Арифметика алгебраических кривых

С. А. СТЕПАНОВ

С. А. СТЕПАНОВ

АРИФМЕТИКА АЛГЕБРАИЧЕСКИХ КРИВЫХ

МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1991

ББК 22.13
С79
УДК 511.5

Степанов С. А. **Арифметика алгебраических кривых.**— М.: Наука. Гл. ред. физ.-мат. лит., 1991.— 368 с.— ISBN 5-02-014607-2.

Дается систематическое изложение современного состояния, а также основных идей и методов одного из древнейших разделов математики — теории диофантовых уравнений. Основное внимание уделено рассмотрению наиболее изученного к настоящему времени случая — уравнений с двумя неизвестными. Изложение иллюстрируется большим числом конкретных примеров.

Для специалистов по теории чисел, алгебраической геометрии, математической логике и дискретной математике, а также для аспирантов и студентов старших курсов, специализирующихся в указанных областях.

Ил. 4. Библиогр. 290 назв.

Рецензент
доктор физико-математических наук профессор *В. А. Исковских*

Научное издание

СТЕПАНОВ Сергей Александрович
АРИФМЕТИКА АЛГЕБРАИЧЕСКИХ КРИВЫХ

Заведующий редакцией *А. П. Баева*
Редактор *И. Е. Морозова*
Художественный редактор *Г. М. Коровина*
Технический редактор *И. Ш. Аксельрод*
Корректор *Н. Д. Дорохова*

ИБ № 41250

Сдано в набор 06.11.90. Подписано к печати 20.11.91. Формат 60×90/16. Бумага тип. № 2. Гарнитура обыкновенная новая. Печать высокая. Усл. печ. л. 23. Усл. кр.-отт. 23. Уч.-изд. л. 23,32. Тираж 2000 экз. Заказ № 520. Цена 6 р.

Издательско-производственное и книготорговое объединение «Наука»
Главная редакция физико-математической литературы
117071 Москва В-71, Ленинский проспект, 15

Четвертая типография издательства «Наука»
630077 Новосибирск, 77, Станиславского, 25

С 1602030000—105 / 053(02)-91 21-91

©«Наука». Физматлит, 1991

ISBN 5-02-014607-2

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Данная книга основана на курсе лекций, прочитанном автором весной 1989 г. в Тата институте фундаментальных исследований (Бомбей), и посвящена наиболее изученному разделу диофантова анализа — теории уравнений с двумя неизвестными.

Проблематика теории диофантовых уравнений обманчиво проста и состоит (при классическом понимании) в отыскании рациональных или целочисленных решений неопределенных полиномиальных уравнений с целыми коэффициентами. Что касается вопроса о роли теории диофантовых уравнений в математике, то ответ на него (в значительной степени предугаданный еще К. Ф. Гауссом в его знаменитом изречении о королевском статусе теории чисел) удалось получить лишь в наши дни, после создания формализованной теории доказательств и теории алгоритмов. Он оказался необычайно эффектным: к теории диофантовых уравнений сводится в некотором смысле слова «почти вся» математика (см. [81 d]).

Указанная универсальность диофантовых уравнений требует, естественно, для их изучения огромного арсенала понятий и методов. В настоящее время этот арсенал достаточно солиден и включает в себя не только классические методы арифметики, геометрии чисел и анализа, но и современные методы алгебраической геометрии, математической логики и теории диофантовых приближений.

Еще сравнительно недавно (см. Диксон [44]) совокупность исследованных к тому времени диофантовых уравнений можно было уподобить многочисленным островам Полинезии и Микронезии, разбросанным по бескопечному простору Тихого океана. Многие из этих уравнений стали знаменитыми (вроде острова Гуам — первого клочка суши, открытого в Океании экспедицией Магеллана, и одновременно, по неведомому стечению обстоятельств, величественнейшей вершины затонувшего горного хребта, вознесшейся над прилегающей к ней Марианской впадиной на целую милю выше, чем Джомолунгма над уровнем моря); некоторые до сих пор сохранили налет экзотичности (вроде острова Таити); другие снискали печальную славу (подобно аттолу Бикини), и, наконец, очень многие диофантовы уравнения весьма специального вида в настоящее время почти полностью забыты (подобно многочисленным необитаемым островам).

Последние десятилетия ознаменовались созданием достаточно общих методов, применимых к широким классам диофантовых уравнений. Доказательство гипотезы Морделла о конечности числа рациональных точек на кривой рода $g > 1$ (Фалтингс [125])

и более ранние результаты о числе точек кривых над конечными полями (см. гл. I, V) привели к созданию сравнительно законченной теории диофантовых уравнений с двумя неизвестными. Значительный прогресс достигнут (см. гл. III) и при исследовании вопроса о структуре множества рациональных точек в исключительном случае кривых рода 1 (эллиптических кривых), а также в вопросе об эффективном перечислении множества целых точек на кривых достаточно общего вида (см. гл. VI). Развитие кругового метода Харди — Литтлвуда открыло возможность для установления целочисленной разрешимости ряда диофантовых уравнений с достаточно большим числом неизвестных. Обобщение метода Туэ на многомерный случай (В. Шмидт [146a]) позволило изучить структуру множества целочисленных решений широкого класса норменных уравнений с произвольным числом неизвестных. Наконец, отрицательное решение 10-й проблемы Гильберта (Ю. В. Матиясевич [82a]) привело к уяснению причин тех трудностей, которые связаны с изучением диофантовых уравнений, и значительно расширило наши представления о роли диофантовых уравнений в математике.

Первоначально автор предполагал нарисовать по возможности широкую картину современного состояния теории диофантовых уравнений, дать представление о всем спектре используемых в ней методов и, в то же время, продемонстрировать их внутреннее единство. Объем книги не позволил, однако, изложить аналитические аспекты теории и, в частности, результаты, полученные с помощью кругового метода Харди — Литтлвуда и методами теории диофантовых приближений. С этими аспектами читатель может познакомиться по книгам И. М. Виноградова [27 c], Р. Вона [28] и В. Шмидта [146 i]. Поэтому было решено ограничиться рассмотрением арифметических, алгебро-геометрических и логических аспектов вопроса. Но и после этого материал оказался слишком обширным. Поэтому значительную его часть пришлось изложить в виде задач (которых в книге более двухсот пятидесяти). Задачи рассчитаны на активно работающего читателя. Некоторые из них (отмеченные звездочкой) — весьма трудные и требуют для своего решения значительных творческих усилий. Как правило, такие задачи снабжены подробными указаниями, а наиболее сложные из них — еще и ссылками на источники.

По некоторым вопросам книга пересекается с «Основами диофантовой геометрии» С. Ленга [70 h]. Но в отличие от последней она не предполагает у читателя столь солидной математической подготовки и, в частности, знания современных методов алгебраической геометрии.

Предварительный текст книги был просмотрен А. Н. Паршиным и С. Ф. Сопруновым (гл. VI, VII). Автор выражает им благодарность за ряд полезных советов и замечаний.

ВВЕДЕНИЕ

В наиболее общей формулировке задача о решении диофантовых (неопределенных) уравнений состоит в отыскании множества $X(k_0)$ всех решений $(x_1, \ldots, x_n) \in k_0^n$ системы полиномиальных уравнений

$$f_i(x_1, \ldots, x_n) = 0, \quad 1 \leqslant i \leqslant m, \tag{1}$$

с коэффициентами из некоторого поля k_0 и в определении алгебраической структуры множества $X(k_0)$.

В классической постановке, восходящей к Диофанту Александрийскому [45], коэффициенты многочленов f_i являются целыми числами, и задача заключается в отыскании всех рациональных решений системы (1) (см. также [140, с. 171; 9]).

В арифметических вопросах, связанных с диофантовыми уравнениями, возникает необходимость в нахождении множества $X(\mathbb{Z})$ всех целочисленных решений системы (1), или, в более общей постановке, множества $X(\mathbb{Z}_{k_0})$ всех наборов $(x_1, \ldots, x_n)$ с компонентами из кольца целых чисел $\mathbb{Z}_{k_0}$ поля k_0, удовлетворяющих этой системе. Пример уравнения

$$y^2 = x^3 - 2,$$

имеющего бесконечное число рациональных решений и лишь два целочисленных решения $(x, y) = (3, \pm 5)$, показывает (см. задачи 1, 2 из § 2 гл. III), что вопрос о целочисленных решениях часто существенно отличается от вопроса о рациональных решениях и требует для своего исследования особых приемов и методов.

На всех этапах своего многовекового развития теория диофантовых уравнений оказывала определяющее влияние на формирование науки нового времени. Становление теории относится к I — III векам н. э. и характеризуется решительным отказом от прежних геометрических традиций греческих математиков и поворотом к арифметико-алгебраическому направлению. Перед средневековой Европой достижения античной математики в указанном направлении неожиданно предстали шестью книгами «Арифметики» Диофанта [45], случайно обнаруженными в 1571 г. в библиотеке Ватикана.

Следующий этап в развитии теории диофантовых уравнений тесно связан с именем Ф. Виета — родоначальника буквенного исчисления, и с именами создателей теории чисел — П. Ферма, Л. Эйлера, Ж. Л. Лагранжа и А. Лежандра, разработавших локальные методы изучения диофантовых уравнений на основе теории сравнений (см. [23 h]). Достижения этих выдающихся уче-

ных были подытожены К. Ф. Гауссом в его знаменитой книге «Disquisitiones arithmeticae [30 a], опубликованной в 1801 г. (см. также [30 c]).

Начало XIX века ознаменовалось открытием тесных взаимосвязей между теорией диофантовых уравнений и другими областями математики — алгеброй, геометрией и анализом. Подтверждением тому служат исследования Ж. Л. Лежандра, К. Ф. Гаусса, Л. Дирихле, Ш. Эрмита по теории квадратичных форм, завершившиеся созданием арифметики квадратичных полей и заложившие основы группового подхода в математике; работы Э. Куммера по изучению уравнения Ферма $x^n + y^n = z^n$, приведшие его к созданию арифметики круговых полей и увенчавшиеся разработкой теории дивизоров для полей алгебраических чисел (Р. Дедекинд, Е. И. Золотарев, Л. Кронекер); наконец, результаты К. Якоби по применению теорем Л. Эйлера и Н. Абеля о сложении эллиптических и абелевых интегралов к сложению рациональных точек на алгебраических кривых, заложившие основы арифметики абелевых многообразий. При этом была обнаружена глубокая аналогия между полями алгебраических чисел и полями алгебраических функций, приведшая, с одной стороны, к созданию арифметической теории функциональных полей и, с другой стороны, к введению в арифметику p-адических чисел (К. Гензель), играющих в числовых полях роль рядов Пюизе для алгебраических функций. Тем самым были заложены основы коммутативной алгебры и современной алгебраической геометрии.

Конец XIX — начало XX веков характеризуется интенсивным проникновением в теорию диофантовых уравнений аналитических методов. Наиболее мощными из них являются метод А. Туэ (см. гл. VI), основанный на применении результатов теории диофантовых приближений (приближений вещественных чисел рациональными), и круговой метод Харди — Литтлвуда (см. [131, 28]), восходящий своими корнями к методу производящих функций Л. Эйлера.

Метод А. Туэ получил свое дальнейшее развитие в работах К. Л. Зигеля, установившего на его основе знаменитую теорему о конечности числа целых точек на кривых рода $g \geqslant 1$ (см. гл. VII). Затем результат Зигеля был перенесен К. Малером на случай квазицелых точек с координатами из произвольного конечного расширения поля рациональных чисел $\mathbb{Q}$. Недавно метод А. Туэ был распространен В. Шмидтом [146e] на случай нескольких переменных, что позволило ему получить многомерное обобщение результата Туэ о конечности числа целочисленных решений норменного диофантова уравнения (*уравнения Туэ*)

$$\operatorname{norm}(\alpha x + \beta y) = a$$

степени $m \geqslant 3$.

Круговой метод Харди — Литтлвуда, основу которого составляет процесс поднятия локальных решений системы полиномиальных уравнений с целыми коэффициентами до ее целочисленных решений, плодотворен лишь в случае, когда число переменных много больше максимальной степени входящих в систему уравнений. Этот метод был значительно усовершенствован И. М. Виноградовым (см. [27 c, 28]), и существенно усиленный его оценками тригонометрических сумм Г. Вейля, привел к практически окончательному решению знаменитой проблемы Варинга о представимости всякого достаточно большого целого N ограниченной суммой n-х степеней целых чисел. Наиболее общий результат, полученный круговым методом, принадлежит Бёрчу [14] и состоит в том, что каждая невырожденная в определенном смысле система однородных уравнений с целыми коэффициентами, имеющих одинаковую степень и зависящих от достаточно большого числа переменных, обладает по меньшей мере одним отличным от нуля целочисленным решением (см. также В. Шмидт [146 j]).

Круговой метод Харди — Литтлвуда в определенном смысле сводит вопрос о разрешимости системы диофантовых уравнений в целых числах к вопросу о разрешимости соответствующей системы сравнений по всем простым модулям. Отчасти поэтому в двадцатых годах нашего столетия возродился интерес к алгебраическим сравнениям и их обобщениям — уравнениям над конечными полями. Изучение таких уравнений методами алгебраической геометрии привело к необходимости их дальнейшей арифметизации и завершилось созданием в «Основаниях» А. Вейля [23 c] алгебро-геометрических принципов исследования решений систем диофантовых уравнений над произвольными полями. Полученные им на этом пути результаты о числе рациональных точек алгебраических кривых, определенных над конечными полями, привели к интересным арифметическим следствиям, касающимся оценок рациональных тригонометрических сумм и сумм характеров (см. комментарии к гл. I и II). Лишь недавно результаты А. Вейля удалось доказать элементарно, опираясь исключительно на классические понятия и методы теории чисел (см. гл. I и V).

Тридцатые годы ознаменовались крупными успехами математической логики в направлении формализации математики. Разработка точного понятия алгоритма привела к обнаружению алгоритмически неразрешимых проблем и открыла возможность для решения знаменитой 10-й проблемы Гильберта о существовании финитного способа, позволяющего определить, разрешимо или не разрешимо в целых числах произвольно заданное диофантово уравнение с целыми коэффициентами. Полученный в 1970 г. Ю. В. Матиясевичем [82 a] результат о совпадении диофантовых и перечислимых множеств привел к отрицательному решению

этой проблемы и дал ясное представление о тех трудностях, с которыми связано изучение общих диофантовых уравнений (см. [41, 81 d]).

Разработка понятия алгоритма внесла в теорию диофантовых уравнений еще один новый момент — вопрос об эффективном перечислении множества всех решений изучаемого уравнения. Многие из методов теории диофантовых уравнений (в том числе и метод А. Туэ) обладают тем недостатком, что позволяют установить лишь конечность числа целочисленных решений определенного класса уравнений (и даже дать границу для этого числа), но не позволяют указать границу для самих решений. Начиная с шестидесятых годов в теории диофантовых уравнений интенсивно разрабатывается эффективный метод, основанный на использовании нижних оценок для модуля линейных форм от логарифмов алгебраических чисел (см. гл. VI). К настоящему времени этим методом получены эффективные границы для целочисленных решений целого ряда классических диофантовых уравнений, в том числе для уравнения Туэ, уравнения Туэ — Малера, гиперэллиптического уравнения и уравнения Каталана.

В самые последние годы пальма первенства при решении трудных задач теории диофантовых уравнений снова перешла к алгебраической геометрии. Построение этальной топологии и разработка теории этальных когомологий привели П. Делиня к доказательству справедливости «гипотезы Римана» для дзета-функции А. Вейля алгебраических многообразий над конечными полями (см. § 1 гл. V). Дальнейшее развитие теории абелевых многообразий и многообразий модулей кривых увенчалось замечательным результатом Г. Фалтингса, доказавшего знаменитую гипотезу Морделла о конечности числа рациональных точек на кривых рода $g > 1$. Оба результата являются, несомненно, наиболее выдающимися достижениями математики XX в. Однако математический аппарат, используемый для доказательства этих результатов, настолько объемен и сложен, что всякое более или менее доступное их изложение возможно в наши дни лишь на уровне разъяснения исходных идей и освещения основных этапов рассуждений (см. обзор Катца [60 b] и дополнение Ю. Г. Зархина, А. Н. Паршина к книге С. Ленга «Основы диофантовой геометрии» [70 h].

Первые две главы книги посвящены систематическому изложению теории уравнений над конечными полями, а также приложениям результатов этой теории к оценкам сумм характеров и к вопросу о распределении квадратичных вычетов и невычетов.

Основными результатами третьей, четвертой и пятой глав являются соответственно теорема Морделла о конечности ранга эллиптической кривой над полем рациональных чисел, теорема Римана — Роха для кривых и базирующееся на ее использовании доказательство теоремы А. Вейля о числе рациональных точек абсолютно неприводимой кривой над конечным полем. Теория

алгебраических кривых изложена с арифметической точки зрения, развитой в монографиях Шевалле [145b], Дойринга [46b] и в лекциях Г. И. Перельмутера.

В шестой и седьмой главах книги излагается «нестандартное» доказательство теоремы Зигеля — Малера о конечности числа квазицелых точек кривой рода $g \geqslant 1$ над полем алгебраических чисел.

Для понимания основного текста книги требуется знакомство с теорией Галуа в объеме «Алгебры» С. Ленга [70 d] и с теорией делимости в полях алгебраических чисел в объеме «Теории чисел» З. И. Боревича, И. Р. Шафаревича [19]. Необходимые сведения из алгебраической геометрии, математической логики и теории диофантовых приближений приведены по мере изложения основного материала. Задачи рассчитаны на активно работающего читателя.

В книге использованы следующие обозначения: $\mathbb{Z}$ — кольцо целых чисел, $\mathbb{N}$ — множество неотрицательных целых чисел; $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ — поля рациональных, действительных и комплексных чисел; $\mathbb{Q}_p$ — поле p-адических чисел; $\mathbb{Z}_p$ — кольцо целых p-адических чисел; F_q — конечное поле характеристики $p > 0$; $\log a$ — логарифм числа $a > 0$ по основанию e ($e = 2{,}718281\ldots$ — неперово число). Знак $\subset$ употребляется для обозначения как строгого, так и нестрогого теоретико-множественного включения (в случаях, приводящих к недоразумениям, точный смысл знака $\subset$ оговаривается особо). Остальные обозначения вводятся по ходу изложения материала.

ГЛАВА I

УРАВНЕНИЯ НАД КОНЕЧНЫМИ ПОЛЯМИ

§ 1. Сравнения

Возникновение теории сравнений тесно связано с изучением диофантовых уравнений. Эта связь основана на том простом факте, что если неопределенное уравнение

$$f(x_1, \ldots, x_n) = 0, \tag{1}$$

где f — многочлен с целыми коэффициентами, имеет целочисленное решение $(x_1, \ldots, x_n)$, то соответствующее ему сравнение

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m} \tag{2}$$

разрешимо для любого модуля m.

Пример 1. Покажем, что целое число вида $4k+3$ нельзя представить суммой двух квадратов целых чисел. Действительно, если бы это было возможно, то было бы разрешимо сравнение

$$x^2 + y^2 \equiv 3 \pmod{4}.$$

Простая проверка показывает, что последнее сравнение не имеет решений, и мы приходим к противоречию.

Во многих случаях оказывается, что локальная разрешимость, т. е. разрешимость сравнения (2) по некоторым модулям m, является также и достаточным условием для разрешимости диофантова уравнения (1).

Пример 2. Справедлива следующая теорема, доказанная Лежандром: *если a, b и c — попарно взаимно простые положительные целые числа, свободные от квадратов, то неопределенное уравнение*

$$ax^2 + by^2 - cz^2 = 0$$

нетривиальным образом разрешимо в целых числах x, y, z тогда и только тогда, когда разрешимы сравнения

$$x^2 - bc \equiv 0 \pmod{a},$$
$$x^2 - ac \equiv 0 \pmod{b},$$
$$x^2 + ab \equiv 0 \pmod{c}.$$

Разрешимость указанных в теореме сравнений можно установить для каждого конкретного набора чисел a, b и c хотя бы простым перебором. Следовательно, теорема Лежандра дает простой

и эффективный критерий разрешимости диофантова уравнения $ax^2 + by^2 - cz^2 = 0$ (доказательство теоремы Лежандра приведено в § 1 гл. III).

1. Основные понятия. Поставим в соответствие каждому целому числу a его остаток $r = a - mq$, $0 \leqslant r \leqslant m-1$, от деления на целое положительное число m. Если двум целым числам a и b соответствует один и тот же остаток r, то они называются *сравнимыми по модулю m*. Для обозначения сравнимости чисел a и b употребляется запись $a \equiv b \pmod{m}$. Ясно, что $a \equiv b \pmod{m}$ тогда и только тогда, когда разность $a - b$ делится на m. Если разность $a - b$ не делится на m, то числа a и b называются *несравнимыми по модулю m*; в этом случае употребляется запись $a \not\equiv b \pmod{m}$.

Подобно обычным равенствам сравнения можно складывать, вычитать и перемножать. Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$ и $ac \equiv bd \pmod{m}$. Действительно, если $a - b = mq$, $c - d = mt$, то $(a-b) \pm (c-d) = (q \pm t)m$. Далее, $(a-b)c = mqc$, так что $ac = bc + mqc$, и $(c-d)b = mtb$, так что $bc = bd + mtb$. Отсюда $ac = bd + (qc + tb)m$ и, значит, $ac \equiv bd \pmod{m}$. В общем случае сравнения делить нельзя. Действительно, мы имеем $36 \equiv 16 \pmod{10}$, $12 \equiv 2 \pmod{10}$, но $3 \not\equiv 8 \pmod{10}$. Однако обе части сравнения можно сократить на множитель, взаимно простой с модулем.

Отношение сравнимости по модулю m является отношением эквивалентности; оно рефлексивно, так как $a \equiv a \pmod{m}$, симметрично, поскольку из $a \equiv b \pmod{m}$ следует $b \equiv a \pmod{m}$, и транзитивно, так как из $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$ следует $a \equiv c \pmod{m}$. Тем самым отношение «$\equiv \pmod{m}$» разбивает множество всех целых чисел $\mathbb{Z}$ на непересекающиеся классы A, B, C, ..., состоящие из всех сравнимых между собой по модулю m целых чисел. Эти классы называются *классами вычетов по модулю m*. Очевидно, что целые числа $0, 1, \ldots, m-1$ лежат в разных классах вычетов, и так как каждое целое число сравнимо по модулю m с одним из этих чисел, то имеется ровно m классов вычетов по модулю m.

Операции сложения, вычитания и умножения сравнений индуцируют аналогичные операции на множестве классов вычетов. Пусть A и B — два класса вычетов по модулю m. Каковы бы ни были числа $a \in A$ и $b \in B$, их сумма $a + b$ всегда лежит в одном и том же однозначно определенном классе $C = A + B$, который назовем суммой классов A и B. Аналогичным образом определяется разность $A - B$ и произведение AB двух классов вычетов по модулю m. Эти классы образуют относительно сложения абелеву группу порядка m. Нулевым элементом этой группы является класс вычетов, состоящий из всех целых кратных числа m, а обратным к классу A является класс $-A$, состоящий из всех элементов класса A, взятых со знаком минус. Более того, классы

вычетов по модулю $m > 1$ образуют коммутативное кольцо. Единичным элементом служит класс E, содержащий целое число 1. Дистрибутивный закон $A(B+C) = AB + AC$ непосредственно следует из дистрибутивного закона для целых чисел.

Любое число из класса вычетов A по модулю m называется *вычетом по модулю* m. Вычет r, $0 \leqslant r \leqslant m-1$, равный остатку от его деления на модуль m, называется *наименьшим неотрицательным вычетом*. Взяв из каждого класса вычетов по одному представителю, получим *полную систему вычетов по модулю* m. Таким образом, множество из m целых чисел образует полную систему вычетов по модулю m тогда и только тогда, когда его элементы несравнимы друг с другом по модулю m. Чаще всего в качестве полной системы вычетов употребляются наименьшие неотрицательные вычеты $0, 1, \ldots, m-1$.

Классы вычетов по модулю m, элементы которых взаимно просты с m, назовем *приведенными классами вычетов*. Взяв из каждого такого класса по одному вычету, получим *приведенную систему вычетов по модулю* m. Приведенную систему вычетов можно составить из чисел полной системы вычетов $0, 1, \ldots, m-1$, взаимно простых с модулем m. Следовательно, приведенная система вычетов по модулю m состоит из $\varphi(m)$ элементов, где $\varphi(m)$ — *функция Эйлера*, равная количеству неотрицательных целых чисел, меньших m и взаимно простых с m.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами. *Решением сравнения* $f(x) \equiv 0 \pmod m$ назовем всякий класс вычетов $x \equiv x_0 \pmod m$, для которого целое число x_0 удовлетворяет условию $f(x_0) \equiv 0 \pmod m$.

Обозначим (a, b) наибольший общий делитель целых чисел a и b. Если $(a, m) = 1$ и x пробегает приведенную систему вычетов по модулю m, то ax также пробегает приведенную систему вычетов по модулю m. Действительно, чисел ax столько же, сколько и чисел x, т. е. $\varphi(m)$. Далее, числа ax несравнимы между собой по модулю m и взаимно просты с m. Следовательно, сравнение $ax \equiv 1 \pmod m$ имеет единственное решение $x \equiv x_0 \pmod m$ такое, что $(x_0, m) = 1$. Другими словами, если A, X — приведенные классы вычетов и E — класс вычетов, содержащий число 1, то уравнение $AX = E$ разрешимо. Таким образом, каждый приведенный класс обратим и тем самым приведенные классы вычетов по модулю m образуют по умножению абелеву группу порядка $\varphi(m)$, единичным элементом которой является класс E. Далее, если $(a, m) = 1$ и x пробегает приведенную систему вычетов, состоящую из наименьших неотрицательных вычетов $r_1, r_2, \ldots, r_{\varphi(m)}$, то наименьшие неотрицательные вычеты ax состоят из тех же чисел $r_1, r_2, \ldots, r_{\varphi(m)}$. Следовательно,

$$\prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{j=1}^{\varphi(m)} ar_j \pmod m$$

и тогда

$$(a^{\varphi(m)} - 1) \prod_{j=1}^{\varphi(m)} r_j \equiv 0 \pmod m.$$

Но числа $r_1, r_2, \ldots, r_{\varphi(m)}$ взаимно просты с модулем m, и в таком случае $a^{\varphi(m)} \equiv 1 \pmod m$. Тем самым установлен следующий результат.

Теорема (Эйлер). *Если целое число a взаимно просто с m, то $a^{\varphi(m)} \equiv 1 \pmod m$.*

Теорема Эйлера означает, что каждый приведенный класс вычетов по модулю m удовлетворяет уравнению $x^{\varphi(m)} - 1 = 0$.

2. Сравнения по простому модулю. Рассмотрим кольцо классов вычетов по простому модулю p. В этом случае все классы вычетов, за исключением нулевого, будут приведенными и, следовательно, образуют по умножению абелеву группу. Таким образом, классы вычетов по простому модулю p образуют конечное поле из p элементов, называемое *простым конечным полем*. В дальнейшем будем обозначать это поле F_p, а его единичный элемент символом 1. В случае простого модуля p имеет место следующее утверждение, являющееся частным случаем теоремы Эйлера.

Малая теорема Ферма. *Если a не делится на простое число p, то $a^{p-1} \equiv 1 \pmod p$.*

Из этой теоремы следует, что $a^p \equiv a \pmod p$ для любого целого числа a. Другими словами, каждый элемент поля F_p удовлетворяет уравнению $x^p - x = 0$.

Для выяснения структуры поля F_p нам потребуется понятие первообразного корня. *Первообразным корнем по модулю m* называется такое целое число η, для которого $\eta^{\varphi(m)} \equiv 1 \pmod m$ и $\eta^\delta \not\equiv 1 \pmod m$ при $1 \leqslant \delta \leqslant \varphi(m) - 1$. Существование первообразных корней для всех простых модулей p устанавливает следующая теорема.

Теорема (Гаусс). *Имеется $\varphi(p-1)$ первообразных корней по простому модулю p.*

Доказательство теоремы будет приведено в следующем параграфе для более общего случая произвольных конечных полей. Из теоремы Гаусса следует, что мультипликативная группа F_p^* поля F_p является циклической группой порядка $p - 1$.

3. Алгебраические сравнения. В заключение параграфа остановимся на вопросе о числе решений алгебраического сравнения $f(x) \equiv 0 \pmod p$ по простому модулю p, где

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

— многочлен с целыми коэффициентами и $a_0 \not\equiv 0 \pmod p$. Два целочисленных многочлена $f(x)$ и $g(x)$ назовем *равными по модулю p*, если все коэффициенты их разности $f(x) - g(x)$ делятся на p. Для обозначения равенства многочленов $f(x)$ и $g(x)$ по модулю p будем использовать запись $f(x) = g(x) \pmod p$. Мы ска-

жем, что класс вычетов $x \equiv x_0 \pmod p$ является s-кратным решением сравнения $f(x) \equiv 0 \pmod p$, если имеет место разложение $f(x) = (x - x_0)^s g(x) \pmod p$, где $s \geqslant 1$ и $g(x)$ — многочлен с целыми коэффициентами, удовлетворяющий условию $g(x_0) \not\equiv 0 \pmod p$. Имеет место следующий результат.

Теорема (Лагранж). *Количество решений сравнения* $f(x) \equiv 0 \pmod p$ *по простому модулю* p, *взятых с их кратностями, не превосходит степени* $n = \deg f$ *многочлена* $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$, $a_0 \not\equiv 0 \pmod p$.

Доказательство. Теорема легко доказывается индукцией по степени n многочлена $f(x)$. Для $n = 1$ утверждение теоремы очевидно, поскольку при $(a_0, p) = 1$ сравнение $a_0x + a_1 \equiv 0 \pmod p$ имеет единственное решение. Если сравнение $f(x) \equiv 0 \pmod p$ степени $n > 1$ имеет s-кратное решение $x \equiv x_0 \pmod p$, то $f(x) = (x - x_0)^s g(x) \pmod p$, где $g(x)$ — многочлен степени $n - s$. Следовательно, каждое решение сравнения $f(x) \equiv 0 \pmod p$ удовлетворяет либо сравнению $x - x_0 \equiv 0 \pmod p$, которое приводит к исходному решению $x \equiv x_0 \pmod p$, либо сравнению $g(x) \equiv 0 \pmod p$, которое по индуктивному предположению имеет не более $n - s$ решений. Тем самым сравнение $f(x) \equiv 0 \pmod p$ имеет самое бо́льшее n решений.

Заметим, что сравнение $f(x) \equiv 0 \pmod m$ можно трактовать как уравнение $f(x) = 0$ над простым конечным полем F_p. При такой интерпретации теорема Лагранжа выражает широко известный факт, что число корней ненулевого многочлена с коэффициентами из произвольного поля не превосходит степени n многочлена $f(x)$.

Рассмотрим простейший тип алгебраических сравнений — *двучленные сравнения* $x^n \equiv a \pmod p$, где $a \not\equiv 0 \pmod p$. Пусть η — первообразный корень по модулю p и пусть $x \equiv \eta^y \pmod p$, $a \equiv \eta^l \pmod p$. Тогда сравнение $x^n \equiv a \pmod p$ эквивалентно линейному сравнению $ny \equiv l \pmod{p-1}$.

Лемма. *Линейное сравнение* $ny \equiv l \pmod m$ *не имеет решений, если* l *не делится на* $d = (m, n)$, *и имеет* d *решений, если* l *делится на* d.

Доказательство. При $d = 1$ сравнение $ny \equiv l \pmod m$ имеет единственное решение. Пусть $d > 1$. Из равенства $ny - l = mq$ следует, что сравнение $ny \equiv l \pmod m$ разрешимо лишь тогда, когда l делится на d. При выполнении этого условия имеем $\frac{n}{d}y - \frac{l}{d} = \frac{m}{d}q$, где $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. Сравнение $\frac{n}{d}y \equiv \frac{l}{d}\left(\mathrm{mod}\,\frac{m}{d}\right)$ имеет единственное решение $y \equiv y_0 \left(\mathrm{mod}\,\frac{m}{d}\right)$, которое дает d решений $y \equiv y_0 \pmod m$, $y \equiv y_0 + \frac{m}{d} \pmod m$, $\ldots$, $y \equiv y_0 + \frac{(d-1)m}{d} \pmod m$ сравнения $ny \equiv l \pmod m$.

Возьмем $m = p - 1$. Из определения первообразного корня следует, что $d = (n, p-1)$ делит l лишь в случае, если $a^{\frac{p-1}{d}} \equiv \eta^{l\frac{p-1}{d}} \equiv 1 \pmod p$; получаем следующий результат.

Критерий Эйлера. *Пусть* p — *простое число и* $d = (n, p-1)$. *Сравнение* $x^n \equiv a \pmod p$, $a \not\equiv 0 \pmod p$, *разрешимо тогда и только тогда, когда* $a^{\frac{p-1}{d}} \equiv 1 \pmod p$. *В случае разрешимости оно имеет* d *различных решений.*

Если сравнение $x^n \equiv a \pmod p$ разрешимо, то число a называется *вычетом степени* n *по модулю* p. В противном случа оно называется *невычетом степени* n *по модулю* p. В частности, при $n = 2$ вычеты и невычеты называются *квадратичными*, при $n = 3$ — *кубическими* и при $n = 4$ — *биквадратичными*.

Заметим, что если $a \not\equiv 0 \pmod p$ — квадратичный вычет по простому модулю $p > 2$, то сравнение $x^2 \equiv a \pmod p$ имеет два решения $x \equiv x_0 \pmod p$ и $x \equiv -x_0 \pmod p$; если же a делится на p, то сравнение $x^2 \equiv a \pmod p$ имеет единственное решение $x \equiv 0 \pmod p$. Для простых $p > 2$ введем в рассмотрение *символ Лежандра* $\left(\frac{a}{p}\right)$, который определяется для всех целых a следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ является квадратичным вычетом по модулю } p \text{ и } a \not\equiv 0 \pmod p; \\ -1, & \text{если } a \text{ является квадратичным невычетом по модулю } p; \\ 0, & \text{если } a \equiv 0 \pmod p. \end{cases}$$

Тогда для количества N_p решений сравнения $x^2 \equiv a \pmod p$ имеем формулу

$$N_p = 1 + \left(\frac{a}{p}\right).$$

Если p — нечетное простое число, то для каждого $a \not\equiv 0 \pmod p$ имеем $a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p$. При этом $a^{\frac{p-1}{2}} - 1$ и $a^{\frac{p-1}{2}} + 1$ не делятся одновременно на p (иначе их разность 2 делилась бы на p). Это замечание позволяет, в случае $n = 2$, следующим образом переформулировать критерий Эйлера:

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

Отсюда легко выводим, что $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ для любых двух це-

лых чисел a, b и что $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ при $a \equiv b \pmod p$. Кроме того, мы видим, что среди чисел $1, 2, \ldots, p-1$ имеется ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов по простому модулю p.

Задачи

1. Используя малую теорему Ферма и теорему Лагранжа, вывести теорему Вильсона: *если p — простое число, то выполняется сравнение* $(p-1)! + 1 \equiv 0 \pmod p$.

Доказать обратное утверждение: *если* $(p-1)! + 1 \equiv 0 \pmod p$, *то p — простое число.*

2. Пусть m и m' — взаимно простые положительные целые числа. Доказать, что если x и x' пробегают полные (приведенные) системы вычетов по модулям m и m' соответственно, то $xm' + x'm$ пробегает полную (приведенную) систему вычетов по модулю mm'.

3. Вывести из результата предыдущей задачи, что функция Эйлера $\varphi(m)$ мультипликативна (арифметическая функция $f(m) \not\equiv 0$ называется *мультипликативной*, если из условия $(m, n) = 1$ следует, что $f(mn) = f(m)f(n)$.

4. Используя мультипликативность функции $\varphi(m)$, показать, что

$$\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right),$$

где произведение берется по всем простым числам p, делящим m. Вывести отсюда соотношение

$$\sum_{d \mid m} \varphi(d) = m.$$

5. Пусть m — положительное целое число, $f(x_1, \ldots, x_n)$ — многочлен с целыми коэффициентами и $i = \sqrt{-1}$. Под *решением сравнения*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod m \qquad (*)$$

будем понимать всякий набор $x_1 \equiv x_1' \pmod m, \ \ldots, \ x_n \equiv x_n' \pmod m$ классов вычетов по mod m, для которого целые числа $x_1', \ldots, x_n'$ удовлетворяют условию $f(x_1', \ldots, x_n') \equiv 0 \pmod m$. Используя соотношение

$$\sum_{x=1}^{m} e^{2\pi i \frac{ax}{m}} = \begin{cases} m, & \text{если } m \text{ делит } a, \\ 0 & \text{в противном случае,} \end{cases}$$

доказать, что число $N(m)$ решений сравнения $(*)$ выражается формулой

$$N(m) = \frac{1}{m} \sum_{a=1}^{m} \sum_{x_1, \ldots, x_n = 1}^{m} e^{2\pi i \frac{a f(x_1, \ldots, x_n)}{m}}.$$

6. Пусть $a_1, \ldots, a_n, b$ — целые числа и $d = (a_1, \ldots, a_n, m)$. Доказать, что для числа $N(m)$ решений линейного сравнения

$$a_1 x_1 + \ldots + a_n x_n \equiv b \pmod m$$

справедливы равенства

$$N(m) = \begin{cases} m^{n-1} d, & \text{если } d \text{ делит } b, \\ 0 & \text{в противном случае.} \end{cases}$$

7. В обозначениях задачи 5 показать, что функция $N(m)$ является мультипликативной, т. е. $N(m_1 m_2) = N(m_1) N(m_2)$ при $(m_1, m_2) = 1$.

8. Пусть p — простое число, $\alpha > 1$ — целое число и $f(x_1, \ldots, x_n)$ — многочлен с целыми коэффициентами. Доказать, что каждое решение $x_1 \equiv x_1' \pmod p, \ \ldots, \ x_n \equiv x_n' \pmod p$ сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod p$, удовлетворяющее хотя бы для одного $j = 1, 2, \ldots, n$ условию

$$\frac{\partial}{\partial x_j} f(x_1', \ldots, x_n') \not\equiv 0 \pmod p,$$

порождает $p^{(\alpha-1)(n-1)}$ различных между собой решений $x_1 \equiv x_1^{(\alpha)} \pmod{p^\alpha}, \ \ldots, \ x_n \equiv x_n^{(\alpha)} \pmod{p^\alpha}$ сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^\alpha}.$$

9. Пусть $p > 2$ — простое число и a, b, c, d — целые числа. Установить, что при $d \not\equiv 0 \pmod p$ число решений сравнения

$$y^2 \equiv x^2 + d \pmod p$$

равно $p - 1$, и вывести отсюда справедливость соотношений

$$\sum_{x=1}^{p} \left(\frac{ax^2 + bx + c}{p}\right) = \begin{cases} \left(\frac{a}{p}\right)(p-1), & \text{если } b^2 - 4ac \equiv 0 \pmod p, \\ -\left(\frac{a}{p}\right), & \text{если } b^2 - 4ac \not\equiv 0 \pmod p. \end{cases}$$

10*. Пусть $p > 3$ — простое число и $a \not\equiv 0 \pmod p$. Доказать, что сравнение

$$x^3 + ax \equiv y \pmod p$$

разрешимо при $p - \frac{1}{3}\left(p - \left(\frac{-3}{p}\right)\right)$ значениях $y = 0, 1, \ldots, p-1$.

11. Доказать, что уравнение

$$x^2 - 7y^2 = 3.$$

не разрешимо в целых числах.

12. Доказать, что уравнение

$$x^3 + y^3 + z^3 = 4$$

не имеет решений в целых x, y, z.

13. Доказать, что целое число n вида $4k + 7$ не может быть представлено в виде суммы квадратов трех целых чисел.

14*. Доказать, что уравнение

$$x^2 + 82y^2 = 2$$

не имеет челочисленных решений и что соответствующее сравнение

$$x^2 + 82y^2 \equiv 2 \pmod m$$

разрешимо при любом модуле m.

15. Доказать, что для простых чисел p вида $4m+3$ сумма

$$S(k)=\sum_{x=1}^{p}\left(\frac{x^3+kx}{p}\right), \quad k\not\equiv 0 \pmod p,$$

равна нулю. Для простых p вида $4m+1$ установить следующие свойства *сумм Якобсталя* $S(k)$:

а) $S(k)$ — четное число;

б) $S(kt^2)=\left(\frac{t}{p}\right)S(k)$;

в) если $\left(\frac{k}{p}\right)=1$ и $\left(\frac{l}{p}\right)=1$, то

$$\left(\frac{1}{2}S(k)\right)^2+\left(\frac{1}{2}S(l)\right)^2=p;$$

г) $|S(k)|<2\sqrt{p}$.

16. Доказать, что для нечетных простых p вида $p=3m+2$ сумма

$$T(l)=\sum_{x=1}^{p}\left(\frac{x^3+l}{p}\right), \quad l\not\equiv 0 \pmod p,$$

равна нулю. Для простых p вида $p=3m+1$ доказать справедливость следующих утверждений:

а) $T(ls^3)=\left(\frac{s}{p}\right)T(l)$;

б) если η — первообразный корень по модулю p, то

$$T(1)+T(\eta^2)+T(\eta^4)=0$$

и

$$T^2(1)+T^2(\eta^2)+T^2(\eta^4)=6p;$$

в) имеет место равенство

$$T^2(1)+T(1)T(\eta^2)+T^2(\eta^2)=3p;$$

г) $|T(l)|<2\sqrt{p}$;

д) уравнение

$$x^2+27y^2=4p$$

разрешимо в целых числах x и y.

17*. Пусть p — простое число и $f(x_1, \ldots, x_n)$ — многочлен с коэффициентами из поля F_p степени $m\geqslant 1$ по совокупности переменных $x_1, \ldots, x_n$. Доказать теорему Варнинга [22]: *если $m<n$, то число N_p решений уравнения $f(x_1, \ldots, x_n)=0$ в элементах поля F_p делится на p.*

(Указание. Представить N_p в виде

$$N_p=\sum_{x_1,\ldots,x_n\in F_p}\left(1-f^{p-1}(x_1, \ldots, x_n)\right)$$

и воспользоваться циклическим строением мультипликативной группы F_p^* поля F_p.)

18. Основываясь на результате задачи 17, установить справедливость следующей теоремы Шевалле [145а]: *если $f(x_1, \ldots, x_n)$ — форма положительной степени m с коэффициентами из F_p и $m<n$, то уравнение $f(x_1, \ldots, x_n)=0$ имеет над полем F_p хотя бы одно ненулевое решение.*

19*. Пусть p — простое число, $m\geqslant 1$ — целое число, F_p — конечное поле, состоящее из чисел $0, 1, \ldots, p-1$ и $d=(m, p-1)$. Доказать, что для суммы

$$T(a, p)=\sum_{x\in F_p}e^{2\pi i\frac{ax^m}{p}},$$

где $i=\sqrt{-1}$ и a — произвольный ненулевой элемент поля F_p, справедлива оценка

$$|T(a, p)|\leqslant (d-1)\sqrt{p}.$$

(Указание. Пусть η — порождающий элемент мультипликативной группы F_p^* поля F_p и $\chi_s(y)$ — характер группы F_p^*, определенный для каждого $s=0, 1, \ldots, d-1$ и каждого $y=\eta^\nu\in F_p^*$ равенством $\chi_s(y)=e^{2\pi i\frac{s\nu}{d}}$. Доказать, что

$$T(a, p)=1+\sum_{y\in F_p^*}\sum_{s=0}^{d-1}\chi_s(y)\,e^{2\pi i\frac{ay}{p}}$$

и что при $s\not\equiv 0$ для модуля *суммы Гаусса*

$$T_s(a)=\sum_{y\in F_p^*}\chi_s(y)\,e^{2\pi i\frac{ay}{p}}$$

справедливо равенство $|T_s(a)|=\sqrt{p}$.)

20. Пусть p — нечетное простое число, $m\geqslant 2$, a — целые числа и $d=(m, p-1)$. Установить следующие свойства сумм

$$T(a)=\sum_{x=1}^{p}e^{2\pi i\frac{x^m+ax}{p}}:$$

а) $\sum_{a=1}^{p}|T(a)|^2=p^2$;

б) при $(a, p)=1$ имеет место оценка $|T(a)|\leqslant\frac{p}{\sqrt{d}}$.

21. Пусть $m_1, \ldots, m_n$ — положительные целые числа, p — простое число, $d_j=(m_j, p-1)$, $1\leqslant j\leqslant n$, и $a_1, \ldots, a_n$ — отличные от нуля элементы поля F_p. Доказать, что для числа N_p решений $(x_1, \ldots, x_n)\in F_p^n$ уравнения

$$a_1x_1^{m_1}+\ldots+a_nx_n^{m_n}=0$$

справедлива оценка

$$\left|N_p-p^{n-1}\right|\leqslant(d_1-1)\ldots(d_n-1)\,p^{\frac{n}{2}-1}(p-1).$$

(Указание. Воспользоваться результатами задач 5 и 19.)

22. Пусть p — простое число, $m_0=\{m_1, \ldots, m_n\}$ — наименьшее общее кратное целых положительных чисел $m_1, \ldots, m_n$ и $d_j=(m_j, p-1)$,

$0 \leqslant j \leqslant n$. Доказать, что для числа N_p решений уравнения

$$a_1 x_1^{m_1} + \ldots + a_n x_n^{m_n} = a_0, \quad a_0, \quad a_1, \ldots, a_n \in F_p^*,$$

в элементах поля F_p справедливо неравенство

$$\left| N_p - p^{n-1} \right| \leqslant (d_0 - 1)(d_1 - 1) \ldots (d_n - 1) p^{\frac{n-1}{2}}.$$

23*. Пусть q — положительное целое число и a — целое число, взаимно простое с q. Установить следующие свойства *сумм Гаусса*

$$T(a, q) = \sum_{x=0}^{q-1} e^{2\pi i \frac{ax^2}{q}};$$

а) если $(q_1, q_2) = 1$, то

$$T(a, q_1 q_2) = T(aq_2, q_1) T(aq_1, q_2);$$

б) если $q = 2^\alpha p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ — каноническое разложение числа q, где $p_1, \ldots, p_s$ — нечетные простые числа, то

$$T(a, q) = T\left(\frac{aq}{2^\alpha}, 2^\alpha\right) \prod_{r=1}^{s} T\left(\frac{aq}{p_r^{\alpha_r}}, p^{\alpha_r}\right);$$

в) справедливы соотношения

$$|T(a, q)| = \begin{cases} \sqrt{q}, & \text{если } q \equiv 1 \pmod 2, \\ \sqrt{2q}, & \text{если } q \equiv 0 \pmod 4, \\ 0, & \text{если } q \equiv 2 \pmod 4; \end{cases}$$

г) если p — нечетное простое число и $\alpha > 1$, то

$$T(a, p^\alpha) = pT(a, p^{\alpha-2}).$$

(Указание. Положить $x = y + p^{\alpha-1} z$, $0 \leqslant y \leqslant p^{\alpha-1} - 1$, $0 \leqslant z \leqslant p - 1$.)

д) если p — нечетное простое число, то

$$T(a, p) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i \frac{ax}{p}} = \left(\frac{a}{p}\right) T(1, p);$$

е) если $\alpha > 3$, то

$$T(a, 2^\alpha) = 2T(a, 2^{\alpha-2}).$$

(Указание. Положить $x = y + 2^{\alpha-2} z$, $0 \leqslant y \leqslant 2^{\alpha-2} - 1$, $0 \leqslant z \leqslant 3$.)

ж) если $\alpha > 1$, то

$$T(a, 2^\alpha) = (-1)^{\frac{\alpha(a^2-1)}{8}} (1 + i^a) 2^{\alpha/2};$$

з) если p — нечетное простое число, то

$$T^2(1, p) = (-1)^{\frac{p-1}{2}} p.$$

24*. Пусть p — нечетное простое число и

$$T(1, p) = \sum_{x=0}^{p-1} e^{2\pi i \frac{x^2}{p}}$$

— *нормированная сумма Гаусса*. Установить следующие свойства матрицы

$$A = \left\| e^{2\pi i \frac{st}{p}} \right\|_{0 \leqslant s, t \leqslant p-1}:$$

а) если $\lambda_1, \ldots, \lambda_p$ — характеристические числа матрицы A, то

$$\sum_{k=1}^{p} \lambda_k = T(1, p);$$

б) квадрат матрицы A имеет вид

$$A^2 = \left\| \begin{matrix} p & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & \boldsymbol{B} & \\ 0 & & & \end{matrix} \right\|,$$

где

$$B = \left\| \begin{matrix} 0 & \ldots & 0 & p \\ 0 & \ldots & p & 0 \\ \cdot & \cdot & \cdot & \cdot \\ p & \ldots & 0 & 0 \end{matrix} \right\|$$

— диагональная матрица;

в) характеристический многочлен матрицы A^2 имеет вид

$$\det(A^2 - tE) = (t - p)^{\frac{p+1}{2}} (t + p)^{\frac{p-1}{2}};$$

г) среди характеристических чисел $\lambda_1^2, \ldots, \lambda_p^2$ матрицы A^2 имеется $\frac{p+1}{2}$ чисел, равных p, и $\frac{p-1}{2}$ чисел, равных $-p$;

д) если среди характеристических чисел $\lambda_1, \ldots, \lambda_p$ матрицы A имеется k, l, m и n чисел, равных $\sqrt{p}$, $-\sqrt{p}$, $i\sqrt{p}$ и $-i\sqrt{p}$ соответственно, то

$$k + l = \frac{p+1}{2}, \quad m + n = \frac{p-1}{2};$$

е) справедливы соотношения

$$T(1, p) = (k - l + (m - n)i)\sqrt{p}$$

и

$$\begin{aligned} k - l &= \pm 1, & m &= n & &\text{при} & p &\equiv 1 \pmod 4, \\ k &= l, & m - n &= \pm 1 & &\text{при} & p &\equiv 3 \pmod 4 \end{aligned}$$

(см. свойство з) из задачи 23);

ж) для определителя матрицы A справедливы равенства

$$\det A = i^{\frac{p(p-1)}{2}} p^{p/2} = i^{2l+m-n} p^{p/2};$$

з) справедливы соотношения

$$\begin{aligned} k - l &\equiv 1 \pmod 4 \quad &&\text{при} \quad p \equiv 1 \pmod 4, \\ m - n &\equiv 1 \pmod 4 \quad &&\text{при} \quad p \equiv 3 \pmod 4. \end{aligned}$$

25. Используя результаты предыдущей задачи, показать, что

$$T(1, p) = \begin{cases} \sqrt{p}, & \text{если } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

26*. Пусть $m > 1$ — нечетное число и $m = p_1 p_2 \dots p_s$ — его разложение на простые множители (не обязательно различные). Для целого a, взаимно простого с m, определим *символ Якоби* равенством

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_s}\right).$$

Исходя из известных свойств символа Лежандра $\left(\frac{a}{p}\right)$ установить аналогичные свойства символа Якоби и, используя эти свойства, а также результаты задач 23, 25, доказать, что

$$T(a, q) = \begin{cases} \left(\frac{a}{q}\right) i^{\left(\frac{q-1}{2}\right)^2} \sqrt{q}, & \text{если } q \equiv 1 \pmod 2, \\ \left(\frac{a}{q}\right)(1 + i^a)\sqrt{q}, & \text{если } q \equiv 0 \pmod 4, \\ 0, & \text{если } q \equiv 2 \pmod 4. \end{cases}$$

27. Пусть l и p — различные нечетные простые числа. Используя результаты задач 23, 25 и 26, доказать справедливость *квадратичного закона взаимности Гаусса*

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}\cdot\frac{p-1}{2}}$$

и двух его *дополнений*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

§ 2. Сравнения по двойному модулю и конечные поля

1. Кольцо $F_p[x]$. Пусть F_p — поле классов вычетов по простому модулю p. Рассмотрим кольцо $F_p[x]$ многочленов от переменного x с коэффициентами из поля F_p. Элементы поля F_p назовем константами кольца $F_p[x]$; единичный элемент поля F_p обозначим 1.

Будем говорить, что многочлен $f(x)$ делит в кольце $F_p[x]$ многочлен $g(x)$, если существует такой многочлен $h(x) \in F_p[x]$, что $g(x) = f(x)h(x)$. Если непостоянный многочлен $f(x)$ не имеет других делителей, кроме α и $\alpha f(x)$, где $\alpha \in F_p$, то $f(x)$ называется *неприводимым* в кольце $F_p[x]$ многочленом. Далее, *наибольшим общим делителем* двух многочленов $f(x)$ и $g(x)$ называется такой многочлен $d(x)$, который является их общим делителем и вместе с тем делится на любой другой общий делитель этих многочленов. Если многочлены f и g не имеют общих делителей, отличных от констант, то они называются *взаимно простыми*. Заметим, что наибольший общий делитель определен с точностью до постоянного множителя $\alpha \in F_p$, $\alpha \neq 0$. Для нахождения наибольшего общего делителя $d = (f, g)$ многочленов f и $g \neq 0$ можно воспользоваться *алгоритмом Евклида* последовательного деления с остатком:

$$\begin{aligned} &f = gh + r, \quad g = rh_1 + r_1, \quad r = r_1h_2 + r_2, \\ &r_1 = r_2h_3 + r_3, \ \dots, \ r_{n-2} = r_{n-1}h_n + r_n, \quad r_{n-1} = r_nh_{n+1}, \end{aligned} \tag{1}$$

где многочлены $r, r_1, \dots, r_n$ удовлетворяют условию

$$0 \leqslant \deg r_n < \dots < \deg r_1 < \deg r < \deg g.$$

Из равенств (1) следует, что всякий общий делитель многочленов f и g делит r_n и, в таком случае, $r_n = d$. Далее, исключая из системы (1) многочлены $r_{n-1}, \dots, r_1, r$, получаем представление наибольшего общего делителя $d = (f, g)$ в виде линейной комбинации

$$d = fu + gv$$

многочленов f и g с коэффициентами $u, v \in F_p[x]$. Отсюда следует, в частности, что если произведение gh многочленов g и h делится в кольце $F_p[x]$ на неприводимый многочлен f, то либо g, либо h делится на f. Действительно, если, например, f не делит g, то из представления $fu + gv = 1$ получаем $fhu + ghv = h$, и тогда f делит h. Это свойство неприводимых многочленов приводит к справедливости следующего утверждения (см. [1, гл. 1, § 2]).

Теорема 1. *Каждый непостоянный многочлен $g(x)$ кольца $F_p[x]$ допускает разложение $g = f_1^{m_1} \dots f_s^{m_s}$ в произведение неприводимых многочленов $f_1, \dots, f_s$; такое разложение единственно с точностью до констант кольца $F_p[x]$ и порядка следования сомножителей.*

С точки зрения делимости кольцо $F_p[x]$ вполне аналогично кольцу целых чисел $\mathbb{Z}$. При этом F_p^* соответствует мультипликативной подгруппе $\{\pm 1\}$ кольца $\mathbb{Z}$. Продолжим развитие этой аналогии. Назовем два многочлена $a(x)$ и $b(x)$ из кольца $F_p[x]$ *сравнимыми по модулю* $f(x) = x^n + \alpha_1 x^{n-1} + \dots + \alpha_{n-1}x + \alpha_n$, $n \geqslant 1$, $\alpha_i \in F_p$, если их разность $a - b$ делится в кольце $F_p[x]$ на многочлен $f(x)$. Сравнения такого рода будем называть, следуя Дедекинду, *сравнениями по двойному модулю* и для обозначения сравнимости $a(x)$ и $b(x)$ по модулю $f(x)$ будем писать $a(x) \equiv b(x) \pmod{f(x)}$. Отношение сравнимости по двойному модулю рефлексивно, симметрично, транзитивно и поэтому разбивает множество всех многочленов с коэффициентами из поля F_p на непересекающиеся классы $A, B, C, \dots$, называемые *классами вычетов по модулю* $f(x)$. Поскольку каждый многочлен $a(x)$ сравним по модулю $f(x)$ с одним и только одним многочленом $r(x)$ вида

$$r(x) = a_1x^{n-1} + a_2x^{n-2} + \dots + a_n,$$

где $a_1, \dots, a_n$ независимо друг от друга пробегают все элементы

поля F_p, то имеется в точности $q = p^n$ классов вычетов по модулю $f(x)$. Сравнения по двойному модулю можно складывать, вычитать и перемножать подобно обычным сравнениям. Эти операции индуцируют аналогичные операции на классах вычетов по модулю $f(x)$, превращая множество классов вычетов по двойному модулю в коммутативное кольцо с единицей. Нулевым элементом этого кольца является класс, состоящий из всех кратных многочлена $f(x)$, а единицей — класс вычетов E, содержащий единичный элемент 1 поля F_p.

Пусть теперь $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_{n-1}x + \alpha_n$ — неприводимый многочлен кольца $F_p[x]$. Если многочлен $a(x)$ из класса вычетов A не делится на $f(x)$, то многочлены a и f взаимно просты и, следовательно, в кольце $F_p[x]$ найдутся такие многочлены u и v, что $fu + av = 1$. В таком случае $a(x)v(x) \equiv 1 \pmod{f(x)}$ и, стало быть, уравнение $AX = E$ имеет единственное решение $X = V$, где V — класс вычетов по модулю $f(x)$, содержащий многочлен $v(x)$. Следовательно, в случае неприводимого многочлена $f(x)$ классы вычетов по модулю $f(x)$, отличные от нулевого класса, образуют по умножению абелеву группу порядка $q - 1$. Таким образом, нами установлен следующий результат.

Теорема 2. *Если $f(x)$ — неприводимый многочлен степени $n \geqslant 1$ из кольца $F_p[x]$, то классы вычетов по модулю $f(x)$ образуют конечное поле F_q, состоящее из $q = p^n$ элементов.*

2. Количество неприводимых в $F_p[x]$ многочленов степени n. Докажем существование для каждого целого $n \geqslant 1$ конечных полей F_q, где $q = p^n$. Для этого, согласно теореме 2, достаточно установить существование в кольце $F_p[x]$ неприводимых многочленов степени n.

Теорема 3. *Для каждого целого $n \geqslant 1$ в кольце $F_p[x]$ существует хотя бы один неприводимый многочлен степени n.*

Доказательство. Пусть g — отличный от нуля нормированный (со старшим коэффициентом 1) многочлен степени n из кольца $F_p[x]$. Положим $Ng = p^n$ и назовем эту величину *нормой многочлена* g. Ясно, что $N(f \cdot g) = Nf \cdot Ng$ для любых двух отличных от нуля нормированных многочленов f и g. Введем в рассмотрение *дзета-функцию*

$$\zeta(s) = \prod_f \left(1 - \frac{1}{(Nf)^s}\right)^{-1}$$

кольца $F_p[x]$, где $s = \sigma + it$ — комплексная переменная с $\sigma = \operatorname{Re} s > 1$, а произведение берется по всем нормированным неприводимым многочленам $f \in F_p[x]$, и заметим, что она представляет собой аналог дзета-функции Римана кольца целых чисел $\mathbb{Z}$. По теореме 1 об однозначности разложения на неприводимые

множители имеем

$$\zeta(s) = \prod_f \left(1 + \sum_{m=1}^{\infty} \frac{1}{(Nf)^{ms}}\right) = 1 + \sum_g \frac{1}{(Ng)^s},$$

где суммирование в правой части ведется по всем нормированным многочленам g кольца $F_p[x]$ положительной степени, и тогда

$$\zeta(s) = 1 + \sum_{n=1}^{\infty} \left(\sum_{\deg g = n} \frac{1}{(Ng)^s} \right).$$

Поскольку в кольце $F_p[x]$ имеется в точности p^n нормированных многочленов степени n, то из последнего равенства получим

$$\zeta(s) = 1 + \sum_{n=1}^{\infty} \frac{p^n}{p^{ns}} = \left(1 - \frac{p}{p^s}\right)^{-1}.$$

Следуя Гауссу, обозначим (n) число нормированных неприводимых многочленов $f \in F_p[x]$ степени n. Тогда, исходя из определения дзета-функции, имеем

$$\zeta(s) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{p^{ns}}\right)^{-(n)}$$

и в таком случае

$$\prod_{n=1}^{\infty} \left(1 - \frac{1}{p^{ns}}\right)^{-(n)} = \left(1 - \frac{p}{p^s}\right)^{-1}.$$

Логарифмируя последнее равенство, получаем соотношение

$$\sum_{n=1}^{\infty} (n) \log\left(1 - \frac{1}{p^{ns}}\right) = \log\left(1 - \frac{p}{p^s}\right),$$

которое, используя известное разложение функции $\log(1 - \tau)$ по степеням τ, можно переписать в виде

$$\sum_{n=1}^{\infty} (n) \sum_{l=1}^{\infty} \frac{p^m}{l p^{lns}} = \sum_{m=1}^{\infty} \frac{p^m}{m p^{ms}}.$$

Сравнивая в обеих частях этого соотношения коэффициенты при p^{-ms}, находим

$$\sum_{n|m} n\,(n) = p^m,$$

откуда по формуле обращения Мёбиуса (см. задачу 18)

$$(n) = \frac{1}{n} \sum_{d|n} \mu(d)\, p^{\frac{n}{d}}.$$

Выражение

$$\sum_{d|n} \mu(d)\, p^{\frac{n}{d}}$$

представляет собой сумму различных степеней простого числа p, взятых со знаками плюс и минус, а следовательно, не может быть равным нулю. В таком случае, поскольку (n) — неотрицательное целое число, имеем $(n) \geqslant 1$ и, стало быть, для всякого $n \geqslant 1$ в кольце $F_p[x]$ существуют неприводимые многочлены степени n.

3. Алгебраическая структура конечных полей. Выясним алгебраическую структуру полей F_q. Пусть многочлен $g(x)$ не делится на неприводимый в кольце $F_p[x]$ многочлен $f(x)$ степени n. Если r пробегает множество R, состоящее из $q-1$ отличных от нуля многочленов вида $a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$, то остатки от деления gr на многочлен f пробегают то же самое множество. Следовательно,

$$\prod_{r\in R} gr \equiv \prod_{r\in R} r \pmod{f(x)}$$

и тогда

$$(g^{q-1} - 1) \prod_{r\in R} r \equiv 0 \pmod{f(x)}.$$

Но многочлены r взаимно просты с f и, значит,

$$g^{q-1} - 1 \equiv 0 \pmod{f(x)}.$$

Переходя к классам вычетов кольца $F_p[x]$ по модулю $f(x)$, получаем следующий аналог малой теоремы Ферма.

Теорема 4. *Каждый отличный от нуля элемент поля F_q, $q = p^n$, удовлетворяет уравнению $z^{q-1} - 1 = 0$.*

Отсюда следует, что каждый элемент поля F_q является корнем многочлена $z^q - z$.

Далее, имеет место следующее обобщение теоремы Лагранжа.

Теорема 5. *Пусть $f(z)$ — отличный от нуля многочлен с коэффициентами из поля F_q. Тогда число корней многочлена $f(z)$ в поле F_q, взятых с их кратностями, не превосходит степени* $\deg f$ *многочлена $f(z)$.*

В дальнейшем единицу поля F_q будем обозначать 1. *Порядком* отличного от нуля элемента α поля F_q назовем наименьшее натуральное число m такое, что $\alpha^m = 1$. Заметим, что если α — элемент порядка m, то равенство $\alpha^j = \alpha^k$ возможно лишь в случае, когда $j \equiv k \pmod{m}$. В частности, взяв $j = q-1$, $k = 0$, получаем по теореме 4, что $q - 1 \equiv 0 \pmod{m}$. Таким образом, порядок каждого ненулевого элемента поля F_q делит число $q-1$. Покажем, что в каждом конечном поле F_q, $q = p^n$, имеется хотя бы один элемент η порядка $q-1$. Этим будет установлено, что

мультипликативная группа F_q^* поля F_q является циклической группой порядка $q-1$.

Теорема 6. *Конечное поле F_q содержит $\varphi(q-1)$ элементов порядка $q-1$, где $\varphi(n)$ — функция Эйлера.*

Доказательство. Пусть m — делитель числа $q-1$. Обозначим $\psi(m)$ число элементов поля F_q порядка m и предположим, что $\psi(m) > 0$. Из этого предположения следует, что в поле F_q существует элемент α порядка m. Степени $1, \alpha, \ldots, \alpha^{m-1}$ этого элемента различны между собой и являются корнями многочлена $z^m - 1$. По теореме 5 эти степени исчерпывают все корни многочлена $z^m - 1$, и, значит, каждый элемент порядка m должен иметь вид α^s при некотором $s = 0, 1, \ldots, m-1$. Если $(s, m) = d > 1$, то элемент α^s имеет порядок m/d, строго меньший m. Если же $(s, m) = 1$ и $\alpha^{sj} = 1$ для некоторого положительного целого $j < m$, то мы должны иметь $sj \equiv 0 \pmod{m}$, что невозможно. Таким образом, элемент α^s имеет порядок m в том и только в том случае, когда $(s, m) = 1$ и, стало быть, $\psi(m) = \varphi(m)$, где $\varphi(m)$ — функция Эйлера. Воспользуемся теперь равенством

$$\sum_{m|q-1} \psi(m) = q - 1$$

и известным соотношением (см., например, [142 а, гл. II, § 2] или задачу 4 из § 1)

$$\sum_{m|q-1} \varphi(m) = q - 1$$

для функции Эйлера $\varphi(m)$. Имеем

$$\sum_{m|q-1} [\varphi(m) - \psi(m)] = 0,$$

и в таком случае $\psi(m) = \varphi(m)$ для всех $m | q-1$. В частности, $\psi(q-1) = \varphi(q-1)$ и, тем самым, теорема доказана.

4. Автоморфизмы конечного поля F_q. Пусть F — произвольное поле и e — единичный элемент этого поля. *Характеристикой поля F* назовем такое наименьшее положительное целое число l (если оно существует), что

$$\sum_{j=1}^{l} e = l \cdot e = 0.$$

Если такого целого l не существует, то скажем, что поле F имеет характеристику нуль. Ясно, что если характеристика l поля F отлична от нуля, то l является простым числом. В поле F_q, состоящем из $q = p^n$ элементов, имеет место равенство $p \cdot 1 = 0$ и, следовательно, характеристика поля F_q равна p. Пусть α, β — произвольные элементы поля характеристики $p > 0$. По формуле

бинома Ньютона имеем

$$(\alpha+\beta)^p=\sum_{j=0}^{p}\binom{p}{j}\alpha^j\beta^{p-j}$$

и так как $\binom{p}{j}=\frac{p!}{j!\,(p-j)!}\equiv 0 \pmod p$ для всех $j=1, 2, \ldots, p-1$, то $(\alpha+\beta)^p=\alpha^p+\beta^p$. Таким образом, для любых двух элементов α, β поля F_q, $q=p^n$, справедливо равенство

$$(\alpha+\beta)^p=\alpha^p+\beta^p.$$

Вернемся к изложенному выше процессу построения поля F_q. Элементами этого поля являются классы вычетов кольца $F_p[x]$ по модулю $f(x)$, где $f(x)$ — неприводимый многочлен степени n с коэффициентами из поля F_p. Обозначим θ класс вычетов, содержащий многочлен $a(x)=x$. Тогда $f(\theta)=0$ и, следовательно, многочлен $f(x)$ является минимальным многочленом элемента $\theta\in F_q$. Из алгоритма деления с остатком $g=fh+r$, $r=a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n$, следует, что каждый элемент α поля F_q представляется в виде линейной комбинации

$$\alpha=r(\theta)=a_1\theta^{n-1}+a_2\theta^{n-2}+\ldots+a_n$$

элементов $1, \theta, \ldots, \theta^{n-1}$ с коэффициентами a_j из поля F_p. Степени $1, \theta, \ldots, \theta^{n-1}$ элемента θ линейно независимы над полем F_p и, стало быть, образуют базис поля F_q над полем F_p. Отсюда следует, что поле F_q является алгебраическим расширением поля F_p степени n.

Возводя обе части равенства $f(\theta)=0$ в степень p, получаем, ввиду малой теоремы Ферма и свойства полей характеристики p, что $f(\theta^p)=0$. Повторяя этот процесс несколько раз, убеждаемся, что, наряду с элементом θ, корнями многочлена $f(x)$ будут также $\theta^p, \ldots, \theta^{p^{n-1}}$. Заметим, что дальнейшее возведение в степень p не имеет смысла, ибо по теореме 4 $\theta^q=\theta$. Покажем, что элементы $\theta, \theta^p, \ldots, \theta^{p^{n-1}}$ различны между собой. Пусть η — элемент поля F_q порядка $q-1$ и пусть $\eta=a_1\theta^{n-1}+a_2\theta^{n-2}+\ldots+a_n$, где $a_j\in F_p$. Если предположить, что $\theta^{p^j}=\theta^{p^k}$ при $0\leqslant j<k\leqslant n-1$, то получим соотношение $\eta^{p^j}=\eta^{p^k}$. В таком случае $\eta^{p^k-p^j}=1$, и так как $1\leqslant p^k-p^j<q-1$, то приходим в противоречие с определением элемента η. Таким образом, для неприводимого многочлена $f(x)=x^n+\alpha_1x^{n-1}+\ldots+\alpha_n$ из кольца $F_p[x]$ справедливо разложение

$$f(x)=\prod_{j=0}^{n-1}(x-\theta^{p^j}).$$

Сопоставление

$$\theta\mapsto\theta^p$$

индуцирует автоморфизм

$$\sigma\colon F_q\to F_q$$

поля F_q, действующий на его элементы $\alpha=a_1\theta^{n-1}+a_2\theta^{n-2}+\ldots+a_n$ по правилу $\sigma(\alpha)=a_1\theta^{(n-1)p}+a_2\theta^{(n-2)p}+\ldots+a_n=(a_1\theta^{n-1}+a_2\theta^{n-2}+\ldots+a_n)^p=\alpha^p$ и оставляющий поле F_p неподвижным. Указанный автоморфизм σ называется *автоморфизмом Фробениуса* поля F_q.

Теорема 7. *Группа автоморфизмов (группа Галуа) поля F_q, $q=p^n$, является циклической группой порядка n с порождающим элементом σ.*

Доказательство. Степени $1, \sigma, \ldots, \sigma^{n-1}$ автоморфизма σ также являются автоморфизмами поля F_q, действующими на элементы $\alpha\in F_q$ по правилу

$$\sigma^j(\alpha)=\alpha^{p^j}.$$

Так как $\sigma^j(\theta)\neq\sigma^k(\theta)$ при $0\leqslant j<k\leqslant n-1$, то эти автоморфизмы различны между собой и, следовательно, исчерпывают все возможные автоморфизмы поля F_q, которых может быть не более, чем n. Теорема доказана.

Пусть Γ_m — группа Галуа поля F_{p^m} и Γ_n — группа Галуа поля F_{p^n}. Поле F_{p^m} является подполем поля F_{p^n} в том и только в том случае, когда Γ_m является подгруппой группы Γ_n. Учитывая этот факт, а также цикличность групп Γ_m и Γ_n, получаем следующий результат.

Теорема 8. *Поле F_{p^m} является подполем поля F_{p^n} тогда и только тогда, когда m делит n.*

Рассмотрим последовательность вложенных друг в друга полей

$$F_p\subset F_{p^{2!}}\subset F_{p^{3!}}\subset\ldots\subset F_{p^{n!}}\subset\ldots$$

и положим

$$\bar{F}_p=\bigcup_{n=1}^{\infty}F_{p^{n!}}.$$

Множество $\bar{F}_p$ является полем, поскольку для любых $\alpha, \beta\in\bar{F}_p$ найдется такое число n, что $\alpha, \beta\in F_{p^{n!}}$, и можно определить сумму $\alpha+\beta$ и произведение $\alpha\beta$ элементов α и β. Далее, всякий многочлен $g(x)$ из кольца $\bar{F}_p[x]$ имеет коэффициенты в некотором поле F_{p^m} и, если $f(x)$ — его неприводимый делитель в кольце $F_{p^m}[x]$, имеющий степень d, то все корни многочлена $f(x)$ лежат в поле $F_{p^{md}}$, являющемся при достаточно большом n подполем поля $F_{p^{n!}}$. Следовательно, корни многочлена $f(x)$ лежат в поле $\bar{F}_p$ и, таким образом, $\bar{F}_p$ является алгебраически замкнутым полем. Поле $\bar{F}_p$ называется *алгебраическим замыканием конечного простого поля F_p*.

Пусть σ — автоморфизм Фробениуса поля F_q, состоящего из $q = p^n$ элементов. Для каждого элемента $\alpha \in F_q$ определим его *норму* $\operatorname{norm}\alpha$ формулой

$$\operatorname{norm}\alpha = \prod_{j=0}^{n-1} \sigma^j(\alpha) = \prod_{j=0}^{n-1} \alpha^{p^j}.$$

Аналогичным образом определяем след

$$\operatorname{tr}\alpha = \sum_{j=0}^{n-1} \sigma^j(\alpha) = \sum_{j=0}^{n-1} \alpha^{p^j}$$

элемента $\alpha \in F_q$. Норма и след являются соответственно мультипликативным и аддитивным гомоморфизмами поля F_q в поле F_p.

Следующая теорема является частным случаем теоремы Гильберта 90.

Теорема 9. *Пусть F_q — конечное поле, состоящее из $q = p^n$ элементов.* Тогда

а) *норма элемента $\alpha \in F_q$ равна 1 в том и только в том случае, если существует ненулевой элемент $\beta \in F_q$, для которого $\alpha = \beta^{1-p}$;*

б) *след элемента $\alpha \in F_q$ равен нулю в том и только в том случае, если существует элемент $\gamma \in F_q$, для которого $\alpha = \gamma - \gamma^p$.*

Доказательство. а) Пусть поле F_q порождается над полем F_p элементом θ, так что $F_q = F_p(\theta)$. Для каждого $j = 0, 1, \ldots, n-1$ и всякого отличного от нуля элемента $\alpha \in F_q$ построим резольвенту Лагранжа — Гильберта

$$R(\alpha, \theta^j) = \theta^j + \alpha\theta^{jp} + \alpha^{1+p}\theta^{jp^2} + \ldots + \alpha^{1+p+\ldots+p^{n-2}}\theta^{jp^{n-1}}.$$

Поскольку определитель

$$\det \left\| \theta^{jp^k} \right\|_{0 \leqslant j,k \leqslant n-1},$$

являющийся определителем Вандермонда, отличен от нуля, то среди элементов $R(\alpha, \theta^j)$, $0 \leqslant j \leqslant n-1$, поля F_q найдется отличный от нуля. Пусть это будет элемент

$$\beta = \xi + \alpha\xi^p + \alpha^{1+p}\xi^{p^2} + \ldots + \alpha^{1+p+\ldots+p^{n-2}}\xi^{p^{n-1}}.$$

Если предположить, что $\operatorname{norm}\alpha = 1$, то получим

$$\alpha\beta^p = \alpha\xi^p + \alpha^{1+p}\xi^{p^2} + \ldots + \alpha^{1+p+\ldots+p^{n-2}}\xi^{p^{n-1}} + \xi = \beta$$

и тогда $\alpha = \beta^{1-p}$. Обратно, если $\alpha = \beta^{1-p}$, то $\operatorname{norm}\alpha = \dfrac{\operatorname{norm}\beta}{\operatorname{norm}\beta^p} = 1$.

б) Поскольку определитель

$$\det \left\| \theta^{jp^k} \right\|_{0 \leqslant j,k \leqslant n-1}$$

отличен от нуля, то среди элементов $\operatorname{tr}1$, $\operatorname{tr}\theta$, ..., $\operatorname{tr}\theta^{n-1}$ имеется по меньшей мере один ненулевой. Пусть $\delta = \theta^j$ и $\operatorname{tr}\delta \neq 0$. Положим

$$\gamma = \frac{1}{\operatorname{tr}\delta}\left[\alpha\delta^p + (\alpha + \alpha^p)\delta^{p^2} + \ldots + (\alpha + \alpha^p + \ldots + \alpha^{p^{n-2}})\delta^{p^{n-1}}\right].$$

Если предположить, что $\operatorname{tr}\alpha = 0$, то получим $\alpha = \gamma - \gamma^p$. Обратно, если $\alpha = \gamma - \gamma^p$, то, очевидным образом, $\operatorname{tr}\alpha = 0$.

5. Единственность поля F_q. В заключение параграфа покажем, что каждое конечное поле F изоморфно одному из рассмотренных нами полей F_q, где $q = p^n$. Поскольку поле F конечно, то оно имеет положительную характеристику p, являющуюся простым числом, и, значит, содержит поле, изоморфное простому конечному полю F_p. Отождествим F_p с его образом в поле F. Поскольку $F_p \subset F$, то поле F является конечномерным векторным пространством над F_p. Пусть размерность этого пространства равна n и пусть $\omega_1, \ldots, \omega_n$ — базис поля F над F_p. Всякий элемент $\alpha \in F$ однозначно представим в виде

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n,$$

где $a_j \in F_p$. Следовательно, поле F состоит из $q = p^n$ элементов. Далее, каждый элемент поля F является корнем многочлена $z^q - z$, и, значит, поле F является полем разложения этого многочлена. Но поле разложения многочлена $z^q - z$ однозначно определено в алгебраическом замыкании $\bar{F}_p$ поля F_p; получаем следующий результат.

Теорема 10. *Каждое конечное поле F_q, состоящее из $q = p^n$ элементов, однозначно определяется в алгебраическом замыкании $\bar{F}_p$ поля F_p как поле разложения многочлена $z^q - z$. Всякое конечное поле F изоморфно одному и только одному из полей F_q.*

С более детальным изложением теории конечных полей читатель может познакомиться по книге [72].

Задачи

1. Доказать, что в конечном поле F_q справедлив следующий аналог теоремы Вильсона:

$$\prod_{\alpha \in F_q^*} \alpha + 1 = 0.$$

2. Доказать индукцией по m и n, что в поле простой характеристики p справедливо равенство

$$\left(\sum_{j=1}^{m} \alpha_j\right)^{p^n} = \sum_{j=1}^{m} \alpha_j^{p^n}.$$

3. Пусть F_q — конечное поле из q элементов и $f(x)$ — неприводимый многочлен из кольца $F_q[x]$ степени m. Доказать, что $f(x)$ делит многочлен $x^{q^n} - x$ тогда и только тогда, когда m делит n.

4. Показать, что в кольце $F_q[x]$ справедливо разложение

$$x^{q^n} - x = \prod_{m|n} \prod_{f_m} f_m(x),$$

где внутреннее произведение берется по всем неприводимым нормированным многочленам степени m. Вывести отсюда, что для количества (m) неприводимых нормированных многочленов степени m из кольца $F_q[x]$ имеет место формула

$$(m) = \frac{1}{m} \sum_{d|m} \mu(d)\, q^{\frac{m}{d}}.$$

5. Пусть α — элемент порядка m поля F_q, где $q = p^n$, и ν — *показатель числа p по модулю m* (наименьшее положительное целое число такое, что $p^\nu \equiv 1 \pmod m$). Доказать, что многочлен $f(x) = \prod_{j=0}^{\nu-1} \left(x - \alpha^{p^j}\right)$ является неприводимым многочленом из кольца $F_p[x]$.

6. Пусть $f(x)$ — неприводимый многочлен степени m из кольца $F_p[x]$. Доказать, что в кольце $F_q[x]$, где $q = p^n$, многочлен $f(x)$ распадается на $d = (m, n)$ неприводимых множителей, каждый из которых имеет степень m/d.

7. Пусть F_q — конечное поле, состоящее из $q = p^n$ элементов, и F_p — его простое подполе. Доказать, что для каждого $\alpha \in F_p^*$ уравнение $\operatorname{norm} x = \alpha$ имеет $(p^n - 1)/(p - 1)$ решений и для каждого $\beta \in F_p$ уравнение $\operatorname{tr} y = \beta$ имеет p^{n-1} решений в элементах поля F_q.

8. В обозначениях предыдущей задачи показать, что

$$\sum_{x \in F_q} e^{2\pi i \frac{\operatorname{tr} \alpha x}{p}} = \begin{cases} q, & \text{если } \alpha = 0, \\ 0, & \text{если } \alpha \neq 0. \end{cases}$$

9. Пусть F_q — конечное поле и F_p — его простое подполе характеристики $p \neq 2$. Для символа

$$\left(\frac{\alpha}{q}\right) = \begin{cases} 0, & \text{если } \alpha = 0, \\ 1, & \text{если } \alpha \neq 0 \text{ и } \alpha \text{—квадрат в поле в } F_q, \\ -1, & \text{если } \alpha \text{ не является квадратом в } F_q, \end{cases}$$

доказать следующие свойства:

а) $\left(\frac{\alpha\beta}{q}\right) = \left(\frac{\alpha}{q}\right)\left(\frac{\beta}{q}\right)$ для любых элементов $\alpha, \beta \in F_q$;

б) $\sum_{\alpha \in F_q} \left(\frac{\alpha}{q}\right) = 0$;

в) $\left(\frac{\alpha}{q}\right) = \left(\frac{\operatorname{norm} \alpha}{p}\right)$, где $\left(\frac{a}{p}\right)$ — символ Лежандра.

10. Пусть $f(x) = ax^2 + bx + c$ — многочлен из кольца $F_q[x]$, где F_q — конечное поле характеристики $p \neq 2$, и $d = b^2 - 4ac$ — дискриминант многочлена $f(x)$. Доказать, что

$$\sum_{x \in F_q} \left(\frac{ax^2 + bx + c}{q}\right) = \begin{cases} \left(\frac{a}{q}\right)(q-1), & \text{если } d = 0, \\ -\left(\frac{a}{q}\right), & \text{если } d \neq 0. \end{cases}$$

11. Пусть F_q — конечное поле характеристики $p \neq 2$. Используя результат предыдущей задачи, показать, что число N_q решений уравнения $ax^2 + by^2 = \alpha$, $d = ab \neq 0$, в элементах поля F_q выражается формулой

$$N_q = \begin{cases} q + \left(\frac{-d}{q}\right)(q-1), & \text{если } \alpha = 0, \\ q - \left(\frac{-d}{q}\right), & \text{если } \alpha \neq 0. \end{cases}$$

12. Пусть F_q — конечное поле характеристики $p \neq 2$ и

$$f(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_n x_n^2$$

— квадратичная форма над полем F_q определителя $d = a_1 \ldots a_n \neq 0$. Доказать индукцией по s, что при $n = 2s$ число решений N_q уравнения

$$f(x_1, \ldots, x_n) = \alpha$$

в элементах поля F_q выражается формулой

$$N_q = \begin{cases} q^{2s-1} + \left(\frac{(-1)^s d}{q}\right)(q-1)\, q^{s-1}, & \text{если } \alpha = 0, \\ q^{2s-1} - \left(\frac{(-1)^s d}{q}\right) q^{s-1}, & \text{если } \alpha \neq 0. \end{cases}$$

13. В обозначениях предыдущей задачи показать, что при $n = 2s + 1$ величина N_q задается формулой

$$N_q = \begin{cases} q^{2s}, & \text{если } \alpha = 0, \\ q^{2s} + \left(\frac{(-1)^s \alpha d}{q}\right) q^s, & \text{если } \alpha \neq 0. \end{cases}$$

14. Пусть

$$D(f) = a_0^{2(m-1)} \prod_{1 \leqslant j < k \leqslant m} (\alpha_j - \alpha_k)^2$$

— *дискриминант многочлена* $f(x) = a_0 \prod_{j=1}^{m} (x - \alpha_j)$ и

$$R(f, g) = a_0^n b_0^m \prod_{j=1}^{m} \prod_{k=1}^{n} (\alpha_j - \beta_k)$$

— *результант многочленов* $f(x) = a_0 \prod_{j=1}^{m} (x - \alpha_j)$ и $g(x) = b_0 \prod_{k=1}^{n} (x - \beta_k)$.

Установить следующие свойства результанта:

а) $R(g, f) = (-1)^{mn} R(f, g)$;

б) если $g = fh + r$, то

$$R(f, g) = a_0^{n - \deg r} R(f, r);$$

в) если $f(x) = f_1(x) f_2(x)$, то

$$R(f, g) = R(f_1, g) R(f_2, g);$$

г) $R(f, g) = a_0^n \prod_{j=1}^{m} g(\alpha_j) = (-1)^{mn} b_0^m \prod_{k=1}^{n} f(\beta_k)$;

д) $R(f, g) = A(x) f(x) + B(x) g(x)$, где A, B — многочлены от x с коэффициентами из поля коэффициентов многочленов f и g;

е) если f — нормированный многочлен степени m, то

$$D(f) = (-1)^{\frac{m(m-1)}{2}} R(f, f') = (-1)^{\frac{m(m-1)}{2}} R(f', f),$$

где f' — производная многочлена f.

15. Используя результаты задачи 14, доказать, что если $f_1(x), \ldots, f_s(x)$ — нормированные многочлены, то

$$D\left(\prod_{j=1}^{s} f_j\right) = \prod_{j=1}^{s} D(f_j) \prod_{1 \leqslant j < k \leqslant s} R^2(f_j, f_k).$$

16*. Используя результат предыдущей задачи, доказать теорему Вороного — Штикельбергера [29, 148]: *если p — нечетное простое число, F_q — конечное поле, состоящее из $q = p^n$ элементов, и $f(x)$ — нормированный многочлен степени m из кольца $F_q[x]$ с отличным от нуля дискриминантом $D(f)$, то для числа s неприводимых делителей многочлена $f(x)$ в кольце $F_q[x]$ справедливо соотношение*

$$(-1)^{m-s} = \left(\frac{D(f)}{q}\right).$$

17. Пусть l, p — различные нечетные простые числа. Рассматривая в кольце $F_p[x]$ разложение многочлена $x^l - 1$ на неприводимые множители и используя теорему Вороного — Штикельбергера, вывести квадратичный закон взаимности Гаусса:

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}\cdot\frac{p-1}{2}}.$$

18. Пусть $\mu(n)$ — *функция Мёбиуса*, определенная для всех целых $n \geqslant 1$ равенствами:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^s, & \text{если } n = p_1 \ldots p_s \text{ есть произведение различных простых чисел } p_1, \ldots, p_s, \\ 0, & \text{если } n \text{ делится на квадрат простого числа,} \end{cases}$$

и $f(n)$ — произвольная *арифметическая функция* (комплекснозначная функция, определенная на множестве положительных целых чисел).

Установить справедливость следующих свойств функции Мёбиуса:

а) Функция $\mu(n)$ мультипликативна.

б) Выполняется соотношение

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases}$$

(Указание. В случае $n > 1$ воспользоваться тем обстоятельством, что все делители $d > 1$ числа $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$, для которых $\mu(d) \neq 0$, имеют вид $d = p_{i_1} \ldots p_{i_\sigma}$, $1 \leqslant i_1 < \ldots < i_\sigma \leqslant s$, а также мультипликативностью функции $\mu(n)$.)

в) Имеет место формула обращения Мёбиуса: *если*

$$g(n) = \sum_{d|n} f(d),$$

то

$$f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right).$$

(Указание. Воспользоваться определением функции $g\left(\frac{n}{d}\right)$ и результатом п. б).

19*. Пусть F_q — конечное поле и $f_1, \ldots, f_s \in F_q[x_1, \ldots, x_n]$ — многочлены положительных степеней $m_1, \ldots, m_s$. Доказать, что если $(m_1 + \ldots + m_s) < n$, то число N_q решений системы уравнений

$$f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0$$

в элементах поля F_q делится на характеристику p поля F_q.

§ 3. L-функции Артина

1. Характеры конечных абелевых групп. Как следует из задачи 5 из § 1 вопрос о числе решений уравнения

$$a_1 x_1^{m_1} + \ldots + a_n x_n^{m_n} = a_0$$

в элементах простого конечного поля F_p сводится к оценке тригонометрической суммы

$$T(a, p) = \sum_{x \in F_p} e^{2\pi i \frac{a x^m}{p}}.$$

Более широкое применение находят суммы

$$T(g) = \sum_{x \in F_p} e^{2\pi i \frac{g(x)}{p}}$$

с произвольным многочленом $g \in F_p[x]$.

Далее, число N_p решений уравнения

$$y^2 = f(x), \; f \in F_p[x],$$

в элементах поля F_p характеристики $p > 2$ выражается формулой

$$N_p = \sum_{x \in F_p} \left(1 + \left(\frac{f(x)}{p}\right)\right) = p + \sum_{x \in F_p} \left(\frac{f(x)}{p}\right).$$

Поэтому вопрос о величине N_p сводится к оценке сумм символов Лежандра

$$S(f) = \sum_{x \in F_p} \left(\frac{f(x)}{p}\right).$$

Для дальнейшего потребуется обобщение сумм $S(f)$ и $T(g)$ на случай произвольного конечного поля F_q.

Напомним, что *характером конечной абелевой группы* G называется гомоморфизм группы G в мультипликативную группу $\mathbb{C}^*$ поля комплексных чисел $\mathbb{C}$. Другими словами, характер группы G — это такая не обращающаяся в нуль комплекснозначная функция χ на G, для которой

$$\chi(xy) = \chi(x)\chi(y)$$

для любых $x, y \in G$.

Так как при гомоморфизме групп единичный элемент отображается на единичный, то $\chi(1)=1$. Если χ_1 и χ_2 — характеры группы G, то произведение $\chi_1\chi_2$, определяемое по формуле $(\chi_1\chi_2)(x)=\chi_1(x)\chi_2(x)$, также является характером группы G. Далее, отображение χ^{-1}, определяемое равенством $\chi^{-1}(x)=\overline{\chi(x)}$, будет, наряду с χ, характером группы G и, значит, характеры группы G образуют по умножению абелеву группу $\overline{G}$ с единичным элементом χ_0 таким, что $\chi_0(x)=1$ для всех $x\in G$. Группа $\overline{G}$ называется *двойственной группой* к группе G.

Пример. Символ Лежандра $\left(\frac{x}{p}\right)$ является характером мультипликативной группы F_p^* простого конечного поля F_p. Функция $e^{2\pi i\frac{x}{p}}$ является характером аддитивной группы этого поля.

Лемма 1. *Пусть G — циклическая группа порядка n и η — ее порождающий элемент. Каждый характер χ группы G имеет вид*

$$\chi_\alpha(\eta^k)=e^{2\pi i\frac{\alpha k}{n}},\quad 0\leqslant k\leqslant n-1,$$

при некотором $\alpha=0, 1, \ldots, n-1$.

Доказательство. Пусть χ — произвольный характер группы G. Имеем $\chi^n(\eta)=\chi(\eta^n)=\chi(1)=1$, и, значит, $\chi(\eta)$ является корнем степени n из 1. Следовательно, $\chi(\eta)=e^{2\pi i\frac{\alpha}{n}}$ при некотором $\alpha=0, 1, \ldots, n-1$ и тогда

$$\chi(\eta^k)=e^{2\pi i\frac{\alpha k}{n}}.$$

Следствие. *Группа характеров $\overline{G}$ циклической группы G изоморфна группе G.*

Доказательство. Все характеры χ_s, $0\leqslant s\leqslant n-1$, различны между собой и образуют циклическую группу порядка n с порождающим элементом χ_1.

Пусть теперь G — произвольная конечная абелева группа порядка $n=p_1^{s_1}\ldots p_r^{s_r}$, где $p_1, \ldots, p_r$ — простые числа. Группа G представляется в виде прямого произведения

$$G=G_1\times\ldots\times G_r$$

циклических групп $G_1, \ldots, G_r$, имеющих порядки $n_1=p_1^{s_1}, \ldots, n_r=p_r^{s_r}$ соответственно (см., например, [136]). Пусть $\eta_1, \ldots, \eta_r$ — порождающие элементы групп $G_1, \ldots, G_r$. Если χ — произвольный характер группы G, то $\chi(\eta_j)=e^{2\pi i\frac{\alpha_j}{n_j}}$ при некотором $\alpha_j=0, 1, \ldots, n_j-1$, а так как каждый элемент $x\in G$ однозначно представим в виде

$$x=\eta_1^{k_1}\ldots\eta_r^{k_r},\quad 0\leqslant k_j\leqslant n_j-1,$$

то

$$\chi(x)=\chi\left(\eta_1^{k_1}\ldots\eta_r^{k_r}\right)=\chi\left(\eta_1^{k_1}\right)\ldots\chi\left(\eta_r^{k_r}\right)=$$
$$=\chi^{k_1}(\eta_1)\ldots\chi^{k_r}(\eta_r)=e^{2\pi i\frac{\alpha_1k_1}{n_1}}\ldots e^{2\pi i\frac{\alpha_rk_r}{n_r}}.$$

Нами установлен следующий результат.

Лемма 2. *Пусть G — конечная абелева группа порядка $n=p_1^{s_1}\ldots p_r^{s_r}$ и $G=G_1\times\ldots\times G_r$ — ее представление в виде прямого произведения циклических групп $G_1, \ldots, G_r$ порядков $n_1=p_1^{s_1}, \ldots, n_r=p_r^{s_r}$ соответственно. Тогда каждый характер χ группы G имеет вид*

$$\chi_{\alpha_1,\ldots,\alpha_r}\left(\eta_1^{k_1}\ldots\eta_r^{k_r}\right)=e^{2\pi i\frac{\alpha_1k_1}{n_1}}\ldots e^{2\pi i\frac{\alpha_rk_r}{n_r}}$$

при некоторых $\alpha_j=0, 1, \ldots, n_j-1$, $1\leqslant j\leqslant r$.

Следствие. *Группа характеров $\overline{G}$ конечной абелевой группы G изоморфна группе G.*

Доказательство. Характеры $\chi_{\alpha_1,\ldots,\alpha_n}$, $0\leqslant\alpha_j\leqslant n_j-1$, $1\leqslant j\leqslant r$, образуют конечную абелеву группу $\overline{G}$, являющуюся прямым произведением циклических групп порядков $n_1, \ldots, n_r$. Стало быть, $\overline{G}$ изоморфна группе G.

Лемма 3. *Пусть G — конечная абелева группа порядка n. Тогда*

$$\sum_{x\in G}\chi(x)=\begin{cases}n, & \text{если } \chi=\chi_0,\\ 0, & \text{если } \chi\neq\chi_0,\end{cases}$$

и

$$\sum_{\chi\in\overline{G}}\chi(x)=\begin{cases}n, & \text{если } x=1,\\ 0, & \text{если } x\neq 1.\end{cases}$$

Доказательство. Если $\chi=\chi_0$, то утверждение очевидно. Пусть $\chi\neq\chi_0$. Тогда существует элемент $x_0\in G$, для которого $\chi(x_0)\neq 1$. Имеем

$$S=\sum_{x\in G}\chi(x)=\sum_{x\in G}\chi(x_0x)=\chi(x_0)S$$

и, значит, $S=0$.

Второе утверждение следует из первого, поскольку группа G естественно изоморфна группе, двойственной к $\overline{G}$.

2. Характеры поля F_q. Перейдем к изучению характеров конечного поля F_q. Ненулевые элементы поля F_q образуют по умножению циклическую группу F_q^* порядка $q-1$. Группа характеров группы F_q^* изоморфна F_q^*. Характер χ_0, равный 1 для всех $x \in F_q^*$, назовем *тривиальным характером*. Каждый характер χ группы F_q^* удовлетворяет уравнению $\chi^{q-1} = \chi_0$. Наименьшее положительное целое d, для которого $\chi^d = \chi_0$, назовем *порядком характера* χ и будем обозначать его через $\operatorname{ord}\chi$. Ясно, что d является делителем числа $q-1$. Далее, если $\chi^s = \chi_0$, то число $s \geqslant 1$ назовем *показателем характера* χ и обозначим его через $\operatorname{ind}\chi$. Легко проверить, что s является показателем характера χ в том и только в том случае, когда $d = \operatorname{ord}\chi$ делит s.

Пусть s — делитель числа $q-1$ и $(F_q^*)^s$ — подгруппа элементов $y \in F_q^*$, представимых в виде $y = x^s$, $x \in F_q^*$. Если χ — характер группы F_q^* показателя s, то мы имеем $\chi(x^s) = \chi^s(x) = 1$. Обратно, если $\chi(y) = 1$ для всех $y \in (F_q^*)^s$, то $\chi^s = \chi_0$. Таким образом, $\chi(x)$ зависит лишь от класса смежности группы F_q^* по подгруппе $(F_q^*)^s$, и, значит, характер χ показателя s можно трактовать как характер факторгруппы $F_q^*/(F_q^*)^s$. Ясно, что имеется в точности s таких характеров.

Расширим определение характера χ группы F_q^*, положив

$$\chi(0) = \begin{cases} 1, & \text{если } \chi = \chi_0, \\ 0, & \text{если } \chi \neq \chi_0. \end{cases}$$

Такой характер χ назовем *мультипликативным характером поля* F_q.

Лемма 4. *Пусть s — положительное число, делящее $q-1$. Тогда*

$$\sum_{\operatorname{ind}\chi = s} \chi(x) = \begin{cases} s, & \text{если } x \in (F_q^*)^s, \\ 0, & \text{если } x \notin (F_q^*)^s \text{ и } x \neq 0, \\ 1, & \text{если } x = 0. \end{cases}$$

Если η — порождающий элемент мультипликативной группы F_q^* поля F_q и $\chi \neq \chi_0$ — мультипликативный характер поля F_q показателя s, то

$$\sum_{j=0}^{s-1} \chi(\eta^j) = 0.$$

Доказательство. При $x \neq 0$ первое утверждение следует из леммы 3; при $x = 0$ имеем

$$\sum_{\operatorname{ind}\chi = s} \chi(x) = \chi_0(0) + \sum_{\substack{\chi \neq \chi_0 \\ \operatorname{ind}\chi = s}} \chi(0) = 1.$$

Для доказательства второго утверждения заметим, что χ является нетривиальным характером факторгруппы $F_q^*/(F_q^*)^s$ и что $1, \eta, \eta^2, \ldots, \eta^{s-1}$ пробегают все элементы этой факторгруппы. Тогда утверждение следует из леммы 3.

Введем теперь в рассмотрение *аддитивные характеры* ψ поля F_q, которые представляют собой характеры аддитивной группы поля F_q.

Лемма 5. *Каждый аддитивный характер ψ поля F_q характеристики p имеет вид*

$$\psi_\beta(x) = e^{2\pi i \frac{\operatorname{tr}(\beta x)}{p}}$$

при некотором $\beta \in F_q$.

Доказательство. Имеем

$$\psi_\beta(x+y) = \psi_\beta(x)\psi_\beta(y)$$

и, стало быть, функции $\psi_\beta(x)$ являются аддитивными характерами поля F_q. Все они различны между собой, и их число равно q. Значит, $\psi_\beta(x)$ исчерпывают все аддитивные характеры поля F_q. Лемма доказана.

3. Производящая функция Артина. Пусть F_{q^ν} — расширение степени ν поля F_q и F_p — простое подполе поля F_q. Группа Галуа Γ_ν поля F_{q^ν} над полем F_q является циклической группой порядка ν. Обозначим σ_ν порождающий элемент группы Γ_ν. Его действие на элементы $x \in F_{q^\nu}$ задается правилом $\sigma_\nu(x) = x^q$. Отображение

$$\operatorname{tr}_\nu x = x + \sigma_\nu(x) + \ldots + \sigma_\nu^{\nu-1}(x) = x + x^q + \ldots + x^{q^{\nu-1}}$$

поля F_{q^ν} в поле F_q назовем *относительным следом* элемента $x \in F_{q^\nu}$, а отображение

$$\operatorname{norm}_\nu x = x \cdot \sigma_\nu(x) \ldots \sigma_\nu^{\nu-1}(x) = x \cdot x^q \ldots x^{q^{\nu-1}}$$

поля F_{q^ν} в поле F_q назовем *относительной нормой* элемента x. Далее, если tr и norm являются следом и нормой из поля F_q в поле F_p, то отображения $\operatorname{Tr}_\nu x = \operatorname{tr}(\operatorname{tr}_\nu x)$ и $\operatorname{Norm}_\nu x = \operatorname{norm}(\operatorname{norm}_\nu x)$ поля F_{q^ν} в поле F_p назовем соответственно *абсолютным следом* и *абсолютной нормой* элемента $x \in F_{q^\nu}$.

Если χ — мультипликативный характер поля F_q, то

$$\chi_\nu(x) = \chi(\operatorname{norm}_\nu x)$$

является характером поля F_{q^ν}. Назовем $\chi_\nu(x)$ *мультипликативным характером, индуцированным характером* χ. Аналогично, если ψ — аддитивный характер поля F_q, то

$$\psi_\nu(x) = \psi(\operatorname{tr}_\nu x)$$

является характером поля F_{q^ν}, который назовем *аддитивным характером, индуцированным характером* ψ.

Пусть $f(x)=x^l+a_1x^{l-1}+\ldots+a_l$, $g(x)=b_0x^n+b_1x^{n-1}+\ldots+b_{n-1}x$ — непостоянные многочлены из кольца $F_q[x]$ и $f=f_1^{s_1}\ldots f_r^{s_r}$ — разложение многочлена f на различные неприводимые множители $f_1, \ldots, f_r \in F_q[x]$. Рассмотрим суммы

$$T_\nu = T_\nu(f, g) = \sum_{x\in F_{q^\nu}} \chi_\nu(f(x))\,\psi_\nu(g(x)) \tag{1}$$

и покажем, что они регулярным образом зависят от целочисленного параметра ν. Для выяснения зависимости T_ν от ν введем в рассмотрение *L-функцию Артина* $L(z)$ комплексного переменного z, которую определим в виде ряда

$$L(z) = L(z, f, g) = \exp\left(\sum_{\nu=1}^{\infty} \frac{T_\nu}{\nu} z^\nu\right), \tag{2}$$

абсолютно сходящегося в круге $|z| < q^{-1}$ и равномерно — в каждом меньшем круге $|z| < q^{-1-\sigma_0}$, где σ_0 — фиксированное положительное число.

В дальнейшем дадим другое определение L-функции Артина $L(z)=L(z, \widetilde{\chi})$, которое (при надлежащем выборе характера $\widetilde{\chi}$) эквивалентно данному и аналогично определению L-ряда Дирихле для полей алгебраических чисел.

Для каждого $\nu \geqslant 1$ положим

$$\beta_\nu = \sum_{i_1+2i_2+\ldots+\nu i_\nu=\nu} \frac{T_1^{i_1}\ldots T_\nu^{i_\nu}}{i_1!\ldots i_\nu!\, 1^{i_1}\ldots \nu^{i_\nu}}, \tag{3}$$

где суммирование ведется по всем неотрицательным целым $i_1, \ldots, i_\nu$ с условием $i_1+2i_2+\ldots+\nu i_\nu=\nu$, и заметим, что β_ν лежат в поле алгебраических чисел $\mathbb{Q}(e^{2\pi i/p})$, полученном из поля рациональных чисел $\mathbb{Q}$ присоединением к нему примитивного корня степени p из 1.

Лемма 6. *Пусть s — положительное целое, делящее $q-1$ и $\deg(f_1\ldots f_r)=m$. Предположим, что выполнено хотя бы одно из следующих двух условий:*

1) *χ — нетривиальный мультипликативный характер поля F_q показателя s и $(s, s_1, \ldots, s_r)=1$;*

2) *ψ — нетривиальный аддитивный характер поля F_q и*

$$b_0 \not\equiv 0, \quad (n, q)=1.$$

Тогда $\beta_\nu = 0$ для всех $\nu > m+n-1$.

Доказательство. Пусть $i_1, \ldots, i_\nu$ — неотрицательные целые числа, удовлетворяющие условию $i_1+2i_2+\ldots+\nu i_\nu=\nu$.

