интегралов $\int u^{(\mu)} \cdot dx$ тоже не имел бы её, так как все эти интегралы на всей римановой поверхности пробегают одну и ту же совокупность значений.

Отсюда в качестве простых следствий вытекает:

V. *Интеграл 1-го рода не может быть выражен через элементарные функции.*

В самом деле, из IV следует, что его выражение через элементарные функции не может содержать логарифмов и потому должно быть равно функции поля $k(x, y)$. Но функция поля $k(x, y)$, если она не есть константа, всегда в каких-нибудь точках обращается в бесконечность, в то время как интеграл 1-го рода таковых не имеет.

VI. *Если интеграл 2-го рода может быть выражен через элементарные функции, то он равен функции поля $k(x, y)$.*

Биномиальными дифференциалами называются дифференциалы вида

$$x^m (x^n + 1)^p dx, \tag{13}$$

где $m$, $n$, $p$ — какие-нибудь рациональные числа. Вопрос об их интегрировании через элементарные фуикции впервые был окончательно решён Чебышевым [100].

Предварительно заметим, что подстановка

$$x = z^\alpha, \tag{14}$$

где $\alpha$ — общий знаменатель чисел $m$ и $n$, приводит дифференциал (13) к такому же виду, но где $m$, $n$ будут целыми числами.

Известно, что интегрирование дифференциала (13) при помощи элементарных функций возможно в следующих трёх случаях:

I) $p$ есть целое число. В самом деле, тогда (13) есть рациональная функция.

II) $\frac{m+1}{n}$ есть целое число. В самом деле, тогда подстановка

$$x^n + 1 = z, \quad x = (z-1)^{\frac{1}{n}}$$

приведёт дифференциал (13) к виду

$$\frac{1}{n} z^p (z-1)^{\frac{m+1}{n}-1} \cdot dz,$$

и после подстановки (14) мы придём к случаю I).

III) $\frac{m+1}{n}+p$ есть целое число. В самом деле, дифференциал (13) можно представить в таком виде:

$$x^{m+np}\cdot(1+x^{-n})\cdot dx. \tag{15}$$

Поступая с этим дифференциалом, как в случае II), мы точно так же придём к случаю I). Чебышев [100] доказал, что интегрирование этого дифференциала при помощи элементарных функций возможно только в этих трёх случаях. Для удобства дальнейших рассуждений произведём подстановку $x=z^{\frac{1}{n}}$:

$$\int x^m(x^n+1)^p\,dx=\frac{1}{n}\int z^{\frac{m+1}{n}-1}\cdot(x+1)^p\cdot dz$$

и, вводя обозначения

$$\frac{m+1}{n}-1=-r,\quad p=-s,$$

рассмотрим интеграл

$$\int x^{-r}(x+1)^{-s}\cdot dx, \tag{16}$$

в котором, как мы предположим, ни $r$, ни $s$, ни $r+s$ не являются целыми числами [т. е. не подходят под случаи I), II), III)].

Из легко проверяемых дифференцированием рекуррентных формул

$$x^{-r+1}(x+1)^{-s+1}= \tag{17}$$

$$=(-r+1)\int x^{-r}(x+1)^{-s}\,dx+(-r-s+2)\int x^{-r+1}(x+1)^{-s}\,dx,$$

$$x^{-r+1}(x+1)^{-s+1}=-(-s+1)\int x^{-r}(x+1)^{-s}dx+ \tag{18}$$

$$+(-r-s+2)\int x^{-r}(x+1)^{-s+1}\,dx$$

мы заключаем, что нахождение интеграла (16) приводится к нахождению таких же интегралов, у которых $r$ или $s$ увеличены (или уменьшены) на единицу. Путём достаточного числа таких редукций мы можем выразить заданный интеграл через алгебраические функции и интеграл типа (16), у которого

$$0<r<1,\quad 0<s<1.$$

Если при этом

$$r+s>1,$$

то интеграл (16) является интегралом 1-го рода, так как остаётся конечным при $x=0$, $x=-1$, $x=\infty$. В силу V он не может быть выражен в конечном виде.

Если

$$r + s < 1,$$

то интеграл (16) остаётся конечным в точках $x = 0$ и $x = -1$. При этом вблизи $x = 0$ при надлежаще подобранной константе интегрирования он разлагается так:

$$(19) \qquad \int x^{-r}(x+1)^{-s}dx = \frac{1}{1-r} \cdot x^{1-r} - \frac{s}{2-r} \cdot x^{2-r} + \ldots,$$

т. е. обращается в нуль с той же скоростью, что и $x^{1-r}$.

Вблизи точки $x = \infty$ интеграл (16) разлагается так:

$$(20) \qquad \int x^{-r}(x+1)^{-s}dx = \frac{1}{1-r-s} \cdot x^{1-r-s} + \frac{s}{r+s} \cdot x^{-r-s} + \ldots,$$

т. е. обращается в бесконечность с той же скоростью, что и $x^{1-r-s}$.

Допустим, что (16) выражается через элементарные функции. Тогда в силу VI, как интеграл 2-го рода, он равен алгебраической функции от $x$. Точно так же произведение

$$(21) \qquad x^{r+s-1}\int x^{-r}(x+1)^{-s}\,dx$$

в силу (20) при $x = \infty$ остаётся конечным, при $x = 0$ в силу (19) стремится к нулю, как

$$x^{1-r} \cdot x^{r+s-1} = x^{s},$$

а при $x = -1$ остаётся конечным. Таким образом выражение (21) остаётся конечным во всех точках римановой поверхности, что в силу обобщённой теоремы Лиувилля невозможно. Таким образом интеграл (16) при сделанных предположениях не может быть выражен в конечном виде, и мы приходим к

Теорема 100 (Чебышева). *Интеграл*

$$\int x^{m}(x^{n}+1)^{p}\,dx$$

*с рациональными показателями $m$, $n$, $p$ выражается через элементарные функции тогда и только тогда, если одно из чисел*

$$p, \quad \frac{m+1}{n}, \quad p + \frac{m+1}{n}$$

*целое.*

Выведем результат Абеля (N. H. Abel) [16], касающийся псевдогиперэллиптических интегралов, т. е. интегралов вида

$$(22) \qquad \int \frac{(x^{\rho} + b_1x^{\rho-1} + \ldots + b_{\rho}) \cdot dx}{\sqrt{x^{2\rho+2} + a_1x^{2\rho+1} + \ldots + a_{2\rho+2}}},$$

выражаемых через элементарные функции. Абель привёл нахождение псевдогиперэллиптических интегралов к вопросу о периодичности

разложения радикала

$$\sqrt{R(x)} = \sqrt{x^{2\rho+2} + a_1 x^{2\rho+1} + \ldots + a_{2\rho+2}}$$

в непрерывную дробь. Это не может считаться решением вопроса, так как, если после получения сколь угодно большого числа звеньев непрерывной дроби периодичность не обнаруживается, то это не гарантирует, что она не обнаружится на последующих звеньях. Окончательно этот вопрос был решён Золотарёвым [7], который, опираясь на созданную им теорию «целых комплексных чисел», привёл вопрос к изучению арифметической природы коэффициентов. Впрочем, Золотарёв ограничился случаем вещественных коэффициентов. Подробное изложение вопроса содержится в диссертации Пташицкого [11], а результат Абеля весьма просто изложен в статье Долбни [3].

Интеграл (22) как функция от верхнего предела имеет логарифмические бесконечности в обеих точках $P_1$, $P_2$, в которых $x$ обращается в бесконечность, и более не имеет особых точек. Отсюда следует, что в его предполагаемом представлении через элементарные функции алгебраический член отсутствует. Далее, если считать представление

$$(23) \qquad \int \frac{b(x)\cdot dx}{\sqrt{R(x)}} = a_1 \log w_1 + a_2 \log w_2 + \ldots + a_k \log w_k$$

нормированным, то в силу IV каждый член $a_\nu \log w_\nu$ может иметь нули и бесконечности только в точках $P_1$, $P_2$, а потому $w_\nu$ при представлении через дивизоры выражается так:

$$w_\nu \equiv \frac{P_1^{m_\nu}}{P_2^{m_\nu}},$$

где $m_\nu$ (положительное или отрицательное) — целое число. Отсюда следует существование показателя $m$, при котором

$$(24) \qquad P_1^m \sim P_2^m.$$

Будем считать $m$ возможно меньшим положительным показателем такого рода. С точки зрения трансцендентной теории алгебраических функций это вполне решает вопрос, так как в силу теоремы Абеля соотношение (24) равносильно сравнению

$$(25) \qquad m \int_{P_1}^{P_2} du_\nu(P) = m \cdot u_\nu(P_2) - m \cdot u_\nu(P_1) \equiv 0 \qquad (\nu = 1, 2, \ldots, \rho),$$

где $u_\nu(P)$ — система интегралов 1-го рода, а знак сравнения $\equiv$ обозначает, что левая часть (25) равна целочисленной линейной

комбинации периодов интеграла $u_\nu(P)$ Это сравнение показывает, что интегралы

$$\int_{P_1}^{P_2} c'u_\nu(P) \qquad (\nu = 1, 2, \ldots, \rho)$$

должны быть рациональными комбинациями периодов. Конечно, установить сравнение (25) для практического примера представляет собой весьма трудную задачу.

Из того, что $m$ есть наименьший положительный показатель, при котором имеет место (24), следует, что все $m_\nu$ делятся на $m$:

$$m_\nu = m \cdot q_\nu \qquad (\nu = 1, 2, \ldots, k).$$

Вводя обозначение

$$\frac{P_1^m}{P_2^m} \equiv \varphi(x, \sqrt{R(x)}) \equiv \varphi,$$

мы будем иметь:

$$w_\nu = \varphi^{q_\nu} \qquad (\nu = 1, 2, \ldots, k).$$

Подставляя в равенство (23), получим:

$$\int \frac{b(x) \cdot dx}{\sqrt{R(x)}} = (a_1 q_1 + a_2 q_2 + \ldots + a_k q_k) \log \varphi(x, \sqrt{R(x)}).$$

Обозначим коэффициент $a_1 q_1 + a_2 q_2 + \ldots + a_k q_k$ через $a$, а функцию $\varphi$ представим в форме

$$\varphi(x, \sqrt{R(x)}) = p(x) + q(x) \cdot \sqrt{R(x)}, \tag{26}$$

где $p(x)$, $q(x)$ — рациональные функции. Тогда

$$\int \frac{b(x)\,dx}{\sqrt{R(x)}} = p(x) + q(x) \cdot \sqrt{R(x)}.$$

Меняя знак при $\sqrt{R}$ (т. е. переходя к другому листу римановой поверхности), получим:

$$-\int \frac{b(x) \cdot dx}{\sqrt{R(x)}} = a \cdot \log(p - q\sqrt{R}).$$

Беря полуразность обоих выражений, будем иметь:

$$\int \frac{b(x) \cdot dx}{\sqrt{R(x)}} = \frac{a}{2} \cdot \log \frac{p + q\sqrt{R}}{p - q\sqrt{R}}. \tag{27}$$

Уничтожая дроби в числителе и знаменателе выражения под знаком логарифма, мы можем считать $p(x)$ и $q(x)$ полиномами, и притом взаимно простыми.

Обратно, если имеет место (24), то при заданном полиноме $R(x)$ мы можем подобрать полином $\rho$-й степени $b(x)$ так, чтобы имело место (27). В самом деле, из представления функции $\varphi$ через дивизоры следует, что она есть целая относительно $x$ функция, т. е. корень квадратного уравнения

$$\varphi^2 - 2p \cdot \varphi + (p^2 - q^2 \cdot R) = 0, \tag{28}$$

коэффициенты которого должны быть полиномами. Итак, $2p$ и $p^2 - q^2R$ — полиномы. Отсюда $p$ и $q^2R$ — полиномы. Но так как, по предположению, $R$ не имеет кратных корней, то и $q$ есть полином. При этом в силу сопряжённости точек $P_1$ и $P_2$ уравнению (28) удовлетворяют функции, представляемые через дивизоры так:

$$\varphi \equiv \frac{P_1^m}{P_2^m}, \qquad \varphi' \equiv \frac{P_2^m}{P_1^m},$$

откуда следует

$$\varphi \cdot \varphi' = \text{const}.$$

Нормируя при $p(x)$ и $q(x)$ числовой множитель, мы можем получить $\varphi \cdot \varphi' = 1$, т. е.

$$p^2(x) - q^2(x) \cdot R(x) = 1. \tag{29}$$

Дифференцируем правую часть формулы (27):

$$\frac{d}{dx}\left(\log\frac{p + q\sqrt{R}}{p - q\sqrt{R}}\right) = \frac{2(pq' - p'q)R + pqR'}{2\sqrt{R}}. \tag{30}$$

С другой стороны, дифференцируя (29)

$$2pp' - q(2q'R + qR') = 0, \tag{31}$$

мы видим, что $p \cdot p'$ делится на $q$. Но так как $p$ и $q$ взаимно просты то $p'$ должен делиться на $q$:

$$p' = q \cdot r. \tag{32}$$

Преобразуя (30) при помощи (29), (30) и (31), будем иметь:

$$\frac{d}{dx}\left(\log\frac{P + q\sqrt{R}}{P - q\sqrt{R}}\right) = \frac{P'}{q\sqrt{R}} = \frac{r}{\sqrt{R}}.$$

Но из (29) видно, что степень $p(x)$ превышает степень $q(x)$ на $\rho + 1$ единиц, в силу чего $r(x)$ есть полином $\rho$-й степени. Поэтому можно подобрать полином $b(x)$ так, чтобы имело место (27).

Итак, задача привелась к решению в полиномах неопределённого уравнения (29), аналогичного уравнению Пелля в теории чисел. Докажем, что уравнение (29) имеет решение тогда и только тогда, когда $\sqrt{R(x)}$ разлагается в периодическую непрерывную дробь

(к сожалению, в теории полиномов это случается не всегда). В дальнейшем будем предполагать известной арифметическую теорию непрерывных дробей. По аналогии с ней, мы можем разлагать в непрерывные дроби и аналитические функции, допускающие разложение вблизи точки $x=\infty$. Будем называть *степенью* функции $f(x)$ и обозначать символом $\delta f(x)$ показатель наивысшей степени её разложения по убывающим степеням $x$. Имеет место

$$\delta\{f(x)+g(x)\} \leqslant \operatorname{Max}\{\delta f(x), \delta g(x)\},$$
$$\delta\{f(x)\cdot g(x)\} = \delta f(x)+\delta g(x).$$

Далее, под *целой частью* $[f(x)]$ функции $f(x)$ мы будем разуметь сумму её членов разложения, имеющих неотрицательные степени. $[f(x)]$ вполне определяется равенством

$$\delta\{f(x)-[f(x)]\}<0. \tag{33}$$

Разложение функции $f(x)$ в непрерывную дробь производится так. Определяют целую часть $a_1$ (полином!) функции $f(x)$, а затем определяют функцию $f_1(x)$ равенством

$$f(x)=a_1+\frac{1}{f_1(x)}.$$

Ясно, что $\delta f_1(x)>0$. Затем определяют целую часть $a_2$ функции $f_1(x)$ и функцию $f_2(x)$ равенством

$$f_1(x)=a_2+\frac{1}{f_2(x)}.$$

Продолжая процесс, мы получим для $f(x)$ выражение

$$f(x)=a_1+\frac{1}{a_2+\ddots+\frac{1}{a_n+\frac{1}{f_n(x)}}} \tag{34}$$

для любого $n$. Здесь $a_1, a_2, \ldots, a_n$ — полиномы, а $\delta f_n(x)>0$. Такое выражение называется *непрерывной дробью*, полиномы $a_1, a_2, \ldots, a_n$ её *звеньями*, а функции $f_n(x)$ — *полными частными*.

Отрезок непрерывной дроби

$$\frac{P_n}{Q_n}=a_1+\frac{1}{a_2+\frac{1}{a_3+\ddots+\frac{1}{a_n}}}, \tag{35}$$

приведённый к виду несократимой дроби $\frac{P_n}{Q_n}$, носит название её *n-й подходящей дроби*. Её числители и знаменатели могут быть определяемы соотношениями

$$P_n = P_{n-1}a_n + P_{n-2}, \quad Q_n = Q_{n-1}a_n + Q_{n-2}. \tag{36}$$

Имеет место

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^n. \tag{37}$$

Из (36) видно, что

$$\delta P_n > \delta P_{n-1}, \quad \delta Q_n > \delta Q_{n-1}, \tag{38}$$

поскольку $a_n$ — полиномы не ниже 1-й степени (только $a_1$ может быть константой и даже нулём). Очевидно также, что

$$\delta P_n \geqslant n-2, \quad \delta Q_n \geqslant n-1. \tag{39}$$

Вычислим степень разности $f(x) - \frac{P_n}{Q_n}$. Вычисляя конечную непрерывную дробь (34) [с последним звеном $f_n(x)$] по правилу (36), будем иметь:

$$f(x) = \frac{P_n \cdot f_n(x) + P_{n-1}}{Q_n \cdot f_n(x) + Q_{n-1}}.$$

Отсюда

$$f(x) - \frac{P_n}{Q_n} = \frac{(-1)^{n-1}}{Q_n(Q_n \cdot f(x) + Q_{n-1})},$$

а также

$$f(x) - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n \cdot f_n(x)}{Q_{n-1}(Q_n \cdot f_n(x) + Q_{n-1})}.$$

Отсюда следует в силу (39)

$$\delta\left(f(x) - \frac{P_n}{Q_n}\right) \leqslant -(2n-1), \tag{40}$$

а также

$$\delta\left(f(x) - \frac{P_n}{Q_n}\right) \leqslant \delta\left(f(x) - \frac{P_{n-1}}{Q_{n-1}}\right) - 2. \tag{41}$$

Справедливо и обратное: если для какой-нибудь рациональной дроби $\frac{P}{Q}$ имеет место

$$\delta Q = m-1, \quad \delta\left(f(x) - \frac{P}{Q}\right) \leqslant -(2m-1), \tag{42}$$

то $\frac{P}{Q}$ есть подходящая дробь разложения функции $f(x)$. Чтобы доказать это, разложим $\frac{P}{Q}$ в непрерывную дробь

$$\frac{P}{Q} = a_1 + \frac{1}{a_2 + \ddots + \frac{1}{a_n}}$$

и определим $f_n(x)$ при помощи равенства

$$f(x) = a_1 + \frac{1}{a_2 + \ddots + \frac{1}{a_n + \frac{1}{f_n(x)}}}, \tag{43}$$

т. е.

$$f(x) = \frac{P \cdot f_n(x) + P_{n-1}}{Q \cdot f_n(x) + Q_{n-1}}, \quad f_n(x) = \frac{Q_{n-1}\left(\frac{P_{n-1}}{Q_{n-1}} - f(x)\right)}{Q\left(f(x) - \frac{P}{Q}\right)}. \tag{44}$$

Но

$$\frac{P_{n-1}}{Q_{n-1}} - f(x) = \left(\frac{P_n}{Q_n} - f(x)\right) - \frac{(-1)^n}{Q_{n-1} \cdot Q},$$

откуда в силу (42) и

$$\delta\left(\frac{1}{Q_{n-1} \cdot Q}\right) \geqslant -(m-1) - (m-2) = -(2m-3)$$

мы будем иметь

$$\delta\left(\frac{P_{n-1}}{Q_{n-1}} - f(x)\right) = -\delta Q_{n-1} - \delta Q,$$

так что второе равенство (44) даст нам:

$$\delta f_n(x) \geqslant \delta Q_{n-1} + (-\delta Q_{n-1} - \delta Q) - \delta Q + (2m-1).$$

Из равенства же (34), $\delta f_n(x) \geqslant 1$ и того, что $a_\nu$ — полиномы, мы постепенно заключаем, что

$$\left[a_n + \frac{1}{f_n(x)}\right] = a_n, \quad \left[a_{n-1} + \frac{1}{a_n + \frac{1}{f_n(x)}}\right] = a_{n-1}, \text{ и т. д.},$$

а это показывает, что (43) есть разложение $f(x)$ в непрерывную дробь, а $\frac{P}{Q}$ — $n$-я подходящая.

Приложим этот результат к решению $p$, $q$ уравнения (29). Перепишем его так:

$$p - q\sqrt{R(x)} = \frac{1}{p + q\sqrt{R(x)}}. \tag{45}$$

Не может быть, чтобы степени $p - q\sqrt{R(x)}$ и $p + q\sqrt{R(x)}$ были одинаковы, так как тогда они равны нулю, и степень их суммы, т. е. $2p$, тоже не превышала бы нуль. Нормируем знак при

$$\sqrt{R(x)}$$

так, чтобы

$$\delta(p - q\sqrt{R(x)}) < 0, \quad \delta(p + q\sqrt{R(x)}) > 0.$$

Представим (45) так:

$$\frac{p}{q} - \sqrt{R(x)} = \frac{1}{q(p + q\sqrt{R})}$$

Если $\delta q = m - 1$, то $\delta p = (m-1) + (\rho + 1) = m + \rho$. Из

$$\delta 2p \leqslant \operatorname{Max}\{\delta(p + q\sqrt{R}), \quad \delta(p - q\sqrt{R})\} = \delta(p + q\sqrt{R})$$

следует

$$\delta(p + q\sqrt{R}) \geqslant \delta p = m + \rho,$$

откуда

$$\delta\left(\frac{p}{q} - \sqrt{R(x)}\right) \leqslant -(m-1) - (m+\rho) \leqslant -(2m-1),$$

так что из доказанного мы заключаем, что $\frac{p}{q}$ есть подходящая дробь разложения $\sqrt{R(x)}$ в непрерывную дробь. Пусть

$$\frac{p}{q} = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}, \tag{46}$$

$$\sqrt{R(x)} = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n + \cfrac{1}{f_n(x)}}}.$$

Представим $f_n(x)$ в форме $\frac{\alpha}{\gamma} + \frac{\beta}{\gamma}\sqrt{R}$, где $\alpha$, $\beta$, $\gamma$ — полиномы от $x$. Из второго равенства (46) имеем

$$\sqrt{R(x)} = \frac{pf_n(x) + P_{n-1}}{qf_n(x) + Q_{n-1}},$$

откуда

$$q\frac{\alpha}{\gamma}\sqrt{R(x)}+q\frac{\beta}{\gamma}R(x)+Q_{n-1}\cdot\sqrt{R(x)}=p\frac{\alpha}{\gamma}+p\frac{\beta}{\gamma}\sqrt{R(x)}+P_{n-1}.$$

Если $\sqrt{R(x)}$ есть иррациональная функция, то это равенство должно быть тождеством относительно $\sqrt{R(x)}$, так что

$$(47)\qquad \begin{cases} q\frac{\alpha}{\gamma}+Q_{n-1}=p\frac{\beta}{\gamma}, \\ p\frac{\alpha}{\gamma}+P_{n-1}=q\frac{\beta}{\gamma}R(x). \end{cases}$$

Умножая первое из равенств на $p$, второе на $-q$ и складывая, получим

$$(-1)^n=\frac{\beta}{\gamma}(p^2-q^2R(x)),$$

так что тождество (29) равносильно тождеству

$$\frac{\beta}{\gamma}=(-1)^n.$$

При этом, если выполняется (29), то из равенств (47) вытекает, что в силу взаимной простоты $p$ и $q$ дробь $\frac{\alpha}{\gamma}$ равна полиному.