Если для каждого $\tau=1, 2, \ldots, \nu$ многочлен

$$\alpha(x)=x^\nu+u_1x^{\nu-1}+\ldots+u_\nu \in F_q[x]$$

имеет в кольце $F_q[x]$ ровно i_τ неприводимых делителей степени τ, то набор $(i_1, \ldots, i_\nu)$ назовем *типом разложения многочлена* $\alpha(x)$. Пусть

$$\alpha(x) = \prod_{\tau=1}^{\nu} \prod_{j=1}^{i_\tau} \prod_{k=0}^{\tau-1} \left(x+\sigma_\tau^k\left(x_j^{(\tau)}\right)\right),$$

где

$$x_1^{(1)}, \ldots, x_{i_1}^{(1)} \in F_q;\ \ldots;\ x_1^{(\nu)}, \ldots, x_{i_\nu}^{(\nu)} \in F_{q^\nu}.$$

Легко видеть, что когда неотрицательные целые $i_1, \ldots, i_\nu$ пробегают все решения уравнения $i_1+2i_2+\ldots+\nu i_\nu=\nu$ и $x_1^{(\tau)}, \ldots, x_{i_\tau}^{(\tau)}$ независимо друг от друга пробегают все элементы полей F_{q^τ}, $1\leqslant\tau\leqslant\nu$, то элементарные симметрические функции этих элементов $u_1, \ldots, u_\nu$ независимо друг от друга пробегают все элементы поля F_q. Далее, функции $u_1, \ldots, u_\nu$ инвариантны при всех перестановках элементов $x_1^{(\tau)}, \ldots, x_{i_\tau}^{(\tau)} \in F_{q^\tau}$, $1\leqslant\tau\leqslant\nu$, а также при замене их на сопряженные над полем F_q. Поэтому, если (согласно основной теореме о симметрических функциях) положить

$$\widetilde{f}(u_1, \ldots, u_\nu) = \prod_{\tau=1}^{\nu} \prod_{j=1}^{i_\tau} \prod_{k=0}^{\tau-1} \sigma_\tau^k f\left(x_j^{(\tau)}\right),$$

$$\widetilde{g}(u_1, \ldots, u_\nu) = \sum_{\tau=1}^{\nu} \sum_{j=1}^{i_\tau} \sum_{k=0}^{\tau-1} \sigma_\tau^k g\left(x_j^{(\tau)}\right)$$

и каждому многочлену $\alpha(x)=x^\nu+u_1x^{\nu-1}+\ldots+u_\nu$ с типом разложения $(i_1, \ldots, i_\nu)$ поставить в соответствие $i_1!\ldots i_\nu!\,1^{i_1}\ldots\nu^{i_\nu}$ возможно повторяющихся наборов

$$\left(x_1^{(1)}, \ldots, x_{i_1}^{(1)};\ \ldots;\ x_1^{(\nu)}, \ldots, x_{i_\nu}^{(\nu)}\right),$$

то получим соотношение

$$\beta_\nu = \sum_{u_1,\ldots,u_\nu\in F_q} \chi\left(\widetilde{f}(u_1, \ldots, u_\nu)\right)\psi\left(\widetilde{g}(u_1, \ldots, u_\nu)\right). \tag{4}$$

В дальнейшем будем считать, что $\nu > m+n-1$. Пусть $\deg f_i = \nu_i$, $1\leqslant i\leqslant r$, и пусть $f_i(x)=\prod_{\mu=1}^{\nu_i}(x+\alpha_{i\mu})$ — разложение многочлена f_i на линейные множители в кольце $F_{q^{\nu_i}}[x]$. Поскольку

$$\prod_{\tau=1}^{\nu} \prod_{j=1}^{i_\tau} \prod_{k=0}^{\tau-1} \left(\sigma_\tau^k\left(x_j^{(\tau)}\right)+\alpha_{i\mu}\right) = \alpha_{i\mu}^\nu + u_1\alpha_{i\mu}^{\nu-1} + \ldots + u_\nu,$$

то имеем

$$\widetilde{f}(u_1, \ldots, u_\nu) = \prod_{i=1}^{r} \prod_{\mu=1}^{\nu_i} (\alpha_{i\mu}^{\nu} + u_1 \alpha_{i\mu}^{\nu-1} + \ldots + u_\nu)^{s_i}.$$

Положим

$$\begin{aligned} &\alpha_{11}^{\nu} + u_1 \alpha_{11}^{\nu-1} + \ldots + u_\nu = \xi_1, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\alpha_{r1}^{\nu} + u_1 \alpha_{r1}^{\nu-1} + \ldots + u_\nu = \xi_r. \end{aligned} \tag{5}$$

Если $u_1, \ldots, u_{\nu-m}$ фиксированы, а $u_{\nu-m+1}, \ldots, u_\nu$ независимо друг от друга пробегают все элементы поля F_q, то $\xi_1, \ldots, \xi_r$ независимо друг от друга пробегают все элементы полей $F_{q^{\nu_1}}, \ldots, F_{q^{\nu_r}}$ соответственно. При этом

$$\widetilde{f}(u_1, \ldots, u_\nu) = \prod_{i=1}^{r} (\operatorname{norm}_{\nu_i} \xi_i)^{s_i} = \prod_{i=1}^{r} \zeta_i^{s_i} \tag{6}$$

и отличные от нуля элементы $\zeta_i = \operatorname{norm}_{\nu_i} \xi_i$ ровно по $\frac{q^{\nu_i}-1}{q-1}$ раз пробегают все элементы мультипликативной группы F_q^* поля F_q.

Далее, по формуле Варинга (см., например, [21, с. 211]) имеем

$$\sum_{\tau=1}^{\nu} \sum_{j=1}^{i_\tau} \sum_{k=0}^{\tau-1} \left(\sigma_\tau^k \left(x_j^{(\tau)}\right)\right)^\mu = \sum_{\lambda_1+2\lambda_2+\ldots+\nu\lambda_\nu=\mu} a_{\lambda_1,\ldots,\lambda_\nu}^{(\mu)} u_1^{\lambda_1} \ldots u_\nu^{\lambda_\nu},$$

где

$$a_{\lambda_1,\ldots,\lambda_\nu}^{(\mu)} = \frac{(-1)^{\lambda_2+2\lambda_3+\ldots+(\nu-1)\lambda_\nu} \mu\,(\lambda_1+\ldots+\lambda_\nu-1)!}{\lambda_1! \ldots \lambda_\nu!},$$

и тогда

$$\widetilde{g}(u_1, \ldots, u_\nu) = \sum_{\mu=1}^{n} b_{n-\mu} \sum_{\lambda_1+2\lambda_2+\ldots+\nu\lambda_\nu=\mu} a_{\lambda_1,\ldots,\lambda_\nu}^{(\mu)} u_1^{\lambda_1} \ldots u_\nu^{\lambda_\nu} =$$

$$= (-1)^{n-1} b_0 n u_n + \widetilde{g}'(u_1, \ldots, u_{n-1}). \tag{7}$$

Учитывая (4), (6), (7), при условии, что $\nu > m+n-1$, получаем

$$\beta_\nu = N \sum_{u_1,\ldots,u_{\nu-m} \in F_q} \psi((-1)^{n-1} b_0 n u_n)\, \psi(\widetilde{g}'(u_1, \ldots, u_{n-1})) \times$$

$$\times \sum_{\zeta_1,\ldots,\zeta_r \in F_q} \chi\left(\zeta_1^{s_1} \ldots \zeta_r^{s_r}\right),$$

где

$$N = \prod_{i=1}^{r} \frac{q^{\nu_i}-1}{q-1}.$$

Пусть χ — нетривиальный характер показателя s и η — порождающий элемент мультипликативной группы F_q^* поля F_q. Тогда

$$\sum_{\zeta_1,\ldots,\zeta_r \in F_q} \chi\left(\zeta_1^{s_1} \ldots \zeta_r^{s_r}\right) = \sum_{\zeta_1,\ldots,\zeta_r \in F_q^*} \chi\left(\zeta_1^{s_1} \ldots \zeta_r^{s_r}\right).$$

Положим $\zeta_i = \eta^{h_i}$, $1 \leqslant i \leqslant r$, так что $\zeta_1^{s_1} \ldots \zeta_r^{s_r} = \eta^{h_1 s_1 + \ldots + h_r s_r}$. Имеем $(s, s_1, \ldots, s_r) = 1$, и, стало быть, если $k_1, \ldots, k_r$ независимо друг от друга пробегают значения $1, 2, \ldots, q-1$, то числа $k_1 s_1 + \ldots + k_r s_r$ с одинаковой кратностью пробегают все элементы $0, 1, \ldots, s-1$ полной системы вычетов по модулю s. В таком случае произведение $\zeta_1^{s_1} \ldots \zeta_r^{s_r}$ по нескольку раз пробегает все элементы факторгруппы $F_q^*/(F_q^*)^s$ и, так как χ — нетривиальный характер этой факторгруппы, то лемме 4

$$\sum_{\zeta_1,\ldots,\zeta_r \in F_q^*} \chi\left(\zeta_1^{s_1} \ldots \zeta_r^{s_r}\right) = 0.$$

Таким образом, если $\chi \neq \chi_0$, то $\beta_\nu = 0$ при всех $\nu > m+n-1$.

Пусть теперь ψ — нетривиальный аддитивный характер поля F_q. Из уравнений (5) следует, что $u_{\nu-m+1}, \ldots, u_\nu$ однозначно определяются по $\xi_1, \ldots, \xi_r, u_1, \ldots, u_{\nu-m}$, и тогда

$$\beta_\nu = N \sum_{\zeta_1,\ldots,\zeta_r \in F_q} \chi\left(\zeta_1^{s_1} \ldots \zeta_r^{s_r}\right) \sum_{u_1,\ldots,u_{\nu-m} \in F_q} \psi((-1)^{n-1} b_0 n u_n)\, \psi \times$$

$$\times (\widetilde{g}'(u_1, \ldots, u_{n-1})).$$

Мы имеем

$$\sum_{u_1,\ldots,u_{\nu-m} \in F_q} \psi((-1)^{n-1} b_0 n u_n)\, \psi(\widetilde{g}'(u_1, \ldots, u_{n-1})) =$$

$$= q^{\nu-m-n} \sum_{u_1,\ldots,u_{n-1} \in F_q} \psi(\widetilde{g}'(u_1, \ldots, u_{n-1})) \sum_{u_n \in F_q} \psi((-1)^{n-1} n b_0 u_n)$$

и так как по условию $b_0 \neq 0$, $(n, q) = 1$, то $u = (-1)^{n-1} b_0 n u_n$ вместе с u_n пробегает все элементы поля F_q. В таком случае, по лемме 3

$$\sum_{u_n \in F_q} \psi((-1)^{n-1} b_0 n u_n) = \sum_{u \in F_q} \psi(u) = 0$$

и, значит, снова получаем, что $\beta_\nu = 0$. Лемма доказана.

Пусть алгебраические числа β_ν определены соотношениями (3). Рассмотрим многочлен

$$P(z) = 1 + \beta_1 z + \ldots + \beta_{m+n-1} z^{m+n-1}$$

и обозначим K минимальное расширение поля $\mathbb{Q}(e^{2\pi i/p})$, в

котором имеет место разложение

$$P(z) = \prod_{j=1}^{m+n-1} (1 - \omega_j z). \tag{8}$$

Теорема 1. *Пусть* $f(x) = f_1^{s_1}(x) \dots f_r^{s_r}(x)$, $g(x) = b_0 x^n + b_1 x^{n-1} + \dots + b_{n-1}x$ — *непостоянные многочлены из кольца* $F_q[x]$ *степеней* l, n *соответственно*, s — *положительное целое число, делящее* $q-1$, *и* $\deg(f_1 \dots f_r) = m$. *Если выполнено хотя бы одно из следующих двух условий:*

1) χ — *нетривиальный мультипликативный характер поля* F_q *показателя* s *и* $(s, s_1, \dots, s_r) = 1$;

2) ψ — *нетривиальный аддитивный характер поля* F_q *и* $b_0 \neq 0$, $(n, q) = 1$, *то L-функция Артина* (2) *имеет вид*

$$L(z) = P(z).$$

Далее, если алгебраические числа $\omega_1, \dots, \omega_{m+n-1}$ *определены разложением* (8), *то для суммы* (1) *справедливо представление*

$$T_\nu = -\sum_{j=1}^{m+n-1} \omega_j^\nu, \quad \nu = 1, 2, \dots$$

Доказательство. По известному комбинаторному тождеству (см., например, [103, с. 84]) имеем

$$\exp\left(\sum_{\nu=1}^{\infty} \frac{T_\nu}{\nu} z^\nu\right) = 1 + \sum_{\nu=1}^{\infty} \beta_\nu z^\nu.$$

и тогда по лемме 6

$$\exp\left(\sum_{\nu=1}^{\infty} \frac{T_\nu}{\nu} z^\nu\right) = P(z).$$

Следовательно, ввиду (8),

$$L(z) = \prod_{j=1}^{m+n-1} (1 - \omega_j z).$$

Далее,

$$\sum_{\nu=1}^{\infty} \frac{T_\nu}{\nu} z^\nu = \sum_{j=1}^{m+n-1} \log(1 - \omega_j z) = -\sum_{\nu=1}^{\infty} \left(\sum_{j=1}^{m+n-1} \omega_j^\nu\right) \frac{z^\nu}{\nu}$$

и, в таком случае,

$$T_\nu = -\sum_{j=1}^{m+n-1} \omega_j^\nu$$

для всех $\nu \geqslant 1$.

Следствие. *L-функция Артина* (2) *аналитически продолжима на всю комплексную плоскость и регулярна в каждой точке этой плоскости.*

Теорема 2. *Пусть* $\omega_1, \dots, \omega_r$ — *комплексные числа и* c, R — *положительные числа. Если*

$$|\omega_1^\nu + \dots + \omega_r^\nu| \leqslant cR^\nu \tag{9}$$

для всех $\nu = 1, 2, \dots$, *то* $|\omega_j| \leqslant R$ *при* $j = 1, 2, \dots, r$.

Доказательство. При достаточно малых значениях $|z|$ имеем

$$\log(1 - \omega z) = -\sum_{\nu=1}^{\infty} \frac{\omega^\nu}{\nu} z^\nu$$

и тогда

$$\log \prod_{j=1}^{r} (1 - \omega_j z) = -\sum_{\nu=1}^{\infty} (\omega_1^\nu + \dots + \omega_r^\nu) \frac{z^\nu}{\nu}.$$

Ввиду условия (9) ряд справа сходится для всех $|z| < R^{-1}$ и, значит, функция

$$\log \prod_{j=1}^{r} (1 - \omega_j z)$$

регулярна в круге $|z| < R^{-1}$. В таком случае $1 - \omega_j z \neq 0$ при $|z| < R^{-1}$ и, следовательно, $|\omega_j| \leqslant R$ для всех $j = 1, 2, \dots, r$.

Задачи

1. Показать, что конечная циклическая группа порядка p^α, где p — простое число, не представима в виде прямого произведения собственных подгрупп.

2. Пусть порядок n конечной циклической группы G равен произведению взаимно простых чисел l и m. Доказать, что G представляется в виде прямого произведения ее циклических подгрупп порядков l и m.

3. Пусть η — элемент максимального порядка конечной абелевой группы G. Доказать, что циклическая группа, порожденная элементом η, выделяется в качестве прямого сомножителя группы G.

4. Пусть F_q — конечное поле и χ, ψ — мультипликативный и аддитивный характеры этого поля. Доказать, что для *суммы Гаусса*

$$T(\chi, \psi) = \sum_{x \in F_q} \chi(x) \psi(x)$$

справедливы соотношения:

а) $T(\chi_0, \psi_0) = q$;

б) если $\chi \neq \chi_0$, то $T(\chi, \psi_0) = 0$;

в) если $\psi \neq \psi_0$, то $T(\chi_0, \psi) = 0$;

г) если $\chi \neq \chi_0$, $\psi \neq \psi_0$, то

$$|T(\chi, \psi)| = q^{1/2}.$$

5. Пусть ψ — нетривиальный аддитивный характер поля F_q, s — положительное целое, делящее $q-1$, и α — отличный от нуля элемент поля F_q.

В обозначениях задачи 4 доказать, что

$$\sum_{x\in F_q}\psi(\alpha x^s)=\sum_{\operatorname{ind}\chi=s}\overline{\chi}(\alpha)\,T(\chi,\psi).$$

Вывести отсюда справедливость оценки

$$\left|\sum_{x\in F_q}\psi(\alpha x^s)\right|\leqslant(s-1)\,q^{1/2}.$$

6. Пусть F_q — конечное поле характеристики $p>2$, ψ — нетривиальный аддитивный характер поля F_q и $a\neq 0$, b, c — элементы поля F_q. Доказать, что

$$\left|\sum_{x\in F_q}\psi(ax^2+bx+c)\right|=q^{1/2}.$$

7. Пусть $f(x_1,\ldots,x_n)$ — многочлен с коэффициентами из конечного поля F_q и ψ — нетривиальный аддитивный характер поля F_q. Доказать, что для числа N_q решений уравнения

$$f(x_1,\ldots,x_n)=0$$

в элементах поля F_q справедлива формула

$$N_q=\frac{1}{q}\sum_{\alpha\in F_q}\sum_{x_1,\ldots,x_n\in F_q}\psi(\alpha f(x_1,\ldots,x_n))=$$

$$=\frac{1}{q}\sum_{\psi}\sum_{x_1,\ldots,x_n\in F_q}\psi(f(x_1,\ldots,x_n))$$

8. Пусть $s_1,\ldots,s_n$ — положительные целые числа и $d_i=(s_i,\ q-1)$, $1\leqslant i\leqslant n$. Используя результаты задач 5 и 7, доказать, что для числа N_q решений уравнения

$$a_1x_1^{s_1}+\ldots+a_nx_n^{s_n}=0,\quad a_1,\ldots,a_n\in F_q^*,$$

в элементах конечного поля F_q справедливо неравенство

$$\left|N_q-q^{n-1}\right|\leqslant(d_1-1)\ldots(d_n-1)(q-1)\,q^{\frac{n}{2}-1}.$$

9. Пусть s — положительное целое, делящее $q-1$. Доказать, что для числа N_q решений уравнения

$$a_1x_1^s+\ldots+a_nx_n^s=0,\quad a_1,\ldots,a_n\in F_q^*,$$

в элементах поля F_q имеет место неравенство

$$\left|N_q-q^{n-1}\right|\leqslant\frac{s-1}{s}\left((s-1)^{n-1}-(-1)^{n-1}\right)(q-1)\,q^{\frac{n}{2}-1}.$$

10. Пусть $s_1,\ldots,s_n$ — положительные целые числа, а s_0 — их наименьшее общее кратное и $d_i=(s_i,\ q-1)$, $0\leqslant i\leqslant n$. Доказать, что для числа N_q решений уравнения

$$a_1x_1^{s_1}+\ldots+a_nx_n^{s_n}=a_0,\quad a_0,\ a_1,\ \ldots,\ a_n\in F_q^*,$$

в элементах конечного поля F_q справедливо неравенство

$$\left|N_q-q^{n-1}\right|\leqslant(d_0-1)(d_1-1)\ldots(d_n-1)\,q^{\frac{n-1}{2}}.$$

11. Пусть $f(x_1,\ldots,x_n)$ — невырожденная квадратичная форма определителя d над полем F_q нечетной характеристики p. Доказать, что число N_q решений уравнения

$$f(x_1,\ldots,x_n)=0$$

в элементах поля F_q выражается формулой

$$N_q=\begin{cases}q^{n-1}, & \text{если } n\equiv 1\pmod 2,\\ q^{n-1}+\left(\dfrac{(-1)^{\frac{n}{2}}d}{q}\right)(q-1)\,q^{\frac{n-2}{2}}, & \text{если } n\equiv 0\pmod 2.\end{cases}$$

Здесь $\left(\dfrac{\alpha}{q}\right)$ — символ, определенный в задаче 9 из § 2.

12. Пусть χ, ψ — нетривиальные мультипликативный и аддитивный характеры конечного поля F_q и

$$S_\nu=S_\nu(\chi,\psi)=\sum_{x\in F_{q^\nu}}\chi_\nu(x)\,\psi_\nu(x).$$

Используя результат теоремы 1, установить справедливость *соотношений Дэвенпорта — Хассе*

$$S_\nu=-(-S_1)^\nu.$$

13. Пусть χ — мультипликативный характер поля F_q порядка 2, ψ — нетривиальный аддитивный характер и $a,\ b\in F_q^*$. Доказать, что для *суммы Клостермана*

$$T(a,\ b)=\sum_{x\in F_q^*}\psi(ax+bx^{-1})$$

справедливо соотношение

$$T(a,\ b)=\sum_{x\in F_q}\chi(x^2-4ab)\,\psi(x).$$

14. Пусть ψ — нетривиальный аддитивный характер поля F_q, n — взаимно простое с q число, $g(x)=b_0x^n+b_1x^{n-1}+\ldots+b_{n-1}x$ — многочлен из кольца $F_q[x]$ степени n.

$$T_\nu=T_\nu(g)=\sum_{x\in F_{q^\nu}}\psi_\nu(g(x))$$

— *тригонометрическая сумма Г. Вейля* и

$$L(z,\ g)=\exp\left(\sum_{\nu=1}^{\infty}\frac{T_\nu}{\nu}z^\nu\right).$$

Доказать справедливость следующих утверждений:
а) L-функция Артина $L(z, g)$ имеет вид

$$L(z, g) = 1 + \beta_1 z + \ldots + \beta_{n-1} z^{n-1};$$

б) если $L(z, g) = \prod_{j=1}^{n-1} (1 - \omega_j z)$, то

$$T_\nu(g) = -\sum_{j=1}^{n-1} \omega_j^\nu;$$

в) справедливо равенство

$$|\beta_{n-1}| = q^{\frac{n-1}{2}}.$$

15. Пусть a, b — отличные от нуля элементы поля F_q, ψ — нетривиальный аддитивный характер поля F_q,

$$T_\nu = T_\nu(a, b) = \sum_{x \in F_{q^\nu}^*} \psi_\nu(ax + bx^{-1})$$

и

$$L(z, a, b) = \exp\left(\sum_{\nu=1}^{\infty} \frac{T_\nu}{\nu} z^\nu\right).$$

Доказать справедливость следующих утверждений:
а) L-функция Артина $L(z, a, b)$ имеет вид

$$L(z, a, b) = 1 + \beta_1 z + \beta_2 z^2;$$

б) если $L(z, a, b) = (1 - \omega_1 z)(1 - \omega_2 z)$, то

$$T_\nu(a, b) = -(\omega_1^\nu + \omega_2^\nu);$$

с) справедливо равенство $|\beta_2| = q$.

16. Пусть $f(x) = f_1^{s_1}(x) \ldots f_r^{s_r}(x)$ — разложение многочлена $f \in F_q[x]$ на неприводимые множители, s — положительное целое число, делящее $q - 1$, и $\deg(f_1 \ldots f_r) = m$. Далее, пусть χ — нетривиальный мультипликативный характер поля F_q показателя s, $(s, s_1, \ldots, s_r) = 1$ и

$$S_\nu = S_\nu(f) = \sum_{x \in F_{q^\nu}} \chi_\nu(f(x)).$$

Доказать справедливость следующих утверждений:
а) L-функция Артина

$$L(z, f) = \exp\left(\sum_{\nu=1}^{\infty} \frac{S_\nu}{\nu} z^\nu\right)$$

имеет вид

$$L(z, f) = 1 + \beta_1 z + \ldots + \beta_{m-1} z^{m-1};$$

б) если $L(z, f) = \prod_{j=1}^{m-1} (1 - \omega_j z)$, то

$$S_\nu(f) = -\sum_{j=1}^{m-1} \omega_j^\nu;$$

в) справедливо равенство

$$|\beta_{m-1}| = q^{\frac{(m-1)}{2}}.$$

§ 4. Суперэллиптическое уравнение и уравнение Артина — Шрейера

Суперэллиптическое уравнение

$$y^s = f(x), \quad f \in F_q[x], \tag{1}$$

и *уравнение Артина — Шрейера*

$$y^q - y = g(x), \quad g \in F_q[x], \tag{2}$$

играют особую роль в теории чисел. Это объясняется тем, что вопрос о числе N_{q^ν} решений уравнений (1) и (2) тесно связан с оценками сумм с мультипликативным характером

$$\sum_{x \in F_q} \chi(f(x)) \tag{3}$$

и сумм с аддитивным характером

$$\sum_{x \in F_q} \psi(g(x)), \tag{4}$$

имеющими многочисленные приложения в самых различных арифметических задачах. Некоторые из этих приложений будут рассмотрены в следующей главе.

1. Суперэллиптическое уравнение и суммы характеров. Обозначим l степень многочлена $f(x)$. При $s = 2$ уравнение (1) называется *гиперэллиптическим*, а при $s > 2$ — *суперэллиптическим*. В частном случае, когда $s = 2$, $l = 3$, 4 и многочлен $f(x)$ имеет различные корни, уравнение (1) называется *эллиптическим*.

Пусть $s' = (s, q - 1)$ и $s = s'r$. Поскольку число r взаимно просто с $q - 1$, то $z = y^r$ вместе с y пробегает все элементы поля F_q и, значит, число решений x, $y \in F_q$ уравнения (1) совпадает с числом решений x, $y \in F_q$ уравнения

$$z^{s'} = f(x),$$

в котором $s' | q - 1$. Поэтому с самого начала можно предполагать, что показатель s в уравнении (1) является делителем числа $q - 1$. В дальнейшем будем считать это условие выполненным.

Лемма 1. *Для количества N_{q^ν} решений уравнения* (1) *в элементах x, y поля F_{q^ν} справедлива формула*

$$N_{q^\nu} = \sum_{\operatorname{ind}\chi=s} \sum_{x\in F_{q^\nu}} \chi_\nu(f(x)) = \sum_{\operatorname{ind}\chi=s} \sum_{x\in F_{q^\nu}} \chi(\operatorname{norm}_\nu f(x)).$$

Доказательство. Пусть t — некоторый элемент поля F_{q^ν}. Для доказательства леммы достаточно установить, что число решений уравнения $y^s = t$ в элементах $y \in F_{q^\nu}$ равно величине

$$\sum_{\operatorname{ind}\chi=s} \chi_\nu(t) = \sum_{\operatorname{ind}\chi=s} \chi(\operatorname{norm}_\nu t).$$

Отображение $t \mapsto \operatorname{norm}_\nu t$ является гомоморфизмом группы $F^*_{q^\nu}$ на группу F^*_q. Ограничение этого отображения на подгруппу $(F^*_{q^\nu})^s$ задает гомоморфизм этой подгруппы на $(F^*_q)^s$. Далее, по лемме 4 из § 3 имеем

$$\sum_{\operatorname{ind}\chi=s} \chi(\operatorname{norm}_\nu t) = \begin{cases} s, & \text{если } \operatorname{norm}_\nu t \in (F^*_q)^s, \\ 0, & \text{если } \operatorname{norm}_\nu t \notin (F^*_q)^s \text{ и } \operatorname{norm}_\nu t \neq 0, \\ 1, & \text{если } \operatorname{norm}_\nu t = 0. \end{cases}$$

Сравним указанные значения суммы

$$\sum_{\operatorname{ind}\chi=s} \chi(\operatorname{norm}_\nu t)$$

с числом решений уравнения $y^s = t$. В первом случае $t \in (F^*_{q^\nu})^s$ и уравнение $y^s = t$ имеет s решений в элементах $y \in F_{q^\nu}$. Во втором случае $t \notin (F^*_{q^\nu})^s$, $t \neq 0$ и уравнение $y^s = t$ не разрешимо. В третьем случае $t = 0$ и уравнение $y^s = t$ имеет единственное решение $y = 0$.

Лемма 2. *Для количества N_{q^ν} решений уравнения* (2) *в элементах x, $y \in F_{q^\nu}$ справедлива формула*

$$N_{q^\nu} = \sum_{\psi} \sum_{x\in F_{q^\nu}} \psi_\nu(g(x)) = \sum_{\psi} \sum_{x\in F_{q^\nu}} \psi(\operatorname{tr}_\nu g(x)).$$

Доказательство. Пусть t — некоторый элемент поля F_{q^ν}. Для доказательства леммы достаточно установить, что число решений уравнения $y^q - y = t$ в элементах $y \in F_{q^\nu}$ равно величине

$$\sum_{\psi} \psi_\nu(t) = \sum_{\psi} \psi(\operatorname{tr}_\nu t).$$

Из теоремы 9 § 2 следует (с заменой F_p на F_q и F_q на F_{q^ν}), что уравнение $y^q - y = t$ разрешимо тогда и только тогда, когда $\operatorname{tr}_\nu t = 0$. При этом, наряду с решением y уравнение $y^q - y = t$

имеет по меньшей мере q решений $y + z$, $z \in F_q$, а поскольку степень многочлена $y^q - y = t$ равна q, то по теореме 5 из § 2 это уравнение, в случае его разрешимости, имеет ровно q решений. С другой стороны, по лемме 3 из § 3 имеем

$$\sum_{\psi} \psi(\operatorname{tr}_\nu t) = \begin{cases} q, & \text{если } \operatorname{tr}_\nu t = 0, \\ 0, & \text{если } \operatorname{tr}_\nu t \neq 0, \end{cases}$$

и лемма тем самым доказана.

2. Число F_q-рациональных точек на кривой $f(x, y) = 0$. Введем сначала важное для дальнейшего понятие абсолютно неприводимого многочлена.

Определение. Многочлен $f(x, y)$ с коэффициентами из поля F называется *абсолютно неприводимым*, если он неприводим над каждым алгебраическим расширением K поля F.

В § 2 гл. V докажем следующий общий результат:

Теорема А. *Пусть $f(x, y)$ — абсолютно неприводимый многочлен из кольца $F_q[x, y]$. Тогда для числа N_{q^ν} решений уравнения*

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

в элементах x, y поля F_{q^ν} справедлива оценка

$$\left| N_{q^\nu} - q^\nu \right| \leqslant c(f)\, q^{\nu/2}.$$

Из этой теоремы следует, что в случае абсолютно неприводимого многочлен $f(x, y)$ величины N_{q^ν} ведет себя приблизительно как q^ν. Покажем, что утверждение теоремы становится неверным, если $f(x, y)$ не является абсолютно неприводимым многочленом.

Пример. Пусть p — простое число вида $p = 8k + 3$ и $f(x, y) = y^2 - 2x^4 - 4x^2 - 2$ — многочлен с коэффициентами из поля F_p. Обозначим α корень в поле F_{p^2} многочлена $z^2 - 2$. Тогда в кольце $F_{p^2}[x, y]$ справедливо разложение

$$f(x, y) = (y - \alpha(x^2 + 1))\,(y + \alpha(x^2 + 1)).$$

Поскольку число 2 не является квадратичным вычетом по модулю p, то указанное разложение не имеет места в $F_p[x, y]$ и, следовательно, многочлен $f(x, y)$ — неприводим в кольце $F_p[x, y]$, но не является абсолютно неприводимым многочленом.

Уравнение $f(x, y) = 0$ разрешимо в элементах x, $y \in F_p$ тогда и только тогда, когда либо $y - \alpha(x^2 + 1) = 0$, либо $y + \alpha(x^2 + 1) = 0$. Отсюда, ввиду линейной независимости над полем F_p элементов 1 и α, получаем

$$y = 0, \quad x^2 + 1 = 0.$$

Но число -1 является квадратичным невычетом по модулю p и,

стало быть, уравнение $f(x, y)=0$ не разрешимо в элементах поля F_p.

Лемма 3. *Пусть $y^s - f(x)$ — многочлен с коэффициентами из поля F. Следующие условия эквивалентны между собой:*

1) *многочлен $y^s - f(x)$ абсолютно неприводим;*

2) *если $f = f_1^{s_1} \dots f_r^{s_r}$ — разложение многочлена $f(x)$ на неприводимые множители в кольце $F[x]$, то $(s, s_1, \dots, s_r)=1$.*

Доказательство. Пусть выполнено условие 1) и предположим, что $d=(s, s_1, \dots, s_r)>1$. Положим $g = f_1^{s_1/d} \dots f_r^{s_r/d}$. Приходим к разложению

$$y^s - f = y^s - g^d = \left(y^{\frac{s}{d}} - g\right)\left(y^{\frac{s(d-1)}{d}} + y^{\frac{s(d-2)}{d}} g + \dots + g^{d-1}\right),$$

противоречащему абсолютной неприводимости многочлена $y^s - f(x)$.

Пусть теперь выполнено условие 2) и предположим, что многочлен $y^s - f(x)$ приводим в кольце $\bar{F}[x, y]$. Положим $K=\bar{F}(x)$. Над алгебраическим замыканием $\bar{K}$ поля K справедливо разложение

$$y^s - f(x) = (y - y_1(x)) \dots (y - y_s(x)),$$

в котором элементы $y_i(x)$ имеют вид $y_i(x)=\zeta^i y(x)$, $1 \leqslant i \leqslant s$, где $y(x)$ — какой-либо корень многочлена $y^s - f(x)$ в поле $\bar{K}$, а ζ — примитивный корень степени s из 1. Из приводимости многочлена $y^s - f(x)$ в кольце $\bar{F}[x, y]$ следует, что для некоторых $i_1, \dots, i_t$, где $t < s$, произведение

$$(y - \zeta^{i_1} y(x)) \dots (y - \zeta^{i_t} y(x))$$

является элементом этого кольца. Свободный член рассматриваемого произведения

$$(-1)^t \zeta^{i_1 + \dots + i_t} y^t(x)$$

принадлежит $\bar{F}[x]$ и, значит, $y^t(x) \in \bar{F}[x]$. Обозначим μ наименьшее положительное целое число, для которого $y^\mu(x) \in \bar{F}[x]$. Тогда число s кратно μ, а так как $y^t(x) \in \bar{F}[x]$ и $t < s$, то $\mu < s$.

Положим $y^\mu(x)=g(x)$. Мы имеем $y^s(x)=f(x)$ и тогда $g^{s/\mu}=f$. Из однозначности разложения $f = f_1^{s_1} \dots f_r^{s_r}$ многочлена f на неприводимые множители следует, что все s_i, $1 \leqslant i \leqslant r$, делятся на $d=s/\mu$, а поскольку $d>1$, то получаем, что $(s, s_1, \dots, s_r)>1$. Но это противоречит условию 2) и, тем самым, лемма доказана.

Следствие. *Пусть $l=\deg f(x)$. Если $(l, s)=1$, то многочлен $y^s - f(x)$ абсолютно неприводим.*

Лемма 4. Пусть

$$f(x, y) = f_0 y^s + f_1(x) y^{s-1} + \dots + f_s(x)$$

— многочлен с коэффициентами из поля F, где f_0 — ненулевая константа, и

$$\nu(f) = \max_{1 \leqslant i \leqslant s} \frac{\deg f_i(x)}{i}.$$

Если $\nu(f)=l/s$, где $(l, s)=1$, то многочлен $f(x, y)$ абсолютно неприводим.

Доказательство. Покажем сначала, что если $f(x, y) = g(x, y)h(x, y)$, то $\nu(f)=\max(\nu(g), \nu(h))$.

Пусть

$$g(x, y) = g_0 y^m + g_1(x) y^{m-1} + \dots + g_m(x)$$

и

$$h(x, y) = h_0 y^n + h_1(x) y^{n-1} + \dots + h_n(x).$$

Тогда

$$f_i(x) = \sum_{j+k=i} g_j(x) h_k(x), \quad 1 \leqslant i \leqslant s,$$

причем степень каждого слагаемого $g_j h_k$ не выше

$$j\nu(g) + k\nu(h) \leqslant (j+k)\max(\nu(g), \nu(h)) = i\max(\nu(g), \nu(h)).$$

Следовательно,

$$\frac{\deg f_i(x)}{i} \leqslant \max(\nu(g), \nu(h)), \quad 1 \leqslant i \leqslant s,$$

и, стало быть,

$$\nu(f) \leqslant \max(\nu(g), \nu(h)).$$

Положим для краткости $\nu=\nu(f)$ и сделаем замену переменного $y \mapsto y^\nu$.

Имеем

$$f(x, y^\nu) = f_0 y^{\nu s} + f_1(x) y^{\nu(s-1)} + \dots + f_s(x) =$$
$$= (g_0 y^{\nu m} + g_1(x) y^{\nu(m-1)} + \dots + g_m(x))(h_0 y^{\nu n} + h_1(x) y^{\nu(n-1)} + \dots$$
$$\dots + h_n(x)) = g(x, y^\nu) h(x, y^\nu),$$

причем

$$\deg f(x, y^\nu) = \nu s$$

и

$$\deg g(x, y^\nu) \geqslant \nu m, \quad \deg h(x, y^\nu) \geqslant \nu n.$$

Стало быть,

$$\deg g(x, y^\nu) = \nu m, \quad \deg h(x, y^\nu) = \nu n$$

и тогда

$$\deg g_j(x) \leqslant \nu j, \quad \deg h_k(x) \leqslant \nu k.$$

Следовательно,

$$\nu(g) \leqslant \nu, \quad \nu(h) \leqslant \nu$$

и, значит, $\nu=\nu(f)=\max(\nu(g), \nu(h))$.

Для доказательства леммы предположим, что многочлен $f(x, y)$ абсолютно приводим и что $f(x, y)=g(x, y)h(x, y)$ — его собственное разложение на множители $g(x, y)$ и $h(x, y)$, где $\deg_y g(x, y)=m<s$ и $\deg_y h(x, y)=n<s$. Имеем

$$\nu(g)=\max_{1\leqslant j\leqslant m}\frac{\deg g_j(x)}{j}=\frac{r}{m'},\quad 1\leqslant m'<s,$$

$$\nu(h)=\max_{1\leqslant k\leqslant n}\frac{\deg h_k(x)}{k}=\frac{t}{n'},\quad 1\leqslant n'<s,$$

и, в таком случае, $\nu(f)\neq\max(\nu(g), \nu(h))$, что противоречит равенству $\nu(f)=\max(\nu(g), \nu(h))$. Полученное противоречие доказывает лемму 4.

Следствие. *Пусть* $n=\deg g(x)$. *Если* $(n, q)=1$, *то многочлен* $y^q-y-g(x)$ *абсолютно неприводим.*

3. Оценка сумм характеров с многочленом. Воспользуемся теперь результатом теоремы A для получения оценок сумм (3) и (4).

Теорема 1. *Пусть* $f(x)$ — *многочлен с коэффициентами из поля* F_q, $f=f_1^{s_1}\dots f^{s_r}$ — *его разложение на неприводимые множители в кольце* $F_q^r[x]$ *и* $m=\deg(f_1\dots f_r)$. *Пусть, далее,* χ — *нетривиальный мультипликативный характер поля* F_q *показателя* s *и* $(s, s_1, \dots, s_r)=1$. *Тогда при всех* $\nu\geqslant 1$ *справедлива оценка*

$$\left|\sum_{x\in F_{q^\nu}}\chi_\nu(f(x))\right|\leqslant(m-1)q^{\nu/2}.$$

Доказательство. Из условий теоремы следует, ввиду леммы 3, что многочлен $y^s-f(x)$ абсолютно неприводим, а тогда, по теореме A, для количества N_{q^ν} решений уравнения $y^s=f(x)$ в элементах x, y поля F_{q^ν} справедлива оценка

$$\left|N_{q^\nu}-q^\nu\right|\leqslant cq^{\nu/2}$$

с некоторой константой c, зависящей от многочлена $y^s-f(x)$. По лемме 1 имеем

$$N_{q^\nu}=q^\nu+\sum_{\substack{\chi\neq\chi_0\\ \operatorname{ind}\chi=s}}\sum\chi_\nu(f(x))$$

и, стало быть,

$$\left|\sum_{\substack{\chi\neq\chi_0\\ \operatorname{ind}\chi=s}}\sum_{x\in F_{q^\nu}}\chi_\nu(f(x))\right|\leqslant cq^{\nu/2}.$$

Далее, по теореме 1 из § 3

$$\sum_{x\in F_{q^\nu}}\chi_\nu(f(x))=-\sum_{j=1}^{m-1}\omega_j^\nu(\chi)$$

и тогда

$$\left|\sum_{\substack{\chi\neq\chi_0\\ \operatorname{ind}\chi=s}}\sum_{j=1}^{m-1}\omega_j^\nu(\chi)\right|\leqslant cq^{\nu/2}$$

для всех $\nu\geqslant 1$. Отсюда, ввиду теоремы 2 того же параграфа $|\omega_j(\chi)|\leqslant q^{1/2}$ для всех рассматриваемых нами j, χ и, следовательно,

$$\left|\sum_{x\in F_{q^\nu}}\chi_\nu(f(x))\right|\leqslant(m-1)q^{\nu/2}.$$

Теорема доказана.

Поскольку имеется $s-1$ нетривиальных характеров χ показателя s, из теоремы 1 мы получаем следующий результат.

Следствие. *Если* $f=f_1^{s_1}\dots f_r^{s_r}$, $\deg(f_1\dots f_r)=m$ *и* $y^s-f(x)$ — *абсолютно неприводимый многочлен из кольца* $F_q[x, y]$, *то для числа* N_{q^ν} *решений уравнения* (1) *в элементах* x, y *поля* F_{q^ν} *справедливо неравенство*

$$\left|N_{q^\nu}-q^\nu\right|\leqslant(s-1)(m-1)q^{\nu/2}.$$

Теорема 2. *Пусть* $g(x)=b_0x^n+b_1x^{n-1}+\dots+b_{n-1}x$ — *многочлен из кольца* $F_q[x]$ *степени* n, *взаимно простой с* q, *и* ψ — *нетривиальный аддитивный характер поля* F_q. *Тогда при любом* $\nu\geqslant 1$ *справедлива оценка*

$$\left|\sum_{x\in F_{q^\nu}}\psi_\nu(g(x))\right|\leqslant(n-1)q^{\nu/2}.$$

Доказательство вполне аналогично доказательству теоремы 1. Поскольку $(n, q)=1$, то по следствию из леммы 4 многочлен $y^q-y-g(x)$ абсолютно неприводим, а тогда, по теореме A, для числа N_{q^ν} решений уравнения $y^q-y=g(x)$ в элементах x, y поля F_{q^ν} справедлива оценка

$$\left|N_{q^\nu}-q^\nu\right|\leqslant c'q^{\nu/2}.$$

По лемме 2 имеем

$$N_{q^\nu}=q^\nu+\sum_{\psi\neq\psi_0}\sum_{x\in F_{q^\nu}}\psi_\nu(g(x))$$

и, значит,

$$\left|\sum_{\psi\neq\psi_0}\sum_{x\in F_{q^\nu}}\psi_\nu(g(x))\right|\leqslant c'q^{\nu/2}.$$

Далее, по теореме 1 из § 3

$$\sum_{x\in F_{q^\nu}}\psi_\nu(g(x))=-\sum_{j=1}^{n-1}\omega_j^\nu(\psi)$$

и тогда

$$\left|\sum_{\psi\neq\psi_0}\sum_{j=1}^{n-1}\omega_j^{\nu}(\psi)\right|\leqslant c'q^{\nu/2}$$

для всех $\nu\geqslant 1$. Отсюда, ввиду теоремы 2 из того же параграфа,

$$|\omega_j(\psi)|\leqslant q^{1/2}$$

для всех рассматриваемых j, ψ и, стало быть,

$$\left|\sum_{x\in F_{q^\nu}}\psi_\nu(g(x))\right|\leqslant(n-1)q^{\nu/2}.$$

Следствие. *Если степень n многочлена $g(x)=b_0x^n+b_1x^{n-1}+\ldots+b_{n-1}x$ из кольца $F_q[x]$ взаимно проста с q, то для числа N_{q^ν} решений уравнения (2) в элементах x, y поля F_{q^ν} справедлива оценка*

$$\left|N_{q^\nu}-q^\nu\right|\leqslant(n-1)(q-1)q^{\nu/2}.$$

Задачи

1* (Морделл [89c]). Пусть p — нечетное простое число, $g(x)=b_0x^n+b_1x^{n-1}+\ldots+b_{n-1}x$ — многочлен из кольца $F_p[x]$ степени не выше n и

$$S(b_0,\ldots,b_{n-1})=\sum_{x=0}^{p-1}e^{2\pi i\frac{g(x)}{p}},\quad i=\sqrt{-1}.$$

Установить следующие свойства сумм $S(b_0,\ldots,b_{n-1})$:

а) справедлива оценка

$$\sum_{b_0,\ldots,b_{n-1}=0}^{p-1}|S(b_0,\ldots,b_{n-1})|^{2n}\leqslant cp^{2n};$$

б) если $\lambda\in F_p^*$ и $\mu\in F_p$, то

$$\sum_{x=0}^{p-1}e^{2\pi i\frac{g(x)}{p}}=\sum_{x=0}^{p-1}e^{2\pi i\frac{g(\lambda x+\mu)}{p}};$$

в) если λ пробегает все элементы из F_p^* и μ пробегает все элементы поля F_p, то многочлен $g(x)$ степени n порождает по меньшей мере $\frac{p(p-1)}{n}$ различных многочленов

$$g(\lambda x+\mu)=b_0'x^n+b_1'x^{n-1}+\ldots+b_{n-1}'x+b_n';$$

г) если $g(x)$ — многочлен степени $n\geqslant 1$ из кольца $F_p[x]$, то справедлива оценка

$$\left|\sum_{x=0}^{p-1}e^{2\pi i\frac{g(x)}{p}}\right|\leqslant c(n)\,p^{1-\frac{1}{n}}.$$

2* (Дэвенпорт [48a]). Пусть p — нечетное простое число, $\alpha_1,\ldots,\alpha_n$ — различные элементы поля F_p и

$$T(\alpha_1,\ldots,\alpha_n)=\sum_{x=0}^{p-1}\left(\frac{(x+\alpha_1)\ldots(x+\alpha_n)}{p}\right).$$

Установить справедливость следующих свойств сумм $T(\alpha_1,\ldots,\alpha_n)$ при $n=3,4$:

а) имеет место соотношение

$$T(\alpha_1,\alpha_2,\alpha_3,\alpha_4)=-1+\left(\frac{a}{p}\right)T(0,1,b),$$

где

$$a=-(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)$$

и

$$b=\frac{(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)}{(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)};$$

б) справедливо равенство

$$\sum_{b=0}^{p-1}T^2(0,1,b)=p^2-2p-1;$$

в) имеет место соотношение

$$T^2(0,1,b)=p+\sum_{z=1}^{p-1}T\left(0,1,\frac{(z-b)^2}{z(1-b)^2}\right).$$

(Указание. В сумме

$$T^2(0,1,b)=\sum_{x,y=1}^{p-1}\left(\frac{x(x+1)(x+b)\,y(y+1)(y+b)}{p}\right)$$

положить $z=xy$ и воспользоваться соотношением а));

г) справедлива оценка

$$|T(0,1,b)|\leqslant cp^{3/4}.$$

(Указание. Применить к сумме

$$\sum_{z=1}^{p-1}T\left(0,1,\frac{(z-b)^2}{z(1-b)}\right)$$

неравенство Коши и воспользоваться равенством б)).

3. Пусть F — поле характеристики $p>0$, $D=\frac{d}{dx}$ — оператор дифференцирования в кольце $F[x]$, действующий на элементы $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ по правилу

$$Df(x)=na_0x^{n-1}+(n-1)a_1x^{n-2}+\ldots+a_{n-1},$$

и N — положительное целое число, меньшее p. Доказать, что если

$$f(\alpha)=Df(\alpha)=\ldots=D^Nf(\alpha)=0,$$

то элемент $\alpha\in F$ является по меньшей мере $(N+1)$-кратным корнем многочлена $f(x)$, т. е. $(x-\alpha)^{N+1}$ делит в кольце $F[x]$ многочлен $f(x)$.

4. Пусть F_q — конечное поле характеристики $p > 2$ и $f(x)$ — отличный от нуля многочлен из кольца $F_q[x]$. Доказать, что все решения $x \in F_q$ уравнения

$$1 \pm f^{\frac{q-1}{2}}(x) = 0$$

являются по меньшей мере двукратными корнями многочлена

$$R(x) = 2f(x)\left(1 \pm f^{\frac{q-1}{2}}(x)\right) + (Df(x))(x^q - x).$$

Вывести отсюда, что для числа N_q решений эллиптического уравнения

$$y^2 = x^3 + ax + b, \quad a, b \in F_q,$$

в элементах $x, y \in F_q$ справедлива оценка

$$|N_q - q| \leqslant \frac{q+3}{2}.$$

5* (А. Г. Постников). Пусть F_q — конечное поле характеристики $p > 2$ и $ax^2 + bx + c$ — многочлен степени 2 из кольца $F_q[x]$ с отличным от нуля дискриминантом $d = b^2 - 4ac$. Используя задачу 4, доказать, что для числа N_q решений уравнения

$$y^2 = ax^2 + bx + c$$

в элементах x, y поля F_q имеет место формула

$$N_q = q - \left(\frac{a}{q}\right),$$

где $\left(\frac{a}{q}\right)$ — символ поля F_q, определенный в задаче 9 из § 2.

6* (С. А. Степанов [117b]). Пусть $l \geqslant 3$ — нечетное число, $p > 9l^2$ — простое число и $N \leqslant \left(\frac{p}{3l}\right)^{1/2}$ — положительное целое число. Пусть, далее, $f(x)$ — бесквадратный многочлен степени l из кольца $F_p[x]$ и $D = 2\frac{d}{dx}$ — оператора дифференцирования в поле $F_p(x)$. Доказать справедливость следующих утверждений:

а) если рациональные функции

$$H_k^{(j)} \in F_p(x), \quad 1 \leqslant k \leqslant j, \quad j = 1, 2, \ldots,$$

задаются рекуррентными соотношениями

$$H_k^{(j)} = DH_k^{(j-1)} + 2(k-1)H_{k-1}^{(j-1)} + f^{-1}H_k^{(j-1)}\frac{df}{dx}, \quad 1 \leqslant k < j,$$

$$H_j^{(j)} = 2^{j-1}j!f^{-1}\frac{df}{dx},$$

то они представимы в виде

$$H_k^{(j)} = \frac{P_k^{(j)}}{f^{j-k+1}},$$

где $P_k^{(j)}$ — многочлены из кольца $F_p[x]$ степени не выше $(l-1)(j-k+1)$;

б) если рациональные функции $r_j^{(i)}(x)$, $t_j^{(i)}(x)$ задаются в поле $F_p(x)$ рекуррентными соотношениями

$$r_j^{(i)} = Dr_j^{(i-1)} - 2jr_{j+1}^{(i-1)} - f^{-1}r_j^{(i-1)}\frac{df}{dx},$$

$$t_j^{(i)} = Dt_j^{(i-1)} - 2(j+1)t_{j+1}^{(i-1)} + f^{-1}r_{j+1}^{(i-1)}\frac{df}{dx}$$

с начальными значениями $r_j^{(0)}$, $t_j^{(0)}$, $j = 1, 2, \ldots$, такими, что $r_j^{(0)} = t_j^{(0)} = 0$ при $j > 2N$, и если

$$R_i^*(x) = \left(1 \pm f^{\frac{p-1}{2}}(x)\right)\sum_{j=1}^{2N} r_j^{(i)}(x)(x^p - x)^{j-1} + \sum_{j=1}^{2N} t_j^{(i)}(x)(x^p - x)^j, \quad i \geqslant 0,$$

то для выполнимости равенств

$$D^s R_i(x) = R_{i+s}^*(x), \quad 1 \leqslant s \leqslant \tau,$$

достаточно выполнимости соотношений

$$2^j j! t_j^{(i)} = \sum_{k=1}^{j} H_k^{(j)} r_k^{(i)}, \quad 1 \leqslant j \leqslant \tau.$$

(Указание. Использовать индукцию по τ);

в) если $r_j^{(i)}$, $t_j^{(i)}$, $1 \leqslant j \leqslant 2N$, многочлены из кольца $F_p[x]$ степени не выше $\frac{p-l}{2} - 1$, среди которых хотя бы один отличен от нуля, то $R_i^*(x)$ — отличный от нуля многочлен из $F_p[x]$;

г) существует отличный от нулевого набор многочленов $r_j^{(0)}$, $t_j^{(0)} \in F_p[x]$ степени не выше $N(N+1)l$, при котором полином

$$R_0(x) = \left(1 \pm f^{\frac{p-1}{2}}(x)\right)\sum_{j=1}^{N} r_j^{(0)}(x)(x^p - x)^{j-1} + \sum_{j=1}^{N} t_j^{(0)}(x)(x^p - x)^j$$

обладает тем свойством, что

$$R_0(x) = DR_0(x) = \ldots = D^{2N-1}R_0(x) = 0$$

для всех решений $x \in F_p$ уравнения

$$1 \pm f^{\frac{p-1}{2}}(x) = 0.$$

(Указание. Для нахождения $r_j^{(0)}$, $t_j^{(0)}$ воспользоваться методом неопределенных коэффициентов, а также утверждением б) с $i = 0$, $\tau = 2N - 1$ и утверждением а));

д) многочлен $R_0(x)$ отличен от нуля, его степень не превосходит величины

$$Np + \frac{l(p-1)}{2} + N(N+1)l$$

и $R_0(x)$ имеет своими корнями кратности по меньшей мере $2N$ все решения $x \in F_p$ уравнения $1 \pm f^{\frac{p-1}{2}}(x) = 0$.

(Указание. Для доказательства того, что $R_0(x) \not\equiv 0$ воспользоваться утверждением в));

е) число N_p решений гиперэллиптического уравнения

$$y^2 = f(x)$$

в элементах x, y поля F_p удовлетворяет неравенству

$$|N_p - p| \leqslant 2l^{3/2}p^{1/2}.$$

(Указание. Взять $N = \left[\left(\frac{p}{3l}\right)^{1/2}\right]$ и сравнить, используя теорему Лагранжа, число корней многочлена $R_0(x)$, взятых с их кратностями, со степенью $R_0(x)$).

7. Пусть F — поле и $D = \frac{d}{dx}$ — оператор дифференцирования в кольце $F[x]$. Определим *гиперпроизводную* D_i (Хассе [133a], Тейхмюллер [121]) порядка $i \geqslant 0$ от многочлена $f \in F[x]$ равенством

$$D_i f(x) = \frac{D^i f(x)}{i!}.$$

Доказать следующие свойства гиперпроизводной D_i:

а) $D_i(f \pm g) = D_i f \pm D_i g$;

б) $D_i(\alpha f) = \alpha D_i f$, $\alpha \in F$;

в) $D_i(f_1 \dots f_s) = \sum_{i_1+\dots+i_s=i} (D_{i_1} f_1) \dots (D_{i_s} f_s)$;

г) $D_i (x-\alpha)^h = \binom{k}{i} (x-\alpha)^{k-i}$;

д) если F — поле характеристики $p \geqslant 0$, $\alpha \in F$ и

$$f(\alpha) = D_1 f(\alpha) = \dots = D_N f(\alpha) = 0,$$

то элемент α является по меньшей мере $(N+1)$-кратным корнем многочлена $f(x)$.

8. Пусть F_q — конечное поле характеристики $p > 2$. Обобщая критерий Эйлера из § 1, доказать, что уравнение

$$y^s = a, \quad a \in F_q^*,$$

разрешимо тогда и только тогда, когда $a^{\frac{q-1}{d}} = 1$, где $d = (s, q-1)$. Показать, что в случае разрешимости уравнение имеет d различных решений.

Доказать, что уравнение $y^s = a$ не разрешимо в том и только в том случае, когда

$$1 + a^{\frac{q-1}{d}} + \dots + a^{\frac{(d-1)(q-1)}{d}} = 0.$$

9* (С. А. Степанов [117e]). Пусть F_q — конечное поле характеристики $p > 2$ и $f(x)$ — бесквадратный многочлен нечетной степени $l < \left(\frac{q}{9}\right)^{1/2}$ из кольца $F_q[x]$.

а) Расширить конструкцию задачи 6 и, используя гиперпроизводные D_i, $1 \leqslant i \leqslant N \leqslant \left(\frac{q}{3l}\right)^{1/2}$, построить отличный от нуля в $F_q[x]$ многочлен

$$R_0(x) = \left(1 \pm f^{\frac{q-1}{2}}(x)\right) \sum_{j=1}^{N} r_j^{(0)}(x) (x^q - x)^{j-1} + \sum_{j=1}^{N} t_j^{(0)}(x) (x^q - x)^j$$

степени не выше

$$Nq + \frac{l(q-1)}{2} + N(N+1)l,$$

имеющий своими корнями кратности по меньшей мере $2N$ все решения $x \in F_q$ уравнения $1 \pm f^{\frac{q-1}{2}}(x) = 0$.

б) Взяв $N = \left[\left(\frac{q}{3l}\right)^{1/2}\right]$ и сравнив число корней многочлена $R_0(x)$ с его степенью, получить для числа N_q решений гиперэллиптического уравнения

$$y^2 = f(x)$$

в элементах x, y поля F_q оценку

$$|N_q - q| \leqslant 2l^{3/2}q^{1/2}.$$

в) Вывести отсюда оценку

$$\left| \sum_{x \in F_q} \left(\frac{f(x)}{q}\right) \right| \leqslant (l-1) q^{1/2},$$

где $\left(\frac{a}{q}\right)$ — обобщенный символ Лежандра из задачи 9 § 2.

10* (С. А. Степанов [117c], В. М. Шмидт [146h]). Пусть l, s — взаимно простые положительные целые числа, F_q — конечное поле из $q > 100sl^2$ элементов, $s \mid q-1$, f — многочлен из кольца $F_q[x]$ степени l и $g = f^{\frac{q-1}{s}}$. Доказать справедливость следующих утверждений:

а) если $R_{i,0}(x)$ — многочлен вида

$$R_{i,0} = \sum_{j=0}^{N} r_{i,j}^{(0)}(x) x^{qj},$$

где $\deg r_{i,j}^{(0)}(x) \leqslant \frac{q}{s} - l$, то из равенства

$$\sum_{i=0}^{s-1} g^i(x) R_{i,0}(x) = 0$$

следует, что $r_{i,j}^{(0)}(x) = 0$ для всех $0 \leqslant i \leqslant s-1$, $0 \leqslant j \leqslant N$;

б) если $h(z)$ — многочлен степени τ, $1 \leqslant \tau \leqslant s-1$, A — множество элементов $x \in F_q$, для которых либо $f(x) = 0$, либо $h(g(x)) = 0$ и $N \geqslant l+1$ — целое число с условием

$$(N+3)^2 \leqslant \frac{2q}{s},$$

то существует ненулевой набор многочленов $r_{i,j}^{(0)} \in F_q[x]$ степени не выше $\frac{q}{s} - l$, при котором полином

$$R_0(x) = f^N(x) \sum_{i=0}^{s-1} \sum_{j=0}^{N'} r_{i,j}^{(0)}(x) g^i(x) x^{qj},$$

$N' = \left[\frac{\tau}{s}(N + l + 1)\right]$, обладает тем свойством, что

$$R_0(x) = D_1R_0(x) = \ldots = D_{N-1}R_1(x) = 0$$

для всех $x \in A$.

(Указание. Воспользоваться методом неопределенных коэффициентов);

в) многочлен $R_0(x)$ отличен от нуля и его степень не превосходит величины

$$\frac{\tau}{s} qN + 4lq;$$

г) для числа N_q решений уравнения

$$y^s = f(x)$$

в элементах x, y поля F_q справедлива оценка

$$N_q \leqslant q + 4ls^{2/2}q^{1/2}.$$

(Указание. Положить $N = \left[\left(\frac{2q}{s}\right)^{1/2}\right] - 3$, $h(z) = z - 1$ и сравнить число корней многочлена $R_0(x)$, взятых с их кратностями, со степенью $R_0(x)$.);

д) для величины N_q справедлива оценка

$$N_q \geqslant q - 4ls^{3/2}q^{1/2}.$$

(Указание. Положить $N = \left[\left(\frac{2q}{s}\right)^{1/2}\right] - 3$, $h(z) = 1 + z + \ldots + z^{s-1}$ и сравнить число корней многочлена $R_0(x)$ с его степенью.);

е) если $f = f_1^{s_1} \ldots f_r^{s_r}$ — разложение многочлена f на неприводимые множители в кольце $F_q[x]$, $\deg(f_1 \ldots f_r) = m$ и χ — нетривиальный мультипликативный характер поля F_q показателя s, то справедлива оценка

$$\left| \sum_{x \in F_q} \chi(f(x)) \right| \leqslant (m-1)\, q^{1/2}.$$

11. Пусть $g(x) = b_0x^n + b_1x^{n-1} + \ldots + b_{n-1}x$ — ненулевой многочлен из кольца $F_q[x]$ и α — некоторый элемент поля F_q. Пусть, далее $\widetilde{N}_\alpha$ — число решений уравнения

$$\mathrm{tr}_\nu g(x) = \alpha$$

в элементах $x \in F_{q^\nu}$. Доказать справедливость следующих утверждений:

а) имеет место равенство

$$\sum_{\alpha \in F_q} \widetilde{N}_\alpha = q^\nu;$$

б) справедливо соотношение $N_{q^\nu} = q\widetilde{N}_0$, где N_{q^ν} — число решений в элементах $x, y \in F_{q^\nu}$ уравнения $y^q - y = g(x)$.

12* (С. А. Степанов [117d], В. М. Шмидт [146h]). Пусть $\nu \geqslant 3$, $k = \left[\frac{\nu}{2}\right]$, N — кратное q число с условием $0 < N \leqslant q^{\nu-k-1}$, $g(x) = b_0x^n + b_1x^{n-1} + \ldots + b_{n-1}x$ — многочлен из кольца $F_q[x]$ степени $n < q$, взаимно простой с q, и

$$h(x) = g^{q^k}(x) + g^{q^{k+1}}(x) + \ldots + g^{q^{\nu-1}}(x).$$

В обозначениях предыдущей задачи доказать справедливость следующих утверждений:

а) Существует отличный от нуля многочлен

$$R_{0,\alpha}(x) = \sum_{i=0}^{q-1} \sum_{j=0}^{N/q} r_{i,j,\alpha}^{(0)}(x)\, h^i(x)\, x^{jq^\nu}$$

из кольца $F_q[x]$ степени не выше

$$Nq^{\nu-1} + q^{\nu+1},$$

обладающий свойством, что каждое решение $x \in F_{q^\nu}$ уравнения

$$\mathrm{tr}_\nu g(x) = \alpha$$

является его корнем кратности по меньшей мере N.

(Указание. Воспользоваться методом неопределенных коэффициентов, рассматривая в качестве таковых многочлены $r_{i,j,\alpha}^{(0)}(x)$, а также критерием кратности корня многочлена из задачи 7);

б) Для величины $\widetilde{N}_\alpha$ справедливо неравенство

$$\widetilde{N}_\alpha \leqslant q^{\nu-1} + q^{k+2}.$$

(Указание. Взять $N = q^{\nu-k+1}$ и сравнить число корней многочлена $R_{0,\alpha}(x)$ с его степенью.)

в) Справедливо неравенство

$$\widetilde{N}_\alpha > q^{\nu-1} - q^{k+3}.$$

(Указание. Воспользоваться соотношением из п. а) предыдущей задачи.)

г) Имеет место неравенство

$$\left| N_{q^\nu} - q^\nu \right| < q^{\left[\frac{\nu}{2}\right]+4};$$

д) Справедливы оценки

$$\left| \sum_{x \in F_{q^\nu}} \psi_\nu(g(x)) \right| \leqslant (n-1)\, q^{\nu/2}, \quad \psi \neq \psi_0,$$

и

$$\left| N_{q^\nu} - q^\nu \right| \leqslant (n-1)(q-1)\, q^{\nu/2}.$$

13. Пусть $\theta_1, \ldots, \theta_n$ — действительные числа. Используя принцип «ящиков Дирихле», установить существование целочисленного набора $(p_1, \ldots, p_n, q)$ с произвольно большим $q > 0$, удовлетворяющего системе неравенств

$$\left| \theta_j - \frac{p_j}{q} \right| < q^{-\left(1+\frac{1}{n}\right)}, \quad 1 \leqslant j \leqslant n.$$

(Указание. Рассмотреть $t^n + 1$ n-мерных точек $(\{s\theta_1\}, \ldots, \{s\theta_n\})$, $s = 0, 1, \ldots, t^n$, где $\{\alpha\}$ — дробная доля числа α, и t^n полуоткрытых кубиков

$$\frac{\nu_1}{t} \leqslant x_1 < \frac{\nu_1 + 1}{t}, \ \ldots, \ \frac{\nu_n}{t} \leqslant x_n < \frac{\nu_n + 1}{t},$$

где $\nu_1, \ldots, \nu_n = 0, 1, \ldots, t-1$.)

14. Пусть $\omega_1, \ldots, \omega_r$ — ненулевые комплексные числа. Используя результат предыдущей задачи, доказать существование бесконечной последовательности положительных целых ν, для которых

$$\operatorname{Re}\left(\omega_1^\nu + \ldots + \omega_r^\nu\right) > \left(1 - \frac{2\pi}{\nu^{1/r}}\right)\left(|\omega_1|^\nu + \ldots + |\omega_r|^\nu\right).$$

15. Пусть ψ — нетривиальный аддитивный характер конечного поля F_q, n — взаимно простое с q число и $g(x) = b_0x^n + b_1x^{n-1} + \ldots + b_{n-1}x$ — многочлен из кольца $F_q[x]$ степени n. Используя результаты предыдущей задачи и задачи 14 из § 3, доказать существование бесконечной последовательности положительных целых ν, для которых выполняется неравенство

$$\left|\sum_{x \in F_q\nu} \psi_\nu(g(x))\right| > (n-1)\, q^{\nu/2}\left(1 - \frac{2\pi}{\nu^{\frac{1}{n-1}}}\right).$$

16. Пусть $f = f_1^{s_1} \ldots f_r^{s_r}$ — разложение многочлена $f \in F_q[x]$ на неприводимые множители и пусть $\deg(f_1 \ldots f_r) = m$. Далее, пусть χ — нетривиальный мультипликативный характер поля F_q показателя s и пусть $(s, s_1, \ldots, s_r) = 1$. Используя результаты задачи 14 и задачи 16 из § 3, доказать существование бесконечной последовательности положительных целых ν, для которых выполняется неравенство

$$\left|\sum_{x \in F_q\nu} \chi_\nu(f(x))\right| > (m-1)\, q^{\nu/2}\left(1 - \frac{2\pi}{\nu^{\frac{1}{m-1}}}\right).$$

17. Пусть a, b — отличные от нуля элементы поля F_q и ψ — нетривиальный аддитивный характер этого поля.

а) Установить абсолютную неприводимость многочлена

$$ax^2 - (y^2 - y)x + b.$$

б) Используя теорему А и результаты задачи 15 из § 4, вывести для суммы Клостермана оценку

$$\left|\sum_{x \in F_q^*\nu} \psi_\nu(ax + bx^{-1})\right| \leqslant 2q^{\nu/2}.$$

ГЛАВА II

РАСПРЕДЕЛЕНИЕ КВАДРАТИЧНЫХ ВЫЧЕТОВ И НЕВЫЧЕТОВ

§ 1. Результаты И. М. Виноградова и Д. Берджесса

1. Теорема Виноградова — Полиа. Пусть $f(x, y)$ — многочлен с целыми коэффициентами и p — простое число. Если многочлен f, рассматриваемый как элемент кольца $F_p[x, y]$, абсолютно неприводим, то из теоремы A § 4 гл. I следует, что для числа N_p решений сравнения

$$f(x, y) \equiv 0 \pmod p \tag{1}$$

справедлива асимптотическая формула

$$N_p = p + O(p^{1/2}).$$

Отсюда следует, что при всех достаточно больших p сравнение (1) разрешимо в элементах x, y полной системы вычетов $0, 1, \ldots, p-1$ по модулю p.

Для многих задач теории чисел важен вопрос о разрешимости сравнения (1) на неполной системе вычетов, когда переменные x, y пробегают некоторые подмножества множества $\{0, 1, \ldots, p-1\}$. Первые общие результаты в указанном вопросе были получены И. М. Виноградовым [27а] и Г. Полиа [97а] при изучении закона распределения квадратичных вычетов и невычетов по простому модулю $p \geqslant 3$. Из этих результатов следует, в частности, что если $H > p^{1/2}\log^{1+\varepsilon}p$, где $\varepsilon > 0$, то квадратичных вычетов и невычетов на отрезке $[1, H]$ асимптотически поровну.

Теорема 1. *Для числа $N_p(H)$ решений сравнения*

$$y^2 - x \equiv 0 \pmod p$$

в целых числах $x = a+1, \ldots, a+H$ и $y = 0, 1, \ldots, p-1$, где $H < p$, справедлива формула

$$N_p(H) = H + O(p^{1/2}\log p).$$

Доказательство. Имеем

$$N_p(H) = \sum_{x=1}^{H}\left(1 + \left(\frac{x+a}{p}\right)\right) = H + \sum_{x=1}^{H}\left(\frac{x+a}{p}\right)$$

и, следовательно, достаточно показать, что

$$\left|\sum_{x=1}^{H}\left(\frac{x+a}{p}\right)\right|\leqslant c_1 p^{1/2}\log p.$$

Для простоты будем считать, что $a=0$.

Рассмотрим сумму Гаусса

$$T=\sum_{y=1}^{p-1}\left(\frac{y}{p}\right)e^{2pi\frac{y}{p}}.$$

При $x\not\equiv 0 \pmod p$ имеем

$$\left(\frac{x}{p}\right)T=\left(\frac{x^{-1}}{p}\right)T=\sum_{y=1}^{p-1}\left(\frac{x^{-1}y}{p}\right)e^{2\pi i\frac{y}{p}}=\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)e^{2\pi i\frac{xt}{p}}$$

и тогда

$$\sum_{x=1}^{H}\left(\frac{x}{p}\right)=T^{-1}\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\sum_{x=1}^{H}e^{2\pi i\frac{xt}{p}}.$$

Отсюда, принимая во внимание равенство $|T|=p^{1/2}$, получаем

$$\left|\sum_{x=1}^{H}\left(\frac{x}{p}\right)\right|\leqslant p^{-1/2}\sum_{t=1}^{p-1}\left|\sum_{x=1}^{H}e^{2\pi i\frac{xt}{p}}\right|.$$

Но

$$\left|\sum_{x=1}^{H}e^{2\pi i\frac{xt}{p}}\right|=\left|\frac{e^{2\pi i\frac{t}{p}}-e^{2\pi i\frac{(H+1)t}{p}}}{1-e^{2\pi i\frac{t}{p}}}\right|\leqslant$$

$$\leqslant\frac{2}{\left|1-e^{2\pi i\frac{t}{p}}\right|}=\frac{2}{\left|e^{\pi i\frac{t}{p}}-e^{-\pi i\frac{t}{p}}\right|}=\frac{1}{\sin\frac{\pi t}{p}}$$

и, значит,

$$\left|\sum_{x=1}^{H}\left(\frac{x}{p}\right)\right|\leqslant p^{-1/2}\sum_{t=1}^{p-1}\frac{1}{\sin\frac{\pi t}{p}}=2p^{-1/2}\sum_{t=1}^{\frac{p-1}{2}}\frac{1}{\sin\frac{\pi t}{p}}.$$

Из графика функции $y=\sin\frac{\pi t}{p}$ легко видеть, что на отрезке $1\leqslant t\leqslant\frac{p-1}{2}$ справедливо неравенство $\sin\frac{\pi t}{p}\geqslant\frac{2t}{p}$ и, в таком случае,

$$\left|\sum_{x=1}^{H}\left(\frac{x}{p}\right)\right|\leqslant p^{1/2}\sum_{t=1}^{\frac{p-1}{2}}\frac{1}{t}\leqslant c_1 p^{1/2}\log p. \qquad (1)$$

Теорема доказана.

Следствие. *Пусть $R(H)$ и соответственно $N(H)$ — количество квадратичных вычетов и невычетов среди чисел $a+1, \ldots, a+H$. Тогда*

$$R(H)=\frac{H}{2}+O\left(p^{1/2}\log p\right),$$

$$N(H)=\frac{H}{2}+O\left(p^{1/2}\log p\right).$$

2. Гипотезы И. М. Виноградова. Пусть $d(p)$ — максимальное расстояние между соседними квадратичными невычетами, $n(p)$ — наименьший квадратичный невычет и $r(p)$ — наименьший простой квадратичный вычет по модулю p среди чисел $1, 2, \ldots, p-1$. И. М. Виноградовым был высказан ряд гипотез о поведении величин $d(p)$, $n(p)$ и $r(p)$, а именно: *для любого заданного* $\varepsilon>0$

$$\text{I. } \frac{d(p)}{p^{\varepsilon}}\to 0, \quad \text{II. } \frac{n(p)}{p^{\varepsilon}}\to 0, \quad \text{III. } \frac{r(p)}{p^{\varepsilon}}\to 0$$

при $p\to\infty$.

В настоящее время мы далеки от доказательства этих гипотез, и особенно трудной представляется гипотеза I. Из расширенной гипотезы Римана для L-рядов Дирихле следует [152, 74], что

$$n(p)=O(\log^2 p), \quad r(p)=O(\log^2 p).$$

В то же время для подтверждения справедливости гипотезы I не удается получить даже подобного рода условные результаты.

Теорема 2 [27а]. *Для наименьшего квадратичного невычета $n(p)$ справедлива оценка*

$$n(p)\leqslant cp^{1/2\sqrt{e}}(\log^2 p),$$

где $c>0$ — абсолютная константа и e — основание натурального логарифма.

Доказательство. Положим $H=[p^{1/2}\log^2 p]$ и рассмотрим числа $1, 2, \ldots, H$. Если $n(p)\leqslant H^{1/2}$, то имеем $n(p)\leqslant p^{1/4}\log p\leqslant p^{1/2\sqrt{e}}\log^2 p$. этом случае утверждение теоремы справедливо.

Пусть теперь $n(p)>H^{1/2}$ и пусть $m\leqslant H$ — положительное целое число, являющееся квадратичным невычетом по модулю p. Поскольку каждый положительный квадратичный невычет n удовлетворяет неравенству $n\geqslant n(p)$, то среди простых делителей числа m может быть лишь один квадратичный невычет (если бы их было больше, то неравенство $n(p)>H^{1/2}$ оказалось бы противоречивым). Следовательно, $m=qt$, где q — простое число, удовлетворяющее условиям $\left(\frac{q}{p}\right)=-1$ и $n(p)\leqslant q\leqslant H$. Далее,

поскольку

$$\sum_{\substack{m=1\\(\frac{m}{p})=1}}^{H} 1+\sum_{\substack{m=1\\(\frac{m}{p})=-1}}^{H} 1=H,$$

то

$$\sum_{m=1}^{H}\left(\frac{m}{p}\right)=\sum_{\substack{m=1\\(\frac{m}{p})=1}}^{H} 1-\sum_{\substack{m=1\\(\frac{m}{p})=-1}}^{H} 1=H-2\sum_{\substack{m=1\\(\frac{m}{p})=-1}}^{H} 1=$$

$$=H-2\sum_{\substack{m=1\\m=qt\\n(p)<q\leqslant H}}^{H} 1=H-2\sum_{n(p)<q\leqslant H}\left[\frac{H}{q}\right]\geqslant$$

$$\geqslant H\left(1-2\sum_{n(p)<q\leqslant H} q^{-1}\right),$$

где последняя сумма берется по всем простым q, лежащим между $n(p)$ и H. Из теоремы 1 следует, что

$$\left|\sum_{m=1}^{H}\left(\frac{m}{p}\right)\right|\leqslant c_2\frac{H}{\log p}$$

и тогда

$$1-2\sum_{n(p)<q\leqslant H} q^{-1}\leqslant\frac{c_2}{\log p}. \qquad (2)$$

Воспользуемся теперь следующим соотношением из теории простых чисел (см. [142а, гл. VII, § 5])

$$\sum_{1<q\leqslant H} q^{-1}=\log\log H+\gamma+O\left(\frac{1}{\log H}\right).$$

Из этого соотношения следует, что

$$\sum_{n(p)<q\leqslant H} q^{-1}=\log\log H-\log\log n(p)+O\left(\frac{1}{\log n(p)}\right)=$$

$$=\log\frac{\log H}{\log n(p)}+O\left(\frac{1}{\log p}\right)$$

и тогда, ввиду (2),

$$\log\frac{\log H}{\log n(p)}\geqslant\frac{1}{2}-\alpha(p),$$

где $0\leqslant\alpha(p)\leqslant c_3/\log p$. Следовательно,

$$\frac{\log H}{\log n(p)}\geqslant e^{1/2-\alpha(p)}$$

и, стало быть,

$$n(p)\leqslant cH^{1/\sqrt{e}}\leqslant cp^{1/2\sqrt{e}}\log^2 p.$$

Теорема доказана.

3. Теорема Берджесса. Для получения более сильных утверждений относительно величин $d(p)$ и $n(p)$, чем те, которые дают теоремы 1 и 2, воспользуемся результатами гл. I.

Предварительно докажем несколько лемм. Следующая лемма принадлежит Дэвенпорту и Эрдешу [49].

Лемма 1. *Пусть $p>2$ — простое число и $h\leqslant p-1$, r — положительные целые числа. Тогда*

$$\sum_{x=0}^{p-1}\left(\sum_{\lambda=1}^{h}\left(\frac{x+\lambda}{p}\right)\right)^{2r}\leqslant(2r)^r ph^r+(2r-1)\,p^{1/2}h^{2r}.$$

Доказательство. Имеем

$$\sum_{x=0}^{p-1}\left(\sum_{\lambda=1}^{h}\left(\frac{x+\lambda}{p}\right)\right)^{2r}=\sum_{\lambda_1,\ldots,\lambda_{2r}=1}^{h}\sum_{x=0}^{p-1}\left(\frac{(x+\lambda_1)\ldots(x+\lambda_{2r})}{p}\right).$$

Разобьем наборы $(\lambda_1, \ldots, \lambda_{2r})$ на два класса. В первый класс отнесем те наборы $(\lambda_1, \ldots, \lambda_{2r})$, в которых не более r различных компонент и число равных между собой компонент четно. Остальные наборы отнесем во второй класс.

Оценим число наборов первого класса. Количество упорядоченных наборов $(\lambda_1, \ldots, \lambda_{2r})$, у которых $s\leqslant r$ компонент $\lambda_{i_1}, \ldots, \lambda_{i_s}$ суть различные между собой числа из множества $\{1, 2, \ldots, h\}$, а каждая из остальных компонент совпадает с одной из указанных, не превышает границы

$$h(h-1)\ldots(h-s+1).$$

При этом компоненты $\lambda_{i_1}, \ldots \lambda_{i_s}$ можно выбрать не более чем

$$(2r-s)!!\leqslant(2r-1)(2r-3)\ldots5\cdot3\cdot1\leqslant(2r)^2$$

различными способами и, значит, число наборов $(\lambda_1, \ldots, \lambda_{2r})$ первого класса не превосходит величины

$$(2r)^r\sum_{s=1}^{r}h(h-1)\ldots(h-s+1)\leqslant(2r)^r h^r.$$

Для каждого такого набора имеем

$$\left|\sum_{x=0}^{p-1}\left(\frac{(x+\lambda_1)\ldots(x+\lambda_{2r})}{p}\right)\right|\leqslant p$$

и, следовательно, вклад наборов первого класса в сумму

$$\sum_{x=0}^{p-1}\left(\sum_{\lambda=1}^{h}\left(\frac{x+\lambda}{p}\right)\right)^{2r}$$

не превышает $(2r)^r ph^r$.

Число наборов второго класса не превосходит общего числа наборов $(\lambda_1, \ldots, \lambda_{2r})$, т. е. величины h^{2r}, и для каждого из них внутренняя сумма

$$S=\sum_{x=0}^{p-1}\left(\frac{(x+\lambda_1)\ldots(x+\lambda_{2r})}{p}\right)$$

имеет вид

$$S=\sum_{x=0}^{p-1}\left(\frac{(x+\alpha_1)^{\nu_1}\ldots(x+\alpha_s)^{\nu_s}}{p}\right),$$

где $\nu_1+\ldots+\nu_s\leqslant 2r$; $\alpha_1, \ldots, \alpha_s$ — попарно несравнимые между собой по модулю p целые числа и $\nu_1, \ldots, \nu_s$ не все четные. В сумме S можно заменить показатели $\nu_1, \ldots, \nu_s$ на величины $e_1, \ldots, e_s$ по правилу

$$e_j=\begin{cases}2, & \text{если } \nu_j \text{ четное},\\ 1, & \text{если } \nu_j \text{ нечетное}.\end{cases}$$

В результате эта сумма примет вид

$$S=\sum_{x=0}^{p-1}\left(\frac{(x+\alpha_1)^{e_1}\ldots(x+\alpha_s^{e_s})}{p}\right),$$

где $e_1+\ldots+e_s\leqslant 2r$ и по крайней мере одно из e_j равно 1. Поскольку характер $\chi(t)=\left(\frac{t}{p}\right)$ имеет показатель 2, то согласно теореме 1 из § 4 гл. I

$$|S|\leqslant(2r-1)p^{1/2}.$$

Таким образом,

$$\sum_{x=0}^{p-1}\left(\sum_{\lambda=1}^{h}\left(\frac{x+\lambda}{p}\right)\right)^{2r}\leqslant(2r)^r ph^r+(2r-1)p^{1/2}h^{2r}$$

и лемма, тем самым, доказана.

Лемма 2. *Пусть N — количество решений сравнения $xy\equiv x'y' \pmod p$, где $1\leqslant x, x'\leqslant H$, $1\leqslant y, y'\leqslant H_1$, $1\leqslant HH_1<p$. Тогда при произвольном $\omega>0$ справедлива оценка*

$$N\leqslant c'(HH_1)^{1+\omega}$$

с некоторой константой $c'=c'(\omega)>0$.

Доказательство. Поскольку $HH_1<p$, то N равно количеству решений в целых числах $1\leqslant x, x'\leqslant H$, $1\leqslant y, y'\leqslant H_1$ уравнения $xy=x'y'$. Обозначим $d(n)$ количество положительных целых x', y', удовлетворяющих уравнению $x'y'=n$, и заметим, что если $n=p_1^{\alpha_1}\ldots p_s^{\alpha_s}$ — каноническое разложение числа n на простые сомножители, то $d(n)=(\alpha_1+1)\ldots(\alpha_s+1)$. В таком случае

$$d(mn)\leqslant d(m)d(n)$$

и

$$N=\sum_{x=1}^{H}\sum_{y=1}^{H_1}d(xy)\leqslant\left(\sum_{x=1}^{H}d(x)\right)\left(\sum_{y=1}^{H_1}d(y)\right).$$

Кроме того, имеем

$$\sum_{z=1}^{t}d(z)=\sum_{1\leqslant xy\leqslant t}1=\sum_{x=1}^{t}\left[\frac{t}{x}\right]\leqslant c''t\log t$$

и, значит,

$$N\leqslant c'(HH_1)^{1+\omega}.$$

Лемма доказана.

Лемма 3 (неравенство Гёльдера). *Пусть a_j, b_j, $1\leqslant j\leqslant M$, и α, β — неотрицательные действительные числа, причем $\frac{1}{\alpha}+\frac{1}{\beta}=1$. Тогда*

$$\sum_{j=1}^{M}a_jb_j\leqslant\left(\sum_{j=1}^{M}a_j^{\alpha}\right)^{1/\alpha}\left(\sum_{j=1}^{M}b_j^{\beta}\right)^{1/\beta}.$$

Доказательство. Будем считать, что не все числа a_j и b_j равны нулю (иначе нечего было бы доказывать). Рассмотрим при $x>0$ функции $f(x)=x$ и $g(x)=\frac{x^{\alpha}}{\alpha}+\frac{1}{\beta}$. Имеем $f(1)=g(1)$ и $f'(1)=g'(1)=1$. Следовательно, прямая $y=x$ является касательной к кривой $y=\frac{x^{\alpha}}{\alpha}+\frac{1}{\beta}$ в точке $(1, 1)$, и поскольку производная $g'(x)=x^{\alpha-1}$, $\alpha>1$, функции $g(x)$ монотонно возрастает вместе с x, то график функции $y=\frac{x^{\alpha}}{\alpha}+\frac{1}{\beta}$ при $x>0$ расположен выше графика функции $y=x$.

Отсюда следует, что

$$x\leqslant\frac{x^{\alpha}}{\alpha}+\frac{1}{\beta}.$$

Если положить $x=uv^{1-\beta}$, где $u>0$, $v>0$, то получим

$$uv^{1-\beta}\leqslant\frac{u^{\alpha}v^{(1-\beta)\alpha}}{\alpha}+\frac{1}{\beta}.$$

Значит,

$$uv = \left(uv^{1-\beta}\right)v^{\beta} \leqslant \frac{u^{\alpha}v^{\alpha+\beta-\alpha\beta}}{\alpha} + \frac{v^{\beta}}{\beta},$$

а так как $\frac{1}{\alpha} + \frac{1}{\beta} = 1$, то

$$uv \leqslant \frac{u^{\alpha}}{\alpha} + \frac{v^{\beta}}{\beta}.$$

Положим

$$u_j = \frac{a_j}{\left(\sum\limits_{j=1}^{M} a_j^{\alpha}\right)^{1/\alpha}}, \quad v_j = \frac{b_j}{\left(\sum\limits_{j=1}^{M} b_j^{\beta}\right)^{1/\beta}}.$$

Тогда из последнего неравенства следует, что

$$\sum_{j=1}^{M} a_j b_j \leqslant \left(\frac{1}{\alpha} + \frac{1}{\beta}\right)\left(\sum_{j=1}^{M} a_j^{\alpha}\right)^{1/\alpha}\left(\sum_{j=1}^{M} b_j^{\beta}\right)^{1/\beta} = \left(\sum_{j=1}^{M} a_j^{\alpha}\right)^{1/\alpha}\left(\sum_{j=1}^{M} b_j^{\beta}\right)^{1/\beta},$$

и тем самым лемма доказана.

Следующий результат Берджесса [13] значительно уточняет теорему 1 и, в свою очередь, приводит к усилению теоремы 2. Как показано в работе [56], этот результат может быть получен методом двойных сумм И. М. Виноградова.

Теорема 3 (Берджесс). *Для любого заданного $\varepsilon > 0$ существует $\delta = \delta(\varepsilon) > 0$ такое, что при $H > p^{1/4+\varepsilon}$ и любом целом a справедлива оценка*

$$\left|\sum_{x=1}^{H}\left(\frac{x+a}{p}\right)\right| \leqslant cHp^{-\delta}, \tag{3}$$

где $c = c(\delta) > 0$ — некоторая константа.

Доказательство. Для простоты изложения будем считать, что $a = 0$. Далее, ввиду оценки (1) можно предполагать, что

$$p^{1/4+\varepsilon} < H < p^{1/2+\varepsilon/8}.$$

Положим

$$r = \left[\frac{1}{\varepsilon}\right] + 1, \quad \delta = \frac{\varepsilon}{4}\left(r + \frac{1}{2}\right)^{-1}, \quad H_1 = \left[Hp^{-\frac{1}{2r}-\delta}\right], \quad H_2 = \left[p^{1/2r}\right].$$

При $1 \leqslant y \leqslant H_1$, $1 \leqslant z \leqslant H_2$ имеем

$$\sum_{x=1}^{H}\left(\frac{x}{p}\right) = \sum_{x=1}^{H}\left(\frac{x+yz}{p}\right) + O\left(Hp^{-\delta}\right).$$

Суммируя обе части этого равенства по всем указанным y и z,

получаем

$$\sum_{x=1}^{H}\left(\frac{x}{p}\right) = W + O\left(Hp^{-\delta}\right),$$

где

$$W = (H_1H_2)^{-1}\sum_{x=1}^{H}\sum_{y=1}^{H_1}\sum_{z=1}^{H_2}\left(\frac{x+yz}{p}\right).$$

Оценим сумму W. Имеем

$$|W| \leqslant (H_1H_2)^{-1}\sum_{\lambda} N(\lambda)\left|\sum_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|,$$

где $N(\lambda)$ — число решений сравнения $xy^{-1} \equiv \lambda \pmod p$ в целых $x = 1, 2, \ldots, H$ и $y = 1, 2, \ldots, H_1$. Положив $\alpha = \frac{r}{r-1}$, $\beta = r$, $a_\lambda = N(\lambda)^{\frac{r-1}{r}}$, $b_\lambda = \left|N(\lambda)^{1/r}\sum\limits_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|$, получаем по лемме 3

$$|W|^r \leqslant (H_1H_2)^{-r}\left(\sum_{\lambda} N(\lambda)\right)^{r-1}\left(\sum_{\lambda} N(\lambda)\left|\sum_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|^r\right).$$

В таком случае

$$|W|^{2r} \leqslant (H_1H_2)^{-2r}\left(\sum_{\lambda} N(\lambda)\right)^{2(r-1)}\left(\sum_{\lambda} N(\lambda)\left|\sum_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|^r\right)^2,$$

и так как (снова по лемме 3 с $\alpha = \beta = 2$)

$$\left(\sum_{\lambda} N(\lambda)\left|\sum_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|^r\right)^2 \leqslant \sum_{\lambda} N(\lambda)^2 \sum_{\lambda}\left|\sum_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|^{2r},$$

то

$$|W|^{2r} \leqslant (H_1H_2)^{-2r}\left(\sum_{\lambda} N(\lambda)\right)^{2(r-1)}\sum_{\lambda} N(\lambda)^2 \sum_{\lambda}\left|\sum_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|^{2r}.$$

Далее, имеем

$$\sum_{\lambda} N(\lambda) = HH_1, \quad \sum_{\lambda} N(\lambda)^2 = N,$$

где N — количество решений сравнения $xy \equiv x'y' \pmod p$ в целых x, x', y, y' из интервалов $1 \leqslant x, x' \leqslant H$, $1 \leqslant y, y' \leqslant H_1$,

и тогда по лемме 2

$$|W|^{2r} \leqslant c'(H_1H_2)^{-2r}(HH_1)^{2(r-1)}(HH_1)^{1+\omega}\sum_{\lambda=0}^{p-1}\left|\sum_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|^{2r}.$$

Отсюда, взяв ω достаточно малым по сравнению с ε, получаем на основании леммы 1, что

$$|W| \leqslant c'' H p^{-\delta}.$$

Следовательно,

$$\left|\sum_{x=1}^{H}\left(\frac{x}{p}\right)\right| \leqslant cHp^{-\delta},$$

и тем самым теорема доказана.

Следствие. *Для любого заданного $\delta > 0$ существует константа $p_0 = p_0(\delta)$ такая, что при $p > p_0$ имеет место неравенство*

$$n(p) < p^{1/4\sqrt{e}+\delta}.$$

Доказательство. Следствие выводится из оценки (3) аналогично тому, как теорема 2 была выведена из оценки (1). Возьмем $\varepsilon > 0$ и положим $H = [p^{1/4+\varepsilon}]$. Если $n(p) \leqslant H^{1/2}$, то $n(p) < p^{1/4\sqrt{e}+\varepsilon/2}$, и в этом случае следствие справедливо.

Пусть теперь $n(p) > H^{1/2}$. Поскольку каждый неотрицательный квадратичный невычет $m \leqslant H$ представляется в виде $m = qt$, где q — простое число с условиями $\left(\frac{q}{p}\right) = -1$ и $n(p) \leqslant q \leqslant H$, то те же рассуждения, которые были использованы при доказательстве теоремы 2, приводят нас к неравенству

$$\sum_{m=1}^{H}\left(\frac{m}{p}\right) \geqslant H\left(1 - 2\sum_{n(p)\leqslant q\leqslant H} q^{-1}\right),$$

где последняя сумма берется по всем простым числам q из интервала $n(p) \leqslant q \leqslant H$. По теореме Берджесса

$$\left|\sum_{m=1}^{H}\left(\frac{m}{p}\right)\right| \leqslant cHp^{-\delta'}$$

и тогда

$$\sum_{n(p)\leqslant q\leqslant H} q^{-1} \geqslant \frac{1}{2} - \alpha(p),$$

где $0 \leqslant \alpha(p) \leqslant c_1 p^{-\delta'}$. Следовательно,

$$\log\frac{\log H}{\log n(p)} \geqslant \frac{1}{2} - \alpha(p)$$

и, значит,

$$n(p) \leqslant c_2 H^{1/\sqrt{e}} < p^{1/4\sqrt{e}+\delta}$$

для всех $p > p_0$. Следствие доказано.

Задачи

1. Пусть $p > 2$ — простое число и $N(\alpha, \beta)$ — количество чисел $x \in \{1, 2, \ldots, p-1\}$, для которых $\left(\frac{x}{p}\right) = \alpha$, $\left(\frac{x+1}{p}\right) = \beta$. Доказать справедливость соотношений:

$$N(1, 1) = \begin{cases} \frac{p-5}{4}, & \text{если } p \equiv 1 \pmod 4, \\ \frac{p-3}{4}, & \text{если } p \equiv 3 \pmod 4, \end{cases}$$

$$N(1, -1) = \begin{cases} \frac{p-1}{4}, & \text{если } p \equiv 1 \pmod 4, \\ \frac{p+1}{4}, & \text{если } p \equiv 3 \pmod 4, \end{cases}$$

$$N(-1, 1) = \begin{cases} \frac{p-1}{4}, & \text{если } p \equiv 1 \pmod 4, \\ \frac{p-3}{4}, & \text{если } p \equiv 3 \pmod 4, \end{cases}$$

$$N(-1, -1) = \begin{cases} \frac{p-1}{4}, & \text{если } p \equiv 1 \pmod 4, \\ \frac{p-3}{4}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

2. Пусть $p > 2$ — простое число. Доказать, что

$$n(p) < \frac{1}{2} + \left(p + \frac{1}{4}\right)^{1/2}.$$

3. Используя результат предыдущей задачи, показать, что при $p > 3$ справедлива оценка $d(p) < 2\sqrt{p}$.

4. Пусть $p > 2$ — простое число, $s < p$ и $(\alpha_1, \ldots, \alpha_s)$ — заданный набор чисел $\alpha_j = \pm 1$, $1 \leqslant j \leqslant s$. Положим

$$N_s(x) = 2^{-s}\prod_{j=1}^{s}\left(1 + \alpha_j\left(\frac{x+j}{p}\right)\right)$$

и обозначим N_s — количество чисел $x \in \{0, 1, \ldots, p-1\}$, для которых

$$\left(\frac{x+1}{p}\right) = \alpha_1, \ldots, \left(\frac{x+s}{p}\right) = \alpha_s.$$

Доказать справедливость следующих утверждений:

а) Имеет место соотношение

$$N_s = \sum_{x=0}^{p-1} N_s(x) + R, \quad |R| \leqslant s.$$

б) Справедливо неравенство

$$\left|N_s - \frac{p}{2^s}\right| \leqslant 2s\sqrt{p}.$$

в) Если $2^s \leqslant \frac{\sqrt{p}}{\log^2 p}$ и $p > p_0$, то найдется хотя бы одно число $x \in \{0, 1, \ldots, p-1\}$, для которого

$$\left(\frac{x+1}{p}\right) = \alpha_1, \ \ldots, \ \left(\frac{x+s}{p}\right) = \alpha_s.$$

г) При $2^s \leqslant \frac{\sqrt{p}}{\log^2 p}$ количество N_s чисел $x \in \{0, 1, \ldots, p-1\}$, для которых

$$\left(\frac{x+1}{p}\right) = \alpha_1, \ \ldots, \ \left(\frac{x+s}{p}\right) = \alpha_s,$$

выражается асимптотической формулой

$$N_s = \frac{p}{2^s}\left(1 + \frac{2\theta}{\log p}\right), \quad |\theta| \leqslant 1.$$

5. Уточнить результаты теорем 1 и 2, доказав справедливость неравенств

$$\left|\sum_{x=1}^{H}\left(\frac{x}{p}\right)\right| \leqslant p^{1/2}\log p, \quad n(p) \leqslant p^{1/2\sqrt{e}}\log^2 p.$$

6. Пусть F_q — конечное поле характеристики $p > 2$ и $\omega_1, \ldots, \omega_n$ — его базис над простым полем F_p. Пусть, далее, χ — нетривиальный мультипликативный характер поля F_q и $V(H)$ — множество элементов $x = x_1\omega_1 + \ldots + x_n\omega_n$ поля F_q с условием $0 \leqslant a_j \leqslant x_j \leqslant a_j + H < p$, $1 \leqslant j \leqslant n$. Обобщая результат теоремы 3, доказать, что для всякого $\varepsilon > 0$ найдутся $\delta = \delta(\varepsilon, \omega_1, \ldots, \omega_n, \chi)$ и $p_0 = p_0(\varepsilon, \omega_1, \ldots, \omega_n, \chi)$ такие, что при $H > p^{1/4+\varepsilon}$, $p > p_0$ справедлива оценка

$$\left|\sum_{x \in V(H)} \chi(x)\right| < (Hp^{-\delta})^n.$$

7. Пусть $p > 2$ — простое число и

$$S(h) = \sum_{x=1}^{h}\left(\frac{x}{p}\right), \quad 1 \leqslant h \leqslant p-1.$$

Доказать справедливость следующих утверждений:

а) имеет место неравенство

$$\sum_{n=1}^{p-1} S^2(h) \geqslant \frac{p^2-1}{12};$$

б) хотя бы для одного $h = 1, 2, \ldots, p-1$ выполняется соотношение

$$|S(h)| \geqslant \left(\frac{p+1}{12}\right)^{1/2}.$$

8*. Пусть $p > 3$ — простое число и $n > 1$ — делитель числа $p-1$. Доказать, что наименьший среди чисел $1, 2, \ldots, p-1$ невычет степени n по модулю p не превосходит величины

$$p^{1/2k}\log^2 p,$$

где $k = e^{\frac{n-1}{n}}$ и e — основание натурального логарифма.

9*. Пусть $p > 3$ — простое число и $1 \leqslant H < p$ — целое число. Доказать, что количество первообразных корней по модулю p, лежащих среди чисел $1, 2, \ldots, H$, равно

$$\frac{\varphi(p-1)}{p-1}H + \theta 2^k p^{1/2}\log p,$$

где $\varphi(m)$ — функция Эйлера, $|\theta| < 1$ и k — число различных простых делителей $p-1$. Вывести отсюда верхнюю границу

$$\eta(p) \leqslant 2^k \frac{p-1}{\varphi(p-1)} p^{1/2}\log p$$

для наименьшего первообразного корня $\eta(p) \in \{1, 2, \ldots, p-1\}$.

10*. В обозначениях задачи 6 доказать, что количество элементов порядка $q-1$ мультипликативной группы F_q^* поля F_q, лежащих в множестве $V(H)$, $H > p^{1/4+\varepsilon}$, $p > p_0$, равно

$$\frac{\varphi(q-1)}{q-1}H^n(1 + O(p^{-n\delta})), \quad \delta > 0.$$

11. Пусть p — нечетное простое число, $(a, p) = 1$ и $1 \leqslant U < p$. Доказать, что

$$\left|\sum_{x=1}^{U} e^{2\pi i\frac{ax^2}{p}}\right| = O(p^{1/2}\log^2 p).$$

12. Пусть p — нечетное простое число, $(a, p) = 1$ и $N_p(U, V)$ — количество решений сравнения

$$ay^2 \equiv x \pmod p$$

с $1 \leqslant x \leqslant U < p$, $1 \leqslant y \leqslant V \leqslant p$. Используя результат предыдущей задачи, установить справедливость формулы

$$N_p(U, V) = \frac{UV}{p} + O(p^{1/2}\log^2 p).$$

13. Пусть p — нечетное простое число и $N_p(A, B)$ — количество решений сравнения

$$x^2 + y^2 \equiv 1 \pmod p$$

с $1 \leqslant x \leqslant A \leqslant p$, $1 \leqslant y \leqslant B \leqslant p$. Используя результат задачи 11, доказать, что

$$N_p(A, B) = \frac{AB}{p} + O(p^{1/2}\log^2 p).$$

14* (С. А. Степанов [117k]). Пусть p — нечетное простое число, $1 \leqslant H \leqslant p$ — целое число, $\mathfrak{M} = \{f_1(x), \ldots, f_m(x)\}$ — множество всех неприводимых нормированных многочленов из кольца $F_p[x]$ степени $n > 1$ и $\chi(x) = \left(\frac{f_s(x)}{p}\right)$, $x \in F_p$, $1 \leqslant s \leqslant m$. Доказать справедливость следующих утверждений:

а) Если $\frac{(H+1)\log 2}{\log p} + 1 < n \leqslant p$, то среди наборов

$$\lambda_s = (\lambda_s(1), \ldots, \lambda_s(H)), \quad 1 \leqslant s \leqslant m,$$

найдутся по меньшей мере два одинаковых.

б) При выполнении условия предыдущего пункта найдутся бесквадратные многочлены $f(x)$, $g(x) \in F_p[x]$ степени $2n$, для которых

$$\sum_{x=1}^{H}\left(\frac{f(x)}{p}\right)=H \quad \text{и} \quad \sum_{x=1}^{H}\left(\frac{g(x)}{p}\right)=-H.$$

в) Если $p>7$ и $1\leqslant H<\dfrac{\log p-\log(2\log p)}{\log 2}$, то найдутся бесквадратные многочлены $f(x)$, $g(x)\in F_p[x]$ степени 2, для которых

$$\sum_{x=1}^{H}\left(\frac{f(x)}{p}\right)=H \quad \text{и} \quad \sum_{x=1}^{H}\left(\frac{g(x)}{p}\right)=-H.$$

15. Пусть p — нечетное простое число, $1\leqslant N\leqslant p$ — целое число, $0<\varepsilon<1/4\pi$ и $\mathfrak{R}=\{f_1(x), \ldots, f_r(x)\}$ — множество всех многочленов из кольца $F_p[x]$ степени не выше n. Пусть, далее, $B_{k_1,\ldots,k_N}$ — N-мерный комплексный «кубик», состоящий из точек

$$z=\left(e^{2\pi i\frac{\theta_1}{p}}, \ldots, e^{2\pi i\frac{\theta_N}{p}}\right),$$

где $(k_s-1)\varepsilon p\leqslant\theta_s<k_s\varepsilon p$, если $1\leqslant k_s\leqslant[\varepsilon^{-1}]-1$, $1\leqslant s\leqslant N$, и $([\varepsilon^{-1}]-1)\varepsilon p<\theta_s<p$, если $k_s=[\varepsilon^{-1}]$. Доказать справедливость следующих утверждений:

а) Если $n\geqslant\dfrac{N\log(1+\varepsilon^{-1})}{\log p}$, то среди точек

$$z_\tau=\left(e^{2\pi i\frac{f_\tau(1)}{p}}, \ldots, e^{2\pi i\frac{f_\tau(N)}{p}}\right), \quad 1\leqslant\tau\leqslant r,$$

найдутся по меньшей мере две точки, лежащие в одном из «кубиков» $B_{k_1,\ldots,k_N}$, $1\leqslant k_1, \ldots, k_N\leqslant[\varepsilon^{-1}]$.

б) Для каждого целого $n\geqslant\dfrac{N\log(1+\varepsilon^{-1})}{\log p}$ найдется отличный от нуля многочлен $f(x)=f_j(x)-f_\tau(x)$, $1\leqslant j, \tau\leqslant r$, степени не выше n, для которого

$$\left|\sum_{x=1}^{N} e^{2\pi i\frac{f(x)}{p}}\right|\geqslant(1-2\pi\varepsilon)N.$$

16*. Пусть m, n — положительные целые числа, p — простое число и $\Lambda(n)$, $\theta(x)$ — *функции Мангольдта и Чебышева*, определенные равенствами

$$\Lambda(n)=\begin{cases}\log p, & \text{если } n=p^m, \ m\geqslant 1,\\ 0, & \text{если } n\neq p^m,\end{cases}$$

$$\theta(x)=\sum_{p\leqslant x}\log p.$$

Установить справедливость следующих утверждений.

а) Выполняются равенства

$$\sum_{d\mid n}\Lambda(d)=\log n, \quad \Lambda(n)=\sum_{d\mid n}\mu(d)\log\frac{n}{d}.$$

б) Имеет место равенство

$$n!=\prod_{p\leqslant n}p^{e_p},$$

где

$$e_p=\sum_{m=1}^{\infty}\left[\frac{n}{p^m}\right].$$

в) При $x\to\infty$ имеем

$$\sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1).$$

(Указание. Воспользовавшись утверждением предыдущего пункта и соотношениями

$$\sum_{m\leqslant x}m^{-1-\delta}=O(1), \quad \delta>0,$$

$$\sum_{m\leqslant x}\log m=x\log x-x+O(\log x),$$

показать, что

$$A(n)\overset{\text{def}}{=}\sum_{p\leqslant n}\left[\frac{n}{p}\right]\log p=n\log n+O(n).$$

Установить, что последнее соотношение справедливо и для нецелых n. Используя неравенство $[x]-2[x/2]\geqslant 0$, вывести отсюда оценку

$$\theta(n)-\theta(n/2)=\sum_{n/2<p\leqslant n}\log p=\sum_{n/2<p\leqslant n}\left[\frac{n}{p}\right]\log p\leqslant$$
$$\leqslant\sum_{p\leqslant n}\left\{\left[\frac{n}{p}\right]-2\left[\frac{n}{2p}\right]\right\}\log p=A(n)-2A(n/2)\leqslant cn.$$

Складывая затем неравенства

$$\theta\left(\frac{n}{2^s}\right)-\theta\left(\frac{n}{2^{s+1}}\right)\leqslant c\frac{n}{2^s}, \quad s=0, 1, 2, \ldots,$$

получить оценку $\theta(n)=O(n)$.

Представить, наконец, целую часть $\left[\dfrac{x}{p}\right]$ числа $\dfrac{x}{p}$ в виде

$$\left[\frac{x}{p}\right]=\frac{x}{p}-\eta_p, \quad 0\leqslant\eta_p<1,$$

и воспользоваться асимптотикой

$$A(x)\overset{\text{def}}{=}\sum_{p\leqslant x}\left[\frac{x}{p}\right]\log p=x\log x+O(x)$$

для суммы $A(x)$.)

г) При $x \to \infty$ имеет место асимптотическая формула

$$\sum_{n \leqslant x} \frac{\Lambda(n)}{n} = \log x + O(1).$$

(Указание. Показать, что

$$\left| \sum_{n \leqslant x} \frac{\Lambda(n)}{n} - \sum_{p \leqslant x} \frac{\log p}{p} \right| \leqslant \sum_{p \leqslant x} \frac{\log p}{p(p-1)} < \infty;$$

и затем воспользоваться результатом предыдущего пункта.)

д) При $x \to \infty$ имеем

$$\sum_{p \leqslant x} \frac{1}{p} = \log \log x + \gamma + O\left(\frac{1}{\log x}\right).$$

(Указание. Воспользоваться соотношением

$$\sum_{p \leqslant x} \frac{1}{p} = \sum_{p \leqslant x} \frac{\log p}{p} \cdot \frac{1}{\log p} = \sum_{2 \leqslant n \leqslant x} \frac{\theta(n) - \theta(n-1)}{n} \cdot \frac{1}{\log n}$$

и, применив к последней сумме преобразование Абеля, показать, что

$$\sum_{p \leqslant x} \frac{1}{p} = \sum_{2 \leqslant m \leqslant x} \left(\sum_{n \leqslant m} \frac{\theta(n) - \theta(n-1)}{n} \right) \left(\frac{1}{\log m} - \frac{1}{\log (m+1)} \right) + c + O\left(\frac{1}{\log x}\right) =$$

$$= \sum_{2 \leqslant m \leqslant x} \left(\sum_{p \leqslant m} \frac{\log p}{p} \right) \left(\frac{1}{\log m} - \frac{1}{\log (m+1)} \right) + c + O\left(\frac{1}{\log x}\right).$$

Затем воспользоваться соотношениями

$$\frac{1}{\log m} - \frac{1}{\log (m+1)} = \frac{1}{m \log^2 m} + O\left(\frac{1}{m^2}\right),$$

$$\sum_{2 \leqslant m \leqslant x} \frac{1}{m \log m} = \log \log x + c' + O\left(\frac{1}{x \log x}\right),$$

$$\sum_{2 \leqslant m \leqslant x} \frac{1}{m \log^2 m} = c'' + O\left(\frac{1}{\log x}\right)$$

и результатом п. в).)