Подставляя в (46) выражение для $f_n(x)$, где $\sqrt{R(x)}$ предположим опять разложенным в непрерывную дробь, мы убедимся, что разложение $\sqrt{R(x)}$ в случае чётного $n$ имеет период

$$(48)\qquad [a_1, (a_2, \ldots, a_n, b+a_1)],$$

а в случае нечётного $n$ имеет период

$$(49)\qquad [a_1, (a_2, \ldots, a_n, b-a_1, -a_2, \ldots, -a_n, -b+a_1)].$$

Итак, чтобы неопределённое уравнение (29) имело решение в полиномах, необходимо и достаточно, чтобы $\sqrt{R(x)}$ разлагался в периодическую непрерывную дробь одного из типов (48) и (49); другими словами, чтобы период начинался со второго звена.

Докажем, что всякое периодическое разложение $\sqrt{R(x)}$ имеет именно эту форму. Для этого мы убедимся, что:

1) все $f_n$ имеют форму $\frac{\alpha_n+\sqrt{R}}{\gamma_n}$, где $\alpha_n$ и $\gamma_n$ — полиномы, причём $\gamma_n$ есть делитель $\alpha_n^2-R$;

2) сопряжённые с $f_n$ функции $f_n'$ имеют степень $<0$, начиная с $n=1$.

Чтобы доказать 1), обратим внимание, что $f_1$ удовлетворяет 1): из

$$\sqrt{R}=a_1+\frac{1}{f_1}$$

мы имеем:

$$f_1=\frac{1}{\sqrt{R}-a_1}=\frac{a_1+\sqrt{R}}{R-a_1^2}.$$

Пусть $f_{n-1}=a_n+\frac{1}{f_n}$ удовлетворяет 1). Тогда

$$f_n=\frac{1}{f_{n-1}-a_n}=\frac{1}{\frac{\sqrt{R}+a_{n-1}-a_n\gamma_{n-1}}{\gamma_{n-1}}}=\frac{\gamma_{n-1}(\sqrt{R}-a_{n-1}+a_n\gamma_{n-1})}{R-(a_{n-1}-a_n\gamma_{n-1})^2}.$$

При этом из нашего предположения следует, что $R-a_{n-1}^2$, и потому $R-(a_{n-1}-a_n\gamma_{n-1})^2$ делится на $\gamma_{n-1}$. Сокращая выражение для $f_n$ на $\gamma_{n-1}$, мы получим выражение, удовлетворяющее 1). Индукция установлена.

Для доказательства 2) для $n=1$ имеем:

$$f_1'=\frac{1}{-\sqrt{R}-a_1},$$

откуда

$$\delta f_1'<0.$$

Предположим, что $\delta f_{n-1}'<0$. Тогда $f_{n-1}'=a_n+\frac{1}{f_n'}$, откуда

$$f_n'=\frac{1}{f_{n-1}'-a_n}.$$

Но $\delta(f_{n-1}'-a_n)=\delta a_n>0$, откуда $\delta f_n'<0$. Индукция установлена.

Равенства

$$f_{n-1}'-a_n=\frac{1}{f_n'},\quad \delta f_{n-1}'<0$$

показывают, что $a_n$ вполне определяется как целая часть от $-\frac{1}{f_n'}$.

Таким образом если непрерывная дробь периодическая, начиная с $n=n_0$, т. е. если $f_{n_0}=f_{n_0+p}$, то и $f_{n_0-1}=f_{n_0+p-1}$ и т. д., вплоть до $f_1=f_{p+1}$, $f_p\neq f$, так как $f=\sqrt{R}$ уже не удовлетворяет свойству 2).

Пусть $f_{p+1}=f_1=\frac{1}{\sqrt{R}-a_1}$. Тогда

$$f_p'=\frac{1}{f_{p+1}'}+a_p=-\sqrt{R}-a_1+a_p.$$

Из $\delta f_p'<0$ следует, что $-a_1+a_p=[R]=a_1$, откуда $a_p=2a_1$. Таким образом в дробях (48) и (49) соответственно $b=a_1$ и $b=-a_1$.

Сопоставляя все наши выводы, мы приходим к следующему результату Абеля:

Теорема 101 (Абеля). *Чтобы для данного полинома $R(x)$ степени $2\rho+2$ существовал такого рода полином $b(x)$ степени $\rho$, чтобы интеграл*

$$\int \frac{b(x)}{\sqrt{R(x)}}\,dx$$

*выражался в элементарных функциях, необходимо и достаточно, чтобы $\sqrt{R(x)}$ разлагался в периодическую непрерывную дробь.*

Современные математики ставят общий вопрос о приведении заданного абелева интеграла к полям низшего жанра, т. е. о нахождении преобразования переменных, приводящего заданный интеграл

$$\int \varphi(x,\ y)\,dx$$

к интегралу

$$\int \psi(u,\ v)\,du,$$

где поле $k(u,\ v)$ имеет меньший жанр, чем поле $k(x,\ y)$.

Эта проблема может быть поставлена, исходя из двух различных точек зрения: трансцендентной и алгебраической. Трансцендентная точка зрения (при которой как бы предполагается известной арифметическая природа периодов интегралов) даёт для решения проблемы довольно ясную картину. Например, известен такой результат: чтобы $\rho_1$ интегралов 1-го рода жанра $\rho\ (\rho_1<\rho)$ приводились к интегралам жанра $\rho_1$, необходимо и достаточно, чтобы их $2\rho\rho_1$ периодов $\Omega_{\mu\nu}\ (\mu=1,\ \ldots,\ \rho_1;\ \nu=1,\ \ldots,\ 2\rho)$ выражались через некоторые величины $\omega_{\mu\lambda}\ (\mu=1,\ \ldots,\ \rho_1;\ \lambda=1,\ \ldots,\ 2\rho_1)$ при помощи целых чисел $m_{\nu\varkappa}$:

$$\Omega_{\mu\nu}=\sum_{\varkappa=1}^{2\rho_1} m_{\nu\varkappa}\omega_{\mu\varkappa}\quad(\mu=1,\ 2,\ \ldots,\ \rho_1;\ \nu=1,\ 2,\ \ldots,\ 2\rho).$$

На практике такого рода результаты по понятной причине оказываются бессильны. В книге Крацера (A. Krazer) [66] на стр. 469—501 приведено несколько такого рода результатов, а также дана литература.

Проблема приведения абелевых интегралов алгебраическим путём до сих пор находится в младенческой стадии своего развития. Кроме приведённых результатов Абеля, Чебышева и Золотарёва, можно указать, например, на сочинения Долбни [4,34], где дано много случаев приведения абелевых интегралов. Общей же теории приведения пока не существует.

Задача нахождения между периодами абелевых интегралов рациональных соотношений имеет значение для теории дифференциальных уравнений, на что указывает Пенлеве (Painlevé) в своём стокгольмском курсе [80].

## § 54. Функции Аппелля

Аппелль (P. Appell) посвятил большой мемуар [18] функциям, однозначным на рассечённой римановой поверхности и претерпевающим при переходе через каждое сечение $A_\nu$, $B_\nu$, $C_\nu$ линейную подстановку

$$\overset{+}{W} = m_\nu \cdot \overset{-}{W} + p_\nu,$$

где $m_\nu$, $p_\nu$ — константы. Нетрудно установить связь между этими функциями и абелевыми интегралами: производные $\frac{dW}{dz}$ приобретают при переходе через сечения множителей и потому могут быть представлены в виде

$$e^{\int \varphi(z,\, w)\cdot dz},$$

где $\int \varphi(z, w) \cdot dz$ — абелев интеграл. Аппелль установил число линейно независимых функций этого рода с заданными бесконечностями, а также нашёл связи между определяющими их константами.

Ещё до этого такие функции были рассмотрены Примом (1869—1870 гг.). В 1911 г. Прим и Рост (F. Prym, G. Rost) [86] выпустили посвящённую этим же функциям книгу, подавляющую роскошью издания и обстоятельностью изложения. В ней авторы, опираясь на принцип Дирихле, определяют, сколько из констант должны быть заданы и сколько оставаться произвольными, чтобы однозначно определить общую «функцию Прима». Они ввели ограничение $|m_\nu| = 1$.

Кёниг (R. König) [65] решает вопросы о константах, входящих в функции Аппелля, при помощи арифметической теории алгебраических функций. Как известно, всякому дивизору нулевого порядка $Q = \frac{P_1 \cdot P_2 \ldots P_s}{P_1' \cdot P_2' \ldots P_s'}$ можно сопоставить функцию

$$e^{\omega_{P_1 P_1'}(P) + \omega_{P_2 P_2'}(P) + \cdots + \omega_{P_s P_s'}(P)}, \tag{1}$$

где $\omega_{P_\nu P_\nu'}(P)$ — элементарные нормированные интегралы 3-го рода, причём в том и только в том случае, когда $Q$ лежит в главном классе, функция (1) представляет собой алгебраическую функцию, т. е. функцию поля $k(z, w)$, соответствующую дивизору $Q$.

С другой стороны, мы видели в § 19, что с дивизорами класса дифференциалов $\mathfrak{W}$ сопоставляется абелев интеграл, бесконечности которого точно указываются знаменателем дивизора. Умножая дивизор

из $\mathfrak{W}$ на дивизор нулевого порядка, Кёниг сопоставляет с полученным дивизором интеграл от функции типа (1), т. е. наиболее общую функцию Аппелля. Это позволяет производить подсчёт констант, входящих в функции Аппелля, при помощи обыкновенной теоремы Римана-Роха.

Пусть $M$ — дивизор нулевого порядка, определяющий «характер» функций Аппелля, и $Q$ — произвольный дивизор. В силу теоремы Римана-Роха имеем:

$$\text{Изм}\left(\frac{\mathfrak{W}M}{Q}\right) = \text{Изм}\left(\frac{Q}{M}\right) + \rho - 1 - \text{Пор } Q.$$

Если Пор $Q \leqslant 0$ и $Q \sim M$, то $\text{Изм}\left(\frac{Q}{M}\right) = 0$ и

$$\text{Изм}\left(\frac{\mathfrak{W}M}{Q}\right) = \rho - 1 - \text{Пор } Q.$$

Полагая $Q = 1$, получим:

$$\text{Изм}\,(\mathfrak{W}M) = \rho - 1,$$

т. е. существует $\rho - 1$ независимых всюду конечных функций Аппелля.

Полагая $Q = \frac{1}{p^k}$ $(k = 1, 2, \ldots)$ получим:

$$\text{Изм}\,(\mathfrak{W}MP^k) = \rho - 1 + k,$$

откуда следует, что существует одна единственная функция Аппелля, имеющая в точке $P$ бесконечность — или логарифмическую, или алгебраическую порядка $k - 1$ $(k = 2, 3, \ldots)$, линейно независимую от функции с низшими бесконечностями в $P$.

Подобным же путём Кёниг выводит обобщение теоремы Вейерштрасса о пробелах:

*Если рассмотрим чисто мультипликативные функции Аппелля, имеющие в точке $P$ бесконечности порядков 1, 2, 3, ..., то в их ряду имеется ровно $\rho - 1$ пробелов, если отвлечься от линейных комбинаций элементов поля $k(z, w)$.*

## § 55. Проблема униформизации

Проблема униформизации состоит в следующем. Пусть задано алгебраическое уравнение

(1) $$f(x, y) = 0.$$

Требуется найти однозначные фуикции

$$x = x(t), \quad y = y(t),$$

тождественно удовлетворяющие уравнению (1).

В случае нулевого жанра ($p = 0$) уравнения (1) проблема униформизации решается элементарно. В случае $p = 1$ она решается при помощи эллиптических функций, т. е. функций, полученных при помощи обращения эллиптических интегралов 1-го рода. Наконец, при $p > 1$ проблема решается при помощи *автоморфных функций*, удовлетворяющих соотношениям

$$f\left(\frac{a_s z + b_s}{c_s z + d_s}\right) = f(z), \tag{2}$$

где дробные линейные подстановки

$$z \to \frac{a_s z + b_s}{c_s z + d_s} \quad (a_s d_s - b_s c_s \neq 0) \qquad (s = 1, 2, \ldots)$$

образуют некоторую дискретную группу. Проблема униформизаций была решена Пуанкаре и подробно изучена Кёбе (P. Koebe). Однако до сих пор отсутствует в достаточной мере эффективное решение проблемы, которое бы позволило пользоваться униформизирующими функциями как инструментом.

С проблемой униформизации можно познакомиться по книге Форда (L. R. Ford) [39] (имеется русский перевод), в которой также приведена обширная литература.

## § 56. Алгебраические функции многих независимых переменных

Непосредственное обобщение методов теории алгебраических функций на функции от нескольких независимых переменных встречает большие затруднения. Применение теории аналитических функций не приводит к таким законченным результатам, как в случае одной независимой переменной, поскольку сама теория аналитических функций не допускает достаточно удовлетворительного обобщения на случай нескольких переменных. Обобщая римановы поверхности, мы сталкиваемся с незнанием полной системы топологических инвариантов поверхностей в многомерных пространствах (замкнутые поверхности в трёхмерных пространствах имеют единственный инвариант—порядок связности).

Арифметическая теория тоже не допускает удовлетворительного обобщения, так как теория идеалов в случае нескольких независимых переменных не приводит к однозначному разложению идеалов на простые идеалы. Бирациональные преобразования не оставляют инвариантными даже измерений идеалов.

Однако при помощи геометрического метода в теории алгебраических функций от двух независимых переменных было получено довольно много результатов. Здесь наиболее продуктивными оказались представители итальянской школы геометров. Основные результаты их работ приведены в большой монографии Пикара (É. Picard) и

Симара (G. Simart) [82], которые, наряду с геометрическим методом, широко пользовались методом теории аналитических функций.

Основными инвариантами алгебраических поверхностей

$$f(x, y, z) = 0 \tag{1}$$

относительно всевозможных бирациональных преобразований являются: 1) *геометрический жанр* $p_g$, т. е. число линейно независимых двойных интегралов 1-го рода (т. е. принимающих всюду конечные значения); 2) *арифметический жанр* $p_a$ или $p_n$, который мы не будем ближе определять; он не превышает $p_g$ и для некоторых поверхностей имеет отрицательное значение; 3) *бижанр* $P_2$, который можно определить как число линейно независимых четверных интегралов в поле $k(x, y, z; \xi, \eta, \zeta)$, где, наряду с (1), имеет место

$$f(\xi, \eta, \zeta) = 0;$$

(4) аналогично определяется *трижанр* $P_3$ и т. д.

Поверхность (1) называется *рациональной*, если все элементы поля $k(x, y, z)$ могут быть рационально выражены через *два* независимых элемента этого поля. Для рациональных поверхностей все перечисленные инварианты равны нулю. Обратно, всякая поверхность, для которой $p_a = P_2 = 0$, рациональна.

По теории алгебраических поверхностей существует современная обзорная монография Зарисского (O. Zariski) [113] с большим литературным указателем.

Юнг (H. W. Jung) в большой серии статей задался целью арифметизировать теорию алгебраических функций двух независимых переменных в духе теории Гензеля. Ему удалось повторить основные результаты итальянских авторов. Странно, что последние никогда его не цитируют. Ссылки на работы Юнга содержатся в его энциклопедической статье [61]. См. также его книгу по алгебраическим поверхностям [63].

Интересная чисто алгебраическая попытка построить теорию дивизоров в поле алгебраических функций любого числа независимых переменных принадлежит Шмейдлеру (W. Schmeidler) [92].

В модернизированном виде (с применением общей теории идеалов) алгебраическая геометрия изложена у Ван-дер-Вардена (B. L. van der Waerden) [105].

## Упражнения к главе IX

1. Доказать, что $2^{2p}$ $\vartheta$-функций с характеристиками $\begin{bmatrix} g_1, g_2, \ldots, g_p \\ h_1, h_2, \ldots, h_p \end{bmatrix}$, где $g_i$ и $h_i$ принимают значения 0 и $1/2$, линейно независимы.

2. Если дивизор $P_1, P_2 \ldots P_p$ порождает класс измерения $s+1$, то тождественно (относительно $P$) равны нулю функция

$$\vartheta\left(u(P) - \sum_{\nu=1}^{p} u(P_\nu) - k\right),$$

а также все её частные производные 1-го, 2-го, ..., $(s-1)$-го порядков, но не все $s$-го порядка (Крацер).

3. Поверхность

$$z = 3xy - x^3$$

допускает бесчисленное множество систем линий переноса (Чеботарёв).

4. Поверхность

$$z = x^4 - 2x^2y - y^2$$

допускает две пары систем линий переноса (Чеботарёв).

5. Гиперповерхность

$$z = x_1^4 - 6x_1^2x_2 + 3x_2^2 + 8x_1x_3$$

в четырёхмерном пространстве допускает бесчисленное множество систем линий переноса (Чеботарёв).

6. Доказать, что интеграл

$$\int \frac{(4x+a)\,dx}{\sqrt{(x^2+ax+b)^2-4abx}}$$

выражается в логарифмах (Абель).

7. Доказать, что интеграл

$$\int \frac{\left(x+\frac{\sqrt{5}+1}{14}\right)dx}{\left(x^2-\frac{\sqrt{5}-1}{2}\right)^2+(\sqrt{5}-)^2\cdot x}$$

выражается в логарифмах (Абель).

8. Доказать, что интеграл

$$\int \frac{(x+A)\,dx}{\sqrt{x(x-1)(x-\alpha)(x-\beta)}},$$

в котором

$$\alpha = 1+4v^2,\ \beta = 12v,$$

где $v$ есть корень уравнения

$$v^3+6v^2-27v+3=0,$$

выражается в логарифмах (Золотарёв).

ГЛАВА X

# СОВРЕМЕННЫЕ ПРОБЛЕМЫ В ТЕОРИИ АЛГЕБРАИЧЕСКИХ ФУНКЦИЙ

Современные проблемы в теории алгебраических функций, под которыми я буду разуметь проблемы, возникшие после первой мировой войны и опирающиеся на результаты «современной алгебры», характерны тем, что в них особое внимание уделено числовому полю, над которым строится поле алгебраических функций. Классическая теория ограничилась случаем алгебраически замкнутого числового поля. В связи с этим в современной теории алгебраических функций встал на очередь вопрос о «рациональных точках на алгебраической кривой». С другой стороны, в случае конечного числового поля теория алгебраических функций приобрела некоторые черты, свойственные теории алгебраических чисел; в частности, оказалось полезным изучение функции, аналогичной $\zeta$-функции Дедекинда.

## § 57. Рациональные точки на алгебраических кривых

Пусть поле $k(x, y)$ задано соотношением

$$f(x, y) = 0 \tag{1}$$

с коэффициентами из поля $k$. *Рациональной точкой* кривой (1) мы будем называть точку поля $k(x, y)$, в которой элементы $x$ и $y$ принимают значения из поля $k$ (или какого-нибудь его алгебраического расширения $k_1$). Вопрос о нахождении рациональных точек при $\rho = 0$ был изучен Гильбертом (D. Hilbert) и Гурвицем (A. Hurwitz) [54]. При $\rho = 1$ Пуанкаре (H. Poincaré) [85] ввёл понятие *ранга* кривой (1). Под этим он разумеет следующее. Пусть $P_1(x_1, y_1)$ и $P_2(x_2, y_2)$ — две рациональные точки. Пусть $x = \varphi(u)$, $y = \psi(u)$ — эллиптические функции, удовлетворяющие соотношению (1), и пусть точкам $P_1$ и $P_2$ соответствуют значения $u_1$ и $u_2$ аргумента $u$. Для эллиптических функций имеет место *теорема сложения*

$$\varphi(u + v) = R[\varphi(u), \psi(u), \varphi(v), \psi(v)],$$
$$\psi(u + v) = S[\varphi(u), \psi(u), \varphi(v), \psi(v)],$$

где $R$ и $S$ — известные рациональные функции с коэффициентами из поля $k$. Отсюда следует, что значению $u_1 + u_2$ тоже соответствуют

рациональные значения $x$, $y$. Вообще, если значениям $u_1, u_2, \ldots, u_s$ аргумента $u$ соответствуют рациональные значения $x$, $y$, то это же имеет место для значения

$$m_1u_1 + m_2u_2 + \ldots + m_su_s, \tag{2}$$

где $m_1, m_2, \ldots, m_s$ — произвольные целые положительные или отрицательные числа. Если притом ни при каких целых значениях $m_1, m_2, \ldots, m_s$ не имеет места сравнение

$$m_1u_1 + m_2u_2 + \ldots + m_su_s \equiv 0 \tag{3}$$

по модулю периодов эллиптических функций $\varphi(u)$, $\psi(u)$, то различным значениям $m_1, m_2, \ldots, m_s$ будут соответствовать различные рациональные точки.

Максимальное число значений $u_1, u_2, \ldots, u_s$, не связанных сравнениями типа (3), называется *рангом* эллиптической кривой (1). Пуанкаре высказал гипотезу о конечности ранга для всякой эллиптической кривой, и Морделл (L. J. Mordell) [73] впервые доказал эту гипотезу. Его доказательство в несколько усовершенствованном виде приведено в книге Б. Н. Делоне и Д. К. Фаддеева ([2], стр. 324—331).

А. Вейль (A. Weil) [108] распространил результат Морделла на кривые произвольного жанра $p > 1$. Для этого, обобщая понятие рациональной точки, он ввёл понятие *рациональной системы точек*, т. е. системы точек, произведение которых даёт идеал в поле $k(x, y)$ (без расширения числового поля $k$) (см. § 15). Будем рассматривать рациональные системы из $\rho$ точек. Тогда, применяя проблему обращения (см. § 50), мы сопоставим каждой рациональной системе точек $P_1, P_2, \ldots, P_\rho$ систему значений переменных $u_1, u_2, \ldots, u_\rho$, причём симметрические функции от координат точек $P_1, P_2, \ldots, P_\rho$ выразятся как *абелевы функции* (т. е. частные от деления $\vartheta$-функций одного и того же порядка) от указанных значений $u_1, u_2, \ldots, u_\rho$.

Для абелевых функций, как и для эллиптических, имеет место теорема сложения. Это позволяет утверждать: если значения $(u_1, u_2, \ldots, u_\rho)$ и $(v_1, v_2, \ldots, v_\rho)$ соответствуют рациональным системам точек $\sum_1$, $\sum_2$, то и $(u_1 + v_1, u_2 + v_2, \ldots, u_\rho + v_\rho)$ соответствует рациональной системе точек. Если символически обозначить последнюю через $\sum_1 + \sum_2$, то рациональным системам

$$\sum_1, \sum_2, \ldots, \sum_s$$

точек будет соответствовать бесчисленное множество рациональных систем точек

$$m_1\sum_1 + m_2\sum_2 + \ldots + m_s\sum_s.$$

Максимальное число независимых среди систем $\sum_1, \sum_2, \ldots, \sum_s$ называется *рангом* кривой (1). Вейль доказал конечность ранга для всякой алгебраической кривой жанра $p > 1$.