§ 2. Большое решето и его применение к задаче о наименьшем квадратичном невычете

1. Большое решето. Трудности, связанные с доказательством гипотезы И. М. Виноградова о наименьшем квадратичном невычете $n(p)$, привели к ослабленной форме проблемы — задаче о поведении $n(p)$ «в среднем» по простым числам p. В этом направлении Ю. В. Линником [73b] при помощи созданного им метода большого решета [73a] было установлено, что гипотеза И. М. Виноградова о наименьшем квадратичном невычете справедлива для подавляющего большинства простых чисел p.

Важнейшие этапы развития метода большого решета и его многочисленные применения подробно освещены в книге Г. Дэвенпорта [48f]. Основу метода составляет следующий общий результат о значениях тригонометрического многочлена на конечном множестве точек.

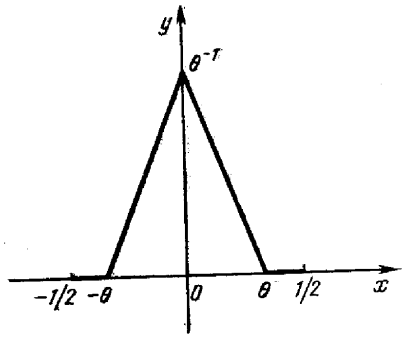


Рис.1

Лемма 1. *Пусть* $a_{-N}, a_{-N+1}, \ldots, a_N$ — *произвольные комплексные числа и*

$$S(x) = \sum_{n=-N}^{N} a_n e^{2\pi i n x}.$$

Пусть, далее, $x_1, \ldots, x_R$ — *произвольные вещественные числа и*

$$\delta = \min_{j \neq k} \| x_j - x_k \|,$$

где $\|\alpha\|$ — *расстояние от* α *до ближайшего целого числа. Тогда*

$$\sum_{r=1}^{R} |S(x_r)|^2 \leqslant 2{,}2 \max\left(\delta^{-1}, 2N\right) \sum_{n=-N}^{N} |a_n|^2.$$

Доказательство. Пусть θ — произвольное число, удовлетворяющее условиям $0 < \theta < \delta/2$ и $\theta \leqslant 1/2N$. Определим периодическую с периодом 1 функцию $\varphi(x)$ следующим образом:

$$\varphi(x) = \begin{cases} \theta^{-1}\left(1 - \theta^{-1}|x|\right), & \text{если } |x| \leqslant \theta, \\ 0, & \text{если } \theta < |x| \leqslant 1/2. \end{cases}$$

Она является непрерывной функцией ограниченной вариации и, следовательно, представима равномерно сходящимся рядом Фурье

$$\varphi(x) = \sum_{n=-\infty}^{\infty} c_n e^{2\pi i n x}.$$

Так как функция $\varphi(x)$ вещественна, то $c_{-n} = \bar{c}_n$, и поскольку она четная (рис. 1), то ряд Фурье функции $\varphi(x)$ содержит лишь косинусы.

Выпишем коэффициенты Фурье

$$c_n = \int_{-1/2}^{1/2} \varphi(x) e^{-2\pi i n x} dx = \frac{2}{\theta} \int_0^{\theta} \left(1 - \frac{x}{\theta}\right) \cos 2\pi n x dx.$$

Интегрируя по частям, получим

$$c_n = \frac{1}{\pi n \theta^2} \int_0^{\theta} \sin 2\pi n x dx = \left(\frac{\sin \pi n \theta}{\pi n \theta} \right)^2.$$

Для изучения тригонометрического многочлена $S(x)$ в окрестности точки $x = x_r$ введем вспомогательный многочлен

$$T(x) = \sum_{n=-N}^{N} \left(\frac{\pi n\theta}{\sin \pi n\theta}\right)^2 a_n e^{2\pi i n x}.$$

По равенству Парсеваля для свертки имеем

$$\int_{-1/2}^{1/2} \varphi(y)\, T(x-y)\, dy = \sum_{n=-N}^{N} a_n e^{2\pi i n x} = S(x)$$

и, значит,

$$S(x) = \int_{-\theta}^{\theta} \varphi(y)\, T(x-y)\, dy.$$

Применяя неравенство Коши, получаем

$$|S(x)|^2 \leqslant \int_{-\theta}^{\theta} \varphi^2(y)\, dy \int_{-\theta}^{\theta} |T(x-y)|^2\, dy,$$

и так как

$$\int_{-\theta}^{\theta} \varphi^2(y)\, dy = \frac{2}{\theta^2} \int_{0}^{\theta} \left(1 - \frac{y}{\theta}\right)^2 dy = \frac{2}{3\theta},$$

то

$$|S(x)|^2 \leqslant \frac{2}{3\theta} \int_{-\theta}^{\theta} |T(x-y)|^2\, dy = \frac{2}{3\theta} \int_{x-\theta}^{x+\theta} |T(z)|^2\, dz.$$

Заменим теперь x на x_r и просуммируем обе части последнего неравенства по всем $r = 1, 2, \ldots, R$. В силу выбора параметров δ и θ интервалы $(x_r - \theta,\ x_r + \theta)$ не пересекаются по mod 1 и тогда

$$\sum_{r=1}^{R} |S(x_r)|^2 \leqslant \frac{2}{3\theta} \sum_{r=1}^{R} \int_{x_r-\theta}^{x_r+\theta} |T(z)|^2\, dz \leqslant \frac{2}{3\theta} \int_{-1/2}^{1/2} |T(z)|^2\, dz.$$

Отсюда, применяя к $T(z)$ равенство Парсеваля, получаем

$$\sum_{r=1}^{R} |S(x_r)|^2 \leqslant \frac{2}{3\theta} \sum_{n=-N}^{N} \left(\frac{\pi n\theta}{\sin \pi n\theta}\right)^4 |a_n|^2.$$

Вспомним ограничение $\theta \leqslant 1/2N$. Коэффициенты $(\pi n\theta/\sin \pi n\theta)^4$ достигают своего максимального значения при $n = \pm N$ и, значит,

$$\sum_{r=1}^{R} |S(x_r)|^2 \leqslant \frac{2}{3\theta} \left(\frac{\pi N\theta}{\sin \pi N\theta}\right)^4 \sum_{n=-N}^{N} |a_n|^2.$$

Позаботимся теперь об оптимальном выборе параметра θ, удовлетворяющего условиям $\theta \leqslant \delta/2$ и $\theta \leqslant 1/2N$. Положим $\pi N\theta = \tau$. Тогда

$$\tau \leqslant \pi N\delta/2, \quad \tau \leqslant \pi/2$$

и

$$\frac{2}{3\theta} \left(\frac{\pi N\theta}{\sin \pi N\theta}\right)^4 = \frac{2\pi N}{3} \cdot \frac{\tau^3}{(\sin \tau)^4}.$$

Функция $\tau^3/\sin^4 \tau$ убывает с возрастанием τ от 0 до τ_0, где τ_0 — единственное решение уравнения

$$\operatorname{tg} \tau = \frac{4}{3}\tau$$

в интервале $(0, \pi/2)$. Если $\tau_0 \leqslant \pi N\delta/2$, то положим $\tau = \tau_0$. Тогда значение рассматриваемой функции в точке τ_0 равно

$$\frac{2\pi N}{3} \cdot \frac{\tau_0^3}{\sin^4 \tau_0}.$$

Если же $\tau_0 > \pi N\delta/2$, то положим $\tau = \frac{\pi N\delta}{2} < \tau_0$. В этом случае значение функции будет равно

$$\frac{2\pi N}{3} \cdot \frac{\tau^3}{\sin^4 \tau} \leqslant \frac{4}{3}\delta^{-1} \left(\frac{\tau}{\sin \tau}\right)^4 < \frac{4}{3}\delta^{-1} \left(\frac{\tau_0}{\sin \tau_0}\right)^4.$$

Из таблиц находим $\tau_0 = 0,8447\ldots$ и тогда

$$\frac{\pi}{3} \cdot \frac{\tau_0^3}{\sin^4 \tau_0} = 2,019\ldots, \quad \frac{4}{3} \left(\frac{\tau_0}{\sin \tau_0}\right)^4 = 2,171\ldots$$

Поскольку оба указанных числа меньше, чем 2,2, получаем утверждение леммы.

Следующая лемма имеет несколько больший арифметический характер.

Лемма 2. *Пусть U и $V > 0$ — целые числа и*

$$S(x) = \sum_{n=U+1}^{U+V} a_n e^{2\pi i n x}.$$

Тогда

$$\sum_{q \leqslant X} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left|S\left(\frac{a}{q}\right)\right|^2 \leqslant 2,2 \max(X^2, V) \sum_{n=U+1}^{U+V} |a_n|^2.$$

Доказательство. В сумме $S(x)$ заменим индекс суммирования n на m по следующей формуле:

$$n = m + U + N + 1,$$

где

$$N = \begin{cases} V/2, & \text{если } V \text{ четное,} \\ (V-1)/2, & \text{если } V \text{ нечетное.} \end{cases}$$

Тогда m изменяется от $-N$ до N, либо от $-N$ до $N-1$. В последнем случае будем считать, что m тоже изменяется до N, полагая $a_N = 0$.

Теперь к сумме

$$\sum_{q \leqslant X} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2$$

можно применить лемму 1. Числа $x_1, x_2, \ldots, x_R$ — это все рациональные числа $\frac{a}{q}$, у которых знаменатели не превосходят числа X. Если $\frac{a}{q} \neq \frac{a'}{q'}$, то

$$\left\| \frac{a}{q} - \frac{a'}{q'} \right\| \geqslant \frac{1}{qq'} \geqslant \frac{1}{X^2}$$

и, значит, $\delta \geqslant 1/X^2$. Применяя лемму 1, получим

$$\sum_{q \leqslant X} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 \leqslant 2{,}2 \max(X^2, 2N) \sum_{m=-N}^{N} |a_m|^2 \leqslant$$

$$\leqslant 2{,}2 \max(X^2, V) \sum_{n=U+1}^{U+V} |a_n|^2,$$

что и требовалось доказать.

Лемма 2 позволяет теперь установить следующий чисто арифметический результат.

Лемма 3. *Пусть $n_1, n_2, \ldots, n_H$ — различные целые положительные числа, не превосходящие V, p — простое число и $N_p(h)$ — количество индексов j, для которых $n_j \equiv h \pmod p$. Тогда для любого $X > 0$*

$$\sum_{p<X} p \sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p} \right)^2 \leqslant 2{,}2 \max(X^2, V) H.$$

Доказательство. Рассмотрим тригонометрическую сумму

$$S(x) = \sum_{j=1}^{H} e^{2\pi i n_j x}$$

и представим ее в виде

$$S(x) = \sum_{n=1}^{V} a_n e^{2\pi i n x},$$

где

$$a_n = \begin{cases} 1, & \text{если } n = n_j \text{ при некотором } j, \\ 0 & \text{в противном случае.} \end{cases}$$

Согласно определению $N_p(h)$ имеем при $a \not\equiv 0 \pmod p$

$$S\left(\frac{a}{p}\right) = \sum_{j=1}^{H} e^{2\pi i \frac{a n_j}{p}} = \sum_{h=0}^{p-1} N_p(h)\, e^{2\pi i \frac{ah}{p}} = \sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p} \right) e^{2\pi i \frac{ah}{p}}.$$

Кроме того, поскольку

$$\sum_{h=0}^{p-1} N_p(h) = H,$$

то

$$\sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p} \right) = 0.$$

Поэтому

$$\sum_{a=1}^{p-1} \left| S\left(\frac{a}{p}\right) \right|^2 = \sum_{a=0}^{p-1} \left| \sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p} \right) e^{2\pi i \frac{ah}{p}} \right|^2 =$$

$$= \sum_{h_1=0}^{p-1} \sum_{h_2=0}^{p-1} \left(N_p(h_1) - \frac{H}{p} \right) \left(N_p(h_2) - \frac{H}{p} \right) \sum_{a=0}^{p-1} e^{2\pi i \frac{a(h_1 - h_2)}{p}},$$

и так как

$$\sum_{a=0}^{p-1} e^{2\pi i \frac{a(h_1-h_2)}{p}} = \begin{cases} p, & \text{если } h_1 \equiv h_2 \pmod p, \\ 0 & \text{в противном случае,} \end{cases}$$

то

$$\sum_{a=1}^{p-1} \left| S\left(\frac{a}{p}\right) \right|^2 = p \sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p} \right)^2.$$

Значит,

$$\sum_{p<X} \sum_{a=1}^{p-1} \left| S\left(\frac{a}{p}\right) \right|^2 = \sum_{p<X} p \sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p} \right)^2,$$

и тогда по лемме 2

$$\sum_{p<X} p \sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p} \right)^2 \leqslant 2{,}2 \max(X^2, V) H.$$

Лемма 3 тем самым доказана.

2. Исключительные простые числа. Выведем теперь из леммы 3 результат, который был установлен Ю. В. Линником в его исходной работе о большом решете.

Теорема 1. *Пусть заданы H различных целых чисел $n_1, n_2, \ldots, n_H$, лежащих между 1 и V, и вещественное число τ, $0<\tau<1$. Назовем простое число $p \leqslant V^{1/2}$ исключительным, если количество классов вычетов по* $\bmod p$, *которым принадлежат числа $n_1, n_2, \ldots, n_H$, меньше чем $(1-\tau)p$.*

Количество исключительных простых чисел $p \leqslant V^{1/2}$ не превосходит величины $2{,}2V(\tau H)^{-1}$.

Доказательство. Из леммы 3 следует, что

$$\sum_{p \leqslant V^{1/2}} p \sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p}\right)^2 \leqslant 2{,}2VH.$$

Обозначим $\mathfrak{P}$ множество исключительных простых чисел $p \leqslant V^{1/2}$ и усилим предыдущее неравенство

$$\sum_{p \in \mathfrak{P}} p \sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p}\right)^2 \leqslant 2{,}2VH.$$

Если $p \in \mathfrak{P}$, то число классов вычетов по модулю p, для которых $N_p(h)=0$ не меньше чем τp, и поэтому для всех $p \in \mathfrak{P}$ имеем

$$\sum_{h=0}^{p-1} \left(N_p(h) - \frac{H}{p}\right)^2 \geqslant \tau p \left(\frac{H}{p}\right)^2 = \tau \frac{H^2}{p}.$$

Значит,

$$\sum_{p \in \mathfrak{P}} p\tau \frac{H^2}{p} \leqslant 2{,}2VH$$

и, следовательно,

$$\sum_{p \in \mathfrak{P}} 1 \leqslant 2{,}2 \frac{V}{\tau H}.$$

Теорема доказана.

3. Теорема Линника. Перейдем к применению метода большого решета к задаче о наименьшем квадратичном невычете. Для этого воспользуемся одним результатом И. М. Виноградова (см. [27а, с. 85]), который сформулируем в следующем виде:

Лемма 4. *Пусть $H(x, y)$ — количество положительных целых чисел $n \leqslant x$, все простые делители которых не превосходят y. При достаточно большом y справедливо неравенство*

$$H(x, y) \geqslant x \exp\left(-c \frac{\log x}{\log y} \log \frac{\log x}{\log y}\right),$$

где c — положительная константа.

Доказательство. Пусть $s = \left[\frac{\log x}{\log y}\right]$ и предположим сначала, что $s<2$, т. е. $y > x^{1/2}$. В этом случае

$$H(x, y) > H(x, x^{1/2}) \geqslant$$

$$\geqslant x - \sum_{x^{1/2}<p\leqslant x} \sum_{\substack{n\leqslant x \\ p|n}} 1 \geqslant x - \sum_{x^{1/2}<p\leqslant x} \frac{x}{p} = x\left(1 - \sum_{x^{1/2}<p\leqslant x} \frac{1}{p}\right),$$

и так как

$$\sum_{p\leqslant x} \frac{1}{p} = \log\log x + \gamma + O\left(\frac{1}{\log x}\right),$$

где γ — некоторая постоянная, то

$$H(x, y) \geqslant x\left(1 - \log 2 + O\left(\frac{1}{\log x}\right)\right) \geqslant x \exp\left(-c \frac{\log x}{\log y} \log \frac{\log x}{\log y}\right).$$

Пусть теперь $s = \left[\frac{\log x}{\log y}\right] \geqslant 2$. Покажем сначала, что лемму достаточно доказать для тех x и y, которые удовлетворяют условиям

$$y^s \leqslant x < y^{s+\frac{1}{s+2}}. \tag{1}$$

Действительно, если лемма доказана при этих условиях и если

$$y^{s+\frac{1}{s+2}} \leqslant x < y^{s+1},$$

то, полагая $\tilde{y} = x^{1/(s+1)}$, имеем

$$\tilde{y}^{s+1} \leqslant x < \tilde{y}^{s+1+\frac{1}{s+3}}$$

и, ввиду того, что $\tilde{y} \leqslant y$, получаем

$$H(x, y) \geqslant H(x, \tilde{y}) \geqslant x \exp(-c(s+1)\log(s+1)).$$

Но поскольку

$$3s \log s \geqslant 2(s+1)\log s \geqslant (s+1)\log(s+1),$$

то

$$H(x, y) \geqslant x \exp\left(-3c \frac{\log x}{\log y} \log \frac{\log x}{\log y}\right).$$

Итак, будем считать условия (1) выполненными и положим

$$\varepsilon = 1/(s+2).$$

Возьмем любое число x_1, удовлетворяющее условию

$$y \leqslant x_1 < y^{2-2\varepsilon},$$

и оценим снизу количество H_1 положительных целых чисел $n \leqslant$

$\leqslant x_1$, делящихся хотя бы на одно простое число p из интервала $y^{1-\varepsilon} < p \leqslant y$. Имеем

$$H_1 = \sum_{y^{1-\varepsilon} < p \leqslant y} \left[\frac{x_1}{p}\right]$$

и, воспользовавшись простейшими результатами из теории распределения простых чисел, получаем

$$H_1 = x_1 \sum_{y^{1-\varepsilon} < p \leqslant y} \frac{1}{p} + O(\pi(y)) =$$

$$= x_1 \log \frac{1}{1-\varepsilon} + O\left(\frac{y}{\log y}\right) = x_1 \log \frac{1}{1-\varepsilon} + O\left(\frac{x_1}{\log x_1}\right).$$

Таким образом, $H_1 > \varepsilon x_1$ для всех достаточно больших y.

Возьмем любое число x_2, удовлетворяющее условию

$$y^2 \leqslant x_2 < y^{3-3\varepsilon},$$

и оценим снизу количество H_2 положительных целых чисел $n \leqslant x_2$, делящихся на произведение каких-либо двух простых p и q из интервала $y^{1-\varepsilon} < p$, $q \leqslant y$. При этом произведения pq и qp, отличающиеся порядком следования множителей, будем считать различными. Имеем

$$H_2 = \sum_{y^{1-\varepsilon} < p,q \leqslant y} \left[\frac{x_2}{pq}\right] = x_2 \left(\sum_{y^{1-\varepsilon} < p \leqslant y} \frac{1}{p}\right)^2 + O\left(\frac{y^2}{\log^2 y}\right) =$$

$$= x_2 \log^2 \frac{1}{1-\varepsilon} + O\left(\frac{x_2}{\log x_2}\right)$$

и, значит, $H_2 > \varepsilon^2 x_2$ для всех достаточно больших y.

Продолжая эти рассуждения, находим, что если $x = x_s$ — любое число, удовлетворяющее условию

$$y^s \leqslant x < y^{s+1-(s+1)\varepsilon} = y^{s+\frac{1}{s+2}},$$

и H_s — количество положительных целых чисел $n \leqslant x$, делящихся на произведение s простых $p_1, \ldots, p_s$ из интервала $y^{1-\varepsilon} < p_1, \ldots, p_s \leqslant y$ (считая за различные произведения, отличающиеся порядком следования множителей), то

$$H_s > \varepsilon^s x_s = \frac{x}{(s+2)^s}$$

для всех достаточно больших y. Стало быть, если x, y удовлетворяют условиям (1), то

$$H(x, y) \geqslant \frac{H_s}{s!} \geqslant \frac{x}{s!\,(s+2)^s}.$$

Но

$$s!\,(s+2)^s \leqslant \exp\left(c \frac{\log x}{\log y} \log \frac{\log x}{\log y}\right).$$

и, значит,

$$H(x, y) \geqslant x \exp\left(-c \frac{\log x}{\log y} \log \frac{\log x}{\log y}\right).$$

Лемма доказана.

Обозначим $N(p \leqslant x,\ n(p) > y)$ количество простых чисел $p \leqslant x$, для которых наименьший положительный квадратичный невычет $n(p)$ превосходит y.

Теорема 2 [73b]. *Имеет место неравенство*

$$N(p \leqslant x,\ n(p) > y) \leqslant \exp\left(c \frac{\log x}{\log y} \log \frac{\log x}{\log y}\right),$$

где $c > 0$ — некоторая константа.

Доказательство. В качестве последовательности

$$n_1, n_2, \ldots, n_H, \tag{2}$$

участвующей в формулировке теоремы 1, возьмем последовательность положительных целых чисел $n \leqslant x^2$, все простые делители которых не превосходят y. Пусть простое число $p \leqslant x$ таково, что $n(p) > y$. Тогда все простые, не превосходящие y, являются квадратичными вычетами по модулю p, а поскольку произведение любого количества квадратичных вычетов снова является квадратичным вычетом, то каждое из чисел последовательности (2) либо является квадратичным вычетом по модулю p, либо делится на p. Значит, для всякого простого числа $p \leqslant x$, для которого $n(p) > y$, элементы последовательности (2) принадлежат самое большее $(p+1)/2$ классам вычетов по модулю p. Далее, имеем

$$\frac{p+1}{2} < p\left(1 - \frac{1}{4}\right)$$

и тогда каждое такое простое число является исключительным с параметром $\tau = 1/4$. Отсюда, ввиду теоремы 1, получаем для величины $N(p \leqslant x,\ n(p) > y)$ оценку

$$N(p \leqslant x,\ n(p) > y) \leqslant c' \frac{x^2}{H},$$

где $H = H(x^2, y)$ — количество положительных целых чисел $n \leqslant x^2$, делящихся лишь на простые числа, не превосходящие y.

По лемме 4 имеем

$$H \geqslant x^2 \exp\left(-c'' \frac{\log x}{\log y} \log \frac{\log x}{\log y}\right)$$

и, стало быть,

$$N(p \leqslant x,\ n(p) > y) \leqslant \exp\left(c \frac{\log x}{\log y} \log \frac{\log x}{\log y}\right).$$

Теорема доказана.

Задачи

1. Доказать, что число 2 является наименьшим квадратичным невычетом для простых p вида $p = 8k + 3$ и $p = 8k + 5$.

2. Вывести из теоремы 2, что при заданном $\varepsilon > 0$ и всех достаточно больших x количество простых p, принадлежащих отрезку $[x^\varepsilon, x]$ и удовлетворяющих условию $n(p) > p^\varepsilon$, не превосходит константы $c = c(\varepsilon)$.

3. Вывести из теоремы 2, что при любом заданном $\varepsilon > 0$ и всех достаточно больших x справедливо неравенство

$$N(p \leqslant x,\ n(p) > p^\varepsilon) \leqslant c(\varepsilon) \log\log x.$$

4*. Установить, что для справедливости оценки $n(p) = O(p^\varepsilon)$ достаточно выполнимости неравенства

$$\left|\sum_{xy \leqslant N} \left(\frac{xy}{p}\right)\right| \leqslant c p^{1/2+\varepsilon},$$

где N — любое число из отрезка $[p \log^{-2} p,\ p \log^2 p]$.

5. Пусть $s > 0$, $0 < \alpha \leqslant 1$ — произвольные действительные числа, $f(n)$ — мультипликативная функция с условием $|f(n)| \leqslant 1$, $g(x)$ — периодическая с периодом 1 функция и $P_s(\alpha)$ — множество целых чисел n из интервала $1 \leqslant n \leqslant \alpha x$, все простые делители которых не превосходят $x^{1/s}$. Доказать, что

$$\left|\sum_{n \in P_s(\alpha)} \frac{f(n)\, g(n\theta)}{n}\right| \leqslant (2s)^s \max_{\substack{1 \leqslant h \leqslant x, \\ 0 \leqslant \theta \leqslant 1}} \left|\sum_{m=1}^{h} \frac{f(m)\, g(m\theta)}{m}\right|.$$

6* (Ю. В. Линник, А. А. Реньи [74]). Пусть p — простое число вида $p = 4k + 1$. Доказать, что если гипотеза Виноградова о том, что

$$n(p) < p^{1/s}$$

при любом $s > 0$ и $p > p_0(s)$, не верна, то имеет место оценка

$$\max_{1 \leqslant h \leqslant p-1} \left|\sum_{m=1}^{h} \left(\frac{m}{p}\right)\right| \leqslant (2s)^{s+2} p^{1/2}.$$

(Указание. Разложить функцию

$$S(x) = \sum_{1 \leqslant m \leqslant xp} \left(\frac{m}{p}\right)$$

в ряд Фурье и для оценки величины

$$\left|S\left(\frac{h}{p}\right)\right| = \left|\sum_{m=1}^{h} \left(\frac{m}{p}\right)\right|$$

воспользоваться неравенством

$$\left|\sum_{n=1}^{N} \frac{\sin n\theta}{n}\right| \leqslant \frac{\pi}{2} + 1,$$

справедливым при любом $N \geqslant 1$, представлением

$$\sum_{n=1}^{p} \left(\frac{n}{p}\right) \frac{\sin 2\pi n\theta}{n} = \sum_{n \in P_s(1)} \frac{\sin 2\pi n\theta}{n} + \sum_{m \in Q_s(1)} \frac{\left(\frac{m}{p}\right)}{m} \sum_{n \in P_s\left(\frac{1}{m}\right)} \frac{\sin 2\pi mn\theta}{n},$$

где $Q_s(\alpha)$ — множество целых чисел m из интервала $1 \leqslant m \leqslant \alpha x$, все простые делители которых больше $x^{1/s}$, и результатом предыдущей задачи с $f(n) \equiv 1$ и $g(x) = \sin 2\pi x$.)

7* (Ю. В. Линник, А. А. Реньи [74]). Пусть p — простое число вида $p = 4k + 1$. Доказать, что если гипотеза Виноградова о том, что

$$r(p) < p^{1/s}$$

при любом $s > 0$ и $p > p_0(s)$, не верна, то

$$\max_{1 \leqslant h \leqslant p-1} \left|\sum_{m=1}^{h} \left(\frac{m}{p}\right)\right| \leqslant c(s)\, p^{1/2}.$$

(Указание. Разложить функцию

$$S(x) = \sum_{1 \leqslant m \leqslant xp} \left(\frac{m}{p}\right)$$

в ряд Фурье и для оценки величины

$$\left|S\left(\frac{h}{p}\right)\right| = \left|\sum_{m=1}^{h} \left(\frac{m}{p}\right)\right|$$

воспользоваться оценкой Дэвенпорта [48d]

$$\sum_{n=1}^{N} \mu(n)\, e^{2\pi i n\theta} = O\left(\frac{N}{\log^A N}\right),$$

равномерной по θ и справедливой для любого $A > 0$, формулой суммирования Абеля, представлением

$$\sum_{n=1}^{p} \left(\frac{n}{p}\right) \frac{\sin 2\pi n\theta}{n} = \sum_{l^2 \leqslant p} \frac{1}{l^2} \left(\sum_{n \in P_s\left(\frac{1}{l^2}\right)} \frac{\mu(n) \sin 2\pi l^2 n\theta}{n} + \right.$$

$$\left. + \sum_{m \in Q_s(1)} \left(\frac{m}{p}\right) \frac{1}{m} \sum_{n \in P_s\left(\frac{1}{ml^2}\right)} \frac{\mu(n) \sin 2\pi l^2 mn\theta}{n} \right)$$

и результатом задачи 5 с $f(n) = \mu(n)$ и $g(x) = \sin 2\pi x$.)

8. Пусть $D_n = \{P_1, \ldots, P_n\}$ — произвольное множество из $n \geqslant 3$ различных точек $P_i = (x_i, y_i)$, $1 \leqslant i \leqslant n$, лежащих в единичном квадрате

$0 \leqslant x, y \leqslant 1$; $\Delta(P_i, P_j, P_k)$ — площадь треугольника с вершинами в точках P_i, P_j, P_k и

$$\Delta_n = \sup_{D_n} \min_{1 \leqslant i < j < k \leqslant n} \Delta(P_i, P_j, P_k).$$

Доказать справедливость неравенства $\Delta_n \geqslant c/n^2$, где $c > 0$ — некоторая абсолютная константа.

(Указание. Рассмотреть простое число p, $n \leqslant p \leqslant 2n$, кривую $y \equiv x^2 \pmod p$ и три произвольные различные точки $P_1 = (x_1, x_1^2)$, $P_2 = (x_2, x_2^2)$, $P_3 = (x_3, x_3^2)$, лежащие на этой кривой. Показать, что $\Delta(P_1, P_2, P_3) \geqslant 1/2$ и, преобразовав квадрат $0 \leqslant x, y \leqslant p-1$ в квадрат $0 \leqslant x, y \leqslant 1$, получить требуемое неравенство.)

9*. Последовательность целых чисел $a_1, \ldots, a_m$ называется *B_s-последовательностью*, если все суммы $a_{i_1} + \ldots + a_{i_s}$, $1 \leqslant i_1 \leqslant \ldots \leqslant i_s \leqslant m$, $s \geqslant 2$, различны между собой. Пусть $F_s(x)$ — максимальное число членов B_s — последовательности, лежащей в интервале $0 \leqslant a \leqslant x$. Доказать справедливость следующих утверждений:

а) Если p — простое число и $q = p^r$, то для каждого $s \geqslant 2$ найдутся целые $a_1, \ldots, a_m$, $1 \leqslant a_i < q^s$, $1 \leqslant i \leqslant m$, такие, что все суммы

$$a_{i_1} + \ldots + a_{i_s}, \quad 1 \leqslant i_1 \leqslant \ldots \leqslant i_s \leqslant m,$$

различны по mod $(q^s - 1)$.

(Указание. Пусть $\alpha_1 = 0, \alpha_2, \ldots, \alpha_q$ — все различные элементы конечного поля F_q, состоящего из $q = p^r$ элементов, и θ — примитивный элемент поля F_{q^s} (т. е. $F_{q^s} = F_q(\theta)$). Пусть, далее, $\theta^{a_i} = \theta + \alpha^i$, $0 \leqslant a_i < q$, $1 \leqslant i \leqslant m$. Показать, что числа $a_1, \ldots, a_m$ удовлетворяют требуемому условию. Для этого предположить, что

$$a_{i_1} + \ldots + a_{i_s} = a_{j_1} + \ldots + a_{j_s}$$

для двух различных наборов $(i_1, \ldots, i_s)$ и $(j_1, \ldots, j_s)$, и, воспользовавшись тем, что θ не может быть корнем никакого многочлена из кольца $F_q[x]$ степени, меньшей s, прийти к противоречию.)

б) Если p — простое число, $q = p^r$ и $s \geqslant 2$, то

$$F_s(q^s) \geqslant q + 1.$$

(Указание. Пусть $a_1, \ldots, a_m$ — целые числа, определенные в п. а). Показать, что последовательность

$$a_1, a_2, \ldots, a_m, a_{m+1} = q^s$$

представляет собой B_s-последовательность. Для этого предположить, что

$$a_{i_1} + \ldots + a_{i_s} = a_{j_1} + \ldots + a_{j_s} \qquad (*)$$

для некоторых различных наборов $(i_1, \ldots, i_s)$ и $(j_1, \ldots, j_s)$. Обозначив μ_i количество появлений a_i в левой части, а ν_i — количество появлений a_i в правой части равенства $(*)$, показать, что $(\mu_1, \ldots, \mu_{m+1}) \neq (\nu_1, \ldots, \nu_{m+1})$ и что

$$\mu_1 + \ldots + \mu_{m+1} = \nu_1 + \ldots + \nu_{m+1} = s.$$

Заменив в соотношении $(*)$ каждое a_{m+1} на a_1 и рассмотрев это соотношение по mod $(q^s - 1)$, прийти к противоречию с результатом п. а), за исключением случая, когда $(\mu_1 + \mu_{m+1}, \mu_2, \ldots, \mu_m) = (\nu_1 + \nu_{m+1}, \nu_2, \ldots, \nu_m)$. В этом случае установить, что $\mu_1 = \nu_1 - \tau$, $\mu_2 = \nu_2, \ldots, \mu_m = \nu_m$, $\mu_{m+1} = \nu_{m+1} + \tau$ при некотором целом $\tau \neq 0$, и прийти к противоречию с условием $a_{i_1} + \ldots + a_{i_s} = a_{i_1} + \ldots + a_{j_s}$.)

в) Имеет место неравенство

$$\lim_{x \to \infty} \inf \frac{F_s(x)}{x^{1/s}} \geqslant 1.$$

(Указание. Воспользоваться результатом п. а) при $r = 1$ и получить оценку

$$F_s(p^s) \geqslant p + 1.$$

Рассмотреть соседние простые числа p и p' такие, что $p \leqslant x^{1/s} \leqslant p'$, и воспользоваться результатом Ингама о том, что

$$p' - p = O(p^{5/8+\varepsilon})$$

при любом $\varepsilon > 0$ (см., например, [142b, гл. V]).)

г) Выполняется неравенство

$$F_2(x) < x^{1/2} + x^{1/4} + 1.$$

(Указание. Пусть $a_1, \ldots, a_m$ есть B_2-последовательность и пусть

$$1 \leqslant a_1 < \ldots < a_m \leqslant x.$$

Тогда все разности $a_j - a_i$, $1 \leqslant i < j \leqslant m$, различны между собой. Назовем число $j - i$ *порядком разности* $a_j - a_i$. Пусть $a_{i_1} - a_{i_2}, a_{i_2} - a_{i_3}, \ldots, i_1 - i_2 = i_2 - i_3 = \ldots = \tau$ — все разности порядка $\tau > 0$. Показать, что сумма всех разностей порядка τ не превосходит величины τx. Вывести отсюда, что сумма всех положительных разностей порядка $\leqslant \mu$, где $1 \leqslant \mu \leqslant m$, не превосходит величины $\frac{1}{2}\mu(\mu+1)x$. Далее, показать, что число таких разностей есть $\mu m - \frac{1}{2}\mu(\mu+1) = \mu\nu$, где $\nu = m - \frac{1}{2}(\mu+1)$, и вывести отсюда, что сумма всех положительных разностей порядка $\leqslant \mu$ не меньше, чем $\frac{1}{2}\mu\nu(\mu\nu+1)$. В результате получить неравенство

$$\mu^2\nu^2 < \mu(\mu+1)x,$$

из которого следует, что

$$m < \frac{1}{2}(\mu+1) + \left(1 + \frac{1}{2\mu}\right)x^{1/2}.$$

Наконец, взять $\mu = [x^{1/4}] + 1$.)

10*. Гипотеза Боуза — Чоулы (см. [20]). В обозначениях задачи 9 при любом $s \geqslant 2$ выполняется соотношение

$$\lim_{x \to \infty} \frac{F_s(x)}{x^{1/s}} = 1.$$

(При $s = 2$ справедливость этой гипотезы следует из результатов предыдущей задачи.)

ИСТОРИЧЕСКИЕ КОММЕНТАРИИ К ГЛАВАМ I И II

Без всякого преувеличения можно сказать, что теория сравнений составляет основу классической теории чисел. Фундамент этой теории был заложен в работах Ферма, Эйлера и Лагранжа. Первое систематическое изложение теории сравнений было дано Гауссом (см. [30a], а также [30c]). Полученные им результаты приведены в § 1 гл. I.

Из задачи 7 § 1 гл. I следует, что вопрос о количестве решений алгебраического сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \pmod m$$

по составному модулю $m = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ сводится, в силу свойства мультипликативности, к аналогичному вопросу для сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^\alpha}$$

по модулю p^α, равному степени простого числа p. В свою очередь, при определенных условиях невырожденности, последний вопрос сводится к вопросу о количестве решений сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \pmod p$$

по простому модулю p. Тем самым сравнения по простому модулю составляют фундамент теории алгебраических сравнений.

Исторически объектом первых исследований в теории алгебраических сравнений по простому модулю явились сравнения

$$f(x, y) \equiv 0 \pmod p \tag{1}$$

с двумя неизвестными. При доказательстве своей знаменитой теоремы о представимости всякого целого положительного числа в виде суммы четырех квадратов Лагранжу [67] потребовалось утверждение о том, что сравнение

$$x^2 + y^2 + 1 \equiv 0 \pmod p \tag{2}$$

разрешимо. Обратим внимание на доказательство этого утверждения, предложенное Лагранжем. Предположим, что указанное сравнение не имеет решений. Тогда, по критерию Эйлера, сравнение

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

должно иметь p решений. Но степень последнего сравнения равна $p-1$ и по теореме Лагранжа оно не может обладать более чем $p-1$ решениями. Полученное противоречие показывает, что сравнение (2) имеет хотя бы одно решение.

Указанный метод Лагранжа был применен Аладовым [3] при изучении вопроса о распределении пар квадратичных вычетов и невычетов. В частности, для количества N_p решений сравнения

$$y^2 \equiv x(x+1) \pmod p$$

им была получена формула

$$N_p = p - (-1)^{\frac{p-1}{2}}.$$

К сожалению, этот метод к концу 19-го столетия был совершенно забыт. Например, последним учебником, в котором изложен метод Лагранжа, является учебник Т. Л. Чебышева «Теория сравнений» [143].

Широкое изучение квадратичных сравнений было предпринято Гауссом [30a, 30b]. Им также были получены точные формулы для количества N_p

решений некоторых кубических и биквадратичных сравнений. Последняя запись в дневнике Гаусса (см. [30b], с. 271) содержит предположение о том, что для количества N_p решений биквадратичного сравнения

$$x^2y^2 + x^2 + y^2 \equiv 1 \pmod p$$

при простом $p = 4k+1$ имеет место формула

$$N_p = (a-1)^2 + 4b^2 - 4,$$

где целые a и b однозначно, с точностью до знака, определяются из представления простого числа p в виде суммы двух квадратов

$$p = a^2 + 4b^2.$$

Это предположение было доказано Херглотцем [134] в 1921 г. при помощи арифметической теории эллиптических функций. Элементарное доказательство результата Херглотца можно найти в книге Хассе [133c].

Весьма эффективная теория эллиптических сравнений частного вида

$$y^2 \equiv x^3 + ax \pmod p, \quad y^2 \equiv x^3 + b \pmod p$$

и связанных с ними сумм

$$\sum_{x=1}^{p} \left(\frac{x^3+ax}{p}\right), \quad \sum_{x=1}^{p} \left(\frac{x^3+b}{p}\right) \tag{3}$$

(см. задачи 15, 16 из § 1 гл. I) была развита Якобсталем [154]. В качестве следствия им было получено явное представление простого числа $p = 4k+1$ в виде суммы двух квадратов. Со свойствами более широкого класса сумм типа (3), называемых суммами Якобсталя, можно познакомиться по работе [123].

Классы вычетов по простому модулю p образуют конечное поле F_p. Поэтому сравнение (1) можно трактовать как алгебраическое уравнение

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

над полем F_p. В 1908 г. на Всемирном конгрессе математиков Пуанкаре [100] высказал мысль, что для изучения сравнений от двух неизвестных можно применить методы теории алгебраических функций. Осуществление этой программы началось с работы Е. Артина [5a], опубликованной им в 1924 г. В этой работе, по аналогии с теорией квадратичных расширений поля рациональных чисел $\mathbb{Q}$, Артин построил теорию квадратичных расширений $F_p(x, \sqrt{f})$ поля рациональных функций $F_p(x)$, получаемых присоединением к полю $F_p(x)$ корней сравнения

$$y^2 \equiv f(x) \pmod p, \tag{4}$$

где f — бесквадратный по модулю p целочисленный многочлен степени $n \geqslant 3$. В частности, им была введена в рассмотрение *ζ-функция поля* $F_p(x, \sqrt{f})$

$$\zeta(s) = \prod_{\mathfrak{p}} (1 - (N\mathfrak{p})^{-s})^{-1}, \tag{5}$$

являющаяся аналогом ζ-функции Дедекинда квадратичных расширений поля $\mathbb{Q}$ (подробности см. в следующей главе), и сделано предположение о том, что для ζ-функции (5) справедлива гипотеза Римана.

Это предположение приводит к следующей оценке для количества N_p решений сравнения (4):

$$|N_p - p| \leqslant \begin{cases} (n-1)\,p^{1/2}, & \text{если } n \text{ нечетное}, \\ (n-2)\,p^{1/2}, & \text{если } n \text{ четное}. \end{cases} \tag{6}$$

Задача о числе решений сравнения (4) очевидным образом сводится к оценке суммы символов Лежандра

$$S = \sum_{x=1}^{p} \left(\frac{f(x)}{p}\right). \tag{7}$$

При этом *гипотеза Артина* приводит к неравенству

$$|S| \leqslant 2\left[\frac{n-1}{2}\right] p^{1/2}.$$

Для оценки сумм (7) Хопфом [138], Дэвенпортом [48a, 48b, 48c] и Морделлом [89c, 89d] был использован *метод кратных сумм* (см. задачи 1 и 2 из § 5 гл. I). Сущность этого метода состоит в отыскании в пространстве параметров $\alpha_1, \ldots, \alpha_n$ множества преобразований T, оставляющих неизменным модуль суммы

$$S(\alpha_1, \ldots, \alpha_n) = \sum_{x=1}^{p} \left(\frac{(x+\alpha_1)\ldots(x+\alpha_n)}{p}\right),$$

и в нахождении верхней границы для среднего значения

$$\widetilde{S} = \sum_{\alpha_1,\ldots,\alpha_n=1}^{p} |S(\alpha_1, \ldots, \alpha_n)|^{2r}.$$

Если удастся найти достаточно много таких преобразований T и точно оценить величину $\widetilde{S}$, то для индивидуальной суммы $S(\alpha_1, \ldots, \alpha_n)$ также получается достаточно хорошая оценка. Однако методом кратных сумм гипотеза Артина не только не была доказана, но даже не был получен истинный порядок оценки по p. По сути дела метод кратных сумм в задачах теории сравнений по простому модулю — это лишь проявление общего метода аналитической теории чисел без учета специфики поля классов вычетов по модулю p, а именно, наличия в нем автоморфизма Фробениуса. Именно этим, по-видимому, объясняется тот факт, что метод кратных сумм не приводит к оптимальным результатам.

В 1936 г. Хассе [133b] (см. также [133d]) на основе развитой им теории алгебраических функций с конечным полем констант доказал гипотезу Артина для многочленов $f(x)$ степени 3 и 4. Элементарное доказательство оценки Хассе

$$|N_p - p| < 2p^{1/2}$$

для количества N_p решений сравнения

$$y^2 \equiv x^3 + ax + b \pmod{p} \tag{8}$$

было предложено Ю. И. Маниным [81a] в 1956 г.

А. Вейль [23d] дал широкое обобщение результата Хассе и для количества N_q решений уравнения

$$f(x, y) = 0 \tag{9}$$

в элементах x, y конечного поля F_q (в случае абсолютно неприводимого многочлена $f(x, y)$) получил оценку

$$|N_q - q| \leqslant 2g\sqrt{q}, \tag{10}$$

где g — род кривой (9). Это позволило ему доказать функциональный аналог гипотезы Римана для ζ-функций абсолютно неприводимых алгебраических кривых, определенных над конечными полями. В качестве следствия

этого результата рядом авторов [23d, 23e, 58, 16a, 57, 98, 96a, 96b] были получены оценки сумм характеров

$$\left|\sum_{x\in F_{q^\nu}} \chi_\nu(f(x))\right| \leqslant c(f)\, q^{\nu/2}$$

и тригонометрических сумм

$$\left|\sum_{\substack{x\in F_{q^\nu}\\ g(x)\neq 0}} e^{2\pi i \frac{\mathrm{tr}(\mathrm{tr}_\nu g(x))}{p}}\right| \leqslant c(g)\, q^{\nu/2}$$

с рациональной функцией $g(x)$.

Доказательство Вейля оценки (10) весьма сложно. В частности, оно потребовало пересмотра основ классической алгебраической геометрии. В рамках классической теории алгебраических функций доказательство оценки Вейля дано в работах [106a], [133d] и [150b]. Наилучший из имеющихся сейчас вариантов алгебро-геометрического доказательства этого результата содержится в работе [83] и в монографии [70a] (см. также [132, с. 463, задача 1.10]).

В 1967 г. А. Г. Постников заметил, что все элементы $x \in F_p$, дающие решения сравнения (8) и удовлетворяющие условию $x^3 + ax + b \not\equiv 0 \pmod{p}$, являются, по меньшей мере, двухкратными корнями многочлена

$$R(x) = 2(x^3 + ax + b)\left(1 - (x^3 + ax + b)^{\frac{p-1}{2}}\right) + (3x^2 + a)(x^p - x),$$

совпадающего по $\mathrm{mod}\,(x^p - x)^2$ с числителем первой рациональной функции в конструкции Манина [81a]. Сравнение числа корней (с учетом их кратности) многочлена $R(x)$ с его степенью позволило А. Г. Постникову получить для количества N_p решений сравнения (8) оценку $N_p \leqslant \frac{3}{2}(p+1)$. Аналогичные рассмотрения для многочлена

$$Q(x) = 2(x^3 + ax + b)\left(1 - (x^3 + ax + b)^{\frac{p-1}{2}}\right) + (3x^2 + a)(x^p - x)$$

привели его к неравенству $N_p \geqslant \frac{1}{2}(p-3)$, из которого следует, в частности, что при $p > 3$ сравнение (8) всегда разрешимо. Заметим, что для квадратичного сравнения

$$y^2 \equiv ax^2 + bx + c \pmod{p}$$

такая конструкция приводит к точному ответу (см. задачу 5 из § 5 гл. I).

Начиная с 1969 г., автором [117b — 117j] разрабатывался элементарный метод доказательства оценки (10), базирующийся на конструкциях, аналогичных конструкциям Манина — Постникова, и идейно близкий к методу Туэ [122] (см. также задачу 4 из § 1 гл. VI) в теории диофантовых приближений. В основе этого метода лежит построение многочленов от переменного x не слишком высокой степени, для которых элементы $x \in F_q$, связанные с решениями уравнения (9), являются корнями достаточно высокой кратности. Сравнение числа корней этих многочленов с их степенями приводит к асимптотике вида (10) для количества решений уравнения (9). В разработке этого метода приняли также участие Н. М. Коробов [63], Старк [116a], В. Шмидт [146f — 146h], Митькин [87] и Бомбьери [16b — 16c]. Наи-

более простой вариант метода был предложен Бомбьери за счет отказа от явных конструкций и привлечения теоремы Римана — Роха. Его результат будет изложен в гл. III. Следует отметить, однако, что явные конструкции обладают тем преимуществом, что с их помощью в некоторых случаях удается получить более сильные оценки, чем те, которые эквивалентны функциональному аналогу гипотезы Римана. Например, в работе [63] при нечетном $n \geqslant 5$ и $p > (n^2+9)/2$ для количества N_p решений сравнения (4) получена оценка

$$|N_p - p| \leqslant (n-1)\left(p - \frac{(n-3)(n-4)}{4}\right)^{1/2},$$

которая усиливает неравенство (6) при достаточно больших n. Другие результаты, улучшающие оценку (6) при $n \asymp p^{1/2}$, получены в работах [116a, 118].

В дополнение к изложенным в § 6 и § 7 результатам о распределении степени вычетов и невычетов отметим следующие факты.

Из расширенной гипотезы Римана для L-рядов Дирихле следует [152], что для наименьшего квадратичного невычета $n(p)$ справедлива оценка

$$n(p) = O(\log^2 p).$$

С другой стороны, из теоремы Линника [73c] о наименьшем простом в арифметической прогрессии легко выводится (см., например, [109, 130]), что

$$n(p) > c \log p$$

для бесконечно многих простых p.

Аналогичный результат

$$n_k(p) > c(k) \log p$$

имеет место и для наименьшего невычета степени $k > 2$ по модулю p.

В работе [151b] Эллиот установил, что при любом $\varepsilon > 0$ и при некоторой положительной константе $c_1 = c_1(\varepsilon)$ неравенство

$$n(p) > c_1 \log p$$

выполняется по меньшей мере для $x^{1-\varepsilon}$ простых $p \leqslant x$. В этой же работе им показано, что при любом $\delta > 0$ и при некотором $\nu = \nu(\delta) > 0$ неравенство

$$n(p) > \log^{1+\delta} p$$

выполняется для менее, чем $c_2(\delta)x^{1-\nu}$ простых $p \leqslant x$. Это привело его к предположению о том, что при любом $\varepsilon > 0$ справедлива оценка

$$n(p) \leqslant c(\varepsilon) \log^{1+\varepsilon} p.$$

Отметим, что из расширенной гипотезы Римана следует [88, с. 114], что

$$n(p) > c \log p \log\log p$$

для бесконечно многих простых p.

В заключение отметим результат Эрдеша [153] о поведении величины $n(p)$ в среднем. Именно, если $\pi(x)$ означает количество простых $p \leqslant x$, то справедливо соотношение

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leqslant x} n(p) = \text{const}.$$

Вывод этого результата основан на использовании большого решета Линника.

Заметим также, что при любом $\varepsilon > 0$ для величины $r(p)$ справедлива [26] оценка

$$r(p) = O(p^{1/4+\varepsilon}).$$

ГЛАВА III

РАЦИОНАЛЬНЫЕ ТОЧКИ НА АЛГЕБРАИЧЕСКИХ КРИВЫХ

§ 1. Рациональные кривые

1. Плоские алгебраические кривые. Пусть k — алгебраически замкнутое поле и k_0 — некоторое подполе поля k. Обозначим $\mathbb{A}^2$ *аффинную плоскость* над полем k, представляющую собой множество всех наборов (α, β) элементов α, β поля k. Набор $P = (\alpha, \beta)$ будем называть *точкой* плоскости $\mathbb{A}^2$, а элементы α, β — координатами точки P.

Плоской алгебраической кривой называется множество всех точек $P = (x, y) \in \mathbb{A}^2$, координаты которых удовлетворяют уравнению

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

где $f(x, y)$ — многочлен с коэффициентами из поля k. Если коэффициенты многочлена $f(x, y)$ принадлежат полю k_0, то говорят, что кривая (1) *определена над полем* k_0.

Точка $P = (x, y)$ кривой (1) называется *k_0-рациональной*, если ее координаты x, y принадлежат полю $k_0 \subset k$.

В дальнейшем нас будут интересовать следующие два случая.

1) Поле k совпадает с полем комплексных чисел $\mathbb{C}$ и k_0 является полем рациональных чисел $\mathbb{Q}$. В этом случае вопрос о множестве $\mathbb{Q}$-рациональных точек кривой (1), определенной над $\mathbb{Q}$, эквивалентен вопросу о множестве решений уравнения $f(x, y) = 0$ в рациональных числах x, y.

2) Поле k_0 является конечным полем F_q, состоящим из $q = p^r$ элементов (p — простое число), и $k = \bar{F}_q$ — его алгебраическое замыкание. В этом случае множество F_q-рациональных точек кривой (1), определенной над F_q, совпадает с множеством решений уравнения $f(x, y) = 0$ в элементах x, y поля F_q. В частности, если F_p — простое конечное число, то вопрос о F_p-рациональных точках кривой (1) равносилен вопросу о решениях сравнения $f(x, y) \equiv 0 \pmod p$.

Если многочлен $f(x, y)$ представляется в виде произведения $f = g \cdot h$ многочленов $g(x, y)$ и $h(x, y)$, то определяемая многочленом $f(x, y)$ кривая является объединением двух кривых, задаваемых уравнениями $g(x, y) = 0$ и $h(x, y) = 0$ соответственно. В случае, когда многочлен $f(x, y)$ неприводим, определяемая

им кривая называется *неприводимой*. Поскольку каждый многочлен раскладывается в произведение конечного числа неприводимых многочленов, то каждая плоская алгебраическая кривая, определенная над полем k_0, является объединением конечного числа неприводимых кривых, называемых ее *неприводимыми* компонентами. При этом может оказаться, что неприводимая компонента алгебраической кривой определена не над полем k_0, а над некоторым его собственным конечным расширением $k' \subset k$. Нам удобно исключить такую возможность и ограничиться рассмотрением класса плоских алгебраических кривых, все неприводимые компоненты которых также определены над полем k_0. В этом случае задача сводится к изучению неприводимых алгебраических кривых, определенных над k_0 и обладающих тем свойством, что они остаются неприводимыми над каждым конечным расширением поля k_0. Такие неприводимые алгебраические кривые называются *абсолютно неприводимыми*.

В дальнейшем под плоской неприводимой кривой, определенной над полем k_0, всегда будем понимать абсолютно неприводимую алгебраическую кривую.

2. Параметризация кривых. Плоская алгебраическая кривая (1) называется *рациональной*, если существуют такие рациональные функции $x(t)$ и $y(t)$, не являющиеся одновременно константами, что

$$f(x(t),\ y(t)) = 0$$

тождественно относительно параметра t. Если $t = t_0$ — значение параметра t, при котором знаменатели рациональных функций $x(t)$ и $y(t)$ отличны от нуля, то точка $P_0 = (x(t_0),\ y(t_0))$ лежит, очевидно, на рассматриваемой рациональной кривой. Это не означает, однако, что, придавая параметру t все допустимые значения, можно, исходя из заданной параметризации $x(t)$, $y(t)$, получить все точки (x, y) кривой (1).

Пример 1. Окружность $x^2 + y^2 = 1$ обладает параметризациями

$$x(t) = \frac{1-t^2}{1+t^2}, \quad y(t) = \frac{2t}{1+t^2}$$

и

$$x'(t) = \frac{1-t^4}{1+t^4}, \quad y'(t) = \frac{2t^2}{1+t^4}.$$

Первая из этих параметризаций при $t \in \mathbb{R} \cup \{\infty\}$ дает все точки окружности, в то время как вторая параметризация приводит лишь к точкам верхней полуокружности: $x^2 + y^2 = 1$, $y \geqslant 0$.

Рассмотренный пример в достаточной степени отражает общую ситуацию. Именно, нетрудно показать (см. [144b, гл. 1, § 1]), что каждая рациональная кривая обладает такой параметризацией $x(t)$, $y(t)$, которая задает взаимно однозначное соответствие между всеми значениями параметра t и всеми точками (x, y) этой кривой, кроме некоторого конечного множества значений t и некоторого конечного множества точек (x, y). Предположим теперь, что коэффициенты многочлена $f(x, y)$ и рациональных функций $x(t)$, $y(t)$ принадлежат полю k_0. Если функции $x(t)$, $y(t)$ задают описанную только что параметризацию кривой (1) и параметр t пробегает все элементы поля k_0, в которых функции $x(t)$, $y(t)$ определены, то наборы $(x(t),\ y(t))$ исчерпывают все k_0-рациональные точки рассматриваемой кривой, за исключением, быть может, конечного их числа. Тем самым указание подходящей параметризации рациональной кривой приводит к описанию множества ее k_0-рациональных точек.

Приведем некоторые примеры рациональных кривых. *Степенью* неприводимой кривой (1) назовем степень определяющего кривую многочлена $f(x, y)$. Кривые степени 1, т. е. прямые, являются, очевидно, рациональными кривыми.

Докажем, что кривая степени 2 рациональна. Возьмем на кривой (1) произвольную точку $P_0 = (x_0,\ y_0)$ и проведем через нее прямую

$$y - y_0 = t(x - x_0)$$

с угловым коэффициентом t. Найдем точки пересечения кривой и этой прямой. Для этого достаточно подставить

$$y = y_0 + t(x - x_0) \tag{2}$$

в уравнение (1). Многочлен

$$f(x,\ y_0 + t(x - x_0))$$

имеет степень 2 и, если положить

$$f(x,\ y_0 + t(x - x_0)) = A(t)x^2 + B(t)x + C(t),$$

где A, B, C — многочлены от t, то для определения x получим уравнение

$$A(t)x^2 + B(t)x + C(t) = 0.$$

Нам известен один корень $x = x_0$ этого уравнения. Поэтому другой корень x однозначно определяется из соотношения

$$x + x_0 = -\frac{B(t)}{A(t)}.$$

Подставляя выражение

$$x = -x_0 - \frac{B(t)}{A(t)} \tag{3}$$

в уравнение (2), находим параметрическое представление

$$y = y_0 + t\left(-2x_0 - \frac{B(t)}{A(t)}\right) \tag{4}$$

второй координаты точки (x, y) кривой степени 2.

При построении параметризации кривой (1), имеющей степень 2, мы исходили из точки (x_0, y_0) этой кривой. Если коэффициенты многочлена $f(x, y)$ и координаты x_0, y_0 точки (x_0, y_0) принадлежат полю k_0, то коэффициенты рациональных функций (3), (4), дающих эту параметризацию, также принадлежат полю k_0. Тем самым можно указать общий вид k_0-рационального решения уравнения степени 2, если только известно хотя бы одно такое решение.

3. Алгебраические кривые второй степени. Вопрос о существовании хотя бы одного k_0-рационального решения является, как правило, довольно тонким. Дадим решение этого вопроса для случая $k_0 = F_q$ и для случая $k_0 = \mathbb{Q}$. В дальнейшем для удобства будем считать, что характеристика поля k_0 отлична от 2.

Любая неприводимая кривая степени 2, определенная над полем k_0, задается уравнением

$$Ax^2 + 2Bxy + Cy^2 + Dx + Ey + F = 0$$

с коэффициентами из k_0. Если определитель $\Delta = AC - B^2$ квадратичной формы $Ax^2 + 2Bxy + Cy^2$ равен нулю, то многочлен

$$f(x, y) = Ax^2 + 2Bxy + Cy^2 + Dx + Ey + F$$

с помощью невырожденного линейного преобразования переменных с коэффициентами из поля k_0 приводится либо к виду

$$ax^2 + y, \quad a \neq 0,$$

либо к виду

$$x^2 - c,$$

где c не является квадратом в поле k_0. Если же $\Delta \neq 0$, то многочлен $f(x, y)$ эквивалентен над полем k_0 многочлену

$$ax^2 + by^2 + c, \quad ab \neq 0.$$

Кривая $x^2 - c = 0$ не имеет k_0-рациональных точек. Существование k_0-рациональных точек на кривой $ax^2 + y = 0$ очевидно и поэтому остается рассмотреть вопрос о существовании k_0-рациональных точек на кривой

$$ax^2 + by^2 + c = 0, \quad ab \neq 0.$$

При $c = 0$ последнее уравнение имеет тривиальное решение $x = 0$, $y = 0$ и ввиду неприводимости кривой это решение является единственным его решением.

Теорема (Лагранж). *Если F_q — конечное поле характеристики $p \neq 2$ и a, b — отличные от нуля элементы этого поля, то уравнение*

$$ax^2 + by^2 + c = 0$$

разрешимо в поле F_q.

Доказательство. Запишем уравнение в виде

$$y^2 = \alpha x^2 + \beta, \quad \alpha \neq 0,$$

и допустим, что последнее уравнение не разрешимо в поле F_q. Тогда по критерию Эйлера (см. § 1 гл. I) многочлен

$$F(x) = 1 + (\alpha x^2 + \beta)^{\frac{q-1}{2}}$$

должен иметь в поле F_q точно q корней. Но степень многочлена $F(x)$ равна $q - 1$ и мы приходим в противоречие с тем, что число корней многочлена не превосходит его степени.

Перейдем к вопросу о существовании $\mathbb{Q}$-рациональных точек на кривой

$$ax^2 + by^2 + c = 0, \quad abc \neq 0. \tag{5}$$

Заметим сначала, что для разрешимости уравнения (5) в рациональных числах x, y необходимо, чтобы не все коэффициенты a, b, c были одного знака. Сделав, если это необходимо, замену переменных

$$x \mapsto \frac{1}{x}, \quad y \mapsto \frac{y}{x},$$

или

$$x \mapsto \frac{x}{y}, \quad y \mapsto \frac{1}{y}$$

можно привести уравнение (5) к виду

$$ax^2 + by^2 - c = 0, \quad a > 0, \quad b > 0, \quad c > 0. \tag{6}$$

Кроме того, можно считать, что a, b, c — взаимно простые в совокупности и свободные от квадратов целые числа.

Пусть $x = p/r$, $y = q/r$ — решение уравнения (6) в числах $x, y \in \mathbb{Q}$. Тогда уравнение

$$ax^2 + by^2 - cz^2 = 0, \quad a > 0, \quad b > 0, \quad c > 0, \tag{7}$$

обладает нетривиальным (отличным от $x = y = z = 0$) целочисленным решением $(x, y, z) = (p, q, r)$. Обратно, если уравнение (7) нетривиальным образом разрешимо в целых x, y, z, то имеем (7) нетривиальным образом разрешимо в целых x, y, z, то имеем $z \neq 0$ и тогда уравнение (6) разрешимо в рациональных числах x, y. Таким образом, вопрос о существовании рациональных точек на кривой (5) сводится (при выполнении указанного выше необходимого условия) к вопросу о нетривиальной разрешимости в целых числах x, y, z уравнения (7).

Если в уравнении (7) коэффициенты $a = da'$ и $b = db'$ имеют общий делитель $d > 1$, то, умножая форму $ax^2 + by^2 - cz^2$ на d и заменяя x, y на $x' = dx$, $y' = dy$, приходим к уравнению

$$a'x'^2 + b'y'^2 - cdz^2 = 0,$$

в котором a' и b' взаимно просты. Повторяя этот процесс несколько раз, получаем уравнение того же вида

$$a'x^2 + b'y^2 - c'z^2 = 0,$$

ложительные бесквадратные коэффициенты
заимно просты.
кандр). *Если a, b и c — попарно взаимно*
ные целые числа, свободные от квадратов,
равнение

$$ax^2 + by^2 - cz^2 = 0 \qquad (8)$$

зом разрешимо в целых числах x, y, z тогда
разрешимы сравнения

$$\begin{aligned} x^2 - bc &\equiv 0 \pmod a, \\ x^2 - ac &\equiv 0 \pmod b, \\ x^2 + ab &\equiv 0 \pmod c. \end{aligned} \qquad (9)$$

в о. Необходимость условий (9) очевидна.
ность.
либо нечетный простой делитель числа c.
г, что сравнение $ax^2 + by^2 \equiv 0 \pmod p$ имеет
ние, скажем $x = \alpha$, $y = \beta$. В таком случае
ладывается по модулю p на линейные мно-

$$= a\beta^{-2}(\beta x + \alpha y)(\beta x - \alpha y) \pmod p.$$

ие верно, разумеется, и для формы $ax^2 +$
ет место равенство (см. § 1 гл. I)

$$cz^2 = l_p(x, y, z)\, m_p(x, y, z) \pmod p, \qquad (10)$$

сленные линейные формы. Аналогичные ра-
и для нечетных простых делителей p ко-
также для $p = 2$, так как

$$-cz^2 = (ax + by - cz)^2 \pmod 2.$$

линейные формы $l(x, y, z)$ и $m(x, y, z)$,
авенства

$$\begin{aligned} y, z) &= l_p(x, y, z) \pmod p, \\ y, z) &= m_p(x, y, z) \pmod p \end{aligned}$$

лителей p коэффициентов a, b и c. Тогда
тучим

$$z^2 = l(x, y, z)\, m(x, y, z) \pmod{abc}. \qquad (11)$$

переменным x, y, z целые значения, удов-
м

$$\sqrt{bc}, \quad 0 \leqslant y < \sqrt{ac}, \quad 0 \leqslant z < \sqrt{ab}. \qquad (12)$$

рассмотрения тривиальный случай $a = b =$
верждение теоремы очевидно), то из попар-

ной взаимной простоты a, b и c следует, что не все числа $\sqrt{bc}$, $\sqrt{ac}$ и $\sqrt{ab}$ будут целыми. Значит, число наборов (x, y, z), удовлетворяющих условиям (12), строго больше, чем $\sqrt{ab} \cdot \sqrt{bc} \cdot \sqrt{ac} = abc$. Рассмотрим значения, принимаемые линейной формой $l(x, y, z)$ при этих значениях переменных. Так как число наборов (x, y, z) с условием (12) больше числа вычетов по модулю abc, то для двух различных наборов (x_1, y_1, z_1) и (x_2, y_2, z_2) имеем

$$l(x_1, y_1, z_1) \equiv l(x_2, y_2, z_2) \pmod{abc}.$$

Отсюда, в силу линейности формы $l(x, y, z)$, получаем, что при $x_0 = x_1 - x_2$, $y_0 = y_1 - y_2$, $z_0 = z_1 - z_2$ выполняется сравнение

$$l(x_0, y_0, z_0) \equiv 0 \pmod{abc}.$$

Следовательно, ввиду (11),

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc}. \qquad (13)$$

Поскольку для наборов (x_1, y_1, z_1) и (x_2, y_2, z_2) выполнены условия (12), то

$$|x_0| < \sqrt{bc}, \quad |y_0| < \sqrt{ac}, \quad |z_0| < \sqrt{ab},$$

и значит,

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Последнее неравенство совместимо со сравнением (13) лишь в случаях, когда

$$ax_0^2 + by_0^2 - cz_0^2 = 0,$$

либо когда

$$ax_0^2 + by_0^2 - cz_0^2 = abc.$$

Первый случай дает нетривиальное решение (x_0, y_0, z_0). Во втором случае существование нетривиального целочисленного решения уравнения (8) следует из тождества

$$ab\left(ax_0^2 + by_0^2 - cz_0^2 - abc\right) = a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c\left(z_0^2 + ab\right)^2.$$

Доказанный результат допускает некоторое уточнение. Именно, как показал Хольцер [137], уравнение (8) обладает, в случае его нетривиальной разрешимости, минимальным нетривиальным целочисленным решением (x, y, z), удовлетворяющим условиям

$$|x| \leqslant \sqrt{bc}, \quad |y| \leqslant \sqrt{ac}, \quad |z| \leqslant \sqrt{ab}.$$

Это дает эффективную процедуру (алгоритм) для нахождения нетривиального целочисленного решения (x, y, z) уравнения (8) и, стало быть, для нахождения (в случае его существования) рационального решения (x, y) уравнения (5). Простой

арифметический вывод результата Хольцера был предложен Морделлом [89h].

4. **Алгебраические кривые степени $n \geqslant 3$.** Перейдем к рассмотрению неприводимых кривых степени $n \geqslant 3$.

Пример 2. Рассмотрим кубическую кривую

$$y^2 = x^3 + x^2, \tag{14}$$

содержащую точку (0, 0). Полагая $y = tx$, получаем

$$x^2(t^2 - x - 1) = 0.$$

Корень $x = 0$ этого уравнения соответствует точке (0, 0). Другой корень $x = t^2 - 1$ определяется из равенства $t^2 - x - 1 = 0$. Из уравнения прямой $y = tx$ находим $y = t(t^2 - 1)$. Таким образом, кривая (14) является рациональной кривой с параметризацией:

$$x = t^2 - 1, \quad y = t(t^2 - 1).$$

В частности, эта кривая имеет бесконечно много $\mathbb{Q}$- рациональных точек.

Пример 3. Покажем, что при $n \geqslant 3$ *кривая Ферма*

$$x^n + y^n = 1$$

не является рациональной кривой, если n не делится на характеристику p поля k.

Предположим противное, что эта кривая рациональна, и пусть $x = x(t)$, $y = y(t)$ — ее параметризация. Запишем рациональные функции $x(t)$ и $y(t)$ в виде

$$x(t) = \frac{p(t)}{r(t)}, \quad y(t) = \frac{q(t)}{r(t)},$$

где p, q, r — взаимно простые в совокупности многочлены из кольца $k[t]$. Тогда получаем тождество

$$p^n(t) + q^n(t) - r^n(t) = 0. \tag{15}$$

Продифференцировав его и сократив результат на n (что возможно в силу того, что n не делится на характеристику поля), приходим к соотношению

$$p^{n-1}(t)p'(t) + q^{n-1}(t)q'(t) - r^{n-1}(t)r'(t) = 0. \tag{16}$$

Рассмотрим (15) и (16) как систему линейных уравнений относительно p^{n-1}, q^{n-1} и r^{n-1} с матрицей

$$\begin{Vmatrix} p & q - r \\ p' & q' - r' \end{Vmatrix}.$$

Исключая из этой системы p^{n-1} и q^{n-1}, получаем равенства

$$q^{n-1}(p'q - pq') = r^{n-1}(p'r - pr'),$$
$$p^{n-1}(p'q - pq') = r^{n-1}(r'q - rq'),$$

из которых, ввиду взаимной простоты многочленов p, q и r,

следует, что

$$p^{n-1} \mid (r'q - rq'), \quad q^{n-1} \mid (p'r - pr'), \quad r^{n-1} \mid (p'q - pq').$$

Обозначим h, l, m степени многочленов p, q, r и будем считать, без уменьшения общности, что $h \geqslant l \geqslant m$. Равенство $r'q - rq' = 0$ возможно лишь в случае, когда многочлены r и q являются константами. Но тогда многочлен p также должен быть константой, и приходим к противоречию. Если $r'q - rq' \neq 0$, то из соотношения $p^{n-1}(r'q - rq')$ следует, что $(n-1)h \leqslant l + m - 1$. В таком случае $(n-3)h \leqslant -1$, и так как $n \geqslant 3$, то снова приходим к противоречию.

Рассмотренные примеры показывают, что среди неприводимых кривых степени $n \geqslant 3$ имеются как рациональные, так и нерациональные кривые. В дальнейшем мы увидим, что вопрос о рациональных кривых вкладывается в более общий вопрос о классификации плоских алгебраических кривых с точностью до бирационального изоморфизма. С такой точки зрения рациональные кривые представляют собой простейший тип алгебраических кривых — это кривые, бирационально изоморфные прямой (кривые рода 0).

В заключение параграфа заметим, что возможность рациональной параметризации кривой (1) может быть использована лишь при изучении рациональных решений уравнения

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

Что касается вопроса о целочисленных решениях этого уравнения, то наличие рациональной параметризации, как правило, не приводит к устранению основных трудностей.

Задачи

1. Доказать, что кубическая кривая $y^2 = x^3 + ax + b$ над полем характеристики $p \neq 2$ рациональна в том и только в том случае, когда многочлен $x^3 + ax + b$ имеет кратный корень.

2. Найти параметризацию кривой

$$ax^3 + bx^2y + cxy^2 + dy^3 = Ax^2 + Bxy + Cy^2.$$

3. Пусть $f_{n-1}(x, y)$ и $f_n(x, y)$ — формы степеней $n-1$ и n. Доказать, что если кривая $f_{n-1}(x, y) + f_n(x, y) = 0$ неприводима, то она рациональна.

4. Пусть $f(x, y)$ — кубическая кривая над полем $\mathbb{Q}$, имеющая обыкновенную двойную точку. Доказать, что все рациональные точки этой кривой могут быть выражены через рациональные значения параметра (точка кривой зазывает *обыкновенной двойной точкой*, если ее кратность равна 2 и кривая имеет в этой точке различные касательные направления).

5. Доказать, что все целочисленные решения (x, y, z) уравнения

$$x^2 + y^2 = z^2,$$

рассматриваемые с точностью до замены x на y, представляются в виде

$$x = r(s^2 - t^2), \quad y = 2rst, \quad z = r(s^2 + t^2),$$

где r, s, t — целые числа, причем s и t взаимно просты и одно из них четно, а другое нечетно.

6. Пусть (x, y, z) — решение уравнения

$$x^4 + y^4 = z^2$$

в положительных целых x, y, z с условием $(x, y) = 1$:

а) доказать, что

$$x^2 = s^2 - t^2, \quad y^2 = 2st, \quad z = s^2 + t^2,$$

где s и t — взаимно простые положительные числа разной четности, причем $t = 2u$ — четное число;

б) вывести из п. а), что $s = v^2$, $u = w^2$ и что положительные целые x, v, w удовлетворяют уравнению

$$x^2 + (2w^2)^2 = v^4;$$

в) используя представление

$$x = a^2 - b^2, \quad 2w^2 = 2ab, \quad v^2 = a^2 + b^2.$$

показать, что $a = \xi^2$, $b = \eta^2$ и что положительные целые ξ, η, v удовлетворяют уравнению

$$\xi^4 + \eta^4 = v^2,$$

вполне аналогичному исходному

$$x^4 + y^4 = z^2;$$

г) из п. а) и б) вывести, что $v < z$;

д) повторяя описанный в п. а) — г) процесс (т. е. применяя *метод бесконечного спуска Ферма*), установить неразрешимость уравнения

$$x^4 + y^4 = z^2$$

в отличных от нуля целых числах x, y, z;

е) установить результат Ферма о неразрешимости в отличных от нуля целых x, y, z уравнения

$$x^4 + y^4 = z^4.$$

7. Доказать справедливость *тождеств Фибоначчи*

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

и Эйлера

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = (a\alpha + b\beta + c\gamma + d\delta)^2 + (a\beta - b\alpha - c\delta + d\gamma)^2 + (a\gamma + b\delta - c\alpha - d\beta)^2 + (a\delta - b\gamma + c\beta - d\alpha)^2.$$

8. Пусть p — простое число вида $p = 4k + 1$:

а) доказать разрешимость сравнения

$$z^2 + 1 \equiv 0 \pmod{p}$$

и вывести отсюда существование целых x и y, удовлетворяющих уравнению

$$x^2 + y^2 = mp,$$

где m — положительное целое число, меньшее p;

б) показать, что если в последнем уравнении $m > 1$, то найдутся такие целые s и t, что

$$s^2 + t^2 = mr,$$

где $r < m$;

в) используя соотношения $x^2 + y^2 = mp$, $s^2 + t^2 = mr$ и тождество Фибоначчи из задачи 7, показать, что

$$m^2 rp = (x^2 + y^2)(s^2 + t^2) = (xs + yt)^2 + (xt - ys)^2;$$

г) доказать, что каждое из чисел $xs + yt$ и $xt - ys$ в последнем равенстве делится на m;

д) показать, что если в уравнении $x^2 + y^2 = mp$ число m строго больше единицы, то найдется положительное целое $m' < m$, для которого уравнение

$$x^2 + y^2 = m'p$$

разрешимо в целых x и y;

е) повторяя рассуждения п. б) — д), установить разрешимость в целых x и y уравнения

$$x^2 + y^2 = p.$$

9. Используя п. е) предыдущей задачи, а также тождество Фибоначчи и тот факт, что целые вида $4k + 3$ не представимы суммой двух квадратов, установить справедливость следующей теоремы Эйлера: *для разрешимости уравнения*

$$x^2 + y^2 = n$$

в целых x, y необходимо и достаточно, чтобы каноническое разложение целого числа n не содержало нечетных степеней простых вида $4k + 3$.

10. Пусть p — простое число вида $4k + 3$:

а) доказать разрешимость сравнения

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

и вывести отсюда существование целых x, y, z, t, удовлетворяющих уравнению

$$x^2 + y^2 + z^2 + t^2 = mp,$$

где m — положительное целое число, меньшее p;

б) применяя рассуждения п. б) — д) задачи 8 и используя вместо тождества Фибоначчи тождество Эйлера из задачи 7 показать, что если в уравнении

$$x^2 + y^2 + z^2 + t^2 = mp$$

число m строго больше единицы, то найдется положительное целое $m' < m$, для которого уравнение

$$a^2 + b^2 + c^2 + d^2 = m'p$$

разрешимо в целых a, b, c, d;

в) повторяя рассуждения п. б), установить разрешимость в целых x, y, z, t уравнения

$$x^2 + y^2 + z^2 + t^2 = p.$$

11. Используя тождество Эйлера и результаты задач 8, 10, установить справедливость *теоремы Лагранжа о* том, что каждое положительное целое представимо суммой четырех квадратов целых чисел.

12. Пусть a — положительное целое число, не являющееся полным квадратом:

а) используя одномерный вариант *теоремы Дирихле* о приближениях (см. задачу 13 из § 4 гл. I) установить существование положительного числа m (можно взять $m = 1 + 2\sqrt{a}$), для которого неравенство

$$|x^2 - ay^2| < m$$

имеет бесконечно много решений в целых x и y. Вывести отсюда существование целого k, $|k| < m$, для которого уравнение

$$x^2 - ay^2 = k$$

обладает бесконечным множеством целочисленных решений (x, y);

б) взяв два целочисленных решения (x', y'), (x'', y'') уравнения $x^2 - ay^2 = k$ с условиями $x'' \equiv x' \pmod{k}$, $y'' \equiv y' \pmod{k}$, $(x'', y'') \neq (-x', y')$ и положив

$$x = \frac{x'x'' - ay'y''}{k}, \quad y = \frac{x'y'' - x''y'}{k},$$

показать, что целые x и y удовлетворяют уравнению

$$x^2 - ay^2 = 1;$$

в) обозначив (x_1, y_1) решение уравнения

$$x^2 - ay^2 = 1$$

в целых $x > 0$, $y > 0$ с наименьшим значением y и определив положительные целые x_n, y_n, $n = 1, 2, \ldots$, равенствами

$$x_n + y_n\sqrt{a} = (x_1 + y_1\sqrt{a})^n, \quad x_n - y_n\sqrt{a} = (x_1 - y_1\sqrt{a})^n,$$

показать, что каждый из наборов (x_n, y_n) удовлетворяет указанному уравнению;

г) доказать, что все целочисленные решения *уравнения Пелля*

$$x^2 - ay^2 = 1$$

исчерпываются наборами (x_n, y_n), $n = 1, 2, \ldots$, где

$$x_n + y_n\sqrt{a} = \begin{cases} (x_1 + y_1\sqrt{a})^n, & \text{если } x_n > 0, \ y_n > 0, \\ -(x_1 + y_1\sqrt{a})^n, & \text{если } x_n < 0, \ y_n < 0, \\ (x_1 + y_1\sqrt{a})^{-n}, & \text{если } x_n > 0, \ y_n < 0, \\ -(x_1 + y_1\sqrt{a})^{-n}, & \text{если } x_n < 0, \ y_n > 0. \end{cases}$$

13. Пусть p — простое число вида $4k + 1$. Доказать, что уравнение

$$x^2 - py^2 = -1$$

имеет бесконечное множество целочисленных решений (x_n, y_n), $n = 0, \pm 1, \pm 2, \ldots$, где

$$x_n + y_n\sqrt{p} = (a + b\sqrt{p})^{2n+1}$$

и (a, b) — некоторое частное решение этого уравнения.

14. Используя результаты задачи 12, установить справедливость следующей теоремы Гаусса: *если уравнение*

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

с целыми коэффициентами разрешимо в целых x, y и если выполнены условия

а) $D = b^2 - 4ac > 0$,
б) *D не является полным квадратом*,
в) $4acf + bde - ae^2 - cd^2 - fb^2 \neq 0$,

то оно имеет бесконечно много целочисленных решений.

15. Используя результаты задачи 12, показать, что если уравнение

$$x^3 + y^3 + z^3 + t^3 = n$$

обладает целочисленным решением (x_0, y_0, z_0, t_0), удовлетворяющим условиям

а) $d = -(x_0 + y_0)(z_0 + t_0) > 0$,
б) d не является полным квадратом,
в) $x_0 \neq y_0$, $z_0 \neq t_0$,

то оно имеет бесконечно много целочисленных решений.

§ 2. Эллиптические кривые

1. Бирациональный изоморфизм кривых. Пусть неприводимые кривые X и Y определены над полем $k_0 \subset k$ уравнениями $f(x, y) = 0$, $g(u, v) = 0$. *Рациональным отображением* кривой X в кривую Y называется такая пара рациональных функций $\varphi(x, y)$ и $\psi(x, y)$, определенных на X, что функция $g(\varphi(x, y), \psi(x, y))$ равна нулю на кривой X.

Определение. Кривые X и Y называются *бирационально изоморфными*, если существуют рациональные отображения X в Y и Y в X, обратные друг другу. Они называются *бирационально изоморфными над полем k_0*, если коэффициенты рациональных функций, задающих бирациональный изоморфизм, принадлежат полю k_0.

На протяжении этого параграфа предполагается, что все рассматриваемые в нем кривые определены над полем рациональных чисел $\mathbb{Q}$.

Теорема 1. *Всякая неприводимая кубическая кривая $f(x, y) = 0$, имеющая рациональную точку, бирационально изоморфна над полем $\mathbb{Q}$ кривой*

$$v^2 = u^3 + au + b.$$

Доказательство. Пусть P — рациональная точка рассматриваемой кубической кривой X. Обозначим Q рациональную точку, в которой касательная к X в точке P снова пересекает X, и примем точку Q за начало координат. Прямая $y = tx$, проходящая через Q, пересекает кривую X в двух других точках, x-координаты которых определяются уравнением

$$Ax^2 + 2Bx + C = 0,$$

где A, B и C — многочлены от параметра t с рациональными коэффициентами степеней 3, 2 и 1 соответственно. Так как P и Q — рациональные точки, а прямая PQ касается кривой X, то многочлен четвертой степени $B^2 - AC$ имеет рациональный корень, скажем $t = t_0$. Полагая

$$t = t_0 + \frac{1}{z},$$

получаем

$$(Ax + B)^2 = B^2 - AC = \frac{g(z)}{z^4},$$

где $g(z)$ — многочлен третьей степени. Применяя теперь линейную подстановку

$$z = ru + s$$

с подходящими рациональными r, s и полагая

$$Ax + B = \frac{v}{(ru + s)^2},$$

приходим к уравнению

$$v^2 = u^3 + au + b.$$

Теорема доказана.

Замечание. Из доказательства теоремы 1 следует, что координаты точек (x, y) и (u, v) связаны между собой соотношениями

$$t = \frac{\alpha u + \beta}{\gamma u + \delta}, \quad y = tx,$$

где $\alpha, \beta, \gamma, \delta \in Q$. Следовательно, рациональным точкам кривой $v^2 = u^3 + au + b$ соответствуют рациональные точки кривой $f(x, y) = 0$ и обратно. Таким образом, при изучении вопроса о рациональных точках кубических кривых $f(x, y) = 0$, имеющих хотя бы одну такую точку, можно ограничиться рассмотрением кривых вида

$$y^2 = x^3 + ax + b.$$

При этом удобно считать бесконечно удаленную точку $(x, y) = (\infty, \infty)$ за рациональную точку кривой $y^2 = x^3 + ax + b$. В проективных координатах ей соответствует рациональная точка $(x, y, z) = (0, 1, 0)$ кривой

$$y^2 z = x^3 + axz^2 + bz^3.$$

Теорема 2. *Если кривая*

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e \tag{1}$$

имеет рациональную точку, то она бирационально изоморфна над Q кривой

$$v^2 = u^3 + a'u + b'.$$

Доказательство. Можем считать, что c является полным квадратом. Далее, полагая в случае необходимости $x = 1/x'$, $y = y'/x'^2$, можем считать, что a также является полным квадратом. Если $a = 0$, то утверждение теоремы очевидно. Если же $a \neq 0$, то, положив $x = x'/\sqrt{a}$, $y = y'/\sqrt{a}$, приходим к случаю $a = 1$. Заменив, наконец, x на $x - b/4$, можем записать уравнение (1) в виде

$$y^2 = x^4 - 6cx^2 + 8dx + e. \tag{2}$$

Бирациональный изоморфизм между этой кривой и кривой $v^2 = u^3 + a'u + b'$ задается соотношениями

$$y = -x^2 + 2u + c, \quad x = \frac{v - d}{u - c}.$$

Действительно, подставляя $y = -x^2 + 2u + c$ в уравнение (2), получаем

$$x^4 - 2(2u + c)x^2 + (2u + c)^2 = x^4 - 6cx^2 + sdx + e.$$

Значит,

$$(u - c)x^2 + 2dx - \left(u^2 + cu + \frac{1}{4}(c^2 - e)\right) = 0$$

и тогда

$$x(u - c) = -d \pm \left(d^2 + u^3 - c^2u + \frac{1}{4}(c^2 - e)(u - c)\right)^{1/2}.$$

В результате приходим к кривой

$$v^2 = u^3 + a'u + b',$$

где $a' = -\frac{3}{4}c^2 - \frac{1}{4}e$, $b' = d^2 - \frac{1}{4}c(c^2 - e)$. Теорема доказана.

2. Сложение точек на эллиптических кривых. Рассмотрим эллиптическую кривую, задаваемую уравнением

$$y^2 = x^3 + ax + b, \tag{3}$$

где $4a^3 + 27b^2 \neq 0$. Определим на кривой (3) операцию сложения точек. Пусть $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ — две различные точки этой кривой. Найдем третью точку $P_3' = (x_3, y_3)$ кривой (3), координаты которой x_3, y_3 рациональным образом выражаются через координаты x_1, y_1, x_2, y_2 точек P_1 и P_2. Для этого проведем через точки P_1 и P_2 прямую

$$\frac{y - y_1}{y_2 - y_1} = \frac{x - x_3}{x_2 - x_1} \tag{4}$$

с текущими координатами x и y. Эта прямая пересекает кривую (3) в трех точках, две из которых P_1 и P_2 известны. Для отыскания третьей точки $P_3' = (x_3, y_3)$ выразим y через x из уравнения (4) и подставим результат в уравнение (3):

$$\left(y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)\right)^2 = x^3 + ax + b. \tag{4'}$$

Два корня x_1 и x_2 этого кубического относительно x уравнения известны. Для нахождения третьего корня x_3 воспользуемся тем, что сумма корней

$$x_1 + x_2 + x_3$$

нормированного кубического многочлена равна коэффициенту при x^2, взятому с обратным знаком. Таким образом,

$$x_1 + x_2 + x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2$$

и, следовательно,

$$x_3 = -x_1 - x_2 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2. \tag{5}$$

Подставляя это значение для x в уравнение прямой (4), находим вторую координату y_3 точки P_3':

$$y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) + y_1.$$

Вместе с точкой P_3' на кривой (3) лежит также и симметричная

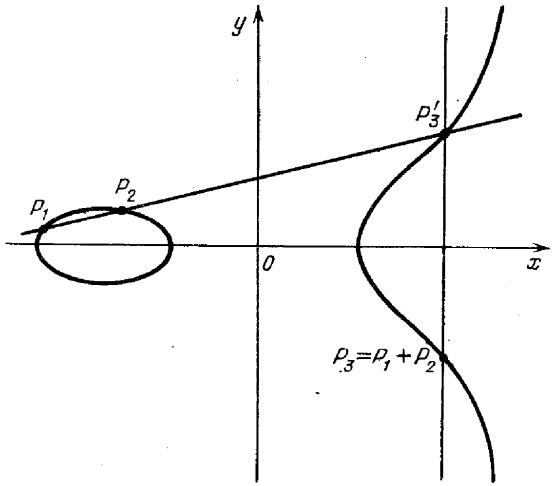


Рис. 2

с ней точка $P_3 = (x_3, -y_3)$. Именно ее (см. рис. 2) будем считать суммой

$$P_3 = P_1 + P_2$$

точек P_1 и P_2 на кривой (3).

В случае $P_1 = P_2$ первая координата x_3 точки P_3 определяется соотношением

$$x_3 = -2x_1 + \frac{(3x_1^2 + a)^2}{4(x_1^3 + ax_1 + b)},$$

которое получается из (5) предельным переходом при $x_2 \to x_1$.

Для дальнейшего нам потребуется другая форма соотношения (5). Пусть

$$x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

— разложение многочлена $x^3 + ax + b$ на линейные множители. Заменим в уравнении (4′) x_1, x_2 и x на $x_1 - \alpha$, $x_2 - \alpha$ и $x - \alpha$, где α — один из элементов α_1, α_2, α_3. Для нахождения $x_3 - \alpha$ воспользуемся тем, что произведение

$$(x_1 - \alpha)(x_2 - \alpha)(x_3 - \alpha)$$

корней этого уравнения равно свободному коэффициенту, взятому со знаком минус. Это приводит к соотношению

$$x_3 - \alpha = \frac{1}{(x_1 - \alpha)(x_2 - \alpha)}\left(\frac{y_1(x_2 - \alpha) - y_2(x_1 - \alpha)}{x_2 - x_1}\right)^2, \qquad (6)$$

которое при $P_1 = P_2$ принимает вид

$$x_3 - \alpha = \left(\frac{x_1^2 - a - 2\alpha x_1 - 2\alpha^2}{2y_1}\right)^2. \qquad (7)$$

3. Теорема Морделла. Покажем, что все рациональные точки эллиптической кривой

$$y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0,$$

определенной над полем $\mathbb{Q}$, рациональным образом выражаются через некоторое конечное множество $S = \{P_1, \ldots, P_r\}$ таких точек. Этот результат впервые был доказан Морделлом [89b]. Приведенное ниже доказательство принадлежит А. Вейлю [23b].

Предварительно сделаем несколько замечаний. Если q — общий знаменатель коэффициентов a и b, то, заменяя в случае необходимости x и y на x/q^2 и y/q^3 соответственно, можем считать, что a и b являются целыми числами. Далее, поскольку дискриминант $\Delta = -(4a^3 + 27b^2)$ многочлена $x^3 + ax + b$ отличен от нуля, то корни α_1, α_2, α_3 этого многочлена различны между собой.

Обозначим $K_\nu = \mathbb{Q}(\alpha_\nu)$, $1 \leqslant \nu \leqslant 3$, расширение поля рациональных чисел $\mathbb{Q}$, полученное присоединением корня α_ν, и заметим, что среди полей K_1, K_2, K_3 могут быть одинаковые. Пусть α — один из элементов α_1, α_2, α_3 и K — одно из полей K_1, K_2, K_3. Запишем уравнение (3) в виде

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = \mathrm{Norm}(x - \alpha)$$

и изучим структуру чисел $x - \alpha$, $x \in \mathbb{Q}$, чьи нормы $\mathrm{Norm}(x - \alpha)$ являются квадратами в $\mathbb{Q}$. Отметим, что введенная нами норма $\mathrm{Norm}(x - \alpha)$ числа $x - \alpha$ отличается, вообще говоря, от обычной нормы $\mathrm{norm}(x - \alpha)$ элемента $x - \alpha$ поля K.

Числа $x - \alpha$ принадлежат множеству $S(\alpha)$ элементов $\beta = t_0 + t_1\alpha + t_2\alpha^2$, $t_0, t_1, t_2 \in \mathbb{Q}$, поля K, нормы которых $\mathrm{Norm}\,\beta$ являются квадратами рациональных чисел. Далее, $S(\alpha)$ содержит в себе подмножество чисел, являющихся квадратами в поле K. Разобьем множество $S(\alpha)$ на классы, отнеся в один класс все элементы вида $\eta\tau^2$, где $\tau \in K$. Ясно, что имеется бесконечное число таких классов.

Если A и B — два класса и $\eta \in A$, $\theta \in B$, то элемент $\eta\theta$ однозначно определяет класс C, состоящий из чисел $\eta\theta\tau^2$, $\tau \in K$. Тем самым можно определить умножение классов по правилу $C = A \cdot B$. Очевидно, что введенная таким образом операция ум-

ножения классов ассоциативна и коммутативна. При этом единичным классом будет класс E, состоящий из квадратов элементов поля K. Далее, операция умножения классов обратима и, стало быть, введенные в рассмотрение классы A, B, C, ... образуют бесконечную абелеву группу. Так как $A^2 = E$, то каждый элемент A этой группы имеет порядок 2.

Лемма 1. *Числа вида $x - \alpha$ поля K, нормы которых являются квадратами рациональных чисел, лежат в конечном множестве классов.*

Доказательство. В равенстве $y^2 = \mathrm{Norm}(x - \alpha)$ положим $x = p/q$, где p, q — взаимно простые целые числа. Тогда получим соотношение

$$(yq^2)^2 = q\,\mathrm{Norm}(p - \alpha q).$$

Поскольку $(p, q) = 1$, то число q взаимно просто с нормой $\mathrm{Norm}(p - \alpha q)$ целого алгебраического числа $p - \alpha q$ и, в таком случае, $q = s^2$. Следовательно, $y = r/s^3$, где $(r, s) = 1$, и тогда

$$r^2 = \mathrm{Norm}(p - \alpha s^2) = (p - \alpha_1 s^2)(p - \alpha_2 s^2)(p - \alpha_3 s^2).$$

В поле K_1 имеется лишь конечное число дивизоров $\mathfrak{a}$, делящих одновременно числа $p - \alpha_1 s^2$ и $(p - \alpha_2 s^2)(p - \alpha_3 s^2)$. Действительно, если $p - \alpha_1 s^2 \equiv 0 \pmod{\mathfrak{a}}$ и $(p - \alpha_2 s^2)(p - \alpha_3 s^2) \equiv 0 \pmod{\mathfrak{a}}$, то $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \equiv 0 \pmod{\mathfrak{a}}$, а поскольку α_1, α_2, α_3 — фиксированные числа, то последнее сравнение выполняется лишь для конечного числа дивизоров $\mathfrak{a}$. Отсюда следует, что

$$p - \alpha_1 s^2 = \mu\xi^2,$$

где μ — одно из чисел некоторой конечной системы и ξ — целое алгебраическое число. Разделив обе части последнего равенства на s^2, получаем

$$x - \alpha_1 = \mu\xi^2,$$

где ξ — некоторый элемент поля K_1. Аналогичный результат справедлив для $x - \alpha_2$ и $x - \alpha_3$. Лемма доказана.

Свяжем теперь закон сложения точек на кривой (3) с операцией умножения введенных в рассмотрение классов A, B, C, ... Для этого сопоставим рациональной точке $P = (x, y)$ кривой (3) число $x - \alpha$ и скажем, что точка P принадлежит классу A, если $x - \alpha$ лежит в этом классе.

Лемма 2. *Если точки P и Q принадлежат классам A и B, то их сумма $P + Q$ принадлежит классу AB.*

Доказательство. Утверждение леммы очевидным образом следует из соотношения (6).

Лемма 3. *Точка $Q = 2P$ принадлежит единичному классу E. Другими словами, если Q имеет координаты (x, y), то $x - \alpha = \tau^2$, $\tau \in K$.*

Доказательство. Утверждение леммы следует из соотношения (7).

Лемма 4. *Если точка $Q = (x, y)$ принадлежит единичному классу E, то существует рациональная точка $P = (x', y')$ такая, что $Q = 2P$.*

Доказательство. Пусть

$$x - \alpha = (u_0 + u_1\alpha + u_2\alpha^2)^2, \tag{8}$$

где u_0, u_1, u_2 — рациональные числа. Тогда

$$x - \alpha = u_0^2 + 2u_0u_1\alpha + (u_1^2 + 2u_0u_2)\alpha^2 + 2u_1u_2\alpha^3 + u_2^2\alpha^4 =$$
$$= u_0^2 + 2u_0u_1\alpha + (u_1^2 + 2u_0u_2)\alpha^2 - 2u_1u_2(a\alpha + b) - u_2^2(a\alpha^2 + b\alpha) =$$
$$= (u_0^2 - 2bu_1u_2) + (2u_0u_1 - 2au_1u_2 - bu_2^2)\alpha + (u_1^2 + 2u_0u_2 - au_2^2)\alpha^2$$

и, следовательно,

$$\begin{aligned} u_0^2 - 2bu_1u_2 &= x, \\ 2u_0u_1 - 2au_1u_2 - bu_2^2 &= -1, \\ u_1^2 + 2u_0u_2 - au_2^2 &= 0. \end{aligned} \tag{9}$$

Исключая u_0 из второго и третьего уравнения, приходим к соотношению

$$u_1^3 + au_1u_2^2 + bu_2^3 = u_2,$$

которое, ввиду того, что $u_2 \neq 0$, можно переписать в виде

$$\frac{1}{u_2^2} = \left(\frac{u_1}{u_2}\right)^3 + a\left(\frac{u_1}{u_2}\right) + b.$$

Положим $x' = u_1/u_2$, $y' = 1/u_2$. Тогда точка $P = (x', y')$ является рациональной точкой кривой (3). Из третьего уравнения системы (9) имеем

$$x'^2 + 2u_0y' - a = 0.$$

Выражая u_0, u_1, u_2 через x', y', получаем

$$u_0 + u_1\alpha + u_2\alpha^2 = \frac{-x'^2 + a}{2y'} + \frac{x'}{y'}\alpha + \frac{1}{y'}\alpha^2.$$

Отсюда и из уравнений (7), (8) находим, что $Q = 2P$. Лемма доказана.

Лемма 5. *Если точки P и Q принадлежат одному и тому же классу, то*

$$P + Q = 2R,$$

где R — рациональная точка кривой (3).

Доказательство. Утверждение леммы следует из лемм 2 и 3, так как точка $P + Q$ принадлежит единичному классу E.

Теорема А (см. [89b], [23b]). *Все рациональные точки кривой* (3) *могут быть получены из некоторого их конечного числа с помощью операции сложения точек.*

Доказательство. По лемме 1 все рациональные точки попадают (по отношению к введенной выше принадлежности) в конечное число классов A, B, C, ... Пусть

$$Q_1=(x_1, y_1), \ldots, Q_m=(x_m, y_m)$$

представители этих различных классов. Предположим, что рациональная точка $P_0=(x, y)$ лежит в том же классе, что и точка Q_{j_1}. Тогда по лемме 5 имеем

$$P_0+Q_{j_1}=2P_1,$$

где P_1 — рациональная точка кривой (3). Аналогичным образом

$$P_1+Q_{j_2}=2P_2,$$

где P_2 — снова рациональная точка рассматриваемой кривой. Таким образом, для всех $k=0, 1, 2, \ldots$ имеем

$$P_k+Q_{j_{k+1}}=2P_{k+1}. \tag{10}$$

Отсюда следует, что точка P_0 линейным образом выражается через точки $Q_1, \ldots, Q_m$ и точку P_{k+1}. Действительно, исключая $P_1, P_2, \ldots, P_k$, получаем

$$P_0+Q_{j_1}+2Q_{j_2}+\ldots+2^kQ_{j_{k+1}}=2^{k+1}P_{k+1}.$$

Покажем, что указанный процесс приводит к конечному множеству точек P_{k+1}.

Перейдем в уравнении (3) к другим координатам, заменив x, y на x/z^2, y/z^3 соответственно. Тогда уравнение (3) запишется в виде

$$y^2=x^3+axz^4+bz^6,$$

и точка $P_0=(x, y)$ будет иметь однородные координаты (xz, y, z^3). Предположим, что x, y, z — целые числа и что $(x, z)=1$.

Вернемся к соотношению

$$P_0+Q_{j_1}=2P_1$$

и обозначим однородные координаты точек P_0, Q_{j_1}, P_1 и $2P_1$ через (x, y, z), (p, q, r), (x_1, y_1, z_1) и (s, t, u). Положим $\lambda_0=\max(|x|, z^2)$, $\rho=\max(|p|, r^2)$, $\lambda_1=\max(|x_1|, z_1^2)$ и $\omega=\max(|s|, u^2)$. Ясно, что $|y|=O(\lambda_0^{3/2})$, где константа в символе «O» зависит лишь от a и b.

Оценим величину ω. Из соотношения (5) имеем

$$x_3=\frac{(x_1x_2+a)(x_1+x_2)+2b-2y_1y_2}{(x_1-x_2)^2}$$

и, значит,

$$\frac{s}{u^2}=\frac{(px+ar^2z^2)(r^2x+pz^2)+2br^4z^4-2qryz}{(r^2x-pz^2)^2}.$$

Так как $(s, u)=1$, то из последнего соотношения следует, что

$$\omega=O(\lambda_0^2).$$

Покажем теперь, что $\lambda_1=O(\omega^{1/4})$. Из формулы (7) имеем

$$(s-\alpha u^2)^{1/2}=\frac{u}{2y_1z_1}(x_1^2-az_1^4-2\alpha x_1z_1^2-2\alpha^2z_1^4)=e_0+e_1\alpha+e_2\alpha^2$$

и, так как $(s-\alpha u^2)^{1/2}$ — целое алгебраическое число из поля K, таковым является и $e_0+e_1\alpha+e_2\alpha^2$. Следовательно, если Δ — дискриминант многочлена x^3+ax+b, то Δe_0, Δe_1, Δe_2 суть целые числа и тогда

$$\Delta(2e_0-ae_2)=\frac{\Delta u}{y_1z_1}x_1^2, \quad -\Delta e_2=\frac{\Delta u}{y_1z_1}z_1^4$$

также являются целыми числами. Далее, так как $(x_1, z_1)=1$, то $\frac{\Delta u}{y_1z_1}$ — целое число и, значит, $x_1^2 \mid \Delta(2e_0-ae_2)$, $z_1^4 \mid \Delta e_2$. Но числа $\Delta(2e_0-ae_2)$ и Δe_2 линейно выражаются через $(s-\alpha_1u^2)^{1/2}$, $(s-\alpha_2u^2)^{1/2}$, $(s-\alpha_3u^2)^{1/2}$ и, стало быть, оценивается величиной $O(\omega^{1/2})$. Следовательно, $x_1^2=O(\omega^{1/2})$, $z_1^4=O(\omega^{1/2})$ и тогда $\lambda_1=O(\omega^{1/4})=O(\lambda_0^{1/2})$.

Применяя указанные рассуждения к каждому из соотношений (10) при $k=0, 1, 2, \ldots$, получим последовательность чисел $\lambda_0, \lambda_1, \lambda_2, \ldots$ таких, что $\lambda_{k+1}=O(\lambda_k^{1/2})$. Эта последовательность ограничена и, значит, однородные целочисленные координаты точек P_{k+1} также ограничены. В таком случае множество точек P_{k+1} конечно, тем самым теорема доказана.

Полученный результат может быть сформулирован также следующим образом.

Теорема В. *Существует такое конечное множество* $\{P_1, \ldots, P_n\}$ *рациональных точек кривой*

$$E: y^2=x^3+ax+b, \quad 4a^3+27b^2\neq 0,$$

что всякая рациональная точка P *этой кривой представляется в виде*

$$P=m_1P_1+\ldots+m_nP_n$$

с целыми $m_1, \ldots, m_n$.

4. Ранг эллиптической кривой. Нетрудно видеть, что введенная операция сложения точек на эллиптической кривой E является коммутативной групповой операцией, нейтральным элементом которой служит бесконечно удаленная рациональная точка O этой кривой. Поскольку рассматриваемая операция задается рациональными функциями с коэффициентами из $\mathbb{Q}$, то она индуцирует аналогичную операцию на множестве $E(\mathbb{Q})$ рациональных точек кривой E, превращая это множество в абелеву группу. Из теоремы B следует, что группа $E(\mathbb{Q})$ является конечно порожденной.

Следует отметить, что в качестве нулевой точки O может быть выбрана любая рациональная точка из $E(\mathbb{Q})$. При этом, естественно, формулы в групповом законе несколько изменят свой вид (см. [1] гл. 18, § 1).

Если рациональная точка P кривой (3) удовлетворяет условию $mP = O$ при некотором целом m, то она называется *точкой конечного порядка эллиптической кривой* $y^2 = x^3 + ax + b$. Множество $\Gamma(\mathbb{Q})$ таких точек является конечной подгруппой группы $E(\mathbb{Q})$. Структуру группы $\Gamma(\mathbb{Q})$ для кривых $y^2 = x^3 + ax + b$ с целыми a и b во многом выясняет следующая теорема Нагелля [90].

Теорема 3. *Пусть* (x', y') *— точка конечного порядка кривой*

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

Тогда $x', y' \in \mathbb{Z}$ *и либо* $y' \neq 0$, *либо* $y'^2 | (4a^3 + 27b^2)$.

Рассмотрение многочисленных примеров привело к предположению (см. [59c]), что группа $\Gamma(\mathbb{Q})$ равномерно ограничена для всех эллиптических кривых над полем $\mathbb{Q}$. Это предположение, даже в более сильной форме, было доказано Мазуром [77a — 77c], установившим справедливость *гипотезы Огга* [94] о том, что группа $\Gamma(\mathbb{Q})$ произвольной эллиптической кривой над полем $\mathbb{Q}$ изоморфна одной из следующих 15 групп: $\mathbb{Z}/l\mathbb{Z}$, $1 \leqslant l \leqslant 10$, $l = 12$ и $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $1 \leqslant m \leqslant 4$.

Более сложным оказался вопрос о *ранге* (числе образующих бесконечного порядка) *группы* $E(\mathbb{Q})$ (*группы Морделла — Вейля*). Этот ранг называется также *рангом* соответствующей *эллиптической кривой*. В большинстве исследованных случаев ранг группы $E(\mathbb{Q})$ оказывается очень малым (равным 0, 1 или 2). Пока неясно, существуют ли эллиптические кривые сколь угодно большого ранга (что считается весьма вероятным). В этом направлении до сих пор получены лишь отдельные факты. Так, А. Нерон [91] доказал, что существует эллиптическая кривая ранга $\geqslant 10$. Грюневальд и Циммерт [36] привели пример эллиптической кривой ранга $\geqslant 8$. Недавно Местру [85] удалось построить примеры эллиптических кривых рангов от 3 до 14 включительно. В частности, согласно его вычислениям, кривая ранга 14 имеет вид $y^2 + 357\,573\,631y = x^3 + 2\,597\,055x^2 - 549\,082x - 19\,608\,054$.

Интересные гипотезы о ранге группы $E(\mathbb{Q})$ были предложены Берчем и Суиннертоном — Дайером [15]. Ограничимся снова рассмотрением кубической кривой

$$E\colon\ y^2 = x^3 + ax + b, \quad \Delta = -(4a^3 + 27b^2) \neq 0 \tag{11}$$

с целыми коэффициентами a и b. При этом мы не теряем общности, поскольку каждая эллиптическая кривая (3) может быть преобразована к такому виду заменой переменных $(x, y) \mapsto (q^2x, q^3y)$ с подходящим положительным $q \in \mathbb{Z}$.