Нетрудно определить сложение рациональных систем чисто алгебраически, не пользуясь $\vartheta$-функциями. При этом нам придётся особо выделить «начальную систему» $\sum_0$. Будем считать $\sum_0$, $\sum_1$, $\sum_2$ также символами, обозначающими дивизоры, являющиеся произведениями точек соответственных систем. Эти дивизоры могут быть определены в поле $k$. Сделаем предположение

$$\text{Изм } (\sum_0) = \text{Изм } (\sum_1) = \text{Изм } (\sum_2) = 1.$$

Дивизор $\sum_1 \sum_2$ имеет порядок $2p$, так что его класс не специален. Применяя теорему Римана-Роха, получим:

$$\text{Изм } (\sum_1 \sum_2) = p + 1.$$

Найдём делящийся на $\sum_0$ дивизор класса $(\sum_1 \sum_2)$. Из Изм $\sum_3 =$ $=$ Изм $\sum_0 = 1$ следует, что дивизор $\sum_3$ определяется однозначно. Его мы и будем считать «суммой» систем $\sum_1$ и $\sum_2$:

$$\sum_3 = \sum_1 + \sum_2 - \sum_0,$$

или просто

$$\sum_3 = \sum_1 + \sum_2.$$

Зигель (C. Siegel) [98] получил замечательный результат относительно *целых рациональных* (для которых значения $x$ и $y$ целы и рациональны) точек кривой (1):

Если кривая (1) имеет бесчисленное множество целых рациональных точек, то для неё $p = 0$, и притом (единственный) примитивный элемент поля $k(x, y)$ выражается через $x$, $y$ с коэффициентами из поля $k$.

## § 58. $Z$-функция

$Z$-функции были впервые введены Артином (E. Artin) [20] для эллиптических полей с конечным числовым полем $k$ и затем в несколько иной форме Шмидтом (F. K. Schmidt) [93] для произвольных полей алгебраических функций с конечным числовым полем $k$.

Пусть $k$ — конечное поле и пусть $p$ будет число его элементов (в общем случае степень простого числа). Пусть поле $k(x, y)$ задано уравнением

$$f(x, y) = 0. \tag{1}$$

Относительно дивизоров поля $k(x, y)$ имеет место следующее:

I. Группа $D$ всех дивизоров (относительно умножения) имеет подгруппу $D_0$ дивизоров нулевого порядка, и факторгруппа $\frac{D}{D_0}$ изоморфна с аддитивной группой всех целых чисел.

Пусть $Q$ — произвольный дивизор и пусть $Q_1$ — дивизор наименьшего порядка $d$, который можно выбрать раз навсегда. Тогда имеет место

$$Q = Q_1^s \cdot Q_0,$$

где $s$ — целое число, а $Q_0$ — дивизор нулевого порядка.

II. Существует только конечное число целых дивизоров, порядок которых не превышает данного числа $n$.

В самом деле, норма целого дивизора $Q$ порядка $\leqslant n$ относительно $k(x)$ есть полином от $x$ степени $\leqslant n$; таких полиномов всего $\leqslant p^{n+1}$.

III. Существует только конечное число классов нулевого порядка.

В самом деле, пусть $Q_0$ — произвольный дивизор нулевого порядка. Возьмём целое число $m \geqslant 2p-1$ и целый дивизор $Q_1$ порядка $m$. Дивизор $Q_0Q_1$ будет иметь порядок $m$, в силу чего его класс $(Q_0Q_1)$ не специален. В силу этого

$$\text{Изм } (Q_0Q_1) = m - p + 1 > 1.$$

Это означает, что класс $(Q_0Q_1)$ содержит целые дивизоры Пусть один из них есть $Q_2$. Тогда

$$Q_0 \sim \frac{Q_2}{Q_1}.$$

Но так как целых дивизоров порядка $m$ всего конечное число, то и число классов порядка нуль конечно, ч. т. д. Обозначим это число через $h$.

Чтобы гарантировать существование целого дивизора порядка $m$, возьмём $m = nq$, где $n$ — порядок элемента $x$. Тогда числитель любого полинома $q$-й степени от $x$ есть целый дивизор порядка $m$.

IV. Если $m$ делится на $d$, то существует ровно $h$ классов $m$-го порядка.

Эти классы получатся, если мы умножим каждый класс нулевого порядка на один и тот же дивизор того же порядка.

V. Если класс $\mathfrak{Q}$ имеет измерение $r$, то в нём содержится ровно $\frac{p^r-1}{p-1}$ дивизоров.

Пусть $Q_1, Q_2, \ldots, Q_r$ — система линейно независимых целых дивизоров класса $\mathfrak{Q}$. Всякий целый дивизор этого класса может быть представлен в форме

$$c_1Q_1 + c_2Q_2 + \ldots + c_rQ_r,$$

где константы $c_i$ пробегают значения из поля $k$, т. е. по $p$ значений каждая. Из получающихся $p^r$ дивизоров надо исключить нулевой, для которого

$$c_1 = c_2 = \ldots = c_r = 0.$$

Но дивизоры определяются с точностью до мультипликативной константы, так что различных дивизоров будет

$$\frac{p^r-1}{p-1}.$$

Пусть $Q$ — целый дивизор, $m$ — его порядок. Введём обозначение

$$|Q| = p^m. \tag{2}$$

Очевидно, что

$$|Q_1Q_2| = |Q_1| \cdot |Q_2|. \tag{3}$$

Определим $Z$-функцию при помощи равенства

$$Z(s) = \prod_P \frac{1}{1-|P|^{-s}}, \tag{4}$$

где $s$ — комплексная переменная, а произведение распространено на все простые дивизоры $P$ поля $k(x, y)$. Это произведение обычным образом преобразовывается в сумму

$$Z(s) = \sum_Q |Q|^{-s}, \tag{5}$$

распространённую на все целые дивизоры поля $k(x, y)$.

Чтобы преобразовать $Z(s)$ к виду, удобному для обозрения, будем собирать вместе члены ряда (5), имеющие тот же порядок $m = nd$. Пусть они образуют классы

$$\mathfrak{Q}_n^{(1)}, \mathfrak{Q}_n^{(2)}, \ldots, \mathfrak{Q}_n^{(h)}.$$

Введём обозначение

$$p_1 = p^d.$$

Тогда формулу (5) можно переписать так:

$$Z(s) = \frac{1}{p-1} \sum_{n=1}^{\infty} \sum_{i=1}^{h} \left(p^{\text{Изм } \mathfrak{Q}_n^{(i)}} - 1\right) \cdot p_1^{-ns} =$$

$$= \frac{1}{p-1} \sum_{n=1}^{\infty} \sum_{i=1}^{h} p^{\text{Изм } \mathfrak{Q}_n^{(i)}} \cdot p_1^{-ns} - \frac{h}{p-1} \cdot \frac{1}{p_1^s - 1}.$$

Разобьём внешнее суммирование полученного ряда на сумму от 1 до $q_0 - 1$ и от $q_0$ до $\infty$, где наименьшее число, при котором

$$q_0 \cdot d \geqslant 2p - 2.$$

Тогда во втором из полученных рядов все классы не специальны, за исключением класса дифференциалов $\mathfrak{W}$, так что для них теорема

Римана-Роха даёт:

$$(6) \qquad \text{Изм } \mathfrak{Q}_n^{(i)} = \text{Пор } \mathfrak{Q}_n^{(i)} - \rho + 1 = nd - \rho + 1.$$

Поэтому суммирование второго ряда даёт:

$$\frac{h}{p-1}\sum_{n=q_0}^{\infty} p^{dn-\rho+1}\cdot p_1^{-ns} = \frac{hp^{1-\rho}}{p-1}\cdot\frac{p_1^{q_0(1-s)}}{1-p_1^{1-s}}\cdot$$

Кроме того, в силу того, что класс $\mathfrak{W}$ удовлетворяет не соотношению (6), а такому:

$$\text{Изм } \mathfrak{W} = \text{Пор } \mathfrak{W} - \rho + 2 = \rho,$$

в выражении для $Z(s)$ появится разность двух членов:

$$\frac{p^{\rho}}{p-1}\cdot p_1^{-q_0 s} - \frac{p^{\rho-1}}{p-1}\cdot p_1^{-q_0 s} = p^{\rho-1}\cdot p_1^{-q_0 s}.$$

Таким образом

$$(7) \qquad Z(s) = \frac{1}{p-1}\sum_{n=1}^{q_0-1}\sum_{i=1}^{h} p^{\text{Изм } \mathfrak{Q}_n^{(i)}}\cdot p_1^{-ns} + \\ + \frac{hp^{1-\rho}}{p-1}\cdot\frac{p_1^{q_0(1-s)}}{1-p_1^{1-s}} - \frac{h}{p-1}\cdot\frac{1}{p_1^{s}-1} + p^{\rho-1}\cdot p_1^{-q_0 s}.$$

Произведённые нами бесконечные суммации законны только для значений $s$, вещественные части которых больше единицы; формула же (7) служит для аналитического продолжения функции $Z(s)$ на всю плоскость. Из неё мы заключаем, что $Z(s)$ имеет период

$$\frac{2\pi i}{\log P_1};$$

далее, она мероморфна, имея простые полюсы в точках

$$s = \frac{2\pi i\nu}{\log p_1} \qquad (-\infty < \nu < +\infty)$$

с вычетами

$$-\frac{h}{(p-1)\log P_1},$$

а также в точках

$$s = 1 + \frac{2\pi i\nu}{\log p_1} \qquad (-\infty < \nu < +\infty)$$

с вычетами

$$\frac{h\cdot P^{1-\rho}}{(p-1)\log P_1}.$$

VI. Всякое поле $k(x, y)$ с конечным числовым полем $k$ непременно содержит дивизоры первого порядка.

Другими словами, $d = 1$. Для доказательства расширим поле $k$, присоединив к нему корень неприводимого в $k$ уравнения $d$-й степени. Из того, что для каждой степени существует одно и только одно конечное поле, следует, что такое расширение можно произвести одним единственным образом. Именно, если $p = \tilde{p}^u$ где $\tilde{p}$ — простое число, то $k$ образуется первообразным корнем уравнения

$$x^{\tilde{p}^u - 1} - 1 = 0,$$

а расширение $k_1$ — первообразным корнем уравнения

$$x^{\tilde{p}^{ud} - 1} - 1 = 0.$$

Присоединяя к $k_1$ элементы $x$, $y$, мы придём к алгебраическому расширению $k_1(x, y)$ поля $k(x, y)$. Возьмём произвольный простой дивизор $P$ поля $k(x, y)$ порядка $m = nd$. Его норма есть неприводимый в поле $k$ полином степени $nd$. В поле $k_1$ он разлагается на $d$ неприводимых множителей, каждый степени $n$. Из этого следует, что в поле $k_1(x, y)$ дивизор $P$ разлагается в произведение $d$ простых дивизоров:

$$P = P_1 \cdot P_2 \ldots P_d,$$

каждый из которых имеет порядок $n$. В частности, входящие в $k(x, y)$ дивизоры порядка $d$ разлагаются в произведения $d$ дивизоров 1-го порядка. Поэтому для поля $k_1(x, y)$ роль $d$ играет 1, а роль $p$ число $p_1 = p^d$. Из

$$|P| = p^m$$

для поля $k(x, y)$ вытекает

$$|P_1| = |P_2| = \ldots = |P_d| = p_1^n = p^{dn} = p^m$$

для поля $k_1(x, y)$. Обращаясь к выражению (4) для $Z(s)$ и сличая множители в обеих функциях

$$Z_{k(x, y)}(s), \quad Z_{k_1(x, y)}(s),$$

соответствующих полям $k(x, y)$ и $k_1(x, y)$, мы видим, что в обе входят одни и те же множители, но во вторую из них каждый множитель входит в $d$ раз чаще. Отсюда мы имеем:

$$Z_{k_1(x, y)}(s) = \{Z_{k(x, y)}(s)\}^d. \tag{8}$$

Отсюда следует, что функция $Z_{k_1(x, y)}(s)$ должна иметь полюсы порядка $d$, что в силу доказанного невозможно, если $d > 1$. Таким образом $d = 1$, ч. т. д.