Если простое число p не делит Δ, то редукция кривой E по $\bmod p$ приводит к эллиптической кривой E_p над полем F_p. Для количества N_p точек кривой E_p с координатами в F_p (включая бесконечно удаленную точку) справедлива формула

$$N_p = p + 1 - \omega_p - \bar{\omega}_p,$$

где $|\omega_p| = p^{1/2}$. Для таких p *локальная L-функция кривой E* определяется по формуле

$$L(E_p, s) = [(1 - \omega_p p^{-s})(1 - \bar{\omega}_p p^{-s})]^{-1}.$$

Аналогичным образом, *локальная ζ-функция кривой E* определяется для простых $p \nmid \Delta$ как ζ-функция кривой E_p над полем F_p по формуле

$$\zeta(E_p, s) = \frac{(1 - \omega_p p^{-s})(1 - \bar{\omega}_p p^{-s})}{(1 - p^{-s})(1 - p^{1-s})}.$$

Для $p | \Delta$ положим

$$\zeta(E_p, s) = [(1 - p^{-s})(1 - p^{1-s})]^{-1}$$

и определим *глобальные L- и ζ-функции кривой E* формулами

$$L(E, s) = \prod_{p \nmid \Delta} L(E_p, s), \quad \zeta(E, s) = \prod_p \zeta(E_p, s).$$

Из этого определения получаем соотношение

$$\zeta(E, s) = \zeta(s)\zeta(1 - s)L^{-1}(E, s),$$

связывающее ζ-функцию $\zeta(E, s)$ кривой E с L-функцией $L(E, s)$ этой кривой и обычной ζ-функцией Римана. Это соотношение имеет особое значение для кривых с комплексным умножением (см. задачу **12**), когда величина $L(E, 1)$ допускает выражение в виде явной формулы, дающей возможность для ее вычисления (см., например, [119a]).

Нетрудно видеть, что произведение $\prod_p L(E_p, s)$ сходится при $\operatorname{Re} s > 3/2$. Существует предположение (доказанное в некоторых специальных случаях), что функция $L(E, s)$, задаваемая этим

произведением, может быть аналитически продолжена на всю комплексную плоскость. При $s \to 1$ приходим формально к равенству

$$L^{-1}(E, 1) = \prod_p \left\{\frac{N_p}{p}\right\}.$$

Очевидно, что бесконечное произведение в правой части последнего равенства не может быть вычислено. Однако конечное произведение

$$f(N) = \prod_{p \leqslant N} \left\{\frac{N_p}{p}\right\}$$

вычислимо вплоть до значений N порядка нескольких тысяч. Исходя из этих вычислений, Берч и Суиннертон-Дайер [15] высказали следующие две взаимосвязанные гипотезы.

Гипотеза 1. *Пусть r — ранг эллиптической кривой E. Существуют положительные константы c' и c'' (зависящие от E) такие, что*

$$c'(\log N)^r \leqslant f(N) \leqslant c''(\log N)^r.$$

Гипотеза 2. *Функция $L(E, s)$ имеет в точке $s = 1$ нуль порядка r.*

За последние годы был получен ряд результатов, подтверждающих справедливость указанных предположений (см. обзоры Касселса [59c], Циммера [141] и Мазура [77d]). Среди них отметим результаты Раджвада [101], Милна [86a] и Коутеса — Уайлса [65]. Особый интерес представляет работа Коутеса и Уайлса, из которой следует (см. [108a, 37, 116c]), что если кривая E над $\mathbb{Q}$ имеет комплексное умножение и содержит рациональную точку бесконечного порядка, то L-функция Хассе — Вейля $L(E, s)$ обращается при $s = 1$ в ноль. При $r = 1$ и при дополнительном предположении о том, что $L(E, 1) = 0$ и первая производная функции $L(E, s)$ отлична от нуля в точке $s = 1$, гипотеза 2 была доказана Гроссом и Загье [34]. Для кривых с комплексным умножением более сильный результат получил Рубин [108b], показавший, что если $r \geqslant 2$, то порядок нуля функции $L(E, s)$ в точке $s = 1$ не меньше 2, и установивший для таких кривых справедливость гипотезы 2 при условии, что порядок нуля функции $L(E, s)$ в точке $s = 1$ не выше 1. В общем случае, но при некотором дополнительном условии на E (которое гипотетически всегда выполняется) В. А. Колывагин [62a, 62b] установил, что если $L(E, 1) \neq 0$, то группа $E(\mathbb{Q})$ конечна.

В заключение параграфа дадим аналитическую формулировку теоремы B. Хорошо известно (см., например, книгу [70g]), что кривая (11) обладает параметризацией

$$x = \mathfrak{P}(z), \quad 2y = \mathfrak{P}'(z),$$

где

$$\mathfrak{P}(z) = \frac{1}{z^2} + \sum_{\omega \in L, \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right]$$

— эллиптическая функция Вейерштрасса с решеткой периодов $L = [\omega_1, \omega_2]$, $\operatorname{Im} \omega_1/\omega_2 > 0$ и инвариантами $a = -15 \sum_{\omega \in L, \omega \neq 0} \omega^{-1}$, $b = -35 \sum_{\omega \in L, \omega \neq 0} \omega^{-6}$. Указанная параметризация задает биекцию между значениями комплексного параметра $z \pmod L$ и комплекснозначными точками $P(z) = \left(\mathfrak{P}(z), \frac{1}{2}\mathfrak{P}'(z)\right)$ кривой E. При этом теорема сложения

$$\mathfrak{P}(z_3) = -\mathfrak{P}(z_1) - \mathfrak{P}(z_2) + \frac{1}{4}\left(\frac{\mathfrak{P}'(z_1) - \mathfrak{P}'(z_2)}{\mathfrak{P}(z_1) - \mathfrak{P}(z_2)}\right)^2$$

точек кривой E имеет параметрическое представление

$$z_1 + z_2 + z_3 \equiv 0 \pmod L.$$

Таким образом, в терминах параметра z теорему B можно переформулировать в следующем виде.

Теорема C. *Все рациональные точки кривой* (11) *задаются параметрически в виде*

$$z = m_1 z_1 + \ldots + m_n z_n,$$

где $z_1, \ldots, z_n$ — некоторые фиксированные значения параметра z и $m_1, \ldots, m_n$ пробегает все целые значения.

С более детальным изложением арифметики эллиптических кривых читатель может познакомиться по книге Сильвермана [111b].

Задачи

1. Пусть $P_0 = (x_0, y_0)$, $y_0 \neq 0$, — рациональная точка кривой

$$y^2 = x^3 + k.$$

Проведя через P_0 касательную

$$y - y_0 = \frac{3x_0^2}{2y_0}(x - x_0),$$

показать, что она пересекает кривую $y^2 = x^3 + k$ в точке $P_1 = (x_1, y_1)$, где

$$x_1 = \frac{9x_0^4 - 8x_0y_0^2}{4y_0^2}, \quad y_1 = \frac{27x_0^6 - 36x_0^3y_0^2 + 8y_0^4}{8y_0^3}.$$

Показать, в частности, что кривая $y^2 = x^3 - 2$ имеет рациональные точки $P_0 = (3, 5)$ и $P_1 = \left(\frac{129}{10^2}, \frac{383}{10^3}\right)$.

2* (Морделл [89g]). Пусть k — целое число, не содержащее в своем каноническом разложении шестой степени простого числа и отличное от 1 и -432. Пусть, далее, кривая

$$y^2 = x^3 + k$$

обладает рациональной точкой $P_0 = (x_0, y_0)$ с условием $x_0 y_0 \neq 0$.

а) Положив $x_0 = p/q^2$, $y_0 = r/q^3$, где $(p, q, r) = 1$, $(p, q) = 1$, $(r, q) = 1$, показать, что точка $P_1 = (x_1, y_1)$ из задачи 1 имеет координату x_1, определяемую соотношением

$$q^2 x_1 = \frac{9p^4}{4r^2} - 2p.$$

б) Доказать, что если $3p^2/2r$ не является целым числом, то $P_1 \neq P_0$.

в) Показать, что если $3p^2/2r$ — целое число, то, применяя к точке P_1 указанный в предыдущей задаче процесс, можно прийти к рациональной точке $P_1' \neq P_0$;

г) Используя результаты из п. а) — в) установить, что кривая

$$y^2 = x^3 + k$$

имеет бесконечное число рациональных точек.

3*. Доказать, что кривая

$$y^2 = x^3 + k$$

имеет при $k = 1$ только пять рациональных точек $(0, 1)(0, -1)$, $(-1, 0)$, $(2, 3)$, $(2, -3)$, а при $k = -432$ — лишь две рациональные точки $(12, 36)$ и $(12, -36)$.

4. Пусть $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ — многочлен с целыми коэффициентами. Предположим, что $a = \alpha^2 \neq 0$ является полным квадратом и что

$$8a^2 d - 4abc + b^3 \neq 0.$$

Положив

$$y = \alpha x^2 + \beta x + \gamma,$$

где $2\alpha\beta = b$, $2\alpha\gamma + \beta^2 = c$, показать, что кривая

$$y^2 = f(x)$$

имеет рациональную точку $P_0 = (x_0, y_0)$ с координатами

$$x_0 = \frac{64a^3 e - 16a^2 c^2 + 8ab^2 c - b^4}{8a^2 d - 4abc + b^3}$$

и

$$y_0 = \alpha x_0^2 + \beta x_0 + \gamma.$$

5. Доказать, что уравнение

$$y^2 = x^3 + 45$$

не разрешимо в целых числах x и y. (Указание: Рассмотреть соответствующее сравнение по модулю 24).

6. Доказать, что уравнение

$$x^4 - 17y^4 = 2z^2$$

не разрешимо во взаимно простых целых x, y, z и что соответствующее сравнение

$$x^4 - 17y^4 \equiv 2z^2 \pmod{p^n}$$

разрешимо при любом простом p и любом целом $n \geqslant 1$.

(Указание. Предположить, что уравнение $x^4 - 17y^4 = 2z^2$ разрешимо во взаимно простых целых x, y, z. Затем, установив с помощью квадратичного закона взаимности Гаусса, что каждый нечетный простой делитель p числа z является квадратичным вычетом по модулю 17, прийти к противоречию с тем, что 2 не является вычетом четвертой степени по модулю 17.)

7. Используя результат предыдущей задачи, показать, что эллиптическая кривая

$$2y^2 = x^4 - 17$$

имеет p-адические точки для каждого простого p и не имеет точек в поле рациональных чисел $\mathbb{Q}$.

8. Пусть a, b, c, d — бесквадратные целые числа с условием $c > b > a$. Используя теорему 3, а также результат Гурвица [38] о том, что кривая

$$A\colon\ ax^3 + by^3 + cz^3 + dxyz = 0$$

не имеет точек конечного порядка, доказать, что если A имеет хотя бы одну рациональную точку, то группа Морделла — Вейля $A(\mathbb{Q})$ этой кривой бесконечна.

(Указание. Провести касательную к рассматриваемой кривой в точке (x, y, z) с целыми взаимно простыми координатами x, y, z и показать, что при подходящем целом $m \geqslant 1$ она пересекает кривую A в точке (x', y', z') также с целыми взаимно простыми координатами

$$x' = \frac{x}{m}(by^3 - cz^3),\quad y' = \frac{y}{m}(cz^3 - ax^3),\quad z' = \frac{z}{m}(ax^3 - by^3),$$

удовлетворяющими условию $|x'y'z'| > |xyz|$.)

9. Доказать, что уравнение

$$y^2 = x^3 - 2$$

не разрешимо в целых $x \neq 3$ и $y \neq \pm 5$. (Указание. Воспользоваться соотношением

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

и однозначностью разложения на простые множители в кольце целых чисел поля $\mathbb{Q}(\sqrt{-2})$).

10. Пусть $\mathfrak{P}(z)$ — эллиптическая функция Вейерштрасса с решеткой периодов L, параметризующая эллиптическую кривую

$$E(\mathbb{C})\colon\ y^2 = x^3 + ax + b,\quad 4a^3 + 27b^2 \neq 0,$$

вложенную в комплексное проективное пространство $\mathbb{P}^2$. Доказать, что отображение

$$z \mapsto \left(1,\ \mathfrak{P}(z),\ \frac{1}{2}\mathfrak{P}'(z)\right)$$

задает аналитический изоморфизм комплексного тора $\mathbb{C}/L$ и кривой $E(\mathbb{C})$.

11. Доказать, что каждый комплексно-аналитический гомоморфизм

$$\lambda\colon\ \mathbb{C}/L \to \mathbb{C}/M$$

представляет собой умножение на такое комплексное число α, что $\alpha L \subset M$.

12. Доказать, что любое число α, $\alpha L \subset L$, задающее комплексно-аналитический эндоморфизм тора $\mathbb{C}/L$, является либо целым рациональным числом ($\alpha \in \mathbb{Z}$), либо элементом кольца целых чисел мнимого квадратичного поля (в последнем случае говорят, что соответствующая эллиптическая кривая $E(\mathbb{C})$ имеет *комплексное умножение*).

13. Доказать, что эллиптическая кривая

$$E(\mathbb{C}):\quad y^2 = x^3 + ax + b$$

допускает следующие автоморфизмы:
1) тождественный автоморфизм $(x, y) \mapsto (x, y)$;
2) $(x, y) \mapsto (x, -y)$, если $ab \neq 0$;
3) $(x, y) \mapsto (-x, \pm iy)$, если $a \neq 0$ и $b = 0$;
4) $(x, y) \mapsto (\rho^m x, \pm y)$, $1 \leqslant m \leqslant 2$, $\rho = e^{2\pi i/3}$, если $a = 0$ и $b \neq 0$.

14. Доказать, что кривые

$$E(\mathbb{C}):\ y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0,$$

и

$$E'(\mathbb{C}):\ y^2 = x^3 + a'x + b', \quad 4a'^3 + 27b'^2 \neq 0,$$

изоморфны между собой тогда и только тогда, когда равны их инварианты

$$\mathcal{J}(E) = \frac{a^3}{4a^3 + 27b^2} \quad \text{и} \quad \mathcal{J}(E') = \frac{a'^3}{4a'^3 + 27b'^2}.$$

15. Пусть f_n — функции на кривой

$$E(\mathbb{C}):\ y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0,$$

задаваемые соотношениями

$$f_1 = 1,$$
$$f_2 = 2y,$$
$$f_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$
$$f_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$$

и

$$f_{2m} = 2f_m\left(f_{m+2}f_{m-1} - f_{m+2}^2 f_{m+1}^2\right), \quad m \geqslant 3,$$
$$f_{2m+1} = f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3, \qquad m \geqslant 2.$$

Пусть, далее,

$$g_n = xf_n^2 - f_{n-1}f_{n+1},$$
$$4yh_n = f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2.$$

Используя формулы сложения точек на кривой $E(\mathbb{C})$, показать, что

$$(nx, ny) = \left(\frac{g_n}{f_n^2}, \frac{h_n}{f_n^3}\right).$$

16. Доказать, что группа $E_N(\mathbb{C})$ точек порядка N эллиптической кривой

$$E(\mathbb{C}):\ y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0,$$

изоморфна группе $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

17. Доказать, что группа $E(\mathbb{Q})$ рациональных точек эллиптической кривой Ферма

$$E:\ x^3 + y^3 = z^3$$

изоморфна $\mathbb{Z}/3\mathbb{Z}$.

18. Пусть (x, y) — произвольная точка эллиптической кривой

$$E:\ y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0,$$

и

$$t(x, y) = \int_0^x \frac{dx}{y}.$$

Доказать справедливость следующей теоремы Эйлера о сложении эллиптических интегралов: *для любых точек* (x_1, y_1) *и* (x_2, y_2) *кривой* E *существует такая третья точка* (x_3, y_3) *этой кривой, что*

$$t(x_1, y_1) + t(x_2, y_2) = t(x_3, y_3)$$

и координаты точки (x_3, y_3) *выражаются в виде рациональных функций с рациональными коэффициентами через координаты точек* (x_1, y_1) *и* (x_2, y_2). Вывести отсюда теорему сложения точек на кривой E.

ГЛАВА IV

ТЕОРЕМА РИМАНА — РОХА

Данная глава посвящена детальному изучению поля рациональных функций на проективной алгебраической кривой. Прежде чем перейти к такому изучению, напомним некоторые общие факты из алгебраической геометрии. Подробнее с этим читатель может познакомиться по книгам [132] и [144b].

§ 1. Аффинные и проективные многообразия

1. Аффинные алгебраические множества. Пусть k — алгебраически замкнутое поле произвольной характеристики и $n \geqslant 1$ — фиксированное целое число. Определим *n-мерное аффинное пространство* $\mathbb{A}^n$ над полем k как множество всех наборов $(x_1, \ldots, x_n)$ с компонентами из k. Элемент $x = (x_1, \ldots, x_n)$, $x_i \in k$, будем называть *точкой пространства* $\mathbb{A}_n$, а x_i — *координатами точки* x.

Положим $T = (T_1, \ldots, T_n)$ и рассмотрим кольцо многочленов $k[T] = k[T_1, \ldots, T_n]$ от неизвестных $T_1, \ldots, T_n$ с коэффициентами из k. *Нулем многочлена* $F \in k[T]$ назовем всякую точку $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$ такую, что $F(x) = 0$.

Алгебраическим (аффинным) множеством X называется множество общих нулей некоторой совокупности многочленов $F_i(T)$ из кольца $k[T]$.

Рассмотрим идеал $\mathfrak{a} \in k[T]$, порожденный совокупностью многочленов $F_i(T)$, задающих алгебраическое множество X. Тогда X можно представить как множество $V(\mathfrak{a})$ общих нулей всех многочленов $F \in \mathfrak{a}$. Всякий идеал $\mathfrak{a}$ такой, что $X = V(\mathfrak{a})$, назовем *определяющим идеалом* алгебраического множества X. Среди определяющих идеалов данного алгебраического множества X имеется наибольший идеал $\mathfrak{a}(X)$, состоящий из всех многочленов кольца $k[T]$, обращающихся в ноль во всех точках $x \in X$. Идеал $\mathfrak{a}(X)$ назовем *идеалом аффинного алгебраического множества* X. Поскольку кольцо $k[T]$ нётерово, то *любой его идеал имеет конечное число образующих*. Поэтому, если $F_1, \ldots, F_r$ — образующие идеала $\mathfrak{a}(X)$, так что

$$\mathfrak{a}(X) = k[T]F_1(T) + \ldots + k[T]F_r(T),$$

то X может быть задано также как множество общих нулей конечного числа многочленов $F_1, \ldots, F_r$.

Нетрудно видеть, что объединение конечного числа алгебраических множеств есть алгебраическое множество и что пересечение любого числа алгебраических множеств снова является алгебраическим множеством. Кроме того, пустое множество и все пространство $\mathbb{A}^n$ являются алгебраическими множествами. Следовательно, если алгебраические множества объявить замкнутыми, а их дополнения в $\mathbb{A}^n$ — открытыми множествами, то пространство $\mathbb{A}^n$ становится топологическим пространством. Введенная таким образом топология называется *топологией Зарисского* пространства $\mathbb{A}^n$. Любое открытое множество U, содержащее точку x, называется *окрестностью* этой точки, а пересечение всех замкнутых множеств, содержащих заданное множество Y, называется его *замыканием* и обозначается $\overline{Y}$.

Пример 1. Выясним, как устроена топология Зарисского аффинной прямой $\mathbb{A}^1$. Каждый идеал $\mathfrak{a}$ в кольце $k[T]$ многочленов от одного неизвестного T имеет вид $\mathfrak{a} = k[T]F(T)$ с некоторым $F \in k[T]$. Поэтому всякое алгебраическое множество в $\mathbb{A}^1$ — это множество нулей одного многочлена. Так как поле k алгебраически замкнуто, то любой ненулевой многочлен имеет в $k[T]$ разложение

$$F(T) = a(T - \alpha_1)\ldots(T - \alpha_m), \quad a, \alpha_1, \ldots, \alpha_m \in k.$$

В таком случае $V(\mathfrak{a}) = \{\alpha_1, \ldots, \alpha_m\}$ и, значит, алгебраическими множествами в $\mathbb{A}^1$ являются всевозможные конечные подмножества прямой $\mathbb{A}^1$. Отметим, в частности, что топология Зарисского прямой $\mathbb{A}^1$ не хаусдорфова.

Теорема Гильберта о нулях [32a]. *Пусть k — алгебраически замкнутое поле, $\mathfrak{a}$ — идеал в кольце $k[T] = k[T_1, \ldots, T_n]$ и $F \in k[T]$ — многочлен, обращающийся в ноль на $V(\mathfrak{a})$. Тогда $F^m \in \mathfrak{a}$ при некотором целом $m \geqslant 1$.*

Доказательство см. в [70d, с. 290], [8, с. 105] или в [52, т. 2, с. 195].

Определение 1. Пусть $\mathfrak{a}$ — идеал коммутативного кольца A с единицей. *Радикалом* $r(\mathfrak{a})$ идеала $\mathfrak{a}$ называется множество всех элементов $a \in A$ таких, что $a^m \in \mathfrak{a}$ при некотором целом $m \geqslant 1$.

Из теоремы Гильберта следует, что идеал $\mathfrak{a}(X)$ алгебраического множества X равен радикалу $r(\mathfrak{a})$ определяющего идеала $\mathfrak{a}$ этого множества. Более того, *имеется взаимно однозначное соответствие между алгебраическими множествами пространства $\mathbb{A}^n$ и радикальными идеалами (идеалами, совпадающими со своими радикалами) кольца $k[T_1, \ldots, T_n]$.*

Дадим теперь краткое описание топологии Зарисского пространства $\mathbb{A}^n$. Поскольку включение $Y \subset X$ равносильно включению $\mathfrak{a}(Y) \supset \mathfrak{a}(X)$ и поскольку, ввиду нётеровости кольца $k[T]$,

всякая возрастающая цепочка $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_s \subset \ldots$ идеалов кольца $k[T]$ стабилизируется, то *имеется взаимно однозначное соответствие между алгебраическими подмножествами Y алгебраического множества X и радикальными идеалами, содержащими $\mathfrak{a}(X)$, и топология Зарисского пространства $\mathbb{A}^n$ нётерова, то есть каждая убывающая цепочка $Y_1 \supset Y_2 \supset \ldots \supset Y_s \supset \ldots$ замкнутых множеств стабилизируется.*

Определение 2. Топологическое пространство X называется *неприводимым*, если его нельзя представить в виде объединения своих собственных замкнутых подмножеств. Это эквивалентно тому, что всякая пара непустых открытых подмножеств в X имеет непустое пересечение, а также тому, что любое непустое открытое множество $U \subset X$ всюду плотно в X (его замыкание $\overline{U}$ совпадает с X).

Из изложенного выше следует, что алгебраическое множество $X \subset \mathbb{A}^n$ (рассматриваемое как топологическое пространство) *неприводимо тогда и только тогда, когда идеал $\mathfrak{a}(X)$ множества X является простым идеалом* кольца $k[T]$. Напомним, что идеал $\mathfrak{p}$ коммутативного кольца A с единицей называется *простым*, если $\mathfrak{p} \neq A$ и из включения $xy \in \mathfrak{p}$ следует, что либо $x \in \mathfrak{p}$, либо $y \in \mathfrak{p}$. Идеал $\mathfrak{m}$ в A называется *максимальным*, если $\mathfrak{m} \neq A$ и не существует идеала $\mathfrak{a}$, удовлетворяющего условию $\mathfrak{m} \subset \mathfrak{a} \subset A$ (включения строгие). Легко видеть, что $\mathfrak{p}$ — простой идеал в том и только в том случае, если факторкольцо $A/\mathfrak{p}$ является областью целостности, и что $\mathfrak{m}$ — максимальный идеал тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

Определение 3. Неприводимое замкнутое подмножество X пространства $\mathbb{A}^n$ (с индуцированной топологией Зарисского) называется *аффинным алгебраическим многообразием*.

Нетрудно видеть, что аффинным многообразиям взаимно однозначно соответствуют простые идеалы кольца $k[T]$ (заметим, что всякий простой идеал радикален).

Пример 2. Пусть F — неприводимый многочлен из кольца $k[T] = k[T_1, \ldots, T_n]$. Поскольку $k[T]$ является кольцом с однозначным разложением на неприводимые множители, то многочлен F порождает в $k[T]$ простой идеал. Следовательно, множество нулей $X = V(\mathfrak{a})$ многочлена F неприводимо и, тем самым, является аффинным многообразием. При $n = 3$ многообразие $X = V(F)$ называется *поверхностью*, а при $n > 3$ — *гиперповерхностью*.

2. Регулярные отображения. *Функцией на алгебраическом множестве* X назовем всякое отображение X в поле k. При этом функция f на X называется *регулярной*, если она индуцирована некоторым многочленом $F \in k[T_1, \ldots, T_n]$. Другими словами, f регулярна, если $f(x) = F(x)$ для всех $x \in X$ $(f = F|_X)$.

Множество всех регулярных на X функций образует кольцо, обозначим его $k[X]$. Более того, это множество является конечно порожденной k-алгеброй. Имеет место естественный эпиморфизм

$$\alpha\colon\ k[T] \to k[X]$$

с ядром

$$\operatorname{Ker}\alpha = \{F \in k[T] \mid F|_X = 0\} = \mathfrak{a}(X),$$

переводящий F в $f = F|_X$ и задающий (в случае непустого X) k-изоморфизм

$$k[X] \simeq k[T]/\mathfrak{a}(X)$$

k-алгебр. Кольцо $k[X]$ называется *аффинным координатным кольцом* множества X.

Так как $k[X]$ есть гомоморфный образ кольца многочленов $k[T]$, то в $k[X]$ имеет место теорема о конечности базиса идеалов, а также следующий аналог теоремы Гильберта о нулях: *если функция $f \in k[X]$ обращается в нуль во всех точках $x \in X$, в которых обращаются в нуль функции $f_1, \ldots, f_r$, то*

$$f^m \in k[X]f_1 + \ldots + k[X]f_r.$$

Пусть Y — замкнутое подмножество алгебраического множества X. Множеству Y можно сопоставить идеал

$$\mathfrak{a}'(Y) = \{f \in k[X] \mid f|_Y = 0\}$$

кольца $k[X]$. Наоборот, каждый идеал $\mathfrak{a}'$ кольца $k[X]$ определяет идеал $\mathfrak{a}$ в $k[T]$, состоящий из всех прообразов элементов $f \in \mathfrak{a}'$ при гомоморфизме $\alpha\colon k[T] \to k[X]$. Идеал $\mathfrak{a}$ содержит в себе $\mathfrak{a}(X)$ и, значит, определяет замкнутое множество $Y \subset X$.

В частности, каждая точка $x \in X$ является замкнутым подмножеством и, стало быть, определяет идеал

$$\mathfrak{m}(x) = \{f \in k[X] \mid f(x) = 0\}.$$

По определению этот идеал является ядром гомоморфизма $k[X] \to k$, сопоставляющего каждой функции $f \in k[X]$ ее значение $f(x)$ в точке x. Так как $k[X]/\mathfrak{m}(x)$ — поле, то идеал $\mathfrak{m}(x)$ максимален. Наоборот, любой максимальный идеал $\mathfrak{m} \subset k[X]$ соответствует некоторой точке $x \in X$. Действительно, он определяет замкнутое подмножество Y множества X. Далее, для любой точки $y \in Y$ имеем $\mathfrak{m} \subset \mathfrak{m}(y)$, а так как $\mathfrak{m}$ максимален, то $\mathfrak{m} = \mathfrak{m}(y)$.

Определение 4. Пусть $X \subset \mathbb{A}^n$ и $Y \subset \mathbb{A}^m$ — замкнутые множества. Отображение $f\colon X \to Y$ называется *регулярным*, если существуют такие регулярные на X функции $f_1, \ldots, f_m$, что $f(x) = (f_1(x), \ldots, f_m(x))$ для всех $x \in X$.

Ясно, что регулярное отображение $f\colon X \to \mathbb{A}^m$, задаваемое функциями $f_1, \ldots, f_m$, будет отображением X в Y лишь в том случае, когда $f_1, \ldots, f_m$, как элементы кольца $k[X]$ удовлетворяют уравнениям множества Y.

Пусть $f\colon X \to Y$ — регулярное отображение X в Y и $g\colon Y \to k$ — произвольная функция на множестве Y. Отображение $f^* =$

$= g \circ f$ можно рассматривать как отображение функций на Y в функции на X. Ввиду этого f^* является отображением $k[Y]$ в $k[X]$ и, более того, гомоморфизма k-алгебры $k[Y]$ в k-алгебру $k[X]$. Справедливо и обратное утверждение, а именно, *всякий гомоморфизм k-алгебр* $\varphi\colon k[Y] \to k[X]$ *имеет вид* $\varphi = f^*$, *где* f — *некоторое регулярное отображение* X *в* Y.

Регулярное отображение $f\colon X \to Y$ замкнутых множеств называется *изоморфизмом*, если оно обладает обратным отображением $g\colon Y \to X$, $f \circ g = 1_Y$, $g \circ f = 1_X$, которое также регулярно. Алгебраические множества X и Y называются в этом случае *изоморфными*. Ясно, что если f — изоморфизм, то f^* является изоморфизмом k-алгебр $k[X]$ и $k[Y]$. Легко проверить, что справедливо и обратное, так что замкнутые множества изоморфны тогда и только тогда, когда их координатные кольца изоморфны над k.

Пример 3. Пусть $k = \bar{F}_q$ — алгебраическое замыкание конечного поля F_q характеристики p и X — алгебраическое множество, определяемое системой уравнений

$$P_i(T) = 0, \quad 1 \leqslant i \leqslant r,$$

где P_i — многочлены из кольца $F_q[T]$.

Рассмотрим отображение σ пространства $\mathbb{A}^n$, задаваемое формулой

$$\sigma(x_1, \ldots, x_n) = (x_1^q, \ldots, x_n^q).$$

Очевидно, что это регулярное отображение. Покажем, что оно переводит X в себя. Действительно, если $x \in X$, то $P_i(x) = 0$, и тогда по свойству поля F_q имеем

$$P_i(x_1^q, \ldots, x_n^q) = (P_i(x_1, \ldots, x_n))^q = 0.$$

Отображение $\sigma\colon X \to X$ называется *отображением Фробениуса*. Его значение заключается в том, что все точки $x \in X$ с координатами из F_q (и только они) остаются неподвижными под действием σ.

Пример 4. Проекция $f(x, y) = x$ гиперболы $xy = 1$ на ось x является регулярным отображением, но не является изоморфизмом, так как это отображение не взаимно однозначно: на гиперболе нет точки (x, y), для которой $f(x, y) = 0$.

Пример 5. Отображение $f(t) = (t^2, t^3)$ прямой на кривую $x^3 = y^2$ взаимно однозначно, однако оно не является изоморфизмом, так как обратное отображение имеет вид $f^{-1}(x, y) = y/x$, а функция y/x не регулярна в начале координат.

3. Рациональные функции на алгебраическом многообразии. Пусть алгебраическое множество X неприводимо. Тогда координатное кольцо $k[X]$ является областью целостности и его можно вложить в поле частных $k(X)$, называемое *полем рациональных функций* на X. Из определения поля частных следует, что $k(X)$ состоит из таких рациональных функций $\varphi = f/g$, $f, g \in k[X]$,

что $g \neq 0$ на X, причем считается, что $f/g = f'/g'$, если $fg' - f'g = 0$ на X.

Рациональная функция $\varphi \in k(X)$ называется *регулярной в точке* $x \in X$, если существует представление $\varphi = f/g$ такое, что $g(x) \neq 0$. В этом случае элемент $f(x)/g(x)$ поля K называется *значением функции* φ в точке x и обозначается $\varphi(x)$. Множество точек, в которых рациональная функция $\varphi \in k(X)$ регулярна, не пусто и открыто. Это множество называется *областью определения функции* φ и обозначается $D(\varphi)$.

Исходя из теоремы Гильберта о нулях в кольце $k[X]$, нетрудно убедиться, что рациональная функция φ, регулярная во всех точках замкнутого множества X, является регулярной функцией на X. Кроме того, из неприводимости X вытекает, что *если рациональная функция* φ *равна нулю на непустом открытом подмножестве из* $D(\varphi)$, *то она равна нулю на всем* X. Отсюда следует, в частности, что *две рациональные функции из* $k(X)$, *совпадающие на непустом открытом подмножестве их общей области определения, совпадают между собой на всем множестве* X.

В заключение укажем другой, обладающий большей общностью, способ построения поля $k(X)$.

Пусть A — коммутативное кольцо с единицей. *Мультипликативно замкнутым множеством* в A называется всякое подмножество $S \subset A$, содержащее 1 и замкнутое относительно умножения. Определим на $A \times S$ отношение равенства, положив $(a, b) = (a', b')$ в том и только в том случае, если $(ab' - a'b)c = 0$ для некоторого $c \in S$. Это отношение рефлексивно, симметрично и транзитивно. Поэтому оно определяет на $A \times S$ отношение эквивалентности. Класс эквивалентности пары (a, b) обозначим a/b, а множество всех таких классов — $S^{-1}A$. Введем на $S^{-1}A$ структуру кольца, определив сложение и умножение по правилам

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$

Кольцо $S^{-1}A$ называется *кольцом частных* A относительно S. Заметим, что если A — область целостности и $S = A - \{0\}$, то указанная конструкция приводит к полю частных кольца A. Отображение $\varphi\colon A \to S^{-1}A$, $\varphi(x) = x/1$, определяет гомоморфизм колец A и $S^{-1}A$. Вообще говоря, он не инъективен.

Если $\mathfrak{p}$ — простой идеал кольца A, то кольцо частных

$$A_{\mathfrak{p}} = \left\{ \frac{a}{b} \,\middle|\, a, b \in A, \quad b \notin \mathfrak{p} \right\}$$

относительно мультипликативно замкнутого множества $S = A - \mathfrak{p}$ называется *локализацией кольца* A относительно $\mathfrak{p}$. Это локальное кольцо с единственным максимальным идеалом

$$\mathfrak{m} = \left\{ \frac{a}{b} \in A_{\mathfrak{p}} \mid a \in \mathfrak{p} \right\}.$$

Пусть X — неприводимое замкнутое множество в $\mathbb{A}^n$, $\mathfrak{a}(X)$ — простой идеал в $k[T]$, соответствующий множеству X, и

$$\mathfrak{O}_X = \left\{ \frac{F}{G} \,\middle|\, F,\ G \in k[T],\ G \notin \mathfrak{a}(X) \right\}$$

— локализация кольца $k[T]$ относительно $\mathfrak{a}(X)$ с максимальным идеалом

$$\mathfrak{M}_X = \left\{ \frac{F}{G} \in \mathfrak{O}_X \mid F \in \mathfrak{a}(X) \right\}.$$

Если $\varphi = f/g$ — элемент поля $k(X)$ и F, G — многочлены из кольца $k[T]$ такие, что $F|_X = f$, $G|_X = g$ и $G \notin \mathfrak{a}(X)$, то соответствие

$$\alpha\colon\ \varphi \to \frac{F}{G} \pmod{\mathfrak{M}_X}$$

задает канонический изоморфизм между $k(X)$ и $\mathfrak{O}_X/\mathfrak{M}_X$. Следовательно, поле $k(X)$ можно отождествить с $\mathfrak{O}_X/\mathfrak{M}_X$.

4. Проективные и квазипроективные многообразия. Определим *n-мерное проективное пространство* $\mathbb{P}^n$ над полем k через соответствующее аффинное пространство $\mathbb{A}^{n+1}$. Назовем две точки $x = (x_0, x_1, \ldots, x_n)$ и $y = (y_0, y_1, \ldots, y_n)$ пространства $\mathbb{A}^{n+1}$ *эквивалентными*, если существует такой элемент $\lambda \in k$, $\lambda \neq 0$, *что* $x_i = \lambda y_i$ для всех $i = 0, 1, \ldots, n$. Затем *точками* $x = (x_0 : x_1 : \ldots : x_n)$ *пространства* $\mathbb{P}^n$ объявим классы эквивалентных между собой ненулевых точек пространства $\mathbb{A}^{n+1}$, определенных над k. Любой набор $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$, $\lambda \neq 0$, задающий точку $x \in \mathbb{P}^n$, будем называть *строкой однородных координат* этой точки.

Рассмотрим градуированное кольцо

$$k[T_0, T_1, \ldots, T_n] = \bigoplus_{m=0}^{\infty} k[T_0, T_1, \ldots, T_n]_m$$

многочленов от неизвестных $T_0, T_1, \ldots, T_n$ с коэффициентами из поля k, где $k[T_0, T_1, \ldots, T_n]_m$ — подгруппа однородных многочленов степени m. Скажем, что точка $x \in \mathbb{P}^n$ является *проективным нулем многочлена* $F \in k[T_0, T_1, \ldots, T_n]$, если F обращается в нуль в каждой строке однородных координат точки x. Легко видеть, что если $x \in \mathbb{P}^n$ — проективный нуль многочлена $F = F_0 + F_1 + \ldots + F_m$, то точка x является проективным нулем и каждой однородной компоненты F_i этого многочлена. Действительно, если $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$ — строка однородных координат точки x, то для всех $\lambda \in k^*$ будем иметь

$$F(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = F_0 + \lambda F_1 + \ldots + \lambda^m F_m = 0.$$

Поскольку поле k алгебраически замкнуто и, значит, содержит бесконечно много элементов, утверждение следует из того, что

отличный от нуля многочлен от одного неизвестного λ не может иметь бесконечного числа нулей.

Идеал $\mathfrak{a}$ кольца $k[T_0, T_1, \ldots, T_n]$ назовем *однородным*, если вместе с каждым своим многочленом F он содержит и все однородные компоненты этого многочлена. Скажем, что точка $x \in \mathbb{P}^n$ является *проективным нулем однородного идеала* $\mathfrak{a} \subset k[T_0, T_1, \ldots, T_n]$, если она является проективным нулем каждого многочлена, лежащего в $\mathfrak{a}$.

Определение 5. *Проективным алгебраическим множеством* $X \subset \mathbb{P}^n$ называется совокупность всех проективных нулей $V(\mathfrak{a})$ некоторого однородного идеала $\mathfrak{a}$. Всякий идеал $\mathfrak{a}$ такой, что $X = V(\mathfrak{a})$, называется *определяющим идеалом* проективного алгебраического множества X.

Среди определяющих идеалов $\mathfrak{a}$ данного проективного множества X имеется наибольший, обозначаемый $\mathfrak{a}(X)$. Он состоит из всех многочленов $F \in k[T_0, T_1, \ldots, T_n]$, обращающихся в нуль во всех точках $x \in X$. Из изложенного выше следует, что идеал $\mathfrak{a}(X)$, называемый *идеалом проективного алгебраического множества* X, является однородным.

Как и в аффинном случае, в пространстве $\mathbb{P}^n$ можно ввести топологию Зарисского, объявив замкнутыми множествами всевозможные алгебраические подмножества этого пространства. При этом нетрудно показать, что проективное алгебраическое множество X (рассматриваемое как топологическое пространство с индуцированной топологией Зарисского) неприводимо тогда и только тогда, когда однородный идеал $\mathfrak{a}(X)$ прост.

Определение 6. Неприводимое замкнутое подмножество пространства $\mathbb{P}^n$ (с индуцированной топологией Зарисского) называется *проективным алгебраическим многообразием* (или просто *проективным многообразием*).

Перейдем к рассмотрению рациональных функций на проективных многообразиях. Здесь встречаемся с важным различием между функциями от однородных и неоднородных координат: рациональная функция

$$f(T_0, T_1, \ldots, T_n) = \frac{P(T_0, T_1, \ldots, T_n)}{Q(T_0, T_1, \ldots, T_n)}$$

не может рассматриваться как функция точки $x \in \mathbb{P}^n$ даже в том случае, когда $Q(x) \neq 0$, ибо ее значение зависит от выбора однородных координат точки x. Однако если P и Q — однородные многочлены одной и той же степени и $Q(x) \neq 0$, то $f(x) = P(x)/Q(x)$ имеет в точке x вполне определенное значение, зависящее лишь от x.

Пусть X — неприводимое замкнутое множество в $\mathbb{P}^n$ и $\mathfrak{O}_X$ — локальное кольцо на X, состоящее из отношений F/G, $G \notin \mathfrak{a}(X)$, однородных многочленов F, G одинаковой степени. Единственным

максимальным идеалом этого кольца является идеал

$$\mathfrak{M}_X = \left\{\frac{F}{G} \in \mathfrak{O}_X \mid F \in \mathfrak{a}(X)\right\}.$$

Факторкольцо $\mathfrak{O}_X/\mathfrak{M}_X$ является полем, которое называется *полем рациональных функций на проективном многообразии* X и обозначается $k(X)$. Рациональная функция $f \in k(X)$ называется *регулярной в точке* $x \in X$, если существует представление $f = F/G$, в котором $G(x) \neq 0$. Множество точек регулярности функции f обозначается $D(f)$. Можно показать, что $D(f) = X$ в том и только в том случае, если $f = \text{const}$ (см. [144b, т. 1, гл. 1, § 5]).

Рассмотрим открытые подмножества

$$\mathbb{A}_i^n = \{x = (x_0: x_1: \ldots: x_n) \in \mathbb{P}^n \mid x_i \neq 0\}, \quad 0 \leqslant i \leqslant n,$$

пространства $\mathbb{P}^n$. Они покрывают, очевидным образом, пространство $\mathbb{P}^n$ и отображения φ_i: $\mathbb{A}_i^n \to \mathbb{A}^n$, переводящие $x = (x_0: x_1: \ldots: x_n) \in \mathbb{A}_i^n$ в $\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right) \in \mathbb{A}^n$, определяют взаимно однозначные соответствия между $\mathbb{A}_i^n$ и аффинным пространством $\mathbb{A}^n$.

Более того, каждое из отображений φ_i задает гомеоморфизм пространства $\mathbb{A}_i^n$ с индуцированной в нем топологией пространства $\mathbb{P}^n$ на пространство $\mathbb{A}^n$ с топологией Зарисского. Отсюда следует, что любое непустое проективное алгебраическое множество $X \subset \mathbb{P}^n$ содержит в себе открытые подмножества $X \cap \mathbb{A}_i^n$, которые, в свою очередь, являются аффинными алгебраическими множествами в $\mathbb{A}_i^n = \mathbb{A}^n$. В частности, каждая точка проективного алгебраического множества обладает открытой окрестностью, являющейся аффинным алгебраическим множеством.

Рассмотрим теперь понятие рациональной функции на алгебраическом многообразии. Пусть X — либо аффинное, либо проективное многообразие, и U — непустое открытое подмножество в X. Тогда U — всюду плотное в X неприводимое множество и, следовательно на U обычным образом возможно определить поле рациональных функций $k(U)$. Если X — аффинное многообразие, то из сказанного в п. 3 следует, что $k(U) = k(X)$. Аналогичное утверждение справедливо и в проективном случае. Указанное свойство аффинных и проективных многообразий совместно с тем фактом, что открытые подмножества $X \cap \mathbb{A}_i^n$ проективного алгебраического множества $X \subset \mathbb{P}^n$ являются аффинными алгебраическими множествами, приводят к следующему более общему понятию многообразия.

Определение 7. *Квазипроективным многообразием* называется открытое подмножество проективного многообразия.

Очевидно, что проективные многообразия являются квазипроективными, нетрудно показать, что и аффинные многообразия также являются квазипроективными многообразиями. Далее, легко видеть, что квазипроективные многообразия являются неприводимыми множествами. *Рациональные функции на квазипроективном многообразии* X определяются как рациональные функции на открытом подмножестве X проективного многообразия $\bar{X}$.

Прежде чем ввести следующее новое понятие установим, что две точки $x = (x_0 : x_1 : \ldots : x_m)$ и $y = (y_0 : y_1 : \ldots : y_m)$ проективного пространства $\mathbb{P}^m$ равны между собой тогда и только тогда, когда $x_i y_j = x_j y_i$ для всех $i, j = 0, 1, \ldots, m$. Действительно, если $x = y$, то существует такой элемент $\lambda \in k^*$, что $y_j = \lambda x_j$, и, в таком случае, $x_i y_j = \lambda x_i x_j = y_i x_j = x_j y_i$. Обратно, если $x_i y_j = x_j y_i$ для всех i, j и если $x_{i_0} \neq 0$, то $x_{i_0} y_j = x_i y_{j_0}$ для всех $j = 0, 1, \ldots, m$ и, значит $y_j = \lambda x_j$.

Определение 8. Пусть X — квазипроективное многообразие в $\mathbb{P}^n$. *Рациональным отображением* φ: $X \to \mathbb{P}^m$ называется отображение, задаваемое набором $\varphi = (\varphi_0, \varphi_1, \ldots, \varphi_m)$ рациональных функций поля $k(X)$, из которых хотя бы одна не равна нулю на X. Набор $\psi = (\psi_0, \psi_1, \ldots, \psi_m)$ задает то же самое рациональное отображение, если $\varphi_i \psi_j = \varphi_j \psi_i$ для всех $i, j = 0, 1, \ldots, m$.

Рациональное отображение φ называется *регулярным в точке* $x \in X$, если существует представление $\varphi = (\varphi_0, \varphi_1, \ldots, \varphi_m)$, в котором все функции φ_i регулярны в точке x (в этом случае $\varphi(x) = (\varphi_0(x): \varphi_1(x): \ldots : \varphi_m(x))$). *Областью определения* $D(\varphi)$ отображения φ называется множество всех точек $x \in X$, в которых все φ_i регулярны хотя бы для одного представления $\varphi = (\varphi_0 : \varphi_1 : \ldots : \varphi_m)$.

Определение 9. Пусть $X \subset \mathbb{P}^n$ и $Y \subset \mathbb{P}^m$ — квазипроективные многообразия. Отображение φ: $X \to Y$ называется *рациональным*, если оно является рациональным отображением X в $\mathbb{P}^m$ и если найдется такое открытое множество $U \subset D(\varphi)$, что $\varphi(U) \subset Y$. Наибольшее из множеств U с указанным свойством обозначается $D_Y(\varphi)$. Рациональное отображение φ: $X \to Y$ называется *регулярным*, если $D_Y(\varphi) = X$ или, другими словами, если $\varphi(X) \subset Y$.

Последнему определению можно придать иную, более удобную для применений форму. Рассмотрим наборы $(F_0 : F_1 : \ldots : F_m)$ однородных многочленов $F_i \in k[T_0, T_1, \ldots, T_m]$ одной и той же степени. Набор $(F_0 : F_1 : \ldots : F_m)$ назовем *допустимым*, если из условия, что $F_i(x) \neq 0$ для некоторого $x \in X$ и некоторого i, следует, что $(F_0(x): F_1(x): \ldots : F_m(x)) \in Y$. Далее, два допустимых набора $(F_0 : F_1 : \ldots : F_m)$ и $(G_0 : G_1 : \ldots : G_m)$ будем считать эквивалентными, если $F_i G_j - G_i F_j = 0$ на X для всех i, j. Систему S допустимых эквивалентных наборов назовем *полной*, если для

любой точки $x \in X$ в системе S найдется допустимый набор $(F_0 : F_1 : \ldots : F_m)$, у которого $F_i(x) \neq 0$ для некоторого $i = 0, 1, \ldots, m$.

Пусть S — полная система эквивалентных допустимых наборов. Отображение $\varphi\colon X \to Y$ называется *регулярным*, если в каждой точке $x \in X$ его можно представить в виде

$$\varphi(x) = (F_0(x) : F_1(x) : \ldots : F_m(x)),$$

где $(F_0 : F_1 : \ldots : F_m) \in S$ и $F_i(x) \neq 0$, хотя бы для одного $i = 0, 1, \ldots, m$.

Определение 10. Регулярное отображение $\varphi\colon X \to Y$ квазипроективных многообразий называется *изоморфизмом*, если оно обладает обратным регулярным отображением $\psi\colon Y \to X$, $\varphi \circ \psi = 1_Y$, $\psi \circ \varphi = 1_X$. Многообразия X и Y называются в этом случае *изоморфными*.

Квазипроективные многообразия X и Y называются *бирационально изоморфными*, если существуют взаимно обратные рациональные отображения $\varphi\colon X \to Y$ и $\psi\colon Y \to X$.

Справедливо следующее утверждение (см., например, [144b, т. 1, с. 62—63]).

Теорема 1. *Квазипроективные многообразия X и Y бирационально изоморфны тогда и только тогда, когда изоморфны поля $k(X)$ и $k(Y)$ рациональных функций на X и Y. Многообразия X и Y бирационально изоморфны в том и только в том случае, если в них содержатся изоморфные друг другу открытые подмножества.*

Отметим, что понятие бирационального изоморфизма грубее понятия изоморфизма, так как существуют бирационально изоморфные многообразия, не изоморфные между собой.

5. **Неособые алгебраические многообразия.** Понятие неособой точки многообразия X можно определить в терминах частных производных функций, задающих X, используя при этом понятие размерности многообразия.

Определение 11. Пусть X — топологическое пространство. Определим его *размерность* $\dim X$ как верхнюю грань множества тех целых n, для которых существует цепочка $X_0 \subset X_1 \subset \ldots \subset X_n$ различных неприводимых подмножеств в X. Размерностью аффинного, проективного и квазипроективного многообразия назовем его размерность как топологического пространства.

Определение 12. Пусть $X \subset \mathbb{A}^n$ — аффинное многообразие и $F_1, \ldots, F_r \in k[T_1, \ldots, T_n]$ — образующие идеала $\mathfrak{a}(X)$. Многообразие X называется *неособым в точке* $x \in X$, если ранг матрицы

$$\left\| \frac{\partial F_i(x)}{\partial x_j} \right\|_{\substack{1 \leqslant i \leqslant r, \\ 1 \leqslant j \leqslant n}}$$

равен $n - s$, где s — размерность многообразия X. В этом случае

точка x называется *неособой точкой* рассматриваемого многообразия. Многообразие называется *неособым*, если оно неособо в каждой своей точке.

Недостатком данного определения является то, что оно зависит от вложения X в аффинное пространство. Дадим внутреннее описание понятия неособенности, свободное от этого недостатка и основанное на использовании локального кольца точки.

Определение 13. Пусть X — квазипроективное многообразие. *Локальным кольцом* $\mathfrak{o}_x$ *точки* $x \in X$ называется совокупность всех рациональных функций $f \in k(X)$, регулярных в точке x.

Единственным максимальным идеалом кольца $\mathfrak{o}_x$ является идеал

$$\mathfrak{m}_x = \{f \in \mathfrak{o}_x \mid f(x) = 0\},$$

состоящий из всех необратимых элементов кольца $\mathfrak{o}_x$.

Если X — аффинное многообразие, $k[X]$ — его координатное кольцо и

$$\mathfrak{m}(x) = \{f \in k[X] \mid f(x) = 0,\ x \in X\}$$

— максимальный идеал этого кольца, то легко видеть, что $\mathfrak{o}_x$ представляет собой локализацию $k[X]_{\mathfrak{m}(x)}$ кольца $k[X]$ относительно простого идеала $\mathfrak{m}(x)$.

При изучении определенных свойств многообразия X иногда достаточно их изучения в некоторой окрестности произвольной точки $x \in X$. Такие свойства будем называть локальными. Квазипроективные многообразия (как и проективные) локально устроены как аффинные многообразия. Именно, *каждая точка x квазипроективного многообразия X имеет окрестность, изоморфную аффинному многообразию.* Далее, если U — окрестность точки $x \in X$, то из равенства $k(U) = k(X)$ следует, что локальное кольцо $\mathfrak{o}_x$ точки x совпадает с множеством функций $f \in k(U)$, регулярных в x. Стало быть, понятие кольца $\mathfrak{o}_x$ также является локальным и, значит, при изучении свойств локальных колец можно ограничиться аффинными многообразиями.

Локальное кольцо $\mathfrak{o}_x$ точки x квазипроективного многообразия X является, кроме того, нётеровым. Для доказательства этого утверждения достаточно установить нётеровость кольца $\mathfrak{o}_x = k[X]_{\mathfrak{m}(x)}$ в случае аффинного многообразия X. Справедливость же последнего утверждения вытекает из следующего общего факта (см. [144b, т. 1, с. 106]).

Предложение 1. *Если A — нётерово кольцо, то его локализация $A_\mathfrak{p}$ относительно каждого простого идеала $\mathfrak{p}$ также является нётеровым кольцом.*

Пусть $\mathfrak{m}_x$ — максимальный идеал кольца $\mathfrak{o}_x$. Будем рассматривать $\mathfrak{m}_x/\mathfrak{m}_x^2$ как векторное пространство над полем вычетов $\mathfrak{o}_x/\mathfrak{m}_x$. Поскольку $\mathfrak{o}_x$ — нётерово кольцо, пространство $\mathfrak{m}_x/\mathfrak{m}_x^2$ конечномерно. Далее, так как поле $\mathfrak{o}_x/\mathfrak{m}_x$ изоморфно полю k, то $\mathfrak{m}_x/\mathfrak{m}_x^2$ можно

рассматривать как векторное пространство над полем k. Размерность пространства $\mathfrak{m}_x/\mathfrak{m}_x^2$ над полем $\mathfrak{o}_x/\mathfrak{m}_x$ или, что то же самое, его размерность над k обозначим $\dim \mathfrak{m}_x/\mathfrak{m}_x^2$.

Определим теперь размерность $\dim X$ аффинного многообразия X в терминах его координатного кольца $k[X]$. Поскольку замкнутые неприводимые подмножества многообразия $X \subset \mathbb{A}^n$ соответствуют простым идеалам кольца $k[T_1, \ldots, T_n]$, содержащим идеал $\mathfrak{a}(X)$, а последние, в свою очередь, соответствуют простым идеалам координатного кольца $k[X]$, то размерность $\dim X$ многообразия X можно трактовать как наибольшую из длин цепочек отличных друг от друга простых идеалов в $k[X]$.

Определение 14. *Высотой $h(\mathfrak{p})$ простого идеала $\mathfrak{p}$* в кольце A называется верхняя грань множества тех целых m, для которых существует цепочка $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_m = \mathfrak{p}$ отличных друг от друга простых идеалов. *Размерностью* $\dim A$ *кольца* A называется верхняя грань высот множества всех его простых идеалов.

Таким образом, размерность аффинного многообразия X может быть определена как размерность его координатного кольца $k[X]$.

Чтобы придать размерности локальный характер, воспользуемся следующими утверждениями.

Предложение 2. *Пусть $A_\mathfrak{p}$ — локализация кольца A относительно простого идеала $\mathfrak{p}$. Все простые идеалы кольца $A_\mathfrak{p}$ находятся во взаимно однозначном соответствии с простыми идеалами кольца A, содержащимися в $\mathfrak{p}$.*

Доказательство см. в [8, с. 56—57].

Предложение 3. *Пусть k — некоторое поле и A — целостное кольцо, являющееся конечно порожденной k-алгеброй. Тогда для любого простого идеала $\mathfrak{p}$ кольца A имеет место соотношение*

$$h(\mathfrak{p}) + \dim A/\mathfrak{p} = \dim A.$$

Размерность кольца A равна степени трансцендентности его поля частных над k.

Доказательство см. в [84, гл. 5, § 14], в [8, гл. II] и в [52, т. 2, гл. 7, § 10].

Пусть x — точка аффинного многообразия X и $\mathfrak{m}(x)$ — максимальный идеал координатного кольца $k[X]$, соответствующий точке x. Так как $\mathfrak{o}_x = k[X]_{\mathfrak{m}(x)}$, то в соответствии с предложением 2 имеем $\dim \mathfrak{o}_x = h(\mathfrak{m}(x))$. С другой стороны, так как $k[X]/\mathfrak{m}(x) \simeq k$, то из предложения 3 получаем $h(\mathfrak{m}(x)) = \dim k[X]$. Следовательно,

$$\dim X = \dim k[X] = \dim \mathfrak{o}_x.$$

Определение 15. Пусть A — нётерево кольцо с максимальным идеалом $\mathfrak{m}$ и полем вычетов $k = A/\mathfrak{m}$. Кольцо A называется *регулярным*, если $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim A$.

Справедливо следующее утверждение (см. [132, гл. 1, § 5]).

Теорема 2. *Аффинное многообразие $X \subset \mathbb{A}^n$ тогда и только тогда неособо в точке $x \in X$, когда локальное кольцо этой точки $\mathfrak{o}_x$ регулярно.*

Исходя из сказанного, приходим к следующему определению неособой точки квазипроективного многообразия.

Определение 16. Квазипроективное многообразие X называется *неособым в точке* $x \in X$, если локальное кольцо $\mathfrak{o}_x$ этой точки является регулярным. Многообразие X называется *неособым*, если оно неособо в каждой своей точке, и *особым* в противном случае. Точка, в которой локальное кольцо не регулярно, называется *особой точкой* многообразия X.

Дадим, наконец, описание неособой точки аффинного многообразия в терминах касательного пространства.

Пусть аффинное многообразие $X \subset \mathbb{A}^n$ определено своим идеалом $\mathfrak{a}(X) = k[T]F_1 + \ldots + k[T]F_r$. Линейная форма

$$d_x F = \sum_{i=1}^{n} \frac{\partial F(x)}{\partial x_i}(T_i - x_i)$$

называется *дифференциалом многочлена* $F \in k[T]_n$ в точке $x = (x_1, \ldots, x_n)$, а множество точек пространства $\mathbb{A}^n$, удовлетворяющих системе линейных уравнений

$$d_x F_1 = \ldots = d_x F_r = 0,$$

называется *касательным пространством* Θ_x многообразия X в точке $x \in X$. Если

$$d_x\left(\frac{F}{G}\right) = \frac{G d_x F - F d_x G}{G^2}, \quad G(x) \neq 0.$$

— дифференциал рациональной функции F/G, $F, G \in k[T]$, в точке x и $f \in \mathfrak{o}_x$ — ограничение функции F/G на X, то *дифференциалом $d_x f$ функции f* является ограничение

$$d_x f = d_x\left(\frac{F}{G}\right)\Big|_{\Theta_x}$$

дифференциала $d_x\left(\frac{F}{G}\right)$ на подпространстве $\Theta_x \subset \mathbb{A}^n$. Легко показать, что $d_x f$ не зависит от конкретного выбора рациональной функции F/G, индуцирующей f.

Введенное выше дифференцирование задает гомоморфизм d_x: $\mathfrak{o}_x \to \Theta_x^*$ локального кольца $\mathfrak{o}_x$ в пространство Θ_x^* линейных форм на Θ_x. Так как $d_x \alpha = 0$ для любого $\alpha \in k$, то изучение этого гомоморфизма можно заменить изучением гомоморфизма d_x: $\mathfrak{m}_x \to \Theta_x^*$. Нетрудно показать, что *гомоморфизм d_x: $\mathfrak{m}_x \to \Theta_x^*$ определяет изоморфизм пространств $\mathfrak{m}_x/\mathfrak{m}_x^2$ и Θ_x^**. Следовательно, $\mathfrak{m}_x/\mathfrak{m}_x^2$

можно рассматривать как касательное пространство квазипроективного многообразия X в точке $x \in X$. При этом точка $x \in X$ является неособой точкой этого многообразия в том и только в том случае, если $\dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 = \dim X$. Если же $\dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 > \dim X$, то x является особой точкой многообразия X.

Задачи

1. Пусть $X = \{x\}$ — одноточечное множество пространства $\mathbb{A}^n$. Найти семейство многочленов, задающее алгебраическое множество X, и идеал этого алгебраического множества.

2. Установить связь между идеалами алгебраических множеств X, $Y \subset \mathbb{A}^n$ и идеалами алгебраических множеств $X \cup Y$ и $X \cap Y$.

3. Пусть $\mathfrak{a}$, $\mathfrak{b}$ — идеалы кольца A с единицей. Их *суммой* $\mathfrak{a} + \mathfrak{b}$ называется множество всех сумм $x + y$, $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. Это — наименьший идеал, содержащий $\mathfrak{a}$ и $\mathfrak{b}$. *Произведением* $\mathfrak{a}\mathfrak{b}$ *идеалов* $\mathfrak{a}$ и $\mathfrak{b}$ называется множество всех конечных сумм $\sum x_i y_i$, где $x_i \in \mathfrak{a}$, $y_i \in \mathfrak{b}$.

Установить справедливость следующих свойств радикала $r(\mathfrak{a})$ идеала $\mathfrak{a}$:

а) $r(r(\mathfrak{a})) = r(\mathfrak{a})$;

б) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$;

в) $r(\mathfrak{a}) = A \Leftrightarrow \mathfrak{a} = A$;

г) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$;

д) если $\mathfrak{p}$ — простой идеал, то $r(\mathfrak{p}^m) = r(\mathfrak{p})$ для всех целых $m \geqslant 1$.

4. Пусть A — некоторое кольцо с единицей и X — множество всех его простых идеалов. Для всякого подмножества $E \subset A$ обозначим $V(E)$ множество всех простых идеалов, содержащих E. Доказать справедливость следующих утверждений:

а) если $\mathfrak{a}$ — идеал, порожденный множеством E, то $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$;

б) $V(0) = X$, $V(A) = \varnothing$;

в) множества $V(E)$ удовлетворяют аксиомам для замкнутых множеств в топологическом пространстве (соответствующая топология на X называется *топологией Зарисского*, а топологическое пространство X называется *простым спектром кольца* A и обозначается $\operatorname{Spec} A$).

5. Изобразить пространства $\operatorname{Spec}\mathbb{Z}$, $\operatorname{Spec}\mathbb{R}$, $\operatorname{Spec}\mathbb{C}[x]$, $\operatorname{Spec}\mathbb{R}[x]$, $\operatorname{Spec}\mathbb{Z}[x]$. Здесь $\mathbb{C}[x]$, $\mathbb{R}[x]$ и $\mathbb{Z}[x]$ — кольца многочленов от неизвестного x с комплексными, действительными и целыми коэффициентами соответственно.

6. Пусть x — точка пространства $X = \operatorname{Spec} A$. Если x рассматривается как идеал в A, будем обозначать ее $\mathfrak{p}_x$. Пусть, далее, $\bar{Y}$ — замыкание множества $Y \subset X$ в топологии пространства X.

Доказать справедливость следующих утверждений:

а) точка x *замкнута* в $X = \operatorname{Spec} A$ тогда и только тогда, когда идеал $\mathfrak{p}_x$ максимален;

б) $\bar{x} = V(\mathfrak{p}_x)$;

в) $y \in \bar{x} \Leftrightarrow \mathfrak{p}_x \subset \mathfrak{p}_y$ (включение нестрогое).

7. Представление замкнутого множества $X \subset \mathbb{A}^n$ в виде $X = \bigcup\limits_i X_i$, где $X_i \not\subset X_j$ при $i \neq j$, называется *несократимым разложением* X на неприводимые замкнутые подмножества X_i, называемые *неприводимыми компонентами* X. Доказать, что несократимое представление замкнутого множества единственно.

8. Пусть X — алгебраическое множество в $\mathbb{A}^3$, определенное уравнениями $x^2 - yz = 0$ и $xz - x = 0$. Показать, что несократимое разложение X содержит три компоненты. Описать эти компоненты и найти их простые идеалы.

9. Пусть $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ — замкнутые множества. Множество пар (x, y), где $x \in X$, $y \in Y$, называется *произведением* X и Y и обозначается $X \times Y$. Доказать, что произведение неприводимых замкнутых множеств неприводимо.

10. Показать, что при естественном отождествлении $\mathbb{A}^{m+n} = \mathbb{A}^m \times \mathbb{A}^n$ топология Зарисского на $\mathbb{A}^{m+n}$ не совпадает с произведением топологий Зарисского на $\mathbb{A}^m$ и $\mathbb{A}^n$.

11. Пусть $f\colon X \to Y$ — регулярное отображение замкнутых множеств $X \subset \mathbb{A}^n$ и $Y \subset \mathbb{A}^m$. Подмножество $T \subset X \times Y$, состоящее из точек $(x, f(x))$, называется *графиком отображения* f. Доказать справедливость следующих утверждений:

а) T — замкнутое подмножество в $X \times Y$;

б) T изоморфно X.

12. Доказать, что любое неприводимое замкнутое множество $X \subset \mathbb{A}^n$ бирационально изоморфно гиперповерхности в некотором аффинном пространстве $\mathbb{A}^m$.

(Указание. Воспользоваться тем, что координатные функции $t_1, \ldots, t_n$ поля $k(X)$ алгебраически зависимы над k, и представить поле $k(X)$ в виде $k(X) = k(y_1, \ldots, y_m, y_{m+1})$, где $y_1, \ldots, y_m$ — алгебраически независимы над k и

$$F(y_1, \ldots, y_m, y_{m+1}) = 0,$$

причем многочлен F неприводим над полем k и $\dfrac{\partial F}{\partial y_{m+1}} \neq 0$.)

13. Доказать, что алгебра A над полем k тогда и только тогда изоморфна кольцу $k[X]$, где X — неприводимое замкнутое множество в $\mathbb{A}^n$, когда A не имеет делителей нуля и порождена над k конечным числом элементов. Вывести отсюда, что расширение K поля k тогда и только тогда изоморфно полю $k(X)$, когда оно порождено конечным числом элементов.

14. Доказать, что отображение f из примера 5 является бирациональным изоморфизмом (следовательно, понятие бирационального изоморфизма является более грубым по сравнению с понятием изоморфизма).

15. Доказать справедливость однородной теоремы Гильберта о нулях: *если $\mathfrak{a} \subset k[T_0, T_1, \ldots, T_n]$ — однородный идеал и $F \in k[T_0, T_1, \ldots, T_n]$ — однородный многочлен положительной степени, обращающийся в нуль во всех точках множества $V(\mathfrak{a}) \subset \mathbb{P}^n$, то $F^m \in \mathfrak{a}$ при некотором целом $m \geqslant 1$.*

(Указание. Переформулировать задачу в терминах пространства $\mathbb{A}^{n+1}$ и воспользоваться обычной теоремой Гильберта о нулях.)

16. Многообразие X называется *рациональным*, если оно бирационально изоморфно пространству $\mathbb{P}^n$ для некоторого $n \geqslant 1$. Доказать справедливость следующих утверждений:

а) любая *коника* в $\mathbb{P}^2$ (кривая, определяемая неприводимым однородным многочленом $F(T_0, T_1, T_2)$ степени 2) является рациональной кривой;

б) кубика $y^2 = x^3$ является рациональной кривой.

17. Пусть X — квазипроективное многообразие и $x \in X$. Показать, что существует взаимно однозначное соответствие между простыми идеалами локального кольца $\mathfrak{o}_x$ и замкнутыми подмногообразиями в X, содержащими точку x.

18. Пусть $X \subset \mathbb{P}^n$ — проективное многообразие размерности s с идеалом $\mathfrak{a}(X)$, порожденным многочленами $F_1, \ldots, F_r \in k[T_0, T_1, \ldots, T_n]$, и пусть $x = (x_0 : x_1 : \ldots : x_n)$ — точка многообразия X. Показать, что точка

$x \in X$ неособа в том и только в том случае, если ранг матрицы $\left\| \frac{\partial F_i(x)}{\partial x_j} \right\|$ равен $n - s$.

(Указание. Рассмотреть соответствующую аффинную якобиеву матрицу и воспользоваться теоремой Эйлера об однородных функциях.)

19. Пусть A — коммутативное кольцо с единицей и $\operatorname{Spec} A$ — спектр этого кольца. С каждой точкой $x \in \operatorname{Spec} A$ связано локальное кольцо $\mathfrak{o}_x$ — это локальное кольцо соответствующего простого идеала $\mathfrak{p}_x \subset A$ (см. задачу 6). Точка $x \in \operatorname{Spec} A$ называется *неособой* (*регулярной*), если ее локальное кольцо $\mathfrak{o}_x$ нётерово и регулярно.

Пусть $\mathfrak{m}_x$ — максимальный идеал кольца $\mathfrak{o}_x$. Тогда $\mathfrak{o}_x/\mathfrak{m}_x = k(x)$, и $\mathfrak{m}_x/\mathfrak{m}_x^2$ является векторным пространством над полем $k(x)$ (которое конечномерно в случае, если $\mathfrak{o}_x$ — нётерово). Векторное пространство

$$\Theta_x = \operatorname{Hom}_{k(x)}\left(\mathfrak{m}_x/\mathfrak{m}_x^2,\ k(x)\right)$$

называется *касательным пространством* к $\operatorname{Spec} A$ в точке x.

Найти касательное пространство к $\operatorname{Spec} \mathbb{Z}$ в точке $x = (0)$ и в точках $x = \mathfrak{p} \neq (0)$.

§ 2. Дивизоры на алгебраических кривых

1. Локальное кольцо точки. Всюду на протяжении этой и последующей глав под алгебраической кривой будем понимать неособое одномерное проективное многообразие. При этом мы не теряем общности, поскольку (см., например, [132, с. 70]) всякая алгебраическая кривая бирационально изоморфна неособой проективной кривой.

Пусть $\mathfrak{o}_x$ — локальное кольцо точки x кривой X и $\mathfrak{m}_x$ — максимальный идеал кольца $\mathfrak{o}_x$.

Лемма. *Справедливо соотношение*

$$\bigcap_{n=1}^{\infty} \mathfrak{m}_x^n = (0).$$

Доказательство. Пусть $\alpha \in \bigcap_{n=1}^{\infty} \mathfrak{m}_x^n$. Тогда $\alpha \in \mathfrak{m}_x^n$ для всех $n = 1, 2, \ldots$. Так как кольцо $\mathfrak{o}_x$ нётерово, то

$$\mathfrak{m}_x = \mathfrak{o}_x u_1 + \ldots + \mathfrak{o}_x u_r = (u_1, \ldots, u_r)$$

и, значит, идеал $\mathfrak{m}_x^n$ порождается всевозможными произведениями $u_{i_1} \ldots u_{i_n}$, $1 \leqslant i_1, \ldots, i_n \leqslant r$. Это равносильно тому, что всякий элемент $\alpha \in \mathfrak{m}_x^n$ имеет вид $\alpha = F_n(u_1, \ldots, u_r)$, где $F_n \in \mathfrak{o}_x[T_1, \ldots, T_r]$ — однородный многочлен степени n. Пусть $\mathfrak{a}$ — идеал в кольце $\mathfrak{o}_x[T_1, \ldots, T_r)$, порожденный всеми такими многочленами $F_n(T_1, \ldots, T_r)$, $n = 1, 2, \ldots$ Поскольку кольцо $\mathfrak{o}_x$ нётерово, то по теореме Гильберта о базисе (см., например, [8, с. 100]) кольцо $\mathfrak{o}_x[T_1, \ldots, T_r]$ также нётерово, и, следовательно, идеал $\mathfrak{a}$ имеет конечный базис, скажем $\mathfrak{a} = (F_{n_1}, \ldots, F_{n_s})$, $n_i \geqslant 1$, который можно составить из тех многочленов F_n, для которых $F_n(u_1, \ldots, u_r) = \alpha$. При каждом фиксированном $n > \max\limits_{1 \leqslant i \leqslant s} n_i$ имеем

$$F_n(T_1, \ldots, T_r) = \sum_{i=1}^{s} G_i(T_1, \ldots, T_r) F_{n_i}(T_1, \ldots, T_r),$$

где G_i — однородные многочлены степени $n - n_i$. Положим $T_1 = u_1, \ldots, T_r = u_r$. Так как $G_i(u_1, \ldots, u_r) \in \mathfrak{m}_x^{n-n_i} \subset \mathfrak{m}_x$, то для элемента $\alpha \in \mathfrak{m}_x^n$ получаем представление

$$\alpha = F_n(u_1, \ldots, u_r) = \sum_{i=1}^{s} G_i(u_1, \ldots, u_r)\alpha = \alpha \sum_{i=1}^{s} G_i(u_1, \ldots, u_r) = \alpha\beta,$$

где $\beta \in \mathfrak{m}_x$. Отсюда следует, что $\alpha(1 - \beta) = 0$, а поскольку $1 - \beta$ — обратимый в кольце $\mathfrak{o}_x$ элемент, то $\alpha = 0$. Лемма доказана.

Теорема 1. *Пусть x — точка кривой X. Тогда*

1) *каждый идеал $\mathfrak{a}$ кольца $\mathfrak{o}_x$, $\mathfrak{a} \neq (0)$, $\mathfrak{a} \neq \mathfrak{o}_x$, является некоторой степенью идеала $\mathfrak{m}_x$;*

2) *$\mathfrak{m}_x$ — единственный ненулевой простой идеал в кольце $\mathfrak{o}_x$;*

3) *$\mathfrak{o}_x$ — кольцо главных идеалов.*

Доказательство. 1) Так как $\mathfrak{a} \neq \mathfrak{o}_x$, то $\mathfrak{a} \subset \mathfrak{m}_x$. Из леммы следует существование такого целого $n \geqslant 1$, что $\mathfrak{a} \subset \mathfrak{m}_x^n$ и $\mathfrak{a} \not\subset \mathfrak{m}_x^{n+1}$. Значит, найдется такой элемент $\alpha \in \mathfrak{a} \subset \mathfrak{m}_x^n$, что $\alpha \notin \mathfrak{m}_x^{n+1}$. Идеал $\mathfrak{m}_x$ — главный, т. е. $\mathfrak{m}_x = t\mathfrak{o}_x$, и, стало быть, $\alpha = t^n u$, где $u \in \mathfrak{o}_x$. Поскольку $\alpha \notin \mathfrak{m}_x^{n+1}$, то $u \notin \mathfrak{m}_x$ и, следовательно, u — обратимый в кольце $\mathfrak{o}_x$ элемент. В таком случае, $t^n = \alpha u^{-1} \in \mathfrak{a}$ и тогда $\mathfrak{m}_x^n \subset \mathfrak{a}$. Значит, $\mathfrak{a} = \mathfrak{m}_x^n$.

2) Так как всякий нетривиальный идеал в кольце $\mathfrak{o}_x$ является степенью $\mathfrak{m}_x$, то $\mathfrak{m}_x$ — единственный простой идеал.

3) Поскольку идеал $\mathfrak{m}_x$ — главный и любой идеал $\mathfrak{a}$ кольца $\mathfrak{o}_x$ имеет вид $\mathfrak{a} = \mathfrak{m}_x^n$, то $\mathfrak{o}_x$ — кольцо главных идеалов.

2. Нормирования. Пусть $L \supset k$ — некоторое расширение поля k. Под *нормированием* поля L над k будем понимать всякое отображение v: $L^* \to \mathbb{Z}$, удовлетворяющее условиям:

1) $v(k^*) = 0$, $v(L^*) = \mathbb{Z}$;

2) $v(xy) = v(x) + v(y)$;

3) $v(x + y) \geqslant \min(v(x), v(y))$.

Доопределим v на все поле L, положив $v(0) = \infty$, и изучим свойства нормирования v.

Поскольку $v(1) = 0$ и $v(-1) = 0$, имеем $v(-y) = v(y)$. Отсюда следует, что $v(x - y) \geqslant \min(v(x), v(y))$.

Предложение 1. *Если $v(x) \neq v(y)$, то $v(x \pm y) = \min(v(x), v(y))$.*

Доказательство. Пусть например, $v(x) < v(y)$. Докажем, что тогда $v(x + y) = v(x)$. Предположим, что это не так, т. е. $v(x + y) > v(x)$. При этом предположении имеем $v(x) =$

$= v(x+y-y) \geqslant \min(v(x+y), v(y)) > v(x)$ и, следовательно, получаем противоречие.

Множество $\mathfrak{o}_v = \{x \in L \mid v(x) \geqslant 0\}$ элементов поля L является, очевидно, кольцом. Идеал $\mathfrak{m}_v = \{x \in \mathfrak{o}_v \mid v(x) > 0\}$ состоит из всех необратимых элементов $x \in \mathfrak{o}_v$ и, значит, является единственным максимальным идеалом кольца $\mathfrak{o}_v$. Поэтому $\mathfrak{o}_v$ — локальное кольцо. Далее, так как $x \notin \mathfrak{o}_v$ в том и только в том случае, когда $x^{-1} \in \mathfrak{m}_v$, то $\mathfrak{o}_v$ является V-кольцом. Кольцо $\mathfrak{o}_v$ называется *кольцом нормирования* поля L, а его максимальный идеал $\mathfrak{m}_v$ — *идеалом нормирования*.

Предложение 2. *Каждое кольцо нормирования $\mathfrak{o}_v$ является кольцом главных идеалов и каждый нетривиальный идеал $\mathfrak{a} \subset \mathfrak{o}_v$ является степенью единственного максимального идеала $\mathfrak{m}_v$ кольца $\mathfrak{o}_v$.*

Доказательство. Пусть $t \in \mathfrak{o}_v$, $v(t) = 1$,— *униформизирующий параметр нормирования v*. Для каждого элемента $x \in \mathfrak{o}_v$ имеем $v(x/t^{v(x)}) = 0$ и, значит, $x = t^{v(x)}u$, где u — обратимый элемент кольца $\mathfrak{o}_v$. Пусть $\mathfrak{a}$ — произвольный нетривиальный идеал кольца $\mathfrak{o}_v$. Так как $v(\alpha) \geqslant 0$ для любого элемента $\alpha \in \mathfrak{a}$, то в $\mathfrak{a}$ имеется элемент a с наименьшим значением $v(a)$. Имеем $a = t^{v(a)}u$, где u — обратимый элемент, и тогда $t^{v(a)} \in \mathfrak{a}$. Отсюда следует, что $(t^{v(a)}) = (t)^{v(a)} = t^{v(a)}\mathfrak{o}_v \subset \mathfrak{a}$. Докажем справедливость обратного включения $\mathfrak{a} \subset (t)^{v(a)}$. Пусть b — произвольный элемент идеала $\mathfrak{a}$. Имеем $v(b) \geqslant v(a)$ и тогда $v(b/a) \geqslant 0$. Значит, $b/a = u' \in \mathfrak{o}_v$ и, стало быть, $b = au' \in (t)^{v(a)}$. Следовательно, $\mathfrak{a} \subset (t)^{v(a)}$ и, таким образом, $\mathfrak{a} = (t)^{v(a)}$. Далее, имеем $(t) = \mathfrak{m}_v$ и тем самым $\mathfrak{a} = \mathfrak{m}^{vv(a)}$. Предложение доказано.

Предложение 3. *Пусть $\mathfrak{o}$ и $\mathfrak{o}'$ — два кольца нормирования поля L над k и пусть $\mathfrak{m}$ и $\mathfrak{m}'$ — их максимальные идеалы. Тогда следующие условия эквивалентны между собой (включения нестрогие)*:

1) $\mathfrak{o} \subset \mathfrak{o}'$, 2) $\mathfrak{m} \supset \mathfrak{m}'$,
3) $\mathfrak{o} = \mathfrak{o}'$, 4) $\mathfrak{m} = \mathfrak{m}'$.

Доказательство. Импликация 3) $\Rightarrow$ 2) очевидна. Докажем справедливость импликации 2) $\Rightarrow$ 1). Пусть $\mathfrak{m}' \subset \mathfrak{m}$ и предположим, что существует элемент $x \in \mathfrak{o}$, не принадлежащий $\mathfrak{o}'$. Тогда $x^{-1} \in \mathfrak{m}'$ и, значит, $x^{-1} \in \mathfrak{m}$. Тем самым, получаем элемент $x^{-1} \in \mathfrak{m}$, обратимый в кольце $\mathfrak{o}$, и приходим к противоречию.

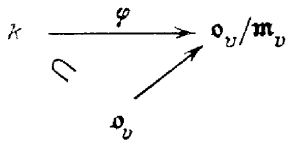
Покажем, что справедлива обратная импликация 1) $\Rightarrow$ 2). Пусть $\mathfrak{o} \subset \mathfrak{o}'$ и предположим, что существует элемент $x \in \mathfrak{m}'$, не принадлежащий $\mathfrak{m}$. Тогда $x^{-1} \in \mathfrak{o} \subset \mathfrak{o}'$ и, значит, элемент $x \in \mathfrak{m}'$ обратим в кольце $\mathfrak{o}'$. Полученное противоречие показывает, что $\mathfrak{m} \supset \mathfrak{m}'$.

Докажем справедливость импликации 1) $\Rightarrow$ 4). Имеем $\mathfrak{o} \subset \mathfrak{o}'$ и тогда $\mathfrak{m} \supset \mathfrak{m}'$. Пересечение $\mathfrak{o} \cap \mathfrak{m}'$ является ненулевым простым идеалом $\mathfrak{p}$ кольца $\mathfrak{o}$, содержащимся в максимальном идеале $\mathfrak{m}$. Но в кольце $\mathfrak{o}$ имеется единственный простой идеал $\mathfrak{m}$ и, значит, $\mathfrak{p} = \mathfrak{m}$. Таким образом, $\mathfrak{o} \cap \mathfrak{m}' = \mathfrak{m}$ и, стало быть, $\mathfrak{m} \subset \mathfrak{m}'$. Отсюда следует, что $\mathfrak{m} = \mathfrak{m}'$.

Покажем, наконец, что справедлива импликация 4) $\Rightarrow$ 3). Действительно, если $x \in \mathfrak{o}'$, но $x \notin \mathfrak{o}$, то имеем $x^{-1} \in \mathfrak{m}$ и, следовательно, $x^{-1} \in \mathfrak{m}'$. Отсюда получаем, что $x \notin \mathfrak{o}'$, и приходим к противоречию.

Предложение 4. *Пусть L — алгебраическое расширение поля рациональных функций $k(T)$ и $\mathfrak{o}_v$ — кольцо нормирования поля L с максимальным идеалом $\mathfrak{m}_v$. Тогда $\mathfrak{o}_v/\mathfrak{m}_v \simeq k$.*

Доказательство. Рассмотрим диаграмму гомоморфизмов



Имеем $\operatorname{Ker}\varphi = \mathfrak{m}_v \cap k = \{0\}$ и, значит, φ — вложение. Отсюда следует, в частности, что естественный гомоморфизм $\mathfrak{o}_v \to \mathfrak{o}_v/\mathfrak{m}_v$ является k-эпиморфизмом. Будем считать теперь, что $k \subset \mathfrak{o}_v/\mathfrak{m}_v$. Так как L — поле отношений кольца $\mathfrak{o}_v$, то его степень трансцендентности над k равна степени трансцендентности $\mathfrak{o}_v$ над k. Далее, так как $\mathfrak{o}_v/\mathfrak{m}_v$ — гомоморфный образ кольца $\mathfrak{o}_v$ и так как $\mathfrak{o}_v/\mathfrak{m}_v$ не изоморфно $\mathfrak{o}_v$, то степень трансцендентности $\mathfrak{o}_v/\mathfrak{m}_v$ над k меньше степени трансцендентности $\mathfrak{o}_v$ над k. Следовательно, степень трансцендентности поля $\mathfrak{o}_v/\mathfrak{m}_v$ над k меньше степени трансцендентности L над k. Но по условию поле L является алгебраическим расширением поля рациональных функций $k(T)$ от одного переменного T и, значит, имеет степень трансцендентности, равную единице. В таком случае, степень трансцендентности поля $\mathfrak{o}_v/\mathfrak{m}_v$ над k равна нулю и, следовательно, $\mathfrak{o}_v/\mathfrak{m}_v$ является алгебраическим расширением поля k. Так как k — алгебраически замкнутое поле, отсюда следует, что $\mathfrak{o}_v/\mathfrak{m}_v$ совпадает с k и предложение, тем самым, доказано.

Предложение 5. *Каждое кольцо нормирования целозамкнуто в своем поле частных L.*

Доказательство. Пусть $x \in L$ и

$$x^n + a_1x^{n-1} + \ldots + a_n = 0, \quad a_i \in \mathfrak{o}_v.$$

Докажем, что $x \in \mathfrak{o}_v$. Предположим, что $x \notin \mathfrak{o}_v$. Тогда $x^{-1} \in \mathfrak{m}_v$, а так как $1 + a_1x^{-1} + \ldots + a_nx^{-n} = 0$ и $a_1x^{-1} + \ldots + a_nx^{-n} \in \mathfrak{m}_v$, то получаем, что $1 \in \mathfrak{m}_v$, и приходим к противоречию. Предложение доказано.

Пусть X — алгебраическая кривая и $\mathfrak{o}_x$ — локальное кольцо точки $x \in X$ с максимальным идеалом $\mathfrak{m}_x$. Свяжем с точкой x нормирование v_x поля функций $L = k(X)$ на кривой X. Пусть (f) — идеал кольца $\mathfrak{o}_x$, порожденный отличной от нуля функцией $f \in \mathfrak{o}_x$, и пусть $(f) = \mathfrak{m}_x^a$, где a — некоторое неотрицательное целое

число. Положим $v_x(f)=a$ и $v_x(0)=\infty$. Ясно, что если $(f)=\mathfrak{m}_x^a$, $(g)=\mathfrak{m}_x^b$, то $v_x(f\cdot g)=a+b=v_x(f)+v_x(g)$. Далее, если $a=\min(a, b)$, то из включения $\mathfrak{m}_x^b\subset\mathfrak{m}_x^a$ следует, что $(f+g)=\mathfrak{m}^c$, где $c\geqslant a$. В таком случае, $c=v_x(f+g)\geqslant a=\min(a, b)=\min(v_x(f), v_x(g))$. Кроме того, если $\alpha\in k^*$, то $(\alpha)=\mathfrak{o}_x=\mathfrak{m}_x^0$ и тогда $v_x(k^*)=0$. Распространим теперь функцию v_x на поле частных L кольца $\mathfrak{o}_x$, положив $v_x(f/g)=v_x(f)-v_x(g)$, и покажем, что $v_x(L^*)=\mathbb{Z}$. Пусть t — *униформизирующий параметр точки* x, так что $\mathfrak{m}_x=(t)$ и $v_x(t)=1$. Для каждого целого a рассмотрим функцию $f=t^au\in L$, где u — обратимый элемент кольца $\mathfrak{o}_x$. Имеем $v_x(f)=a$ и, тем самым, отображение v_x: $L^*\to\mathbb{Z}$ является отображением L^* на $\mathbb{Z}$. Следовательно, оно задает нормирование поля L над k.

Покажем теперь, что $\mathfrak{o}_{v_x}=\mathfrak{o}_x$ и $\mathfrak{m}_{v_x}=\mathfrak{m}_x$. Очевидно, что $\mathfrak{o}_x\subset\mathfrak{o}_{v_x}$. Пусть $f\in\mathfrak{o}_{v_x}$, т. е. $v_x(f)=a\geqslant 0$. Так как $f=t^au$, где u — обратимый элемент кольца $\mathfrak{o}_x$, и $t^a\in\mathfrak{o}_x$, то имеем $f\in\mathfrak{o}_x$. Таким образом, $\mathfrak{o}_{a_x}\subset\mathfrak{o}_x$ и, следовательно, $\mathfrak{o}_{v_x}=\mathfrak{o}_x$. Аналогичным образом доказывается, что $\mathfrak{m}_{v_x}=\mathfrak{m}_x$ и, стало быть, нами установлен следующий результат.

Теорема 1. *Каждая точка x алгебраической кривой X определяет каноническое нормирование v_x поля $k(X)$ над k, обладающее свойствами:*

1) *если $f=t^au$ — элемент поля $k(X)$, где $v_x(t)=1$ и u обратим в кольце $\mathfrak{o}_x$, то $v_x(f)=a$;*

2) $\mathfrak{o}_{v_x}=\mathfrak{o}_x$ *и* $\mathfrak{m}_{v_x}=\mathfrak{m}_x$.

Теорема 2. *Сопоставление $x\mapsto v_x$ задает биективное соответствие между точками x алгебраической кривой X и нормированиями v_x поля $k(X)$ над k.*

Доказательство. Докажем инъективность рассматриваемого отображения. Пусть $x\neq y$ — точки многообразия $X\subset\mathbb{P}^n$ и $\mathfrak{m}_x$, $\mathfrak{m}_y$ — максимальные идеалы локальных колец $\mathfrak{o}_x$, $\mathfrak{o}_y$ этих точек. Точка x является алгебраическим подмножеством в X и ее идеал $\mathfrak{a}(x)$ представляет собой совокупность однородных многочленов, обращающихся в точке x в ноль. Так как $y\neq x$, то в идеале $\mathfrak{a}(x)$ существует такой однородный многочлен F, что $F(y)\neq 0$. Предположим, что координата x_0 точки $x=(x_0:x_1:\ldots:x_n)$ отлична от нуля. Тогда $T_0\notin\mathfrak{a}(x)$ и получаем представление $f=F/T_0^m$, $m=\deg F$, некоторой рациональной функции $f\in\mathfrak{m}_x\subset\mathfrak{o}_x$. Покажем, что $f\notin\mathfrak{m}_y$. Предположим противное: $f\in\mathfrak{m}_y$. Тогда f имеет представление $f=F_1/G_1$, где $F_1(y)=0$ и $G_1(y)\neq 0$. При этом $G_1F-F_1T_0^m\in\mathfrak{a}(X)$ и, значит, $G_1(y)F(y)-F_1(y)y_0^m=0$. Так как $F_1(y)=0$, $G_1(y)\neq 0$, то $F(y)=0$, и приходим в противоречие с выбором многочлена F. Таким образом, $\mathfrak{m}_x\neq\mathfrak{m}_y$ и, стало быть, разным точкам x, $y\in X$ соответствуют разные идеалы $\mathfrak{m}_x$ и $\mathfrak{m}_y$.

Установим сюръективность отображения. Пусть v — произвольное нормирование поля $k(X)$ над k. Будем считать, что $T_i\notin\mathfrak{a}(X)$ для всех $i=0, 1, \ldots, n$. Положим $f_{ij}=T_i/T_j$. Функции f_{ij} не равны нулю на кривой X, и среди них найдется функция $f_{i_0j_0}$ с наименьшим значением $v(f_{ij})$: $v(f_{i_0j_0})=\min\limits_{0<i,j<n} v(f_{ij})$. Тогда $v(f_{ij}/f_{i_0j_0})\geqslant 0$ для всех i, j и, в частности, $v(f_{ij_0}/f_{i_0j_0})\geqslant 0$. Но $f_{ij_0}/f_{i_0j_0}=T_i/T_{i_0}$ и, значит, $T_i/T_{i_0}\in\mathfrak{o}_v$ для всех $i=0, 1, \ldots, n$. Будем считать, без уменьшения общности, что $i_0=0$. В таком случае $t_i=T_i/T_0\in\mathfrak{o}_v$. Обозначим $Y=\mathbb{A}_0^n\cap X$ аффинную часть многообразия X. Функции t_i являются *координатными функциями* кольца $k[Y]$, так что $k[Y]=k[t_1, \ldots, t_n]$. Пусть $\mathfrak{a}(Y)$ — идеал аффинного многообразия Y. Так как $k[Y]=k[T_1, \ldots, T_n]/\mathfrak{a}(Y)$, то условие $F(t_1, \ldots, t_n)=0$ эквивалентно тому, что $F\in\mathfrak{a}(Y)$. Пусть $F\in\mathfrak{a}(Y)$ и $x_i\equiv t_i(\mathrm{mod}\,\mathfrak{m}_v)$. Так как $t_i\in\mathfrak{o}_v$, то $x_i\in\mathfrak{o}_v/\mathfrak{m}_v=k$, а поскольку $F(t_1, \ldots, t_n)\equiv 0\ (\mathrm{mod}\,\mathfrak{m}_v)$, то $F(x_1, \ldots, x_n)=0$. Таким образом, координаты точки $x=(x_1, \ldots, x_n)$ удовлетворяют уравнениям многообразия Y и, значит, $x\in Y$. При определении локального кольца $\mathfrak{o}_x$ точки x достаточно ограничиться рассмотрением открытой части Y многообразия X. Поэтому можно считать, что $\mathfrak{o}_x=\left\{\dfrac{f(t_1, \ldots, t_n)}{g(t_1, \ldots, t_n)}\,\middle|\,g(x_1, \ldots, x_n)\neq 0\right\}$. Покажем, что $\mathfrak{o}_x\subset\mathfrak{o}_v$. Поскольку $t_i\in\mathfrak{o}_v$ и $k\subset\mathfrak{o}_v$, то $f(t_1, \ldots, t_n)$, $g(t_1, \ldots, t_n)\in\mathfrak{o}_v$, а так как $g(x_1, \ldots, x_n)\neq 0$, то $g(t_1, \ldots, t_n)\not\equiv 0(\mathrm{mod}\,\mathfrak{m}_v)$. Значит, $g(t_1, \ldots, t_n)\notin\mathfrak{m}_v$ и тогда элемент $g(t_1, \ldots, t_n)$ обратим в кольце $\mathfrak{o}_v$. Следовательно, $\dfrac{f(t_1, \ldots, t_n)}{g(t_1, \ldots, t_n)}\in\mathfrak{o}_v$ и, стало быть, $\mathfrak{o}_x\subset\mathfrak{o}_v$. Воспользовавшись теперь предложением 3, получаем $\mathfrak{o}_x=\mathfrak{o}_v$. Теорема доказана.

Из этой теоремы следует, что изучение кривой X можно заменить изучением нормирований ее поля рациональных функций $k(X)$. Сама кривая X отступает при этом на задний план.

Теорема 3 (об аппроксимации). *Пусть $x_1, \ldots, x_s$ — попарно различные точки кривой X, $f_1, \ldots, f_s$ — произвольные функции из поля $L=k(X)$ и $m_1, \ldots, m_s$ — любые наперед заданные целые числа. Тогда в поле L существует такая функция f, что $v_{x_i}(f-f_i)\geqslant m_i$, для всех $i=1, 2, \ldots, s$.*

Следствие. *Если $x_1, \ldots, x_s$ — попарно различные точки кривой X и $m_1, \ldots, m_s$ — любые наперед заданные числа, то существует функция $f\in L$ такая, что $v_{x_i}(f)=m_i$, $1\leqslant i\leqslant s$.*

Доказательство теоремы. Докажем теорему индукцией по s. Для $s=1$ утверждение теоремы очевидно. Пусть утверждение теоремы справедливо для всех $s'<s$. Докажем его справедливость для s. Доказательство разобьем на три этапа.

1) Докажем сначала, что нормирования $v_1, \ldots, v_s$ $(v_i=v_{x_i})$, рассматриваемые как функции на L^*, линейно независимы над

полем рациональных чисел $\mathbb{Q}$. Предположим, что это не так, и пусть

$$v_s = \sum_{i=1}^{s-1} \lambda_i v_i, \quad \lambda_i \in \mathbb{Q}. \tag{1}$$

Покажем, что $\lambda_i \geqslant 0$ для всех $i = 1, 2, \ldots, s-1$. Допустим, что среди чисел λ_i имеются отрицательные. По индуктивному предположению и следствию из него можно найти такой элемент $\varphi \in k(X)$, что

$$v_i(\varphi) = \begin{cases} 1, & \text{если} \quad \lambda_i \geqslant 0, \\ 0, & \text{если} \quad \lambda_i < 0. \end{cases}$$

Аналогичным образом, существует такой элемент $\psi \in k(X)$, что

$$v_i(\psi) = \begin{cases} 0, & \text{если} \quad \lambda_i \geqslant 0, \\ 1, & \text{если} \quad \lambda_i < 0. \end{cases}$$

Так как $v_i(\varphi) \neq v_i(\psi)$, то имеем $v_i(\varphi+\psi) = \min(v_i(\varphi), v_i(\psi)) = 0$ для всех $i = 1, 2, \ldots, s-1$. Значит, ввиду (1), $v_s(\varphi+\psi) \geqslant 0$. С другой стороны, $v_s(\varphi) \geqslant 0$, $v_s(\psi) < 0$ и тогда $v_s(\varphi+\psi) = \min(v_s(\varphi), v_s(\psi)) < 0$. Полученное противоречие показывает, что в соотношении (1) все коэффициенты λ_i неотрицательны. Поскольку не все λ_i равны нулю, то можем считать, что $\lambda_1 > 0$. Покажем, что среди чисел $\lambda_2, \ldots, \lambda_{s-1}$ также найдется хотя бы одно положительное. Пусть это не так. Тогда $v_s = \lambda_1 v_1$ и, следовательно, $v_{x_s} = v_{x_1}$. В таком случае $x_s = x_1$ и приходим в противоречие с тем, что точки $x_1, \ldots, x_s$ попарно различны. Таким образом, получаем соотношение

$$v_1 = \frac{v_s}{\lambda_1} - \sum_{i=2}^{s-1} \frac{\lambda_i}{\lambda_1} v_i = \sum_{i=2}^{s} \lambda_i^* v_i,$$

в котором хотя бы один коэффициент λ_i^* отрицателен. Но по доказанному выше этого не может быть и, значит, предположение о линейной зависимости $v_1, \ldots, v_s$ над полем $\mathbb{Q}$ приводит к противоречию.

2) Покажем теперь, что существуют функции $\varphi_1, \ldots, \varphi_s \in L$ такие, что

$$\det \|v_i(\varphi_j)\|_{1 \leqslant i,j \leqslant s} \neq 0.$$

Используем для этого индукцию по s. При $s = 1$ утверждение очевидно. Пусть утверждение справедливо для всех $s' < s$. Тогда существуют такие рациональные функции $\varphi_1, \ldots, \varphi_{s-1}$, что

$$\det \|v_i(\varphi_j)\|_{1 \leqslant i,j \leqslant s-1} \neq 0.$$

Рассмотрим определитель

$$\Delta = \det \begin{Vmatrix} v_1(\varphi_1) & \ldots & v_1(\varphi_{s-1}) & v_1(\varphi) \\ \vdots & & \vdots & \vdots \\ v_{s-1}(\varphi_1) & \ldots & v_{s-1}(\varphi_{s-1}) & v_{s-1}(\varphi) \\ v_s(\varphi_1) & \ldots & v_s(\varphi_{s-1}) & v_s(\varphi) \end{Vmatrix},$$

и докажем, что существует такой элемент $\varphi \in L$, при котором $\Delta \neq 0$. Допустим, что такого элемента нет. Разложим определитель Δ по последнему столбцу. Тогда получим, что для всех $\varphi \in L$ выполняется соотношение

$$\lambda_1 v_1(\varphi) + \ldots + \lambda_s v_s(\varphi) = 0,$$

где не все λ_i равны нулю, поскольку по индуктивному предположению

$$\lambda_s = \det \|v_i(\varphi_j)\|_{1 \leqslant i,j \leqslant s-1} \neq 0.$$

В результате приходим к противоречию с линейной независимостью $v_1, \ldots, v_s$.

3) Пусть $\Delta \neq 0$ и r, $1 \leqslant r \leqslant s$,— фиксированное целое число. Тогда существуют такие $\lambda_{jr} \in \mathbb{Q}$, что

$$\sum_{j=1}^{s} \lambda_{jr} v_i(\varphi_j) = \begin{cases} -1, & \text{если} \quad i = r, \\ 1, & \text{если} \quad i \neq r. \end{cases}$$

Выберем целое $m \geqslant 1$ таким образом, чтобы $m\lambda_{jr} \in \mathbb{Z}$, $m + v_i(f_j) \geqslant \max(m_1, \ldots, m_s)$ для всех $i, j = 1, 2, \ldots, s$, и рассмотрим функции

$$g_r = \prod_{j=1}^{s} \varphi_j^{m\lambda_{jr}}, \quad h_r = (1 + g_r^{-1})^{-1}, \quad f = \sum_{r=1}^{s} h_r f_r.$$

Так как

$$v_i(g_r) = \sum_{j=1}^{s} m\lambda_{ir} v_i(\varphi_j) = \begin{cases} -m, & \text{если} \quad i = r, \\ m, & \text{если} \quad i \neq r, \end{cases}$$

то при $i \neq r$ имеем

$$v_i(h_r) = -v_i(1 + g_r^{-1}) = -\min(v_i(1), v_i(g_r^{-1})) = -\min(0, -m) = m.$$

Далее, поскольку

$$h_i - 1 = \frac{1}{1 + g_i^{-1}} - 1 = \frac{g_i^{-1}}{1 + g_i^{-1}},$$

$$v_i(h_i - 1) = -v_i(g_i) - v_i(1 + g_i^{-1}) = m - \min(v_i(1), v_i(g_i^{-1})) = m - \min(0, m) = m,$$

и тогда

$$v_i(f-f_i)=v_i\Big(\sum_{r\neq i}h_rf_r+(h_i-1)f_i\Big)\geqslant$$

$$\geqslant\min\big(v_i(h_1)+v_i(f_1),\ \ldots,\ v_i(h_{i-1})+v_i(f_{i-1}),\ v_i(h_i-1)+v_i(f_i),$$
$$v_i(h_{i+1})+v_i(f_{i+1}),\ \ldots,\ v_i(h_s)+v_i(f_s)\big)=$$
$$=\min_r(m+v_i(f_r))\geqslant\max(m_1,\ \ldots,\ m_s)\geqslant m_i.$$

Теорема доказана.

Доказательство следствия. Пусть t_i — униформизирующий параметр в точке x_i и $f_i=t_i^{m_i}$, так что $v_{x_i}(f_i)=m_i$. По теореме об аппроксимации существует функция $f\in L$ такая, что $v_{x_i}(f-f_i)\geqslant m_i+1$ для всех $i=1,\ 2,\ \ldots,\ s$. Для этой функции f имеем $v_{x_i}(f)=v_{x_i}(f-f_i+f_i)=\min\big(v_{x_i}(f-f_i),\ v_{x_i}(f_i)\big)=m_i$, $1\leqslant i\leqslant s$, что и требовалось доказать.

Пример. Пусть $X=\mathbb{P}^1$, так что $\mathfrak{a}(X)=0$. Любая функция $\varphi\in k(X)$ представима в виде $\varphi=F(T_0,\ T_1)/G(T_0,\ T_1)$, где F, G — многочлены одинаковой степени. Положим $t=T_1/T_0$. Тогда $\varphi=F(1,\ t)/G(1,\ t)=f(t)/g(t)$ и, значит, $k(X)=k\big(\mathbb{A}_0^1\big)=k(t)$ есть чисто трансцендентное расширение поля k. Любая точка $x\in\mathbb{P}^1$ имеет вид $x=(x_0:x_1)$. Если $x_0\neq 0$, то $x=(1:x_1/x_0)=(1:x')$. Кроме того, в $\mathbb{P}^1$ имеется бесконечно удаленная точка $x_\infty=(0:1)$. Рассмотрим точку $x=(1:x')$. Локальное кольцо $\mathfrak{o}_x$ точки x имеет вид

$$\mathfrak{o}_x=\left\{\frac{f(t)}{g(t)}\in k(t)\mid g(x')\neq 0\right\}.$$

Его максимальный идеал $\mathfrak{m}_x$ состоит из функций $f(t)/g(t)\in\mathfrak{o}_x$ таких, что $f(x')=0$. Найдем униформизирующий параметр t' идеала $\mathfrak{m}_x$. Так как $f(x')=0$, то $(t-x')$ делит многочлен $f(t)$ и, значит,

$$\frac{f(t)}{g(t)}=(t-x')^a\frac{h(t)}{g(t)},$$

где $h/g\in\mathfrak{o}_x$ и $h/g\notin\mathfrak{m}_x$. Таким образом, $\mathfrak{m}_x=(t-x')\mathfrak{o}_x$ и, следовательно, униформизирующий параметр идеала $\mathfrak{m}_x$ имеет вид $t'=t-x'$. Так как $v_x(f/g)=0$, то при $a>0$ величина $v_x(f/g)$ определяет порядок нуля функции f/g в точке x, а при $a<0$ — порядок полюса f/g в этой точке. В бесконечно удаленной точке $x_\infty=(0:1)$ униформизирующим параметром является $t'=1/t$. Локальное кольцо $\mathfrak{o}_{x_\infty}$ этой точки состоит из всех рациональных функций $f(t)/g(t)$ таких, что $\deg f(t)\leqslant\deg g(t)$. Максимальный идеал $\mathfrak{m}_{x_\infty}$ кольца $\mathfrak{o}_{x_\infty}$ это множество всех рациональных функций f/g, для которых $\deg f<\deg g$. Величина $v_{x_\infty}(f/g)$

определяется равенством

$$v_{x_\infty}\left(\frac{f}{g}\right)=\deg g-\deg f.$$

Определение 1. Пусть x — точка алгебраической кривой X и f — не равная нулю функция из $k(X)$. Если $f\in\mathfrak{m}_x$, то точка x называется *нулем функции* f, а величина $v_x(f)$ — *порядком этого нуля*. Если $f^{-1}\in\mathfrak{m}_x$, то точка x называется *полюсом функции* f; величина $v_x(f^{-1})$ называется *порядком полюса* функции $f\notin\mathfrak{o}_x$ в точке x.

3. Дивизоры. *Дивизором на алгебраической кривой* X назовем всякое выражение

$$D=\sum_{x\in X}a_x\cdot x,\quad a_x\in\mathbb{Z},$$

в котором все a_x равны нулю, за исключением конечного их числа. Множество дивизоров на кривой X образует свободную абелеву группу с базой X. Эта группа называется *группой дивизоров алгебраической кривой* X и обозначается $\mathrm{Div}(X)$.

Степенью дивизора $D=\sum_{x\in X}a_x\cdot x$ называется сумма его коэффициентов: $\deg D=\sum_{x\in X}a_x$. Имеем $\deg(D+D')=\deg D+\deg D'$, и, значит, отображение $\deg\colon \mathrm{Div}(X)\to\mathbb{Z}$ является гомоморфизмом. Легко проверить, что указанное отображение — эпиморфизм. *Ядром отображения* $\deg\colon \mathrm{Div}(X)\to\mathbb{Z}$ является *группа дивизоров нулевой степени*, которую обозначим $\mathrm{Div}^0(X)$. Так как

$$\mathrm{Div}(X)/\mathrm{Div}^0(X)\simeq\mathbb{Z},$$

то факторгруппа $\mathrm{Div}(X)/\mathrm{Div}^0(X)$ представляет собой свободную абелеву группу ранга 1.

Определение 2. Дивизор

$$D=\sum_{x\in X}a_x\cdot x$$

называется *положительным* (символическая запись: $D\geqslant 0$), если все его коэффициенты a_x неотрицательны.

Понятие положительного дивизора позволяет определить отношение частичного порядка в множестве дивизоров на кривой X. Именно, будем считать $D'\geqslant D''$, если только $D'-D''\geqslant 0$.

Дивизоры

$$(D',\ D'')=\sum_{x\in X}\min\big(a'_x,\ a''_x\big)\cdot x$$

и

$$\{D',\ D''\}=\sum_{x\in X}\max\big(a'_x,\ a''_x\big)\cdot x$$

назовем соответственно *наибольшим общим делителем* и *наименьшим общим кратным дивизоров* $D'=\sum_{x\in X}a'_x\cdot x$ и $D''=\sum_{x\in X}a''_x\cdot x$.

Ясно, что $D' \geqslant (D', D'')$, $D'' \geqslant (D', D'')$, $\{D', D''\} \geqslant D'$, $\{D', D''\} \geqslant D''$ и $\{D', D''\} = D' + D'' - (D', D'')$.

Определение 3. Пусть $f, g \in L = k(X)$ и

$$D = \sum_{x \in X} a_x \cdot x$$

— фиксированный дивизор на кривой X. Будем говорить, что функции f и g *сравнимы* по $\bmod D$ $(f \equiv g (\bmod D))$, если $v_x(f - g) \geqslant a_x$ для всех $x \in X$.

Легко видеть, что если $f \equiv g (\bmod D)$ и $f' \equiv g' (\bmod D)$, то $\alpha f + \beta f' \equiv \alpha g + \beta g' (\bmod D)$, при любых $\alpha, \beta \in k$. В частности, все функции f, сравнимые с нулем по $\bmod D$, образуют линейное пространство над полем k, которое обозначим $L(D)$.

Пусть $D = \sum_{x \in X} a_x \cdot x$ — дивизор на X и S — любое конечное множество попарно различных точек кривой X. Будем говорить, это функции $f, g \in k(X)$ *сравнимы* по $\bmod D$ *на множестве* S $\left(f \underset{S}{\equiv} g (\bmod D)\right)$, если $v_x(f - g) \geqslant a_x$ для всех $x \in S$. Множество функций $f \in k(X)$ таких, что $f \underset{S}{\equiv} 0 (\bmod D)$, представляет собой линейное пространство над полем k. Обозначим это пространство $L(S, D)$, и заметим, что $L(D) \subset L(S, D)$ для любого S.

Пусть f — непостоянная функция поля $L = k(X)$. Тогда элемент f трансцендентен над k и поле L является алгебраическим расширением поля $k(f)$ конечной степени $[L : k(f)]$.

Для изучения рациональных функций на алгебраической кривой воспользуемся следующим общим результатом.

Теорема. *На проективном многообразии нет всюду регулярных непостоянных функций.*

Доказательство см. [144, т. 1, с. 78], или [132, с. 37].

Теорема 4. *Каждая непостоянная функция на кривой X имеет хотя бы один полюс и хотя бы один нуль.*

Доказательство. Если функция $f \in k(X)$ не имеет полюсов на X, то она всюду регулярна, и, значит, $f = \text{const} \in k$. Далее, если функция f не имеет нулей, то функция f^{-1} регулярна на всей кривой X и тогда снова $f = \text{const}$. Теорема доказана.

Покажем, теперь, что всякая непостоянная функция $f \in k(X)$ имеет лишь конечное число нулей и полюсов. Предварительно докажем следующий результат.

Лемма 1. *Пусть*

$$D = \sum_{x \in X} a_x \cdot x, \quad D' = \sum_{x \in X} a'_x \cdot x.$$

Если $D \geqslant D'$, то для любого конечного множества S точек кривой X выполняются соотношения

$$L(S, D) \subset L(S, D')$$

и

$$\dim_k L(S, D')/L(S, D) = \sum_{x \in S} (a_x - a'_x).$$

Доказательство. Положим

$$D_S = \sum_{x \in S} a_x \cdot x \quad \text{и} \quad D'_S = \sum_{x \in S} a'_x \cdot x.$$

Ввиду того, что $D \geqslant D'$, имеем $a_x \geqslant a'_x$ и, стало быть, $\sum_{x \in S} (a_x - a'_x) = m \geqslant 0$. Кроме того, $L(S, D) = L(S, D_S)$, $L(S, D') = L(S, D'_S)$ и $L(S, D) \subset L(S, D')$.

Если $m = 0$, то $a'_x = a_x$ для всех $x \in S$, и тогда $D'_S = D_S$. В таком случае $L(S, D') = L(S, D)$ и утверждение леммы справедливо.

Пусть теперь $m \geqslant 1$. Очевидно, что существует последовательность дивизоров

$$D'_S = D_0 < D_1 < D_2 < \ldots < D_m = D_S,$$

в которой $D_i = D_{i-1} + x_i$, $x_i \in S$, для всех $i = 1, 2, \ldots, m$. Тогда мы имеем цепочку

$$L(S, D_S) = L(S, D_m) \subset L(S, D_{m-1}) \subset \ldots \subset L(S, D_0) = L(S, D'_S)$$

вложенных друг в друга пространств. Лемма будет доказана, если докажем, что $L(S, D_{m-i})/L(S, D_{m-i+1})$ — одномерные пространства при всех $i = 1, 2, \ldots, m$. Положим $D' = \sum_{x \in S} a'_x \cdot x$ и $D = \sum_{x \in S} a_x \cdot x = D' + x'$, где $x' \in S$. Тогда достаточно доказать, что $\dim L(S, D')/L(S, D) = 1$. Из теоремы об аппроксимации следует, что существует функция $f \in k(X)$, которая удовлетворяет условию $v_x(f) = a'_x$ для всех $x \in S$. Далее,

$$a_x = \begin{cases} a'_x, & \text{если } x \neq x', \\ a'_x + 1, & \text{если } x = x', \end{cases}$$

и тогда $f \in L(S, D')$, $f \notin L(S, D)$.

Рассмотрим класс функций $\bar{f}$, сравнимых с f по $\bmod L(S, D)$. Этот класс представляет собой ненулевой элемент факторпространства $L(S, D')/L(S, D)$ и надо доказать, что каждый другой ненулевой элемент этого факторпространства пропорционален $\bar{f}$. Другими словами, надо показать, что для каждой функции $u \in L(S, D')$ найдется элемент $\alpha \in k$ такой, что $u - \alpha f \in L(S, D)$. Так как $u \in L(S, D')$, то $v_x(u) \geqslant a'_x = v_x(f)$ и, значит, $v_x(uf^{-1}) \geqslant 0$ для всех $x \in S$. Таким образом, $uf^{-1} \in \mathfrak{o}_x$ при всех $x \in S$, а поскольку $\mathfrak{o}_x/\mathfrak{m}_x = k$, то $uf^{-1} (\bmod \mathfrak{m}_x) \in k$ для каждого $x \in S$. В частности, $uf^{-1} (\bmod \mathfrak{m}_{x'}) = \alpha \in k$ и, стало быть, $uf^{-1} - \alpha \in \mathfrak{m}_{x'}$.

Отсюда следует, что $(u-\alpha f)f^{-1}\in\mathfrak{m}_{x'}$ и тогда $v_{x'}((u-\alpha f)f^{-1})\geqslant 1$. Значит $v_{x'}(u-\alpha f)\geqslant v_{x'}(f)+1=a_{x'}$, а так как при $x\neq x'$, $x\in S$, имеем $v_x(u-\alpha f)\geqslant\min(v_x(u),\ v_x(f))\geqslant a_x'=a_x$, то $v_x(u-\alpha f)\geqslant a_x$ для всех $x\in S$. Стало быть, $u-\alpha f\in L(S,\ D)$ и тем самым лемма доказана.

Теорема 5. *Пусть $L=k(X)$ — поле функций на алгебраической кривой X. Число нулей и число полюсов каждой непостоянной функции $f\in L$, с учетом их кратностей, не превосходит одной и той же величины $[L:k(f)]$.*

Доказательство. Достаточно установить, очевидно, справедливость теоремы для числа нулей функции f. Пусть $x_1,\ \ldots,\ x_s$ — все нули функции f. Надо доказать, что

$$\sum_{i=1}^{s}v_{x_i}(f)\leqslant[L:\ k(f)].$$

Рассмотрим множество $S=\{x_1,\ \ldots,\ x_r\}$ нулей функции f и положим $D=\sum_{i=1}^{r}a_i\cdot x_i$, где $a_i=v_{x_i}(f)\geqslant 1$. Мы имеем $D\geqslant 0$ и по лемме 1

$$\dim_k L(S,\ 0)/L(S,\ D)=\sum_{i=1}^{r}a_i=\sum_{i=1}^{r}v_{x_i}(f)=\deg D=m.$$

Пусть $f_1,\ \ldots,\ f_m\in L(S,\ 0)$ — представители классов вычетов $\bar f_1,\ \ldots,\ \bar f_m$ по $\bmod L(S,\ D)$, образующих базис факторпространства $L(S,\ 0)/L(S,\ D)$ над полем k. Покажем, что $f_1,\ \ldots,\ f_m$ линейно независимы над полем $k(f)$. Предположим, что это не так, и пусть

$$\sum_{j=1}^{m}u_jf_j=0,$$

где $u_j\in k(f)$ и $(u_1,\ \ldots,\ u_m)\neq(0,\ \ldots,\ 0)$. Но можно считать, что $u_j\in k[f]$ и что $u_j=g_jf+\alpha_j$, где $g_j\in k[f]$, $\alpha_j\in k$ и $(\alpha_1,\ \ldots,\ \alpha_m)\neq(0,\ \ldots,\ 0)$. Тогда $f\sum_{j=1}^{m}g_jf_j=-\sum_{j=1}^{m}\alpha_jf_j$, и так как

$$v_{x_i}\left(f\sum_{j=1}^{m}g_jf_j\right)=v_{x_i}(f)+v_{x_i}\left(\sum_{j=1}^{m}g_jf_j\right)\geqslant a_i$$

для каждой точки $x_i\in S$, то $v_{x_i}\left(\sum_{j=1}^{m}\alpha_jf_j\right)\geqslant a_i\geqslant 0$ для всех $x_i\in S$.

Следовательно, $\sum_{j=1}^{m}\alpha_jf_j\equiv 0\,(\bmod L(S,D))$ и, значит, $\sum_{j=1}^{m}\alpha_j\bar f_j=0$. Из линейной независимости $\bar f_1,\ \ldots,\ \bar f_m$ следует, что $\alpha_1=\ldots=\alpha_m=0$, и приходим в противоречие с выбором $\alpha_1,\ \ldots,\ \alpha_m$. Полученное противоречие показывает, что $f_1,\ \ldots,\ f_m$ линейно независимы над полем $k(f)$ и тогда $m\leqslant[L:k(f)]$. Но $m=\sum_{i=1}^{r}v_{x_i}(f)$ и, значит,

$$\sum_{i=1}^{r}v_{x_i}(f)\leqslant[L:\ k(f)].$$

В частности,

$$\sum_{i=1}^{s}v_{x_i}(f)\leqslant[L:\ k(f)],$$

и теорема, тем самым, доказана.

Следствие. *Пусть f — отличная от нуля функция на кривой X. Тогда $v_x(f)=0$ для почти всех $x\in X$ (для всех $x\in X$, кроме конечного их числа). Далее, $v_x(f)=0$ для всех $x\in X$ лишь в том случае, если $f\in k^*$.*

Приведенное следствие показывает, что можно ввести в рассмотрение дивизор

$$(f)=\sum_{x\in X}v_x(f)\cdot x.$$

Этот дивизор называется *дивизором функции*.

Определение 4. Дивизор D называется *главным* или *линейно эквивалентным нулю*, если существует функция $f\in L=k(X)$, такая, что

$$D=(f)=\sum_{x\in X}v_x(f)\cdot x.$$

Теорема 6. *Главные дивизоры образуют подгруппу $P(X)$ группы $\mathrm{Div}(X)$. Имеет место естественный изоморфизм $L^*/k^*\simeq P(X)$.*

Доказательство. Имеем $(f)-(g)=\sum_{x\in X}v_x(f/g)\cdot x=(f/g)$ и, значит, $P(X)$ — подгруппы группы $\mathrm{Div}(X)$.

Рассмотрим отображение $\varphi\colon L^*\to P(X)$, ставящее в соответствие функции f ее дивизор (f). Так как $(f\cdot g)=(f)+(g)$, то φ — гомоморфизм. Очевидно, что φ — эпиморфизм. Далее,

$$\operatorname{Ker}\varphi=\{f\in L^*\mid(f)=0\}=\{f\in k^*\}$$

и, значит, $L^*/k^*\to P(X)$ — изоморфизм.

Определение 5. Пусть f — непостоянная функция на кривой X. Дивизор

$$(f)_0=\sum_{\substack{x\in X\\ v_x(f)\geqslant 0}}v_x(f)\cdot x$$

называется *дивизором нулей* функции f, а дивизор

$$(f)_\infty=\sum_{\substack{x\in X\\ v_x(f)\leqslant 0}}v_x(f)\cdot x$$

— *дивизором полюсов* функции f.

Теорема 7. *Если* $f \in L = k(X)$ *и* $f \notin k$, *то*

$$\deg(f)_0 = \deg(f)_\infty = [L : k(f)].$$

Доказательство. Рассмотрим подкольцо $k[f^{-1}]$ поля $L = k(X)$ и найдем базис поля L, целый над $k[f^{-1}]$. Имеем $k(f) = k(f^{-1})$ и тогда $[L : k(f)] = [L : k(f^{-1})] = m$. Пусть $u_1, \ldots, u_m$ — базис поля L над $k(f)$. Каждый элемент u_i алгебраичен над $k(f)$ и, следовательно, $u_i v_i$ является целым над $k[f^{-1}]$ при некотором $v_i \in k[f^{-1}]$. Поэтому базис $w_1, \ldots, w_m$, где $w_i = u_i v_i$, будет целым над $k[f^{-1}]$.

Пусть $S = \{x_1, \ldots, x_s\}$ — множество всех нулей функции f. Если $x \notin S$, то $f^{-1} \in \mathfrak{o}_x$ и тогда $k[f^{-1}] \subset \mathfrak{o}_x$. Так как кольцо $\mathfrak{o}_x$ целозамкнуто, отсюда следует, что $w_j \in \mathfrak{o}_x$ и, значит, $v_x(w_j) \geqslant 0$ для всех $j = 1, 2, \ldots, m$. Выберем целое $\mu \geqslant 1$ таким образом, чтобы

$$\mu > \max_{i,j} \left(-v_{x_i}(w_j)\right),$$

и для каждого $\nu > \mu$ рассмотрим функции $f^{-r}w_j$, $0 \leqslant r \leqslant \nu - \mu$. Докажем, что $(\nu - \mu + 1)m$ элементов $f^{-r}w_j$, $0 \leqslant r \leqslant \nu - \mu$, $1 \leqslant j \leqslant m$, линейно независимы над полем k. Пусть, наоборот,

$$\sum_{r=0}^{\nu-\mu} \sum_{j=1}^{m} \lambda_{rj} f^{-r} w_j = 0$$

при некоторых отличных в совокупности от нуля $\lambda_{rj} \in k$. Тогда

$$\sum_{j=1}^{m} \left(\sum_{r=0}^{\nu-\mu} \lambda_{rj} f^{-r} \right) w_j = 0$$

и, значит,

$$\sum_{r=0}^{\nu-\mu} \lambda_{rj} f^{-r} = 0$$

для каждого $j = 1, 2, \ldots, m$. Но элемент f^{-1} трансцендентен над k и, в таком случае, $\lambda_{rj} = 0$ для всех r и j. Получаем противоречие.

Пусть $L_\nu = \{f^{-r}w_j\}$ — линейное пространство над полем k размерности $(\nu - \mu + 1)m$, порожденное функциями $f^{-r}w_j$, и пусть $(f)_0 = D$. Рассмотрим пространство $L(-\nu D)$ и покажем, что $L_\nu \subset L(-\nu D)$. Для каждого $x_i \in S$ имеем

$$v_{x_i}(f^{-r}w_j) = v_{x_i}(w_j) - r v_{x_i}(f) > -\mu - r v_{x_i}(f) = -(\mu - r v_{x_i}(f)) \geqslant$$
$$\geqslant -\left(\mu v_{x_i}(f) + r v_{x_i}(f)\right) = -(\mu + r) v_{x_i}(f) \geqslant -\nu v_{x_i}(f);$$

если же $x \notin S$, то

$$v_x(f^{-r}w_j) = r v_x(f^{-1}) + v_x(w_j) \geqslant 0.$$

Значит, $f^{-r}w_j \in L(-\nu D)$ и, следовательно, $L_\nu \subset L(-\nu D)$. Так как

$\nu D \geqslant 0$, то $L(S, 0) \subset L(S, -\nu D)$, причем

$$\dim_k L(S, -\nu D)/L(S, 0) = \sum_{x \in S} \nu v_x(f) = \nu \deg D = \nu \deg(f)_0.$$

Кроме того, $L(-\nu D) \subset L(S, -\nu D)$ и

$$\dim_k L(-\nu D)/L(-\nu D) \cap L(S, 0) \leqslant$$
$$\leqslant \dim_k L(S, -\nu D)/L(S, 0) = \nu \deg(f)_0.$$

Покажем, что $L(-\nu D) \cap L(S, 0) \subset k$. Действительно, если $g \in L(-\nu D) \cap L(S, 0)$, то $v_{x_i}(g) \geqslant 0$ для всех $x_i \in S$ и $v_x(g) \geqslant 0$ для каждого $x \notin S$. В таком случае, по теореме 4, $g \in k$ и, стало быть, $\dim_k L(-\nu D) \leqslant \nu \deg(f)_0 + 1$. Следовательно,

$$\dim_k L_\nu = (\nu - \mu + 1)m \leqslant \nu \deg(f)_0 + 1,$$

или

$$\deg(f)_0 \geqslant m\left(1 - \frac{\mu - 1}{\nu}\right) - \frac{1}{\nu}.$$

Устремляя ν в бесконечности, получаем

$$\deg(f)_0 \geqslant m = [L : k(f)],$$

а так как по теореме 5

$$\deg(f)_0 \leqslant m = [L : k(f)],$$

то

$$\deg(f)_0 = [L : k(f)].$$

Далее, поскольку $(f)_\infty = (f^{-1})_0$ и $\deg(f)_\infty = \deg(f^{-1})_0 = [L : k(f^{-1})] = [L : k(f)]$, то $\deg(f)_\infty = [L : k(f)]$. и, тем самым, теорема доказана.

Следствие. *Если* f *— отличная от нуля функция на кривой* X, *то* $\deg(f) = 0$.

Доказательство. Если $f \in k$, то $v_x(f) = 0$ для всех $x \in X$ и тогда $\deg(f) = 0$. Если же $f \notin k$, то $(f) = (f)_0 - (f)_\infty$ и снова $\deg(f) = \deg(f)_0 - \deg(f)_\infty = 0$. Следствие доказано.

Имеем

$$P(X) \subset \mathrm{Div}^0(X) \subset \mathrm{Div}(X).$$

Факторгруппа $\mathrm{Cl}(X) = \mathrm{Div}(X)/P(X)$ называется *группой классов дивизоров* на кривой X, а ее подгруппа $\mathrm{Cl}^0(X) = \mathrm{Div}^0(X)/P(X)$ — *группой классов дивизиров нулевой степени*. Два дивизора D и D' называются *линейно эквивалентными* ($D \sim D'$), если они лежат в одном и том же классе смежности группы $\mathrm{Div}(X)$ по подгруппе $P(X)$, т. е. когда $D' = D + (f)$ для некоторой функции $f \in k(X)$. Линейно эквивалентные между собой дивизоры имеют одинаковую степень.

Задачи

1. Пусть K — поле и Γ — вполне упорядоченная абелева группа. Под *нормированием поля* K будем понимать всякий гомоморфизм $v\colon K^* \to \Gamma$ мультипликативной группы K^* поля K в Γ, удовлетворяющий условию

$$v(x+y) \leqslant \min(v(x), v(y)).$$

Нормирование v называется *тривиальным*, если оно отображает K^* в 0. Два нормирования v и v' называются *эквивалентными*, если существует сохраняющий порядок изоморфизм λ между $v(K^*)$ и $v'(K^*)$ такой, что $v'(x) = \lambda \circ v(x)$ для всех $x \in K^*$. Доопределим v на всем поле K, положив $v(0) = \infty$.

Подкольцо $\mathfrak{o}$ поля K называется *кольцом нормирования*, если оно обладает тем свойством, что для всякого $x \in K$ либо $x \in \mathfrak{o}$, либо $x^{-1} \in \mathfrak{o}$.

Доказать справедливость следующих утверждений:

а) кольцо нормирования $\mathfrak{o}$ является локальным кольцом;

б) максимальный идеал $\mathfrak{m}$ кольца $\mathfrak{o}$ состоит из всех необратимых элементов кольца $\mathfrak{o}$;

в) кольцо $\mathfrak{o}$ целозамкнуто в поле K;

г) каждое кольцо нормирования $\mathfrak{o}$ имеет вид $\mathfrak{o} = \mathfrak{o}_v$, где $\mathfrak{o}_v$ — множество элементов x поля K, удовлетворяющих условию $v(x) \geqslant 0$ для некоторого нормирования v поля K;

д) имеется биективное соответствие между кольцами нормирования и классами эквивалентных нормирований поля K.

2. Доказать, что в конечном поле F_q нет нетривиальных нормирований.

3. Пусть p — простое число. Каждое рациональное число $x \neq 0$ однозначно представляется в виде $x = p^{\nu}\frac{a}{b}$, где целые числа a и b не делятся на p. Показать, что функция

$$v_p(x) = \nu \in \mathbb{Z}, \quad v_p(0) = \infty,$$

задает нормирование поля рациональных чисел $\mathbb{Q}$. Оно называется *p-адическим нормированием* поля $\mathbb{Q}$.

4. Пусть ρ — произвольное вещественное число, удовлетворяющее условию $0 < \rho < 1$, и v_p — p-адическое нормирование поля $\mathbb{Q}$. Доказать, что функция

$$|x|_p = \rho^{v_p(x)}$$

обладает свойствами:

1) $|x|_p \geqslant 0$ для всех $x \in \mathbb{Q}$ и $|x|_p = 0$ лишь при $x = 0$;
2) $|x \cdot y|_p = |x|_p \cdot |y|_p$;
3) $|x+y|_p \leqslant \max(|x|_p, |y|_p)$.

Функция $|x|_p$ называется *p-адической нормой* поля $\mathbb{Q}$.

5. Доказать, что если p-адическая норма поля $\mathbb{Q}$ имеет вид $|x|_p = p^{-v_p(x)}$, то для каждого ненулевого числа $x \in \mathbb{Q}$ выполняется соотношение

$$|x| \prod_p |x|_p = 1,$$

где $|x|$ — обычное абсолютное значение рационального числа x.

6. Последовательность $\{x_n\}$ элементов поля $\mathbb{Q}$ называется *фундаментальной* или *последовательностью Коши* относительно p-адической нормы, если $|x_m - x_n|_p \to 0$ при $m, n \to \infty$. Две фундаментальные последовательности $\{x_n\}$ и $\{y_n\}$ называются *эквивалентными*, если $|x_n - y_n|_p \to 0$ при $n \to \infty$. Доказать справедливость следующих утверждений:

а) множество всех фундаментальных последовательностей разбивается на непересекающиеся классы эквивалентных между собой последовательностей (множество таких классов обозначается $\mathbb{Q}_p$);

б) если α и β — два класса из $\mathbb{Q}_p$ и $\{x_n\} \in \alpha$, $\{y_n\} \in \beta$, то классы $\alpha + \beta$ и $\alpha \cdot \beta$, содержащие последовательности $\{x_n + y_n\}$ и $\{x_n y_n\}$, определены однозначно по α, β и не зависят от конкретного выбора последовательностей $\{x_n\}$, $\{y_n\}$. Они называются соответственно *суммой* и *произведением классов* α и β;

в) множество $\mathbb{Q}_p$ является полем относительно определенных в п. б) операций сложения и умножения;

г) если $\{x_n\} \in \alpha$, то $\{|x_n|_p\}$ — фундаментальная последовательность в поле вещественных чисел $\mathbb{R}$ и $\lim\limits_{n\to\infty} |x_n|_p$ не зависит от конкретного выбора последовательности $\{x_n\}$. Этот предел называется *p-адической нормой* элемента $\alpha \in \mathbb{Q}_p$ и обозначается $|\alpha|_p$;

д) поле $\mathbb{Q}$ изоморфно вкладывается в $\mathbb{Q}_p$ путем сопоставления элементу $x \in \mathbb{Q}$ последовательности $(x, x, \ldots)$;

е) поле $\mathbb{Q}$ (при его отождествлении со своим изоморфным образом) всюду плотно в $\mathbb{Q}_p$;

ж) поле $\mathbb{Q}_p$ является полным относительно p-адической нормы $|\alpha|_p$ (любая фундаментальная последовательность $\{x_n\}$ элементов поля $\mathbb{Q}_p$ сходится к некоторому элементу $\alpha \in \mathbb{Q}_p$ ($|x_n - \alpha|_p \to 0$ при $n \to \infty$);

з) поле $\mathbb{Q}_p$ определено единственным образом с точностью до изоморфизма над $\mathbb{Q}$, сохраняющего p-адическую сходимость. Оно называется *полем p-адических чисел*.

7. Доказать, что поле $\mathbb{Q}_p$ изоморфно полю всех сходящихся по p-адической норме рядов

$$\sum_{\nu=m}^{\infty} a_\nu p^\nu, \quad a_\nu \in \mathbb{Z}, \quad 0 \leqslant a_\nu \leqslant p-1, \quad a_m \neq 0.$$

8. Замыкание кольца $\mathbb{Z}$ в поле $\mathbb{Q}_p$ относительно p-адической топологии называется *кольцом целых p-адических чисел* и обозначается $\mathbb{Z}_p$. Доказать, что кольцо $\mathbb{Z}_p$ компактно.

9. Доказать, что для различных простых p и p' поля $\mathbb{Q}_p$ и $\mathbb{Q}_{p'}$ не изоморфны между собой. Показать, что всякое поле $\mathbb{Q}_p$ не изоморфно полю вещественных чисел $\mathbb{R}$.

10. Пусть a — целое, не делящееся на простое число p. Доказать, что в поле $\mathbb{Q}_p$ последовательность $\{a^{p^n}\}$ сходится и ее предел α удовлетворяет условию $\alpha^{p-1} = 1$. Показать, что в поле $\mathbb{Q}_p$ многочлен $T^{p-1} - 1$ полностью раскладывается на линейные множители.

11. Нормирование v поля K называется *дискретным*, если v является гомоморфизмом K^* на $\mathbb{Z}$. Доказать, что эпиморфизм $v\colon K^* \to \mathbb{Z}$ является нормированием поля K в том и только в том случае, если $v(n \cdot e) \geqslant 0$ для всех целых кратных $n \cdot e$, $n \geqslant 1$, единичного элемента e поля K.

12. Пусть $\mathfrak{o}$ — кольцо дискретного нормирования поля K. Доказать справедливость следующих утверждений:

а) в максимальном идеале $\mathfrak{m}$ кольца $\mathfrak{o}$ имеет такой элемент t, что $v(t)$ порождает группу $\mathbb{Z}$. Элемент t называется *униформизирующим* (или *локальным*) *параметром идеала* $\mathfrak{m}$;

б) всякий элемент $x \in K$ представляется в виде $x = ut^n$, где u — обратимый элемент кольца $\mathfrak{o}$ и $n \in \mathbb{Z}$;

в) $\mathfrak{m} = t\mathfrak{o}$;

г) каждый идеал $\mathfrak{a} \neq (0)$ в кольце $\mathfrak{o}$ является главным и имеет вид $\mathfrak{a} = \mathfrak{m}^r$ при некотором целом $r \geqslant 0$.

13. Пусть k — произвольное поле и $k(t)$ — поле рациональных функций над k. Каждую рациональную функцию $\varphi \in k(t)$ можно однозначно представить в виде

$$\varphi = t^m \frac{f(t)}{g(t)}, \quad f(0) \neq 0, \quad g(0) \neq 0,$$

где f, g — многочлены. Доказать, что функция

$$v(\varphi) = m, \quad v(0) = \infty,$$

задает нормирование поля $k(t)$. Показать, что пополнение поля $k(t)$ относительно нормы

$$|\varphi|_v = \rho^{v(\varphi)}, \quad 0 < \rho < 1,$$

изоморфно *полю* $k((t))$ *формальных степенных рядов*, состоящему из всех рядов вида

$$\sum_{\nu=m}^{\infty} a_\nu t^\nu, \quad a_\nu \in k, \quad a_m \neq 0,$$

с обычными правилами действий над степенными рядами.

14. Пусть $k(x, y)$ — поле рациональных функций от x и y над полем k. Для произвольного целого ν положим $x_\nu = xy^{-\nu}$. Отличную от нуля рациональную функцию $\varphi(x, y) \in k(x, y)$ представим в виде

$$\varphi(x, y) = \varphi\left(x_\nu y^\nu, y\right) = y^n \frac{f(x_\nu, y)}{g(x_\nu, y)},$$

где многочлены f и g не делятся на y. Показать, что функция $v_\nu(\varphi) = n$, $v_\nu(0) = \infty$ определяет нормирование поля $k(x, y)$.

15. Пусть x, x' — точки на эллиптической кривой

$$E\colon\ x_0 x_2^2 = x_1^3 + a x_0 x_1^2 + b x_0^3, \quad 4a^3 + 27b^2 \neq 0.$$

Доказать, что сопоставление $x \mapsto C_x$ точке $x \in E$ класса $C_x \in \mathrm{Cl}^0(E)$, содержащего дивизор $x - x'$, задает взаимно однозначное соответствие между точками кривой E и элементами группы $\mathrm{Cl}(E)$.

16. В условиях предыдущей задачи показать, что $C_x + C_y + C_z = 0$ в том и только в том случае, если точки x, y, z лежат на одной прямой.

17. В условиях задачи **15** выяснить закон сложения классов C_x, $C_y \in \mathrm{Cl}^0(E)$ в терминах точек x, $y \in E$, если в качестве x' взята бесконечно удаленная точка.

18. В условиях задачи **15** доказать, что группа $\mathrm{Cl}^0(E)$ имеет ровно четыре элемента второго порядка. Найти соответствующие им точки на кривой E.

§ 3. Теорема Римана — Роха на алгебраической кривой

1. Теорема Римана. Пусть $L = k(X)$ — поле рациональных функций на алгебраической кривой X, D — дивизор на X и

$$L(D) = \{f \in L \mid f \equiv 0 \pmod{D}\}$$

— линейное пространство над k, состоящее из рациональных функций на кривой X, сравнимых с нулем по $\bmod D$.

Теорема 1. *Для любого дивизора* $D \in \mathrm{Div}(X)$ *размерность* $\dim_k L(D)$ *пространства* $L(D)$ *конечна. Более того, если* $D \geqslant D'$, *то*

$$\dim_k L(D') - \dim_k L(D) \leqslant \deg D - \deg D' = \deg(D - D').$$

Доказательство. Поскольку $D \geqslant D'$, то $L(D) \subset L(D')$. Покажем, что

$$\dim_k L(D')/L(D) \leqslant \deg D - \deg D'.$$

Пусть $D = \sum_{x \in X} a_x \cdot x$, $D' = \sum_{x \in X} a'_x \cdot x$ и S — множество точек $x \in X$, для которых либо $a_x \neq 0$, либо $a'_x \neq 0$. По лемме 1 из § 2 имеем

$$\dim_k L(S, D')/L(S, D) = \deg D - \deg D' = \sum_{x \in S} (a_x - a'_x) = \deg(D - D').$$

Далее, справедливо равенство

$$L(D) = L(D') \cap L(S, D).$$

Действительно, так как $L(D) \subset L(D')$ и $L(D) \subset L(S, D)$, то

$$L(D) \subset L(D') \cap L(S, D).$$

Обратно, если $f \in L(D') \cap L(S, D)$, то $v_x(f) \geqslant a_x$ для всех $x \in S$ и $v_x(f) \geqslant 0$ при $x \notin S$. Тогда $v_x(f) \geqslant a_x$ для всех $x \in X$ и, значит, $f \in L(D)$. Следовательно,

$$L(D) \supset L(D') \cap L(S, D)$$

и, стало быть,

$$L(D) = L(D') \cap L(S, D).$$

В таком случае

$$L(D')/L(D) = L(D')/L(D') \cap L(S, D)$$

и поскольку (см. [70d, с. 95; 8, с. 29])

$$L(D')/L(D') \cap L(S, D) \simeq (L(D') + L(S, D))/L(S, D) \subset L(S, D')/L(S, D),$$

то

$$\dim_k L(D')/L(D) \leqslant \deg D - \deg D'.$$

Для данного дивизора D' возьмем такой дивизор D, что $D \geqslant D'$ и $\deg D > 0$. Имеем $L(D) = \{0\}$ и тогда

$$\dim_k L(D') < \infty.$$

Далее, поскольку для любых двух дивизоров $D \geqslant D'$ пространства $L(D)$ и $L(D')$ конечномерны, то

$$\dim_k L(D') - \dim_k L(D) \leqslant \deg D - \deg D'$$

и тем самым теорема доказана.

Положим $l(D)=\dim_k L(D)$ и $i(D)=l(D)+\deg D$. Если $D'\geqslant D$, то из теоремы 1 следует, что $i(D')\geqslant i(D)$.

Теорема 2. *Функция $i(D)$ является функцией классов дивизоров: $i(D)=i(D')$ при $D\sim D'$.*

Доказательство. Поскольку $\deg D$ является функцией классов дивизоров, то теорему достаточно доказать для $l(D)$. Пусть $D'=D+(f)$, $f\neq 0$ и $D=\sum_{x\in X} a_x\cdot x$, $D'=\sum_{x\in X} a'_x\cdot x$. Установим изоморфизм пространств $L(D)$ и $L(D')$. Если $u\in L(D)$, то $v_x(uf)=v_x(u)+v_x(f)\geqslant a_x+v_x(f)=a'_x$ и, значит, $uf\in L(D')$. В таком случае отображение $u\mapsto uf$ является линейным отображением $L(D)$ в пространство $L(D')$. Поскольку $f\neq 0$, то это отображение биективно.

Теорема 3. *Функция $i(D)$ ограничена снизу.*

Доказательство. Зафиксируем функцию $f\in L=k(X)$, $f\notin k$, и обозначим $D_0=(f)_0=\sum_{x\in X} a^0_x\cdot x$ дивизор нулей функции f. Из доказательства теоремы 7 § 2 следует существование таких целых $\mu=\mu(f)$ и $\tau=(\mu-1)\deg D_0$, что

$$i(-\nu D_0)=l(-\nu D_0)+\deg(-\nu D_0)\geqslant -\tau$$

для всех $\nu>\mu$. Отсюда получаем ограниченность $i(D)$ на семействе $\{-\nu D_0\}$.

Покажем теперь, что для любого дивизора $D=\sum_{x\in X} a_x\cdot x$ найдется эквивалентный ему дивизор D', удовлетворяющий условию $D'\geqslant -\nu D_0$ при всех $\nu>\mu'\geqslant\mu$. Пусть $x_1,\ \ldots,\ x_s$ — все нули функции f и $f(x)\neq 0$. Тогда $f^{-1}(x)=\alpha_x\in k$ и $v_x(f^{-1}-\alpha_x)\geqslant 1$. Определим функцию $g\neq 0$ равенством

$$g=\prod_{\substack{x\in X,\\ v_x(f)\leqslant 0,\\ a_x<0}} (f^{-1}-\alpha_x)^{-\alpha_x}$$

и положим $D'=D+(g)=\sum_{y\in X} a'_y\cdot y$. Выберем $\nu>\mu$ настолько большим, чтобы $a_{x_i}\geqslant -\nu a^0_{x_i}$ при всех $i=1,\ 2,\ \ldots,\ s$, и покажем, что $D'\geqslant -\nu D_0$, т. е. что $a'_y\geqslant -\nu a^0_y$ для всех $y\in X$. При $y=x_i$ это верно по выбору числа ν. Пусть теперь $y\neq x_i$. В этом случае $a^0_y=0$ и мы должны показать, что $a'_y=a_y+v_y(g)\geqslant 0$. Заметим, что поскольку $f(y)\neq 0$, то $v_y(f)\leqslant 0$ и $v_y(f^{-1})\geqslant 0$. Если множества точек $x\in X$, по которым берется произведение в определении функции g, пусто, то $g=1$, и тогда $a'_y\geqslant v_y(1)=0$. Пусть это множество не пусто. Предположим сначала, что $a_y\geqslant 0$. Имеем $v_y(f^{-1})\geqslant 0$ и, значит, $v_y(f^{-1}-\alpha_x)\geqslant 0$. В таком случае $v_y(g)\geqslant 0$

и тогда $a'_y=a_y+v_y(g)\geqslant 0$. Пусть $a_y<0$. В этом случае

$$a'_y=a_y+v_y(g)=a_y+\sum_{\substack{v_x(f)\leqslant 0,\\ a_x<0}}(-a_x)\,v_y(f^{-1}-\alpha_x)=$$

$$=a_y-a_y v_y(f^{-1}-\alpha_y)+\sum_{\substack{x\neq y,\\ v_x(f)\leqslant 0,\\ a_x<0}}(-a_x)\,v_y(f^{-1}-\alpha_x)\geqslant$$

$$\geqslant -a_y\left(v_y(f^{-1}-\alpha_y)-1\right)\geqslant 0$$

и теорема доказана.

Из теоремы 3 следует, что $i(D)\geqslant -\tau$ для всех $D\in\mathrm{Div}(X)$ и, значит, на некотором дивизоре D функция $i(D)$ принимает свое минимальное значение.

Определение 1. *Родом алгебраической кривой X* называется целое число g, удовлетворяющее условию

$$-g+1=\min_{D\in\mathrm{Div}(X)} i(D).$$

Так как $i(D)=l(D)+\deg D\geqslant -g+1$ для всякого дивизора D, то, полагая $D=0$, получаем $i(0)=l(0)=1\geqslant -g+1$. Следовательно, род g кривой X является неотрицательным целым числом. С некоторыми способами вычисления рода и с примерами кривых рода 0,1 читатель может познакомиться по задачам 11—15 данного параграфа.

Теорема Римана. *Если X — алгебраическая кривая рода g, то для каждого дивизора $D\in\mathrm{Div}(X)$ выполняется неравенство*

$$i(D)=l(D)+\deg D\geqslant -g+1.$$

2. Распределения. Дальнейшей нашей целью является изучение величины

$$\lambda(D)=l(D)+\deg D+g-1=i(D)+g-1.$$

По теореме Римана $\lambda(D)\geqslant 0$ для всех $D\in\mathrm{Div}(X)$. При некотором D достигается равенство $\lambda(D)=0$, и это равенство выполняется для всех $D'\leqslant D$.

Рассмотрим кольцо F всех (в самом широком смысле) функций r: $X\to L=k(X)$, определенных на кривой X со значениями в поле L. Для каждой функции $r\in F$ и для каждой точки $x\in X$ положим $v_x(r)=v_x(r(x))$.

Определение 2. Функция r: $X\to L$ называется *распределением*, если для почти всех точек $x\in X$ (для всех $x\in X$, кроме их конечного числа) выполняется условие $v_x(r)\geqslant 0$.

Пусть R — множество всех распределений. Покажем, что R является подкольцом кольца F. Действительно, если $r,\ r'\in R$, то

$$v_x(r\pm r')\geqslant\min(v_x(r),\ v_x(r')),$$

$$v_x(r\cdot r')=v_x(r)+v_x(r')$$

и, значит, $v_x(r\pm r')\geqslant 0$, $v_x(r\cdot r')\geqslant 0$ для почти всех $x\in X$.

Пусть $f \in L$ — функция на X. Обозначим r_f функцию, которая в каждой точке $x \in X$ принимает значение f. Так как f имеет конечное число полюсов, то $v_x(r_f) \geqslant 0$ для почти всех x и, значит, r_f является распределением. Распределение r_f называется *главным распределением*. Отображение $L \to R$ является, очевидно, мономорфизмом и поэтому мы можем отождествить L с его образом в R при указанном отображении. Тогда R является векторным пространством над L и, значит, над полем k.

Пусть $D = \sum_{x \in X} a_x \cdot x$ — дивизор на X и $r \in R$ — некоторое распределение. Будем говорить, что r сравнимо с нулем по $\bmod D$ ($r \equiv 0 \pmod D$), если $v_x(r) \geqslant a_x$ для всех $x \in X$. Если $r = r_f$, то это определение совпадает с определением функции, сравнимой с нулем по $\bmod D$. Очевидно, что все распределения, сравнимые с нулем по $\bmod D$, образуют линейное пространство

$$R(D) = \{r \in R \mid r \equiv 0 \pmod D\} = \{r \in R \mid v_x(r) \geqslant a_x \text{ для всех } x \in X\}$$

над полем k, и можно считать, что $L(D) \subset R(D)$. Распределения r и r' назовем *сравнимыми* по $\bmod D$ ($r \equiv r' \pmod D$), если $r - r' \equiv 0 \pmod D$.

Теорема 4 (о распределениях). *Если* $D \geqslant D'$, *то* $R(D) \subset R(D')$ *и*

$$\dim_k R(D')/R(D) = \deg D - \deg D'.$$

Доказательство. Пусть $D = \sum_{x \in X} a_x \cdot x$, $D' = \sum_{x \in X} a'_x \cdot x$ и S — такое конечное множество точек, что $a_x = a'_x = 0$ при всех $x \notin S$. По лемме 1 из § 2 имеем

$$\dim_k L(S, D')/L(S, D) = \deg D - \deg D'$$

и поэтому для доказательства теоремы достаточно показать, что

$$R(D')/R(D) \simeq L(S, D')/L(S, D).$$

Для каждой функции $u \in L(S, D')$ введем в рассмотрение распределение

$$r^u(x) = \begin{cases} u, & \text{если } x \in S, \\ 0, & \text{если } x \notin S, \end{cases}$$

и покажем, что $r^u \in R(D')$. Действительно, если $x \in S$, то $v_x(r^u) = v_x(u) \geqslant a'_x$, а если $x \notin S$, то $v_x(r^u) = \infty$. Значит, $v_x(r^u) \geqslant a'_x$ для всех $x \in X$ и тогда $r^u \in R(D')$. В таком случае сопоставление $u \mapsto r^u$ задает k-линейное отображение $\alpha\colon L(S, D') \to R(D')$ пространства $L(S, D')$ в пространстве $R(D')$. Обозначим $\lambda = \pi \circ \alpha$ составное отображение

$$\lambda\colon L(S, D') \xrightarrow{\alpha} R(D') \xrightarrow{\pi} R(D')/R(D),$$

где π — естественный гомоморфизм $R(D')$ на $R(D')/R(D)$. Ядром отображения λ является пространство

$$\operatorname{Ker} \lambda = \{u \in L(S, D') \mid r^u \in R(D)\} = L(S, D),$$

и для доказательства теоремы достаточно показать, что отображение λ сюръективно.

Пусть $\bar{r} \in R(D')/R(D)$ и r — представитель класса $\bar{r}$ в $R(D')$. По теореме об аппроксимации существует такой элемент $u \in L$, что $v_x(u - r) \geqslant a_x$ для всех $x \in S$. Так как

$$v_x(u) = v_x(u - r + r) \geqslant \min\{v_x(u - r), v_x(r)\} \geqslant a'_x$$

для всех $x \in S$, то $u \in L(S, D')$. Покажем, что $\lambda(u) = \pi(\alpha(u)) = \bar{r}$. Для этого достаточно доказать, что $\bar{r} = \bar{r}^u$ или, что $r \equiv r^u \pmod D$. Следовательно, достаточно показать, что $v_x(r - r^u) \geqslant a_x$ для всех $x \in X$. Но если $x \in S$, то $v_x(r - r^u) = v_x(r - u) \geqslant a_x$ по выбору функции u. Если же $x \notin S$, то $v_x(r - r^u) = v_x(r) \geqslant a'_x = 0 = a_x$. Теорема доказана.

Отождествим снова поле L с его образом в R при рассмотренном выше отображении $L \to R$. Тогда сумму $R(D) + L$ можно рассматривать как подпространство пространства R.

Теорема Римана — Роха (первая форма). *Для любого дивизора* D *факторпространство* $R/R(D) + L$ *конечномерно и его размерность над полем* k *равна* $\lambda(D) = l(D) + \deg D + g - 1 = i(D) + g - 1$.

Доказательство. Доказательство теоремы разобьем на три этапа.

1) Докажем сначала, что если $D \geqslant D'$, то

$$\dim_k (R(D') + L)/R(D) + L = i(D) - i(D').$$

Предварительно покажем, что имеет место равенство

$$R(D') \cap (R(D) + L) = R(D) + L(D').$$

В самом деле, правая часть равенства очевидным образом входит в левую. Возьмем элемент $r' = r + f$ из левой части, где $r' \in R(D')$, $r \in r(D)$ и $f \in L$. Так как $r, r' \in R(D')$, $R(D) \subset R(D')$, то $f \in L(D')$ и, значит, левая часть входит в правую. Равенство доказано.

Применяя теорему об изоморфизме (см. [70d, с. 95; 8, с. 29]), получаем

$$\begin{aligned}(R(D') + L)/R(D) + L &= (R(D') + R(D) + L)/R(D) + L \simeq \\ &\simeq R(D')/R(D') \cap (R(D) + L) \simeq R(D')/R(D) + L(D') \simeq \\ &\simeq \{R(D')/R(D)\}/\{(R(D) + L(D'))/R(D)\} \simeq \\ &\simeq \{R(D')/R(D)\}/\{L(D')/L(D') \cap R(D)\}.\end{aligned}$$

Но $L(D')\cap R(D)=L(D)$ и тогда

$$(R(D')+L)/R(D)+L\simeq\{R(D')/R(D)\}/\{L(D')/L(D)\}.$$

Таким образом

$$\dim_k(R(D')+L)/R(D)+L=$$
$$=\dim_k R(D')/R(D)-\dim_k L(D')/L(D)=$$
$$=\deg D-\deg D'-l(D')+l(D)=i(D)-i(D').$$

2) Покажем теперь, что

$$\dim_k R/R(D)+L\leqslant\lambda(D).$$

Пусть $D=\sum\limits_{x\in X}a_x\cdot x$ и $r_1,\ \ldots,\ r_m$ — линейно независимые над k по $\mathrm{mod}\,(R(D)+L)$ элементы пространства R. Для каждой точки $x\in X$ положим

$$a'_x=\min(a_x,\ v_x(r_1),\ \ldots,\ v_x(r_m)).$$

Так как $r_1,\ \ldots,\ r_m$ — распределения, то можно указать такое конечное множество S точек x, что $v_x(r_i)\geqslant 0$ и $a_x=0$ для всех $x\notin S$. Поэтому имеет смысл дивизор $D'=\sum\limits_{x\in X}a'_x\cdot x$. Для всех $x\in X$ имеем $a_x\geqslant a'_x$ и, значит, $D\geqslant D'$. Кроме того, $v_x(r_i)\geqslant a'_x$ для всех $x\in X$ и $i=1,\ 2,\ \ldots,\ m$. Тогда $r_i\in R(D')$ и, тем более, $r_i\in R(D')+L$. Таким образом, если $\bar r_1,\ \ldots,\ \bar r_m$ — классы вычетов по $\mathrm{mod}\,(R(D)+L)$, содержащие $r_1,\ \ldots,\ r_m$ соответственно, то $\bar r_1,\ \ldots,\ \bar r_m\in(R(D')+L)/R(D)+L$ и, следовательно,

$$m\leqslant i(D)-i(D')\leqslant i(D)+g-1=\lambda(D).$$

3) Покажем, наконец, что

$$\lambda(D)\leqslant\dim_k R/R(D)+L.$$

Пусть D_0 такой дивизор, что $i(D_0)=-g+1$ и пусть $D\geqslant D'$, $D_0\geqslant D'$ (в качестве D' можно взять, например, наибольший общий делитель $(D,\ D_0)$ дивизоров D и D_0). Имеем $i(D')=-g+1$ и тогда

$$\dim_k(R(D')+L)/R(D)+L=i(D)-i(D')=i(D)+g-1=\lambda(D).$$

Но $(R(D')+L)/R(D)+L$ является подпространством пространства $R/R(D)+L$ и, значит,

$$\dim_k R/R(D)+L\geqslant\lambda(D).$$

Теорема доказана.

3. Дифференциалы. Для приложений более удобна иная форма теоремы Римана — Роха, основанная на понятии дифференциала.

Пусть $D=\sum\limits_{x\in X}a_x\cdot x$ и $L(-D)=\{f\in L\mid v_x(f)+a_x\geqslant 0$ для всех $x\in X\}=\{f\in L\mid (f)+D\geqslant 0$, либо $f=0\}$. Если в теореме Римана — Роха заменить D на $-D$, то получим

$$l(-D)-\deg D+g-1=\dim_k R/R(-D)+L,$$

или

$$l(-D)=\deg D-g+1+\dim_k R/R(-D)+L.$$

Определение 3. *Дифференциалом* на кривой X называется всякий линейный функционал $\omega\colon R\to k$ на пространстве распределений R, аннулирующий подпространство $R(-D)+L$ при некотором $D\in\mathrm{Div}(X)$ $(\omega|_{R(-D)+L}=0)$.

Определение 4. Если дифференциал ω и дивизор D связаны соотношением $\omega|_{R(-D)+L}=0$, то будем говорить, что ω *сравним с нулем по* $\mathrm{mod}\,D$ и писать $\omega\equiv 0\ (\mathrm{mod}\,D)$.

Укажем основные свойства дифференциалов.

Предложение 1. *Множество всех дифференциалов на* X *образует линейное пространство над* k.

Доказательство. Если ω и ω' — дифференциалы, то существуют такие дивизоры D и D', что $\omega|_{R(-D)+L}=0$ и $\omega'|_{R(-D')+L}=0$. Пусть α, β — элементы поля k. Ясно, что $\alpha\omega+\beta\omega'|_L=0$. Положим $D_0=(D,\ D')$, так что $D_0\leqslant D$ и $D_0\leqslant D'$. Тогда $-D_0\geqslant -D$, $-D_0\geqslant -D'$ и, следовательно, $R(-D_0)\subset R(-D)$, $R(-D_0)\subset R(-D')$. В таком случае $\alpha\omega+\beta\omega'|_{R(-D_0)}=0$ и, значит, $\alpha\omega+\beta\omega'|_{R(-D_0)+L}=0$. Таким образом, линейная комбинация $\alpha\omega+\beta\omega'$ дифференциалов ω и ω' снова является дифференциалом. Предложение, тем самым, доказано.

Предложение 2. *Если* $\omega\equiv 0\ (\mathrm{mod}\,D)$ *и* $D'\leqslant D$, *то* $\omega\equiv 0\ (\mathrm{mod}\,D')$.

Доказательство очевидным образом следует из включения $R(-D')\subset R(-D)$.

Предложение 3. *Если* $\omega\equiv 0\ (\mathrm{mod}\,D)$ *и* $\omega\equiv 0\ (\mathrm{mod}\,D')$, *то* $\omega\equiv 0\ (\mathrm{mod}\,D_0)$, *где* $D_0=\{D,\ D'\}$ — *наименьшее общее кратное дивизоров* D *и* D'.

Доказательство. Пусть $D=\sum\limits_{x\in X}a_x\cdot x$, $D'=\sum\limits_{x\in X}a'_x\cdot x$ и $D_0=\sum\limits_{x\in X}a^0_x\cdot x$, где $a^0_x=\max(a_x,\ a'_x)$. Для доказательства предложения достаточно установить, что

$$R(-D_0)\subset R(-D)+R(-D').$$

Для каждого $r\in R(-D_0)$ положим

$$r'(x)=\begin{cases}r(x), & \text{если } a^0_x=a_x\geqslant a'_x,\\ 0, & \text{в противном случае.}\end{cases}$$

Ясно, что r' является распределением. Более того, если $r'(x)\neq 0$, то $(r')v^x\geqslant -a^0_x=-a_x$ и, стало быть, $r'\in R(-D)$. Представим

$r \in R(-D_0)$ в виде $r = r' + r''$ и покажем, что $r'' \in R(-D')$. В самом деле, если $r''(x) \neq 0$, то $r(x) \neq r'(x)$ и тогда $r'(x) = 0$. В таком случае $r''(x) = r(x)$, и, следовательно, $v_x(r'') = v_x(r) \geqslant -a_x^0 = -a_x'$. Значит, $r'' \in R(-D')$. Таким образом, каждый элемент $r \in R(-D_0)$ представим в виде $r = r' + r''$, где $r' \in R(-D)$, $r'' \in R(-D')$, что и требовалось доказать.

Обозначим Δ *линейное пространство всех дифференциалов над полем* k. Множество

$$\Delta(D) = \{\omega \in \Delta \mid \omega \equiv 0 \pmod{D}\}$$

является конечномерным подпространством этого пространства. Действительно, поскольку $\Delta(D)$ — пространство линейных функционалов на $R/R(-D)+L$, $\Delta(D)$ является двойственным к $R/R(-D)+L$ пространством: $\Delta(D) = (R/R(-D)+L)^*$. По теореме Римана — Роха пространство $R/R(-D)+L$ конечномерно и, значит, размерность $\delta(D) = \dim_k \Delta(D)$ пространства $\Delta(D)$ совпадает с размерностью $\dim_k R/R(-D)+L$ пространства $R/R(-D)+L$.

Тем самым можно переформулировать теорему Римана — Роха следующим образом:

Теорема Римана — Роха (вторая форма). *Для любого дивизора* D *имеет место равенство*

$$l(-D) = \deg D - g + 1 + \delta(D).$$

Заметим, что $l(-D)$, $\deg D$ являются функциями классов дивизоров. Поэтому $\delta(D)$ также является функцией классов дивизоров и, стало быть, если $C \in \mathrm{Cl}(X)$ — класс дивизора D, то последнее равенство можно переписать в виде

$$l(-C) = \deg C - g + 1 + \delta(C).$$

Пример. Пусть k — поле комплексных чисел и $L = k(z)$ — поле рациональных функций от комплексного переменного z с коэффициентами из k (поле рациональных функций на аффинной прямой $\mathbb{A}^1$). Для всякой функции $f \in k(z)$ символ $f\,dz$ назовем *дифференциальной формой* на $\mathbb{A}^1$. Если $r \in R$ — произвольное распределение поля L, то можно определить вычет выражения $rf\,dz$ в точке $x \in \mathbb{A}^1 \cup \{x_\infty\}$ (x_∞ — бесконечно удаленная точка) при помощи равенства

$$\mathrm{Res}_x(rf\,dz) = \frac{1}{2\pi i}\int_\Gamma r(x) f\,dz,$$

где Γ — замкнутый контур, не содержащий внутри себя других полюсов функции $r(x)f$, кроме, быть может, самой точки x. Определим скалярное произведение $(f\,dz, r)$ равенством

$$(f\,dz, r) = \sum_{x \in \mathbb{A}^1 \cup \{x_\infty\}} \mathrm{Res}_x(rf\,dz).$$

Если $r = r_\varphi$ — главное распределение, то согласно теореме о вычетах

$$(f\,dz, r_\varphi) = \sum_{x \in \mathbb{A}^1 \cup \{x_\infty\}} \mathrm{Res}(\varphi f\,dz) = 0$$

и, значит, скалярное произведение $(f\,dz, r)$ аннулирует пространство L. Далее, положим $v_x(f\,dz) = v_x(f)$, если $x \in \mathbb{A}^1$; $v_{x_\infty}(f\,dz) = v_{x_\infty}(f) - 2$ и для каждого дивизора $D = \sum_{x \in \mathbb{A}^1 \cup \{x_\infty\}} a_x \cdot x$ рассмотрим пространства

$$\Omega(D) = \{f\,dz \mid v_x(f\,dz) \geqslant a_x\}$$

и

$$R(-D) = \{r \in R \mid v_x(r) \geqslant -a_x\}.$$

Так как для любой точки $x \in \mathbb{A}^1 \cup \{x_\infty\}$ и при любых $f\,dz \in \Omega(D)$, $r \in R(-D)$ имеем $\mathrm{Res}_x(rf\,dz) = 0$, то скалярное произведение (fdz, r), $fdz \in \Omega(D)$, аннулирует пространство $R(-D)+L$. Следовательно, линейный функционал $\omega(r) = (fdz, r)$ является дифференциалом на проективной прямой $\mathbb{P}^1 = \mathbb{A}^1 \cup \{x_\infty\}$.

Используя теорему Римана — Роха, нетрудно доказать (см. [145b, гл. II, § 5]), что справедливо и обратное, а именно, что каждый линейный функционал на пространстве распределений R, аннулирующий подпространство $R(-D)+L$, имеет вид $\omega = (f\,dz, r)$ для некоторого дифференциальной формы $f\,dz \in \Omega(D)$. Аналогичный результат о двойственности пространств $\Omega(D)$ и $R/R(-D)+L$ справедлив также и для общего случая — поля $L = k(X)$ рациональных функций на кривой X (см. [110c, с. 28; 70e, гл. 1, § 5] и задачи 1—10 данного параграфа).

Покажем теперь, что пространство дифференциалов Δ можно рассматривать как линейное пространство над полем L. Для этого введем умножение дифференциалов $\omega \in \Delta$ на элементы $f \in L$. Именно, определим произведение $f\omega$ равенством $(f\omega)(r) = \omega(r_f r)$ и покажем, что оно также является дифференциалом, Действительно, если $r, r' \in R$ и $\alpha, \beta \in k$, то имеем

$$(f\omega)(\alpha r + \beta r') = \omega(r_f(\alpha r + \beta r')) =$$
$$= \omega(\alpha r_f r + \beta r_f r') = \alpha\omega(r_f r) + \beta\omega(r_f r') =$$
$$= \alpha(f\omega)(r) + \beta(f\omega)(r').$$

Далее, если $\omega \equiv 0 \pmod{D}$ и $r \in R(-D-(f))$, то $r_f r \in R(-D)$ и, значит, функционал $f\omega$ аннулирует подпространство $R(-D-(f))+L$ пространства R. Легко проверить, что введенное умножение обладает свойствами:

а) $(f+f')\omega = f\omega + f'\omega$,
б) $f(\omega+\omega') = f\omega + f\omega'$,
в) $(ff')\omega = f(f'\omega)$,
г) $1 \cdot \omega = \omega$.

Следовательно, Δ является линейным пространством над L.

Теорема 5 (о пространстве дифференциалов). *Пространство Δ является одномерным пространством над полем $L = k(X)$.*

Доказательство. Покажем сначала, что существует хотя бы один отличный от нуля дифференциал $\omega \in \Delta$. По теореме Римана — Роха имеем

$$\delta(D) = -\deg D + g - 1 + l(-D).$$

Возьмем строго положительный дивизор D', удовлетворяющий условию $\deg D' > 1 - g$, и положим $D = -D'$. Тогда

$$l(-D) = \dim_k L(-D) = \dim_k L(D') = 0$$

и, стало быть,

$$\delta(D) = \deg D' + g - 1 > 0.$$

Следовательно, в пространстве $\Delta(D)$ найдется дифференциал $\omega \neq 0$.

Пусть ω' — любой другой дифференциал пространства Δ. Покажем, что $\omega' = f\omega$ для некоторого элемента $f \in L$. Пусть $\omega \equiv 0 \pmod{D}$, $\omega' \equiv 0 \pmod{D'}$ и D_0 — такой положительный дивизор, что

$$\deg D_0 > g - 1 - \deg D,$$
$$\deg D_0 > g - 1 - \deg D',$$
$$\deg D_0 > 3g - 2 - \deg D - \deg D'.$$

Рассмотрим пространства $L(-D_0 - D)$, $L(-D_0 - D')$ и положим $m = \dim_k L(-D_0 - D)$, $m' = \dim_k L(-D_0 - D')$. Учитывая выбор дивизора D_0 и используя теорему Римана — Роха, имеем

$$m \geqslant \deg D_0 + \deg D - g + 1 > 0.$$
$$m' \geqslant \deg D_0 + \deg D' - g + 1 > 0.$$

Пусть $f_1, \ldots, f_m$ и $f_1', \ldots, f_{m'}'$ — базисы пространств $L(-D_0 - D)$ и $L(-D_0 - D')$ соответственно. Рассмотрим дифференциалы $f_1\omega, \ldots, f_m\omega, f_1'\omega', \ldots, f_{m'}'\omega'$ и покажем, что все они принадлежат пространству $\Delta(-D_0)$. В самом деле, $f_i\omega \equiv 0 \pmod{((f_i) + D)}$ и, так как $f_i \in L(-D_0 - D)$, то $(f_i) \geqslant -D_0 - D$. Стало быть, $(f_i) + D \geqslant -D_0$ и, значит, $f_i\omega \equiv 0 \pmod{(-D_0)}$. Аналогичным образом $f_i'\omega' \equiv 0 \pmod{(-D_0)}$ и, следовательно, $f_1\omega, \ldots, f_m\omega, f_1'\omega', \ldots, f_{m'}'\omega' \in \Delta(-D_0)$.

Оценим размерность пространства $\Delta(-D_0)$. В силу теоремы Римана — Роха имеем

$$\dim_k \Delta(-D_0) = \deg D_0 + g - 1 + l(D_0).$$

Так как D_0 — положительный дивизор, то $l(D_0) = \dim_k L(D_0) \leqslant 1$ и тогда

$$\dim_k \Delta(-D_0) \leqslant \deg D_0 + g.$$

Далее, поскольку

$$m + m' \geqslant 2\deg D_0 + \deg D + \deg D' - 2g + 2 > \deg D_0 + g,$$

то имеем

$$\dim_k \Delta(-D_0) < m + m'.$$

Отсюда следует, что дифференциалы $f_1\omega, \ldots, f_m\omega, f_1'\omega', \ldots, f_{m'}'\omega'$ линейно зависимы над полем k, т. е. существуют такие отличные в совокупности от нуля элементы $\lambda_1, \ldots, \lambda_m, \lambda_1', \ldots, \lambda_{m'}'$ поля k, для которых

$$\sum_{i=1}^{m} \lambda_i f_i\omega + \sum_{i=1}^{m'} \lambda_i' f_i'\omega' = 0.$$

В таком случае

$$g\omega + g'\omega' = 0$$

и для доказательства теоремы остается показать, что $g' = \sum_{i=1}^{m'} \lambda_i' f_i' \neq 0$. Предположим противное, что $g' = 0$. Тогда в силу линейной независимости функций $f_1', \ldots, f_{m'}'$ получим $\lambda_1' = \ldots = \lambda_{m'}' = 0$ и, стало быть, $g\omega = 0$. Но по выбору дифференциала ω имеем $\omega \neq 0$, и следовательно, $g = \sum_{i=1}^{m} \lambda_i f_i = 0$. Из линейной независимости функций $f_1, \ldots, f_m$ вытекает, что $\lambda_1 = \ldots = \lambda_m = 0$ и, в таком случае, приходим в противоречие с выбором элементов $\lambda_1, \ldots, \lambda_m, \lambda_1', \ldots, \lambda_m'$. Таким образом, $g' \neq 0$ и, значит, $\omega' = -(g/g')\omega$. Теорема доказана.

Определение 5. Если $\omega \equiv 0 \pmod{(0)}$, то дифференциал ω называется *целым* или *дифференциалом первого рода*.

Теорема 6. *Размерность пространства $\Delta(0)$ дифференциалов первого рода равна роду g кривой X.*

Доказательство. По теореме Римана — Роха имеем

$$l(-D) = \deg D - g + 1 + \delta(D).$$

Положим $D = (0)$. Утверждение теоремы следует из того, что $l(0) = \dim_k L(0) = 1$ и $\deg(0) = 0$.

4. Канонический класс. В заключение параграфа введем в рассмотрение канонический класс дивизоров на кривой X.

Теорема 7 (о дифференциалах). *Для каждого ненулевого дифференциала ω существует дивизор (ω), обладающий следующими свойствами:*

1) $\omega \equiv 0 \pmod{(\omega)}$;

2) *если* $\omega \equiv 0 \pmod{D}$, *то* $D \leqslant (\omega)$.

Дивизор (ω) определен однозначно и может быть охарактеризован как дивизор D наибольшей степени, для которого $\omega \equiv 0 \pmod{D}$.

Доказательство. Покажем, сначала, что степени всех дивизоров, удовлетворяющих условию $\omega \equiv 0 \pmod{D}$, ограниче-

ны сверху одним и тем же числом. Прежде всего заметим, что поскольку $\omega \neq 0$, то $\delta(D) = \dim_k \Delta(D) \geqslant 1$. Докажем теперь, что $l(-D) = \dim_k L(-D) \leqslant g$. Если $D = (0)$, то утверждение следует из предыдущей теоремы. Пусть $D \neq (0)$ и пусть $f_1, \ldots, f_m$ — базис пространства $L(-D)$ над полем k. Рассмотрим дифференциалы $f_1\omega, \ldots, f_m\omega$. Они линейно независимы над полем k. Далее, поскольку $f_i\omega \equiv 0 \pmod{((f_i)+D)}$ и $(f_i)+D \geqslant 0$, то имеют место сравнения $f_i\omega \equiv 0 \pmod{(0)}$. Значит, все дифференциалы $f_1\omega, \ldots, f_m\omega$ являются дифференциалами первого рода, и их число m не превосходит $\dim_k \Delta(0) = g$. Таким образом, $m = l(-D) \leqslant g$ и, следовательно, ввиду теоремы Римана — Роха

$$\deg D \leqslant l(-D) + g - 1 - \delta(D) \leqslant 2g - 2.$$

Выберем среди дивизоров D, удовлетворяющих условию $\omega \equiv 0 \pmod{D}$, дивизор максимальной степени и обозначим его (ω). По построению имеем $\omega \equiv 0 \pmod{(\omega)}$. Далее, если $D' = (\omega)$ и D — произвольный дивизор, удовлетворяющий условию $\omega \equiv 0 \pmod{D}$, то ввиду предложения 3 имеем $\omega \equiv 0 \pmod{D_0}$, где $D_0 = (D', D)$. Поэтому, если предположим, что $D > D'$ для некоторого D, то получим, что $\omega \equiv 0 \pmod{D_0}$, где $\deg D_0 > \deg D'$. Но это противоречит выбору дивизора $D' = (\omega)$ и полученное противоречие показывает, что $D \leqslant D'$. Теорема доказана.

Определение 6. Дивизор (ω), удовлетворяющий условиям предыдущей теоремы, называется *дивизором отличного от нуля дифференциала* ω.

Следствие 1. *Если* $f \in L$, $f \neq 0$ *и* $\omega \in \Delta$, $\omega \neq 0$, *то* $(f\omega) = (f)+(\omega)$.

Доказательство. Пусть $f\omega \equiv 0 \pmod{D}$. Тогда $\omega = f^{-1}(f\omega) \equiv 0 \pmod{((f^{-1})+D)}$ и, так как $(f^{-1}) = -(f)$, то $\omega \equiv 0 \pmod{(D-(f))}$. Отсюда следует, что $D-(f) \leqslant (\omega)$ и, в таком случае, $D \leqslant (f)+(\omega)$. В частности, $(f\omega) \leqslant (f)+(\omega)$ и поскольку $f\omega \equiv 0 \pmod{((f)+(\omega))}$, то $(f)+(\omega) \leqslant (f\omega)$. Значит, $(f\omega) = (f)+(\omega)$, и следствие, тем самым, доказано.

Следствие 2. *Отличный от нуля дифференциал* ω *принадлежит пространству* $\Delta(D)$ *в том и только в том случае, если* $D \leqslant (\omega)$.

Доказательство. Если $D \leqslant (\omega)$, то $\omega \equiv 0 \pmod{D}$ и, значит, $\omega \in \Delta(D)$. Обратно, если $\omega \in \Delta(D)$, то $\omega \equiv 0 \pmod{D}$, и тогда $D \leqslant (\omega)$.

Следствие 3. *Ненулевой дифференциал* ω *является дифференциалом первого рода в том и только в том случае, если дивизор* (ω) *положителен.*

Следствие 4. *Дивизоры всех отличных от нуля дифференциалов лежат в одном и том же классе линейно эквивалентных между собой дивизоров.*

Доказательство. Пусть $\omega \neq 0$ — фиксированный дифференциал. Любой другой ненулевой дифференциал ω' имеет по теореме 5 вид $\omega' = f\omega$, $f \in L^*$, и по следствию 1 $(\omega') = (f)+(\omega)$. Если ω' пробегает все отличные от нуля дифференциалы, то (ω') пробегает все дивизоры, линейно эквивалентные дивизору (ω).

Определение 7. Класс линейно эквивалентных между собой дивизоров, содержащий дивизор (ω) отличного от нуля дифференциала ω, называется *каноническим классом.*

Обозначим канонический класс W.

Теорема 8. *Имеют место равенства* $l(-W) = \dim_k L(-W) = g$, $\delta(W) = 1$ *и* $\deg W = 2g - 2$.

Доказательство. Покажем сначала, что $l(-(\omega)) = g$. Ввиду теоремы 6 для этого необходимо установить изоморфизм пространств $L(-(\omega))$ и $\Delta(0)$. Докажем, что такой изоморфизм задается посредством сопоставления $f \to f\omega$. Действительно, условие $f \in L(-(\omega))$ равносильно тому, что $f \equiv 0 \pmod{(-(\omega))}$. В свою очередь, последнее условие равносильно условию $(f\omega) = (f)+(\omega) \geqslant 0$, которое, в силу следствия 3, равносильно тому, что $f\omega \in \Delta(0)$.

Покажем теперь, что если ω — отличный от нуля дифференциал, то $\delta((\omega)) = \dim_k \Delta((\omega)) = 1$. В самом деле, поскольку $\omega \in \Delta((\omega))$ и $\omega \neq 0$, то $\delta((\omega)) \geqslant 1$. Далее, если $\omega' = f\omega$, где f — произвольная функция из L, то условие $\omega' = f\omega \in \Delta((\omega))$ равносильно, ввиду следствия 2, тому, что $(\omega) \leqslant (f\omega) = (f)+(\omega)$. Последнее условие равносильно условию $(f) \geqslant 0$, которое, в свою очередь, равносильно условию $f \in k$. Таким образом, $\Delta((\omega)) \simeq k$ и, следовательно, $\delta((\omega)) = \delta(W) = 1$.

Согласно теореме Римана — Роха имеем

$$l(-W) = \deg W - g + 1 + \delta(W),$$

и по доказанному выше

$$l(-W) = l(-(\omega)) = g, \quad \delta(W) = \delta((\omega)) = 1.$$

В таком случае

$$\deg W = 2g - 2,$$

тем самым теорема доказана.

Следствие. *Если* $\deg D > 2g - 2$, *то*

$$l(-D) = \deg D - g + 1.$$

Доказательство. По теореме Римана — Роха имеем $l(-D) = \deg D - g + 1 + \delta(D)$. Покажем, что если $\deg D > 2g - 2$, то $\Delta(D) = 0$. Предположим противное, что $\Delta(D) \neq 0$. Тогда в $\Delta(D)$ найдется отличный от нуля дифференциал ω, и, ввиду следствия 2, $(\omega) \geqslant D$. В таком случае $2g - 2 = \deg(\omega) \geqslant \deg D > 2g - 2$. Получаем противоречие. Значит, $\Delta(D) = 0$ и тогда $\delta(D) = \dim_k \Delta(D) = 0$. Следствие доказано.

Теорема Римана — Роха (третья форма). *Для любого класса* $C \in \mathrm{Cl}(X)$ *справедливо равенство* *)

$$l(-C) = \deg C - g + 1 + l(C - W).$$

Доказательство. Достаточно доказать, что $\delta(D) = l(D-(\omega)) = \dim_k L(D-(\omega))$, где ω — некоторый отличный от нуля дифференциал. Пусть $\omega' = f\omega \in \Delta(D)$. Это эквивалентно тому, что $D \leqslant (f\omega) = (f) + (\omega)$ и, значит, неравенству $(f) + (\omega) - D \geqslant 0$. Но последнее неравенство равносильно условию $f \in L(D-(\omega))$ и, следовательно, сопоставление $f \mapsto f\omega$ задает изоморфизм пространств $\Delta(D)$ и $L(D-(\omega))$. Теорема доказана.

Для всякого класса $C \in \mathrm{Cl}(X)$ обозначим $C^* = W - C$ сопряженный ему класс и положим

$$\rho(C) = l(C) - \frac{1}{2}\deg C.$$

Теорема Римана — Роха (четвертая форма). *Для любого класса* $C \in \mathrm{Cl}(X)$ *имеет место равенство*

$$\rho(C^*) = \rho(C).$$

Доказательство. Имеем

$$\deg C^* = \deg(W - C) = 2g - 2 - \deg C.$$

Поэтому

$$\rho(C^*) = l(-C^*) - g + 1 + \frac{1}{2}\deg C = l(C - W) - g + 1 + \frac{1}{2}\deg C$$

и согласно предыдущей теореме

$$\rho(C^*) = l(-C) - \frac{1}{2}\deg C = \rho(C).$$

Следствие. *Справедливы равенства*

$$l(-C) = \begin{cases} 0, & \text{если } \deg C < 0, \\ 1, & \text{если } C = 0, \\ 0, & \text{если } C \neq 0 \text{ и } \deg C = 0, \\ g-1, & \text{если } C \neq W \text{ и } \deg C = 2g-2, \\ g, & \text{если } C = W. \end{cases}$$

Доказательство. Пусть D — дивизор, лежащий в C. Если $D < 0$, то $l(-C) = 0$. Пусть $\deg C < 0$. Предположим, что $f \in L(-D)$ и $f \neq 0$. Тогда получим, что $(f) + D \geqslant 0$. В таком случае $\deg D \geqslant 0$ и полученное противоречие показывает, что если $\deg C < 0$, то $L(-C) = 0$.

*) Пространство $L(-D)$ и его размерность $l(-D)$ часто обозначаются $L(D)$ и $l(D)$. В этих обозначениях теорема Римана — Роха имеет вид

$$l(C) = \deg C - g + 1 + l(W - C).$$

Пусть $C = 0$. Если $f \in L(-D)$, то $(f) + (0) \geqslant 0$ и тогда $(f) \geqslant 0$. В таком случае $f \in k$ и, значит, $l(-C) = 1$.

Пусть $C \neq 0$ и $\deg C = 0$. Предположим, что $L(-D) \neq 0$. Если $f \in L(-D)$ и $f \neq 0$, то $(f) + D \geqslant 0$. Но поскольку $\deg((f) + D) = 0$, то $(f) + D = 0$ и тогда $D = (f^{-1})$. Отсюда получаем, что $C = 0$ и приходим к противоречию. Таким образом, $L(-D) = 0$ и, значит, $l(-C) = 0$.

Если $C \neq W$ и $\deg C = 2g - 2$, то $W - C \neq 0$ и $\deg(W - C) = 0$. По доказанному выше $l(C - W) = 0$ и тогда, согласно теореме Римана — Роха в третьей форме

$$l(-C) = \deg C - g + 1 = g - 1.$$

Наконец, если $C = W$, то по теореме 8 $l(-C) = g$. Следствие доказано.

Задачи

1. *Дифференцированием поля* K называется всякое его отображение D в себя, удовлетворяющее условиям:

$$D(y + z) = Dy + Dz,$$
$$D(y \cdot z) = yDz + zDy,$$
$$D\left(\frac{y}{z}\right) = \frac{zDy - yDz}{z^2}.$$

Дифференцирование D называется *тривиальным*, если $Dy = 0$ для каждого элемента $y \in K$. Оно называется *тривиальным на подполе* $k \subset K$, если $Dy = 0$ для всех $y \in k$.

Если $F(T)$ — многочлен от неизвестного T с коэффициентами из поля K, то обозначим $F^D(T)$ многочлен, полученный из F применением D ко всем его коэффициентам, а $F'(T)$ — формальную производную многочлена F по переменной T.

Доказать справедливость следующих утверждений:

а) Каждое дифференцирование поля K тривиально на его *простом подполе* (поле, порожденном единицей 1 поля K).

б) Если поле $L = K(z)$ порождено над K элементом z, являющимся корнем многочлена $F(T)$, то для любого элемента $y \in L$, удовлетворяющего соотношению

$$F^D(z) + F'(z)y = 0$$

существует единственное дифференцирование D^* поля L, совпадающее с D на K и такое, что $D^*z = y$.

Дифференцирование D^* называется *продолжением дифференцирования* D на поле L.

в) Дифференцирования D поля K образуют линейное пространство над K, если положить $(D + D')u = Du + D'u$ и $(yD)u = y(Du)$.

г) Каждое дифференцирование D поля $L = k(X)$ рациональных функций на алгебраической кривой X, тривиальное на k, однозначно определяется его заданием на некотором элементе $z \in L$.

(Указание. Воспользоваться тем, что в поле $L = k(X)$ существует элемент z, для которого L является сепарабельным расширением поля $k(z)$ (см. [70d, гл. 10, § 6]), а также результатом п. б).)

д) Все дифференцирования поля $L = k(X)$, тривиальные на k, образуют одномерное линейное пространство Λ над полем L.

е) Спаривание

$$(D, u) \mapsto Du, \quad u \in L = k(X)$$

определяет L-линейный функционал du на пространстве Λ, удовлетворяющий условиям

$$d(y + u) = dy + du,$$
$$d(y \cdot u) = y\,du + u\,dy$$

(здесь $y\,du$ определяется отображением $(D, y\,du) \mapsto y\,Du$).

Пространство L-линейных функционалов du, двойственное к Λ, называется *пространством дифференциальных форм* на алгебраической кривой X и обозначается Ω.

ж) Поле $L = k(X)$ сепарабельно над $k(z)$ в том и только в том случае, если элемент dz порождает пространство Ω. Если поле L сепарабельно над $k(z)$, то каждая дифференциальная форма ω^* на X имеет вид $\omega^* = ydz$, где $y \in L$.

2. Пусть $k((t))$ — *поле формальных степенных рядов*

$$y = \sum_{\nu=n}^{\infty} a_\nu t^\nu, \quad a_n \neq 0,$$

с коэффициентами из алгебраически замкнутого поля k. Зададим дискретное нормирование v поля $k((t))$, положив $v(y) = n$. Число n назовем *порядком* элемента $y \in k((t))$. Всякий элемент $u \in k((t))$ порядка $n = 1$ назовем *локальным параметром* поля $k((t))$. Соотношение

$$D_t y = \sum_{\nu=n}^{\infty} \nu a_\nu t^{\nu-1}$$

определяет дифференцирование поля $k((t))$. Коэффициент a_{-1} ряда $y = \sum a_\nu t^\nu$ называется его *вычетом* относительно локального параметра t и обозначается $\mathrm{Res}_t(y)$.

Доказать справедливость следующих утверждений:

а) Если элемент $y \in k((t))$ имеет вид $y = \sum a_\nu u^\nu$, где $u = \sum b_\nu t^\nu$, то $D_t y = D_u y \cdot D_t u$.

б) Если y, z — два элемента поля $k((t))$ и u — отличный от t локальный параметр, то

$$\mathrm{Res}_u(yD_u z) = \mathrm{Res}_t(yD_t z).$$

в) Если t — ненулевой элемент поля $k((u))$ порядка $e \geqslant 1$, то поле $k((u))$ является алгебраическим расширением поля $k((t))$ степени e.

г) Если t — ненулевой элемент поля $k((u))$ порядка $e \geqslant 1$, то для любого $y \in k((u))$ справедливо соотношение

$$\mathrm{Res}_u(yD_u t) = \mathrm{Res}_t(\mathrm{tr}\, y),$$

где tr — след из поля $k((u))$ в поле $k((t))$.

(Указание. Показать сначала, что доказываемое соотношение является формальным тождеством, не связанным с характеристикой поля k. Поэтому можно считать, что $\mathrm{char}\, k = 0$. В этом случае $t = w^e$, где w — некоторый локальный параметр поля $k((u))$, и тогда, согласно б), достаточно установить равенство

$$\mathrm{Res}_w(yD_w t) = \mathrm{Res}_t(\mathrm{tr}\, y).$$

Ввиду линейности, справедливость последней формулы достаточно проверить для элементов y вида $y = u^s$, $s \in \mathbb{Z}$.)

3. Пусть y, z — элементы поля $k((u))$ и ydz — дифференциальная форма этого поля. Определим *вычет* $\mathrm{Res}\,(ydz)$ *дифференциальной формы* ydz равенством

$$\mathrm{Res}(ydz) = \mathrm{Res}_w(yD_w z),$$

где w — некоторый локальный параметр поля $k((u))$. Показать, что если t — ненулевой элемент из поля $k((u))$ порядка $e \geqslant 1$, то

$$\mathrm{Res}_u(y(D_u t)du) = \mathrm{Res}_t(\mathrm{tr}(y)dt).$$

4. Пусть t — ненулевой элемент порядка $e \geqslant 1$ из поля $k((u))$. Доказать справедливость следующих утверждений:

а) Каждое дискретное нормирование v поля $k((t))$ единственным образом продолжается до дискретного нормирования v^* поля $k((u))$.

б) Для всех отличных от нуля элементов $y \in k((t))$ справедливо соотношение $v^*(y) = ev(y)$.

5. Пусть $L = k(X)$ — поле функций на алгебраической кривой X и t — униформизирующий параметр точки $x \in X$. Доказать справедливость следующих утверждений:

а) Каждый элемент y локального кольца $\mathfrak{o}_x$ точки x имеет единственное разложение в степенной ряд

$$y = \sum_{\nu=0}^{\infty} a_\nu t^\nu, \quad a_\nu \in k.$$

б) Поле L вкладывается в поле формальных степенных рядов $k((t))$. (Указание. Воспользоваться тем, что L изоморфно полю частных кольца $\mathfrak{o}_x$.)

в) Если u — другой униформизирующий параметр точки $x \in X$, то $k((u)) = k((t))$.

6. Пусть y — некоторый элемент поля $L = k(X)$ рациональных функций на кривой X, t — униформизирующий параметр точки $x \in X$ и z — такой элемент поля L, что $dy = zdt$. Доказать, что $z = D_t y$, где D_t — дифференцирование поля формальных степенных рядов $k((t))$.

7*. (Ленг [10e, гл. 1, § 5], Серр [10c, гл. 2, п. 7—13]). Пусть $L = k(X)$ — поле функций на кривой X и z — такой элемент поля L, что L является сепарабельным алгебраическим расширением поля $k(z)$. Каждое каноническое дискретное нормирование v_x поля $k(z)$ имеет конечное число продолжений $v_{x_1}, \ldots, v_{x_r}$ до дискретных нормирований поля L (см. [70d, гл. 12, § 6; 145b, гл. 4, § 1 и 46b, гл. 4, § 33]). Если $t_1, \ldots, t_r$ — униформизирующие параметры точек $x_1, \ldots, x_r$, то t является элементом порядка $e_i \geqslant 1$ и тогда $k((t_i))$ — расширение степени e_i поля $k((t))$. Таким образом, каждая точка $x_i \in X$, $1 \leqslant i \leqslant r$, определяет вложение поля L в конечное расширение поля $k((t))$.

Пусть $\omega^* = ydz$ — дифференциальная форма на X и t_i — униформизирующий параметр точки $x_i \in X$. Определим *вычет* $\mathrm{Res}_{x_i}(\omega^*)$ *дифференциальной формы* ω^* в точке x_i равенством

$$\mathrm{Res}_{x_i}(\omega^*) = \mathrm{Res}_{t_i}\left(yD_{t_i} z\right).$$

Доказать справедливость следующих утверждений:

а) Для всякого $y \in L$ имеет место равенство

$$\mathrm{Res}_x(\mathrm{tr}\,(y)\,dz) = \sum_{i=1}^{r} \mathrm{Res}_{x_i}(ydz),$$

где tr — след из поля L в поле $k(z)$.

б) Для любой дифференциальной формы $\omega^* = y\,dz$ на кривой X выполняется соотношение (*теорема о вычетах*)

$$\sum_{x\in X} \operatorname{Res}_x(\omega^*) = 0.$$

(Указание. Установить сначала справедливость указанного соотношения для поля $k(z)$ и затем воспользоваться результатом п. а).)

8. Пусть t — униформизирующий параметр точки x кривой X и $L_x = k((t))$ — соответствующее полю $L = k(X)$ в точке x поле формальных степенных рядов. Рассмотрим ограниченное прямое произведение

$$A = \prod_{x\in X}{}' L_x$$

полей L_x. Элементами A являются бесконечные векторы $u = (\ldots, u_x, \ldots)$ с компонентами $u_x \in L_x$, удовлетворяющими тому условию, что $v_x(u_x) \geqslant 0$ для почти всех $x \in X$. Операции покомпонентного сложения и умножения превращают A в кольцо. Это кольцо называется *кольцом аделей*. Поле L вкладывается в A посредством отображения $u \mapsto (\ldots, u, \ldots)$. Доказать, что кольцо аделей A изоморфно кольцу распределений R.

9. Пусть $u = (\ldots, u_x, \ldots)$ — *адель* и $\omega^* = y\,dz$ — дифференциальная форма на кривой X. Доказать, что спаривание

$$(u, y\,dz) = \sum_{x\in X} \operatorname{Res}_x(u_x\ y\,dz)$$

определяет дифференциал ω на X.

10. Пусть v_x — каноническое нормирование поля $L = k(X)$ и t — униформизирующий параметр точки x кривой X. Дифференциальная форма $\omega^* = y\,dz$ на X называется *регулярной* в точке x, если $v_x(yD_tz) \geqslant 0$.

Установить изоморфизм между пространством Δ дифференциалов на кривой X и пространством Ω ее дифференциальных форм. Вывести отсюда, что род g кривой X равен размерности над полем k подпространства всюду регулярных на X дифференциальных форм $\omega^* = y\,dz$.

11. Кривая X называется *плоской*, если она задается однородным уравнением

$$F(x_0 : x_1 : x_2) = 0.$$

Доказать, что род g плоской кривой X выражается формулой

$$g = \frac{(n-1)(n-2)}{2},$$

где n — степень кривой X.

(Указание. Установить, что каждая всюду регулярная на X дифференциальная форма ω^*, с точностью до замены $x = x_1/x_0$ на $y = x_2/x_0$, имеет вид

$$\omega^* = \frac{P(x, y)}{F'_y(1, x, y)}\,dx,$$

где P — многочлен степени не выше $n-3$. Затем воспользоваться результатом предыдущей задачи.)

12*. Регулярное отображение $f\colon X \to Y$ кривой X на кривую Y называется *конечным отображением*, а кривая X — *накрытием кривой* Y. Имеем вложение $f^*\colon k(Y) \to k(X)$ поля $k(Y)$ в $k(X)$. Степень $k(X)$ над $k(Y)$ называется *степенью конечного отображения* f и обозначается $\deg f$. Если $k(X)$ — сепарабельное расширение поля $k(Y)$, то отображение f и накрытие X также называются *сепарабельными*. Пусть v_x — каноническое нормирование и t — локальный параметр в точке $y \in Y$. Величину $e_x = v_x(f^*(t))$ назовем *индексом ветвления* отображения f в точке x. Если $e_x > 1$, то говорят, что

отображение f *разветвлено* в точке x. При этом точку $y = f(x)$ называют *точкой ветвления*. Если $e_x = 1$, то говорят, что отображение f *неразветвлено* в точке $x \in X$.

Конечное отображение $f\colon X \to Y$ индуцирует гомоморфизм $f^*\colon \operatorname{Div}(Y) \to \operatorname{Div}(X)$, который определяется следующим образом. Пусть t — униформизирующий параметр точки $y = f(x)$ и v_x — соответствующее точке x нормирование поля $k(X)$. Положим $f^*y = \sum_{\substack{x\in X,\\ f(x)=y}} v_x(f^*(t))\cdot x$. Так как f — конечное отображение, то указанная сумма конечна, и, значит, f^*y — дивизор на X. Этот дивизор не зависит от выбора униформизирующего параметра t. Распространим определение f^* по линейности на все дивизоры кривой Y. Ясно, что f^* сохраняет линейную эквивалентность и, стало быть, индуцирует гомоморфизм $\operatorname{Cl}(Y) \to \operatorname{Cl}(X)$.

Пусть $g(X)$ — род кривой X, $g(Y)$ — род кривой Y и $f : X \to Y$ — конечное сепарабельное отображение степени $\deg f = n$. Доказать, что если $\operatorname{char} k = 0$, или если $\operatorname{char} k = p$ и p не делит ни одно из чисел e_x, то справедлива следующая *формула Гурвица* для рода $g(X)$:

$$2g(X) - 2 = n(2g(Y) - 2) + \sum_{x\in X}(e_x - 1).$$

13. Доказать, что кривая X рациональна в том и только в том случае, когда ее род равен нулю.

14. Показать, что кривая

$$x_2^2x_0 = x_1^3 + ax_1x_0^2 + bx_0^3, \quad 4a^3 + 27b^2 \neq 0,$$

над полем k характеристики $p \neq 2, 3$ имеет род $g = 1$.

15. Доказать, что если кривая X над полем характеристики $p \neq 2, 3$ имеет род $g = 1$, то оно бирационально изоморфна кривой

$$x_2^2x_0 = x_1^3 + ax_1x_0^2 + bx_0^3, \quad 4a^3 + 27b^2 \neq 0.$$

(Указание. Воспользоваться теоремой Римана — Роха.)

16. Пусть X — кривая и $x_1, \ldots, x_r$ — некоторые ее точки. Показать, что существует рациональная функция $f \in k(X)$, имеющая полюсы в каждой из точек x_i и регулярная всюду вне этих точек.

17*. Пусть x — произвольная точка кривой X рода $g \geqslant 1$ и $L_s(X)$ — множество функций $f \in L = k(X)$, имеющих в точке x единственный полюс порядка $s \geqslant 1$. Установить справедливость следующей теоремы Вейерштрасса: *множество* $L_s(x)$ *пусто равно для* g *значений* s, *лежащих в интервале* $1 \leqslant s \leqslant 2g - 1$.

(Указание. Воспользоваться теоремой Римана — Роха.)

ГЛАВА V

ГИПОТЕЗА РИМАНА ДЛЯ КОНГРУЕНЦ-ДЗЕТА-ФУНКЦИИ

§ 1. Дзета-функции алгебраических кривых и многообразий

1. Рациональные точки многообразия. До сих пор мы рассматривали алгебраические многообразия, определенные над алгебраически замкнутым полем k. Для арифметических приложений важны многообразия, определенные над некоторым алгебраически незамкнутым подполем k_0 поля k. Изучим специфику таких многообразий.

Пусть k_0 — подполе поля k. Будем говорить, что точка $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$ *рациональна над* k_0, если $x_i \in k_0$ для всех $i = 1, 2, \ldots, n$. Точка $x = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n$ называется *рациональной над* k_0, если существует такая строка однородных координат $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$, $\lambda \neq 0$, что $\lambda x_i \in k_0$ при всех $i = 0, 1, \ldots, n$. Это эквивалентно тому, что если $x_i \neq 0$, то $x_j/x_i \in k_0$ при всех $j = 0, 1, \ldots, n$. Множество точек многообразия X, рациональных над k_0, назовем множеством k_0-рациональных точек этого многообразия и обозначим $X(k_0)$.

Определение 1. Будем говорить, что многообразие X *определено над полем* $k_0 \subset k$, если идеал $\mathfrak{a}(X)$ этого многообразия обладает базисом, состоящим из многочленов с коэффициентами из k_0.

Пусть $\mathfrak{a}_{k_0}(X) = k_0[T]F_1 + \ldots + k_0[T]\ F_r \subset k_0[T]$ — идеал многообразия X, определенного над k_0, и $\mathfrak{a}(X) = k[T]F_1 + \ldots + k[T]F_r \subset k[T]$ — идеал этого многообразия в кольце $k[T]$. Тогда справедливо соотношение

$$\mathfrak{a}_{k_0}(X) = \mathfrak{a}(X) \cap k_0[T].$$

Отсюда следует, что если σ — автоморфизм поля k над k_0 и x — точка многообразия X, определенного над k_0, то σx является точкой многообразия X.

Пример. Пусть $k_0 = F_q$ — конечное поле из q элементов и $k = \bar{F}_q$ — алгебраическое замыкание поля F_q, являющееся расширением Галуа поля F_q. Если $X \subset \mathbb{A}^n$ — аффинное алгебраическое многообразие, определенное над полем k_0, то автоморфизм $\sigma\colon x \to x^q$ поля k определяет *автоморфизм Фробениуса*

$$\sigma\colon (x_1, \ldots, x_n) \to (x_1^q, \ldots, x_n^q)$$

многообразия X, оставляющий неподвижными все k_0-рациональные точки $(x_1, \ldots, x_n) \in X$. Далее, поле $k' = F_{q^\nu}$ является циклическим расширением поля k_0 степени ν и оно инвариантно относительно σ^ν. Автоморфизмы

$$\sigma^i\colon (x_1, \ldots, x_n) \to (x_1^{q^i}, \ldots, x_n^{q^i}), \quad 1 \leqslant i \leqslant \nu - 1,$$

многообразия X переводят k'-рациональную точку $(x_1, \ldots, x_n) \in X$ в k'-рациональные точки

$$(x_1^q, \ldots, x_n^q), \ldots, (x_1^{q^{\nu-1}}, \ldots, x_n^{q^{\nu-1}}) \in X,$$

и автоморфизм

$$\sigma^\nu\colon (x_1, \ldots, x_n) \to (x_1^{q^\nu}, \ldots, x_n^{q^\nu})$$

оставляет неподвижными все k'-рациональные точки многообразия X.

2. Рациональные дивизоры на кривой. Пусть $k_0 = F_q$ — конечное поле и $k = \bar{F}_q$ — его алгебраическое замыкание. Рассмотрим алгебраическую кривую X, определенную над полем k_0, и обозначим σ автоморфизм Фробениуса поля k над k_0. Образ точки $x \in X$ при автоморфизме σ, обозначим $\sigma(x)$ и заметим, что $\sigma(x) \in X$.

Пусть $k(X)$ — поле рациональных функций на кривой X. Каждая функция $f \in k(X)$ представляется в виде $f = F/G$, где $F, G \in k[T]$ — однородные многочлены одной и той же степени и G не принадлежит идеалу $\mathfrak{a}(X)$ кривой X.

Определение 2. Функция $f \in k(X)$ называется *рациональной* над k_0, если имеется представление $f = F/G$, где $F, G \in k_0[T]$ и $G \notin \mathfrak{a}(X)$.

Поскольку $\mathfrak{a}_{k_0}(X) = \mathfrak{a}(X) \cap k_0[T]$, то многочлен $G \in k_0[T]$ не принадлежит $\mathfrak{a}(X)$ в том и только в том случае, если $G \notin \mathfrak{a}_{k_0}(X)$. Поэтому рациональную над k_0 функцию f можно определить также как функцию, обладающую представлением $f = F/G$, где $F, G \in k_0[T]$ и $G \notin \mathfrak{a}_{k_0}(X)$. При этом считаем, что F/G и F_1/G_1 определяют одну и ту же функцию, если $FG_1 - F_1G = 0$ на X.

Рациональные над k_0 функции на X образуют поле $k_0(X) \subset k(X)$. Каждая функция $f \in k(X)$ может быть представлена в виде

$$f = \sum_{i=1}^{s} \alpha_i f_i,$$

где $\alpha_i \in k$, $f_i \in k_0(X)$ и поэтому $k(X)$ является тензорным произведением

$$k(X) = k_0(X) \otimes_{k_0} k$$

полей $k_0(X)$ и k над полем k_0.

Определение 3. Дивизор $D = \sum_{x \in X} a_x \cdot x$ на кривой X называется *рациональным над* k_0, если $D = \sigma D$, где

$$\sigma D = \sum_{x \in X} a_x \cdot \sigma(x).$$

Множество рациональных над k_0 дивизоров образуют подгруппу $\mathrm{Div}_{k_0}(X)$ группы $\mathrm{Div}(X)$.

Пусть $\mathrm{Gal}(k/k_0)$ — группа Галуа поля k над полем k_0. Введем на кривой X отношение эквивалентности, назвав две точки $x, y \in X$ *эквивалентными* между собой ($x \sim y$) в том и только в том случае, если существует такой элемент $\tau \in \mathrm{Gal}(k/k_0)$, что $y = \tau(x)$.

Каждая точка $x \in X$ однозначно определяет поле $k_0(x)$, порожденное ее координатами. В аффинном случае имеем $k_0(x) = k_0(x_1, \ldots, x_n)$. Пусть $x = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n$ и $x_i \neq 0$. Покажем, что $k_0(x) = k_0(x_0/x_i, x_1/x_i, \ldots, x_n/x_i)$. Действительно, если $x_j \neq 0$ при $j \neq i$, то

$$\frac{x_s}{x_j} = \left(\frac{x_s}{x_i}\right) \Big/ \left(\frac{x_j}{x_i}\right) \in k_0\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

и, значит,

$$k_0\left(\frac{x_0}{x_j}, \frac{x_1}{x_j}, \ldots, \frac{x_n}{x_j}\right) \subset k_0\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

Аналогично,

$$k_0\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right) \subset k_0\left(\frac{x_0}{x_j}, \frac{x_1}{x_j}, \ldots, \frac{x_n}{x_j}\right)$$

и тогда

$$k_0\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right) = k_0\left(\frac{x_0}{x_j}, \frac{x_1}{x_j}, \ldots, \frac{x_n}{x_j}\right).$$

Таким образом, поле $k_0(x)$ определено однозначно и можем считать, что $k_0(x) = k_0(x_1, \ldots, x_n)$, где x_i — *нормированные координаты точки* $x = (1 : x_1 : \ldots : x_n) \in \mathbb{P}^n$.

Ясно, что поле $k_0(x)$ является конечным расширением поля k_0 и, значит, $k_0(x) = F_{q^\nu}$ при некотором целом $\nu \geqslant 1$. Покажем, что класс эквивалентных с x точек кривой X полностью определяется действием на x группы Галуа поля $k_0(x)$.

Предложение 1. *Если* $x \in X$ *и* $k_0(x) = F_{q^\nu}$, *то класс эквивалентных с* x *точек кривой* X *образует множество*

$$\{\sigma^i(x)\}_{0 \leqslant i \leqslant \nu - 1}.$$

Доказательство. Имеем $\sigma^i(x) \sim \sigma^j(x)$ при любых $i, j = 0, 1, \ldots, \nu - 1$. Покажем, что все точки $\sigma^i(x)$, $0 \leqslant i \leqslant \nu - 1$, различны между собой. Допустим, что $\sigma^i(x) = \sigma^j(x)$ при $0 \leqslant i < j \leqslant \nu - 1$. Обозначим $x_1, \ldots, x_n$ нормированные координаты точки x. Тогда $\sigma^{j-i}(x_s) = x_s$ для всех $s = 1, 2, \ldots, n$ и, значит, $x_s \in F_{q^{j-i}}$. В таком случае $F_{q^\nu} \subset F_{q^{j-i}}$, и мы приходим к противоречию.

Покажем теперь, что все эквивалентные с x точки $y \in X$ исчерпываются точками $\sigma^i(x)$, $0 \leqslant i \leqslant \nu - 1$. Пусть точка y эквивалентна точке x. Тогда $y = \tau(x)$, где τ — некоторый автоморфизм поля k над k_0, и достаточно рассмотреть ограничение этого автоморфизма на поле $k_0(x) = F_{q^\nu}$. При таком ограничении τ является автоморфизмом поля F_{q^ν} и, следовательно, $\tau = \sigma^i$ при некотором $i = 0, 1, \ldots, \nu - 1$. Предложение доказано.

Определение 4. *Простым рациональным над* k_0 *дивизором* называется любой дивизор, представимый в виде

$$\mathfrak{p} = \sum_{x \in X}{}' x,$$

где штрих означает, что x по одному разу пробегает все точки некоторого класса эквивалентности.

Данное определение корректно, так как согласно предложению 1 рассматриваемая в нем сумма конечна. Ввиду того же предложения дивизор $\mathfrak{p}$ рационален над k_0. Точки x, входящие в дивизор $\mathfrak{p}$, называются его *компонентами*. Если x — компонента дивизора $\mathfrak{p}$, то он может быть записан в виде

$$\mathfrak{p} = \mathfrak{p}_x = \sum_{i=1}^{\nu} \sigma^{i-1}(x),$$

где $\nu = [k_0(x) : k_0]$ — степень поля $k_0(x)$ над k_0. Поэтому степень $\deg \mathfrak{p}$ дивизора $\mathfrak{p}$ равна $[k_0(x) : k_0]$. Легко видеть, что

$$\mathfrak{p}_x = \mathfrak{p}_y \Leftrightarrow x \sim y.$$

Предложение 2. *Дивизор* $D \in \mathrm{Div}(X)$ *рационален над* k_0 *тогда и только тогда, когда он представляется в виде*

$$D = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \cdot \mathfrak{p}, \quad a_{\mathfrak{p}} \in \mathbb{Z},$$

где почти все $a_{\mathfrak{p}}$ *равны нулю.*

Доказательство. Если дивизор $D = \sum_{x \in X} a_x \cdot x$ рационален над k_0, то при некотором $\nu \geqslant 1$ таком, что $\sigma^\nu(x) = x$ для всех x, входящих в D с ненулевыми a_x, имеем

$$\sum_{x \in X} a_x \cdot x = \sum_{x \in X} a_x \cdot \sigma(x) = \ldots = \sum_{x \in X} a_x \cdot \sigma^{\nu-1}(x).$$

Отсюда следует, что все эквивалентные между собой точки входят в дивизор D с одинаковыми коэффициентами и тогда

$D = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \cdot \mathfrak{p}$. Обратное утверждение очевидно. Предложение доказано.

Пусть x — компонента простого рационального над k_0 дивизора $\mathfrak{p}$. Точка x определяет каноническое нормирование v_x поля $L = k(X)$. Обозначим $v_x|_{L_0}$ ограничение этого нормирования на поле $L_0 = k_0(X)$. Легко видеть, что локальные кольца в L_0 точек $x, y \in X$ совпадают лишь в случае, когда $x \sim y$. Приходим к следующему результату.

Предложение 3. *Для совпадения $v_x|_{L_0}$ и $v_y|_{L_0}$ на поле $L_0 = k_0(X)$ необходимо и достаточно, чтобы точки x и y были эквивалентны между собой.*

Это предложение показывает, что сопоставление $\mathfrak{p} \mapsto v_{\mathfrak{p}} = v_x|_{L_0}$ задает биективное соответствие между простыми рациональными дивизорами над k_0 и нормированиями поля функций $L_0 = k_0(X)$. Заметим, что если $\mathfrak{o}_{\mathfrak{p}} \subset k_0(X)$ — кольцо нормирования $v_{\mathfrak{p}}$ и $\mathfrak{m}_{\mathfrak{p}}$ — максимальный идеал этого кольца, то

$$\mathfrak{o}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} \simeq k_0(x),$$

где x — некоторая компонента дивизора $\mathfrak{p}$.

Предложение 4. *Главный дивизор (f) рационален над k_0 тогда и только тогда, когда $f \in k_0(X)$.*

Доказательство. Пусть дивизор $(f) = \sum_{x \in X} v_x(f) \cdot x$ рационален над k_0 и пусть $f = F/G$, $G \notin \mathfrak{a}(X)$, — некоторое представление функции $f \in k(X)$. Из рациональности дивизора (f) следует, что наряду с точкой x многочлен F (соответственно G) имеет своими нулями все сопряженные над полем k_0 точки $\sigma^i(x)$ и тогда $F, G \in k_0[T]$. Следовательно, $f \in k_0(X)$. Обратное утверждение очевидным образом следует из предложения 2.

Определение 5. Класс дивизоров $C \in \mathrm{Cl}(X)$ называется *рациональным над k_0*, если он содержит хотя бы один рациональный над k_0 дивизор.

Рациональные над k_0 классы дивизоров образуют подгруппу группы $\mathrm{Cl}(X)$. Обозначим ее $\mathrm{Cl}_{k_0}(X)$. Вложение

$$\mathrm{Div}_{k_0}(X) \to \mathrm{Div}(X)$$

индуцирует эпиморфизм

$$\mathrm{Div}_{k_0}(X) \to \mathrm{Cl}_{k_0}(X).$$

Ядром этого эпиморфизма является группа $P_{k_0}(X)$ главных рациональных над k_0 дивизоров и, значит,

$$\mathrm{Cl}_{k_0}(X) \simeq \mathrm{Div}_{k_0}(X)/P_{k_0}(X).$$

Пусть D' — рациональный над k_0 дивизор и $L_0(-D') = L(-D') \cap k_0(X)$ — линейное над полем k_0 пространство. Тогда

$$L(-D') = L_0(-D') \otimes_{k_0} k$$

и, следовательно,

$$\dim_{k_0} L_0(-D') = \dim_k L(-D').$$

Далее, пусть R_0 — линейное над полем k_0 пространство распределений со значениями в $L_0 = k_0(X)$ и Δ_0 — соответствующее ему линейное над k_0 пространство дифференциалов. Имеем

$$R = R_0 \otimes_{k_0} k, \quad \Delta = \Delta_0 \otimes_{k_0} k$$

и, в таком случае,

$$\dim_{L_0} \Delta_0 = \dim_L \Delta = 1.$$

Значит, канонический класс $W \in \mathrm{Cl}(X)$ содержит рациональный над k_0 дивизор (ω') отличного от нуля дифференциала $\omega' \in \Delta_0$ и, стало быть, справедливо следующее утверждение.

Предложение 5. *Канонический класс рационален над k_0.*

Заметим теперь во всех результатах, связанных с теоремой Римана — Роха, дивизоры на рациональные над k_0 дивизоры, классы дивизоров на рациональные над k_0 классы дивизоров и размерности над полем k на размерности над k_0. Тогда эти результаты сохраняются (ср. Дойринг [46b, гл. 2], Шевалле [145b, гл. 2]) и приходим к справедливости следующего утверждения.

Теорема Римана — Роха. *Для всякого рационального над k_0 класса дивизоров C имеет место равенство*

$$\dim_{k_0} L_0(-C) = \deg C - g + 1 + \dim_{k_0} L_0(C - W),$$

которое в симметрической форме записывается в виде

$$\rho(C) = \rho(C^*),$$

где

$$C^* = W - C, \text{ и } \quad \rho(C) = \dim_{k_0} L_0(-C) - \tfrac{1}{2} \deg C.$$

Пусть $\mathrm{Div}^0_{k_0}(X) \subset \mathrm{Div}_{k_0}(X)$ — *группа рациональных над k_0 дивизоров степени нуль* и

$$\mathrm{Cl}^0_{k_0}(X) \simeq \mathrm{Div}^0_{k_0}(X)/P_{k_0}(X)$$

— группа рациональных над k_0 классов дивизоров нулевой степени.