Из этой теоремы следует, что в формуле (7) мы должны положить $p_1 = p$, $q_0 = 2\rho - 2$, так что

$$(9)\quad Z(s) = \frac{1}{\rho - 1} \cdot \sum_{n=1}^{2\rho-3} \sum_{i=1}^{h} p^{\text{Изм } \Phi_n^{(i)}} \cdot p^{-ns} + \\ + \frac{hp^{-(\rho-1)(2s-1)}}{(p-1)(1-p^{1-s})} - \frac{h}{p-1} \cdot \frac{1}{p^s - 1} + p^{-(\rho-1)(2s-1)}.$$

VII. Имеет место функциональное соотношение

$$(10)\quad Z(1-s) = p^{(\rho-1)(2s-1)} \cdot Z(s).$$

Вместо него можно рассматривать равносильное ему соотношение

$$(11)\quad \Xi(s) = \Xi(-s),$$

полагая

$$(12)\quad \Xi(s) = p^{s(\rho-1)} \cdot Z\left(\frac{1}{2} + s\right).$$

Для $Z$-функций имеет место так называемое *риманово предположение*, состоящее в том, что все нулевые точки $Z$-функций имеют вещественные части $\frac{1}{2}$. Это было доказано Гассе (H. Hasse) [44] для случая эллиптических полей, а затем Вейлем (A. Weil) [109, 110] для общего случая. Доказательство этого предположения даёт возможность произвести асимптотические оценки числа решений некоторых сравнений с двумя неизвестными при весьма больших простых модулях (Морделл; L. J. Mordell) [74]. Оно также играет роль в отделах теории алгебраических функций, которые смыкаются с высшими отделами теории алгебраических чисел. Именно, изучение *комплексного умножения эллиптических функций* привело к понятию *полей классов*. См. Гассе [43, 45, 46].

## СИСТЕМАТИЧЕСКИЙ ПУТЕВОДИТЕЛЬ ПО ЛИТЕРАТУРЕ

Наиболее полным курсом по арифметической теории алгебраических функций является книга Гензеля (K. Hensel) и Ландсберга (G. Landsberg) [51], из которой я много заимствовал при составлении настоящей книги. По ней можно также познакомиться со многими геометрическими результатами, выведенными арифметическим путём. Эта книга не является чисто арифметической, поскольку её авторы в своих выводах широко пользуются теорией аналитических фувкций, римановыми поверхностями и рядами.

Весьма близкой по установкам, но значительно меньшей по объёму книгой арифметнко-функционального направления является книга Юнга (H. W. E. Jung) [62]. В ней не всё выводится до коица; она ценна многочисленными примерами.

Выдержанная до конца арифметическая теория изложена в статье Дедекинда (R. Dedekind) и Вебера (H. Weber) [32]. Её содержание изложено также в 3-м томе курса алгебры Вебера [106], но здесь теория идеалов заменена теорией функционалов, которую Вебер развил по идеям Кронекера (L. Kronecker).

В статьях Шмидта (F. K. Schmidt) [93, 94] содержится современное изложение арифметической теории, в котором числовое поле $k$ не предполагается ни алгебраически замкнутым, ви даже совершенным.

Из литературных обзоров по арифметической теории алгебраических функций укажем на энциклопедическую статью Гензеля [50], а также на статью Э. Нётер (E. Noether) [77]. Имеется обзор Гассе (H. Hasse) [48], посвящённый современным проблемам, связывающим теорию алгебраических функций с теорией чисел.

К арифметическому направлению примыкает книга Фильдса (J. Ch. Fields) [38], в которой выводы опираются на разложения в степенные ряды. В ней все выводы даны при самых общих предположениях и довольно громоздки.

Перейдём к функциональному направлению. Первое систематическое изложение теории, основанное на римановых поверхностях, сделано Нейманном (C. Neumann) [76]. Весьма тщательное современное обоснование теории римановых поверхностей и её применения в теории алгебраических, а также более общих функций дано Вейлем (H. Weyl) [111]. Первоначальные сведения по теории алгебраических функций в функциональном направлении хорошо получить по книжке Ландфридта (E. Landfriedt) [68].

Прекрасная книга Крацера (A. Krazer) [66] посвящена высшим отделам теории $\vartheta$-функциям и проблемам обращения; в ней содержится много литературных ссылок. С этим же отделом можно познакомиться по другой книжке Ландфридта. Наиболее обстоятельно проблема обращения изложена в диссертации Роста (G. Rost) [91].

Следуя знаменитому мемуару Абеля (N. H. Abel) [17], Брио (Ch. Briot) [26] изложил теорию в функциональном направлении, для подсчётов применяя диаграмму Ньютона, а вместо римановых поверхностей пользуясь обходами вокруг критических точек (lacets). Так же поступают в своей книге Клебш (A. Clebsch) и Гордан (P. Gordan) [30] и Долбня в своей диссертации [4].

Почти одновременно с Риманом и даже более полно теория абелевых интегралов и функций была развита на лекциях Вейерштрасса (K. Weierstrass) [107]. Его изложение широко использует разложения функций в ряды по нескольким переменным. В направлении Вейерштрасса написана на русском

и французском языках книга Тихомандрицкого [12, 101], а также небольшая книжка Ермакова [5], в которой весьма чётко выражены основные идеи теории, но не всегда верны доказательства и даже формулировки.

Обозначения и термины у Вейерштрасса значительно отличаются от римановых. Обозначений Вейерштрасса придерживается также Шоттки (F. Schottky) [95]. Обширная монография Бэкера (H. F. Baker) [21], посвящённая абелевым функциям, следует, главным образом, Вейерштрассу, но часто пользуется методами геометрической и арифметической теорий. Она содержит массу примеров. Её элементарные главы написаны несколько бегло.

В смешанно-функционально-геометрическом направлении написана книга Аппелля (P. Appell) и Гурса (É. Goursat) [19]. Она представляет типичный образец французской книги со всеми её достоинствами и недостатками. В таком же направлении написана современная небольшая монография Блисса (G. A. Bliss) [22]; по ней удобно знакомиться с некоторыми специальными пунктами теории; в частности, там детально разобран вопрос о разрешении особых точек.

С геометрической теорией алгебраических функций можно познакомиться по прекрасной книге Энриквеса (F. Enriques) и Чизини (O. Chisini) [36]. Геометрическая теория (или алгебраическая геометрия) является наиболее развитой из рассматриваемых теорий; в её направлении было получено наибольшее количество результатов. Познакомиться с ними можно или по обзорной монографии Брилля (A. Brill) и Нётера (M. Noether) [25], или по более современной монографии Севери (F. Severi), переведённой на немецкий язык Лёффлером (E. Löffler) [97]. Доступное введение в теорию даёт статья Грёбнера (W. Gröbner) [41].

Перейдём к обзору литературы по главам и параграфам настоящей книги (две последние главы здесь не рассматриваются, поскольку они сами являются обзорами).

## Глава I. Теория полей

Штейниц (E. Steinitz) [99] в классическом мемуаре, впоследствии переизданном в виде книги, положил начало современной теории полей, с которой можно также познакомиться по книге Гаупта (O. Haupt) [49] или ван-дер-Вардена (B. L. van-der-Waerden) [104].

§ 4. *Расширения полей, алгебраические.* С ними подробнее можно познакомиться по любому курсу теории алгебраических чисел, в частности, по Гекке ( E. Hecke) [1] (имеется русский перевод), а также по цитированному мемуару Штейница.

§ 5. *Кратные корни. Совершенные поля.* С абстрактной теорией корней алгебраических уравнений можно, например, познакомиться по книжке Гассе [47], а на русском языке — по учебнику Окунева [9]. О совершенных полях говорится у Штейница.

§ 7. *Теорема Люрота.* Она впервые доказана у Люрота (P. Lüroth) [72] геометрическим путём. Нетто (E. Netto) [75] дал алгебраическое доказательство, воспроизведённое во 2-м томе курса Вебера (H. Weber) [106], стр. 472—474. Оно эффективно. Штейниц [99] предложил новое доказательство, интересное по идее, но не эффективное. Островский (A. Ostrowski) [79] несколько видоизменил доказательство Штейница и доказал несколько других фактов. В настоящей книге приведено эффективизированное доказательство Островского.

## Глава II. Поле алгебраических функций

Кроме цитированных статьи Дедекинда и Вебера [32] и книг Вебера [106] и Гензеля-Ландсберга [51], обоснованию теории поля алгебраических функций посвящены две современные статьи Шмидта (F. K. Schmidt) [93, 94].

В них особое внимание уделено полям простой характеристики, для которых обычное изложение теории неприменимо, поскольку их дискриминант иногда обращается в нуль, в силу чего понятие дополнительного базиса на них распространить невозможно. Шмидт вводит понятие квазидополнительного базиса, что даёт ему возможность ввести инвариантный класс дивизора, аналогичный классу дифференциалов. Я предпочёл просто рассматривать класс дифференциалов внутри подполя типа $k(x^{p^r}, y^{p^s})$ поля $k(x, y)$.

§§ 8—11. С вводимыми в этих параграфах понятиями можно подробно познакомиться по курсам теории алгебраических чисел.

§ 12. *Нормальный базис.* Определение нормального базиса я, с некоторым видоизменением, взял у Дедекинда-Вебера. У Гензеля-Ландсберга, Юнга и Шмидта оно другое — более общее. Кроме того, данное здесь понятие нормального базиса относится к его поведению вблизи $z = \infty$, в то время как у перечисленных авторов оно прилагается к конечным точкам — они строят базисы идеалов, целых и дробных.

Также у Дедекинда-Вебера взято определение показателей. У Шмидта оно заменено более общим современным понятием оценки (Bewertung), которое в последнее время завоёвывает себе всё больше и больше прав гражданства в различных отделах алгебры. При нашем изложении в нём не было настоятельной необходимости; с другой стороны, его введение лишило бы изложение большой доли наглядности.

## Глава III. Измерение классов

Литература та же.

## Глава IV. Теорема Римана-Роха и её приложения

§§ 22, 23. Теорема Римана-Роха. Вывод взят у Дедекинда-Вебера.

§ 24. Теорема Нётера о пробелах. См. М. Нётер (M. Noether) [78]. Ни у Дедекинда-Вебера, ни у Гензеля-Ландсберга эта теорема в общем виде не помещена. У Гензеля-Ландсберга она приведена только для Вейерштрассова случая. В настоящем виде, не столь точно формулированном, она приведена у Бэкера [21], а также у Чеботарёва [103].

§ 25. *Точки Вейерштрасса.* Их теория была дана Гурвицем (A. Hurwitz) [57]. Она изложена у Гензеля-Ландсберга [51], где рассмотрены также определители Вронского более низких порядков и освещено геометрическое значение их числителей.

§ 26. *Теорема Клиффорда и её обобщение.* См. Клиффорд (W. K. Clifford) [31]. Даётся также в книге Севери [97], стр. 131. Изложенное здесь обобщение дано Чеботарёвым [103], в не вполне корректном виде. Здесь исправлены и выводы, и самые результаты.

## Глава V. Структура полей алгебраических функций

§§ 28—30. *Понятие и элементарные свойства групп преобразований* даны у Чеботарёва [14]. С конечными группами и их приложением к теории Галуа (что понадобится в § 41) можно познакомиться по другой книге Чеботарёва [13].