Теорема 1. *Число элементов группы $\mathrm{Cl}^0_{k_0}(X)$ конечно.*

Доказательство. Покажем, прежде всего, что для каждого неотрицательного целого ν имеется лишь конечное число

рациональных над k_0 положительных дивизоров степени ν. Докажем сначала справедливость этого утверждения для простых рациональных над k_0 дивизоров. Пусть x — компонента простого рационального над k_0 дивизора $\mathfrak{p}$ степени ν и $k_0(x) = F_{q^\nu}$. Тогда дивизору $\mathfrak{p}$ соответствует рациональная над полем F_{q^ν} точка x кривой $X \subset \mathbb{P}^n$ и, следовательно, достаточно показать, что на X имеется лишь конечное число таких точек. Без уменьшения общности можно считать, что точка x имеет вид $x = (1 : x_1 : \ldots : x_n)$, где $x_i \in F_{q^\nu}$ — ее нормированные координаты. Число таких точек не больше чем $q^{\nu n}$ и, значит, общее число точек x, рациональных над F_{q^ν} не превосходит величины $(n+1)q^{\nu n}$. Таким образом, число простых рациональных над k_0 дивизоров $\mathfrak{p}$ степени ν конечно.

Пусть теперь $D = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \cdot \mathfrak{p}$ — произвольный рациональный над k_0 положительный дивизор степени ν. Имеем

$$\deg D = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \deg \mathfrak{p} = \nu$$

и, значит, число таких дивизоров не превосходит количества решений в неотрицательных целых $a_{\mathfrak{p}}$, $\deg \mathfrak{p}$ уравнения

$$\sum_{\mathfrak{p}} a_{\mathfrak{p}} \deg \mathfrak{p} = \nu.$$

Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ — все простые рациональные над k_0 дивизоры степени не выше ν и пусть $\deg \mathfrak{p}_i = \nu_i$, $a_{\mathfrak{p}_i} = a_i$. Тогда задача сводится к вопросу о числе решений в неотрицательных целых a_i уравнения

$$\sum_{i=1}^{s} a_i \nu_i = \nu.$$

Но число таких решений не превосходит величины $(\nu+1)s$ и, следовательно, число рациональных над k_0 положительных дивизоров степени ν конечно.

Установим, наконец, конечность группы $\mathrm{Cl}^0_{k_0}(X)$. Рассмотрим некоторую непостоянную функцию $g \in k_0(X)$ и положим $f = g^s$, где s — достаточно большое положительное целое число. Поскольку $g \neq \mathrm{const}$, то $\deg(g)_0 > 0$ и тогда $\deg(f)_0 = s\deg(g)_0 = \nu \geqslant 2g$. Зафиксируем f, ν и докажем, что каждый рациональный над k_0 дивизор нулевой степени линейно эквивалентен разности двух рациональных над k_0 положительных дивизоров степени ν. Так как по доказанному выше число рациональных над k_0 положительных дивизоров степени ν конечно, отсюда будет следовать, что число рациональных над k_0 классов дивизоров нулевой степени также конечно. Пусть $D \in \mathrm{Div}^0_{k_0}(X)$. По теореме Римана — Роха

$$\dim_{k_0} L_0(D - (f)_0) \geqslant \deg(f)_0 - g + 1 \geqslant g + 1 \geqslant 1$$

и, значит, существует такая ненулевая функция $u \in k_0(X)$, что $(u) + (f)_0 - D \geqslant 0$. Положим $D' = (f)_0$ и $D'' = (u) + (f)_0 - D$. Дивизоры D', D'' являются рациональными над k_0 положительными дивизорами одной и той же степени ν. Из соотношения $D = D' - D'' + (u)$ следует, что дивизор D линейно эквивалентен разности $D' - D''$. Тем самым теорема доказана.

Обозначим h число элементов группы $\mathrm{Cl}^0_{k_0}(X)$.

Предложение 6. *Если род g кривой X* равен нулю, то $h = 1$.

Доказательство. Достаточно установить, что при $g = 0$ каждый дивизор D степени нуль является главным дивизором. Если $\deg D = 0$, то по теореме Римана $\dim_k L(D) \geqslant 1$ и, значит, существует такая отличная от нуля функция f, что $(f) \geqslant D$. Степень положительного дивизора $(f) - D$ равна нулю и, следовательно, $D = (f)$. Предложение доказано.

Обозначим $e \geqslant 1$ наименьшую из степеней всех строго положительных рациональных над k_0 дивизоров и заметим, что степень каждого рационального над k_0 дивизора D имеет вид $\deg D = me$ при некотором $m \in \mathbb{Z}$.

Предложение 7. *Пусть $C_1, \ldots, C_h$ — все рациональные над k_0 классы дивизоров нулевой степени и C_0 — фиксированный рациональный класс степени e. Тогда каждый рациональный над k_0 класс дивизоров C степени νe однозначно представляется в виде $C = \nu C_0 + C_i$, где i — одно из чисел $1, 2, \ldots, h$. В частности, имеется в точности h рациональных над k_0 дивизоров степени νe.*

Доказательство. Поскольку степень всякого рационального над k_0 дивизора кратна e, то степень каждого рационального над k_0 класса дивизоров имеет вид νe при некотором целом ν. Пусть C — произвольный рациональный над k_0 класс дивизоров степени νe. Класс νC_0 также имеет степень νe и, значит, разность $C - \nu C_0$ представляет собой рациональный над k_0 класс степени нуль. В таком случае $C = \nu C_0 + C_i$ при некотором $i = 1, 2, \ldots, h$ и предложение, тем самым, доказано.

Для каждого рационального над k_0 класса дивизоров C положим

$$l_0(-C) = \dim_{k_0} L_0(-C).$$

Теорема 2. *Число $n(C)$ различных рациональных над k_0 положительных дивизоров, лежащих в рациональном над k_0*

классе C, выражается формулой

$$n(C) = \frac{q^{l_0(-C)} - 1}{q - 1}.$$

Доказательство. Пусть $D_0 \in C$ — рациональный над k_0 дивизор. Рассмотрим пространство $L_0(-D_0)$, и каждой отличной от нуля функции $f \in L_0(-D_0)$ сопоставим рациональный над k_0 положительный дивизор $D = D_0 + (f)$ из C.

Обратно, пусть $D \in C$ — рациональный над k_0 положительный дивизор. Тогда существует такая отличная от нуля функция $f \in L_0(-D_0)$, что $D = D_0 + (f)$.

Таким образом, сопоставление $f \mapsto D = D_0 + (f)$ определяет отображение множества всех отличных от нуля функций пространства $L_0(-D_0)$ на множество всех рациональных над k_0 положительных дивизоров класса C. Если $D = D_0 + (f) = D_0 + (g)$, то $(f) = (g)$ и, значит, $f = \alpha g$, где $\alpha \in k_0^*$. Стало быть, если $|L_0(-D_0)|$ — число элементов пространства $L_0(-D_0)$, то

$$n(C) = \frac{|L_0(-D_0)| - 1}{q - 1},$$

а так как $|L_0(-D_0)| = q^{l_0(-C)}$, то

$$n(C) = \frac{q^{l_0(-C)} - 1}{q - 1}.$$

Теорема доказана.

3. Дзета-функция кривой. Введем в рассмотрение дзета-функцию алгебраической кривой X, определенной над полем k_0.

Определение 6. *Дзета-функцией алгебраической кривой X* называется функция комплексного переменного $s = \sigma + i\tau$, задаваемая рядом

$$\zeta(X, s) = \sum_D (ND)^{-s},$$

где D пробегает все рациональные над k_0 положительные дивизоры кривой X и $ND = q^{\deg D}$.

Заметим, что если $D = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \cdot \mathfrak{p}$, то

$$ND = q^{\sum a_{\mathfrak{p}} \deg \mathfrak{p}} = \prod_{\mathfrak{p}} (q^{\deg \mathfrak{p}})^{a_{\mathfrak{p}}} = \prod_{\mathfrak{p}} (N_{\mathfrak{p}})^{a_{\mathfrak{p}}},$$

и если x — компонента простого рационального над k_0 дивизора $\mathfrak{p}$, то

$$N_{\mathfrak{p}} = q^{[k_0(x):\, k_0]}.$$

Теорема 3. *Пусть e — наименьшая из степеней всех строго положительных рациональных над полем k_0 дивизоров. Ряд*

$$\zeta(X, s) = \sum_D (ND)^{-s}, \quad s = \sigma + i\tau,$$

абсолютно сходится в области $\sigma > 1$ и представляет в этой области рациональную функцию вида

$$\zeta(X, s) = F(q^{-s}) + \frac{hq^{1-g}q^{(1-s)\max(0,\,2g-2+e)}}{(q-1)(1-q^{e(1-s)})} - \frac{h}{(q-1)(1-q^{-es})},$$

где $F(q^{-s})$ — многочлен от q^{-s} степени не выше $2g-2$.

Доказательство. Прежде всего заметим, что из теоремы Римана — Роха вытекает справедливость следующих соотношений:

$$l_0(-C) = \begin{cases} 0, & \text{если } \deg C > 0, \\ 1, & \text{если } C = 0, \\ 0, & \text{если } C \neq 0 \text{ и } \deg C = 0, \\ g-1, & \text{если } C \neq W \text{ и } \deg C = 2g-2, \\ g, & \text{если } C = W, \\ \deg C - g + 1, & \text{если } \deg C > 2g-2. \end{cases}$$

Далее, поскольку $\deg W = ve = 2g-2$, то $(2g-2)/e$ при $g \geqslant 1$ является целым числом.

Имеем

$$\zeta(X, s) = \sum_D (ND)^{-s} = \sum_C \sum_{D \in C} (ND)^{-s} = \sum_C \sum_{D \in C} q^{-s\deg D} = \sum_C n(C)\, q^{-s\deg C}$$

и, следовательно, ввиду теоремы 2

$$\zeta(X, s) = \sum_C q^{-s\deg C} \frac{q^{l_0(-C)} - 1}{q-1} = \frac{1}{q-1} \sum_{\deg C \geqslant 0} \left(q^{l_0(-C) - s\deg C} - q^{-s\deg C}\right) = \frac{1}{q-1} \sum_{\deg C \geqslant 0} q^{l_0(-C) - s\deg C} - \frac{1}{q-1} \sum_{\deg C \geqslant 0} q^{-s\deg C}.$$

Если $\sigma > 1$, то

$$\sum_{\deg C \geqslant 0} q^{-s\deg C} = \sum_{\nu=0}^{\infty} \sum_{\deg C = \nu e} q^{-s\deg C} = h \sum_{\nu=0}^{\infty} q^{-e\nu s} = \frac{h}{1 - q^{-es}},$$

и тогда

$$\zeta(X, s) = \frac{1}{q-1} \sum_{\deg C \geqslant 0} q^{l_0(-C) - s\deg C} - \frac{h}{(q-1)(1-q^{-es})}.$$

При $g=0$ каждый класс C, для которого $\deg C \geqslant 0$ удовлетворяет условию $\deg C > 2g-2$. Кроме того, ввиду предложения 6 имеем $h=1$ и, значит, в этом случае

$$\zeta(X,s) = \frac{1}{q-1}\sum_{\nu=0}^{\infty}\sum_{\deg C=\nu e} q^{\deg C+1-s\deg C} - \frac{1}{(q-1)(1-q^{-es})} =$$

$$= \frac{q}{q-1}\sum_{\nu=0}^{\infty} q^{e(1-s)\nu} - \frac{1}{(q-1)(1-q^{-es})} =$$

$$= \frac{q}{(q-1)(1-q^{e(1-s)})} - \frac{1}{(q-1)(1-q^{-es})}.$$

Пусть теперь $g \geqslant 1$. Тогда

$$\zeta(X,s) = \frac{1}{q-1}\sum_{0\leqslant \deg C\leqslant 2g-2} q^{l_0(-C)-s\deg C} +$$

$$+ \frac{1}{q-1}\sum_{\deg C>2g-2} q^{l_0(-C)-s\deg C} - \frac{h}{(q-1)(1-q^{-es})} =$$

$$= \frac{1}{q-1}\sum_{\nu=0}^{\frac{2g-2}{e}} q^{-es\nu}\sum_{j=1}^{h} q^{l_0\left(-C_j^{(\nu e)}\right)} +$$

$$+ \frac{h}{q-1}\sum_{\nu=\frac{2g-2}{e}+1}^{\infty} q^{e(1-s)\nu-g+1} - \frac{h}{(q-1)(1-q^{-es})},$$

где $C_j^{(\nu e)}$ — рациональный над k_0 класс дивизоров степени νe, и значит

$$\zeta(X,s) = F\left(q^{-s}\right) + \frac{hq^{1-g}q^{(1-s)(2g-2+e)}}{(q-1)(1-q^{e(1-s)})} - \frac{h}{(q-1)(1-q^{-es})}.$$

Многочлен $F(q^{-s})$ имеет вид

$$F\left(q^{-s}\right) = \frac{1}{q-1}\sum_{\nu=0}^{\frac{2g-2}{e}} q^{-es\nu}\sum_{j=1}^{h} q^{l_0\left(-C_j^{(\nu e)}\right)}$$

и, следовательно, является многочленом от q^{-s} степени не выше $2g-2$. Теорема доказана.

Из теоремы 3 следует, что $\zeta(X, s)$ аналитически продолжается до мероморфной на всей комплексной плоскости $\mathbb{C}$ функции, имеющей полюсы первого порядка в точках

$$s_\mu = \frac{2\pi i}{e\log q}\mu \text{ и } \quad s_m = 1 - \frac{2\pi i}{e\log q}m, \quad \mu, m \in \mathbb{Z}.$$

Теорема 4. *При $\sigma > 1$ имеет место равенство*

$$\zeta(X,s) = \prod_{\mathfrak{p}}\left(1-(N\mathfrak{p})^{-s}\right)^{-1},$$

где $\mathfrak{p}$ — пробегает все простые рациональные над k_0 дивизоры кривой X.

Доказательство. Пусть $M \geqslant 1$ — целое число и $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ — все простые рациональные над k_0 дивизоры с условием $\deg \mathfrak{p}_j \leqslant M$. Положим

$$\prod_M = \prod_{j=1}^{m}\left(1-(N\mathfrak{p}_j)^{-s}\right)^{-1}.$$

Если $\sigma > 1$, то

$$\left(1-(N\mathfrak{p}_j)^{-s}\right)^{-1} = \sum_{\nu_j=0}^{\infty}(N\mathfrak{p}_j)^{-\nu_j s}$$

и тогда

$$\prod_M = \prod_{j=1}^{m}\left(\sum_{\nu_j=0}^{\infty}(N\mathfrak{p}_j)^{-\nu_j s}\right) =$$

$$= \sum_{\nu_1,\ldots,\nu_m=0}^{\infty}\frac{1}{(N\mathfrak{p}_1)^{\nu_1 s}\ldots(N\mathfrak{p}_m)^{\nu_m s}} = \sum_{D'}(ND')^{-s},$$

где D' — рациональные над k_0 дивизоры, имеющие в своем разложении лишь простые дивизоры $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$:

$$D' = \nu_1\mathfrak{p}_1 + \ldots + \nu_m\mathfrak{p}_m.$$

Устремляя M к бесконечности, приходим к равенству

$$\prod_{\mathfrak{p}}\left(1-(N\mathfrak{p})^{-s}\right)^{-1} = \sum_{D}(ND)^{-s} = \zeta(X,s).$$

Теорема доказана.

Предложение 8. *Существует рациональный над k_0 класс дивизоров степени 1.*

Доказательство. Пусть e — наименьшая степень всех рациональных над k_0 строго положительных дивизоров. Тогда для доказательства теоремы достаточно показать, что $e=1$.

Рассмотрим поле $k_0' = F_{q^e}$, являющееся расширением поля k_0 степени $e \geqslant 1$. Если $\mathfrak{p}$ — произвольный простой рациональный над k_0 дивизор степени ν, то он представляется в виде

$$\mathfrak{p} = \sum_{i=1}^{\nu}\sigma^{i-1}(x),$$

где x — некоторая F_{q^ν} — рациональная точка кривой X. Поскольку

ку $e|\nu$, то при переходе от поля k_0 к полю k_0' класс эквивалентности

$$\{\sigma^{i-1}(x)\}_{1\leqslant i\leqslant \nu}$$

над полем k_0 распадается на $e=(\nu,\ e)$ классов эквивалентности

$$\{\sigma^{e(i-1)+j-1}(x)\}_{1\leqslant i\leqslant \nu/e},\quad 1\leqslant j\leqslant e,$$

над полем k_0' и, значит, простой рациональный над k_0 дивизор $\mathfrak{p}$ распадается на e простых рациональных над k_0' дивизоров $\mathfrak{p}_1', \ldots, \mathfrak{p}_e'$, соответствующих указанным классам эквивалентности над k_0'. Пусть

$$\zeta'(X,s)=\prod_{\mathfrak{p}'}(1-(N\mathfrak{p}')^{-s})^{-1}$$

— дзета-функция кривой X над полем k_0'. Имеем

$$\zeta'(X,s)=\prod_{\mathfrak{p}'}(1-q^{-se\deg\mathfrak{p}'})^{-1}=\prod_{j=1}^{e}\left(\prod_{\mathfrak{p}_j'}\left(1-q^{-se\deg\mathfrak{p}_j'}\right)^{-1}\right)$$

и, так как $e\deg\mathfrak{p}_j'=\deg\mathfrak{p}$,

$$\zeta'(X,s)=\prod_{j=1}^{e}\left(\prod_{\mathfrak{p}_j}(1-q^{-s\deg\mathfrak{p}})^{-1}\right.=\left.(\zeta(X,s)\right)^{e}.$$

По теореме 3 функции $\zeta'(X,\ s)$ и $\zeta(X,\ s)$ имеют при $s=1$ полюс одного и того же порядка, равного 1, и тогда из последнего соотношения следует, что $e=1$. Предложение доказано.

Теперь, после того, как показали, что $e=1$, можно уточнить результат теоремы 3.

Предложение 9. *Дзета-функция $\zeta(X,\ s)$ представляет собой рациональную функцию от q^{-s} вида*

$$\zeta(X,s)=\frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

где

$$P(q^{-s})=\sum_{j=0}^{2g}\sigma_j q^{-js}$$

и $\sigma_0=1$, $\sigma_{2g}=q^g$.

Доказательство. При $g=0$ имеем

$$\zeta(X,s)=\frac{q}{(q-1)(1-q^{1-s})}-\frac{1}{(q-1)(1-q^{-s})}=\frac{1}{(1-q^{-s})(1-q^{1-s})}.$$

Пусть теперь $g=1$. Тогда

$$\zeta(X,s)=$$
$$=\frac{1}{q-1}\sum_{\deg C=0}q^{l_0(-C)-s\deg C}+\frac{hq^{1-s}}{(q-1)(1-q^{1-s})}-\frac{h}{(q-1)(1-q^{-s})}=$$
$$=\frac{h-1}{q-1}+\frac{q}{q-1}+\frac{hq^{1-s}}{(q-1)(1-q^{1-s})}-\frac{h}{(q-1)(1-q^{-s})}=$$
$$=\frac{1+(h-q-1)q^{-s}+q\cdot q^{-2s}}{(1-q^{1-s})(1-q^{-s})}.$$

Наконец, если $g\geqslant 2$, то

$$\zeta(X,s)=\frac{1}{q-1}\sum_{\deg C=0}q^{l_0(-C)-s\deg C}+$$
$$+\frac{1}{q-1}\sum_{1\leqslant\deg C\leqslant 2g-3}q^{l_0(-C)-s\deg C}+\frac{1}{q-1}\sum_{\deg C=2g-2}q^{l_0(-C)-s\deg C}+$$
$$+\frac{hq^{1-g}q^{(1-s)(2g-1)}}{(q-1)(1-q^{1-s})}-\frac{h}{(q-1)(1-q^{-s})}=$$
$$=\frac{h+q-1}{q-1}+\frac{1}{q-1}\sum_{1\leqslant\deg C\leqslant 2g-3}q^{l_0(-C)-s\deg C}+$$
$$+\frac{(h-1)q^{g-1-s(2g-2)}+q^{g-s(2g-2)}}{q-1}+\frac{hq^{1-g}q^{(1-s)(2g-1)}}{(q-1)(1-q^{1-s})}-\frac{h}{(q-1)(1-q^{-s})}=$$
$$=\frac{1}{q-1}\sum_{j=1}^{2g-3}\alpha_j q^{-sj}+\frac{(h+q-1)(q^{g-1}q^{-2(g-1)s}+1)}{q-1}+$$
$$+\frac{hq^g q^{-(2g-1)s}}{(q-1)(1-q^{1-s})}-\frac{h}{(q-1)(1-q^{-s})}=$$
$$=\frac{1+\sigma_1 q^{-s}+\ldots+\sigma_{2g-1}q^{-(2g-1)s}+q^g q^{-2gs}}{(1-q^{-s})(1-q^{1-s})}.$$

Предложение доказано.

Теорема 5. *Дзета-функция $\zeta(X,\ s)$ удовлетворяет уравнению*

$$q^{(g-1)(2s-1)}\zeta(X,\ s)=\zeta(X,\ 1-s).$$

Доказательство. При $g=0$ имеем

$$\zeta(X,1-s)=\frac{1}{(1-q^s)(1-q^{s-1})}=q^{1-2s}\zeta(X,s).$$

Пусть теперь $g=1$. Тогда

$$\zeta(X,1-s)=\frac{1+(h-q-1)q^{s-1}+q\cdot q^{2s-2}}{(1-q^s)(1-q^{s-1})}=\zeta(X,s).$$

Пусть, наконец, $g\geqslant 2$. Запишем $\zeta(X,\ s)$ в виде

$$\zeta(X,\ s)=\zeta_1(X,\ s)+\zeta_2(X,\ s),$$

где

$$\zeta_1(X, s) = \frac{1}{q-1} \sum_{1 \leqslant \deg C \leqslant 2g-3} q^{l_0(-C) - s \deg C}$$

и

$$\zeta_2(X, s) = 1 + q^{-(g-1)(2s-1)} + \\ + \frac{h}{q-1}\left(1 + q^{-(g-1)(2s-1)} + \frac{q^g q^{-(2g-1)s}}{1-q^{1-s}} - \frac{1}{1-q^{-s}}\right).$$

Имеем

$$\zeta_2(X, 1-s) = \\ = 1 + q^{(g-1)(2s-1)} + \frac{h}{q-1}\left(1 + q^{(g-1)(2s-1)} + \frac{q^g q^{(2g-1)(s-1)}}{1-q^s} - \frac{1}{1-q^{s-1}}\right) = \\ = q^{(g-1)(2s-1)} \zeta_2(X, s)$$

и, значит, достаточно показать, что

$$\zeta_1(X, 1-s) = q^{(g-1)(2s-1)} \zeta_1(X, s).$$

Положим

$$\rho(C) = l_0(-C) - \frac{1}{2} \deg C.$$

Тогда

$$\zeta_1(X, s) = \frac{1}{q-1} \sum_{1 \leqslant \deg C \leqslant 2g-3} q^{l_0(-C) - s \deg C} = \\ = \frac{1}{q-1} \sum_{1 \leqslant \deg C \leqslant 2g-3} q^{\rho(C) - \left(s - \frac{1}{2}\right) \deg C}$$

и по теореме Римана — Роха

$$\rho(C) = \rho(W - C).$$

Заметим, что, когда C пробегает классы дивизоров с условием

$$1 \leqslant \deg C \leqslant 2g-3,$$

$W - C$ пробегает те же классы, только в обратном порядке. В таком случае

$$\zeta_1(X, s) = \frac{1}{q-1} \sum_{1 \leqslant \deg C \leqslant 2g-3} q^{\rho(C) - \left(s - \frac{1}{2}\right) \deg C} = \\ = \frac{1}{q-1} \sum_{1 \leqslant \deg(W-C) \leqslant 2g-3} q^{\rho(W-C) - \left(s - \frac{1}{2}\right)(2g-2-\deg C)} = \\ = \frac{1}{q-1} \sum_{1 \leqslant \deg C \leqslant 2g-3} q^{\rho(C) - \left(s - \frac{1}{2}\right)(2g-2-\deg C)}$$

и, следовательно,

$$\zeta_1(X, 1-s) = \frac{1}{q-1} \sum_{1 \leqslant \deg C \leqslant 2g-3} q^{\rho(C) - \left(\frac{1}{2} - s\right) \deg C} = \\ = q^{(g-1)(2s-1)} \left(\frac{1}{q-1} \sum_{1 \leqslant \deg C \leqslant 2g-3} q^{\rho(C) - \left(s - \frac{1}{2}\right)(2g-2-\deg C)}\right) = \\ = q^{(g-1)(2s-1)} \zeta_1(X, s).$$

Теорема доказана.

Положим $q^{-s} = t$ и $\zeta(X, s) = Z(X, t)$.

Теорема 6. *В круге $|t| < q^{-1}$ имеет место равенство*

$$Z(X, t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{N_{q^\nu}}{\nu} t^\nu\right),$$

где N_{q^ν} — число F_{q^ν}-рациональных точек кривой X.

Доказательство. Прежде всего заметим, что условие $|t| < q^{-1}$ равносильно условию $\sigma > 1$. При $\sigma > 1$ имеем

$$\zeta(X, s) = \prod_{\mathfrak{p}} (1 - (N\mathfrak{p})^{-s})^{-1} = \\ = \prod_{\mathfrak{p}} (1 - q^{-s \deg \mathfrak{p}})^{-1} = \prod_{\mathfrak{p}} (1 - t^{\deg \mathfrak{p}})^{-1} = Z(X, t)$$

и тогда

$$\log Z(X, t) = -\sum_{\mathfrak{p}} \log(1 - t^{\deg \mathfrak{p}}) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{t^{m \deg \mathfrak{p}}}{m} = \\ = \sum_{\nu=1}^{\infty} \left(\sum_{m \deg \mathfrak{p} = \nu} \frac{1}{m}\right) t^\nu = \sum_{\nu=1}^{\infty} \left(\sum_{\deg \mathfrak{p} \mid \nu} \deg \mathfrak{p}\right) \frac{t^\nu}{\nu}.$$

Положим

$$N_\nu^* = \sum_{\deg \mathfrak{p} \mid \nu} \deg \mathfrak{p}.$$

В таком случае

$$Z(X, t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{N_\nu^*}{\nu} t^\nu\right)$$

и, стало быть, для доказательства теоремы достаточно показать, что

$$N_\nu^* = \sum_{\deg \mathfrak{p} \mid \nu} \deg \mathfrak{p} = N_{q^\nu}.$$

Рассмотрим множество $\mathfrak{N}_\nu$ всех F_{q^ν}-рациональных точек кривой X. Это множество разбивается на классы эквивалентных между собой точек, образующие простые рациональные над k_0 дивизоры $\mathfrak{p}$. Поэтому

$$N_{q^\nu} = \sum_{\mathfrak{p}}{}' \deg \mathfrak{p},$$

где штрих означает, что сумма берется по всем указанным классам эквивалентности множества $\mathfrak{N}_\nu$.

Покажем, что простой рациональный над k_0 дивизор $\mathfrak{p}$ представляется одним из рассматриваемых нами классов в том и только в том случае, когда $\deg \mathfrak{p} | \nu$. Действительно, пусть $\mathfrak{p}$ соответствует одному из классов эквивалентности и пусть x — компонента дивизора $\mathfrak{p}$. Имеем $[k_0(x) : k_0] = \deg \mathfrak{p}$, и, так как x — рациональная над F_{q^ν} точка, $k_0(x) \subset F_{q^\nu}$. В таком случае

$$k_0 \subset k_0(x) \subset F_{q^\nu}$$

и, следовательно, $\deg \mathfrak{p} | \nu$.

Обратно, пусть $\deg \mathfrak{p} | \nu$. Если x — компонента простого рационального над k_0 дивизора $\mathfrak{p}$, то условие $\deg \mathfrak{p} | \nu$ означает, что $[k_0(x) : k_0]$ делит $[F_{q^\nu} : k_0]$ и, значит,

$$k_0 \subset k_0(x) \subset F_{q^\nu}.$$

Стало быть, точка $x \in X$ рациональна над полем F_{q^ν} и, следовательно, дивизор $\mathfrak{p}$ соответствует одному из классов эквивалентности множества $\mathfrak{N}_\nu$.

Из сказанного следует, что $N_\nu^* = N_{q^\nu}$ и тем самым теорема доказана.

Согласно предложению 9 функция $Z(X, t)$ имеет вид

$$Z(X, t) = \frac{P(t)}{(1-t)(1-qt)},$$

где

$$P(t) = 1 + \sum_{j=1}^{2g-1} \sigma_j t^j + q^g t^{2g}, \quad \sigma_j \in \mathbb{Q}.$$

Пусть

$$P(t) = \prod_{i=1}^{2g} (1 - \omega_i t)$$

— разложение многочлена $P(t)$ на линейные множители в некотором конечном расширении поля рациональных чисел $\mathbb{Q}$.

Теорема 7. *Для числа N_{q^ν} рациональных над полем F_{q^ν} точек кривой X рода g справедлива формула*

$$N_{q^\nu} = q^\nu + 1 - \sum_{i=1}^{2g} \omega_i^\nu.$$

Доказательство. Имеем

$$Z(X, t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{N_{q^\nu}}{\nu} t^\nu\right) = \frac{\prod_{i=1}^{2g}(1-\omega_i t)}{(1-t)(1-qt)}$$

и тогда

$$\sum_{\nu=1}^{\infty} \frac{N_{q^\nu}}{\nu} t^\nu = \sum_{i=1}^{2g} \log(1-\omega_i t) - \log(1-t) - \log(1-qt) =$$

$$= \sum_{\nu=1}^{\infty} \frac{1}{\nu} \left(q^\nu + 1 - \sum_{i=1}^{2g} \omega_i^\nu\right) t^\nu.$$

Сравнивая коэффициенты при одинаковых степенях переменной t, получаем

$$N_{q^\nu} = q^\nu + 1 - \sum_{i=1}^{2g} \omega_i^\nu.$$

Теорема доказана.

По аналогии с дзета-функцией $\zeta(X, s)$ можно рассмотреть L-функцию Артина кривой X, определенной над конечным полем $k_0 = F_q$. Для этого обозначим χ характер конечного порядка группы $\mathrm{Cl}_{k_0}(X)$ (гомоморфизм группы $\mathrm{Cl}_{k_0}(X)$ в мультипликативную группу $\mathbb{C}^*$ поля комплексных чисел $\mathbb{C}$, удовлетворяющий тому условию, что $\chi^m(C) = 1$ при некотором целом $m \geqslant 1$ для всех $C \in \mathrm{Cl}_{k_0}(X)$. Распространим характер χ на группу $\mathrm{Div}_{k_0}(X)$, положив

$$\chi(D) = \chi\left(D + P_{k_0}(X)\right)$$

для каждого дивизора $D \in \mathrm{Div}_{k_0}(X)$, и определим L-функцию Артина комплексного переменного $s = \sigma + i\tau$ в виде ряда

$$L(X, \chi, s) = \sum_D \chi(D)(ND)^{-s},$$

где D пробегает все рациональные над k_0 положительные дивизоры кривой X. Этот ряд абсолютно сходится при $\sigma > 1$, и при таких σ справедливо равенство

$$L(X, \chi, s) = \prod_{\mathfrak{p}} \left(1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s}\right)^{-1},$$

где $\mathfrak{p}$ пробегает все простые рациональные над k_0 дивизоры кривой X.

Покажем, что если характер χ не тривиален на группе $\mathrm{Cl}_{k_0}^0(X)$, то L-функция $L(X, \chi, s)$ является многочленом от q^{-s}

степени $2g-2$. Действительно, представляя каждый класс $C \in \mathrm{Cl}_{k_0}(X)$ в виде

$$C = C' + \nu C_0,$$

где $C' \in \mathrm{Cl}^0_{k_0}(X)$ и C_0 — фиксированный рациональный над k_0 класс дивизоров степени 1, получаем

$$L(X, \chi, s) = \sum_{\deg C \geqslant 0} \chi(C) q^{-s \deg C} \frac{q^{l_0(-C)} - 1}{q-1} =$$

$$= \frac{1}{q-1} \sum_{C'} \chi(C') \sum_{\nu=0}^{\infty} \chi^\nu(C_0) \left(q^{l_0(-C'-\nu C_0)} - 1\right) q^{-\nu s} =$$

$$= \frac{1}{q-1} \sum_{C'} \chi(C') \sum_{\nu=0}^{2g-2} \chi^\nu(C_0) \left(q^{l_0(-C'-\nu C_0)} - 1\right) q^{-\nu s} +$$

$$+ \frac{1}{q-1} \sum_{C'} \chi(C') \sum_{\nu=2g-1}^{\infty} \chi^\nu(C_0) \left(q^{\nu-g+1} - 1\right) q^{-\nu s}.$$

Поскольку характер χ не тривиален на $\mathrm{Cl}^0_{k_0}(X)$, то (см. п. 1 § 3 гл. I)

$$\sum_{C'} \chi(C') = 0$$

и тогда

$$L(X, \chi, s) = \sum_{\nu=0}^{2g-2} \sigma_\nu q^{-\nu s},$$

где

$$\sigma_\nu = \frac{1}{q-1} \sum_{C'} \chi(C' + \nu C_0) \left(q^{l_0(-C'-\nu C_0)} - 1\right).$$

Пусть W — канонический класс группы $\mathrm{Cl}(X)$. Имеем

$$l_0(-C'-W) = \begin{cases} g-1, & \text{если } C' \neq 0, \\ g, & \text{если } C' = 0, \end{cases}$$

и, стало быть,

$$\sigma_{2g-2} = \frac{1}{q-1} \sum_{C'} \chi(C' + W) \left(q^{l_0(-C'-W)} - 1\right) =$$

$$= \frac{\chi(W)}{q-1} \left(\sum_{C' \neq 0} \chi(C') q^{g-1} + q^g \right) = \chi(W) q^{g-1} \neq 0.$$

Покажем, наконец, что для любого характера χ конечного порядка L-функция Артина $L(X, \chi, s)$ удовлетворяет функциональному уравнению

$$q^{s(g-1)} L(X, \chi, s) = \chi(W) q^{(1-s)(g-1)} L(X, \bar{\chi}, 1-s),$$

где W — канонический класс и $\bar{\chi}(C) = \overline{\chi(C)}$ — комплексно сопряженный с χ характер. Действительно, если характер χ не тривиален на группе $\mathrm{Cl}^0_{k_0}(X)$, то по теореме Римана — Роха имеем

$$L(X, \chi, s) = \frac{1}{q-1} \sum_{0 \leqslant \deg C \leqslant 2g-2} \chi(C) q^{l_0(-C) - s \deg C} =$$

$$= \frac{1}{q-1} \sum_{0 \leqslant \deg C \leqslant 2g-2} \chi(C) q^{\deg C - g + 1 + l_0(C-W) - s \deg C} =$$

$$= \frac{\chi(W) q^{g-1-(2g-2)s}}{q-1} \sum_{0 \leqslant \deg C \leqslant 2g-2} \bar{\chi}(W - C) q^{l_0(C-W) - (1-s)\deg(W-C)} =$$

$$= \frac{\chi(W) q^{g-1-(2g-2)s}}{q-1} \sum_{0 \leqslant \deg C \leqslant 2g-2} \bar{\chi}(C) q^{l_0(-C) - (1-s)\deg C} =$$

$$= \chi(W) q^{g-1-(2g-2)s} L(X, \bar{\chi}, 1-s).$$

Если же характер χ тривиален на $\mathrm{Cl}^0_{k_0}(X)$, то, полагая снова

$$C = C' + \nu C_0,$$

где $C' \in \mathrm{Cl}^0_{k_0}(X)$ и $\deg C_0 = 1$, а также

$$\chi(C_0) = e^{2\pi i \alpha},$$

получаем

$$L(X, \chi, s) = \frac{1}{q-1} \sum_{C'} \sum_{\nu=0}^{\infty} e^{2\pi i \alpha \nu} \left(q^{l_0(-C'-\nu C_0)} - 1\right) q^{-\nu s} =$$

$$= \frac{1}{q-1} \sum_{C'} \sum_{\nu=0}^{\infty} \left(q^{l_0(-C'-\nu C_0)} - 1\right) q^{-\nu(s - 2\pi i \alpha / \log q)} = \zeta\left(X, s - \frac{2\pi i \alpha}{\log q}\right).$$

В соответствии с теоремой 5 имеем

$$\zeta\left(X, s - \frac{2\pi i \alpha}{\log q}\right) = q^{2(g-1)\frac{2\pi i \alpha}{\log q}} q^{(g-1)(1-2s)} \zeta\left(X, 1 - s + \frac{2\pi i \alpha}{\log q}\right) =$$

$$= e^{4\pi i (g-1)\alpha} q^{(g-1)(1-2s)} \zeta\left(X, 1 - s + \frac{2\pi i \alpha}{\log q}\right) =$$

$$= \chi(W) q^{(g-1)(1-2s)} \zeta\left(X, 1 - s + \frac{2\pi i \alpha}{\log q}\right)$$

и тогда

$$L(X, \chi, s) = \chi(W) q^{(g-1)(1-2s)} L(X, \bar{\chi}, 1-s).$$

Чтобы получить класс L-функций, приводящий в частном случае к функции $L(z)$ из § 3 гл. I, необходимо расширить определение характера χ поля $k_0(X)$.

Пусть $\mathfrak{f}$ — строго положительный рациональный над k_0 дивизор и $\mathrm{Div}_{\mathfrak{f}}(X) \subset \mathrm{Div}_{k_0}(X)$ — группа дивизоров, взаимно простых с $\mathfrak{f}$. Обозначим $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ множество простых рациональных над k_0 дивизоров, содержащихся в $\mathfrak{f}$, и положим

$$P_{\mathfrak{f}}(X) = \left\{(f) \in P_{k_0} \mid f \underset{S}{\equiv} 1 \pmod{\mathfrak{f}}\right\}.$$

Легко проверить, что $P_{\mathfrak{f}}(X)$ является подгруппой (называемой *лучом по* $\bmod \mathfrak{f}$) группы главных рациональных над k_0 дивизоров, взаимно простых с $\mathfrak{f}$. Факторгруппа

$$\mathrm{Cl}_{\mathfrak{f}}(X) = \mathrm{Div}_{\mathfrak{f}}(X)/P_{\mathfrak{f}}(X)$$

называется *группой классов дивизоров по* $\bmod \mathfrak{f}$. Определим *характер* $\chi_{\mathfrak{f}}$ *по* $\bmod \mathfrak{f}$ как гомоморфизм группы $\mathrm{Cl}_{\mathfrak{f}}(X)$ в мультипликативную группу комплексных чисел, равных по абсолютной величине 1, и распространим его на группу $\mathrm{Div}_{k_0}(X)$, положив

$$\chi_{\mathfrak{f}}(D) = \begin{cases} \chi_{\mathfrak{f}}(D + P_{\mathfrak{f}}(X)), & \text{если } D \text{ взаимно прост с } \mathfrak{f}, \\ 0, & \text{в противном случае.} \end{cases}$$

Положим теперь

$$L(X, \chi_{\mathfrak{f}}, s) = \sum_{D \geqslant 0} \chi_{\mathfrak{f}}(D)(ND)^{-s}$$

и заметим, что при $\mathrm{Re}\, s > 1$

$$L(X, \chi_{\mathfrak{f}}, s) = \prod_{\mathfrak{p}} \left(1 - \chi_{\mathfrak{f}}(\mathfrak{p})(N\mathfrak{p})^{-s}\right)^{-1}.$$

Если $\chi_{\mathfrak{f}}$ — *примитивный характер по* $\bmod \mathfrak{f}$ (не являющийся характером ни по какому меньшему модулю), то L-функция $L(X, \chi_{\mathfrak{f}}, s)$ является (см. [46b, § 30]) многочленом от $z = q^{-s}$ степени $2g - 2 + \deg \mathfrak{f}$ и удовлетворяет функциональному уравнению

$$q^{s(g-1+\deg \mathfrak{f}/2)} L(X, \chi_{\mathfrak{f}}, s) = \eta q^{(1-s)(g-1+\deg \mathfrak{f}/2)} L(X, \bar{\chi}_{\mathfrak{f}}, 1-s),$$

где $\eta = \eta(\chi_{\mathfrak{f}})$ — постоянная с условием $|\eta| = 1$.

Положив теперь $X = \mathbb{P}^1$ и выбрав надлежащим образом дивизор $\mathfrak{f}$ (называемый *кондуктором* примитивного характера $\chi_{\mathfrak{f}}$, приходим к L-функции $L(\mathbb{P}^1, \chi_{\mathfrak{f}}, s)$, соответствующей в аффинном случае функции $L(z)$ из § 3 гл. I (см., например, [98a, с. 10—23]).

4. Дзета-функция многообразия. В заключение параграфа остановимся на некоторых результатах, касающихся *дзета-функции* $\mathrm{Z}(X, t)$ *n-мерного проективного неособого многообразия* X, определенного над полем $k_0 = F_q \subset k$ (назовем ее *дзета-функцией*

Вейля многообразия X). С этого момента будем считать, что поле k имеет бесконечную степень трансцендентности над k_0 и что поле $k_0(X)$ вложено в поле k.

Определение 7. Многообразие X, определенное над полем k_0, называется *абсолютным*, если оно остается многообразием над каждым алгебраическим расширением k' поля k_0. Это означает, что если $\mathfrak{a} = \mathfrak{a}(X)$ — идеал многообразия X, то радикал расширенного идеала $\mathfrak{a}k'[T]$ является простым идеалом в кольце $k'[T]$.

Пусть k' и k'' — расширения поля k_0, удовлетворяющие условиям: $k_0 \subset k' \subset k$, $k_0 \subset k'' \subset k$.

Определение 8. Расширения k' и k'' поля k_0 называются *линейно разделенными* над k_0, если выполнены следующие эквивалентные между собой условия:

1) если элементы $x_1, \ldots, x_m$ поля k' линейно независимы над k_0, то они также линейно независимы над k'';

2) если элементы $y_1, \ldots, y_n$ поля k'' линейно независимы над k_0, то они также линейно независимы над k'.

Справедливо следующее утверждение.

Предложение 10. *Пусть* k_0 *— совершенное поле. Многообразие* X, *определенное над полем* k_0, *является абсолютным в том и только в том случае, если поля* $\bar{k}_0$ *и* $k_0(X)$ *линейно разделены над* k_0 *или, что то же самое, если поле* k_0 *алгебраически замкнуто в* $k_0(X)$.

Доказательство см. в [146h, гл. 6, § 6].

Отметим, что в условиях предложения 10 сам идеал $\mathfrak{a}\bar{k}_0[T]$ является простым в кольце $\bar{k}_0[T]$. Отсюда следует, что гиперповерхность $X \subset \mathbb{P}^n$, определяемая уравнением $f = 0$, где $f \in k_0[T]$, является абсолютным многообразием в том и только в том случае, когда f — абсолютно неприводимый многочлен.

Пусть $X \subset \mathbb{P}^n$ — абсолютное неособое многообразие, определенное над конечным полем $k_0 = F_q$, и пусть N_{q^ν} — число его F_{q^ν}-рациональных точек. Определим дзета-функцию $\mathrm{Z}(X, t)$ многообразия X равенством

$$\mathrm{Z}(X, t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{N_{q^\nu}}{\nu} t^\nu\right).$$

В 1949 г. А. Вейль [23g] высказал ряд гипотез относительно функции $\mathrm{Z}(X, t)$:

1) если $r = \dim X$, то степенной ряд, определяющий функцию $\mathrm{Z}(X, t)$, *абсолютно сходится в круге* $|t| < q^{-r}$ комплексной плоскости $\mathbb{C}$;

2) $\mathrm{Z}(X, t)$ *является рациональной функцией комплексного переменного* t вида

$$\mathrm{Z}(X, t) = \frac{P_1(t) P_3(t) \ldots P_{2r-1}(t)}{P_0(t) P_2(t) \ldots P_{2r}(t)},$$

где

$$P_i(t) = \prod_{j=1}^{B_i} (1 - \omega_{ij} t), \quad 0 \leqslant i \leqslant 2r,$$

и

$$P_0(t) = 1 - t, \quad P_{2r}(t) = 1 - q^r t;$$

3) $Z(X, t)$ *удовлетворяет функциональному уравнению*

$$Z(X, 1/q^r t) = \pm q^{r\chi/2} t^\chi Z(X, t),$$

где

$$\chi = \sum_{i=0}^{2r} (-1)^i B_i;$$

4) для функции $Z(X, t)$ *справедлива «гипотеза Римана»*

$$|\omega_{ij}| = q^{i/2}, \quad 0 \leqslant i \leqslant 2r, \quad 1 \leqslant j \leqslant B_i;$$

5) если X представляет собой редукцию по $\mathrm{mod}\,\mathfrak{p}$ неособого комплексного проективного многообразия $X_{\mathbb{C}}$, определенного над конечным расширением F поля рациональных чисел $\mathbb{Q}$, где $\mathfrak{p}$ — простой идеал поля F с нормой $N\mathfrak{p} = q$, то *степень* B_i *многочлена* $P_i(t)$, $0 \leqslant i \leqslant 2r$, *совпадает с* i*-мерным числом Бетти многообразия* $X_{\mathbb{C}}$, *а число* χ *— с характеристикой Эйлера — Пуанкаре этого многообразия.*

Позже Дойринг [46a] предположил, что *коэффициенты многочленов* $P_i(t)$, $0 \leqslant i \leqslant 2r$, *являются целыми рациональными числами и, в частности, что* ω_{ij} *— целые алгебраические числа.*

Все эти предположения справедливы при $r = 1$.

Пусть X — многообразие размерности $r > 1$. Справедливость предположения 1) была установлена Вейлем и Ленгом [71], показавшими, что

$$N_{q^\nu} = q^{r\nu} + O\left(q^{(r-1/2)\nu}\right)$$

(см. также [92, 146g и 146h, гл. 5, § 5; гл. 6, § 7]).

Рациональность $Z(X, t)$ и функциональное уравнение были впервые установлены Дворком [39a — c] с помощью методов p-адического анализа (по поводу этого доказательства см. также доклад Серра [110b] и книгу Коблица [61]). Другое доказательство рациональности дзета-функции Вейля $Z(X, t)$ и вывод функционального уравнения 3) были даны Гротендиком [35a, b] на основе развитой им и М. Артином [7b] теории этальных когомологий (см. также М. Артин [6] и Милн [86b]). Подход Гротендика оказался весьма плодотворным и привел к представлению функции $Z(X, t)$ в виде

$$Z(X, t) = \frac{P_1(t) P_3(t) \dots P_{2r-1}(t)}{P_0(t) P_2(t) \dots P_{2r}(t)},$$

где $P_i(t)$ — многочлены с коэффициентами из поля l-адических чисел $\mathbb{Q}_l$ (l — простое число, отличное от характеристики p поля

$k_0 = F_q$), а также к новому определению чисел Бетти B_i многообразия $\overline{X}$ (полученного из X расширением поля F_q до $\overline{F}_q$) как размерностей $\dim H^i(\overline{X}, \mathbb{Q}_l)$ *групп* l*-адических когомологий* $H^i(\overline{X}, \mathbb{Q}_l)$, рассматриваемых как векторные пространства над $\mathbb{Q}_l$. При этом выяснилось совпадение степеней $\deg P_i(t)$ многочленов $P_i(t)$, $0 \leqslant i \leqslant 2r$, с определенными таким образом числами Бетти B_i.

Завершение грандиозной программы по изучению функции $Z(X, t)$, заложенной в работах А. Вейля [23b], Дворка [39a] и Серра [110a] было осуществлено Делинем [42a, b], установившим, что многочлены $P_i(t)$ в указанном выше представлении для функции $Z(X, t)$ имеют целые рациональные коэффициенты, не зависящие от l, и что они записываются в виде

$$P_i(t) = \prod_{j=1}^{B_i} (1 - \omega_{ij} t),$$

где ω_{ij} — целые алгебраические числа, удовлетворяющие условиям

$$|\omega_{ij}| = q^{i/2}, \quad 0 \leqslant i \leqslant 2r, \quad 1 \leqslant j \leqslant B_i.$$

Для комплексных многообразий $X_{\mathbb{C}}$ и их редукций X по $\mathrm{mod}\,\mathfrak{p}$ из этого результата следует совпадение обоих определений чисел Бетти B_i (классического и l-адического) и, значит, справедливость всех указанных выше гипотез для дзета-функции $Z(X, t)$.

Доказательство гипотез А. Вейля привело к ряду арифметических результатов. Укажем некоторые из них.

Пусть ψ_ν — аддитивный характер поля F_{q^ν}, $a \in F_q^*$ и

$$T_{n,\nu}(a) = \sum_{\substack{x_1, \dots, x_n \in F_{q^\nu} \\ x_1 \dots x_n = a}} \psi_\nu(x_1 + \dots + x_n)$$

— *обобщенная сумма Клостермана.* Как показал Делинь [42a] (см. также [110d, 60b, c]), L-ряд

$$L_n(a, t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{T_{n,\nu}(a)}{\nu} t^\nu\right)$$

входит в качестве множителя в соответствующую дзета-функцию $Z(X, t)$ абсолютного неособого многообразия X, определенного над полем F_q, и представляется в виде

$$L_n(a, t) = \left\{\prod_{i=1}^{n} (1 - \omega_i t)\right\}^{(-1)^n},$$

где

$$|\omega_i| = q^{\frac{n-1}{2}}, \quad 1 \leqslant i \leqslant n.$$

Отсюда, ввиду того, что

$$T_{n,\nu}(a) = (-1)^n \sum_{i=1}^{n} \omega_i^{\nu},$$

следует оценка

$$|T_{n,\nu}(a)| \leqslant n q^{\frac{\nu(n-1)}{2}}.$$

Далее, пусть $f(x_1, \ldots, x_n)$ — многочлен степени $m \geqslant 1$ с коэффициентами из поля F_q и

$$S_{n,\nu}(f) = \sum_{x_1,\ldots,x_n \in F_{q^\nu}} \psi_\nu(f(x_1, \ldots, x_n))$$

— *n-кратная тригонометрическая сумма Г. Вейля.* Если число m взаимно просто с характеристикой поля F_q и старшая форма

$$f_m = \sum_{i_1+\ldots+i_n=m} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$$

многочлена f определяет неособую гиперповерхность

$$f_m(x_1, \ldots, x_n) = 0$$

в проективном пространстве $\mathbb{P}^{n-1}$ над алгебраическим замыканием $\bar{F}_q$ поля F_q, то справедлива следующая оценка (Делинь [42a]):

$$|S_{n,\nu}(f)| \leqslant (m-1)^n q^{\nu n/2}.$$

Аналогичный результат для сумм

$$T_{n,\nu}(f) = \sum_{x_1,\ldots,x_n \in F_{q_\nu}} \chi_\nu(f(x_1, \ldots, x_n))$$

с квадратичным мультипликативным характером χ_ν был получен Г. И. Перельмутером [96c, d], показавшим, что если многочлен f и его старшая форма f_m определяют неособые гиперповерхности $f=0$ и $f_m=0$ в пространствах $\mathbb{A}^n$ и $\mathbb{P}^{n-1}$ над полем $\bar{F}_q$, то

$$|T_{n,\nu}(f)| \leqslant c(m, n) q^{\nu n/2}$$

(см. также [42c]).

Заметим, что представление функции $Z(X, t)$ в виде

$$Z(X, t) = \frac{P_1(t) P_3(t) \ldots P_{2r-1}(t)}{P_0(t) P_2(t) \ldots P_{2r}(t)},$$

где $P_0(t) = 1-t$, $P_{2r}(t) = 1 - q^r t$ и

$$P_i(t) = \prod_{j=1}^{B_i} (1 - \omega_{ij} t), \quad 1 \leqslant i \leqslant 2r-1,$$

приводит к соотношению

$$N_{q^\nu} = q^{\nu r} + 1 + \sum_{i=1}^{2r-1} (-1)^i \sum_{j=1}^{B_i} \omega_{ij}^{\nu}.$$

Отсюда следует, что задача о числе N_{q^ν} рациональных над F_{q^ν} точек многообразия X размерности $r > 1$, определенного над полем F_q, сводится к изучению структуры многочленов

$$P_i(t) = \prod_{j=1}^{B_i} (1 - \omega_{ij} t), \quad 1 \leqslant i \leqslant 2r-1,$$

и, в частности, к вычислению чисел Бетти B_i соответствующего комплексного многообразия $X_{\mathbb{C}}$. Тем самым, в отличие от одномерного случая, эта задача не эквивалентна «гипотезе Римана» для дзета-функции $Z(X, t)$ и требует дополнительных геометрических исследований. Во всех изученных к настоящему времени случаях (приводящих, в частности, к указанным выше оценкам сумм $T_{n,\nu}(a)$, $S_{n,\nu}(f)$ и $T_{n,\nu}(f)$) функция $Z(X, t)$ имеет весьма специальный вид. Типичную ситуацию дает пример сумм

$$T^*_{n,\nu}(f) = \sum_{x_0,x_1,\ldots,x_n \in F_{q^\nu}} \chi_\nu(f(x_0, x_1, \ldots, x_n)),$$

где f — однородный многочлен степени $m = 2s$ с коэффициентами из поля F_q характеристики $p > 2$. Если

$$L^*_n(f, t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{T^*_{n,\nu}(f)}{\nu} t^\nu\right),$$

то соответствующая этому ряду дзета-функция $Z^*(X, t)$ представляется в виде

$$Z^*(X, t) = \frac{L^*_n(f, t)}{(1-t)(1-qt)\ldots(1-q^n t)}.$$

Далее, если T_{n+1} — множество всех наборов $\tau = (\tau_0, \tau_1, \ldots, \tau_n)$ неотрицательных целых чисел $\tau_0, \tau_1, \ldots, \tau_n$, удовлетворяющих условию $\tau_0 + \tau_1 + \ldots + \tau_n = s$ и

$$x^\tau = x_0^{\tau_0} x_1^{\tau_1} \ldots x_n^{\tau_n},$$

то соответствующее сумме $T^*_{n,\nu}(f)$ многообразие X задается в проективном пространстве $\mathbb{P}^N$, $N = \frac{(n+1)(n+2)\ldots(n+s)}{s!}$, системой уравнений

$$\begin{cases} z^2 = F(\ldots, y_\tau, \ldots), \\ y_\sigma y_\tau = y_\mu y_\nu, \quad \sigma, \tau, \mu, \nu \in T_{n+1}, \ \sigma + \tau = \mu + \nu, \end{cases}$$

где $F(\ldots, y_\tau, \ldots)$ — такая квадратичная форма, что $F(\ldots, x^\tau, \ldots) = f(x_0, x_1, \ldots, x_n)$. Числа Бетти B_i, $0 \leqslant i \leqslant 2n$, многообразия $X_{\mathbb{C}}$

определяются (см. [96c]) равенствами

$$B_i = \begin{cases} 1, & \text{если } i = 2l, \quad i \neq n, \\ 0, & \text{если } i = 2l+1, \quad i \neq n, \\ m^{-1}\{(m-1)^{n+1} + (-1)^n\} + \frac{1}{2}\{1 + (-1)^n\}, \\ \qquad \text{если } i = n, \end{cases}$$

и $L_n^*(f, t) = P_n(t)^{(-1)^n}$, где $P_n(t)$ — многочлен степени B_n.

Другим важным следствием справедливости гипотез А. Вейля явилось доказательство Делиня *гипотезы Рамануджана* о порядке роста коэффициентов Фурье $\tau(n)$ параболической формы веса 12 относительно $SL_2(\mathbb{Z})$:

$$\Delta(z) = e^{2\pi i z}\prod_{n=1}^{\infty}(1 - e^{2\pi i n z})^{24} = \sum_{n=1}^{\infty}\tau(n)e^{2\pi i n z}, \quad i = \sqrt{-1}.$$

Эта гипотеза заключалась в том, что

$$|\tau(n)| \leqslant d(n)n^{11/2}$$

для всех $n \geqslant 1$, где $d(n)$ — число делителей положительного целого n. Ввиду соотношений:

1) $\tau(mn) = \tau(m)\tau(n)$, если $(m, n) = 1$,

2) $\tau(p^{s+1}) = \tau(p)\tau(p^s) - p^{11}\tau(p^{s-1})$, если p — простое и $s \geqslant 1$,

достаточно установить, что

$$|\tau(p)| \leqslant 2p^{11/2}$$

для всех простых чисел p.

Если рассмотреть многочлен Гекке

$$1 - \tau(p)t + p^{11}t^2 = (1 - \alpha(p)t)(1 - \overline{\alpha}(p)t),$$

то последнее предположение эквивалентно равенству

$$|\alpha(p)| = |\overline{\alpha}(p)| = p^{11/2}.$$

Если можно найти такое неособое абсолютное многообразие X размерности $r \geqslant 12$, определенное над полем F_p, что многочлен $1 - \tau(p)t + p^{11}t$ делит многочлен $P_{11}(t)$, входящий в дзета-функцию

$$Z(X, t) = \frac{P_1(t)P_3(t)\ldots P_{2r-1}(t)}{P_0(t)P_2(t)\ldots P_{2r}(t)}$$

этого многообразия, то гипотеза Рамануджана становится следствием «гипотезы Римана» для $Z(X, t)$. Конструкция такого многообразия X была осуществлена усилиями Эйхлера, Шимуры, Куги и Ихары (см. [66, 55a, b]). Однако соответствующее этому многообразию X комплексное многообразие $X_{\mathbb{C}}$ оказалось не компактным и, стало быть, лежащим вне границ справедливости для $Z(X, t)$ гипотез А. Вейля. Делинь указал способ гладкой компактификации этого многообразия и, тем самым, получил многообразие X^*, определенное над полем F_p, обладающее всеми свойствами, необходимыми для вывода гипотезы Рамануджана из «гипотезы Римана» для дзета-функции $Z(X^*, t)$.

Задачи

1. Пусть $X = \mathbb{P}^1$ — проективная прямая над полем $k = \overline{F}_q$. Доказать справедливость следующих утверждений:

а) $Z(\mathbb{P}^1, t) = \dfrac{1}{(1-t)(1-qt)}$;

б) $Z\left(\mathbb{P}^1, \dfrac{1}{qt}\right) = qt^2 Z(\mathbb{P}^1, t)$;

в) числа Бетти проективной комплексной прямой $\mathbb{P}^1_{\mathbb{C}}$ определяются равенствами

$$B_0 = B_2 = 1 \quad \text{и} \quad B_1 = 0;$$

г) характеристика Эйлера — Пуанкаре прямой $\mathbb{P}^1_{\mathbb{C}}$ равна

$$\chi = \sum_{i=0}^{2}(-1)^i B_i = 2.$$

(Указание. С определением чисел Бетти и методами их вычисления можно познакомиться по книге [47].)

2. Доказать, что дзета-функция проективной кривой $X \subset \mathbb{P}^2$, заданной над полем F_q уравнением

$$x^2 + y^2 - z^2 = 0,$$

имеет вид

$$Z(X, t) = \frac{1}{(1-t)(1-qt)}.$$

3. Пусть $X \subset \mathbb{A}^n$ — аффинная кривая, определенная над полем F_q характеристики $p > 2$, и N_{q^ν} — число F_{q^ν}-рациональных точек этой кривой. Определим дзета-функцию $Z(X, t)$ кривой X равенством

$$Z(X, t) = \exp\left(\sum_{\nu=1}^{\infty}\frac{N_{q^\nu}}{\nu}t^\nu\right).$$

Доказать справедливость следующих утверждений:

а) $Z(\mathbb{A}^1, t) = \dfrac{1}{1-qt}$;

б) $Z(\mathbb{A}^n, t) = \dfrac{1}{1-q^n t}$;

в) если $X \subset \mathbb{A}^2$ задается над полем F_q уравнением $x^2 + y^2 = 1$, то

$$Z(X, t) = \begin{cases} \dfrac{1-t}{1-qt} & \text{при } q \equiv 1 \pmod 4, \\ \dfrac{1+t}{1-qt} & \text{при } q \equiv 3 \pmod 4; \end{cases}$$

г) если $X \subset \mathbb{A}^2$ задается над F_q уравнением $y^2 = x^3$, то

$$Z(X, t) = \frac{1}{1 - qt};$$

д) если $X \subset \mathbb{A}^2$ задается над F_q уравнением $y^2 = x^3 + x^2$, то

$$Z(X, t) = \frac{1 - t}{1 - qt}.$$

4. Пусть $X \subset \mathbb{P}^2$ — эллиптическая кривая, определенная над полем F_q. Доказать справедливость следующих утверждений:

а) $Z(X, t) = \dfrac{1 + \sigma_1 t + qt^2}{(1 - t)(1 - qt)}$;

б) $Z\left(X, \dfrac{1}{qt}\right) = Z(X, t)$;

в) если $X_{\mathbb{C}}$ — соответствующая X комплексная эллиптическая кривая, то $B_0 = B_2 = 1$ и $B_1 = 2$;

г) если $1 + \sigma_1 t + qt^2 = (1 - \omega t)(1 - \overline{\omega} t)$, то

$$|\omega| = |\overline{\omega}| = q^{1/2};$$

д) для числа N_{q^ν} рациональных над полем F_{q^ν} точек кривой X справедлива формула

$$N_{q^\nu} = q^\nu + 1 - (\omega^\nu + \overline{\omega}^\nu);$$

е) имеет место оценка

$$\left| N_{q^\nu} - q^\nu - 1 \right| \leqslant 2q^{\nu/2}.$$

5. Пусть X — проективная кривая рода g, определенная над полем F_q. Установить справедливость следующих утверждений:

а) дзета-функция кривой X удовлетворяет функциональному уравнению

$$Z\left(X, \frac{1}{qt}\right) = q^{\chi/2} t^\chi Z(X, t), \quad \chi = 2 - 2g;$$

б) коэффициенты многочлена $P(t)$ в представлении

$$Z(X, t) = \frac{P(t)}{(1 - t)(1 - qt)}$$

являются целыми рациональными числами;

в) если

$$P(t) = \prod_{i=1}^{2g} (1 - \omega_i t),$$

то

$$\omega_i \omega_{2g-i+1} = q, \quad 1 \leqslant i \leqslant 2g.$$

6. Пусть $X = \mathbb{P}^n$ — проективное n-мерное пространство над полем $\overline{F}_q$. Исходя из определения дзета-функции, показать, что

$$Z(\mathbb{P}^n, t) = \frac{1}{(1 - t)(1 - qt) \dots (1 - q^n t)}.$$

Установить для $Z(\mathbb{P}^n, t)$ справедливость гипотез А. Вейля.

7. Пусть $Z(X, t) = \dfrac{\prod_{i=1}^{a} (1 - \omega_i t)}{\prod_{j=1}^{b} (1 - \omega_j^* t)}$ — дзета-функция неособого абсолютного многообразия $X \subset \mathbb{P}^n$ размерности r, определенного над полем F_q. Доказать, что функциональное уравнение для $Z(X, t)$ эквивалентно выполнимости соотношений

$$\omega_i \omega_{a-i+1} = q^r, \quad 1 \leqslant i \leqslant a,$$

$$\omega_j^* \omega_{b-j+1}^* = q^r, \quad 1 \leqslant j \leqslant b.$$

8*. Многообразие $X \subset \mathbb{P}^n$, определенное над полем $k_0 \subset k$, называется *линейным*, если оно задается совокупностью линейных уравнений. Совокупность всех m-мерных линейных многообразий X_m пространства $\mathbb{P}^n$, определенных над k_0, называется *многообразием Грассмана* и обозначается $G_{m,n}$. Установить справедливость следующих утверждений:

а) многообразие $G_{m,n}$ имеет размерность $r = (m + 1)(n - m)$;

б) $G_{m,n}$ является абсолютным неособым многообразием;

в) если $k_0 = F_q$ и $k = \overline{F}_q$, то для числа N_{q^ν} рациональных над полем F_{q^ν} точек многообразия $G_{m,n}$ справедлива формула

$$N_{q^\nu} = P_{m,n}(q^\nu),$$

где $P_{m,n}$ — многочлен вида

$$P_{m,n}(T) = \frac{T^{n+1} - 1}{T^{m+1} - 1} \cdot \frac{T^n - 1}{T^m - 1} \cdots \frac{T^{n-m+1} - 1}{T - 1};$$

г) $Z(G_{m,n}, t) = \prod_{i=1}^{r} \dfrac{1}{(1 - q^i t)^{B_{2i}}}$, где целые числа B_{2i} определяются разложением

$$P_{m,n}(T) = \sum_{i=0}^{r} B_{2i} T^i;$$

д) числа B_{2i} удовлетворяют соотношениям

$$B_0 = B_{2r} = 1, \qquad B_{2(r-i)} = B_{2i}, \quad 1 \leqslant i \leqslant 2r - 1$$

и совпадают с числами Бетти соответствующего комплексного грассманова многообразия.

9*. Установить рациональность дзета-функции $Z(X, t)$ проективной гиперповерхности X, определенной над полем F_q уравнением

$$a_0 x^m + a_1 x_1^m + \dots + a_r x_r^m = 0, \quad a_i \in F_q^*.$$

10. Пусть $X \subset \mathbb{A}^n$ — гиперповерхность, определенная над F_q и N_{q^ν} — число ее F_{q^ν}-рациональных точек. Доказать справедливость следующих утверждений:

а) коэффициенты a_m ряда

$$Z(X, t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{N_{q^\nu}}{\nu} t^\nu \right) = 1 + \sum_{m=1}^{\infty} a_m t^m$$

являются неотрицательными целыми числами;

б) при всех $m = 1, 2, \ldots$ справедлива оценка

$$a_m \leqslant q^{mn}.$$

11*. Пусть p — простое число, $\mathbb{Q}_p$ — поле p-адических чисел, K — конечное расширение поля $\mathbb{Q}_p$ степени n и $\operatorname{norm}\alpha$ — норма элемента $\alpha \in K$ над полем $\mathbb{Q}_p$. Положим

$$v_p(\alpha) = \frac{1}{n} v_p(\operatorname{norm}\alpha) \text{ и } |\alpha|_p = p^{-v_p(\alpha)}$$

(см. задачи 1—12 из § 5 гл. IV).

Образ поля K при отображении v_p является подгруппой аддитивной группы $(1/n)\mathbb{Z} = \{x \in \mathbb{Q} \mid nx \in \mathbb{Z}\}$ и представляется в виде $(1/e)\mathbb{Z}$, где e — некоторое положительное целое число, делящее n. Число e называется *индексом ветвления* поля K над $\mathbb{Q}_p$. Если $e = 1$, то говорят, что поле K — *неразветвленное расширение* поля $\mathbb{Q}_p$. Если же $e = n$, то K называется *вполне разветвленным расширением* поля $\mathbb{Q}_p$. Пусть $\mathfrak{o}_p = \{x \in K \mid |x|_p \leqslant 1\}$ — локальное кольцо поля K и $\mathfrak{m}_p = \{x \in \mathfrak{o}_p \mid |x|_p < 1\}$ — максимальный идеал этого кольца. Поле $\mathfrak{o}_p/\mathfrak{m}_p$ является конечным расширением поля F_p и называется *полем вычетов* для K. Степень $\mathfrak{o}_p/\mathfrak{m}_p$ над F_p называется *степенью поля вычетов*.

Доказать справедливость следующих утверждений:

а) Индекс ветвления e и степень s поля вычетов связаны соотношением $es = n$.

(Указание. Пусть π — элемент поля K, для которого $v_p(\pi) = 1/e$, и $x_1, \ldots, x_s$ — такие элементы этого поля, что $|x_i|_p = 1$ и их образы при редукции по $\bmod \mathfrak{m}_p$ образуют базис поля $\mathfrak{o}_p/\mathfrak{m}_p$ над F_p. Покажите, что элементы $x_i\pi^j$, $1 \leqslant i \leqslant s$, $0 \leqslant j \leqslant e-1$ составляют базис поля K над $\mathbb{Q}_p$.)

б) Пусть K — вполне разветвленное расширение поля $\mathbb{Q}_p$ и π — такой элемент поля K, что $v_p(\pi) = 1/e$. Тогда π является корнем *многочлена Эйзенштейна*

$$f(x) = x^e + a_1x^{e-1} + \ldots + a_e,$$

где $a_i \in \mathbb{Z}_p, a_i \equiv 0 \pmod p$, $1 \leqslant i \leqslant e$, и $a_e \not\equiv 0 \pmod{p^2}$. Обратно, если α — корень многочлена Эйзенштейна, то $\mathbb{Q}_p(\alpha)$ — вполне разветвленное расширение поля $\mathbb{Q}_p$.

(Указание. Воспользоваться тем, что многочлен Эйзенштейна $f(x)$ неприводим над $\mathbb{Q}_p$.)

в) Существует ровно одно неразветвленное расширение K_s степени s поля $\mathbb{Q}_p$, которое получается присоединением к полю $\mathbb{Q}_p$ примитивного корня степени $p^s - 1$ из 1.

(Указание. Пусть $\bar{f} = x^s + \bar{a}_1x^{s-1} + \ldots + \bar{a}_s$ — минимальный многочлен порождающего элемента $\bar{\eta}$ мультипликативной группы $F^*_{p^s}$ поля F_{p^s} и f — многочлен из кольца $\mathbb{Z}_p[x]$, редукция которого по $\bmod p$ приводит к $\bar{f}$. Показать, что многочлен f неприводим в $\mathbb{Z}_p[x]$ и что корень η многочлена f порождает неразветвленное расширение $K_s = \mathbb{Q}_p(\eta)$ степени s поля $\mathbb{Q}_p$. Показать, далее, что в поле K_s существует элемент α, для которого $\alpha^{p^s-1} - 1 = 0$.)

г) Если K — расширение поля $\mathbb{Q}_p$ степени n с индексом ветвления e и степенью поля вычетов s, то $K = K_s(\pi^*)$, где π^* — корень некоторого многочлена Эйзенштейна с коэффициентами из неразветвленного расширения K_s.

д) Если K — конечное расширение поля $\mathbb{Q}_p$ степени n с индексом ветвления e и степенью поля вычетов s, а π — такой элемент этого расширения, что $v_p(\pi) = 1/e$, то каждый элемент $\alpha \in K$ однозначно представим в виде

$$\alpha = \sum_{i=m}^{\infty} \alpha_i\pi^i,$$

где $m = ev_p(\alpha)$ и $\alpha_i^{p^s} = \alpha_i$ при всех $i \geqslant m$.

е) Конечные неразветвленные расширения поля $\mathbb{Q}_p$ исчерпываются всеми расширениями, которые получаются присоединением к $\mathbb{Q}_p$ корней из 1 степени, взаимно простой с p.

12*. Объединение всех конечных неразветвленных расширений поля $\mathbb{Q}_p$ называется *максимальным неразветвленным расширением* поля $\mathbb{Q}_p$ и обозначается K^{nr}. Кольцо

$$\mathfrak{o}^{nr} = \{x \in K^{nr} \mid |x|_p \leqslant 1\}$$

является локальным кольцом с максимальным идеалом

$$\mathfrak{m}^{nr} = \{x \in \mathfrak{o}^{nr} \mid |x|_p < 1\}.$$

Поле $\mathfrak{o}^{nr}/\mathfrak{m}^{nr}$ совпадает с алгебраическим замыканием $\overline{F}_p$ поля F_p. Каждый элемент $\bar{x} \in \overline{F}_p$ обладает единственным представителем $x \in \mathfrak{o}^{nr}$ (*представителем Тейхмюллера*), который является корнем из 1 в $\mathfrak{o}^{nr}$ и редуцируется в $\bar{x} \pmod{\mathfrak{m}^{nr}}$. По этой причине кольцо $\mathfrak{o}^{nr}$ называется *поднятием поля* $\overline{F}_p$ в характеристику нуль или *кольцом векторов Витта поля* $\overline{F}_p$.

Установить справедливость следующих утверждений:

а) алгебраическое замыкание $\overline{\mathbb{Q}}_p$ поля $\mathbb{Q}_p$ не полно относительно сходимости по p-адической норме.

(Указание: Пусть a_i — примитивный корень из 1 степени $p^{2^i}-1$ в поле $\overline{\mathbb{Q}}_p$. Положить

$$\alpha_j = \sum_{i=0}^{r_j} a_ip^{n_i}, \quad \alpha_j \in K^{nr},$$

и выбрать возрастающую последовательность целых чисел

$$0 = n_0 < n_1 < n_2 < \ldots$$

таким образом, чтобы последовательность $\{\alpha_j\}$ являлась фундаментальной, но не сходилась ни к какому элементу $\alpha \in \overline{\mathbb{Q}}_p$);

б) пополнение Ω_p поля $\overline{\mathbb{Q}}_p$ по p-адической норме $|\ |_p$ является полным алгебраически замкнутым полем;

в) множества $\mathbb{Q}_p$, $\overline{\mathbb{Q}}_p$ и Ω_p имеют одну и ту же мощность;

г) поле Ω_p имеет несчетную степень трансцендентности над $\overline{\mathbb{Q}}_p$ (т. е. Ω_p нельзя представить в виде алгебраического расширения поля, полученного из $\overline{\mathbb{Q}}_p$ присоединением счетного числа элементов $\alpha_i \in \Omega_p$).

13. Пусть R — некоторое кольцо и $R[[x]]$ — *кольцо формальных степенных рядов*

$$f(x) = \sum_{i=0}^{\infty} a_ix^i$$

от переменного x с коэффициентами из R. Ряд $f(x) \in \Omega_p[[x]]$ называется

сходящимся в точке $x_0 \in \Omega_p$, если в поле Ω_p сходится последовательность его частичных сумм

$$S_N(x_0) = \sum_{i=0}^{N} a_i x_0^i.$$

Доказать справедливость следующих утверждений:

а) ряд $f(x) = \sum_{i=0}^{\infty} a_i x^i \in \Omega_p[[x]]$ сходится в точке $x_0 \in \Omega_p$ **тогда и только тогда, когда**

$$|a_i x_0^i|_p \to 0 \text{ при } i \to \infty;$$

б) каждый ряд $f(x) \in \mathbb{Z}_p[[x]]$ сходится в круге $|x|_p < 1$, $x \in \Omega_p$;

в) всякий ряд $f(x) \in \Omega_p[[x]]$, сходящийся в некотором круге $|x|_p < r$, представляет в нем непрерывную функцию;

г) ряд

$$\log(1+x) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{x^i}{i} \in \mathbb{Q}_p[[x]]$$

сходится при $|x|_p < 1$ и расходится при $|x|_p \geqslant 1$ (напомним, что $|\alpha|_p = p^{-v_p(\alpha)}$);

д) ряд

$$\exp x = \sum_{i=0}^{\infty} \frac{x^i}{i!} \in \mathbb{Q}_p[[x]]$$

сходится в круге $|x|_p < p^{-1/(p-1)}$ и расходится в каждой точке $x \in \Omega_p$, лежащей вне его;

е) в круге $|x|_p < p^{-1/(p-1)}$ имеют место равенства

$$\log \exp x = x, \quad \exp \log(1+x) = 1 + x;$$

ж) ряд

$$\sin x = \sum_{i=0}^{\infty} (-1)^i \frac{x^{2i+1}}{(2i+1)!} \in \mathbb{Q}_p[[x]]$$

сходится в круге $|x|_p < p^{-1/(p-1)}$.

14. Найти ошибку в следующем «доказательстве» иррациональности числа π. Пусть $\pi = a/b$ и p — простое число, не делящее a. Тогда

$$0 = \sin(bp\pi) = \sin(ap) = \sum_{i=0}^{\infty} (-1)^i \frac{(ap)^{2i+1}}{(2i+1)!} \equiv ap \pmod{p^2},$$

что невозможно.

§ 2. Число рациональных точек алгебраической кривой над конечным полем

В этом параграфе дается доказательство теоремы А, сформулированной в § 4 гл. I. Пусть X — неособая проективная кривая рода g, определенная над конечным полем $k_0 = F_q$. Теорема А является частным случаем следующего утверждения.

Теорема В. *Для числа* N_{q^ν} *рациональных над полем* F_{q^ν} *точек кривой* X *справедлива оценка*

$$\left| N_{q^\nu} - q^\nu - 1 \right| \leqslant 2gq^{\nu/2}. \tag{1}$$

Доказательство теоремы В разобьем на два этапа. Вначале установим справедливость оценки

$$\left| N_{q^\nu} - q^\nu - 1 \right| \leqslant cq^{\nu/2} \tag{2}$$

с некоторой достаточно большой константой c, а затем, воспользовавшись аппаратом дзета-функций, развитым в предыдущем параграфе, получим оценку (1).

1. Предварительная оценка. Пусть $k = \overline{F}_q$ — алгебраическое замыкание поля $k_0 = F_q$. Метод, который мы применим для вывода неравенства (2), состоит в построении отличной от нуля функции $f \in k(X)$, имеющей нули достаточно высокого порядка почти во всех F_{q^ν}-рациональных точках кривой X и обладающей не слишком большим числом полюсов. Неравенство (2) получается при этом в результате сравнения числа нулей и полюсов рациональной функции f (см. комментарии к гл. I). Конструкцию функции f с указанными свойствами осуществим, следуя Бомбьери [16b, c], с помощью теоремы Римана — Роха.

Заметим, что поскольку каждое расширение F_{q^μ} поля $k_0 = F_q$ также является полем определения кривой X, то без уменьшения общности можно считать, что $q = p^{2r}$.

Лемма. *Если* $q = p^{2r}$ *и* $q^\nu > (g+1)^4$, *то*

$$N_{q^\nu} \leqslant q^\nu + 1 + (2g+1)q^{\nu/2}.$$

Доказательство. Будем считать, что на кривой X имеется хотя бы одна F_{q^ν}-рациональная точка y (иначе нечего было бы доказывать). Обозначим R_m линейное над полем k пространство функций $f \in k(X)$, регулярных вне y и имеющих в точке y полюс порядка не выше m. Это пространство обладает следующими свойствами (некоторые из них очевидны):

1) $\dim_k R_{m+1} \leqslant \dim_k R_m + 1$;

2) *если* $m > 2g-2$, *то*

$$\dim_k R_m = m - g + 1$$

(см. следствие теоремы 8 из § 6 гл. IV);

3) *если* $f(x) \in R_m$, то $f(x^{q^\nu}) \in R_{mq^\nu}$;

4) *в пространстве* R_m *существует такой базис* $f_1, \ldots, f_s$, *что* $v_y(f_i) < v_y(f_{i+1})$ *при всех* $i = 1, 2, \ldots, s-1$.

Действительно, имеем

$$(0) \subset k = R_0 \subset R_1 \subset \ldots \subset R_m$$

и тогда

$$R_m = \bigoplus_{i=0}^{m} R_i/R_{i-1}.$$

Ввиду свойства 1)

$$\dim_k R_i/R_{i-1} \leqslant 1,$$

и, значит, указанный базис можно получить, если в R_i выбрать (когда это возможно) элемент f_j, не лежащий в R_{i-1}.

Пусть n, τ — неотрицательные целые числа и $u_1, \ldots, u_s$ — некоторые элементы пространства R_n. Рассмотрим функцию

$$f(x) = u_1^{p^\tau}(x) f_1(x^{q^\nu}) + \ldots + u_s^{p^\tau}(x) f_s(x^{q^\nu})$$

и докажем следующее утверждение:

5) *если* $np^\tau < q^\nu$, *то функция* f *равна нулю в* $k(X)$ *тогда и только тогда, когда все* u_i, $1 \leqslant i \leqslant s$, *равны нулю.*

В самом деле, предположим, что $f \neq 0$ и что i_0 — первое значение $i = 1, 2, \ldots, s$, при котором $u_i \neq 0$. При всех $x \in X$ имеем

$$u_{i_0}^{p^\tau}(x) f_{i_0}(x^{q^\nu}) = -u_{i_0+1}^{p^\tau}(x) f_{i_0+1}(x^{q^\nu}) - \ldots - u_s^{p^\tau}(x) f_s(x^{q^\nu})$$

и тогда по свойству 4)

$$p^\tau v_y(u_{i_0}) + q^\nu v_y(f_{i_0}) \geqslant \min_{i>i_0}\left(p^\tau v_y(u_i) + q^\nu v_y(f_i)\right) \geqslant$$

$$\geqslant -np^\tau + q^\nu v_y(f_{i_0+1}).$$

В таком случае

$$p^\tau v_y(u_{i_0}) \geqslant -np^\tau + q^\nu\left(v_y(f_{i_0+1}) - v_y(f_{i_0})\right) \geqslant -np^\tau + q^\nu > 0$$

и, значит, функция u_{i_0} обращается в точке y в нуль. Поскольку эта функция регулярна во всех остальных точках $x \in X$, то $u_{i_0} = 0$, и мы приходим к противоречию, которое доказывает справедливость утверждения 5);

6) *если* m, $n > 2g-2$ *и*

$$(m-g+1)(n-g+1) > np^\tau + m - g + 1,$$

то существуют отличные в совокупности от нуля элементы $u_1, \ldots, u_s \in R_n$, *для которых функция*

$$u_1^{p^\tau}(x) f_1(x) + \ldots + u_s^{p^\tau}(x) f_s(x)$$

тождественно равна нулю.

Действительно, рассматриваемая функция регулярна вне y и имеет в точке y полюс порядка $l \leqslant np^\tau + m$. Множество таких функций образуют линейное пространство над k размерности не выше $np^\tau + m - g + 1$ (см. свойство 2)). Поскольку каждая функция u_i пробегает векторное пространство размерности $n-g+1$

и поскольку по свойству 2) $s = m-g+1$, то найдутся такие $u_1, \ldots, u_s \in R_n$, не все равные нулю, для которых

$$u_1^{p^\tau}(x) f_1(x) + \ldots + u_s^{p^\tau}(x) f_s(x) = 0$$

при всех $x \in X$. Утверждение 6) доказано.

Если x — рациональная над полем F_{q^ν} точка, то имеем $x^{q^\nu} = x$ и, значит, при выполнении условий m, $n > 2g-2$, $np^\tau < q^\nu$, $(m-g+1)(n-g+1) > np^\tau + m - g + 1$ существует отличная от нуля функция $f(x)$, обращающаяся в нуль в каждой F_{q^ν}-рациональной точке x кривой X, отличной от y. Кроме того, поскольку f имеет вид $f = \varphi^{p^\tau}$, то каждая такая точка является нулем функции f кратности по меньшей мере p^τ. Таким образом, f имеет по меньшей мере $(N_{q^\nu} - 1)p^\tau$ нулей с учетом их кратностей.

С другой стороны, функция f регулярна вне y и имеет в точке y полюс порядка не выше $np^\tau + mq^\nu$. Поскольку число нулей функции f совпадает с числом ее полюсов, отсюда следует, что при всех m, n, τ, удовлетворяющих условиям m, $n > 2g-2$, $np^\tau < q^\nu$, $(m-g+1)(n-g+1) > np^\tau + m - g + 1$, справедливо неравенство

$$(N_{q^\nu} - 1)p^\tau \leqslant np^\tau + mq^\nu.$$

Возьмем $p^\tau = q^{\nu/2}$, $n = q^{\nu/2} - 1$ и $m = q^{\nu/2} + 2g$. При $q^\nu > (g+1)^4$ все указанные выше условия выполняются и тогда

$$N_{q^\nu} \leqslant q^\nu + 1 + (2g+1)q^{\nu/2}.$$

Лемма доказана.

Перейдем к доказательству оценки (2).

Теорема С. *Если* $q = p^{2r}$ *и* $q > c' = c'(X)$, *то справедливо соотношение*

$$N_{q^\nu} = q^\nu + O(q^{\nu/2})$$

с константой в символе «O*», не зависящей от* ν.

Доказательство. Поле $k(X)$ содержит чисто трансцендентное подполе $k(u)$ и является сепарабельным расширением поля $k(u)$. В таком случае существует нормальное расширение поля $k(u)$, которое нормально также и над $k(X)$ (см. [70d, гл. 8, § 1]). Геометрически ситуация может быть представлена в виде

$$X' \to X \to \mathbb{P}^1,$$

где $X' \to \mathbb{P}^1$ и $X' \to X$ — *накрытия Галуа* с группами Галуа G и H, где H — подгруппа группы G. Указанная ситуация реализуется, вообще говоря, над некоторым конечным расширением поля F_{q^ν}. Переходя в случае необходимости к такому расширению, будем считать без уменьшения общности, что эта ситуация реализуется над полем F_{q^ν}.

Пусть x — неразветвленная относительно накрытия $X' \to \mathbb{P}^1$ рациональная над F_{q^ν} точка проективной прямой $\mathbb{P}^1$. Если x' — точка кривой X', лежащая над x, то для некоторого $\alpha \in G$ имеем представление

$$\alpha(x') = x'^{q^\nu},$$

называемое *подстановкой Фробениуса* элемента α. Обозначим g' род кривой X' и через m — порядок элемента α. Отображение $\alpha(x')$ переводит кривую X' в изоморфную ей над полем $F_{q^{m\nu}}$ кривую X'_α. Если $N_{q^\nu}(X'_\alpha)$ — число F_{q^ν}-рациональных точек кривой X'_α, то в соответствии с леммой имеем

$$N_{q^\nu}(X'_\alpha) \leqslant q^\nu + 1 + (2g' + 1)\, q^{\nu/2}.$$

Кроме того,

$$\sum_{\alpha \in G} N_{q^\nu}(X'_\alpha) = |G|\, N_{q^\nu}(\mathbb{P}^1) + O(1),$$

где константа $O(1)$ возникает от точек ветвления накрытия $X' \to \mathbb{P}^1$. Так как $N_{q^\nu}(\mathbb{P}^1) = q^\nu + 1$, то

$$N_{q^\nu}(X'_\alpha) = q^\nu + O\left(q^{\nu/2}\right),$$

причем постоянная, входящая в символ «O», зависит лишь от $|G|$ и g. Далее, имеем

$$\sum_{\alpha \in H} N_{q^\nu}(X'_\alpha) = |H|\, N_{q^\nu} + O(1)$$

и, в таком случае,

$$N_{q^\nu} = q^\nu + O\left(q^{\nu/2}\right).$$

Теорема доказана.

2. Оценка А. Вейля. Перейдем к доказательству теоремы B. В § 1 было показано, что дзета-функция $Z(X, t)$ кривой X рода g, определенной над полем $k_0 = F_q$, имеет вид

$$Z(X, t) = \frac{P(t)}{(1-t)(1-qt)},$$

где

$$P(t) = 1 + \sum_{i=1}^{2g-1} \sigma_i t^i + q^g t^{2g}$$

— многочлен с целыми коэффициентами. Кроме того, там же было показано, что если

$$P(t) = \prod_{i=1}^{2g} (1 - \omega_i t),$$

то

$$N_{q^\nu} = q^\nu + 1 - \sum_{i=1}^{2g} \omega_i^\nu. \qquad (3)$$

Покажем, что все нули ω_i^{-1} функции $Z(X, t)$ лежат на окружности $|t| = q^{-1/2}$. Это равносильно тому, что все нули функции $\zeta(X, s) = Z(X, t)$ лежат на прямой $\operatorname{Re} s = 1/2$. Из теоремы C следует, что ряд

$$\frac{Z'(X, t)}{Z(X, t)} - \frac{q}{1-qt} - \frac{1}{1-t} = \sum_{\nu=1}^{\infty} \left(N_{q^\nu} - q^\nu - 1\right) t^{\nu-1}$$

абсолютно сходится в круге $|t| < q^{-1/2}$. Значит, функция $Z(X, t)$ не имеет нулей при $|t| < q^{-1/2}$. В силу функционального уравнения она не имеет нулей и при $|t| > q^{-1/2}$. В таком случае, все нули функции $Z(X, t)$ лежат на окружности $|t| = q^{-1/2}$ и, следовательно, $|\omega_i| = q^{1/2}$ при всех $i = 1, 2, \ldots, 2g$.

Из соотношения (3) имеем

$$\left|N_{q^\nu} - q^\nu - 1\right| \leqslant \sum_{i=1}^{2g} |\omega_i|^\nu$$

и, стало быть,

$$\left|N_{q^\nu} - q^\nu - 1\right| \leqslant 2g q^{\nu/2}.$$

Теорема B доказана.

Задачи

1. Пусть X — кривая рода g, определенная над полем F_q и пусть N_{q^ν} — число F_{q^ν}-рациональных точек этой кривой. Показать, что N_q, $N_{q^2}, \ldots, N_{q^g}$ однозначно определяют N_{q^ν} для всех $\nu \geqslant g + 1$.

2. Пусть χ — мультипликативный характер и ψ — аддитивный характер поля F_q. Доказать, что для числа N_{q^ν} решений системы уравнений

$$y^s = f(x), \quad z^q - z = g(x)$$

в элементах $x, y, z \in F_{q^\nu}$ имеет место равенство

$$N_{q^\nu} = \sum_{\operatorname{ind} \chi = s} \sum_{\psi} \sum_{x \in F_{q^\nu}} \chi_\nu(f(x))\, \psi_\nu(g(x)).$$

3. Доказать, что если f, g — многочлены из кольца $F_q[x]$ степеней l, n соответственно и $(s, l) = (n, q) = 1$, то уравнения

$$y^s = f(x), \quad z^q - z = g(x)$$

определяют абсолютную кривую в аффинном пространстве $\mathbb{A}^3$ над полем $k = \overline{F_q}$.

4. Пусть $f = f_1^{s_1} \ldots f_r^{s_r}$ — разложение многочлена $f \in F_q[x]$ степени l на неприводимые множители и пусть $m = \deg(f_1 \ldots f_r)$. Пусть, далее, $g \in F_q[x]$ — многочлен степени n и χ — нетривиальный мультипликативный характер показателя s, ψ — нетривиальный аддитивный характер поля F_q. Доказать, что если $(l, s) = (n, q) = 1$, то имеет место оценка

$$\left|\sum_{x \in F_{q^\nu}} \chi_\nu(f(x))\, \psi_\nu(g(x))\right| \leqslant (m + n - 1)\, q^{\nu/2}.$$

(Указание. Воспользоваться результатами двух предыдущих задач, результатами § 3 гл. I и теоремой B.)

5*. Пусть $X \subset \mathbb{A}^n$ — кривая, определенная над полем F_q системой уравнений

$$y_1^{s_1} = f_1(x), \ \ldots, \ y_n^{s_n} = f_n(x),$$

где $f_1, \ldots, f_n$ — многочлены степени не выше m. Пусть, далее, $l = \{s_1, \ldots, s_n\}$ — наименьшее общее кратное чисел $s_1, \ldots, s_n$ и $s = s_1 \ldots s_n$.

Доказать справедливость следующих утверждений:

а) Если $s_i \mid q - 1$ при всех $i = 1, 2, \ldots, n$ и χ — мультипликативный характер поля F_q порядка l, то для числа N_q рациональных над F_q точек кривой X имеет место формула

$$N_q = \sum_{i_1=0}^{s_1-1} \ldots \sum_{i_n=0}^{s_n-1} \left(\sum_{x \in F_q} \chi\left(f_1^{\frac{i_1 l}{s_1}}(x) \ldots f_n^{\frac{i_n l}{s_n}}(x) \right) \right).$$

б) Если $k = \overline{F}_q$ и $[k(X) : k(x)] = s$, то для всякого ненулевого набора $(i_1, \ldots, i_n)$ многочлен

$$f_1^{\frac{i_1 l}{s_1}}(x) \ldots f_n^{\frac{i_n l}{s_n}}(x)$$

не является l-й степенью в кольце $k[x]$.

в) Если $[k(X) : k(x)] = s$ и $q > 100 l^3 m^2 n^2$, то для величины N_q справедлива оценка

$$|N_q - q| < 5mnsl^{5/2} q^{1/2}.$$

(Указание. Показать, что число N_q решений системы уравнений

$$y_1^{s_1} = f_1(x), \ \ldots, \ y_n^{s_n} = f_n(x)$$

в элементах $x, y_1, \ldots, y_n \in F_q$ равно числу решений системы

$$y_1^{s_1'} = f_1(x), \ \ldots, \ y_n^{s_n'} = f_n(x),$$

где $s_i' = (s_i, q-1)$, $1 \leqslant i \leqslant n$, и воспользоваться результатами двух предыдущих пунктов, а также результатом задачи 10 из § 4 гл. I.)

6. Пусть $p > 2$ — простое число и n — фиксированное целое положительное число. Доказать, что для числа N_n элементов $x \in F_p$, удовлетворяющих условию

$$\left(\frac{x+1}{p}\right) = \ldots = \left(\frac{x+n}{p}\right) = 1$$

справедлива асимптотическая формула

$$N_n = \frac{p}{2^n} + O(p^{1/2}).$$

(Указание. Рассмотреть кривую $X \subset \mathbb{A}^n$, задаваемую над F_p системой уравнений

$$y_1^2 = x + 1, \ \ldots, \ y_n^2 = x + n$$

и воспользоваться результатом предыдущей задачи.)

7. Пусть p — простое число. Отождествим поле F_p с числами $0, 1, \ldots, p-1$ и рассмотрим множество F_p^n наборов $x = (x_1, \ldots, x_n)$, $0 \leqslant x_i < p$. Для двух наборов $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$, удовлетворяющих условию $0 \leqslant a_i < b_i < p$, $1 \leqslant i \leqslant n$, положим

$$B = B(a, b) = \{x = (x_1, \ldots, x_n) \in F_p^n \mid a_i \leqslant x_i < b_i, \ 1 \leqslant i \leqslant n\}.$$

Пусть V — некоторое подмножество в F_p^n и N' — число элементов $x \in V$, представимых в виде $x = y - y'$, $y, y' \in B$, и засчитываемых столько раз, сколько имеется таких представлений. Обозначим $(u, z) = u_1 z_1 + \ldots + u_n z_n$ — скалярное произведение наборов $u = (u_1, \ldots, u_n) \in F_p^n$ и $z = (z_1, \ldots, z_n) \in F_p^n$.

Доказать справедливость соотношения

$$p^n N' = \sum_{x \in V} \sum_{y, y' \in B} \sum_{z \in F_p^n} e^{2\pi i \frac{(x-y+y', z)}{p}}.$$

8*. Пусть $f_1(x), \ldots, f_s(x)$ — многочлены из кольца $F_p[x_1, \ldots, x_n]$, V — множество решений системы

$$f_1(x) = \ldots = f_s(x) = 0$$

в элементах $x = (x_1, \ldots, x_n) \in F_p^n$ и

$$S(V) = \max_{z \neq 0} \left| \sum_{x \in V} e^{2\pi i \frac{(x,z)}{p}} \right|.$$

Пусть, далее, $B = B(0, b)$ и $|A|$ — число элементов множества $A \subset F_p^n$.

Доказать справедливость следующих утверждений:

а) Для числа N' элементов $x \in V$, представимых в виде $x = y - y'$, $y, y' \in B$, и засчитываемых с соответствующими кратностями (см. предыдущую задачу) имеет место неравенство

$$pN' \geqslant |V| \cdot |B|^2 - p^n |B| \cdot S(V).$$

б) Если $f \in F_p[x_1, \ldots, x_n]$, то

$$p^s \sum_{x \in V} e^{2\pi i \frac{f(x)}{p}} = \sum_{x \in F_p^n} \sum_{t \in F_p^s} e^{2\pi i \frac{F(x,t)}{p}},$$

где $F(x, t) = t_1 f_1(x) + \ldots + t_s f_s(x) + f(x)$.

в) Пусть многочлены $f_1, \ldots, f_s$ удовлетворяют условиям:

(I) $2 \leqslant \deg f_i \leqslant m$, $1 \leqslant i \leqslant s$;

(II) система уравнений $f_1 = \ldots = f_s = 0$ определяет абсолютное многообразие в аффинном пространстве $\mathbb{A}^n$ над полем $\overline{F}_p$;

(III) для всех достаточно больших p и всех ненулевых наборов $(t_1, \ldots, t_s) \in F_p^s$ старшая форма $\varphi(x)$ многочлена $t_1 f_1(x) + \ldots + t_s f_s(x)$ определяет неособое проективное многообразие $X \subset \mathbb{P}^{n-1}$.

Тогда

$$S(V) \leqslant (m-1)^n p^{n/2}.$$

(Указание. Воспользоваться соотношением из предыдущего пункта и для каждого ненулевого набора $(t_1, \ldots, t_s) \in F_p^s$ применить оценку Делиня

$$\left| \sum_{x \in F_p^n} e^{2\pi i \frac{F(x,t)}{p}} \right| \leqslant (m-1)^n p^{n/2},$$

где $F(x, t) = t_1 f_1(x) + \ldots + t_s f_s(x) + x_1 z_1 + \ldots + x_n z_n$.)

г) Если N — число решений в элементах $x \in F_p^n$ системы уравнений

$$f_1(x) = \ldots = f_s(x) = 0,$$

представимых в виде $x = y - y'$, $y, y' \in B = (0, b)$, то при любом $\varepsilon > 0$, $p > p_0(\varepsilon)$ и при условии, что

$$|B| > (1+\varepsilon)(m-1)^n p^{s+n/2},$$

выполняется неравенство $N \geqslant 1$.

(Указание. Воспользоваться результатами п. а), в), оценкой Вейля — Ленга, а также тем, что $N > 0$ при $N' > 0$.)

9*. (Майерсон [78]). Пусть многочлены $f_1, \ldots, f_s \in F_p[x_1, \ldots, x_n]$ удовлетворяют условиям (I) — (III) п. в) предыдущей задачи и пусть при любом $\varepsilon > 0$ и $p > p_0(\varepsilon)$ выполнено соотношение

$$\prod_{i=1}^{n} (b_i - a_i) \geqslant (1+\varepsilon)(2m-2)^n p^{s+n/2},$$

где $0 \leqslant a_i < b_i < p$, $1 \leqslant i \leqslant n$. Доказать, что система уравнений

$$f_1(x) = \ldots = f_s(x) = 0$$

имеет решение $x = (x_1, \ldots, x_n) \in F_p^n$, для которого $a_i \leqslant x_i < b_i$ при всех $i = 1, 2, \ldots, n$. В частности, существует решение $x = (x_1, \ldots, x_n)$ указанной системы с условием $0 \leqslant x_i \leqslant 2(1+\varepsilon)^{1/n}(m-1)p^{s/n+1/2}$, $1 \leqslant i \leqslant n$.

(Указание: Пусть $c = (c_1, \ldots, c_n)$ — «центр» параллелепипеда $B = B(a, b)$, где c_i — наибольшее целое, не превосходящее $(a_i + b_i)/2$. Показать, что

$$B - c = \{x \in F_p^n \mid x = y - c,\ y \in B\}$$

содержит множество всех наборов $x \in F_p^n$, представимых в виде $x = y - y'$, где $y, y' \in B'(0, b')$ и $|B'| \geqslant 2^{-n}|B|$. Далее, показать, что система

$$f_1'(x) = \ldots = f_s'(x) = 0,$$

где

$$f_i'(x) = f_i(x + c), \quad 1 \leqslant i \leqslant s,$$

удовлетворяет условиям (I) — (III) задачи 8 и применить к ней результат п. г) задачи 8).

10. Пусть $f(x, y)$ — абсолютно неприводимый многочлен степени $m > 1$ с коэффициентами из поля F_p. Доказать, что если при любом $\varepsilon > 0$ и $p > p_0(\varepsilon)$ выполнено условие

$$(b-a)(d-c) > (1+\varepsilon)(2m-2)^2 p^{3/2},$$

где $0 \leqslant a < b < p$ и $0 \leqslant c < d < p$, то уравнение $f(x, y) = 0$ имеет решение

$(x, y) \in F_p^2$, для которого

$$a \leqslant x < b, \quad c \leqslant y < d.$$

В частности, существует решение (x, y) этого уравнения с условием

$$0 \leqslant x \leqslant 2(1+\varepsilon)^{1/2}(m-1)p^{3/4}, \quad 0 \leqslant y \leqslant 2(1+\varepsilon)^{1/2}(m-1)p^{3/4}.$$

(Указание. Воспользоваться схемой решения задач 8, 9 и оценкой Бомбьери

$$\left| \sum_{\substack{x,y \in F_p \\ f(x,y)=0}} e^{2\pi i \frac{z_1 x + z_2 y}{p}} \right| \leqslant (m-1)^2 p^{1/2},$$

справедливой (см. [17, лемма 4]) для каждого ненулевого набора $(z_1, z_2) \in F_p^2$.)

ГЛАВА VI

ЦЕЛЫЕ ТОЧКИ НА КРИВЫХ И НЕСТАНДАРТНАЯ АРИФМЕТИКА

§ 1. Целые точки на алгебраических кривых

1. Уравнение Туэ. Множество рациональных точек на кривых рода $g=0$ и $g=1$, определенных над $\mathbb{Q}$, может быть как конечным, так и бесконечным (на кривых рода $g=0$ это множество либо пусто, либо бесконечно). Примером кривых рода $g=1$ с конечным числом рациональных точек служат кривые $y^2=x^3+1$ и $x^3+y^3=1$. С другой стороны, кривые $y^2=x^3+3$ (см. задачу 2 из § 2 гл. III) и $x^3+y^3=6$ (см. [43], с. 340) имеют бесконечное число рациональных точек.

Положение в корне меняется, если рассмотреть кривые рода $g>1$, определенные над полем $\mathbb{Q}$. Доказанная в 1983 г. Фалтингсом [125] гипотеза Морделла утверждает, что *на всякой такой кривой лежит лишь конечное число точек с координатами из* $\mathbb{Q}$. На самом деле Фалтингс установил значительно более сильный результат, а именно, что каждая кривая рода $g>1$, определенная над конечным расширением K поля $\mathbb{Q}$, имеет лишь конечное число точек с координатами из всякого конечного расширения L поля K (с историей вопроса и основными идеями этого доказательства читатель может познакомиться по дополнению к русскому переводу книги Ленга [70h], написанному Ю. Г. Зархиным и А. Н. Паршиным). Отметим, что доказательство Фалтингса гипотезы Морделла существенно использует идеи и результаты более ранних работ И. Р. Шафаревича [144a], Дж. Тейта [120a, b], А. Н. Паршина [95a, b, c], С. Ю. Аракелова [4a, b] и Ю. Г. Зархина [53a, b].

Из результата Фалтингса следует, например, что *кривая Ферма*

$$x^n+y^n=1$$

при $n\geqslant 4$ имеет лишь конечное число не только рациональных точек, но также и точек с координатами из любого фиксированного конечного расширения поля $\mathbb{Q}$. В частности, при всяком $n\geqslant 4$ уравнение

$$x^n+y^n=z^n \tag{1}$$

имеет лишь конечное число решений в целых взаимно простых числах x, y и z. Более того, из результата Фалтингса легко следует [135], что предположение Ферма о том, что при $n\geqslant 3$ уравнение (1) не разрешимо в отличных от нуля целых x, y и z, справедливо для «почти всех» показателей n (отношение $N(t)/t$, где $N(t)$ — число тех $n\leqslant t$, для которых теорема Ферма не верна, стремится к нулю при $t\to\infty$).

Для вывода этого утверждения воспользуемся тем, что предположение Ферма достаточно доказать для всех простых чисел $p>2$. Согласно результату Фалтингса для каждого $p>2$ уравнение $x^p+y^p=z^p$ имеет лишь конечное число решений (x, y, z) во взаимно простых целых x, y, z. Обозначим эти решения (x_i, y_i, z_i), $1\leqslant i\leqslant \nu(p)$, и положим

$$H(p)=\max_{1\leqslant i\leqslant \nu(p)} |x_iy_iz_i|.$$

Если u, v, w — взаимно простые целые числа, удовлетворяющие условию $u^{sp}+v^{sp}=w^{sp}$, $uvw\neq 0$, где $s\geqslant 1$ — целое число, то $(u^s, v^s, w^s)=(x_i, y_i, z_i)$ при некотором i, $1\leqslant i\leqslant \nu(p)$, и тогда $|uvw|^s\leqslant H(p)$. Учитывая неравенство $|uvw|\geqslant 2$, приходим к оценке $s\leqslant H(p)$, и заключаем отсюда, что предположение Ферма справедливо для всех показателей $n\equiv 0 \pmod p$ таких, что $n>pH(p)$.

Покажем теперь, что $N(t)\leqslant \varepsilon t$ для любого $\varepsilon>0$ и для всех $t\geqslant t_0(\varepsilon)$. Для этого выберем $\tau=\tau(\varepsilon)$ таким образом, что

$$\prod_{2<p\leqslant\tau}\left(1-\frac{1}{p}\right)<\varepsilon/2,$$

и положим

$$q=\prod_{2<p\leqslant\tau} p, \quad r=r(\varepsilon)=\max_{2<p\leqslant\tau} pH(p).$$

Воспользовавшись решетом Эратосфена, получаем (см. задачу 18 из § 2 гл. I)

$$\begin{aligned}
N(t)&\leqslant r+\#\{n\in\mathbb{Z}\mid r<n\leqslant t,\ (n, q)=1\}\leqslant\\
&\leqslant r+\#\{n\in\mathbb{Z}\mid 1\leqslant n\leqslant t,\ (n, q)=1\}=\\
&=r+\sum_{n\leqslant t}\sum_{d\mid(n,q)}\mu(d)=r+\sum_{d\mid q}\mu(d)\left[\frac{t}{d}\right]\leqslant\\
&\leqslant r+\sum_{d\mid q}\mu(d)\frac{t}{d}+\sum_{d\mid q}1\leqslant\\
&\leqslant r+t\prod_{2<p\leqslant\tau}(1-1/p)+2^{\tau}\leqslant\varepsilon t,
\end{aligned}$$

если только $t\leqslant t_0(\varepsilon)$. Следовательно, $N(t)=o(t)$ при $t\to\infty$.

Доказательство указанного выше результата Фалтингса требует привлечения алгебро-геометрического аппарата, далеко выходящего за рамки данной книги, и поэтому мы ограничимся рассмотрением более простого вопроса о конечности числа целых точек на кривой рода $g\geqslant 1$.

Первый общий результат в задаче о числе целых точек на кривой рода $g\geqslant 1$ был получен в 1909 г. А. Туэ [122], устано-

вившим конечность множества целочисленных решений носящего теперь его имя уравнения

$$f(x, y) = m, \tag{2}$$

где $f \in \mathbb{Z}[x, y]$ — неприводимая форма степени $n \geqslant 3$ и m — отличное от нуля целое число. Доказательство Туэ указанного результата основано на том факте, что алгебраические числа не могут слишком хорошо приближаться рациональными числами. Это свойство алгебраических чисел впервые было обнаружено Лиувиллем [75], который показал, что для заданного алгебраического числа α степени $n \geqslant 3$ и для любых взаимно простых целых чисел p и $q > 0$ выполняется неравенство

$$|\alpha - p/q| > c/q^n,$$

где c — положительная константа, зависящая лишь от α. Туэ значительно усилил оценку Лиувилля, доказав, что при произвольном $\varepsilon > 0$ и $\nu = \frac{n}{2} + 1 + \varepsilon$ справедливо неравенство

$$|\alpha - p/q| > c'/q^{\nu} \tag{3}$$

с некоторой постоянной $c' > 0$, зависящей лишь от α и ε (см. задачу 4).

Вывод результата Туэ о конечности множества целочисленных решений уравнения (2) из оценки (3) весьма прост. Действительно, пусть

$$f(x, y) = a_n y^n \prod_{i=1}^{n} \left(\frac{x}{y} - \alpha_i\right)$$

и (x, y) — целочисленное решение уравнения (2) с достаточно большим значением $|y|$. Без уменьшения общности будем считать, что $y > 0$ и что

$$\left|\alpha_1 - \frac{x}{y}\right| < \ldots < \left|\alpha_n - \frac{x}{y}\right|.$$

Имеем

$$|a_n| \prod_{i=1}^{n} \left|\alpha_i - \frac{x}{y}\right| = \frac{|m|}{y^n}$$

и тогда

$$|\alpha_1 - x/y| \leqslant c''/y^n.$$

Последнее неравенство при достаточно большом y противоречит неравенству (3), и полученное противоречие показывает, что уравнение (2) может иметь лишь конечное число решений в целых числах x и y. Заметим, что постоянная c' в оценке (3) не эффективна. Это связано с тем, что метод Туэ позволяет

установить лишь конечность числа решений неравенства

$$|\alpha - p/q| < 1/q^{\nu},$$

но не дает возможности указать границу для самих решений (p, q) этого неравенства. Поэтому результат Туэ устанавливает лишь конечность множества целочисленных решений уравнения (2), но не приводит к явной границе для самих этих решений. Аналогичным недостатком обладает и указанный выше результат Фалтингса.

Иной, но также неэффективный метод исследования целочисленных решений уравнения (2), при дополнительном условии, что многочлен $f(x, 1)$ имеет хотя бы один комплексный корень, был позже предложен Сколемом [112a]. Этот метод основан на редукции вопроса о количестве целочисленных решений *уравнения Туэ* (2), рассматриваемого как норменное уравнение

$$f(x, y) = \operatorname{norm}(x - \alpha y) = m$$

для неполного модуля $\{x - \alpha y\}$ в поле алгебраических чисел K степени $n \geqslant 3$, к задаче об исследовании целых $\mathfrak{p}$-адических решений $(u_1, \ldots, u_r)$ системы показательных уравнений

$$\operatorname{tr}\left(a_i \zeta_1^{u_1} \ldots \zeta_r^{u_r}\right) = 0, \quad \zeta \leqslant i \leqslant n, \tag{4}$$

где $\mathfrak{p}$ — некоторый простой идеал поля разложения многочлена $f(x, 1)$, a_i — фиксированные элементы этого поля и $\zeta_1, \ldots, \zeta_r$ — основные единицы поля K. При этом бесконечность множества целочисленных решений уравнения (2) равносильна бесконечности множества решений системы (4) в целых числах $u_1, \ldots, u_r$, и идея метода состоит в том, что в некоторых случаях удается установить конечность числа решений системы (4) не только в целых рациональных, но даже в целых $\mathfrak{p}$-адических числах $u_1, \ldots, u_r$. Реализация этой идеи сводится к следующему. Вкладываем $\mathbb{Z}$ в кольцо целых $\mathfrak{p}$-адических чисел $\mathbb{Z}_{\mathfrak{p}}$ и рассматриваем систему (4) как локально-аналитическое многообразие над $\mathbb{Z}_{\mathfrak{p}}$. Из предположения о бесконечности множества целочисленных решений системы (4) и из компактности кольца $\mathbb{Z}_{\mathfrak{p}}$ вытекает, что на локальном многообразии, задаваемом системой (4), должна лежать некоторая аналитическая кривая. Тем самым вопрос о конечности множества целочисленных решений уравнения (2) оказывается равносильным более простому вопросу о неразрешимости системы показательных уравнений в формальных степенных рядах.

С подробным изложением *методов Туэ* и *Сколема* читатель может познакомиться по книгам [127d, гл. 4, 19, гл. 4] (см. также задачи **4** и **13**). Явные верхние границы для числа решений уравнений (2) в целых взаимно простых x и y, зависящие лишь

от m и n, но не зависящие от коэффициентов формы f, были получены в работах [18, 111a и 149].

В 1952 г. А. О. Гельфонд [31a, с. 219—220] указал, что результат Туэ может быть эффективизирован, если только удастся получить достаточно хорошие нижние оценки для модуля линейных форм

$$L_n = x_1 \log \alpha_1 + \ldots + x_n \log \alpha_n$$

от логарифмов алгебраических чисел $\alpha_1, \ldots, \alpha_n$ с коэффициентами $x_1, \ldots, x_n \in \mathbb{Z}$. Такие оценки были получены в 1966 г. А. Бейкером [10a, см. также 10e] и привели к явной границе

$$\max(|x|, |y|) \leqslant c_0 |m|^{\theta} \tag{5}$$

для всех целочисленных решений (x, y) уравнений (2) с эффективно вычислимыми по заданной форме f постоянными c_0 и θ. В свою очередь оценка (5) позволила получить (см. [127b]) эффективное степенное усиление

$$|\alpha - p/q| > c(\alpha, \delta)/q^{n-\delta}$$

неравенства Лиувилля (см. также [127e, гл. 11 и 127d, гл. 9]).

Аналогичный эффективный анализ целочисленных решений $(x, y, z_1, \ldots, z_s)$, $z_1 \geqslant 0, \ldots, z_s \geqslant 0$, допускает и более общее *уравнение Туэ — Малера*

$$f(x, y) = m p_1^{z_1} \ldots p_s^{z_s}, \tag{6}$$

где $p_1, \ldots, p_s$ — фиксированные простые числа (см. [115c, гл. 5]), что приводит к явной границе для решений уравнения Туэ (2) в *квазицелых числах* x и y (рациональных числах, знаменатели которых делятся лишь на простые числа из заданного множества $S = \{p_1, \ldots, p_s\}$.

Все указанные результаты, касающиеся уравнений (2), (6), без труда переносятся на конечные расширения K поля $\mathbb{Q}$ (см. [115c, гл. 5]).

2. Суперэллиптические уравнения. Другой класс неопределенных уравнений, допускающих эффективный анализ, составляют *суперэллиптические уравнения*

$$y^s = f(x), \tag{7}$$

где $s \geqslant 2$ и $f \in \mathbb{Z}[x]$ — многочлен степени $n \geqslant 3$.

Простейшим уравнением такого типа, имеющим собственную глубокую историю (см. [89f]), является эллиптическое уравнение

$$y^2 = x^3 + k. \tag{8}$$

Конечность множества целочисленных решений этого уравнения впервые была установлена Морделлом [89a], связавшим эти решения с целочисленными решениями конечного числа кубических уравнений вида (2) и воспользовавшимся затем результатом Туэ. Явная граница

$$\max(|x|, |y|) < \exp\{10^{10} |k|^{104}\}$$

для целочисленных решений (x, y) уравнения (8) была впервые получена А. Бейкером [10c], а затем усилена Старком [116b]

$$\max(|x|, |y|) < \exp(c(\varepsilon) |k|^{1+\varepsilon}),$$

где $\varepsilon > 0$ — произвольное число, а $c(\varepsilon)$ — эффективно определяется по ε, и В. Г. Спринджуком [115c]

$$\max(|x|, |y|) < \exp\{a|k| (\log(|k| + 1))^6\},$$

где a — эффективно вычислимая абсолютная постоянная (см. также [64]). Тем не менее многие естественные вопросы, связанные с уравнением (8), остаются невыясненными до сих пор. В частности, неизвестно, для каких k это уравнение разрешимо в целых или рациональных x и y.

Явная граница для целых точек на произвольной эллиптической кривой была указана А. Бейкером и Коутесом [11].

Первый шаг в исследовании целочисленных решений *гиперэллиптического уравнения*

$$y^2 = f(x) \tag{9}$$

был сделан Зигелем [54c], доказавшим их конечность в предположении, что многочлен $f(x)$ имеет по меньшей мере три простых корня α_1, α_2 и α_3. Идея Зигеля заключалась в сведении уравнения (9) к конечному числу уравнений Туэ вида

$$ax^3 + by^3 = c \tag{10}$$

над фиксированным конечным расширением K поля $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ и в установлении конечности множества решений этих уравнений Туэ в целых числах поля K. При доказательстве последнего факта Зигель дал обобщение метода Туэ и, в частности, распространил его результат о рациональных приближениях на случай аппроксимации алгебраических чисел алгебраическими же числами из фиксированного конечного расширения поля $\mathbb{Q}$.

Эффективный анализ уравнения (10), проведенный А. Бейкером [10d], позволил ему указать для целочисленных решений (x, y) уравнения (9) явную границу

$$\max(|x|, |y|) < \exp\exp\exp(n^{10n} H), \tag{11}$$

где n — степень и H — высота многочлена $f(x)$ (см. также [10e]). Аналогичным образом была получена (см. [10d]) оценка

$$\max(|x|, |y|) < \exp\exp\exp\left((5s)^{10} n^{10n^3} H^{n^2}\right) \tag{12}$$

для целочисленных решений (x, y) суперэллиптического уравнения (7). Неравенства (11), (12) позже были существенно усилены В. Г. Спринджуком [115a, b] (см. также [115c]).

С другими эффективными результатами в теории диофантовых уравнений читатель может познакомиться по книге Тайдемана и Шори [147].

3. Целые точки на кривых рода $g \geqslant 1$. В 1929 г. Зигель [54a] установил общий результат о конечности числа целых точек на кривой рода $g \geqslant 1$. Рассуждения Зигеля основывались на следующих фундаментальных фактах: во-первых, на полученном им самим усилении и обобщении (см. [54a]) теоремы Туэ о рациональной аппроксимации алгебраических чисел на случай приближения их алгебраическими числами из фиксированного поля и, во-вторых, на известном результате А. Вейля [23a] (см. также [70h, гл. 6]) о конечности ранга группы рациональных точек на кривой рода $g \geqslant 1$, обобщающий соответствующий результат Морделла для случая эллиптических кривых (при $g > 1$ элементами этой группы являются не сами рациональные точки, а некоторые их наборы).

Заметим, что оба эти факта неэффективны и что без их эффективизации метод Зигеля не в состоянии привести к явным границам для координат целых точек на рассматриваемых кривых.

В случае кривых рода 1 результат Зигеля был распространен Малером [79a] на *квазицелые точки* (координаты которых являются квазицелыми числами относительно некоторого заданного множества $S = \{p_1, \ldots, p_s\}$ простых чисел $p_1, \ldots, p_s$).

Широкое обобщение результатов Зигеля и Малера было дано Ленгом [70b] (см. также [70h, гл. 8]) и Левеком [68b], показавшими, что на всякой кривой X рода $g \geqslant 1$, определенной над конечным расширением K поля $\mathbb{Q}$, имеется лишь конечное число *квазицелых K-рациональных точек* (точек с координатами из K, знаменатели которых делятся лишь на простые дивизоры из заданного конечного множества $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Назовем этот общий результат *теоремой Зигеля — Малера* и заметим, что он также неэффективен, как и исходный результат Зигеля.

Несколько позже будет приведено доказательство теоремы Зигеля — Малера, предложенное А. Робинсоном и Рокеттом [105] и основанное на использовании методов нестандартной арифметики. По сравнению с ранее известными доказательствами оно обладает тем преимуществом, что не требует привлечения неэффективного результата А. Вейля о конечности ранга K-рациональных точек на кривой. Тем самым неэффективность теоремы Зигеля — Малера остается связанной лишь с использованием в ее доказательстве неэффективных результатов, касающихся аппроксимации алгебраических чисел алгебраическими числами из заданного конечного расширения поля $\mathbb{Q}$. Другим преимуществом этого доказательства является то, что оно с предельной ясностью раскрывает идейную сторону метода Зигеля.

В заключение параграфа заметим, что в основе построения нестандартной арифметики, которая будет использована нами при

доказательстве теоремы Зигеля — Малера, лежат методы математической логики. Применение таких методов в арифметических вопросах далеко не единичное явление. Подтверждением тому служит новое решение 17-й проблемы Гильберта о представимости всякой положительно определенной над $\mathbb{R}$ или над $\mathbb{Q}$ рациональной функции $f(x_1, \ldots, x_n)$ суммой квадратов рациональных функций, данное А. Робинсоном [104a] с помощью методов нестандартного анализа и существенно отличающееся от первоначального ее решения, предложенного Артином [5b]. Другим примером плодотворности методов математической логики в арифметических задачах является доказательство справедливости (для всех достаточно больших простых p) гипотезы Артина (см. [19, с. 68]) о нетривиальной p-адической представимости нуля заданной p-адической формой степени m от $n < m^2$ переменных ([2], [50a, b]). Еще одним примером может служить работа [155], посвященная конструктивным аспектам теоремы неприводимости Гильберта. Результатом такого слияния алгебры, теории чисел и алгебраической геометрии с математической логикой явилось создание нового направления в математике — теории псевдо-алгебраически замкнутых полей (см. [129]).

Задачи

1. *Степенью* $\deg \alpha$ *алгебраического числа* α называется степень *минимального многочлена* $P \in \mathbb{Z}[x]$ этого числа (многочлена наименьшей положительной степени со взаимно простыми коэффициентами, корнем которого является α). Если старший коэффициент многочлена $P(x)$ равен 1, то α называется *целым алгебраическим числом*.

Пусть α — алгебраическое число степени $n \geqslant 2$, $P(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ — минимальный многочлен числа α и $\alpha^{(2)}, \ldots, \alpha^{(n)}$ — его сопряженные в поле $\mathbb{C}$. Доказать, что для всех взаимно простых целых p и $q > 0$ выполняется неравенство (*неравенство Лиувилля*)

$$|\alpha - p/q| > c/q^n,$$

где

$$c = a_0^{-1} \prod_{i=2}^{n} (1 + |\alpha| + |\alpha^{(i)}|)^{-1}.$$

(Указание. Рассмотреть отличное от нуля целое число

$$m = q^n P(p/q) = q^n a_0 (p/q - \alpha) \prod_{i=2}^{n} (p/q - \alpha^{(i)})$$

и воспользоваться тем, что $|m| \geqslant 1$.)

2. Пусть $1, \alpha_1, \ldots, \alpha_m$ — вещественные алгебраические числа, $x_0, x_1, \ldots, x_m$ — целые числа и $X = \max_{0 \leqslant i \leqslant m} |x_i|$. Доказать, что если степень алгебраического числа

$$\alpha = x_0 + x_1\alpha_1 + \ldots + x_m\alpha_m \neq 0$$

равна n, то справедливо неравенство

$$|\alpha| \geqslant c' X^{1-n},$$

где $c' = c'(\alpha_1, \ldots, \alpha_n)$ — положительная эффективно вычислимая постоянная.

(Указание. Воспользоваться тем, что норма целого алгебраического числа $a\alpha$, $a \in \mathbb{Z}$, удовлетворяет неравенству $|\mathrm{norm}\,(a\alpha)| \geqslant 1$).

3. Обобщение теоремы Лиувилля. Пусть $m < n$ — положительные целые числа и $\alpha_1, \ldots, \alpha_m$ — вещественные алгебраические числа, причем $1, \alpha_1, \ldots, \alpha_m$ — линейно независимы над полем $\mathbb{Q}$ и степень поля $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ над $\mathbb{Q}$ равна n. Доказать, что существует такая эффективно вычислимая постоянная $c'' = c''(\alpha_1, \ldots, \alpha_m) > 0$, что при всех взаимно простых целых $p_1, \ldots, p_m$ и $q > 0$ выполняется неравенство

$$\max_{1 \leqslant i \leqslant m} |\alpha_i - p/q| \geqslant c''/q^{-n/m}.$$

(Указание. Положить

$$c'' = \min\left(\frac{1}{6m}, \frac{c'}{m3^n}\right),$$

где c' — эффективная константа из предыдущей задачи, и предположить, что

$$|\alpha_i - p_i/q| < c''q^{-n/m}$$

для всех $i = 1, 2, \ldots, m$. Положить затем $X = [2q^{1/m}] + 1$ и с помощью принципа «ящиков Дирихле» установить существование отличных в совокупности от нуля целых чисел $x_0, x_1, \ldots, x_m$, не превосходящих по абсолютной величине X и таких, что

$$|x_0 + x_1\alpha_1 + \ldots + x_m\alpha_m| < X^{-m}.$$

При отличном от нуля целом

$$a = x_0q + x_1p_1 + \ldots + x_mp_m$$

прийти к противоречию с неравенством $|a| \geqslant 1$, а при $a = 0$ — с оценкой

$$|x_0 + x_1\alpha_1 + \ldots + x_m\alpha_m| \geqslant c'X^{1-n}$$

из предыдущей задачи.)

4*. (Туэ [122], Н. И. Фельдман [127d]). *Высотой* $H(f)$ *и длиной* $L(f)$ *многочлена*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$$

назовем величины

$$H(f) = \max_{0 \leqslant i \leqslant n} |a_i|, \quad L(f) = \sum_{i=0}^{n} |a_i|,$$

а *высотой* $H(\alpha)$ и *длиной* $L(\alpha)$ *алгебраического числа* α — высоту и длину минимального многочлена этого числа. Пусть α — целое алгебраическое число степени $n \geqslant 3$, ε — произвольное положительное число и $\nu = \frac{n}{2} + 1 + \varepsilon$. Пусть, далее, m — положительное целое число, $0 < \delta < n/2$ и

$$M = \left[m\left(\frac{n}{2} + \delta - 1\right)\right].$$

Доказать справедливость следующих утверждений:

а) Существует эффективная постоянная $A = A(\alpha, \delta) > 0$; отличные в совокупности от нуля целые a_{ij}, $0 \leqslant i \leqslant M$, $0 \leqslant j \leqslant n-1$, не превосходящие по абсолютной величине A^m и многочлены $f, g \in \mathbb{Z}[x]$, $h \in \mathbb{Z}[x, \alpha]$

с условиями $\deg f \leqslant m + M$, $\deg g \leqslant m + M$, $\deg h \leqslant M$, $L(f) \leqslant A^m$, $L(g) \leqslant A^m$ такие, что

$$\alpha f(x) - g(x) = (x - \alpha)^m \sum_{i=0}^{M} \left(\sum_{j=0}^{n-1} a_{ij}\alpha^j\right) x^i = (x - \alpha)^m h(x, \alpha).$$

(Указание. Выбрать отличные в совокупности от нуля целые a_{ij} такими, чтобы выполнялось неравенство

$$\max(|a_{ij}|) \leqslant B^m,$$

где $B = B(\alpha, \delta)$ — эффективная постоянная, и чтобы коэффициенты многочлена

$$(x - \alpha)^m h(x, \alpha) = \sum_{k=0}^{m+M} \sum_{l=0}^{n-1} \left(\sum_{i=0}^{M} \sum_{j=0}^{n-1} b_{ijkl}a_{ij}\right) x^k\alpha^l$$

при всех произведениях $x^k\alpha^l$, $0 \leqslant k \leqslant m + M$, $2 \leqslant l \leqslant n - 1$, обращались в нуль. Для этого нетривиальным образом разрешить в целых a_{ij} ($|a_{ij}| \leqslant B^m$) систему из $r = (n-2)(m + M + 1)$ целочисленных линейных уравнений

$$\sum_{i=0}^{M} \sum_{j=0}^{n-1} b_{ijkl}a_{ij} = 0, \quad 0 \leqslant k \leqslant m + M, \quad 2 \leqslant l \leqslant n - 1,$$

относительно $s = n(M + 1) > r$ неизвестных a_{ij}.)

б) Если σ, τ — неотрицательные, p и $q > 0$ — взаимно простые целые числа и

$$P_{\sigma,\tau} = \det \begin{Vmatrix} f^{(\sigma)} & g^{(\sigma)} \\ f^{(\tau)} & g^{(\tau)} \end{Vmatrix} \in \mathbb{Z}[x],$$

где f, g — многочлены из п. а), то среди чисел

$$P_{\sigma,\tau}(p/q), \qquad 0 \leqslant \sigma, \tau < [2m\delta + n - 1]$$

имеется хотя бы одно отличное от нуля.

(Указание. Воспользоваться соотношениями

$$\alpha f - g = (x - \alpha)^m h, \quad \alpha f' - g' = (x - \alpha)^{m-1} h^*$$

и установить, что

$$P_{0,1} = \det \begin{Vmatrix} f & g \\ f' & g' \end{Vmatrix} = P^{m-1}Q,$$

где P — минимальный многочлен числа α и $Q \in \mathbb{Z}[x]$ — отличный от нуля многочлен степени не выше $2m\delta - n - 2$. Далее, воспользоваться формулой Лейбница для производной от произведения и показать, что

$$P_{0,1}^{(\mu)} = \sum_{\rho=0}^{\mu} \binom{\mu}{\rho} P_{\rho,\mu-\rho+1}.$$

Наконец, предположив, что $P_{\sigma,\tau}(p/q) = 0$ для всех $\sigma, \tau = 0, 1, \ldots, [2m\delta + n - 1]$, прийти к противоречию с тем, что $Q(x) \not\equiv 0$.)

в) Если $|q\alpha - p| < 1$, $0 \leqslant s \leqslant [2m\delta + n - 1]$ и (в обозначениях п. а))

$$a_s = q^{m+M-s}f^{(s)}(p/q)(s!)^{-1}, \qquad b_s = q^{m+M-s}g^{(s)}(p/q)(s!)^{-1},$$

то

$$|a_s| \leqslant Cq^{m(\delta+n/2)}, \quad |b_s| \leqslant Cq^{m(\delta+n/2)}$$

и

$$|a_s\alpha - b_s| \leqslant D^m q^M |q\alpha - p|^{m-2m\delta-n+1},$$

где C, D — эффективные положительные постоянные, зависящие лишь от α и δ.

г) Существуют такие эффективные положительные константы q_0 и ω, зависящие лишь от α и ε, что если неравенство

$$|\alpha - p/q| < q^{-\nu}$$

разрешимо в целых взаимно простых $p = p_1$ и $q = q_1 > q_0$, то оно не разрешимо в целых взаимно простых $p = p_2$ и $q = q_2 > q_1^{\omega}$.

(Указание. Взять

$$\delta = \varepsilon(4n + 4 + 8\varepsilon)^{-1}, \quad q_0 = \max(C^{1/\varepsilon}, D^{1/\varepsilon}),$$
$$\omega = (2 + (n-1)(n + 2\varepsilon))(4 + 2\varepsilon)\varepsilon^{-1}$$

и предположить, вопреки утверждению, что p_1/q_1 и p_2/q_2 — решения неравенства $|\alpha - p/q| < q^{-\nu}$. Затем, воспользовавшись результатом п. б), найти целые σ_0, τ_0, $0 \leqslant \sigma_0$, $\tau_0 \leqslant [2m\delta + n - 1]$, для которых $P_{\sigma_0,\tau_0}(p_1/q_1) \neq 0$, и вывести отсюда, что хотя бы одно из целых чисел

$$a_{\sigma_0}p_2 - b_{\sigma_0}q_2, \quad a_{\tau_0}p_2 - b_{\tau_0}q_2$$

отлично от нуля. Наконец, обозначив s соответствующее из чисел σ_0, τ_0 и воспользовавшись результатом предыдущего пункта, показать, что

$$|a_s p_2 - b_s q_2| \leqslant q_2 |a_s\alpha - b_s| + |a_s| \cdot |q_2\alpha - p_2| \leqslant q_2^{\theta_1} + q_2^{\theta_2},$$

где

$$\theta_1 < -\frac{\log 2}{\log q_2}, \quad \theta_2 < -\frac{\log 2}{\log q_2}.$$

Затем прийти к противоречию с неравенством

$$|a_s p_2 - b_s q_2| \geqslant 1.)$$

д) Неравенство

$$|\alpha - p/q| < q^{-\nu}$$

имеет лишь конечное число решений в целых взаимно простых числах p и $q > 0$.

(Указание. Воспользоваться результатом предыдущего пункта.)

е) Теорема Туэ. *Если α' — алгебраическое число степени $n \geqslant 3$, то неравенство*

$$|\alpha' - p/q| < q^{-\nu}$$

имеет лишь конечное число решений в целых взаимно простых p и $q > 0$.

(Указание. Воспользоваться тем, что если $Q'(x) = b_0x^n + b_1x^{n-1} + \ldots + b_n$ — минимальный многочлен числа α', то $\alpha = b_0\alpha'$ — целое алгебраическое число. Затем применить к α результат предыдущего пункта.)

5. Пусть $f \in \mathbb{Z}[x, y]$ — неприводимая форма степени $n \geqslant 3$ и $g \in \mathbb{Z}[x, y]$ — произвольный многочлен степени $m < \frac{n}{2} - 1$. Доказать, что уравнение

$$f(x, y) = g(x, y)$$

имеет лишь конечное число решений в целых числах x и y.

6. Пусть $m \in \mathbb{Z}$ и $f \in \mathbb{Z}[x, y]$ — форма степени $n \geqslant 2$, обладающая свойством, что среди корней многочлена $f(x, 1)$ нет вещественных. Вывести эффективную верхнюю границу для модулей целочисленных решений x и y уравнения

$$f(x, y) = m.$$

7. Доказать справедливость следующего обобщения теоремы Туэ. *Пусть $f \in \mathbb{Z}[x, y]$ — форма степени $n \geqslant 3$, причем*

$$f(x, y), \neq \delta(\alpha x + \beta y)^n,$$

где $\alpha, \beta, \delta \in \mathbb{Z}$, и

$$f(x, y) \neq d(ax^2 + bxy + cy^2)^{n/2},$$

где $a, b, c, d \in \mathbb{Z}$, $b^2 > 4ac$ и $n = 2k$. Тогда при любом целом $m \neq 0$ уравнение

$$f(x, y) = m$$

имеет лишь конечное число решений в целых числах x и y.

(Указание. Разложить $f(x, y)$ на неприводимые в кольце $\mathbb{Z}[x, y]$ множители

$$f(x, y) = A\prod_{i=1}^{s} f_i(x, y), \quad A \in \mathbb{Z},$$

и рассмотреть следующие возможные случаи:

1) $f = d(ax^2 + bxy + cy^2)^{n/2}$, $b^2 < 4ac$;

2) среди неприводимых форм $f_i \in \mathbb{Z}[x, y]$ есть:

а) формы степени $n' \geqslant 3$;

б) две непропорциональные линейные формы $\alpha x + \beta y$ и $\alpha' x + \beta' y$;

в) две непропорциональные формы второй степени

$$ax^2 + bxy + cy^2 \quad \text{и} \quad a'x^2 + b'xy + c'y^2;$$

г) линейная форма $\alpha x + \beta y$ и форма второй степени $ax^2 + bxy + cy^2$.)

8. Пусть $m \neq 0$ — целое число и

$$f(x, y) = a_0\prod_{i=1}^{n}(x - \alpha_i y) \in \mathbb{Z}[x, y].$$

Воспользовавшись результатом задачи 7, показать, что если среди чисел $\alpha_1, \ldots, \alpha_n$ есть три различных, то уравнение

$$f(x, y) = m$$

имеет лишь конечное число решений $x, y \in \mathbb{Z}$.

9*. Пусть k и m — отличные от нуля целые числа. Доказать, что для каждого целого $n \geqslant 3$ уравнение

$$x^2 - k = my^n$$

имеет лишь конечное число решений в целых числах x и y.

(Указание. Если $\sqrt{k} = l \in \mathbb{Z}$ и (x, y) — целочисленное решение уравнения

$$x^2 - k = my^n,$$

то, исходя из соотношения

$$(x + l)(x - l) = my^n,$$

установить, что

$$x + l = Ar^n, \quad x - l = Bs^n, \quad r, s \in \mathbb{Z},$$

где A и B — целые числа, все простые делители которых входят в

каноническое разложение числа $2lm$. Вывести отсюда, что

$$x+l=au^n, \quad x-l=bv^n, \quad u, v\in\mathbb{Z},$$

где целые a и b принимают лишь конечное число значений для всех рассматриваемых решений (x, y). Затем, воспользовавшись результатом задачи 8, показать, что при любых фиксированных a и b уравнение

$$au^n-bv^n=2l$$

имеет лишь конечное число решений в целых u и v.

Если $\sqrt{k}=\theta\notin\mathbb{Z}$ и (x, y) — целочисленное решение уравнения

$$x^2-k=my^n,$$

то, переходя в равенстве

$$(x+\theta)(x-\theta)=my^n$$

к целым дивизорам квадратичного поля $K=\mathbb{Q}(\theta)$, получить соотношения

$$(x+\theta)=\mathfrak{a}\mathfrak{b}^n, \quad (x-\theta)=\mathfrak{a}'\mathfrak{b}'^n,$$

где $\mathfrak{a}$ и $\mathfrak{a}'$ делят $(2\theta m)^{n-1}$. Затем, воспользовавшись существованием такого целого дивизора $\mathfrak{c}$, что $\mathfrak{b}\mathfrak{c}=(\alpha)$ и $N\mathfrak{c}\leqslant c_0(\theta)$, где $N\mathfrak{c}$ — норма дивизора $\mathfrak{c}$ и $c_0>0$ — эффективная константа (см. [19, с. 246]), прийти к равенствам

$$x+\theta=(A+B\theta)(u+v\theta)^n, \quad x-\theta=(A-B\theta)(u-v\theta)^n,$$

где $qA, qB, u, v\in\mathbf{Z}$ и $q=(N\mathfrak{c})^n$ — положительное целое число. Показать, что для всех целочисленных решений (x, y) уравнения

$$x^2-k=my^n$$

рациональные числа A, B принимают лишь конечное число значений. Исключив из полученных равенств x, получить конечное число уравнений

$$\frac{(a+b\theta)(u+v\theta)^n-(a-b\theta)(u-v\theta)^n}{\theta}=2q$$

и установить, что их левые части представляют собой формы от u, v степени n с коэффициентами из $\mathbb{Z}$. Показать, что при $b=0$ каждое целочисленное решение (u, v) любого из этих уравнений удовлетворяет условию $|v|\leqslant 2q$. Доказать, наконец, что при $b\neq 0$ многочлен

$$P(z)=(a+b\theta)(z+\theta)^n-(a-b\theta)(z-\theta)^n$$

не имеет кратных корней, и воспользовавшись результатом предыдущей задачи показать, что каждое из указанных уравнений имеет лишь конечное число решений в целых u и v).

10. Доказать, что если a и m — отличные от нуля целые числа, то при всяком целом $n\geqslant 3$ уравнение

$$ax^2+bx+c=my^n$$

имеет лишь конечное число решений в целых числах x и y.

(Указание. Предположив существование целочисленного решения (x, y) рассматриваемого уравнения, свести задачу к исследованию целочисленных решений уравнения $x'^2-k=m'y'^n$).

11. Доказать справедливость следующего результата Полиа [97b]: *если a, b, c — целые числа и $a\neq 0$, $b^2-4ac\neq 0$, то наибольший простой делитель $P[f(x)]$ значений многочлена $f(x)=ax^2+bx+c$ при целых x стремится к бесконечности вместе с x.*

(Указание. Предположить, что для бесконечной последовательности целочисленных значений x выполняется равенство $f(x)=\pm p_1^{\nu_1}\dots p_s^{\nu_s}$,

где $p_1, \dots, p_s$ — фиксированные простые числа, и прийти к противоречию с результатом предыдущей задачи).

12. Пусть m, n — заданные целые положительные числа и $n\neq 2^s$. Доказать справедливость следующих утверждений:

а) Уравнение

$$x^n+y^n=mp^z$$

имеет лишь конечное число решений в положительных взаимно простых числах $x, y\in\mathbb{Z}$, простых числах p и целых числах z.

(Указание. Ограничиться рассмотрением случая, когда n — нечетное простое число. Предположив, что решений (x, y, p, z) бесконечно много, и воспользовавшись разложением

$$x^n+y^n=(x+y)(x^{n-1}-x^{n-2}y+\dots-xy^{n-2}+y^{n-1}),$$

показать, что

$$x+y=m_1p^{z_1}, \quad x^{n-1}-x^{n-2}y+\dots-xy^{n-2}+y^{n-1}=m_2p^{z_2}.$$

Затем, положив $\nu=\min(z_1, z_2)$ и рассмотрев сравнения

$$x+y\equiv 0 \pmod{p^\nu}, \quad x^{n-1}-x^{n-2}y+\dots-xy^{n-2}+y^{n-1}\equiv 0 \pmod{p^\nu},$$

прийти к противоречию с тем, что

$$n\not\equiv 0 \pmod{p^\nu}$$

для достаточно большого модуля p^ν.)

б) Если p фиксированное простое число, то уравнение

$$x^n+y^n=mp^z$$

имеет лишь конечное число решений в целых x, y, z с условием $(x, y)=1$.

13*. Пусть $\alpha_1, \dots, \alpha_n, \lambda_1, \dots, \lambda_n$ — алгебраические числа, причем ни одно из отношений α_i/α_j при $i\neq j$ не является корнем из 1, и $K=\mathbb{Q}(\alpha_1, \dots, \alpha_n, \lambda_1, \dots \lambda_n)$. Пусть, далее, p — нечетное простое число, не делящее ни одно из чисел α_i; $\mathfrak{p}$ — простой дивизор поля K, делящий p; $|\ |_\mathfrak{p}$ — определяемая этим дивизором $\mathfrak{p}$-адическая норма поля K; $K_\mathfrak{p}$ — пополнение поля K по норме $|\ |_\mathfrak{p}$; $\overline{\mathbb{Q}}_p$ — алгебраическое замыкание поля p-адических чисел $\mathbb{Q}_p$ и Ω_p — пополнение поля $\overline{\mathbb{Q}}_p$ по p-адической норме $|\ |_p$. Поле $K_\mathfrak{p}$ содержит $\mathbb{Q}_p$ и имеет над ним конечную степень. Следовательно, поле $K_\mathfrak{p}$ изоморфно вкладывается в Ω_p и норма $|\ |_\mathfrak{p}$ совпадает с нормой $|\ |_p$, индуцированной этим вложением (см. задачи **11—13** из § 1 гл. V). Используя локальный метод Сколема, доказать, что показательное уравнение

$$\lambda_1\alpha_1^x+\dots+\lambda_n\alpha_n^x=0$$

имеет лишь конечное число решений в целых числах x.

(Указание. Пусть $\mathfrak{p}^e$ — максимальная степень простого дивизора $\mathfrak{p}$, делящая p, и $N=(N\mathfrak{p})^e-(N\mathfrak{p})^{e-1}$, где $N_\mathfrak{p}$ — норма дивизора $\mathfrak{p}$. Тогда для любого $\alpha\in K$, взаимно простого с $\mathfrak{p}$, $\alpha^N\equiv 1 \pmod{\mathfrak{p}^e}$, и значит, $|\alpha^N-1|_p<p^{-1}$. Поэтому определен p-адический логарифм $\log\alpha^N$ числа α^N и для всех $t\in\Omega_p$ с условием $|t|_p\leqslant 1$ определена p-адическая функция

$$\alpha^{Nt}=\exp(t\log\alpha^N).$$

Предположить, что уравнение

$$\lambda_1\alpha_1^x+\dots+\lambda_n\alpha_n^x=0$$

имеет бесконечно много решений в целых x и, полагая $x = Nt + y$, $0 \leqslant y < N$, переписать его в виде

$$\mu_1\beta_1^t + \ldots + \mu_n\beta_n^t = 0,$$

где $\mu_i = \lambda_i\alpha_i^y$ и $\beta_i = \alpha_i^N$. При заданном y рассмотреть левую часть последнего уравнения как аналитическую функцию от переменного $t \in \Omega_p$, имеющую по предположению бесконечное число нулей в круге $|t|_p \leqslant 1$. Показать, что при указанных ограничениях на α_i эта функция не равна тождественно нулю, и прийти к противоречию с тем, что отличная от нуля p-адическая аналитическая функция не может иметь в ограниченном круге бесконечно много нулей.)

§ 2. Алгебраические системы и модели

Данный и последующий параграфы включены в книгу лишь ради полноты изложения и предназначаются читателю, не знакомому с нестандартным анализом. В них разъясняются основные принципы нестандартного подхода в математике и приводятся результаты, которые в дальнейшем будут использованы при нестандартном доказательстве теоремы Зигеля — Малера. Основу этого доказательства составляет факт существования нестандартного расширения $^*K$ заданного поля алгебраических чисел K. Чтобы не слишком загромождать идейную сторону, ограничимся построением нестандартных расширений $^*\mathbb{N}$ и $^*\mathbb{R}$, соответственно, множества неотрицательных целых чисел $\mathbb{N}$ и поля действительных чисел $\mathbb{R}$. Для построения нестандартного расширения $^*K$ поля алгебраических чисел K достаточно внести необходимые изменения в используемом при этом формальном языке L. Нестандартный анализ берет свое начало от юношеской мечты Лейбница о построении универсального исчисления, охватывающего все разделы классической математики. В частности, Лейбниц предполагал, что *система действительных чисел $\mathbb{R}$ может быть расширена до некоторой новой системы $^*\mathbb{R}$, содержащей в себе бесконечно малые величины и обладающей тем свойством, что она наследует истинность всех утверждений, справедливых* $\mathbb{R}$. При этом он трактовал бесконечно малые величины не как функции, стремящиеся к нулю, а как «идеальные числа», обладающие теми же свойствами, что и конечные числа (см. [69, с. 166, 192]). Однако, в такой широкой формулировке принцип Лейбница приводит к явным противоречиям. Например, при переходе от $\mathbb{R}$ к $^*\mathbb{R}$ нарушается аксиома Архимеда (*для каждого $x \in \mathbb{R}$ существует такое $n \in \mathbb{N}$, что $x < n$*). Действительно, если $\varepsilon > 0$ — бесконечно малое число, то для всех $n \in \mathbb{N}$ должны иметь $n\varepsilon < 1$ или, что то же самое, $\varepsilon^{-1} > n$. Аналогичным образом, при расширении $\mathbb{R}$ до $^*\mathbb{R}$ нарушается свойство полной упорядоченности и аксиома полноты множества $\mathbb{R}$ (см. задачу 3). Стало быть, *всякое расширение поля действительных чисел $\mathbb{R}$, содержащее бесконечно малые величины, с необходимостью должно быть неархимедовым* (см. задачи 2, 8).

Само по себе построение собственного неархимедова расширения поля действительных чисел $\mathbb{R}$, содержащего некоторые бесконечно малые величины, не представляет особого труда. Примером такого расширения является поле рациональных функций $\mathbb{R}(\varepsilon)$ от некоторого бесконечно малого элемента ε (см. задачу 8). Однако поле $\mathbb{R}(\varepsilon)$ обладает одним весьма существенным недостатком — оно содержит слишком мало функций, наследующих определенные свойства класса всех функций действительного переменного x. Следовательно, поле $\mathbb{R}(\varepsilon)$ менее всего подходит на роль расширения $^*\mathbb{R}$, которое «наследует истинность всех утверждений, справедливых в $\mathbb{R}$». Действительно, чтобы максимальным образом обеспечить выполнимость последнего условия, нужно иметь такое неархимедово расширение $^*\mathbb{R}$ поля $\mathbb{R}$, при котором каждая функция $f\colon \mathbb{R} \to \mathbb{R}$ допускает некоторое естественное продолжение до функции $^*f\colon {}^*\mathbb{R} \to {}^*\mathbb{R}$, сохраняющей определенные свойства исходной функции f.

Построение расширения $^*\mathbb{R}$ поля действительных чисел $\mathbb{R}$ обладающего всеми необходимыми свойствами, впервые было осуществлено А. Робинсоном [104b] в 1961 г. В результате этого построения (почти 300 лет спустя) принцип Лейбница получил, наконец, строгую математическую формулировку. Построенное А. Робинсоном неархимедово расширение $^*\mathbb{R}$ поля $\mathbb{R}$ стало называться *нестандартным расширением* этого поля (или *полем гипердействительных чисел*), а возникшее при этом новое направление в математике, базирующееся на понятиях и методах математической логики, получило название «*нестандартный анализ*».

Основу нестандартного анализа составляет теория моделей (изучающая связь между формальными языками и алгебраическими системами) и, в частности, *теорема компактности А. И. Мальцева* (см. п. 5).

При этом весьма существенными являются следующие два обстоятельства:

1) все утверждения классического анализа выразимы в формальном языке математической логики;

2) подавляющее большинство утверждений математического анализа выразимо в логике первого порядка (см. заключительную часть данного параграфа).

Ввиду теоремы компактности Мальцева все утверждения обычного математического анализа, выразимые в логике первого порядка, остаются справедливыми и в неархимедовом расширении $^*\mathbb{R}$ поля $\mathbb{R}$. Однако распространение с $\mathbb{R}$ на $^*\mathbb{R}$ предложений, выразимых в логиках высших порядков (таких как свойство полной упорядоченности или аксиома полноты), связано с весьма значительными трудностями. Чтобы преодолеть их, А. Робинсон предложил для формального анализа предложений в языке высшего порядка использовать язык первого порядка (не до-

пускаются кванторы $\forall x$ и $\exists y$, а допускаются только ограниченные кванторы, например, $\forall x \in \mathbb{R}$ и $\exists y \in \mathbb{N}$). При таком подходе свойства поля $\mathbb{R}$, выразимые в логике первого порядка, переносятся на ${}^*\mathbb{R}$ без изменений, а свойства, выразимые в логике высших порядков, переносятся на ${}^*\mathbb{R}$ с тем ограничением, что преобразованные кванторы $\forall$ и $\exists$ действуют лишь на так называемых *внутренних множествах*. Это привело к следующему уточнению принципа Лейбница: *существует неархимедово расширение* ${}^*\mathbb{R}$ *поля действительных чисел* $\mathbb{R}$, *содержащее в себе бесконечно малые элементы и обладающее теми же свойствами, выразимыми в формальном языке математической логики, что и исходное поле* $\mathbb{R}$. Поскольку среди действительных чисел нет бесконечно малых, из этого уточнения принципа Лейбница следует, что свойство быть бесконечно малым не может быть выражено в формальном языке математической логики, или, как будем говорить в дальнейшем, множество бесконечно малых элементов является *внешним подмножеством* ${}^*\mathbb{R}$. Следует подчеркнуть, что в сформулированном только что принципе речь идет лишь о сохранении формального смысла предложений. Содержательный смысл высказываний при переходе от $\mathbb{R}$ к ${}^*\mathbb{R}$ может существенно измениться. Например, аксиома Архимеда «*для каждого* $x \in \mathbb{R}$ *существует такое* $n \in \mathbb{N}$, *что* $x < n$» преобразуется в высказывание «*для каждого* $x \in {}^*\mathbb{R}$ *существует такое* $n \in {}^*\mathbb{N}$, *что* $x < n$», которое уже не будет аксиомой Архимеда для ${}^*\mathbb{R}$, а означает просто, что для каждого элемента $x \in {}^*\mathbb{R}$ найдется превосходящее его *гипернатуральное число* $n \in {}^*\mathbb{N}$. Поэтому при перенесении высказываний с поля $\mathbb{R}$ на ${}^*\mathbb{R}$ нужна особая осторожность.

Поле $\mathbb{R}^*$ вполне оправдывает свое название, поскольку оно устроено весьма нестандартно. Оно содержит множество гипернатуральных чисел ${}^*\mathbb{N}$ и является упорядоченным неархимедовым полем (см. задачи **9—16**). Множество $^*F = \{x \in {}^*\mathbb{R} \mid |x| < n$ для некоторого $n \in \mathbb{N}\}$ конечных элементов поля ${}^*\mathbb{R}$, где $|x| = \max(x, -x)$, является подкольцом этого поля, содержащим в себе $\mathbb{R}$, а множество $^*I = \{x \in {}^*\mathbb{R} \mid x = 0$ или $x^{-1} \in {}^*\mathbb{R} - {}^*F\}$ бесконечно малых элементов поля ${}^*\mathbb{R}$ является максимальным идеалом кольца $^*F$. Поле действительных чисел $\mathbb{R}$ изоморфно факторкольцу $^*F/{}^*I$, так что каждое действительное число x входит в ${}^*\mathbb{R}$ (при отождествлении $\mathbb{R}$ с $^*F/{}^*I$) вместе с целым классом $x + {}^*I$ бесконечно близких к нему чисел, называемым (из уважения к Лейбницу) *монадой* числа x. При этом монады различных действительных чисел x и y не пересекаются между собой. Таким образом, при микроскопическом рассмотрении гипердействительной прямой ${}^*\mathbb{R}$ оказывается, что наряду с каждой точкой $x \in \mathbb{R}$ эта прямая содержит целый (бесконечный) класс бесконечно близких к ней точек.

Ознакомившись со строением «в малом», посмотрим на его строение «в большом». Назовем два гипердействительных числа x и y эквивалентными, если их разность $x - y$ есть конечное число. Это отношение эквивалентности разбивает множество гипердействительных чисел ${}^*\mathbb{R}$ на непересекающиеся классы, которые естественно назвать *галактиками*. Каждая галактика представляет собой объединение бесконечного числа монад. Одну из галактик (которую естественно назвать нашей) составляют конечные гипердействительные числа $^*F$. Каждая из галактик расположена на гипердействительной прямой ${}^*\mathbb{R}$ целиком по одну сторону от другой. Между любыми двумя галактиками находится третья (а значит, бесконечно много других галактик). Среди галактик нет ни «самой левой», ни «самой правой» (если галактика G содержит x, а $\omega \in {}^*\mathbb{R} - {}^*F$ — бесконечно большое положительное число, то $x + \omega$ лежит в галактике, расположенной правее G, а $x - \omega$ лежит в галактике, расположенной левее G).

С более детальным обсуждением необычайной структуры гипердействительной прямой ${}^*\mathbb{R}$ читатель может познакомиться по книге В. А. Успенского [124].

Построение нестандартного расширения ${}^*\mathbb{R}$ поля $\mathbb{R}$ наиболее естественно, по-видимому, проводить на основе теоремы компактности А. И. Мальцева. В данной книге предпочтение отдается другому пути, базирующемуся на понятии *ультрапроизведения* (см. [113а, гл. 3]) и требующему самых минимальных сведений из математической логики. Опущенные в изложении детали читатель может восстановить либо самостоятельно, либо по книге [40b].

1. Суперструктуры. При построении нестандартного расширения поля $\mathbb{R}$ удобно использовать тот факт, что все математические объекты и отношения между ними могут быть истолкованы на языке теории множеств. Перечислим, не вдаваясь в подробности, основные понятия этой теории, которые нам потребуются в дальнейшем (существование всех рассматриваемых множеств гарантировано принимаемой неявно расширенной системой аксиом Цермело — Френкеля *ZFC*; см. [113b, гл. 1 и 51, гл. 2]).

Пустое множество $\varnothing$ является единственным множеством, не содержащим элементов. Мы будем (ради удобства) рассматривать также и другие объекты, не содержащие элементов (а значит, не являющиеся множествами). Эти объекты (см. ниже) называются *индивидами*.

Для любого множества X совокупность его подмножеств

$$P(X) = \{Y \mid Y \subset X\}$$

назовем *множеством-степенью* множества X. Упорядоченный набор объектов $x_1, \ldots, x_n$ в дальнейшем будем обозначать $\langle x_1, \ldots, x_n \rangle$. Для любых двух множеств X и Y определим их

декартово произведение $X \times Y$ как

$$X \times Y = \{\langle x, y\rangle \mid x \in X,\ y \in Y\}$$

и положим

$$X^n = \{\langle x_1, \ldots, x_n\rangle \mid x_i \in X,\ 1 \leqslant i \leqslant n\}.$$

Конечное множество, состоящее из элементов $x_1, \ldots, x_n$, обозначим $\{x_1, \ldots, x_n\}$.

Если $R \subset X \times Y$, то R называется *отношением* (в случае $X = Y$ оно называется отношением на X). Иногда вместо $\langle x, y\rangle \in R$ употребляется запись $R(x, y)$. Под *областью определения* $D(R)$ *отношения* R понимается множество всех x таких, что $R(x, y)$ для некоторого y. Если $f \subset X \times Y$ — отношение и для каждого $x \in X$ существует в точности один элемент $y \in Y$ такой, что $\langle x, y\rangle \in f$, то f называется *отображением множества* X в Y, или *функцией* с областью определения X и значениями в Y. При этом элемент $y \in Y$ обозначаем $f(x)$. Если $Z \subset X$, то полагаем

$$f(Z) = \{f(x) \mid x \in Z\}$$

и называем $f(Z)$ *образом множества* Z при отображении f. При $f(X) = Y$ отображение f называется отображением X на Y; если же $f(x) = f(y)$ влечет $x = y$, то f называется *взаимно однозначным отображением*.

Если f отображает X^n в Y, то f называется *функцией от* n *аргументов* (или n-*местной* функцией) с областью определения X^n и значениями в Y (обозначение: $f(x_1, \ldots, x_n)$).

Введем теперь понятие *предиката*, т. е. функции $R(x_1, \ldots, x_n)$, значениями которой являются высказывания об упорядоченных наборах $\langle x_1, \ldots, x_n\rangle$. Для этого рассмотрим «особое» двухэлементное множество $Y = \{0, 1\}$, где 1 — истина, а 0 — ложь, и определим на нем операции *конъюнкции* $\wedge$; *дизъюнкции* $\vee$, *импликации* $\Rightarrow$ и *отрицания* $\neg$ обычным образом:

y_1	y_2	$y_1 \wedge y_2$	$y_1 \vee y_2$	$y_1 \Rightarrow y_2$	$\neg y_1$
1	1	1	1	1	0
1	0	0	1	0	0
0	1	0	1	1	1
0	0	0	0	1	1

Функцию $R(x_1, \ldots, x_n)$, определенную на множестве X^n со значениями в $Y = \{0, 1\}$, назовем n-*местным предикатом* на X^n. С теоретико-множественной точки зрения предикат определяется заданием множества $R \subset X^n$. При этом $R(x_1, \ldots, x_n)$ понимается как высказывание: *упорядоченный набор* $\langle x_1, \ldots, x_n\rangle$ *принадлежит* R. В соответствии с этим вместо $R(x_1, \ldots, x_n)$ часто

употребляется запись $\langle x_1, \ldots, x_n\rangle \in R$. Предикат $R(x_1, \ldots, x_n)$ при $n = 1$ называется *свойством*, а при $n > 1$ — *отношением*. С исчислением предикатов читатель может познакомиться по книге [93b]. Простейшим примером предиката является обычное отношение $<$ на множестве положительных целых чисел; имеем

$$(1 < 2) = 1, \quad (3 < 2) = 0, \quad (1 < 2) \wedge (3 < 2) = 0,$$
$$(1 < 2) \vee (3 < 2) = 1.$$

Символ $=$ будем рассматривать как символ двухместного предиката, определенного на любом множестве.

Всюду в дальнейшем $\mathbb{N}$ обозначает множество неотрицательных целых чисел. Иногда область определения функции называется *индексным множеством* и вместо функции говорится об *индексированном семействе*. Следовательно, индексированное семейство с индексным множеством I — это отображение X с областью определения I. В этом случае для каждого $i \in I$ вместо $X(i)$ пишем X_i, а само индексированное семейство обозначаем $\{X_i \mid i \in I\}$. Если индексным множеством является $\mathbb{N}$, то индексированное семейство называется *последовательностью*. Если $\{X_i \mid i \in I\}$ — индексированное семейство множеств, то

$$\bigcup_{i \in I} X_i, \quad \bigcap_{i \in I} X_i, \quad \prod_{i \in I} X_i$$

обозначают соответственно *объединение*, *пересечение* и *декартово произведение* семейства.

Определение 1. Пусть I — некоторое непустое множество. Тогда $F \subset P(I)$ называется *фильтром* на I, если

1) $X \in F$, $Y \in P(I)$ и $X \subset Y$ влечет $Y \in F$;
2) $X, Y \in F$ влечет $X \cap Y \in F$;
3) $\varnothing \notin F$, $I \in F$.

Из условия 2) следует, что пересечение любого конечного числа элементов фильтра также принадлежит фильтру.

Пример 1. Пусть $X \subset I$ и $X \neq \varnothing$. Тогда семейство

$$F = \{Y \in P(I) \mid X \subset Y\}$$

является фильтром на I.

Определение 2. Фильтр F на I называется *ультрафильтром*, если из включения $F \subset F'$, где F' — также фильтр на I, следует $F = F'$.

Пример 2. Пусть $X = \{x\}$ для некоторого $x \in I$. Тогда семейство

$$F = \{Y \in P(I) \mid X \subset Y\}$$

является ультрафильтром (называемым *тривиальным*).

Справедливо следующее утверждение, являющееся слабой формой аксиомы выбора (см. [113b, гл. 2]).

Предложение 1. *Если F' — фильтр на I, то существует ультрафильтр F на I такой, что $F' \subset F$.*

Определение 3. Пусть F — ультрафильтр на I. Положим

$$\mu_X = \mu_F(X) = \begin{cases} 1, & \text{если } X \in F, \\ 0, & \text{если } X \notin F, \end{cases}$$

и назовем отображение μ множества $P(I)$ в множество $\{0, 1\}$ *мерой, порожденной ультрафильтром F.*

Очевидно, что $\mu(\varnothing) = 0$, $\mu(I) = 1$ и что $\mu(X_1 \cup \ldots \cup X_n) = 0$, если $\mu(X_i) = 0$ для каждого $i = 1, 2, \ldots, n$.

Нестандартный подход к решению задач начинается с выбора подходящего *множества индивидов* S. Так, множество S может быть множеством действительных чисел, множеством точек топологического пространства, множеством элементов поля алгебраических чисел K и так далее. По техническим причинам полезно считать, что объекты из S не являются множествами, т. е. если $x \in S$, то утверждение $y \subset x$ ложно и $P(x) = \varnothing$.

Пусть S — некоторое множество индивидов. Расширим S до такого множества, которое включало бы в себя все множества, необходимые для изучения S. Для этого определим сначала иерархию

$$S_0 = S, \quad S_{n+1} = S_n \cup P(S_n), \quad n \in \mathbb{N}.$$

Затем положим

$$\widehat{S} = \bigcup_{n \in \mathbb{N}} S_n$$

и назовем $\widehat{S}$ *суперструктурой* с индивидами S. Каждый элемент из S называется индивидом суперструктуры $\widehat{S}$, а каждый элемент разности $\widehat{S} - S$ — множеством в $\widehat{S}$. Заметим, что $\varnothing \subset S$, так что $\varnothing \in \widehat{S}$.

Определение 4. Множество $X \subset \widehat{S}$ называется *транзитивным в $\widehat{S}$* (или просто *транзитивным*), если для любого $x \in X$ либо $x \in S$, либо $x \subset X$.

Транзитивность X в $\widehat{S}$ эквивалентна тому, что из $x \in X - S$ и $y \in x$ следует $y \subset X$. Нетрудно видеть, что каждое множество S_n транзитивно в $\widehat{S}$. Суперструктура $\widehat{S}$ обладает также следующими свойствами:

1) *если X, $Y \in \widehat{S} - S$ и f — отображение X в Y, то $f \in \widehat{S}$, $f(x) \in \widehat{S}$ для каждого $x \in X$ и $f(Z) \in \widehat{S}$ для каждого $Z \subset X$;*

2) *если I, $Y \in \widehat{S} - S$ и $X_i \in Y$ для каждого $i \in I$, то*

$$\bigcup_{i \in I} X_i \in \widehat{S} \text{ и } \prod_{i \in I} X_i \in \widehat{S}.$$

2. Стандартный и нестандартный универсумы. Пусть S — некоторое множество индивидов. Основой для дальнейшего будет служить понятие универсума.

Определение 5. Подмножество U множества $\widehat{S}$ называется *универсумом* с индивидами S, если

1) $\varnothing \in U$;
2) $S \subset U$;
3) если x, $y \in U$, то $\{x, y\} \in U$;
4) U транзитивно в $\widehat{S}$.

Из сказанного в предыдущем пункте легко следует, что *суперструктура $\widehat{S}$ является универсумом с индивидами S.*

Пусть x, $y \in \widehat{S}$. Если существует единственное $z \in \widehat{S}$, для которого $\langle y, z \rangle \in x$, то положим $x \restriction y = z$; в противном случае положим $x \restriction y = \varnothing$. Операция $\restriction$ обладает следующими свойствами:

1) *если f — функция с областью определения $D(f)$ и $y \in D(f)$, то $f \restriction y = f(y)$;*

2) *$x \restriction y \in \widehat{S}$ для всех x, $y \in \widehat{S}$.*

Далее, транзитивность универсума U приводит к следующему свойству замкнутости: если x, $y \in U$, то $\langle x, y \rangle \in U$ и $x \restriction y \in U$.

Суперструктуру $\widehat{S}$ назовем *стандартным универсумом*. Покажем как можно построить другой универсум (называемый *нестандартным универсумом*), индивиды которого включают S и чьи свойства тесно связаны со свойствами $\widehat{S}$. Для этой цели выберем некоторое непустое индексное множество I и рассмотрим меру μ, порожденную ультрафильтром F на I. Скажем, что некоторое свойство выполняется *для почти всех $i \in I$*, если множество элементов i, для которых оно истинно, имеет меру 1. В конструкции, которая будет предложена, используются функции f, отображающие I в $\widehat{S}$. Положим $f_i = f(i)$ и для каждого $n \in \mathbb{N}$ обозначим V_n множество таких f, что $f_i \in S_n$ для почти всех $i \in I$. Далее, положим $V = \bigcup_{n \in \mathbb{N}} V_n$ и заметим, что имеется естественное вложение стандартного универсума $U = \widehat{S}$ в V, при котором элемент $f \in \widehat{S}$ отождествляется с «постоянной» функцией, такой что $f_i = f$ для всех $i \in I$. Если f, $g \in V_0$ и $f_i = g_i$ для почти всех $i \in I$, то будем писать $f \sim g$. Легко видеть, что отношение «$\sim$» является отношением эквивалентности на V (и, в частности, на V_0).

Для каждого $f \in V_0$ положим

$$\bar{f} = \{g \in V_0 \mid g \sim f\}$$

и обозначим

$$W = \{\bar{f} \mid f \in V_0\}$$

множество непересекающихся между собой классов эквивалент-

ности, на которые разбивается отношением «$\sim$» множество V_0. В силу естественного вложения $\widehat{S}$ в V можно отождествить каждый элемент $x \in S$ с соответствующим элементом $\bar{x} \in W$. Таким образом, можно считать, что $S \subset W$.

Определим теперь универсум $^*U$ с индивидами W, который назовем *нестандартным универсумом*. Для этого построим сначала суперструктуру $\widehat{W}$:

$$W_0 = W,\ W_{n+1} = W_n \cup P(W_n),\ n \in \mathbb{N},\quad \widehat{W} = \bigcup_{n \in \mathbb{N}} W_n,$$

а затем каждому элементу $f \in V_n$ сопоставим некоторый элемент $\bar{f} \in W_n$. Множество таких элементов $\bar{f}$ обозначим $^*U$, и для их определения воспользуемся индукцией по n. Элемент $\bar{f}$ был уже определен для каждого $f \in V_0$, причем таким образом, что $\bar{f} \in W = W_0$. Пусть $\bar{f}$ определен для каждого $f \in V_n$, $n \geqslant 0$, таким образом, что $\bar{f} \in W_n$. Тогда для $f \in V_{n+1} - V_n$ положим $\bar{f} = \{\bar{g} \mid g \in V_n$ и $g_i \in f_i$ для почти всех $i = I\}$. В силу предположения имеем $\bar{g} \in W_n$ для каждого $\bar{g} \in \bar{f}$, и тогда $\bar{f} \subset W_n$. В таком случае, $\bar{f} \in W_{n+1}$ и, тем самым, получаем индуктивное определение элементов $\bar{f} \in W_n$ для всех $n \in \mathbb{N}$ с условием, что $f \in V_n$ влечет $\bar{f} \in W_n$. Положим, наконец,

$$^*U = \{\bar{f} \mid f \in V\}$$

и назовем $^*U$ *нестандартным универсумом*, соответствующим $U = \widehat{S}$. Важно отметить, что $^*U$ зависит не только от U, но также от индексного множества I и ультрафильтра F. Несколько позже увидим, что $^*U$ на самом деле является универсумом.

При естественном вложении $\widehat{S} \subset V$ каждому элементу $f \in \widehat{S}$ соответствует элемент $\bar{f} \in {}^*U$. Элементы $\bar{f}$, для которых $f \in \widehat{S}$, называются *стандартными элементами* $^*U$. Остальные элементы универсума $^*U$ (если они существуют) называются *нестандартными элементами*. В частности, *стандартными индивидами* являются в точности элементы множества S, а *нестандартными индивидами* — элементы разности $W - S$.

Легко видеть, что если $f,\ g \in V$ и $h_i = \{f_i,\ g_i\}$ для каждого $i \in I$, то $h \in V$ и $\bar{h} = \{\bar{f},\ \bar{g}\}$. Более того, $^*U$ транзитивно в $\widehat{W}$ и, в таком случае, множество $^*U$ является универсумом с индивидами W.

Нетрудно убедиться, что *если* $f,\ g \in V$, *то*:

1) $\bar{f} \in \bar{g}$ *тогда и только тогда, когда* $f_i \in g_i$ *для почти всех* $i \in I$;

2) $\bar{f} = \bar{g}$ *тогда и только тогда, когда* $f_i = g_i$ *для почти всех* $i \in I$.

Кроме того, *если* $h \in V$, *то*:

3) $\bar{h} = \langle \bar{f},\ \bar{g} \rangle$ *в том и только в том случае, когда* $h_i = \langle f_i,\ g_i \rangle$ *для почти всех* $i \in I$.

Наконец, *если* $f,\ g \in V$ *и* $h_i = f_i \restriction g_i$ *для почти всех* $i \in I$, *то*:

4) $h \in V$ *и* $\bar{h} = \bar{f} \restriction \bar{g}$.

3. Алгебраические системы. Для каждого универсума U построим теперь язык L_U, который необходим для формулировок утверждений, касающихся U.

Основу каждого языка составляют *логические связки* $\wedge$ (и), $\vee$ (или), $\neg$ (не), $\Rightarrow$ (влечет), $\Leftrightarrow$ (если и только если), *символ равенства* $=$, *кванторы* $\forall$ (для всех), $\exists$ (существует), а также бесконечная последовательность переменных $x,\ y,\ z,\ \ldots$ и круглые скобки ( ), необходимые для однозначного прочтения формул.

Кроме этих логических символов можно ввести множество L *функциональных, предикатных* и *константных символов*. Например, язык $L = \{+,\ 0\}$ абелевых групп содержит функциональный символ $+$ и константный символ 0; язык $L = \{\in\}$ теории множеств содержит лишь предикатный символ $\in$ и не имеет функциональных и константных символов.

Каждому функциональному символу $f \in L$ и каждому предикатному символу $R \in L$ поставим в соответствие неотрицательное целое число $\#(f)$ и $\#(R)$. Если $m = \#(f)$, то f называется *m-местным функциональным символом*; если $n = \#(R)$, то R называется *n-местным предикатным символом*. Например, имеем $\#(+) = \#(\in) = 2$.

Если дан язык L, то имеется естественное понятие алгебраической системы для языка L. Под алгебраической системой $\mathfrak{M}$ понимается непустая совокупность объектов M, которая является областью действия кванторов, вместе с интерпретацией основных предикатных, функциональных и константных символов из L.

Определение 7. *Алгебраической системой* для языка L называется пара $\mathfrak{M} = \langle M,\ \theta \rangle$, где M — непустое множество и θ — отображение с областью определения L (будем писать x' вместо $\theta(x)$) такое, что:

1) если $R \in L$ — n-местный предикатный символ, то $R' \subset M^n$;

2) если $f \in L$ — n-местный функциональный символ, то $f'\colon M^n \to M$;

3) если $c \in L$ — константный символ, то $c' \in M$.

Константный символ c, соответствующий объекту c', назовем *именем* объекта c'. Обычно будем опускать штрих у f, R, c, и применять слегка путающую практику использования одной и той же буквы для обозначения символов языка L и их интерпретаций в M.

Пример 3. Алгебраическая система $\mathfrak{G} = \langle G,\ +,\ 0 \rangle$, где G — некоторое непустое множество, является абелевой группой.

Пример 4. Алгебраическая система $\mathfrak{N} = \langle \mathbb{N},\ +,\ \cdot,\ 0,\ 1 \rangle$, где $\mathbb{N}$ — множество неотрицательных целых чисел, а $\cdot$ суть операция умножения, называется *арифметикой*.

Обратимся к синтаксическим понятиям языка L. Всякая конечная последовательность, элементами которой являются основные символы языка L, называются *выражениями*. Из множества выражений выделим те, которым можно придать смысл.

Определение 7. *Термы* языка L есть наименьшее множество выражений, содержащее переменные x, y, z, ..., все константные символы и замкнутое относительно следующего правила образования: если t_1, ..., t_n — термы языка L и если $f \in L$ — n-местный функциональный символ, то выражение $f(t_1, \ldots, t_n)$ также является термом. Терм, не содержащий переменных, называется *замкнутым термом*.

Например, выражения

$$(x+y), \quad (x+0), \quad ((x+y)+0)$$

являются термами языка $L = \{+, 0\}$.

Если в L нет функциональных символов, то правило образования бессодержательно и множество термов состоит только из переменных и константных символов.

Определение 8. *Атомная формула* языка L — это выражение одного из следующих двух типов:

$$(t_1 = t_2) \quad \text{и} \quad R(t_1, \ldots, t_n),$$

где t_1, ..., t_n — термы языка L, а $R \in L$ — произвольный n-местный предикатный символ.

Например, выражения

$$x = y, \quad x \in y$$

являются атомными формулами языка $L = \{\in\}$. В языке $L = \{+, 0\}$ абелевых групп предикатных символов нет и поэтому атомными формулами являются лишь утверждения о равенстве термов, например, выражения

$$(x+y=z), \quad (x+y=y+x), \quad (x+y)+z=x+(y+z).$$

Определение 9. *Формулы первого порядка* языка L есть наименьшее множество выражений, содержащее атомные формулы и замкнутое относительно следующего правила образования:

1) если φ и ψ — формулы, то выражения

$$\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \Rightarrow \psi)$$

также являются формулами;

2) если φ — формула и x — переменная, то $(\exists x)\varphi$ и $(\forall x)\varphi$ также являются формулами.

Например, выражения

$$(x+y=0), \quad (\exists y(x+y=0)), \quad (\forall x(\exists y(x+y=0)))$$

являются формулами языка $L = \{+, 0\}$ абелевых групп.

Определение 10. Множество $F(\varphi)$ *свободных переменных* формулы φ определяется следующим образом:

1) если φ — атомная формула, то $F(\varphi)$ есть в точности множество переменных, входящих в φ;

2) $F(\neg\varphi) = F(\varphi)$;

3) $F(\varphi \wedge \psi) = F(\varphi \vee \psi) = F(\varphi \Rightarrow \psi) = F(\varphi) \cup F(\psi)$;

4) $F(\exists x\varphi) = F(\forall x\varphi) = F(\varphi) - \{x\}$.

Например, в формуле $(x+y=0)$ обе переменные x и y — свободные; в формуле $(\exists y(x+y=0))$ свободной переменной является лишь x; в формуле $(\forall x(\exists y(x+y=0)))$ свободных переменных вообще нет.

Определение 11. Формулы, не содержащие свободных переменных, называются *высказываниями* в L.

Например, формула

$$(X \neq \varnothing) \vee (\exists x \in X)(x = x)$$

представляет собой высказывание «X есть множество», а формула (X есть множество) $\wedge$ (Y есть множество) $\wedge$ $(\forall x \in Y)(x \in X)$ представляет собой высказывание «Y есть подмножество X».

До сих пор термы, формулы и высказывания в L являлись конечными совокупностями символов. Чтобы придать высказываниям определенный смысл (задать семантику для языка L), свяжем их с алгебраическими системами при помощи отношения выполнимости $\mathfrak{M} \models \varphi$.

Пусть $\mathfrak{M} = \langle M, \cdot \rangle$ — алгебраическая система для языка L. *Интерпретацией* в $\mathfrak{M}$ назовем функцию s с областью определения, равной множеству переменных языка L, и областью значений, равной некоторому подмножеству из M. Будем понимать s как приписывание значения $s(x)$ переменной x. Значит, для каждого терма t языка L можно определить функцию t', отображающую интерпретации s на элементы множества M.

Определение 12. Пусть $\mathfrak{M}$ — алгебраическая система. Для терма t языка L определим t' следующим образом:

1) если t — константный символ c, то $t'(s) = c'$ для всех s;

2) если t переменная x, то $t'(s) = s(x)$ для всех s;

3) если t — терм $f(t_1, \ldots, t_n)$, то

$$t'(s) = f'(t_1'(s), \ldots, t_n'(s))$$

для всех s.

Пример 5. Пусть $L = \{+, \cdot, 0, 1\}$ — язык колец и $t = x^2 + 2x + 1$ — терм этого языка. Тогда t' для любого кольца $\mathfrak{R}$ есть функция из L в $\mathfrak{R}$. Если $s(x) = a$, то $t'(s) = a^2 + 2a + 1$.

В последующем определении мы используем символ $s\binom{a}{x}$ для обозначения интерпретации s', которая совпадает с s, за исключением $s'(x) = a$.

Определение 13. Пусть $\mathfrak{M} = \langle M, \cdot \rangle$ — алгебраическая система для языка L. Для всех интерпретаций s и всех формул φ определим отношение

$$\mathfrak{M} \vDash \varphi[s]$$

(читается: формула φ истинна в $\mathfrak{M}$ при интерпретации s) следующим образом:

1) $\mathfrak{M} \vDash (t_1 = t_2)\,[s]$ равносильно $t_1'(s) = t_2'(s)$;

2) $\mathfrak{M} \vDash R(t_1, \ldots, t_n)\,[s]$ равносильно $(t_1'(s), \ldots, t_n'(s)) \in R'$;

3) $\mathfrak{M} \vDash \neg \varphi\,[s]$ равносильно тому, что неверно $\mathfrak{M} \vDash \varphi\,[s]$;

4) $\mathfrak{M} \vDash (\varphi \wedge \psi)\,[s]$ равносильно $\mathfrak{M} \vDash \varphi\,[s]$ и $\mathfrak{M} \vDash \psi\,[s]$;

5) $\mathfrak{M} \vDash (\varphi \vee \psi)\,[s]$ равносильно $\mathfrak{M} \vDash \varphi\,[s]$ или $\mathfrak{M} \vDash \psi\,[s]$;

6) $\mathfrak{M} \vDash (\varphi \Rightarrow \psi)\,[s]$ равносильно тому, что или не выполняется $\mathfrak{M} \vDash \varphi\,[s]$, или $\mathfrak{M} \vDash \psi\,[s]$;

7) $\mathfrak{M} \vDash (\exists x \varphi)\,[s]$ равносильно существованию $a \in M$ такого, что $\mathfrak{M} \vDash \varphi\left[s\begin{pmatrix} a \\ x \end{pmatrix}\right]$;

8) $\mathfrak{M} \vDash (\forall x \varphi)\,[s]$ равносильно тому, что для всех $a \in M$ имеет место $\mathfrak{M} \vDash \varphi\left[s\begin{pmatrix} a \\ x \end{pmatrix}\right]$.

Заметим, что в 1) знак $=$ использован в двух различных смыслах, а именно, в качестве действительного равенства $t_1'(s) = t_2'(s)$ и в качестве символа для равенства в формуле $(t_1 = t_2)$. Такое неоднозначное использование знака $=$ не должно привести к недоразумениям.

Нетрудно видеть, что справедливость $\mathfrak{M} \vDash \varphi\,[s]$ зависит только от значений $s(x)$ для переменных, которые действительно свободны в φ. Это означает, что если $s(x) = s'(x)$ для всех x, свободных в φ, то $\mathfrak{M} \vDash \varphi\,[s]$ тогда и только тогда, когда $\mathfrak{M} \vDash \varphi\,[s']$. Таким образом, если $\varphi = \varphi(x_1, \ldots, x_n)$ и $a_1 = s(x_1), \ldots, a_n = s(x_n)$, то вместо $\mathfrak{M} \vDash \varphi\,[s]$ можно без смущения писать $\mathfrak{M} \vDash \varphi(a_1, \ldots, a_n)$. Точно так же, если φ — высказывание, то истинность или ложность $\mathfrak{M} \vDash \varphi\,[s]$ совершенно не зависит от s. Поэтому будем писать

$$\mathfrak{M} \vDash \varphi$$

(читается: $\mathfrak{M}$ является *моделью* для φ), если $\mathfrak{M} \vDash \varphi\,[s]$ для какой-либо интерпретации s.

Определение 14. Алгебраическая система $\mathfrak{M}$ является *моделью множества высказываний* Φ, если $\mathfrak{M} \vDash \varphi$ для всех $\varphi \in \Phi$.

Если даны две алгебраические системы $\mathfrak{M}$ и $\mathfrak{N}$ для языка L, то они называются *элементарно эквивалентными* (записывается: $\mathfrak{M} \equiv \mathfrak{N}$), в том и только в том случае, если $\mathfrak{M} \vDash \varphi$ равносильно $\mathfrak{N} \vDash \varphi$ для всех высказываний φ языка L. В случае изоморфизма $\mathfrak{M} \simeq \mathfrak{N}$ имеем $\mathfrak{M} \equiv \mathfrak{N}$.

В заключение параграфа дадим краткое описание спектра логик, используемых в математических теориях. Задание логики равносильно заданию синтаксиса и семантики языка L. Пусть $\mathfrak{M} = \langle M, \cdot \rangle$ — алгебраическая система для языка L. Логика первого порядка является самой слабой логикой, в которой, в частности, кванторы $\forall$ и $\exists$ всегда действуют только на элементах множества M. Логика второго порядка разрешает одному из кванторов действовать на подмножествах множества M и на функциях F, отображающих, скажем, $M \times M$ в M. Логика третьего порядка разрешает использовать кванторы по множествам функций и т. д. Слабая логика второго порядка разрешает использовать кванторы по конечным подмножествам множества M и по натуральным числам.

Выразительная сила языка логики первого порядка достаточно велика и имеются всякие основания рассматривать логику первого порядка в качестве основного языка математики (согласно *тезису Гильберта* вся классическая математика выразима в логике первого порядка; см. [113а, гл. 1, § 5]).

4. Принцип перманентности. Для каждого универсума U построим соответствующий язык L_U, взяв в качестве предикатного символа $\in$, в качестве функциональных символов $\langle\ \rangle$, $\restriction$ и в качестве константных символов элементы некоторого множества M, взаимно однозначно соответствующего U. Для каждого константного символа $c \in M$ обозначим c' соответствующий ему элемент универсума U и назовем c *именем* элемента c' (в тех случаях, когда позволяет ситуация, будем опускать штрих у c, и для обозначения элемента из U и его имени будем употреблять одну и ту же букву c).

Рассмотрим U как алгебраическую систему для языка L_U и для выражения истинности высказывания φ в U воспользуемся записью $U \vDash \varphi$ (если φ ложно в U, то будем писать $U \nvDash \varphi$). Если t — замкнутый терм языка L_U, то $t' = t(s)$ обозначим его образ при интерпретации s и назовем t' *значением терма* t в U.

Более конкретно, определим значение t' следующим образом:

1) если t — константный символ c, то положим $t' = c'$ для всех $c \in U$;

2) $(\langle t_1, t_2 \rangle)' = \langle t_1', t_2' \rangle$;

3) $(t_1 \restriction t_2)' = t_1' \restriction t_2'$.

Это позволяет определить t' рекурсией по длине терма t (по числу вхождений в t функциональных символов $\langle\ \rangle$ и $\restriction$). Включение $t' \in U$ следует из результатов п. 2 и индукции по длине терма t. Поскольку t' — множества, то для них имеет смысл предикатный символ $\in$.

Определим теперь по рекурсии отношение $U \vDash \varphi$ для высказываний φ в языке L_U:

1) $U \vDash (t_1 = t_2) \Leftrightarrow t_1' = t_2'$;

2) $U \vDash (t_1 \in L_2) \leftrightarrow t_1' \in t_2'$;
3) $U \vDash \neg\varphi \Leftrightarrow$ не верно, что $U \vDash \varphi$;
4) $U \vDash (\varphi \wedge \psi) \leftrightarrow U \vDash \varphi$ и $U \vDash \psi$;
5) $U \vDash (\exists x_i \in t)\,\varphi(x_i) \leftrightarrow U \vDash \varphi(c)$ для некоторого $c' \in t'$.

Это определение представляет собой рекурсию относительно общего числа вхождений в высказывание символов $\neg$, $\wedge$ и $\exists$. Заметим, что поскольку мы имеем дело с высказываниями, то t_1, t_2 в 1), 2) и t в 5) должны быть замкнутыми терминами (для которых определены их значения t_1', t_2' и t'). Заметим, кроме того, что при задании семантики языка L_U можно ограничиться лишь символами $=, \in, \neg, \wedge, \exists, (\ ), \langle\ \rangle, \mid$. Остальные символы $\vee, \Rightarrow, \Leftrightarrow, \forall$ могут быть получены из $\neg$, $\wedge$ и $\exists$.

Формулы в L_U могут быть использованы не только для формулировок утверждений об универсуме U, но также для определения подмножеств U.

Определение 15. Пусть $X \subset U$. Тогда X называется *определимым подмножеством* U, если существует формула $\varphi = \varphi(x)$, содержащая свободную переменную x такая, что

$$X = \{c' \in U \mid U \vDash \varphi(c)\}.$$

В этом случае φ называется *определением* X в языке L_U.

В дальнейшем будем рассматривать ровно два универсума: стандартный универсум $U = S$ и нестандартный универсум $^*U$. Положим $L_U = L$, $L_{^*U} = {}^*L$ и вместо $U \vDash \varphi$, $^*U \vDash \varphi$ будем писать (ради краткости) $\vDash\varphi$, $^* \vDash \varphi$. Если φ формула в L, то $^*\varphi$ будем обозначать формулу в $^*L$, полученную из φ заменой каждого константного символа, входящего в φ, на соответствующий константный символ $\bar{c}$ (мы используем тот факт, что $\bar{c}'$ является стандартным элементом $^*U$ при каждом $c' \in U$). Если, в частности, $c' \in S$ для каждого c, входящего в φ, то $^*\varphi = \varphi$ (в этом случае φ является формулой как в L, так и в L).

В данном пункте будет показано, что всякое математическое утверждение относительно U, формализованное в языке L, имеет интерпретацию в $^*U$ и что эта интерпретация истинна в $^*U$ тогда и только тогда, когда исходное утверждение истинно в U. Отсюда следует, что алгебраические системы U и $^*U$ элементарно эквивалентны и что нестандартный универсум $^*U$ можно рассматривать как модель для множества высказываний, истинных в $L = L_U$. Назовем $^*U$ *нестандартной моделью* для L. Наиболее существенным для дальнейшего является то обстоятельство, что в формулах языка L нами не допускаются кванторы $\forall x$ (для всех x) и $\exists y$ (существует y), а допускаются только *ограниченные кванторы* (выражения вида $(\forall x \in y)\,\varphi(x)$ и $(\exists x \in y)\,\varphi(x)$, являющиеся сокращениями для формул $\forall x (x \in y \Rightarrow \varphi(x))$ и $\exists x (x \in y \wedge \varphi(x))$; см. п. 5 в определении отношения $U \vDash \varphi$).

В дальнейшем будем считать, что в формуле $\varphi(x_1, \ldots, x_n)$ явно указаны лишь свободные переменные $x_1, \ldots, x_n$.

Теорема 1 [76]. *Пусть* $\varphi = \varphi(x_1, \ldots, x_n)$, $n \geqslant 0$, — *формула в* L *и пусть* $f_1, \ldots, f_n \in V$. *Тогда*

$$^* \vDash {}^*\varphi(\bar{f}_1, \ldots, \bar{f}_n)$$

в том и только в том случае, когда

$$\vDash \varphi(f_{i1}, \ldots, f_{in})$$

для почти всех $i \in I$.

Доказательство этого результата основано на индукции по числу вхождений в формулу φ символов $\neg$, $\wedge$ $\exists$ и приведено в книге [40b]. Обсуждение теоремы 1 в более широком контексте можно найти в книгах [113а, гл. 3] и [12].

Важным частным случаем теоремы 1 является случай $n = 0$, приводящий к следующему утверждению.

Принцип перманентности. *Пусть* φ — *высказывание в* L. *Тогда* $^* \vDash {}^*\varphi$ *в том и только в том случае, когда* $\vDash\varphi$.

Принцип перманентности является одним из основных инструментов нестандартного анализа. Математическая теорема, эквивалентная $\vDash\varphi$ (φ — некоторое высказывание в L) может быть доказана путем проверки того, что $^* \vDash {}^*\varphi$. Заметим, что если φ содержит только константные символы c при $c' \in S$, то принцип перманентности допускает более простую форму: $^* \vDash \varphi \Leftrightarrow \vDash \varphi$. Из принципа перманентности вытекает, что если $\varphi(x)$ и $\psi(x)$ — формулы в L, причем

$$\{c' \in U \mid \vDash \varphi(c)\} = \{c' \in U \mid \vDash \psi(c)\},$$

то

$$\{c' \in {}^*U \mid {}^* \vDash {}^*\varphi(c)\} = \{c' \in {}^*U \mid {}^* \vDash {}^*\psi(c)\}.$$

Этот факт может быть использован для задания следующей важной операции на определимых множествах.

Пусть $X = \{c' \in U \mid \vDash \varphi(c)\}$, где φ — формула в L. Положим

$$^*X = \{c' \in {}^*U \mid {}^* \vDash {}^*\varphi(c)\}$$

и заметим, что $^*X$ не зависит от частной формулы φ, используемой для определения X, а зависит только от множества X.

В частности, поскольку

$$U = \{c' \in U \mid \vDash (c = c)\}$$

— определимое множество, мы имеем

$$^*(U) = \{c' \in {}^*U \mid {}^* \vDash (c = c)\} = {}^*U,$$

что оправдывает введенное ранее обозначение $^*U$ для нестандартного универсума. Аналогичным образом, для каждого $n \in \mathbb{N}$ имеем $^*(U - S_n) = {}^*U - {}^*S_n$ и $^*x = \bar{x}$ для всякого $x \in (U - S)$. Поэтому в дальнейшем вместо $\bar{x}$ почти всегда будем использовать обозначение $^*x$. Для полноты положим $^*x = x$ при $x \in S$ и заметим, что стандартными элементами универсума $^*U$ являются в точности элементы вида $^*x$ при $x \in U$.

Нетрудно убедиться, что введенная операция обладает следующими свойствами:

1) *если* $X \subset S$, *то* $X \subset {}^*X$ *и* ${}^*X \cap S = X$;

2) *если* $x, y \in U$, *то* $x = y \Leftrightarrow {}^*x = {}^*y$, $x \in y \Leftrightarrow {}^*x \in {}^*y$, ${}^*\langle x, y\rangle = \langle {}^*x, {}^*y\rangle$ и ${}^*(x \restriction y) = ({}^*x \restriction {}^*y)$;

3) *если* X, Y *определимые подмножества* U, *то* ${}^*(X \cup Y) = {}^*X \cup {}^*Y$, ${}^*(X \cap Y) = {}^*X \cap {}^*Y$ *и* ${}^*(X - Y) = {}^*X - {}^*Y$;

4) ${}^*\varnothing = \varnothing$, ${}^*\{x_1, \ldots, x_n\} = \{{}^*x_1, \ldots, {}^*x_n\}$ *и* ${}^*U = \bigcup\limits_{n \in \mathbb{N}} {}^*S_n$.

5. **Теорема направленности.** Хотя нами в достаточной степени развита техника нестандартного анализа, мы даже не показали еще, что имеет место строгое включение $S \subset W$ (если $S = W$, то ${}^*U = U$). Легко видеть, что без дополнительных предположений относительно индексного множества I нельзя исключить вырожденный случай $S = W$.

Выберем в качестве I достаточно большое множество (чтобы обеспечить строгое включение $S \subset W$ в случае бесконечного множества S и тем самым гарантировать существование нестандартных элементов, достаточно положить $I = S$ и задать на I какой-либо нетривиальный ультрафильтр). Ключевым понятием при этом является понятие направленности.

Определение 16. Отношение $R \in U$ называется *направленным*, если для всяких $x_1, \ldots, x_n \in D(R)$ найдется такой элемент x, что $\langle x_i, x\rangle \in R$ при всех $i = 1, 2, \ldots, n$.

Справедливо следующее утверждение, установленное А. Робинсоном [104d] (см. также [40b]).

Теорема направленности. *Пусть* $R \in U$ *— направленное отношение. Тогда существует такой элемент* $y \in {}^*U$, *что* $\langle {}^*x, y\rangle \in {}^*R$ *для всех* $x \in D(R)$.

Покажем, что в случае бесконечного S теорема направленности гарантирует существование нестационарных индивидов. Предположим, что $\mathbb{N} \subset S$. Тогда $\mathbb{N} \in \widehat{S}$, $\mathbb{P}(\mathbb{N}) \in \widehat{S}$ и т. д. Отсюда следует, что $\mathbb{N} \subset {}^*\mathbb{N}$. Рассмотрим отношение

$$R = \{\langle x, y\rangle \mid x \in \mathbb{N}, y \in \mathbb{N}, x < y\}.$$

Это отношение направлено, так как $D(R) = \mathbb{N}$, и если $x_1, \ldots, x_n \in \mathbb{N}$, а x больше, чем $x_1, \ldots, x_n$, то

$$x_1 R x, \ldots, x_n R x.$$

По теореме направленности существует элемент $y \in {}^*U$ такой, что

$$\langle x, y\rangle \in {}^*R$$

для всех $x \in \mathbb{N}$ (здесь ${}^*x = x$, так как $x \in \mathbb{N} \subset S$). Поскольку $R \subset \mathbb{N} \times \mathbb{N}$, то ${}^*R \subset {}^*\mathbb{N} \times {}^*\mathbb{N}$ и, значит, $y \in {}^*\mathbb{N}$. Допустим, что $y \in \mathbb{N}$. Тогда ${}^*y = y$ и, так как ${}^*\vDash \langle {}^*x, {}^*y\rangle \in {}^*R$, по принципу перманентности $\vDash \langle x, y\rangle \in R$. Другими словами, $x < y$ для всех $x \in \mathbb{N}$ и, стало быть, $y \in \mathbb{N}$ является наибольшим неотрицательным целым числом. Ввиду того, что такого числа не существует, заключаем, что $y \in {}^*\mathbb{N} - \mathbb{N}$. Таким образом, ${}^*\mathbb{N} - \mathbb{N} \neq \varnothing$, и поскольку $y \in {}^*\mathbb{N} - \mathbb{N}$, то $y \notin S$. Значит, y — нестандартный индивид. Тем самым установлено существование нестандартных индивидов.

Приведенные выше рассуждения показывают, что нестандартные индивиды существуют в точности в том случае, когда S бесконечно. Действительно, в случае бесконечного S множество $\mathbb{N}$ может быть биективно вложено в S. С другой стороны, если S конечно, то нетрудно показать, что нестандартных элементов не существует.

Так как ${}^*R$ является нестандартным продолжением отношения $<$ с множества $\mathbb{N}$ на ${}^*\mathbb{N}$, то для всех $x, y \in {}^*\mathbb{N}$, таких, что $\langle x, y\rangle \in {}^*R$, будет $x < y$. Для обозначения того, что $x < y$ или $x = y$, будем употреблять запись $x \leqslant y$.

Если расширить язык L, включив в него предикатный символ $<$, то наличие на $\mathbb{N}$ линейного порядка может быть выражено следующим образом:

$$\mathbb{N} \vDash \forall x \neg (x < x),$$

$$\mathbb{N} \vDash \forall x \forall y \forall z ((x < y) \wedge (y < z) \Rightarrow (x < z)),$$

$$\mathbb{N} \vDash \forall x \forall y ((x < y) \vee (y < x) \vee (x = y)).$$

По принципу перманентности заключаем, что отношение $<$ линейно упорядочивает ${}^*\mathbb{N}$.

Покажем теперь, что всякий элемент множества ${}^*\mathbb{N} - \mathbb{N}$ больше любого неотрицательного целого числа.

Предложение 2. *Если* $u \in {}^*\mathbb{N} - \mathbb{N}$ *и* $n \in \mathbb{N}$, *то* $n < u$.

Доказательство. Предположим противное, что $u \leqslant n$ для некоторого $n \in \mathbb{N}$. Пусть n — минимальное из таких чисел. Имеем

$$\mathbb{N} \vDash \forall x ((x \leqslant 0) \Rightarrow (x = 0))$$

и тогда, в соответствии с принципом перманентности,

$${}^*\mathbb{N} \vDash \forall x ((x \leqslant 0) \Rightarrow (x = 0)).$$

Из семантики языка ${}^*L$ следует, что $0 < u$, и тогда $n \neq 0$. Положив теперь $n = m + 1$, получаем $m \in \mathbb{N}$ и $m < u \leqslant m + 1$. Так как $m + 1$ — стандартный элемент, то $u \neq m + 1$ и, следовательно, $m < u < m + 1$.

Имеем

$$\mathbb{N} \vDash \forall x \neg (m < x < m + 1)$$

(здесь $\vDash \varphi$ снова означает, что φ истинно в $\mathbb{N}$), и, так как $u \in {}^*\mathbb{N}$, принцип перманентности дает

$${}^*\mathbb{N} \vDash \neg (m < u < m + 1).$$

Полученное противоречие доказывает предложение.

Определение 17. Элемент $u \in {}^*\mathbb{N}$ называется *конечным*, если $u \in \mathbb{N}$, и *бесконечным* (или *бесконечным целым числом*), если $u \in {}^*\mathbb{N} - \mathbb{N}$.

Следовательно, конечными элементами ${}^*\mathbb{N}$ являются стандартные элементы, а бесконечными — нестандартные элементы. Мы установили существование лишь одного бесконечного элемента множества ${}^*\mathbb{N}$. На самом деле таких чисел имеется бесконечно много. Для их построения рассмотрим функцию $\pi \in U$ с областью определения $D(\pi) = \mathbb{N} \times \mathbb{N}$ и такую, что

$$\pi(\langle m, n\rangle) = m + n.$$

Положим для любых $m, n \in {}^*\mathbb{N}$

$$m + n = {}^*\pi(\langle m, n\rangle) \in {}^*\mathbb{N}.$$

Тогда при $u \in {}^*\mathbb{N} - \mathbb{N}$ имеем

$$u + 1, u + 2, \ldots \in {}^*\mathbb{N}.$$

Применяя принцип перманентности к $\vDash \forall x (x < x + 1)$, где $\vDash \varphi$ означает истинность высказывания φ в $\mathbb{N}$ и $x + 1$ — сокращенная запись выражения $\pi \restriction \langle x, 1\rangle$, получим

$$u < u + 1 < u + 2 < u + 3 < \ldots$$

Следовательно, элементы $u + 1$, $u + 2$, ... являются бесконечными. Аналогичным образом, если $u \in {}^*\mathbb{N} - \mathbb{N}$, то все элементы $u - 1$, $u - 2$, ... также являются бесконечными.

Таким образом, начав с бесконечного целого числа u, получаем блок бесконечных целых:

$$\ldots < u - 3 < u - 2 < u - 1 < u < u + 1 < u + 2 < u + 3 < \ldots$$

(штрих у чисел 1, 2, 3... опускаем).

Из принципа перманентности следует, что нет такого $v \in {}^*\mathbb{N}$, для которого

$$u < v < u + 1.$$

Однако для каждого данного блока существует другой блок, состоящий из больших элементов. Например, если $v = u + u$, где $u \in {}^*\mathbb{N} - \mathbb{N}$, то $u + m < v - n$ для всех $m, n \in \mathbb{N}$. Кроме того, $v < v + n < v + v$ и т. д. Двигаясь в обратном направлении, выводим (из принципа перманентности), что если $u \in {}^*\mathbb{N} - \mathbb{N}$, то или u, или $u + 1$ имеет вид $v + v$, где v — бесконечный элемент. Так как $v < u$, отсюда следует, что не существует первого блока. Более того, порядок блоков плотный. Действительно, пусть блок, содержащий v, предшествует блоку, содержащему u:

$$\ldots < v - 2 < v - 1 < v < v + 1 < v + 2 < \ldots$$

$$\ldots < u - 2 < u - 1 < u < u + 1 < u + 2 < \ldots.$$

Поскольку или $u + v$, или $u + v + 1$ можно записать в виде $z + z$,

то

$$v + m < z < u - n$$

для всех $m, n \in \mathbb{N}$.

В итоге получаем: ${}^*\mathbb{N}$ состоит из начального сегмента $\mathbb{N}$, за которым следует упорядоченное множество блоков; порядок на этом множестве блоков плотный без первого и последнего элемента; каждый блок изоморфен в смысле порядка целым числам

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

Хотя ${}^*\mathbb{N} - \mathbb{N}$ является непустым подмножеством ${}^*\mathbb{N}$, это подмножество не имеет наименьшего элемента. Поскольку любое непустое подмножество $\mathbb{N}$ имеет наименьший элемент, возникает кажущееся противоречие с принципом перманентности.

Предложение 3. *Пусть* $X \subset {}^*\mathbb{N}$ *таково, что* $X \in {}^*U$ *и* $X \neq \varnothing$. *Тогда* X *содержит наименьший элемент.*

Доказательство. Пусть $M = P(\mathbb{N})$. Согласно принципу перманентности для множеств имеем $X \in {}^*M$. Далее, так как каждое непустое подмножество множества $\mathbb{N}$ содержит наименьший элемент, то имеем

$$M \vDash \forall X ((X = \varnothing) \vee (\exists m \in X)(\forall x \in X)(m \leqslant x)).$$

Принцип перманентности дает

$${}^*M \vDash \forall X ((X = \varnothing) \vee (\exists m \in X)(\forall x \in X)(m \leqslant x)).$$

Так как $X \in {}^*M$ и $X \neq \varnothing$, то из семантики языка ${}^*L$ следует, что существует такой элемент $m \in X$, что $m \leqslant x$ для всех $x \in X$. Другими словами, m — наименьший элемент множества X.

Следствие. ${}^*\mathbb{N} - \mathbb{N} \notin {}^*U$.

Множества из $\widehat{W}$, принадлежащие ${}^*U$, называются *внутренними*; множества из $\widehat{W}$, не являющиеся внутренними, называются *внешними*. Мы показали, что множество ${}^*\mathbb{N} - \mathbb{N}$ внешнее и, следовательно, установили существование внешних множеств. Из теоремы 1 вытекает также (см. [40b]) справедливость следующего утверждения.

Теорема 2 (о внутренних множествах). *Пусть* X — *внутреннее множество и* Y — *определимое подмножество* ${}^*U$. *Тогда множество* $X \cap Y$ *внутреннее.*

Следствие 1. *Если* $X \subset Y$, *где* X — *внутреннее и* Y — *определимо в* ${}^*U$, *то* Y — *внутреннее множество.*

Следствие 2. $\mathbb{N}$ — *внешнее множество.*

Доказательство. Предположим, что $\mathbb{N}$ — внутреннее множество, т. е. $\mathbb{N} \in {}^*U$. Тогда, положив $\mathbb{N} = M' \in {}^*U$, можно определить ${}^*\mathbb{N} - \mathbb{N}$ следующим образом:

$${}^*\mathbb{N} - \mathbb{N} = \{a' \in {}^*U \mid * \vDash ((a \in {}^*M) \wedge \neg (a \in M))$$

(существование константного символа M в ${}^*L$ следует из предположения, что $M' = \mathbb{N}$ — внутреннее множество).

Так как $^*\mathbb{N}$ — внутреннее множество и $^*\mathbb{N}-\mathbb{N}\subset\mathbb{N}$, то получаем, что $^*\mathbb{N}-\mathbb{N}$ — также внутреннее множество, и приходим к противоречию со следствием предложения 3.

Следствие 3. *Если $X\subset S$ и X бесконечно, то X — внешнее множество.*

Справедливы, кроме того, следующие утверждения.

Теорема 3. *Если X и Y — внутренние множества, то $X\times Y$ — также внутреннее множество.*

Теорема 4. *Пусть X, Y — внутренние множества универсума $^*U$ и $f\colon X\to Y$ — отображение X в Y. Если $t=t(x)$ — такой терм языка $^*L$, что $f(a')=t(a')$ для каждого $a'\in X$, то функция f (рассматриваемая как множество) является внутренней.*

Нами достаточно подробно разъяснены основные аспекты нестандартного подхода в анализе, чтобы подвести некоторые итоги и сформулировать общие принципы такого подхода при изучении произвольных математических структур. Нестандартный подход основан на том факте, что каждая математическая структура M допускает *нестандартное расширение* $^*M$, наследующее свойства структуры M. Указанную взаимосвязь между M и $^*M$ удобно сформулировать в виде общих *принципов нестандартного расширения.*

Первый из этих принципов выражает тот факт, что $^*M$ является моделью структуры M.

Принцип перманентности. *Каждое математическое утверждение относительно M имеет интерпретацию в $^*M$, и эта интерпретация истинна в $^*M$ в том и только в том случае, когда исходное утверждение истинно в M.*

Отметим, что математическое утверждение относительно M понимается как высказывание в формальном языке L исчисления предикатов на M. Этот язык содержит имена (константные символы) для всех индивидов, а также для всех объектов высшего порядка в M (например, для множеств индивидов, отношений между индивидами, отношений между множествами и так далее). Исходя из этих символов и располагая достаточным запасом переменных, каждое высказывание в L строим за конечное число шагов с использованием логических связок и кванторов в соответствии с правилами исчисления предикатов. При этом кванторы могут действовать не только на индивидах, но и на объектах любого заданного типа.

В большинстве случаев описание математических утверждений относительно M в языке L связано с большими трудностями. Поэтому для описания таких утверждений используем обычный математический язык, если только ясно, что имеется возможность трансляции этого языка на формальный язык L.

Основное свойство нестандартных моделей связано с концепцией интерпретации математических утверждений относительно

M в нестандартном расширении $^*M$. Эта интерпретация выбирается специальным образом в соответствии со следующими правилами:

1) логические связки при их интерпретации сохраняют свой обычный смысл;

2) каждый индивид в M имеет то же самое имя в $^*M$ и кванторы по индивидам (например, «существует число» или «для всех чисел») сохраняют свой смысл в $^*M$;

3) имена других объектов в M (множеств, отношений между индивидами, отношений между множествами и так далее) также обозначают соответствующие объекты в $^*M$, которые называются *стандартными объектами.* Однако кванторы действуют не на всем классе объектов в $^*M$ (примерами являются: «существует отношение» или «для всех множеств»), а лишь на некотором их *подклассе*, который состоит из так называемых *внутренних объектов* (множеств, отношений и так далее). Среди внутренних объектов имеются стандартные объекты.

Рассмотрим, например, случай $M=\mathbb{N}$ неотрицательных целых чисел. Из принципа Пеано математической индукции следует, что каждое непустое ограниченное подмножество множества M имеет максимальный элемент. Это утверждение требует для своей формулировки в формальном языке L привлечения квантора, действующего на множествах. В соответствии с 3) его интерпретация в $^*\mathbb{N}$ должна касаться лишь внутренних множеств. Отсюда следует, что всякое непустое ограниченное внутреннее подмножество $^*\mathbb{N}$ содержит максимальный элемент. Непустое ограниченное подмножество $^*\mathbb{N}$, не содержащее максимального элемента, необходимо должно быть внешним. Примером такого внешнего подмножества в $^*\mathbb{N}$ служит множество $\mathbb{N}$, которое ограничено в $^*\mathbb{N}$ всяким нестандартным элементом $x\in{}^*\mathbb{N}$.

Отметим, что понятия *стандартного* и *внутреннего* объектов относятся к определениям нестандартного расширения. Более точно, нестандартное расширение $^*M$ структуры M определяется как структура высшего порядка, расширяющая M, в которой некоторые объекты отмечаются как стандартные или внутренние, и для которой выполняются основные принципы нестандартного расширения.

Следующий принцип касается отношений в структуре M. Пусть R является n-местным отношением между индивидами в M. В соответствии с 3) R является некоторым стандартным n-местным отношением в $^*M$. Пусть $a_1, \ldots, a_n$ — индивидумы структуры M и пусть отношение $R(a_1, \ldots, a_n)$ выполнено в M. Согласно принципу перманентности указанное утверждение истинно в $^*M$. Другими словами, новое отношение R в $^*M$ является расширением исходного отношения в M. Таким образом, мы приходим к следующему принципу (который является след-

ствием принципа перманентности, но который мы предпочитаем сформулировать отдельно).

Принцип нестандартного расширения для отношений. *Каждое отношение в M единственным образом расширяется до стандартного отношения того же типа в $^*M$. Расширенное отношение обозначается тем же символом, что и исходное. Каждое свойство исходного отношения, выражаемое в языке L, выполняется и для расширенного стандартного отношения при условии, что оно имеет интерпретацию в $^*M$.*

Указанный принцип имеет место не только для отношений между индивидами, но и для отношений между объектами высшего порядка.

Рассмотрим в качестве примера случай $M = K$, где K — поле алгебраических чисел конечной степени. В нем имеются тернарные отношения $a + b = c$ и $a \cdot b = c$. Эти отношения расширяются до некоторых стандартных отношений в $^*K$, для которых мы используем те же символы сложения и умножения. Исходные тернарные отношения удовлетворяют всем аксиомам поля. Следовательно, этим аксиомам поля удовлетворяют и расширенные стандартные отношения. Отсюда получаем, что $^*K$ является надполем поля K. Покажем, что K алгебраически замкнуто в поле $^*K$. Для этого достаточно показать, что каждый многочлен $f \in K[x]$ степени $n \geqslant 1$ имеет корень в $^*K$ в том и только в том случае, когда он имеет корень в K. Но утверждение о том, что f имеет корень в K принадлежит языку поля K и, следовательно, это утверждение (по принципу перманентности) истинно в K тогда и только тогда, когда оно истинно в $^*K$.

Из приведенных выше двух принципов еще не следует, что $^*M$ является собственным расширением M (они тривиальным образом справедливы для $^*M = M$). В противоположность к ним, следующий принцип утверждает, что $^*M$ содержит (в случае бесконечного M) некоторые *нестандартные объекты* (чем объясняется его название «нестандартное расширение»).

Принцип нестандартного расширения для направленных бинарных отношений. *Если бинарное отношение R направлено в M, то существует такой элемент $x \in {}^*M$, что $R(^*a, x)$ выполняется для всех $a \in D(R)$.*

Другими словами, возможно бесконечная система условий $\langle ^*a, x\rangle \in R$ разрешима в $^*M$, если только любая ее конечная подсистема разрешима в M. Этот принцип можно рассматривать как специальный случай теоремы компактности А. И. Мальцева: *если каждое конечное подмножество T_0 произвольного множества T высказываний логики первого порядка обладает моделью, то существует модель и для самого множества T* (см. [113а, гл. 1, или 51, § 17, 21]).

Если M — бесконечная структура, то сформулированный только что принцип гарантирует существование нестандартных

индивидов в $^*M$. Действительно, рассмотрим отношение неравенства $a \neq b$ между индивидами M, областью определения которого является сама структура M. Так как M бесконечна, это отношение направлено, и мы получаем, что существует индивид $x \in {}^*M$, отличный от всех $a \in M$ (т. е. нестандартный индивид).

Рассмотрим теперь более общую ситуацию. Пусть A — любое множество в M (например, множество индивидов). В соответствии с 3) A определяет некоторое стандартное множество $^*A$ в $^*M$, характеристические свойства которого при их интерпретации в $^*M$ идентичны с характеристическими свойствами множества A в M. Отсюда следует, что $^*A$ является расширением множества A (A состоит из тех стандартных элементов, которые содержатся в $^*A$). Если A — конечное множество, состоящее, скажем, из n элементов, то $^*A$ совпадает с A. Это следует из того, что утверждение о том, что A состоит из n элементов, принадлежит языку L и, следовательно, остается истинным при его интерпретации в $^*M$. С другой стороны, если A бесконечно, то мы можем рассмотреть отношение неравенства $a \neq b$, ограниченное на A, и по аналогии с изложенным выше показать, что $^*A$ содержит нестандартный элемент.