§ 31. *Группа преобразований в себя.* См. Гурвиц [57]. Это изложено также у Гензеля-Ландсберга.

§ 32. *Особые точки.* См. Кронекер (L. Kronecker) [67]. У Гензеля-Ландсберга содержится достаточно подробная теория особых точек с арифметической точки зрения, но с геометрическим толкованием. См. также Блисс [22].

§ 33. *Теорема Кронекера.* Изложена у Гензеля-Ландсберга и подробно рассматривается у Блисса [22], где отдельно рассматривается в функциональной и в проективной формулировках. Здесь изложение Гензеля-Ландсберга арифметизировано, т. е. я избежал пользования разложениями в ряды.

§ 34. *Число параметров поля алгебраических функций.* Первоначальное, не строгое, доказательство дано Риманом (B. Riemann) [89]. Приводимое здесь доказательство взято из Гензеля-Ландсберга.

§ 35. *Подполя.* Изложено, хотя не так подробно, у Гурвица [56, 57]. См. также Юнг (H. W. E. Jung) [60].

§ 36. *Результаты Гурвица в теории групп преобразований в себя.* См. Гурвиц [57].

### Глава VI. Применение теории аналитических функций

§ 37. *Сведения из общей теории аналитических функций.* См. любой курс теории аналитических функций, например, Привалова [10].

§ 38. *Диаграмма Ньютона.* Её идея, повидимому, принадлежит Ньютону (J. Newton) [8]. Эту диаграмму впервые применил к теории алгебраических функций Пюизё (V. Puiseux) [87]. Наиболее полно все доказательства проведены у Гензеля-Ландсберга [51]. В монографии Чеботарёва [15] указана вся обширная сфера применения диаграммы Ньютона, а также приведена относящаяся к ней литература.

### Глава VII. Риманова поверхность

§ 40. *Построение римановой поверхности.* См. статью Римана [89], книгу Неймана [76], Аппелля (P. Appell) и Гурса (É. Goursat) [19], Гензеля-Ландсберга [51], Юнга [62]. Более строгое топологическое и теоретико-функциональное обоснование теории римановых поверхностей дано Вейлем (H. Weyl) [111]. См. также статью Радо (T. Radó) [88].

§ 41. *Группа монодромии.* Это понятие впервые встречается у Жордана (C. Jordan) [59], стр. 277—279. Понятие группы монодромии фактически используется у Гурвица [56, 57].

Опубликован отрывок из письма покойного Гербраида (J. Herbrand) [52] к Э. Нётер, в котором он указывает на решённую им проблему определения поля коэффициентов, присоединение которого к полю $k$ достаточно для того, чтобы группа Галуа поля $k(x, y):k(x)$ совпала с группой монодромии. Согласно его утверждению, проблема усложняется, если группа Галуа имеет центр. Среди его бумаг никаких дальнейших указаний на способ решения проблемы не оказалось.

§ 42. *Элементарные сведения из топологии.* Они даются у Неймана [76] и у Гензеля-Ландсберга [51]. Подробнее с ними можно познакомиться по какому-нибудь курсу комбинаторной топологии, например, по Зейферту (H. Seifert) и Трельфаллю (W. Threlfall) [6], глава VI (имеется русский перевод).

§ 43. *Порядок связности римановой поверхности.* См. книгу Неймана [76] и Гензеля-Ландсберга [51].

§ 44. *Число замкнутых вещественных ветвей кривой.* Первоначальное доказательство Гарнака (A. Harnack) [42] имеет геометрический характер. Приводимое мной доказательство взято из литографированного курса лекций Клейна (F. Klein) [64] и содержится также в книге Севери (97].

Работы Гильберта (D. Hilbert) [53] и Петровского (J. Petrowsky) [81] посвящены вопросам взаимного расположения ветвей кривой.

### Глава VIII. Абелевы интегралы

Содержание этой главы изложено более подробно во всех цитированных книгах теоретико-функционального направления, в особенности в книге Бэкера (H. F. Baker) [21]. В статье Дедекинда-Вебера [32] содержится чисто арифметический метод их классификации.

§ 47. *Теорема Абеля.* См. мемуар Абеля [17]. Подробно — в книге Бэкера.

---

## УКАЗАТЕЛЬ ЛИТЕРАТУРЫ


А) На русском языке:

1. *Э. Гекке.* Лекции по теории алгебраических чисел. М., 1940.
2. *Б. Н. Делоне* и *Д. К. Фаддеев.* Теория иррациональностей третьей степени. Труды Матем. ин-та им. Стеклова, т. 9. М. — Л., 1940.
3. *И. П. Долбня.* Новое доказательство теоремы Абеля, относящейся до интегрирования дифференциалов вида $\frac{\rho dx}{\sqrt{R}}$, $\rho$ и $R$ — целые функции. Собр. протоколов заседаний секции физ.-мат. наук о-ва естествознания при Казанском ун-те **6** (1888), стр. 307—324.
4. *И. Долбня.* Исследование по теории абелевых интегралов. Спб., 1896.
5. *В. П. Ермаков.* Теория абелевых функций без римановых поверхностей. Киев, 1897.
6. *Г. Зейферт* и *В. Трельфалль.* Топология. М., 1938.
7. *Е. И. Золотарёв.* Теория целых комплексных чисел с приложением к интегральному исчислению. Докт. дисс. Спб., 1874. См. также Полное собрание сочинений, вып. 1, Л., 1931, стр. 161—360.
8. *Исаак Ньютон.* Математические работы. Метод флюксий и бесконечных рядов с приложением к геометрии кривых. М., 1937, стр. 33—44.
9. *Л. Я. Окунев.* Высшая алгебра. М., 1940.
10. *И. И. Привалов.* Введение в теорию функций комплексного переменного. М., 1927.
11. *И. Л. Пташицкий.* Об интегрировании в конечном виде эллиптических дифференциалов. Спб., 1888.
12. М. А. *Тихомандрицкий.* Основания теории абелевых интегралов. Харьков, 1895.
13. *Н.Чеботарёв.* Основы теории Галуа. 1. Л., 1934.
14. *Н. Г. Чеботарёв.* Теория групп Ли. М., 1940.
15. *Н. Г. Чеботарёв.* Многоугольник Ньютона и его роль в современном развитии математики. Исаак Ньютон. Сборник статей к трёхсотлетию со дня рождения. М., 1943, стр. 99—126.

B) На иностранных языках:

16. *N. H. Abel.* Sur l'intégration de la formule différentielle $\frac{\rho \cdot dx}{\sqrt{R}}$, $R$ et $\rho$ étant des fonctions entières. — Journ. für reine angew. Math. **1** (1826), p. 185—221. — Oeuvres complètes **1**, Kristiania, 1881, p. 104—144.
17. *N. H. Abel.* Mémoire sur une propriété générale d'une classe très-étendue de fonctions transcendentes. — Mém. prés. par divers savants **7** (1841). — Oeuvres complètes **1**, Kristiania 1881, p. 145—211.
18. *P. Appell.* Sur les intégrales de fonctions à multipicateurs et leur application au développement des fonctions abéliennes en series trigonométriques. — Acta Math. **13** (1890), p. 1—174.
19. *P. Appell* et *É. Goursat.* Théorie des fonctions algébriques et de leurs intégrales. — 1-ère éd., Paris, 1895. — 2-e éd., Paris, 1929.
20. *E. Artin.* Quadratische Körper im Gebiete der höheren Kongruenzen. — Math. Zeitschr. **19** (1924); I, S. 153—206; II, S. 207—246.

21. *H. F. Baker.* Abel's Theorem and the Allied Theory Including the Theory of the Theta Functions. — Cambridge, 1897.
22. *G. A. Bliss.* Algebraic Functions. Amer. Math. Soc. Coll. Publ., **16**. New. York, 1933.
23. *A. Brill.* Über Entsprechen von Punktsystemen auf einer Kurve. — Math. Ann. **6** (1873), S. 33—65.
24. *A. Brill.* Über die Korrespondenzformel. Math. Ann. **7** (1874), S. 607—622.
25. *A. Brill* und *M. Noether.* Die Entwicklung der Theorie der algebraischen Funktionen in älterer und neuerer Zeit. Jahresber., DMV 3 (1894).
26. *Ch. Briot.* Théorie des fonctions abéliennes. Paris, 1879.
27. *G. Castelnuovo.* Sulla razionalità delle involuzioni piane. Math. Ann. **44** (1894), p. 125—155.
28. *A. Cayley.* Note sur la correspondance de deux points sur une courbe. C. R. **62** (1866), p. 586—590.
29. *E. B. Christoffel.* Vollständige Theorie der Riemannschen ϑ-Function. Math. Ann. **54** (1901), S. 347—399.
30. *A. Clebsch* und *P. Gordan.* Theorie der Abel'schen Functionen. Lpz., 1866.
31. *W. K. Clifford.* On the Classification of Loci. Philos. Trans. of Roy. Soc. of London **169** (1878), p. 663—681. Coll. Papers, p. 329—331.
32. *R. Dedekind* und *H. Weber.* Theorie der algebraischen Funktionen einer Veränderlichen. Journ. reine angew. Math. **92** (1879), S. 181—290.
33. *M. Deuring.* Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper. I. Journ. reine angew. Math. **177** (1937), S. 161—191. — II. Journ. reine angew. Math. **183** (1940), S. 25—36.
34. *J. Dolbnia.* Oeuvres mathématiques. Paris, 1913.
35. *F. Enriques.* Sopra una involuzione non razionale dello spazio. Rendic. Lincei **21** (1912), p. 81—83.
36. *F. Enriques* et *P. Chisini.* Courbes et fonctions algébriques d'une variable. Paris, 1926.
37. *G. Fano.* Sopra alcune varietà algebriche a tre dimensioni avente tutti i generi nulli. Atti Acc. Sc. Torino **43** (1908), p. 541—552.
38. *J. Ch. Fields.* Theory of the Algebraic Functions of a Complex Variable. Berlin, 1906.
39. *L. R. Ford.* Automorphic Functions. New York, 1929.
40. *A. Göpel.* Theoriae transcendentium Abelianarum primi ordinis adumbratio levis. — Journ. reine angew. Math. **35** (1847), S. 277. — Ostwalds Klassiker des ex. Wiss., Nr. 67.
40[1]. *H. Grell.* Beziehungen zwischen den Idealen verschiedener Ringe. — Math. Ann. 97 (1927), S. 490—523.
41. *W. Gröbner.* Severis Begründung der algebraischen Geometrie mittels des «Metodo rapido». Abh. Math. Sem. Hans. Univ. **12** (1938), S. 340—353.
42. *A. Harnack.* Ueber die Vielheiligkeit der ebenen algebraischen Curven. — Math. Ann. **10** (1876), S. 189—198.
43. *H. Hasse.* Neue Begründung der komplexen Multiplikation. — Journ. reine angew. Math. **165** (1931), S. 65—88.
44. *H. Hasse.* Beweis des Analogon der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. — Gött. Nachr., 1933, S. 253—262.
45. *H. Hasse.* Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. Abh. Math. Sem. Univ. Hamburg **10** (1934), S. 325—384.
46. *H. Hasse.* Zur Theorie der abstrakten elliptischen Funktionenkörper. Journ. reine angew. Math. **175** (1936), I, S. 55—62; II, S. 69—88; III, S. 193—208.
47. *H. Hasse.* Höhere Algebra. II. Sammlung Göschen., Nr. 932, Lpz. — B., 1937.

48. *H. Hasse.* Zur arithmetischen Theorie der algebraischen Funktionenkörper. Jahresber. DMV **52** (1942), S. 1—48.
49. *P. Haupt.* Einführung in die Algebra I, II, Leipzig, 1929.
50. *K. Hensel.* Arithmetische Theorie der algebraischen Funktionen. Encycl. der math. Wiss. II C. 5. Lpz., 1921.
51. *K. Hensel* und *G. Landsberg.* Theorie der algebraischen Funktionen einer Variablen und ihre Anwendung auf algebraische Kurven und Abelsche Integrale. Lpz., 1902.
52. *J. Herbrand.* Zur Theorie der algebraischen Funktionen. (Aus Briefen an E. Noether.) — Math. Ann. **106** (1932), S. 502.
53. *D. Hilbert.* Über die reellen Züge algebraischer Kurven. Math. Ann. **38** (1891), S. 115—139. Ges. Abh. **2**, Berlin, 1933, S. 415—436.
54. *D. Hilbert* und *A. Hurwitz.* Über die diophantischen Gleichungen von Geschlecht Null. Acta Math. **14** (1891), S. 217—224. Hilbert, Ges. Abh., **2**, Berlin, 1933, S. 258—263. Hurwitz, Math. Werke **2**, Basel, 1933, S. 116—121.
55. *A. Hurwitz.* Über algebraische Korrespondenzen und das verallgemeinerte Korrespondenzprinzip. Lpz., Ber. 1886, S. 10—38. Math. Ann. **28** (1887), S. 561—585. Math. Werke **1**, Basel, 1932, S. 163—188.
56. *A. Hurwitz.* Über Riemannsche Flächen mit gegebenen Verzweigungspunkten. Math. Ann. **39** (1891), S. 1—61. Math. Werke **1**, Basel, 1932, S. 321—383.
57. *A. Hurwitz.* Über algebraische Gebilde mit eindeutigen Transformationen in sich. Math. Ann. **41** (1893), S. 403—442. Math. Werke **1**, Basel, 1932, S. 391—430.
58. *C. G. J. Jacobi.* De functionalibus duarum variabilum quadrupliciter periodicis, quibus Theoria transcendentium Abelianarum innititus. Journ. für reine angew. Math. **13** (1835), S. 55—78.
59. *C. Jordan.* Traité des substitutions et des équations algébriques. Paris, 1870, p. 277—279.
60. *H. W. E. Jung.* Über die Transformation algebraischer Körper vom Range Eins. Journ. für reine angew. Math. **127** (1904), S. 103—115.
61. *H. W. E. Jung.* Arithmetische Theorie der algebraischen Funktionen zweier unabhängiger Veränderlichen. Encykl. der math. Wiss. II, C. 6. Lpz., 1921.
62. *H. W. E. Jung.* Einführung in die Theorie der algebraischen Funktionen einer Veränderlichen. Berlin — Leipzig, 1923.
63. *H. W. E. Jung.* Algebraische Flächen. Hannover, 1925.
64. *F. Klein.* Autographierte Vorlesungen über Riemannsche Flächen. — Göttingen, 1892.
65. *R. König.* Zur arithmetischen Theorie der auf einem algebraischen Gebilde existierenden Funktionen. Lpz. — Ber. **69** (1911), S. 348—368.
66. *A. Krazer.* Lehrbuch der Thetafunktionen. Lpz., 1903.
67. *L. Kronecker.* Über die Discriminante algebraischer Funktionen einer Variablen. Journ. reine angew. Math. **91** (1881), S. 301—334.
68. *E. Landfriedt.* Theorie der algebraischen Funktionen und ihrer Integrale. Sammlung Schubert XXXI. Lpz., 1902.
69. *E. Landfriedt.* Thetafunktionen und hyperelliptische Funktionen. Sammlung Schubert XLVI. Lpz., 1902.
70. *S. Lie.* Die Theorie der Translationsflächen und das Abelsche Theorem. Lpz. Ber. **48** (1896), S. 141—198.
71. *S. Lie.* Das Abel'sche Theorem und die Translationsmannigfaltigkeiten. Lpz. Ber. **49** (1897), S. 181—248.
72. *P. Lüroth.* Beweis eines Satzes über rationale Curven. Math. Ann. **9** (1876), S. 163—165.
73. *L. J. Mordell.* On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees. — Proc. Cambr. Philos. Soc. **21** (1922), p. 179—192.

74. *L. J. Mordell.* The number of solutions of some congruences in two variables. Math. Zeitschr. **37** (1933), p. 193—209.
75. *E. Netto.* Beweis eines Lüroth-Gordanschen Satzes. Math. Ann. **46** (1895), S. 310—318.
76. *C. Neumann.* Vorlesungen über Riemann's Theorie der Abelschen Integrale. 2-te Aufl. Lpz., 1884.
77. *E. Noether.* Die arithmetische Theorie der algebraischen Funktionen einer Veränderlichen in ihrer Beziehung zu den übrigen Theorien und zu der Zahlkörpertheorie. Jahresber. DMV **28** (1919), S. 182—203.
78. *M. Noether.* Beweis und Erweiterung eines algebraisch funktionentheoretischen Satzes des Herrn Weierstrass. Journ. reine angew. Math. **97** (1884), S. 224—229.
79. *A. Ostrowski.* Bemerkungen über die Struktur von Ringen, die aus Polynomen in einer Variabel bestehen. Acta Arithm. **1** (1935), S. 19—42.
80. *P. Painlévé.* Leçons sur la théorie analytique des équations différentielles professées à Stockholm. Paris, 1897.
81. *J. Petrowsky.* On the topology of Real Plane Algebraic Curves. Ann. of Math. **39** (1938), p. 189—209.
82. *É. Picard* et *G. Simart.* Théorie des fonctions algébriques de deux variables indépendantes. Tome 1, 2. Paris, 1897, 1900, 1904, 1906.
83. *H. Poincaré.* Remarques diverses sur les fonctions abéliennes. Journ. de math. pures et appl. (5) **1** (1895), p. 219—314.
84. *H. Poincaré.* Sur les surfaces de translation. Bull. Soc. Math. de France **29** (1901), p. 61—86.
85. *H. Poincaré.* Sur les propriétés arithmétiques des courbes algébriques. Journ. de math. pures et appl. (5) **7** (1901), p. 161—233.
86. *F. Prym* und *G. Rost.* Theorie der Prymschen Funktionen erster Ordnung im Anschluss an die Schöpfung Riemanns. Lpz., 1911.
87. *V. Puiseux.* Recherches sur les fonctions algébriques. Journ. de math. pures et appl. **15** (1850), p. 365—480.
88. *T. Radò.* Über den Begriff der Riemannschen Fläche. Acta Univ. Szeged. **2** (1924).
89. *B. Riemann.* Theorie der Abelschen Funktionen. Journ. für reine angew. Math. **54** (1857), S. 115—155. — Ges. math. Werke. Lpz. 1876, S. 129.
89¹. *B. Riemann.* Über das Verschwinden der Theta-Functionen. 1865. Ges. math. Werke. Lpz. 1876, S. 198.
90. *G. Rosenhain.* Mémoire sur les fonctions de deux variables et à quatre périodes qui sont les inverses des intégrales ultra-elliptiques de la première classe. Mém. prés. par divers savants. Sc. math. et phys. **11** (1851), p. 383. Ostwalds Klassiker der ex. Wiss., Nr. 65.
91. *G. Rost.* Theorie der Riemann'schen Thetafunktion. Hab. Schrift. Würzburg, 1901.
92. *W. Schmeidler.* Über Verzweigungspunkte bei Körpern von algebraischen Funktionen mehrerer Veränderlicher. Journ. für reine angew. Math. **167** (1932), S. 248—263.
93. *F. K. Schmidt.* Analytische Zahlentheorie in Körpern der Charakteristik *p*. Math. Zeitschr. **33** (1931). S. 1—32.
94. *F. K. Schmidt.* Zur arithmetischen Theorie der algebraischen Funktionen. I. — Math. Zeitschr. **41** (1936), S. 415—438.
95. *F. Schottky.* Abriss einer Theorie der Abelschen Functionen von drei Variabeln. Lpz., 1880.
96. *F. Schottky.* Zur Theorie der Abelschen Functionen von vier Variabeln. Journ. für reine angew. Math. **102** (1887), S. 304—352.
97. *F. Severi.* Vorlesungen über algebraische Geometrie. Übersetzt von D-r E. Löffler. Lpz. — B., 1921.
98. *C. Siegel.* Über einige Anwendungen diophantischer Approximationen. Abh. Preus. Akad. Berlin, 1929.

99. *E. Steinitz.* Algebraische Theorie der Körper. Journ. für reine angew. Math. **137** (1910), S. 167—309. — Abdruck: B. — Lpz., 1930.
100. *P. Tchebycheff.* Sur l'intégration des différentielles irrationnelles. Journ. de math. pures et appl. (1) **18** (1853), p. 87—111. — Oeuvres 1, St.-Petersbourg, 1899, p. 147—168.
101. *M. Tikhomandritzky.* Elements de la théorie des intégrales abéliennes. St.-Petersbourg, 1911.
102. *N. Tschebotaröw.* Über Flächen, welche Imprimitivitätssysteme in Bezug auf eine gegebene kontinuierliche Transformationsgruppe enthalten (Verallgemeinerte Schiebungsflächen). Rec. math. **34** (1927), S. 149—206.
103. *N. Tschebotaröw.* Über eine Verallgemeinerung eines Cliffordschen Satzes. Rendic. Circ. Mat. Pal. **55** (1931), p. 1—11.
104. *B. L. van der Waerden.* Moderne Algebra. I, II. Berlin, 1930, 1931.
105. *B. L. van der Waerden.* Einführung in die algebraische Geometrie. Berlin, 1939.
105¹. *H. Weber.* Über gewisse in der Theorie der Abelschen Functionen auftredende Ausnahmefälle. Math. Ann. **13** (1878), S. 35—48.
106. *H. Weber.* Lehrbuch der Algebra. Bd. 2. Braunschweig, 1899; Bd. 3. Braunschweig, 1908.
107. *K. Weierstrass.* Vorlesungen über die Theorie des Abelschen Transzendenten. Ges. math. Werke, Bd. 4. Berlin, 1902.
108. *A. Weil.* L'arithmétique sur les courbes algébriques. Acta Math. **52** (1928), p. 1—35.
109. *A. Weil.* Sur les fonctions algébriques à corps de constantes finis. C. R. **210** (1940), p. 592—594.
110. *A. Weil.* Riemann hypothesis in function-fields. Proc. Nation. Acad. of Sc. of USA **27** (1941), p. 345—347.
111. *H. Weyl.* Die Idee der Riemannschen Flächen. — 2-te Aufl. Lpz. — B., 1923.
112. *W. Wirtinger.* Untersuchungen über Thetafunctionen. Lpz., 1895.
113. *O. Zariski.* Algebraic Surfaces. Erg. der Math. und ihrer Grenzgebiete. III, 5. Berlin, 1935.
114. *O. Zariski.* Algebraic varieties over ground fields of characteristic zero. Amer. Journ. of Math., **62** (1940), p. 187—221.
115. *H. G. Zeuthen.* Lehrbuch der abzählenden Methoden der Geometrie., Lpz. u. B., 1914.

## ИМЕННОЙ УКАЗАТЕЛЬ



## ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

| Стр. | Строка | Напечатано | Должно быть | По чьей вине |
|---|---|---|---|---|
| 200 | 2 стр. сверху | $b_i \left(\frac{w^2}{u_i^2}\right)_{p_i} =$ | $b_i \left(\frac{w^2}{u_i^2}\right)_{P_i}$ | Ред. |
| 323 | 1 стр. сверху | условиям. | условиям, число которых равно | « |
| 381 | Строки 3, 7, 11 снизу | $\log P_1$ | $\log p_1$ | » |

Заказ 964. Чеботарев.