Принцип нестандартного расширения для множеств. *Каждое множество A в M определяет единственным образом некоторое стандартное множество $^*A$ в $^*M$; если A определяется в L формулой φ, то ее интерпретация в $^*M$ определяет множество $^*A$. Исходное множество A состоит в точности из стандартных элементов, принадлежащих $^*A$. Множество $^*A$ содержит нестандартные элементы (т. е. является собственным расширением A) в том и только в том случае, когда A бесконечно.*

Последние два принципа справедливы не только для отношений и множеств индивидов, но и для отношений и множеств объектов высшего типа. Пусть A — множество объектов высшего типа (множество отношений или функций и т. д.). В этом случае элемент $a \in A$, являясь объектом высшего типа, не обязан содержаться в структуре $^*M$. Тем не менее, каждый такой объект расширяется единственным образом до стандартного объекта из $^*A$ и, если мы сопоставим каждому $a \in A$ соответствующий ему стандартный объект, то получим вложение A в $^*A$. Отождествим теперь элементы из A с соответствующими им стандартными объектами и будем рассматривать A как подмножество множества $^*A$ (нестандартное расширение $^*A$ множества A всегда в дальнейшем будем понимать именно в этом смысле). Например, мы не различаем отношения в M и соответствующие их расширения в $^*M$.

Выше мы показали, что всякое бесконечное множество A в M, рассматриваемое как подмножество $^*A$, необходимо внешнее. Сформулируем это свойство в виде следующего принципа.

Принцип выделения внешних множеств. *Каждое бесконечное множество A, которое состоит только из стандартных элементов, необходимо внешнее в $^*M$. Другими словами, всякое бесконечное внутреннее множество в $^*M$ содержит нестандартный элемент.*

Как уже отмечали, нестандартное расширение $^*M$ данной структуры M не единственно. Отметим также, что имеется несколько способов построения нестандартных расширений. В предыдущем параграфе был построен нестандартный универсум $^*U$ с помощью ультрапроизведений. С другой стороны, нестандартное расширение $^*M$ структуры M можно определить аксиоматически, взяв за основу сформулированные выше принципы.

Предположим, что для данной структуры высшего порядка M выбрали определенное нестандартное расширение $^*M$. Пусть A — некоторое множество в M (множество индивидов или множество объектов более высокого типа). Известно, что A единственным образом определяет некоторое стандартное множество $^*A$ в $^*M$, состоящее из внутренних объектов того же типа, что и объекты из A. Рассмотрим теперь A не только как множество, но как подструктуру высшего порядка структуры M и, аналогичным образом, рассмотрим $^*A$ как подструктуру структуры $^*M$. Тогда, как легко видеть, $^*A$ является нестандартным расширением структуры A. Таким образом, фиксированное нестандартное расширение $^*M$ структуры M содержит нестандартное расширение $^*A$ каждой подструктуры A структуры M. Другими словами, имеем функтор

$$A \mapsto {}^*A,$$

переводящий подструктуру A структуры M в нестандартное ее расширение $^*A$, являющееся подструктурой структуры $^*M$. По принципу перманентности этот функтор точен (см., например, [126, т. 1, ч. 1]) не только относительно включения $A \subset B$, но также относительно всех других отношений между подструктурами, которые могут быть выражены в языке L. Поэтому в качестве M можем взять некоторый фиксированный универсум, содержащий в себе все математические структуры, которые представляют интерес с точки зрения того или иного раздела математики (алгебры, теории чисел, математического анализа и т. д.). Этим замечанием мы воспользуемся в дальнейшем при выборе универсума, связанного с изучением нестандартных расширений полей алгебраических чисел.

Нам удобно будет придерживаться следующей точки зрения. Возьмем фиксированный универсум M, который, как структура высшего порядка, содержит все математические структуры, интересные с точки зрения теории алгебраических чисел. Более точно, M должен содержать все поля алгебраических чисел и их пополнения относительно их различных нормирований. Затем,

выбрав фиксированное нестандартное расширение $^*M$ универсума M, рассмотрим каждую структуру A, которая встретится в дальнейших рассуждениях в качестве подструктуры из M. Тогда, в соответствии со сказанным выше, нестандартное расширение $^*A$ структуры A однозначно определяется как некоторая подструктура из $^*M$.

Для наших целей удобно взять в качестве M множество неотрицательных целых чисел $\mathbb{N}$; вернее, M представляет собой полную структуру высшего порядка, базирующуюся на множестве $\mathbb{N}$. Подструктурами этого универсума являются в точности те структуры, которые могут быть описаны на языке неотрицательных целых чисел. Так, M содержит все целые числа $\mathbb{Z}$ (которые могут быть описаны как классы эквивалентности пар натуральных чисел). Далее, M содержит рациональные числа $\mathbb{Q}$ (пары целых чисел), а также действительные числа $\mathbb{R}$ и p-адические числа $\mathbb{Q}_p$ (последовательности рациональных чисел). Если K — поле алгебраических чисел конечной степени n и $\omega_1, \ldots, \omega_n$ — базис этого поля над $\mathbb{Q}$, то элементы поля K могут быть описаны их координатами в этом базисе, то есть наборами $\langle x_1, \ldots, x_n \rangle$ рациональных чисел. Значит, K также содержится в M.

Для более детального знакомства с техникой нестандартного анализа рекомендуем читателю книги [40b] и [104c].

Задачи

1. Доказать, что для всякого *упорядоченного* (отношением $<$) *поля* K справедливы следующие утверждения:

а) имеет место неравенство $0 < 1$;

б) для всех $x \in K$ выполняется соотношение $x < x + 1$;

в) неравенство $x < y$ влечет неравенство $-y < -x$;

г) если $|x| = \max(x, -x)$, то

$$|x \cdot y| = |x| \cdot |y| \quad \text{и} \quad |x + y| \leqslant |x| + |y|;$$

д) возможны вложения:

$$\mathbb{N} \subset \mathbb{Q} \subset K.$$

2. Упорядоченное поле K называется *архимедовым*, если для каждого $x \in K$ существует $n \in \mathbb{N}$ такое, что $x < n$. В противном случае называется *неархимедовым*.

Установить справедливость следующих свойств архимедова поля K (считать, что $\mathbb{Q} \subset K$):

а) если $x, y \in K$ и $x > 0$, $y > 0$, $y - x > 1$, то для некоторого $n \in \mathbb{N}$ выполняется $x < n < y$;

б) если $x, y \in K$ и $x < y$, то существует $r \in \mathbb{Q}$, такое, что $x < r < y$.

3. Элемент $s \in K$ называется *верхней гранью* непустого множества X упорядоченного поля K, если $x \leqslant s$ для всех $x \in X$. Если, кроме того, никакое $u \in K$ такое, что $u < s$, не является верхней гранью множества X, то s называется *наименьшей верхней гранью* множества X.

Упорядоченное поле K называется *полным*, если любое непустое подмножество X поля K, имеющее верхнюю грань, имеет и наименьшую верхнюю грань.

Доказать справедливость следующих утверждений:

а) полное упорядоченное поле K является архимедовым.

(Указание. Воспользоваться тем, что возможно вложение $\mathbb{N} \subset K$ и предположив, что K не является архимедовым, прийти к противоречию);

б) если K, K' — полные упорядоченные поля, то существует единственное отображение φ поля K в поле K' такое, что (считаем $\mathbb{Q} \in K$, $\mathbb{Q} \subset K'$):

1) $\varphi(r) = r$ для всех $r \in \mathbb{Q}$,

2) $\varphi(x) < \varphi(y)$ в том и только в том случае, если $x < y$ при $x, y \in K$.

(Указание. Пусть $\varphi(x)$ для $x \in K$ есть наименьшая верхняя грань в K' множества

$$A'_x = \{r' \in \mathbb{Q} \mid r' < x\}.$$

Воспользовавшись результатом п. б) задачи 2, показать, что $\varphi(r) = r$ при $r \in \mathbb{Q}$ и что $\varphi(x) < \varphi(y)$ равносильно $x < y$.

Установить единственность отображения φ, исходя из противного.)

4. Пусть K — упорядоченное поле и

$$F = \{x \in K \mid |x| < n \text{ для некоторого } n \in \mathbb{N}\},$$
$$I = \{x \in K \mid x = 0 \text{ или } x^{-1} \in K - F\},$$

где $|x| = \max(x, -x)$. Если $x \in F$, то x называется *конечным элементом*; если $x \in K - F$, то x называется *бесконечным элементом*; элементы множества I называются *бесконечно малыми*. Доказать справедливость следующих утверждений:

а) если K — архимедово поле, то $F = K$ и $I = \{0\}$;

б) $x \in I$ тогда и только тогда, когда $|x| \leqslant 1/n$ для всех $n \in \mathbb{N} - \{0\}$;

в) F является подкольцом поля K;

г) I является идеалом в F.

5. Если x, y — элементы упорядоченного поля K и $x - y \in I$, то назовем x, y *бесконечно близкими* и для выражения этого факта воспользуемся записью $x \approx y$ (при $x - y \notin I$ пишем $x \not\approx y$).

Доказать справедливость следующих утверждений:

а) отношение $\approx$ является отношением эквивалентности на K и, следовательно, на F;

б) если $F \to F/I$ — естественный гомоморфизм F на F/I и ${}^0x$ — образ элемента $x \in F$ при этом гомоморфизме, то ${}^0x = {}^0y$ тогда и только тогда, когда $x \approx y$;

в) если $x \in K - I$, то $x^{-1} \in F$;

г) I — максимальный идеал кольца F;

д) факторкольцо F/I является полем;

е) если $x \in F - I$, $x > 0$ и $y \in I$, то $x + y > 0$;

ж) если $x, y \in F$, $x < y$, $x \not\approx y$ и $x \approx x'$, $y \approx y'$, то $x' < y'$;

з) если $x, y \in F$ и $x \leqslant y$, то ${}^0x \leqslant {}^0y$;

и) F/I является упорядоченным полем (считаем ${}^0x < {}^0y$, если $x < y$ и $x \not\approx y$);

к) возможно вложение: $\mathbb{Q} \subset F/I$;

л) при $r \in \mathbb{Q} \subset F/I$ имеет место равенство ${}^0r = r$;

м) F/I является архимедовым полем.

6. Доказать, что не существует множества аксиом логики первого порядка, характеризующих поле действительных чисел $\mathbb{R}$ с точностью до изоморфизма.

(Указание. Установить, что множество высказываний логики первого порядка, истинных в $\mathbb{R} = \langle \mathbb{R}, +, \cdot, <, 0, 1 \rangle$ счетно и воспользоваться следующей теоремой Лёвенгейма-Сколемана (см., например, [113 а], гл. 1—2): *пусть $\varkappa$ — бесконечный кардинал и T — множество аксиом первого порядка мощности $\leqslant \varkappa$; если существует модель, в которой все аксиомы T истинны, то существует модель для T, множество элементов которой имеет мощность $\leqslant \varkappa$.*)

7. Показать, что аксиома полноты для поля действительных чисел $\mathbb{R}$: $\forall X \subset R$ ($X \neq \varnothing$ и ограничено $\Rightarrow X$ имеет наименьшую верхнюю грань) не выразима в логике первого порядка.

8. Пусть $\mathbb{R}$ — поле действительных чисел, τ — некоторый элемент, не принадлежащий $\mathbb{R}$, и $K = \mathbb{R}(\tau)$ — поле рациональных функций от τ с коэффициентами из $\mathbb{R}$. Если

$$f = P(\tau)/Q(\tau)$$

— какое-либо представление отличного от нуля элемента $f \in K$ в виде частного двух многочленов $P = \tau^k(a_0 + a_1\tau + \ldots + a_m\tau^m)$ и $Q = \tau^l(b_0 + b_1\tau + \ldots + b_n\tau^n)$, где $a_0 \neq 0$, $b_0 \neq 0$, то при $a_0b_0 > 0$ назовем f *положительным* (обозначение: $f > 0$), а при $a_0b_0 < 0$ — *отрицательным* (обозначение: $f < 0$). Как обычно, положим $f < g$, если только $f - g < 0$.

Доказать справедливость следующих утверждений:

а) отношение $f < g$ в поле $K = \mathbb{R}(\tau)$ не зависит от выбора конкретных представлений для элементов f и g;

б) поле K является упорядоченным (отношением $<$) полем, содержащим $\mathbb{R}$ в качестве собственного подполя;

в) поле K является неархимедовым (существует элемент $f \in K$, для которого $f > n$ при любом $n \in \mathbb{N}$);

г) в поле K не существует элемента f такого, что $f^2 = \tau$.

9. Пусть K — архимедово упорядоченное поле, содержащееся в множестве S индивидов стандартного универсума U. Доказать, что нестандартное расширение ${}^*K$ поля K является неархимедовым упорядоченным полем.

10. Пусть $K \subset S$ — архимедово упорядоченное поле и

$${}^*F = \{x \in {}^*K \mid |x| < n \text{ для некоторого } n \in \mathbb{N}\},$$
$${}^*I = \{x \in {}^*K \mid x = 0 \text{ или } x^{-1} \in {}^*K - {}^*F\}.$$

Доказать, что естественный гомоморфизм (см. задачу 5)

$${}^*F \to {}^*F/{}^*I$$

является изоморфизмом поля K в ${}^*F/{}^*I$.

В дальнейшем поле K будем отождествлять с его образом в ${}^*F/{}^*I$ при этом изоморфизме.

11. В обозначениях предыдущей задачи установить справедливость следующих утверждений:

а) ${}^*\mathbb{N} \cap {}^*F = \mathbb{N}$;

б) множества K, ${}^*F$, ${}^*I$ и ${}^*K - {}^*F$ являются внешними подмножествами ${}^*K$.

(Указание. Воспользоваться теоремой о внутренних множествах и результатом предыдущего пункта.)

12. Доказать справедливость теоремы Дедекинда: *если A, B — непустые подмножества архимедова упорядоченного поля $K \subset S \subset U$, такие, что из $a \in A$, $b \in B$ следует $a < b$, то найдется такой элемент $c \in {}^*F/{}^*I$, что $a \leqslant c \leqslant b$ для всех $a \in A$ и $b \in B$* (считаем, что K вложено в ${}^*F/{}^*I$).

(Указание. Пусть R — отношение, состоящее из всех таких пар $\langle a, b \rangle$, что $a \in A$, $b \in K$, $a \leqslant b$ и b меньше всех элементов множества B. Показать, что R — направленное отношение, и, воспользовавшись теоремой направленности, установить существование такого $x \in {}^*U$, что $\langle a, x \rangle \in {}^*R$ для всех $a \in A$. Доказать, что $x \in {}^*K$ и, воспользовавшись принципом перманентности, а также определением отношения R, показать, что $a \leqslant x \leqslant b$ для всех $a \in {}^*A$, $b \leqslant {}^*B$. Наконец, воспользовавшись результатом пункта з) задачи 5, установить, что $a = {}^0a \leqslant {}^0x \leqslant {}^0b = b$ и положить $c = {}^0x$.)

13. Пусть $K \subset S$ — архимедово упорядоченное поле. Доказать, что ${}^*F/{}^*I$ — полное упорядоченное поле.

(Указание. Пусть $Z \in {}^*F/{}^*I$ — непустое подмножество, имеющее верхнюю грань в ${}^*F/{}^*I$. Показать, что множества $Y = \{y \in K \subset {}^*F/{}^*I \mid y$ —

верхняя грань множества Z) и $X = K - Y$ удовлетворяют всем условиям теоремы Дедекинда. Применив теорему Дедекинда, найти такое $z \in {}^*F/{}^*I$, что $x \leqslant z \leqslant y$ для любых $x \in X$ и $y \in Y$. Используя включения $\mathbb{Q} \subset K \subset {}^*F/{}^*I$ и архимедовость поля ${}^*F/{}^*I$, установить, что z является верхней гранью множества Z. Показать, затем, что z — наименьшая верхняя грань множества Z.)

14. Пусть K — архимедово упорядоченное поле и $\mathbb{Q} \subset K \subset S \subset U$. Доказать, что для каждого $x \in K$ существует $r \in {}^*\mathbb{Q}$, такое, что $x \approx r$.

(Указание. Воспользоваться плотностью $\mathbb{Q}$ в K (см. задачу 2) и принципом перманентности.)

15. Дать нестандартное построение поля действительных чисел $\mathbb{R}$:

а) Установить существование полного упорядоченного поля $\mathbb{R}$.

(Указание. Положить $K = \mathbb{Q}$, $\mathbb{R} = {}^*F/{}^*I$ и воспользоваться результатом задачи 13.)

б) Показать, что если K, K' — полные упорядоченные поля, содержащиеся в некотором множестве стандартных индивидов S, и если φ — единственное отображение K на K', сохраняющее порядок и тождественное на $\mathbb{Q}$ (см. задачу 3), то при $x, y \in {}^*K$ неравенство $x < y$ равносильно неравенству $\varphi(x) < \varphi(y)$, и $\varphi(r) = r$ для всех $r \in {}^*\mathbb{Q}$.

в) Показать, что если $x \in K$ и $r \in {}^*\mathbb{Q}$, то $x \approx r$ тогда и только тогда, когда $\varphi(x) \approx r$.

г) Показать, что при всех $x, y \in K$ справедливы соотношения

$$\varphi(x + y) = \varphi(x) + \varphi(y), \quad \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

(Указание. Воспользоваться результатом задачи 14 и результатом предыдущего пункта.)

д) Доказать, что существует единственное с точностью до изоморфизма полное упорядоченное поле $\mathbb{R}$ (поле действительных чисел).

(Указание. Воспользоваться результатами пунктов а) и г).)

16. Пусть ${}^*\mathbb{R}$ — нестандартное расширение поля действительных чисел $\mathbb{R}$. В силу задачи 9 ${}^*\mathbb{R}$ является неархимедовым упорядоченным полем. Его элементы назовем *гипердействительными числами*. Имеем $\mathbb{Q} \subset \mathbb{R} \subset {}^*\mathbb{R}$ (последнее включение строгое, так как ${}^*\mathbb{R}$ содержит бесконечные элементы). Пусть ${}^*F$ — множество конечных элементов и ${}^*I$ — множество бесконечно малых элементов поля ${}^*\mathbb{R}$.

Установить справедливость следующих утверждений:

а) естественный гомоморфизм

$${}^*F \to {}^*F/{}^*I$$

задает единственный изоморфизм между $\mathbb{R}$ и ${}^*F/{}^*I$;

б) если ${}^0x$ — образ элемента $x \in {}^*F$ при гомоморфизме

$${}^*F \to {}^*F/{}^*I = \mathbb{R},$$

то

$${}^0(x + y) = {}^0x + {}^0y, \quad {}^0(x \cdot y) = {}^0x \cdot {}^0y,$$

$$x \leqslant y \Rightarrow {}^0x \leqslant {}^0y, \qquad x \in R \Rightarrow {}^0x = x;$$

в) если $x \approx 0$ и $y \approx 0$, то $x + y \approx 0$;

г) если $x \approx 0$ и $y \in {}^*F$, то $x \cdot y \approx 0$;

д) $x \not\approx 0$, то $x^{-1} \in {}^*F$;

е) если $x \not\approx 0$ и $x \approx y$, то $x^{-1} \approx y^{-1}$;

ж) для любого $x \in \mathbb{R}$ существует $r \in {}^*\mathbb{Q}$, такое, что $x \approx r$.

17. Пусть $\{x_n \mid n \in \mathbb{N}\}$ — последовательность действительных чисел и $\{x_n \mid n \in {}^*\mathbb{N}\}$ — ее интерпретация в ${}^*\mathbb{R}$. Доказать справедливость следующих утверждений:

а) $x_n \to x$ тогда и только тогда, когда $x_n \approx x$ для всех $n \in {}^*\mathbb{N} - \mathbb{N}$;

б) точка x является предельной точкой последовательности $\{x_n\}$ в том и только том случае, если $x_n \approx x$ для некоторого $n \in {}^*\mathbb{N} - \mathbb{N}$.

§ 3. Нестандартные расширения полей алгебраических чисел

1. Арифметика поля алгебраических чисел. Пусть K — конечное расширение поля рациональных чисел $\mathbb{Q}$. Арифметическая структура поля K может быть описана при помощи его простых дивизоров, которые определяются в терминах нормирований этого поля. Более точно, *простой дивизор* $\mathfrak{p}$ поля K определяется как класс эквивалентных между собой нормирований этого поля. Для такого описания удобно расширить введенное ранее понятие нормирования и наряду с *неархимедовыми нормированиями* (которые в гл. IV назывались просто нормированиями) рассмотреть *архимедовы нормирования* (см. задачу 2). В соответствии с этими двумя типами нормирований вводятся два типа простых дивизоров — *неархимедовы простые дивизоры и архимедовы простые дивизоры.*

Пусть $\mathfrak{p}$ — неархимедов простой дивизор поля K. Среди определяющих его нормирований имеется единственное нормирование v, для которого $v(K^*) = \mathbb{Z}$. Такое дискретное нормирование обозначим $v_\mathfrak{p}$ и назовем $v_\mathfrak{p}$ *$\mathfrak{p}$-адической порядковой функцией* поля K. Нормирование $v_\mathfrak{p}$ однозначным образом определяет *$\mathfrak{p}$-адическую норму*

$$\|x\|_\mathfrak{p} = (N\mathfrak{p})^{-v_\mathfrak{p}(x)} \tag{1}$$

поля K, где $N\mathfrak{p}$ — *неархимедова норма дивизора* $\mathfrak{p}$, равная числу элементов его поля классов вычетов.

Пусть теперь $\mathfrak{p}$ — архимедов простой дивизор поля K. Среди всех нормирований, определяющих $\mathfrak{p}$, имеется единственное нормирование, которое индуцирует на поле $\mathbb{Q}$ обычное абсолютное значение. Обозначим это нормирование $|\ |_\mathfrak{p}$ и введем в рассмотрение *архимедову норму* $\|\ \|_\mathfrak{p}$, положив

$$\|x\|_\mathfrak{p} = \begin{cases} |x|_\mathfrak{p}, & \text{если } \mathfrak{p} \text{ вещественный дивизор,} \\ |x|_\mathfrak{p}^2, & \text{если } \mathfrak{p} \text{ комплексный дивизор.} \end{cases} \tag{2}$$

Как обычно, архимедов простой дивизор $\mathfrak{p}$ называется *вещественным* или *комплексным* в соответствии с тем, будет ли связанное с ним $\mathfrak{p}$-адическое пополнение по норме $\|\ \|_\mathfrak{p}$ изоморфно полю действительных чисел $\mathbb{R}$ или же полю комплексных чисел $\mathbb{C}$.

Введенные нами нормы обладают тем свойством, что для любого $x \in K$, $x \neq 0$

$$\prod_\mathfrak{p} \|x\|_\mathfrak{p} = 1, \tag{3}$$

где $\mathfrak{p}$ пробегает все простые дивизоры поля K, как архимедовы, так и неархимедовы. Произведение в соотношении (3) является

конечным, так как для каждого заданного ненулевого элемента $x \in K$ имеется лишь конечное число простых дивизоров $\mathfrak{p}$, для которых $\|x\|_{\mathfrak{p}} \neq 1$ (см. задачу 14).

Для всякого архимедова простого дивизора $\mathfrak{p}$ положим $v_{\mathfrak{p}}(x) = -\log \|x\|_{\mathfrak{p}}$, $N\mathfrak{p} = e$, где e — основание натурального логарифма, и назовем $v_{\mathfrak{p}}(x)$ *архимедовой порядковой функцией* поля K, а $N\mathfrak{p}$ — *архимедовой нормой дивизора* $\mathfrak{p}$.

2. Арифметика нестандартного расширения поля алгебраических чисел. Пусть $^*K$ — нестандартное расширение поля K и V — множество всех простых дивизоров последнего поля. В соответствии с принципом перманентности нестандартное расширение $^*V$ множества V интерпретируется как множество всех *внутренних простых дивизоров* поля $^*K$, которые определяются обычным образом как классы эквивалентных между собой нетривиальных внутренних нормирований поля $^*K$. При такой интерпретации всякое истинное утверждение относительно простых дивизоров из V приводит к аналогичному истинному утверждению относительно дивизоров из $^*V$.

Арифметика поля $^*K$ может быть описана следующим образом. В поле $^*K$ имеются два типа внутренних простых дивизоров: *архимедовы* и *неархимедовы*. Пусть $\mathfrak{p}$ — неархимедов внутренний простой дивизор. Среди всех внутренних нормирований поля $^*K$, определяющих $\mathfrak{p}$, имеется единственное нормирование v, для которого $v(^*K - \{0\}) = {}^*\mathbb{Z}$, где $^*\mathbb{Z}$ — аддитивная группа стандартных и нестандартных целых чисел. Такое нормирование поля $^*K$ обозначим $v_{\mathfrak{p}}$ и назовем $v_{\mathfrak{p}}$ *$\mathfrak{p}$-адической порядковой функцией* поля $^*K$. Таким образом, $v_{\mathfrak{p}}$ является обычным нормированием поля $^*K$ в смысле Крулля с единственным дополнительным условием, присущим лишь нестандартному расширению, что $v_{\mathfrak{p}}$ — внутреннее нормирование. Поле вычетов по неархимедову простому дивизору $\mathfrak{p}$ не обязательно конечно. Однако оно *звездно конечно* в том смысле, что при некотором $n \in {}^*\mathbb{N}$ имеет место внутренняя биекция этого поля вычетов на интервал $1 \leqslant \nu \leqslant n$, лежащий в $^*\mathbb{N}$. Ясно, что понятие звездной конечности представляет собой интерпретацию обычного понятия конечности. Указанное число $n \in {}^*\mathbb{N}$ определяется единственным образом и называется *нормой* $N\mathfrak{p}$ *простого дивизора* $\mathfrak{p}$. Поэтому в поле $^*K$ можно ввести неархимедову $\mathfrak{p}$-адическую норму $\|x\|_{\mathfrak{p}}$ по формуле (1), интерпретируемой в $^*K$. Значениями этой нормы являются неотрицательные элементы поля $^*\mathbb{Q}$.

Если $\mathfrak{p}$ — архимедов внутренний простой дивизор поля $^*K$, то среди определяющих его нормирований имеется единственное нормирование, которое индуцирует в поле $^*\mathbb{Q}$ обычное стандартное абсолютное значение. Обозначим это нормирование $|x|_{\mathfrak{p}}$. Интерпретация в $^*K$ формулы (2) приводит к определению архимедовой нормы $\|x\|_{\mathfrak{p}}$ поля $^*K$. Простой дивизор $\mathfrak{p}$ называется при этом *вещественным* или *комплексным* в соответствии с тем, будет ли пополнение поля $^*K$ по норме $\|x\|_{\mathfrak{p}}$ изоморфно $^*\mathbb{R}$ или $^*\mathbb{C}$.

Для каждого ненулевого элемента $x \in {}^*K$ имеет место формула (3), которая является интерпретацией соответствующей формулы, истинной в K, и в которой $\mathfrak{p}$ пробегает все внутренние простые дивизоры поля $^*K$. Рассматриваемое в этой формуле произведение является при этом *звездно конечным*, поскольку для заданного ненулевого $x \in {}^*K$ звездно конечно множество тех $\mathfrak{p} \in {}^*V$, для которых $\|x\|_{\mathfrak{p}} \neq 1$.

Для полноты изложения сделаем несколько общих замечаний о звездно конечных произведениях. Пусть A — внутренняя абелева группа, записываемая мультипликативно, и $\{\alpha_i\}$ — некоторая внутренняя последовательность элементов группы A со звездным носителем. Это означает, что индекс i пробегает некоторое внутреннее множество I; отображение $i \mapsto \alpha_i$ является внутренним отображением I в A и множество тех i, для которых $\alpha_i \neq 1$, является звездно конечным. При таких условиях произведение $\prod_{i \in I} \alpha_i$ корректным образом определяет некоторый элемент группы A. Указанное определение представляет собой интерпретацию обычного определения конечного произведения. Звездно конечные произведения удовлетворяют всем правилам, справедливым для конечных произведений и выразимым в языке L. Звездно конечное произведение не является, вообще говоря, произведением в смысле обычной алгебры, но тем не менее оно является некоторым оператором, свойственным структуре нестандартного расширения. Возникающая здесь ситуация во многом аналогична ситуации в математическом анализе, когда рассматриваются бесконечные произведения, которые не являются произведениями в смысле алгебры, а определяются при помощи предельного перехода.

В соответствии с принципом нестандартного расширения для отношений каждый простой дивизор $\mathfrak{p}$ поля K может быть единственным образом расширен до *стандартного простоя дивизора* поля $^*K$. Это стандартное расширение обозначается тем же самым символом $\mathfrak{p}$ и обладает теми же свойствами, что и исходный простой дивизор. Например, оба рассматриваемых дивизора имеют одну и ту же норму $N\mathfrak{p}$ и для каждого отличного от нуля элемента $x \in K$ задают одну и ту же норму $\|x\|_{\mathfrak{p}}$. Ввиду этого будем рассматривать простые дивизоры $\mathfrak{p} \in V$ как стандартные простые дивизоры множества $^*V$. При таком отождествлении V с множеством стандартных элементов из $^*V$ видно, что $^*V$ является расширением множества V. Ввиду бесконечности V и в соответствии с принципом нестандартного расширения для множеств выводим, что $^*V$ является собственным расширением V и что V — внешнее подмножество множества $^*V$. Из сказанного

следует, что *в поле $^*K$ существуют нестандартные простые дивизоры.*

3. Нестандартные простые дивизоры. Выясним основные свойства нестандартных простых дивизоров поля $^*K$.

Лемма 1. *Каждый нестандартный простой дивизор $\mathfrak{p}$ поля $^*K$ тривиален на K. В частности, такой дивизор $\mathfrak{p}$ обязательно неархимедов. Норма $N\mathfrak{p}$ нестандартного простого дивизора является бесконечным элементом множества $^*\mathbb{N}$. Если $x \in {}^*K$ таков, что $\|x\|_{\mathfrak{p}} > 1$, то $\|x\|_{\mathfrak{p}}$ является бесконечным элементом поля $^*\mathbb{Q}$*

Доказательство. Пусть x — ненулевой элемент поля K. Множество S тех $\mathfrak{q} \in V$, для которых $\|x\|_{\mathfrak{q}} \neq 1$, конечно и, следовательно, в соответствии с принципом расширения для множеств, это множество не изменяется при переходе к $^*V$. Другими словами, если $\mathfrak{q}$ — внутренний простой дивизор из $^*V$, для которого $\|x\|_{\mathfrak{q}} \neq 1$, то $\mathfrak{q} \in S$. В частности, так как $S \subset V$, то каждый простой дивизор $\mathfrak{q}$, для которого $\|x\|_{\mathfrak{q}} \neq 1$, необходимо стандартный. Таким образом, если $\mathfrak{p}$ — нестандартный простой дивизор, то $\|x\|_{\mathfrak{p}} = 1$ для всех ненулевых $x \in K$. Отсюда следует, что $\mathfrak{p}$ тривиален на K. Кроме того, поскольку архимедово нормирование нетривиально на $\mathbb{Q}$, мы видим, что $\mathfrak{p}$ — неархимедов простой дивизор.

Из тривиальности $\mathfrak{p}$ на K следует, что поле K изоморфно вкладывается в поле вычетов $^*K/\mathfrak{p}$. В частности, поле $^*K/\mathfrak{p}$ — бесконечно. С другой стороны, из сказанного выше следует, что поле $^*K/\mathfrak{p}$ звездно конечно, и, значит, существует внутренняя биекция этого поля на интервал $1 \leqslant \nu \leqslant N\mathfrak{p}$ из множества $^*\mathbb{N}$. Отсюда заключаем, что $N\mathfrak{p}$ является нестандартным и, стало быть, бесконечным элементом множества $^*\mathbb{N}$.

Если $\|x\|_{\mathfrak{p}} > 1$, то $v_{\mathfrak{p}}(x) < 0$. Отсюда, учитывая, что $v_{\mathfrak{p}}(x) \in {}^*\mathbb{Z}$, получаем (в силу принципа нестандартного расширения для отношений) неравенство $v_{\mathfrak{p}}(x) \leqslant -1$ (очевидным образом справедливое в $\mathbb{Z}$). В таком случае $\|x\|_{\mathfrak{p}} \geqslant N\mathfrak{p}$ и, следовательно, $\|x\|_{\mathfrak{p}}$ — бесконечный элемент поля $^*\mathbb{Q}$. Лемма доказана.

Пусть $\delta \geqslant 1$ — стандартное действительное число. Рассмотрим множество элементов $x \in K$, содержащихся в параллелотопе

$$\|x\|_{\mathfrak{p}} \leqslant \delta \tag{4}$$

для всех $\mathfrak{p} \in V$. Хорошо известно (см., например, [24, с. 164]), что множество таких $x \in K$ конечно. Согласно принципу нестандартного расширения для множеств рассматриваемое множество остается неизменным при переходе к $^*K$, и, следовательно, если $x \in {}^*K$ удовлетворяет условиям (4) для $\mathfrak{p} \in {}^*V$, то x является стандартным элементом поля $^*K$. Другими словами, если x — нестандартный элемент поля $^*K$, то условия (4) не выполняются и, значит, существует по меньшей мере один простой дивизор $\mathfrak{p} \in {}^*V$, для которого

$$\|x\|_{\mathfrak{p}} > \delta.$$

Этот дивизор $\mathfrak{p}$ может зависеть, вообще говоря, от выбора $\delta \in \mathbb{R}$. Покажем, что на самом деле можно найти такой простой дивизор $\mathfrak{p} \in {}^*V$, для которого неравенство $\|x\|_{\mathfrak{p}} > \delta$ выполняется для всех $\delta \in \mathbb{R}$. Для установления этого факта обозначим S_x множество тех $\mathfrak{p} \in {}^*V$, для которых $\|x\|_{\mathfrak{p}} > 1$ и рассмотрим отдельно два случая.

1. Множество S_x конечно. Пусть $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ — последовательность простых дивизоров из $^*V$, для которых $\|x\|_{\mathfrak{p}_n} > n$ для всех $n \in \mathbb{N} - \{0\}$. Каждый член этой последовательности содержится в конечном множестве S_x, и тогда найдется такой элемент $\mathfrak{p} \in S_x$, что $\mathfrak{p}_n = \mathfrak{p}$ для бесконечно многих $n \in \mathbb{N} - \{0\}$. Такой простой дивизор $\mathfrak{p}$ удовлетворяет неравенству $\|x\|_{\mathfrak{p}} > n$ и для всех $n \in \mathbb{N} - \{0\}$ и, значит, $\|x\|_{\mathfrak{p}}$ является бесконечным элементом поля $^*\mathbb{Q}$.

2. Множество S_x бесконечно. По самому своему определению множество S_x является внутренним, а так как оно бесконечно, то (согласно принципу выделения внешних множеств) S_x содержит нестандартный простой дивизор $\mathfrak{p}$, для которого $\|x\|_{\mathfrak{p}} > 1$. Из леммы 1 следует, что в этом случае $\|x\|_{\mathfrak{p}}$ является бесконечным элементом поля $^*\mathbb{Q}$. Приходим к следующему результату.

Лемма 2. *Пусть x — нестандартный элемент поля $^*K$. Тогда существует простой дивизор $\mathfrak{p} \in {}^*V$, для которого $\|x\|_{\mathfrak{p}}$ является бесконечным элементом поля $^*\mathbb{Q}$.*

Часто удобнее пользоваться логарифмическим значением нормы $\|x\|_{\mathfrak{p}}$:

$$w_{\mathfrak{p}}(x) = -\log \|x\|_{\mathfrak{p}} = v_{\mathfrak{p}}(x) \log (N\mathfrak{p}). \tag{5}$$

При этом бесконечно большому значению $\|x\|_{\mathfrak{p}}$ соответствует значение $w_{\mathfrak{p}}(x)$, которое меньше любого стандартного действительного числа.

Если $\mathfrak{p}$ — неархимедов простой дивизор, то $w_{\mathfrak{p}}$ является аддитивным нормированием поля $^*K$ в смысле Крулля; оно отличается от нормированной порядковой функции $v_{\mathfrak{p}}$ только множителем $\log(N\mathfrak{p})$. Следовательно, в неархимедовом случае нормирование $w_{\mathfrak{p}}(x)$ обладает свойствами

$$w_{\mathfrak{p}}(xy) = w_{\mathfrak{p}}(x) + w_{\mathfrak{p}}(y), \tag{6}$$

$$w_{\mathfrak{p}}(x + y) \geqslant \min\left(w_{\mathfrak{p}}(x), w_{\mathfrak{p}}(y)\right). \tag{7}$$

Если $\mathfrak{p}$ — архимедов простой дивизор, то первое из указанных

свойств сохраняется и выражает тот факт, что отображение $w_\mathfrak{p}\colon {}^*K \to {}^*\mathbb{R}$ является гомоморфизмом мультипликативной группы поля ${}^*K$ в аддитивную группу поля ${}^*\mathbb{R}$. Второе же свойство должно быть несколько модифицировано следующим образом.

Мы имеем

$$\|x\|_\mathfrak{p} = \begin{cases} |x|_\mathfrak{p}, & \text{если } \mathfrak{p} \text{ — вещественный дивизор,} \\ |x|_\mathfrak{p}^2, & \text{если } \mathfrak{p} \text{ — комплексный дивизор,} \end{cases}$$

и

$$|x+y|_\mathfrak{p} \leqslant |x|_\mathfrak{p} + |y|_\mathfrak{p} \leqslant 2\max(|x|_\mathfrak{p}, |y|_\mathfrak{p}).$$

Отсюда во всех случаях получаем неравенство

$$\|x+y\|_\mathfrak{p} \leqslant 4\max(\|x\|_\mathfrak{p}, \|y\|_\mathfrak{p}),$$

из которого следует, что

$$w_\mathfrak{p}(x+y) \geqslant -\log 4 + \min(w_\mathfrak{p}(x), w_\mathfrak{p}(y)). \tag{8}$$

Возникающее при этом дополнительное слагаемое $-\log 4$ конечно и исчезает лишь в случае, когда имеем дело с величинами бесконечного порядка. Остановимся на этом вопросе более подробно.

Напомним, что гипердействительное число $\alpha \in {}^*\mathbb{R}$ называется конечным, если существует положительное число $\delta \in \mathbb{R}$, для которого

$$-\delta \leqslant \alpha \leqslant \delta.$$

В частности, каждое стандартное гипердействительное число конечно. Если указанное неравенство выполняется для всякого действительного $\delta > 0$, то число α называется бесконечно малым. Каждое конечное гипердействительное число α бесконечно близко к стандартному числу α', которое представляет собой дедекиндово сечение в $\mathbb{R}$, определяемое по α.

Конечные гипердействительные числа образуют аддитивную подгруппу в ${}^*\mathbb{R}$, которую обозначим ${}^*\mathbb{R}_{\text{fin}}$. Если два числа $\alpha, \beta \in {}^*\mathbb{R}$ таковы, что их разность $\alpha - \beta$ является конечным гипердействительным числом, то скажем, что α и β — числа одного и того же *порядка значимости* и будем писать $\alpha \overset{\circ}{=} \beta$. Это означает, что α и β определяют один и тот же класс вычетов в факторгруппе

$$\mathring{\mathbb{R}} = {}^*\mathbb{R}/{}^*\mathbb{R}_{\text{fin}}.$$

Заметим, что естественная проекция ${}^*\mathbb{R} \to \mathring{\mathbb{R}}$ сохраняет имеющееся в ${}^*\mathbb{R}$ отношение порядка. Поэтому, если $\alpha, \beta \in {}^*\mathbb{R}$, то запись

$$\alpha \overset{\circ}{\leqslant} \beta$$

будет означать, что порядок значимости числа α не превосходит порядка значимости числа β. Это означает, что существует такое число $\delta \in {}^*\mathbb{R}_{\text{fin}}$, что $\beta - \alpha \geqslant \delta$. Легко проверить, что указанное отношение действительно является отношением порядка на факторгруппе $\mathring{\mathbb{R}}$.

Возвращаясь теперь к соотношениям (6)—(8), мы видим, что их можно переписать в виде

$$w_\mathfrak{p}(xy) \overset{\circ}{=} w_\mathfrak{p}(x) + w_\mathfrak{p}(y),$$

$$w_\mathfrak{p}(x+y) \overset{\circ}{\geqslant} \min(w_\mathfrak{p}(x), w_\mathfrak{p}(y)).$$

Это означает, что составное отображение

$$\mathring{w}_\mathfrak{p}\colon {}^*K \xrightarrow{w_\mathfrak{p}} {}^*\mathbb{R} \xrightarrow{\text{proj}} \mathring{\mathbb{R}}$$

является нормированием поля ${}^*K$ в смысле Крулля. Указанное нормирование тривиально на K. Действительно, если x — ненулевой элемент поля K и $\mathfrak{p}$ — стандартный простой дивизор, то $w_\mathfrak{p}(x) = -\log \|x\|_\mathfrak{p}$ суть стандартный и, следовательно, конечный элемент поля ${}^*\mathbb{R}$. В таком случае мы имеем, что $w_\mathfrak{p}(x) \overset{\circ}{=} 0$. Если же $\mathfrak{p}$ — нестандартный простой дивизор, то ввиду леммы 1 $w_\mathfrak{p}(x) = 0$ и, значит, $w_\mathfrak{p}(x) \overset{\circ}{=} 0$. Таким образом, нами получен следующий результат.

Теорема 1. *Каждый простой дивизор $\mathfrak{p} \in {}^*V$ определяет нормирование $\mathring{w}_\mathfrak{p}$ поля ${}^*K$ со значениями в группе $\mathring{\mathbb{R}}$, тривиальное на поле K.*

Если $\mathfrak{p}$ — стандартный простой дивизор, то нетрудно проверить, что множество значений нормирования $\mathring{w}_\mathfrak{p}$ совпадает со всей группой $\mathring{\mathbb{R}}$ и что его поле вычетов изоморфно $\mathfrak{p}$-адическому пополнению поля K. Если же $\mathfrak{p}$ — нестандартный простой дивизор, то множество значений нормирования $\mathring{w}_\mathfrak{p}$ является собственной подгруппой группы $\mathring{\mathbb{R}}$. В этом случае нормирование $\mathring{w}_\mathfrak{p}$ эквивалентно исходному нормированию $w_\mathfrak{p}$ и оба эти нормирования имеют изоморфные группы значений и поля вычетов.

Если x — нестандартный элемент поля ${}^*K$, то по лемме 2 существует по меньшей мере один простой дивизор $\mathfrak{p} \in {}^*V$, для которого $w_\mathfrak{p}(x) \overset{\circ}{<} 0$ (это означает, в частности, что $\mathring{w}_\mathfrak{p}$ не обращается в нуль на x). Следовательно, рассматриваемые нормирования $\mathring{w}_\mathfrak{p}$ могут быть использованы для построения теории дивизоров поля ${}^*K$, которая описывает ${}^*K$ по отношению к K как к его основному полю. Ситуация вполне аналогична случаю поля

функций на кривой, где также имеется поле констант. Оставшуюся часть параграфа посвятим развитию теории дивизоров поля $*K$.

4. Внутренние дивизоры. Начнем рассуждения с понятия дивизора в алгебраическом числовом поле K. Это понятие вводится обычным образом (см., например, [19, гл. 3]) с одним дополнительным условием, что наряду с неархимедовыми простыми рассматриваются также и архимедовы простые дивизоры. При рассмотрении дивизоров поля K мы будем использовать аддитивную запись.

Определение 1. *Группой дивизоров* $\mathfrak{D}$ поля K называется прямая сумма

$$\mathfrak{D} = \mathfrak{D}' \oplus \mathfrak{D}'',$$

где $\mathfrak{D}'$ — свободный $\mathbb{R}$-модуль, порожденный архимедовыми простыми дивизорами и $\mathfrak{D}''$ — свободный $\mathbb{Z}$-модуль, порожденный неархимедовыми простыми дивизорами.

Это означает, что каждый дивизор $\mathfrak{a} \in \mathfrak{D}$ имеет единственное представление в виде

$$\mathfrak{a} = \sum_{\mathfrak{p}} \alpha_{\mathfrak{p}} \cdot \mathfrak{p}, \tag{9}$$

где $\mathfrak{p}$ пробегает все простые дивизоры из V, а коэффициенты $\alpha_{\mathfrak{p}}$ удовлетворяют следующим условиям:

1) $\alpha_{\mathfrak{p}} \in \mathbb{R}$, если $\mathfrak{p}$ — архимедов простой дивизор;

2) $\alpha_{\mathfrak{p}} \in \mathbb{Z}$, если $\mathfrak{p}$ — неархимедов простой дивизор;

3) $\alpha_{\mathfrak{p}} = 0$ для почти всех $\mathfrak{p} \in V$ (всех $\mathfrak{p} \in V$ за исключением их конечного числа).

Другими словами, группа $\mathfrak{D}$ может быть представлена как группа всех функций $\alpha\colon V \to \mathbb{R}$, удовлетворяющих условиям 1)—3).

Каждый ненулевой элемент $x \in K$ определяет дивизор $(x) \in \mathfrak{D}$, а именно *главный дивизор*

$$(x) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(x) \cdot \mathfrak{p}. \tag{10}$$

Отображение $x \mapsto (x)$ задает гомоморфизм $K^* \to \mathfrak{D}$ мультипликативной группы K^* в аддитивную группу $\mathfrak{D}$. Ядро этого гомоморфизма состоит из корней из 1, содержащихся в K. В частности, указанное ядро конечно. Множество главных дивизоров образуют подгруппу $\mathfrak{P}$ группы $\mathfrak{D}$.

Определение 2. Факторгруппа $\mathfrak{C} = \mathfrak{D}/\mathfrak{P}$ называется *группой классов дивизоров* поля K.

Дадим теперь интерпретацию введенных выше понятий в нестандартном расширении $*K$ поля K. При такой интерпретации $*\mathfrak{D}$ представляет собой группу всех внутренних дивизоров. Внутренние простые дивизоры $\mathfrak{p} \in *V$ содержатся в $*\mathfrak{D}$ и каждый дивизор $\mathfrak{a} \in *\mathfrak{D}$ допускает единственное представление в виде

(9), где $\mathfrak{p}$ пробегает все простые дивизоры из $*V$. При этом коэффициенты $\alpha_{\mathfrak{p}}$ удовлетворяют следующим условиям:

*1) $\alpha_{\mathfrak{p}} \in *\mathbb{R}$, если $\mathfrak{p}$ — архимедов простой дивизор;

*2) $\alpha_{\mathfrak{p}} \in *\mathbb{Z}$, если $\mathfrak{p}$ — неархимедов простой дивизор;

*3) множество тех $\mathfrak{p} \in *V$, для которых $\alpha_{\mathfrak{p}} \neq 0$, звездно конечно.

*4) функция $\mathfrak{p} \mapsto \alpha_{\mathfrak{p}}$, задающая отображение $*V$ в $*\mathbb{R}$, внутренняя.

Другими словами, группа $*\mathfrak{D}$ может быть представлена как группа всех внутренних функций $\alpha\colon *V \to *\mathbb{R}$, удовлетворяющих условиям *1)—*3).

Как и в случае поля K, имеет место разложение

$$*\mathfrak{D} = *\mathfrak{D}' \oplus *\mathfrak{D}'',$$

где $*\mathfrak{D}'$ — архимедова, а $*\mathfrak{D}''$ — неархимедова компоненты группы $*\mathfrak{D}$.

Отображение $K \to \mathfrak{D}$, задаваемое при помощи сопоставления $x \mapsto (x)$, имеет стандартное расширение

$$*K \to *\mathfrak{D},$$

которое описывается формулой (10). Так как ядро отображения $K \to \mathfrak{D}$ конечно, оно не расширяется при переходе к $*K$ и, следовательно, ядро отображения $*K \to *\mathfrak{D}$ конечно и состоит в точности из корней из 1, содержащихся в K. Образ мультипликативной группы поля $*K$ при гомоморфизме $*K \to *\mathfrak{D}$ назовем *группой внутренних главных дивизоров* и обозначим ее $*\mathfrak{P}$.

Определение 3. Факторгруппа $*\mathfrak{C} = *\mathfrak{D}/*\mathfrak{P}$ называется *группой классов внутренних дивизоров* поля $*K$.

Обозначим коэффициент $\alpha_{\mathfrak{p}}$ в соотношении (9) $v_{\mathfrak{p}}(\mathfrak{a})$ и определим $\mathfrak{p}$-*адическую норму* $\|\mathfrak{a}\|_{\mathfrak{p}}$ дивизора $\mathfrak{a} \in *\mathfrak{D}$ равенством

$$\|\mathfrak{a}\|_{\mathfrak{p}} = (N\mathfrak{p})^{-v_{\mathfrak{p}}(\mathfrak{a})}.$$

Нам снова удобнее будет логарифмическое значение этой нормы

$$w_{\mathfrak{p}}(\mathfrak{a}) = -\log \|\mathfrak{a}\|_{\mathfrak{p}} = v_{\mathfrak{p}}(\mathfrak{a}) \log (N\mathfrak{p}).$$

Заметим, что для архимедова $\mathfrak{p}$ мы определили $N\mathfrak{p}$ таким образом, что $\log(N\mathfrak{p}) = 1$. Стало быть, в этом случае $w_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{a})$.

Каждый дивизор $\mathfrak{a} \in *\mathfrak{D}$ однозначно определяется заданием значений $w_{\mathfrak{p}}(\mathfrak{a})$ для всех $\mathfrak{p} \in *V$. В частности, можно сложение дивизоров задать соотношениями

$$w_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = w_{\mathfrak{p}}(\mathfrak{a}) + w_{\mathfrak{p}}(\mathfrak{b})$$

для всех $\mathfrak{p} \in *V$. Отношения

$$w_{\mathfrak{p}}(\mathfrak{a}) \leqslant w_{\mathfrak{p}}(\mathfrak{b})$$

для всех $\mathfrak{p}$ задают отношение частичного порядка $\mathfrak{a} \leqslant \mathfrak{b}$ на $^*\mathfrak{D}$. Если $\mathfrak{a} \leqslant \mathfrak{b}$, то будем говорить, что $\mathfrak{b}$ делит $\mathfrak{a}$. Дивизоры $\mathfrak{c}$ и $\mathfrak{b}$, для которых $w_\mathfrak{p}(\mathfrak{c}) = \max\left(w_\mathfrak{p}(\mathfrak{a}),\ w_\mathfrak{p}(\mathfrak{b})\right)$ и $w_\mathfrak{p}(\mathfrak{b}) = \min\left(w_\mathfrak{p}(\mathfrak{a}),\ w_\mathfrak{p}(\mathfrak{b})\right)$, называются соответственно *наименьшим общим кратным* $\mathfrak{c} = \{\mathfrak{a}, \mathfrak{b}\}$ и *наибольшим общим делителем* $\mathfrak{b} = (\mathfrak{a}, \mathfrak{b})$ дивизоров $\mathfrak{a}$ и $\mathfrak{b}$.

Назовем число

$$\sigma(\mathfrak{a}) = \sum_\mathfrak{p} w_\mathfrak{p}(\mathfrak{a}) = \sum_\mathfrak{p} v_\mathfrak{p}(\mathfrak{a}) \log(N\mathfrak{p}) \tag{11}$$

размером дивизора

$$\mathfrak{a} = \sum_\mathfrak{p} v_\mathfrak{p}(\mathfrak{a}) \cdot \mathfrak{p}.$$

Если формула (11) рассматривается в $\mathfrak{D}$, то она задает гомоморфизм $\sigma\colon \mathfrak{D} \to \mathbb{R}$. Если же эта формула рассматривается как интерпретация в $^*\mathfrak{D}$ (в этом случае сумма звездно конечна), то получаем гомоморфизм $\sigma\colon {}^*\mathfrak{D} \to {}^*\mathbb{R}$, который представляет собой стандартное расширение гомоморфизма $\sigma\colon \mathfrak{D} \to \mathbb{R}$. В любом из этих случаев гомоморфизм σ сюръективен. Обозначим его ядро соответственно $\mathfrak{D}_0$ и $^*\mathfrak{D}_0$. Принимая во внимание соотношение (3), которое может быть переписано в виде

$$\sum_\mathfrak{p} w_\mathfrak{p}(x) = 0,$$

мы видим, что главные дивизоры содержатся соответственно в $\mathfrak{D}_0$ и $^*\mathfrak{D}_0$. Назовем факторгруппы $\mathfrak{C}_0 = \mathfrak{D}_0/\mathfrak{P}$ и $\mathfrak{C} = {}^*\mathfrak{D}_0/{}^*\mathfrak{P}$ *группами классов дивизоров размера нуль*.

Будем рассматривать $\mathfrak{D}$ как подгруппу группы $^*\mathfrak{D}$, т. е. как подгруппу всех стандартных дивизоров. Дивизор $\mathfrak{a} \in {}^*\mathfrak{D}$ назовем *конечным*, если существует такой стандартный дивизор $\mathfrak{c} > 0$, $-\mathfrak{c} \leqslant \mathfrak{a} \leqslant \mathfrak{c}$. Мы видим, в частности, что все стандартные дивизоры конечны. Если неравенства $-\mathfrak{c} \leqslant \mathfrak{a} \leqslant \mathfrak{c}$ выполняются для каждого стандартного $\mathfrak{c} > 0$, то дивизор $\mathfrak{a}$ назовем *бесконечно малым*. Это означает, что $w_\mathfrak{p}(\mathfrak{a}) = 0$ для неархимедова $\mathfrak{p}$ и что $w_\mathfrak{p}(\mathfrak{a})$ — бесконечно малое гипердействительное число для архимедова $\mathfrak{p}$. Каждый конечный дивизор $\mathfrak{a}$ бесконечно близок к соответствующему стандартному дивизору ${}^0\mathfrak{a}$.

Конечные дивизоры образуют подгруппу $^*\mathfrak{D}_{\text{fin}}$ группы $^*\mathfrak{D}$.

Определение 4. Факторгруппа

$$\mathring{\mathfrak{D}} = {}^*\mathfrak{D}/{}^*\mathfrak{D}_{\text{fin}}$$

называется *группой дивизорных порядков значимости*.

Как и в случае гипердействительных чисел, запись $\mathfrak{a} \mathring{=} \mathfrak{b}$ будет означать, что дивизоры $\mathfrak{a}$ и $\mathfrak{b}$ имеют один и тот же *порядок значимости* и, следовательно, определяют один и тот же

класс вычетов в группе $\mathring{\mathfrak{D}}$. Далее, запись $\mathfrak{a} \mathring{\leqslant} \mathfrak{b}$ будет означать, что существует такой дивизор $\mathfrak{c} \in {}^*\mathfrak{D}_{\text{fin}}$, что $\mathfrak{b} - \mathfrak{a} \geqslant \mathfrak{c}$. В соответствии с этим получаем отношение частичного порядка на $\mathring{\mathfrak{D}}$, обладающее тем свойством, что оно наследует отношение частичного порядка на $^*\mathfrak{D}$ при естественной проекции ${}^*\mathfrak{D} \to \mathring{\mathfrak{D}}$. При этом сохраняются операции взятия наибольшего общего делителя и наименьшего общего кратного.

Группа $\mathring{\mathfrak{D}}$ будет играть центральную роль в наших дальнейших рассмотрениях. Мы можем рассматривать $\mathring{\mathfrak{D}}$ как группу, состоящую из тех же самых элементов, что и группа $^*\mathfrak{D}$, но вместо знака $=$ использовать знак $\mathring{=}$, задающий один и тот же порядок значимости. В этом смысле следующая лемма фактически содержит утверждение о группе $\mathring{\mathfrak{D}}$.

Лемма 3. *Пусть* $\mathfrak{a}$, $\mathfrak{b}$ — *внутренние дивизоры из* $^*\mathfrak{D}$. *Для того чтобы выполнялось соотношение* $\mathfrak{a} \mathring{\leqslant} \mathfrak{b}$, *необходимо и достаточно, чтобы*

$$w_\mathfrak{p}(\mathfrak{a}) \mathring{\leqslant} w_\mathfrak{p}(\mathfrak{b})$$

для всех $\mathfrak{p} \in {}^*V$. *В частности, соотношение* $\mathfrak{a} \mathring{=} \mathfrak{b}$ *эквивалентно выполнимости соотношений* $w_\mathfrak{p}(\mathfrak{a}) \mathring{=} w_\mathfrak{p}(\mathfrak{b})$ *для всех* $\mathfrak{p} \in {}^*V$.

Доказательство. Если $\mathfrak{a} \mathring{\leqslant} \mathfrak{b}$, то существует стандартный дивизор $\mathfrak{c}$, для которого $\mathfrak{b} - \mathfrak{a} \geqslant \mathfrak{c}$. Отсюда следует, что

$$w_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) = w_\mathfrak{p}(\mathfrak{b}) - w_\mathfrak{p}(\mathfrak{a}) \geqslant w_\mathfrak{p}(\mathfrak{c}).$$

Так как $\mathfrak{c}$ — стандартный элемент, то $w_\mathfrak{p}(\mathfrak{c})$ — стандартное гипердействительное число, и, в таком случае, $w_\mathfrak{p}(\mathfrak{a}) \mathring{\leqslant} w_\mathfrak{p}(\mathfrak{b})$.

Обратно, предположим, что $w_\mathfrak{p}(\mathfrak{a}) \mathring{\leqslant} w_\mathfrak{p}(\mathfrak{b})$ для каждого $\mathfrak{p} \in {}^*V$. Это означает, что существуют также стандартные гипердействительные числа $\gamma_\mathfrak{p}$, что $w_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) \geqslant \gamma_\mathfrak{p}$. По определению имеем

$$w_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) = v_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) \log(N\mathfrak{p}).$$

Если $\mathfrak{p}$ — нестандартный простой дивизор, то его норма $N\mathfrak{p}$ является бесконечным элементом множества $^*\mathbb{N}$ и таковым же элементом поля $^*\mathbb{R}$ является $\log(N\mathfrak{p})$. Следовательно, если $v_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) < 0$, то получаем $w_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) < \gamma_\mathfrak{p}$ и приходим к противоречию. В таком случае $v_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) \geqslant 0$ и тогда $w_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) \geqslant 0$ для каждого нестандартного простого дивизора $\mathfrak{p}$.

Обозначим S множество тех $\mathfrak{p} \in {}^*V$, для которых $w_\mathfrak{p}(\mathfrak{b} - \mathfrak{a}) < 0$. Тогда S — внутреннее множество, не содержащее нестандартных дивизоров. Отсюда, в соответствии с принципом выде-

ления внешних множеств, заключаем, что S — конечное множество. Каждый элемент $\mathfrak{p} \in S$ является стандартным и поэтому $\log(N\mathfrak{p})$ — стандартное положительное число. В таком случае числа $\gamma_{\mathfrak{p}}/\log(N\mathfrak{p})$ — также стандартные для всех $\mathfrak{p} \in S$. Пусть γ — стандартная нижняя граница для этих чисел. Можно считать, что $\gamma \in \mathbb{Z}$, и тогда дивизор

$$\mathfrak{c} = \gamma \sum_{\mathfrak{p} \in S} \mathfrak{p}$$

является стандартным дивизором, удовлетворяющим неравенству $\mathfrak{c} \leqslant \mathfrak{b} - \mathfrak{a}$. Действительно, для $\mathfrak{p} \in S$ имеем по построению

$$w_{\mathfrak{p}}(\mathfrak{c}) = \gamma \log(N\mathfrak{p}) \leqslant \gamma_{\mathfrak{p}} \leqslant w_{\mathfrak{p}}(\mathfrak{b} - \mathfrak{a}).$$

Если же $\mathfrak{p} \notin S$, то

$$w_{\mathfrak{p}}(\mathfrak{c}) = 0 \leqslant w_{\mathfrak{p}}(\mathfrak{b} - \mathfrak{a}).$$

Таким образом, нами найден стандартный дивизор $\mathfrak{c}$, для которого $\mathfrak{b} - \mathfrak{a} \geqslant \mathfrak{c}$. Значит, $\mathfrak{a} \leqslant \mathfrak{b}$ и лемма, тем самым, доказана.

Для дивизора $\mathfrak{a} \in {}^*\mathfrak{D}$ обозначим $\overset{\circ}{w}_{\mathfrak{p}}(\mathfrak{a})$ порядок значимости числа $w_{\mathfrak{p}}(\mathfrak{a})$, так что $\overset{\circ}{w}_{\mathfrak{p}}(\mathfrak{a}) \in \overset{\circ}{\mathbb{R}}$. Согласно лемме 3 $w_{\mathfrak{p}}(\mathfrak{a})$ зависит только от порядка значимости дивизора $\mathfrak{a}$. Другими словами, если мы рассмотрим дивизор $\mathfrak{a}$ как элемент группы $\overset{\circ}{\mathfrak{D}}$, то $\overset{\circ}{w}_{\mathfrak{p}}(\mathfrak{a})$ корректным образом определяется как элемент из $\overset{\circ}{\mathbb{R}}$. Если $\mathfrak{p}$ пробегает все элементы из ${}^*V$, то получаем функцию $\mathfrak{p} \mapsto \overset{\circ}{w}_{\mathfrak{p}}(\mathfrak{a})$, задающую отображение из ${}^*V$ в ${}^*\mathbb{R}$. Лемма 3 показывает, что $\mathfrak{a} \in \overset{\circ}{\mathfrak{D}}$ определяется этой функцией единственным образом. Таким образом, группа $\overset{\circ}{\mathfrak{D}}$ может быть точно представлена как некоторая группа функций, задающих отображение ${}^*V$ в $\overset{\circ}{\mathbb{R}}$.

Пусть x — ненулевой элемент поля K. Рассмотрим главный дивизор $(x) \in {}^*D$ и его образ в $\overset{\circ}{\mathfrak{D}}$. Функция, представляющая этот образ, имеет вид $\mathfrak{p} \mapsto \overset{\circ}{w}_{\mathfrak{p}}(x)$, где $\overset{\circ}{w}_{\mathfrak{p}}$ — введенное выше нормирование Крулля поля ${}^*K$ над K. Значит, если рассматривать (x) как элемент группы $\overset{\circ}{\mathfrak{D}}$, то он содержит информацию о значении x во всех нормированиях $\overset{\circ}{w}_{\mathfrak{p}}$. Ввиду этого элемент $(x) \in \overset{\circ}{\mathfrak{D}}$ надо рассматривать как «главный дивизор» элемента x относительно нормирований $\overset{\circ}{w}_{\mathfrak{p}}$. Если каждому $x \in {}^*K$ сопоставим его главный дивизор $(x) \in \overset{\circ}{\mathfrak{D}}$, то получим составное отображение

$${}^*K \to {}^*\mathfrak{D} \xrightarrow{\text{proj}} \overset{\circ}{\mathfrak{D}},$$

состоящее из внутреннего отображения ${}^*K \to {}^*\mathfrak{D}$ и проекции ${}^*\mathfrak{D}$ на $\overset{\circ}{\mathfrak{D}}$. В этом смысле элементы из $\overset{\circ}{\mathfrak{D}}$ будем называть «дивизорами», а группу $\overset{\circ}{\mathfrak{D}}$ — «группой дивизоров».

Если x — стандартный элемент, то (x) также стандартный элемент и, в таком случае, $(x) = 0$. С другой стороны, если x — нестандартный элемент поля ${}^*K$, то ввиду леммы 2 имеем $(x) \neq 0$. Следовательно, лемма 2 дает описание ядра составного отображения ${}^*K \to \overset{\circ}{\mathfrak{D}}$ и утверждает, что это ядро представляет собой мультипликативную группу поля K. Можно выразить этот факт другими словами, сказав, что последовательность отображений

$$1 \to K \to {}^*K \to \overset{\circ}{\mathfrak{D}}$$

точна. Опишем теперь образ отображения ${}^*K \to \overset{\circ}{\mathfrak{D}}$. Для этого рассмотрим гомоморфизм σ: ${}^*\mathfrak{D} \to {}^*\mathbb{R}$, определенный соотношением (11). Если $\mathfrak{a} = \mathfrak{b}$, то $\sigma(\mathfrak{a}) = \sigma(\mathfrak{b})$ и, следовательно, σ определяет отображение σ: $\overset{\circ}{\mathfrak{D}} \to \overset{\circ}{\mathbb{R}}$, которое сюръективно ввиду сюръективности исходного гомоморфизма σ. Ядро этого отображения состоит из тех внутренних дивизоров $\mathfrak{a}$, для которых размер $\sigma(\mathfrak{a})$ конечен. Для каждого такого дивизора $\mathfrak{a}$ можно найти дивизор $\mathfrak{a}_0$, удовлетворяющий условиям: $\mathfrak{a}_0 = 0$ и $\sigma(\mathfrak{a}_0) = 0$. Действительно, если $\sigma(\mathfrak{a}) = \delta$, где δ — некоторое конечное гипердействительное число, и $\mathfrak{p}$ — архимедов простой дивизор, то $\sigma(\delta\mathfrak{p}) = \delta$ и, следовательно, можно положить $\mathfrak{a}_0 = \mathfrak{a} - \delta\mathfrak{p}$. Отсюда следует, что каждый элемент из $\overset{\circ}{\mathfrak{D}}_0$ может быть представлен дивизором размера 0, т. е. дивизором из ${}^*\mathfrak{D}_0$. Другими словами, $\overset{\circ}{\mathfrak{D}}_0$ состоит из порядков значимости дивизоров, имеющих нулевой размер.

Из формулы (3) следует, что размер любого главного дивизора равен нулю. Отсюда получаем, что образ введенного составного отображения ${}^*K \to \overset{\circ}{\mathfrak{D}}$ содержится в $\overset{\circ}{\mathfrak{D}}_0$.

Теорема 2. *Каждый дивизор в $\overset{\circ}{\mathfrak{D}}_0$ — главный, т. е. является образом некоторого ненулевого элемента x поля ${}^*K$ при отображении ${}^*K \to \overset{\circ}{\mathfrak{D}}$. Более того, последовательность отображений*

$$1 \to K \to {}^*K \to \overset{\circ}{\mathfrak{D}} \xrightarrow{\sigma} \overset{\circ}{\mathbb{R}} \to 0$$

точна.

Доказательство. Пусть $\mathfrak{a} \in {}^*\mathfrak{D}$. Надо показать, что образ дивизора $\mathfrak{a}$ в $\overset{\circ}{\mathfrak{D}}_0$ представляет собой главный дивизор. Это означает, что в поле ${}^*K$ имеется такой элемент x, что $\mathfrak{a} = \overset{\circ}{(x)}$ или что $\mathfrak{a} = (x) + \mathfrak{b}$ для некоторого конечного дивизора $\mathfrak{b} \in {}^*\mathfrak{D}_0$. Таким образом, достаточно показать, что $\mathfrak{a}$ *эквивалентен* некоторому конечному дивизору $\mathfrak{b}$ ($\mathfrak{a} \sim \mathfrak{b}$). Для этого достаточно, в свою очередь, установить существование такого стандартного дивизора $\mathfrak{c} \geqslant 0$, для которого справедливо следующее утверждение: *каждый дивизор* $\mathfrak{a} \in {}^*\mathfrak{D}_0$ *эквивалентен некоторому дивизору* $\mathfrak{b} \in {}^*\mathfrak{D}_0$, *удовлетворяющему условию* $-\mathfrak{c} \leqslant \mathfrak{b} \leqslant \mathfrak{c}$.

Это утверждение является интерпретацией в ${}^*\mathfrak{D}$ соответствующего утверждения в $\mathfrak{D}$ и справедливо в ${}^*\mathfrak{D}$ в том и только в том случае, если исходное утверждение справедливо в $\mathfrak{D}$. Таким образом, достаточно установить справедливость следующего утверждения: *каждый дивизор* $\mathfrak{a} \in \mathfrak{D}$ *эквивалентен некоторому дивизору* $\mathfrak{b} \in \mathfrak{D}_0$, *удовлетворяющему условию* $-\mathfrak{c} \leqslant \mathfrak{b} \leqslant \mathfrak{c}$.

Согласно определению группы $\mathfrak{D}$ имеет место разложение $\mathfrak{D} = \mathfrak{D}' \oplus \mathfrak{D}''$, где $\mathfrak{D}'$ — архимедова часть и $\mathfrak{D}''$ — неархимедова часть группы дивизоров $\mathfrak{D}$. Если ввести в рассмотрение проекцию $\mathfrak{D} \to \mathfrak{D}''$, имеющую своим ядром $\mathfrak{D}'$, то двойное отображение $K \to \mathfrak{D} \to \mathfrak{D}''$ приводит к факторгруппе $\mathfrak{C}'' = \mathfrak{D}''/\mathfrak{P}$, представляющей собой неархимедову часть группы классов дивизоров $\mathfrak{C} = \mathfrak{D}/\mathfrak{P}$. Хорошо известно (см. [19, гл. 3]), что $\mathfrak{C}$ — конечная группа, порядок которой называется числом классов h поля K.

Ограничение проекции $\mathfrak{D} \to \mathfrak{D}''$ на $\mathfrak{D}_0$ остается сюръективным. Действительно, пусть $\mathfrak{a}'' = \mathfrak{D}''$, $\sigma(\mathfrak{a}'') = \delta$ и $\mathfrak{p}$ — архимедов простой дивизор. Тогда дивизор $\mathfrak{a}'' - \delta\mathfrak{p}$ имеет размер 0 и проектируется на $\mathfrak{a}''$.

В силу сюръективности проекции $\mathfrak{D}_0 \to \mathfrak{D}''$ существуют дивизоры $\mathfrak{c}_1, \ldots, \mathfrak{c}_h \in \mathfrak{D}_0$, образы которых в $\mathfrak{D}''$ представляют различные классы в $\mathfrak{C}''$. Обозначим эти образы $\mathfrak{c}_1'', \ldots, \mathfrak{c}_h''$ и рассмотрим произвольный дивизор $\mathfrak{a} \in \mathfrak{D}_0$. Его образ в $\mathfrak{D}''$ эквивалентен (по модулю главных дивизоров в $\mathfrak{D}''$) одному из дивизоров $\mathfrak{c}_j''$. Поэтому в $\mathfrak{D}$ мы имеем эквивалентность $\mathfrak{a} \sim \mathfrak{c}_j + \mathfrak{a}'$, где $\mathfrak{a}' \in \mathfrak{D}' \cap \mathfrak{D}_0$.

Для изучения дивизора $\mathfrak{a}'$ положим $\mathfrak{D}_0' = \mathfrak{D}' \cap \mathfrak{D}_0$ и заметим, что группа $\mathfrak{D}_0'$ представляет собой ядро в $\mathfrak{D}'$ отображения $\sigma\colon \mathfrak{D}' \to \mathbb{R}$. По определению, $\mathfrak{D}'$ является свободным $\mathbb{R}$ модулем, порожденным архимедовыми простыми дивизорами. Другими словами, если r — число архимедовых простых дивизоров, то $\mathfrak{D}'$ представляет собой действительное r-мерное векторное пространство. Так как отображение $\sigma\colon \mathfrak{D}' \to \mathbb{R}$ является $\mathbb{R}$-линейным, то $\mathfrak{D}_0'$ представляет собой $(r-1)$-мерное подпространство в $\mathfrak{D}'$. Это подпространство содержит те главные дивизоры, которые полностью содержатся в $\mathfrak{D}'$ и, следовательно,

являются дивизорами единиц $u \in K$. По теореме Дирихле (см. [19, гл. 2]) группа единиц поля K является конечно порожденной группой ранга $r-1$. Более того, если $u_1, \ldots, u_{r-1}$ — основные единицы, то их главные дивизоры $(u_1), \ldots, (u_{r-1})$ образуют базис $\mathfrak{D}_0'$ над полем $\mathbb{R}$.

Из сказанного следует, что каждый дивизор $\mathfrak{a}' \in \mathfrak{D}_0'$ единственным образом представляется в виде

$$\mathfrak{a}' = \sum_{i=1}^{r-1} \alpha_i \cdot (u_i), \quad \alpha_i \in \mathbb{R}.$$

Пусть $n_i = [\alpha_i]$, так что $\alpha_i = n_i + \delta_i$, где $0 \leqslant \delta_i < 1$. Тогда

$$\mathfrak{a}' = \sum_{i=1}^{r-1} n_i \cdot (u_i) + \sum_{i=1}^{r-1} \delta_i \cdot (u_i) = (u) + \mathfrak{b}' \sim \mathfrak{b}',$$

где $u = u_1^{n_1} \ldots u_{r-1}^{n_{r-1}}$ — единица поля K и $\mathfrak{b}' = \sum_{i=1}^{r-1} \delta_i \cdot (u_i)$. Поскольку коэффициенты δ_i дивизора $\mathfrak{b}'$ ограничены, то $\mathfrak{b}'$ содержится в ограниченной области. Следовательно, можно указать такой дивизор $\mathfrak{c}' \geqslant 0$, не зависящий от δ_i, что $-\mathfrak{c}' \leqslant \mathfrak{b}' \leqslant \mathfrak{c}'$. Именно, если $\mathfrak{c}_i'$ — наименьшее общее кратное дивизоров 0, (u_i), $-(u_i)$, то в качестве $\mathfrak{c}'$ может быть выбран дивизор

$$\sum_{i=1}^{r-1} \mathfrak{c}_i'.$$

Мы показали, что каждый дивизор $\mathfrak{a}' \in \mathfrak{D}_0'$ эквивалентен некоторому дивизору $\mathfrak{b}'$ такому, что $-\mathfrak{c}' \leqslant \mathfrak{b}' \leqslant \mathfrak{c}'$. Следовательно, по сказанному выше, каждый дивизор $\mathfrak{a} \in \mathfrak{D}_0$ эквивалентен некоторому дивизору $\mathfrak{c}_j + \mathfrak{b}'$, где $1 \leqslant j \leqslant h$ и $-\mathfrak{c}' \leqslant \mathfrak{b}' \leqslant \mathfrak{c}'$. Положим

$$\mathfrak{c} = \mathfrak{c}_0 + \mathfrak{c}',$$

где $\mathfrak{c}_0$ — наименьшее общее кратное дивизоров $0, \pm\mathfrak{c}_1, \ldots, \pm\mathfrak{c}_h$. Тогда дивизор $\mathfrak{a}$ эквивалентен дивизору $\mathfrak{b} = \mathfrak{c}_j + \mathfrak{b}'$, который удовлетворяет условию $-\mathfrak{c} \leqslant \mathfrak{b} \leqslant \mathfrak{c}$. Теорема доказана.

Заметим, что при доказательстве теоремы 2 нами существенным образом были использованы теорема Дирихле об единицах и теорема о конечности числа классов h. Легко видеть, что доказанная только что теорема фактически эквивалента этим двум теоремам.

В заключении параграфа хотелось бы отметить аналогию между утверждением теоремы 2 и соответствующим утверждением для полей рациональных функций с коэффициентами из K. Именно, в последнем случае каждый дивизор степени нуль также является главным. В этом отношении расширение ${}^*K$ поля K вполне подобно полю рациональных функций и, значит, ${}^*K$

можно рассматривать в некотором смысле как поле функций односвязного пространства. Из дальнейшего будет видно, что по отношению к некоторому его функциональному подполю поле $^*K$ во многом аналогично полю функций универсального накрывающего пространства.

Задачи

1. *Нормой* $\|\ \|$ поля K называется функция, определенная на K, принимающая неотрицательные вещественные значения и удовлетворяющая следующим аксиомам:

1) $\|x\| = 0 \Leftrightarrow x = 0$;

2) $\|xy\| = \|x\| \cdot \|y\|$;

3) существует константа $c > 0$ такая, что $\|1 + x\| \leqslant c$ при всех $\|x\| \leqslant 1$.

Норма $\|\ \|$ поля K называется *тривиальной*, если $\|x\| = 1$ для всех $x \neq 0$. Две нормы $\|\ \|_1$ и $\|\ \|_2$ поля K называются *эквивалентными*, если существует положительное действительное число τ такое, что

$$\|x\|_2 = \|x\|_1^\tau$$

для всех $x \in K$. Норма $\|\ \|$ поля K называется *дискретной*, если найдется такое $\delta > 0$, что из условия $1 - \delta < \|x\| < 1 + \delta$ следует равенство $\|x\| = 1$.

Доказать справедливость следующих утверждений:

а) Всякая норма поля K эквивалентна норме с константой $c = 2$.

б) Для нормы с константой $c = 2$ справедливо неравенство треугольника

$$\|x + y\| \leqslant \|x\| + \|y\|.$$

(Указание. Установить индукцией по s, что

$$\left\| \sum_{i=1}^{2^s} x_i \right\| \leqslant 2^s \max_{1 \leqslant i \leqslant 2^s} \|x_i\|$$

и вывести отсюда, что для любого целого $n \geqslant 1$ справедливо неравенство

$$\left\| \sum_{i=1}^{n} x_i \right\| \leqslant 2n \max_{1 \leqslant i \leqslant n} \|x_i\|.$$

Используя последнее неравенство, показать, что

$$\|x + y\| \leqslant \{4(n+1)(\|x\| + \|y\|)^n\}^{1/n};$$

затем перейти к пределу при $n \to \infty$.)

в) Если $\|\ \|$ — дискретная норма поля K, то найдется такое действительное число ρ, $0 < \rho < 1$, что значения нормы $\|\ \|$ на отличных от нуля элементах поля K совпадают с множеством $\{\rho^v \mid v \in \mathbb{Z}\}$ (если $\|x\| = \rho^v$, то $v = v(x)$ называется *порядковой функцией* элемента $x \neq 0$, а отображение $v\colon K^* \to \mathbb{Z}$ — *дискретным нормированием* поля K).

2. Норма $\|\ \|$ поля K называется *неархимедовой*, если в аксиоме 3) (см. предыдущую задачу) можно положить $c = 1$, т. е. если

$$\|x + y\| \leqslant \max(\|x\|, \|y\|).$$

В противном случае норма $\|\ \|$ называется *архимедовой*. Установить справедливость следующих свойств неархимедовых норм:

а) если $\|x\| < \|y\|$, то $\|x + y\| = \|y\|$;

б) множество тех $x \in K$, для которых $\|x\| \leqslant 1$, является подкольцом поля K (которое называется *кольцом нормирования* поля K относительно нормы $\|\ \|$ и обозначается $\mathfrak{o}$);

в) две нормы поля K эквивалентны тогда и только тогда, когда им соответствует одно и то же кольцо нормирования $\mathfrak{o}$;

г) множество $\mathfrak{m}$ элементов x поля K, таких, что $\|x\| < 1$ является единственным максимальным идеалом кольца $\mathfrak{o}$ (этот идеал однозначно определяет соответствующий *неархимедов простой дивизор* $\mathfrak{p}$ поля K);

д) если e — единичный элемент поля K, то норма $\|\ \|$ неархимедова в том и только в том случае, если $\|n \cdot e\| \leqslant 1$ для всех $n \in \mathbb{Z}$;

е) любая норма поля K ненулевой характеристики p необходимо неархимедова.

3*. Установить справедливость следующей теоремы Островского: *всякая нетривиальная норма поля рациональных чисел* $\mathbb{Q}$ *эквивалентна либо p-адической норме* $|x|_p = p^{-v_p(x)}$, *либо обычной абсолютной величине* $|x|$.

(Указание. Рассмотреть два случая: либо $\|a\| > 1$ для некоторого целого $a > 1$, либо $\|a\| \leqslant 1$ для всех целых $a \geqslant 1$.

В первом случае представить произвольное целое $x \geqslant 1$ в виде

$$x = x_0 + x_1 a + \ldots + x_{s-1} a^{s-1}, \quad 0 \leqslant x_i \leqslant a - 1,$$

и показать, что

$$\|x\| \leqslant c' x^\alpha,$$

где c' не зависит от x и $0 < \alpha \leqslant 1$. Затем, заменив x на x^n и устремив n к бесконечности, получить неравенство

$$\|x\| \leqslant x^\alpha.$$

Далее, положив $x = a^s - y$, где $0 < y \leqslant a^s - a^{s-1}$, получить с помощью аналогичных рассуждений неравенство

$$\|x\| \geqslant x^\alpha.$$

Вывести отсюда, что нормирование $\|\ \|$ поля $\mathbb{Q}$ эквивалентно в этом случае обычной абсолютной величине $|\ |$.

Во втором случае показать, что норма $\|\ \|$ неархимедова и что множество тех $x \in \mathbb{Z}$, для которых $\|x\| < 1$, не пусто и является простым идеалом кольца $\mathbb{Z}$, порожденным простым числом p. Вывести отсюда, что в таком случае норма $\|\ \|$ эквивалентна p-адической норме $|\ |_p$.)

4. Пусть $\|\ \|_m$, $1 \leqslant m \leqslant n$, — неэквивалентные между собой нетривиальные нормы поля K и $x_1, \ldots, x_n$ — заданные элементы этого поля. Доказать, что в поле K найдется такой элемент x, для которого при любом $\varepsilon > 0$ выполняется система неравенств

$$\|x - x_m\|_m < \varepsilon, \quad 1 \leqslant m \leqslant n.$$

(Указание. Положить

$$x = \sum_{m=1}^{n} \frac{\alpha_m^s}{1 + \alpha_m^s} x_m,$$

где s — достаточно большое целое число, и показать, что достаточно найти такие элементы $\alpha_1, \ldots, \alpha_n \in K$, что $\|\alpha_m\|_m > 1$ и $\|\alpha_m\|_l < 1$ при $l \neq m$. Для доказательства последнего утверждения воспользоваться индукцией по $n \geqslant 2$.)

5. Поле K называется *полным* относительно нормы $\|\ \|$, если оно полно как метрическое пространство по отношению к метрике $\|x - y\|$, т. е. если каждая фундаментальная последовательность x_n элементов этого поля ($\|x_m - x_n\| \to 0$ при $m, n \to \infty$) имеет в нем предел по норме $\|\ \|$.

Доказать справедливость следующих утверждений:

а) всякое поле K с нормой $\|\ \|$ может быть вложено в единственное с точностью до изоморфизма поле $\widetilde{K}$ с нормой $\|\ \|$, продолжающей исходную норму и обладающей тем свойством, что по отношению к ней $\widetilde{K}$ является замыканием поля K;

б) продолженная норма $\|\ \|$ неархимедова в поле $\widetilde{K}$ тогда и только тогда, когда она неархимедова в поле K;

в) любое сохраняющее норму вложение поля K в полное поле L может быть единственным образом продолжено до вложения $\widetilde{K}$ в L.

6*. Пусть K — поле с неархимедовой нормой $\|\ \|$. Множество элементов $u \in K$, для которых $\|u\| = 1$, называется *группой единиц* поля K (по отношению к рассматриваемой норме). Пусть $\mathfrak{m}$ — максимальный идеал кольца нормирования $\mathfrak{o}$ поля K (см. задачу 2) и $\mathfrak{p}$ — соответствующий этому идеалу неархимедов простой дивизор поля K. Назовем факторкольцо $\mathfrak{o}/\mathfrak{m}$ полем вычетов простого дивизора $\mathfrak{p}$ (в случае, когда K — конечное расширение поля рациональных чисел $\mathbb{Q}$, поле $\mathfrak{o}/\mathfrak{m}$ конечно и число его элементов называется *нормой* $N\mathfrak{p}$ неархимедова простого дивизора $\mathfrak{p}$). Если норма $\|\ \|$ дискретна, то $\mathfrak{m}$ — главный идеал, и если $\mathfrak{m} = (\pi)$, то всякий элемент $x \in K$ имеет вид $x = \pi^v u$, где $v = v(x)$ — порядковая функция элемента x и u — единица кольца $\mathfrak{o}$.

Пусть K' — конечное расширение степени n поля K, $\mathfrak{o}'$ и $\mathfrak{m}'$ — кольцо нормирования и максимальный идеал этого кольца, соответствующие норме поля K', которая является продолжением нормы $\|\ \|$ поля K на K'. Предположим, что норма $\|\ \|$ дискретна. Тогда продолженная норма поля K' также дискретна и, следовательно, $\mathfrak{m}' = (\pi')$. Пусть $\Gamma = \mathbb{Z}$ и Γ' — группы значений нормирований полей K и K', соответствующие рассматриваемым нормам. Группа Γ' является подгруппой группы Γ. Индекс $e = (\Gamma : \Gamma')$ подгруппы Γ' в группе Γ назовем *индексом ветвления* поля K', а степень f поля $\mathfrak{o}'/\mathfrak{m}'$ над полем $\mathfrak{o}/\mathfrak{m}$ — *степенью поля вычетов*.

Предположим, что поле K полно относительно дискретной нормы $\|\ \|$ и что его поле вычетов $\mathfrak{o}/\mathfrak{m}$ конечно. В этих предположениях доказать справедливость следующих утверждений:

а) Кольцо нормирования $\mathfrak{o}$ поля K состоит из тех и только тех элементов $x \in K$, которые представляются в виде

$$x = \sum_{n=0}^{\infty} x_n \pi^n,$$

где x_n независимо друг от друга пробегают некоторое множество представителей факторкольца $\mathfrak{o}/\mathfrak{m}$ в кольце $\mathfrak{o}$.

б) Кольцо $\mathfrak{o}$ компактно в топологии, индуцированной нормой $\|\ \|$.

в) Поле K локально компактно.

г) Индекс ветвления e поля K' и степень поля вычетов f связаны соотношением $ef = n = [K' : K]$.

(Указание. Выбрать элементы $\omega_1, \ldots, \omega_f$ из K' таким образом, чтобы их классы вычетов составляли базис поля $\mathfrak{o}'/\mathfrak{m}'$ над $\mathfrak{o}/\mathfrak{m}$. Показать, что если $\alpha_1, \ldots, \alpha_f$ независимо друг от друга пробегают множество представителей $\mathfrak{o}/\mathfrak{m}$ в $\mathfrak{o}$, то элементы $\alpha_1\omega_1 + \ldots + \alpha_f\omega_f$ образуют систему представителей $\mathfrak{o}'/\mathfrak{m}'$ в $\mathfrak{o}'$. Учитывая соотношение $\pi = \pi'^e u'$, где u' — единица кольца $\mathfrak{o}'$, вывести отсюда, что каждый элемент $x \in \mathfrak{o}'$ допускает разложение

$$x = \sum_{i=0}^{e-1} \sum_{j=1}^{f} \sum_{n=0}^{\infty} x_{i,j,n} \pi'^i \omega_j \pi^n.$$

Показать, что ef элементов $\omega_j\pi'^i$ составляют множество образующих кольца $\mathfrak{o}'$ над $\mathfrak{o}$ и что они линейно независимы над K.)

7. Доказать, что если K — локально компактное поле в топологии, индуцированной неархимедовой нормой $\|\ \|$, то:

а) поле K полно;

б) его поле вычетов $\mathfrak{o}/\mathfrak{m}$ конечно;

в) нормирование $\|\ \|$ дискретно.

8. Пусть k — поле с нормой $|\ |$ и V — векторное пространство над полем k. Вещественнозначная функция $\|\ \|$ на V называется *нормой*, если:

1) $\|x\| > 0$ для всех ненулевых элементов $x \in V$;

2) $\|x + y\| \leqslant \|x\| + \|y\|$;

3) $\|ax\| = |a| \cdot \|x\|$ для всех $a \in k$ и $x \in V$.

Две нормы $\|\ \|$ и $\|\ \|_*$ на пространстве V называются *эквивалентными*, если существуют константы c и c^* такие, что

$$\|x\| \leqslant c\|x\|_* \leqslant c^*\|x\|$$

для всех $x \in V$.

Пусть k — полное относительно нормы $|\ |$ локально компактное поле и пусть пространство V — конечномерно. Доказать, что если $\omega_1, \ldots, \omega_n$ — базис пространства V над k, то каждая норма на V эквивалентна норме

$$\|x\| = \left\| \sum_{i=1}^{n} x_i\omega_i \right\| = \max_i |x_i|.$$

9. Пусть K — расширение поля k. Мы скажем, что норма $\|\ \|$ поля K является *продолжением нормы* $|\ |$ поля k, если $\|x\| = |x|$ для всех $x \in k$.

Пусть, далее, k — полное относительно нормы $|\ |$ локально компактное поле и K — расширение поля k конечной степени $[K : k] = n$. При этих предположениях установить справедливость следующих утверждений:

а) Существует единственное продолжение нормы $|\ |$ поля k на поле K, а именно

$$\|x\| = |\mathrm{norm}_{K/k} x|^{1/n}.$$

(Указание. Рассмотреть поле K как векторное n-мерное пространство над полем k. Для доказательства единственности нормы $\|\ \|$ поля K воспользоваться результатом предыдущей задачи, а также тем, что две нормы поля K, индуцирующие одинаковую топологию, необходимо эквивалентны. Для доказательства существования нормы поля K проверить, что функция

$$\|x\| = |\mathrm{norm}_{K/k} x|^{1/n}$$

удовлетворяет всем аксиомам 1)—3) нормы (см. задачу 1). Для проверки условия 3) воспользоваться тем, что функция $\|x\|$ непрерывна на компакте $\{x \mid |x| = 1\}$ и отлична на нем от нуля.)

б) Если $\omega_1, \ldots, \omega_n$ — базис поля K над полем k, то для любых $x_1, \ldots, x_n \in k$, отличных в совокупности от нуля, найдутся положительные константы c_1 и c_2 такие, что

$$c_1 \leqslant \frac{\left\| \sum_{i=1}^{n} x_i\omega_i \right\|}{\max_i \|x_i\|} \leqslant c_2.$$

в) Поле K, полное относительно нормы $\|\ \|$, локально компактно.

10. Пусть A и B — два коммутативных кольца, содержащих поле k, причем B имеет конечную размерность n над k. Пусть $\omega_1, \ldots, \omega_n$ — базис кольца B над k и $\omega_1 = 1$. Тогда кольцо B с точностью до изоморфизма определяется таблицей умножения

$$\omega_i\omega_j = \sum_{s=1}^{n} a_{ijs}\omega_s, \quad a_{ijs} \in k.$$

Определим новое кольцо C, содержащее поле k, элементами которого являются выражения вида

$$\sum_{i=1}^{n} \alpha_i \omega_i^*, \quad \alpha_i \in A,$$

где ω_i^* имеют тот же закон умножения

$$\omega_i^* \omega_j^* = \sum_{s=1}^{n} a_{ijs} \omega_s^*,$$

что и ω_i. Сопоставления

$$\alpha \mapsto \alpha \omega_1^*, \quad \sum_{i=1}^{n} \beta_i \omega_i \mapsto \sum_{i=1}^{n} \beta_i \omega_i^*$$

задают изоморфные вложения колец A и B в кольцо C.

Кольцо C определяется кольцами A, B с точностью до изоморфизма и не зависит от конкретного выбора базиса $\omega_1, \ldots, \omega_n$. Оно называется *тензорным произведением*

$$C = A \otimes_k B$$

колец A и B над полем k.

Предположим теперь, что A и B — поля, содержащие k, и что B — конечное сепарабельное расширение поля k степени $[B : k] = n$. В этих предположениях доказать справедливость следующих утверждений:

а) Кольцо $C = A \otimes_k B$ является прямой суммой

$$C = \bigoplus_{1 \leqslant i \leqslant m} K_i$$

конечного числа полей K_i, каждое из которых содержит в себе изоморфный образ полей A и B.

(Указание. Показать, что если β — порождающий элемент поля B над k и $f \in k[x]$ — минимальный многочлен степени n элемента β, то $A \otimes_k B = A[\beta^*]$, где $1, \beta^*, \ldots, \beta^{*n-1}$ линейно независимы над A и $f(\beta^*) = 0$. Далее, показать, что если

$$f(x) = \prod_{i=1}^{m} f_i(x)$$

— разложение многочлена f на неприводимые в кольце $A[x]$ множители, то многочлены f_i различны и, если $K_i = A(\beta_i)$, где $f_i(\beta_i) = 0$, то отображения

$$A \otimes_k B \xrightarrow{\varphi_i} K_i,$$

задаваемые формулами

$$g(\beta^*) \xrightarrow{\varphi_i} g(\beta_i), \quad g \in A[x],$$

являются гомоморфизмами колец. Вывести отсюда, что кольцевой гомоморфизм

$$A \otimes_k B \xrightarrow{\varphi_1 \oplus \ldots \oplus \varphi_m} \bigoplus_{1 \leqslant i \leqslant m} K_i$$

является изоморфизмом и что гомоморфизм колец

$$B \to A \otimes_k B \xrightarrow{\varphi_i} K_i$$

представляет собой вложение.)

б) Если $F \in k[x]$ — характеристический многочлен элемента $\beta \in B$ и $G_i \in A[x]$, $1 \leqslant i \leqslant m$,— характеристические многочлены образов элемента β при отображениях

$$B \to A \otimes_k B \xrightarrow{\varphi_i} K_i,$$

то

$$F(x) = \prod_{i=1}^{m} G_i(x).$$

в) Для каждого элемента $\beta \in B$ имеют место равенства

$$\operatorname{norm}_{B/k} \beta = \prod_{i=1}^{m} \operatorname{norm}_{K_i/A} \beta,$$

$$\operatorname{tr}_{B/k} \beta = \sum_{i=1}^{m} \operatorname{tr}_{K_i/A} \beta.$$

11*. Пусть K — сепарабельное расширение поля k конечной степени $[K : k] = n$. Доказать, что существует не более n различных продолжений нормы $|\ |$ поля k на K. Показать далее, что если $\|\ \|_i$, $1 \leqslant i \leqslant m$ — все различные продолжения нормы $|\ |$ на K и $\widetilde{k}$, $\widetilde{K}_i$ — пополнения полей k и K по нормам $|\ |$ и $\|\ \|_i$ соответственно, то имеет место равенство

$$\widetilde{k} \otimes_k K = \bigoplus_{1 \leqslant i \leqslant m} \widetilde{K}_i.$$

(Указание. Воспользоваться результатами задач 5, 9 и 10.)

12*. Пусть K — конечное расширение поля рациональных чисел $\mathbb{Q}$ и L — конечное расширение поля K. Обозначим $\widetilde{L}$ пополнение поля L по норме $\|\ \|$ этого поля, $\widetilde{K}$ — замыкание поля K в поле $\widetilde{L}$ и $L\widetilde{K}$ — *композит полей* L и $\widetilde{K}$ (наименьшее подполе поля $\widetilde{L}$, содержащее L и K).

Доказать, что поле $L\widetilde{K}$ полно относительно индуцированной нормы. Вывести отсюда, что $L\widetilde{K} = \widetilde{L}$.

(Указание. Композит $L\widetilde{K}$ является конечным расширением поля $\widetilde{K}$. Пусть $\omega_1, \ldots, \omega_m$ — базис поля $L\widetilde{K}$ над $\widetilde{K}$. Показать, что для любой фундаментальной последовательности

$$x_n = x_{1n}\omega_1 + \ldots + x_{mn}\omega_m, \quad x_{sn} \in \widetilde{K},$$

последовательности коэффициентов x_{sn} сходятся в поле $\widetilde{K}$.)

13*. Пусть K — конечное расширение поля рациональных чисел $\mathbb{Q}$, $\mathfrak{p}$ — неархимедов простой дивизор поля K и $\mathfrak{m} = (\pi)$ — соответствующий ему максимальный идеал кольца нормирования $\mathfrak{o}$ поля K. Пусть далее p — простое число, порождающее идеал $\mathfrak{m} \cap \mathbb{Z}$. Тогда $p = \pi^{e_\mathfrak{p}} u$ для некоторого целого $e_\mathfrak{p} \geqslant 1$ и некоторой единицы u из кольца $\mathfrak{o}$. Простой дивизор $\mathfrak{p}$ однозначно определяет две нормы $|\ |_\mathfrak{p}$ и $\|\ \|_\mathfrak{p}$, а именно, такие нормы, для которых

$$|\pi|_\mathfrak{p} = 1/p^{1/e_\mathfrak{p}}, \quad |p|_\mathfrak{p} = 1/p$$

и

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

Если $f_{\mathfrak{p}}$ — степень поля $\mathfrak{o}/\mathfrak{m}$ над полем $\mathbb{Z}/p\mathbb{Z}$, то

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

для любого ненулевого элемента $x \in K$. Множество норм поля K, состоящее из всех $\mathfrak{p}$-адических норм $|\ |_{\mathfrak{p}}$, а также из вещественных и обычных комплексных норм $|\ |$, назовем *канонической системой норм* поля K. Систему всех $\mathfrak{p}$-адических норм $\|\ \|_{\mathfrak{p}}$, а также всех вещественных и комплексных норм вида $\|\ \| = |\ |^2$ назовем *квазиканонической системой норм* поля K. Пусть $K_{\mathfrak{p}}$ — пополнение поля K по архимедовой или неархимедовой норме $|\ |_{\mathfrak{p}}$ канонической системы, $\overline{K}_{\mathfrak{p}}$ — алгебраическое замыкание поля $K_{\mathfrak{p}}$ и L — конечное расширение поля K. Доказать, что два вложения

$$\sigma, \tau\colon L \to K_{\mathfrak{p}}$$

поля L над K индуцируют одну и ту же норму поля L в том и только в том случае, когда они сопряжены над полем $K_{\mathfrak{p}}$ (сопряженность над $K_{\mathfrak{p}}$ означает, что существует изоморфизм поля $\sigma LK_{\mathfrak{p}}$ на поле $\tau LK_{\mathfrak{p}}$, тождественный на $K_{\mathfrak{p}}$).

(Указание. Если вложения σ и τ сопряжены, то ввиду однозначности продолжения нормы с $K_{\mathfrak{p}}$ на $\overline{K}_{\mathfrak{p}}$, они индуцируют на L одинаковые нормы.

Для доказательства обратного утверждения установить, что если $\theta : \tau L \to \sigma L$ — некоторый K-изоморфизм, то его можно продолжить до $K_{\mathfrak{p}}$-изоморфизма полей $\tau LK_{\mathfrak{p}}$ и $\sigma LK_{\mathfrak{p}}$.)

14*. Пусть K — конечное расширение степени n поля рациональных чисел $\mathbb{Q}$ и $|\ |_p$ — некоторая каноническая норма поля $\mathbb{Q}$. Если $|\ |_{\mathfrak{p}}$ — продолжение $|\ |_p$ на поле K, то будем говорить, что простой дивизор $\mathfrak{p}$ лежит над простым дивизором p и писать $\mathfrak{p}|p$ (мы используем одно и то же обозначение p для неархимедова простого дивизора поля $\mathbb{Q}$ и для порождающего его максимального идеала).

Пусть $\mathfrak{m}$ — максимальный идеал кольца нормирования $\mathfrak{o}$ поля K, соответствующий неархимедову простому дивизору $\mathfrak{p}$. Если $\mathfrak{m} = (\pi)$, $\mathfrak{m} \cap \mathbb{Z} = (p)$ и $p = \pi^{e_{\mathfrak{p}}} u$, где u — некоторая единица кольца $\mathfrak{o}$, то целое число $e_{\mathfrak{p}} \geqslant 1$ называется *индексом ветвления* простого дивизора $\mathfrak{p}$ в p. Если $\mathfrak{p}$ — архимедов или неархимедов простой дивизор поля K, лежащий над p, и $K_{\mathfrak{p}}, \mathbb{Q}_p$ — пополнения полей K, $\mathbb{Q}$ по каноническим нормам $|\ |_{\mathfrak{p}}$, $|\ |_p$ соответственно, то число $n_{\mathfrak{p}} = [K_{\mathfrak{p}}\colon \mathbb{Q}_p]$ называется *локальной степенью*.

Доказать справедливость следующих утверждений:

а) Если поле K имеет r вещественных и $2s$ комплексных вложения в поле комплексных чисел $\mathbb{C}$, так что $n = r + 2s$, то каноническая система содержит r вещественных и s комплексных архимедовых норм. Локальная степень для случая вещественных и комплексных норм равна 1 и 2 соответственно.

б) Если $v_{\mathfrak{p}}(K^*)$ и $v_p(\mathbb{Q}^*)$ — группы значений дискретных нормирований $v_{\mathfrak{p}}$ и v_p, соответствующих каноническим нормам $|\ |_{\mathfrak{p}}$ и $|\ |_p$, индекс ветвления $e_{\mathfrak{p}}$ простого дивизора $\mathfrak{p}$ совпадает с индексом ветвления поля K (см. задачу 6).

в) Если $f_{\mathfrak{p}}$ — степень поля вычетов неархимедова простого дивизора $\mathfrak{p}$ поля K, то

$$e_{\mathfrak{p}}f_{\mathfrak{p}} = n_{\mathfrak{p}}.$$

(Указание. Воспользоваться результатами предыдущего пункта и п. г) задачи 6.)

г) Для каждого простого дивизора p поля $\mathbb{Q}$ имеет место соотношение

$$n = \sum_{\mathfrak{p}|p} n_{\mathfrak{p}}.$$

(Указание. Выбрать элемент $\alpha \in K$ таким образом, что $K = \mathbb{Q}(\alpha)$. Показать, что если

$$f = f_1 \dots f_r$$

— разложение на неприводимые в кольце $\mathbb{Q}_p[x]$ множители минимального многочлена $f \in \mathbb{Z}[x]$ элемента α, то все f_i различны. Вывести отсюда, что вложения поля K в алгебраическое замыкание $\overline{\mathbb{Q}}_p$ поля $\mathbb{Q}_p$ находятся во взаимно однозначном соответствии с корнями многочленов f_i и что вложения сопряжены тогда и только тогда, когда элемент α отображается ими в корни одного и того же многочлена f_i. Затем воспользоваться результатом предыдущей задачи и показать, что локальные степени совпадают со степенями многочленов f_i.)

д) Для каждого простого дивизора p поля $\mathbb{Q}$ и для всякого элемента x поля K выполняются соотношения

$$\operatorname{norm}_{K/\mathbb{Q}} x = \prod_{\mathfrak{p}|p} \operatorname{norm}_{K_{\mathfrak{p}}/\mathbb{Q}_p} x,$$

$$\operatorname{tr}_{K/\mathbb{Q}} x = \sum_{\mathfrak{p}|p} \operatorname{tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p} x.$$

е) Для каждой канонической нормы $|\ |_p$ поля $\mathbb{Q}$ и для всякого элемента $x \in K$ имеет место соотношение

$$\prod_{\mathfrak{p}|p} |x|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = |\operatorname{norm}_{K/\mathbb{Q}} x|_p.$$

(Указание. Воспользоваться результатами предыдущего пункта и п. а) задачи 9.)

ж) Для всякого ненулевого элемента $x \in K$ найдется не более конечного числа канонических норм $|\ |_{\mathfrak{p}}$ поля K, для которых

$$|x|_{\mathfrak{p}} > 1.$$

з) Если x — произвольный ненулевой элемент поля K и $\|\ \|_{\mathfrak{p}}$ пробегает все квазиканонические нормы поля K, то $\|x\mathfrak{p}\|_1 =$ для почти всех $\mathfrak{p}$ и

$$\prod_{\mathfrak{p}} \|x\|_{\mathfrak{p}} = 1.$$

(Указание. Воспользоваться результатами п. д), е), а также результатом задачи 5 из § 2, гл. IV.)

ГЛАВА VII

ТЕОРЕМА ЗИГЕЛЯ — МАЛЕРА

Пусть K — конечное расширение поля рациональных чисел $\mathbb{Q}$ и X — плоская аффинная алгебраическая кривая рода g, определенная над K уравнением

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

Теорема Зигеля — Малера утверждает, что *если* $g \geqslant 1$, *то на кривой* X *имеется лишь конечное число точек* (x', y') *с квазицелыми координатами* $x', y' \in K$.

В данной главе дается нестандартное доказательство этой теоремы, основанное на использовании арифметики фиксированного нестандартного расширения $^*K$ поля K.

§ 1. Нестандартный эквивалент теоремы Зигеля — Малера

1. Функциональные дивизоры. Арифметическая структура поля K может быть описана при помощи простых дивизоров $\mathfrak{p}$ этого поля, определяемых как классы эквивалентных между собой нетривиальных нормирований поля K.

Пусть $^*K$ — фиксированное нестандартное расширение поля K. Поле K алгебраически замкнуто в $^*K$. Элементы поля K называются *стандартными*, а элементы поля $^*K$, не принадлежащие K, называются *нестандартными* элементами поля $^*K$. Точка $(x', y') \in {}^*K \times {}^*K$ называется *нестандартной*, если хотя бы одна из ее координат нестандартна.

Предположим, что вопреки утверждению теоремы Зигеля — Малера на кривой X имеется бесконечно много K-рациональных точек с квазицелыми координатами по отношению к некоторому конечному множеству простых дивизоров $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ поля K. Тогда, в соответствии с принципом нестандартного расширения для отношений, на кривой X существует нестандартная точка (x', y') с координатами x', y', являющимися квазицелыми элементами поля $^*K$ по отношению к тому же самому множеству простых дивизоров S. По построению множество S состоит только из стандартных простых дивизоров $\mathfrak{p}$ и, стало быть, знаменатели элементов x' и y' не делятся ни на какой нестандартный дивизор поля $^*K$.

Как было отмечено выше, поле K алгебраически замкнуто в $^*K$. В таком случае, поскольку точка (x', y') нестандартна, то по крайней мере одна из ее координат трансцендентна над K.

Отсюда следует, что (x', y') — *общая точка* кривой X над полем K. Это означает, что поле функций $K(X)$ на этой кривой K-изоморфно полю $F = K(x', y')$, и при отождествлении $K(X)$ с F получаем включение $F \subset {}^*K$ (см. замечание в конце п. 2 данного параграфа), которое можно интерпретировать как *представление рациональных функций из* F *нестандартными алгебраическими числами*. В силу указанного изоморфизма род поля F равен роду g кривой X.

Поле F порождается над его полем констант K двумя рациональными функциями x' и y', которые при их интерпретации в виде алгебраических чисел поля $^*K$ содержат в своих знаменателях лишь стандартные дивизоры этого поля. Тогда справедливость теоремы Зигеля — Малера вытекает из следующего утверждения.

Теорема А. *Пусть* F *— поле алгебраических функций от одного переменного над полем* K *и пусть* F *вложено в* $^*K$, *так что*

$$K \subset F \subset {}^*K.$$

Если F *поле рода* $g \geqslant 1$, *то знаменатель каждой непостоянной функции* $x \in F$ *делится по меньшей мере на один нестандартный простой дивизор поля* $^*K$.

Легко показать, что справедливо и обратное, а именно, что теорема А следует из теоремы Зигеля — Малера. Таким образом, теорема А может рассматриваться как нестандартный эквивалент теоремы Зигеля — Малера.

Теорема А допускает иную формулировку, в которой вместо непостоянных функций участвуют простые дивизоры поля F (классы эквивалентных между собой нормирований поля F над K). Такие дивизоры, в отличие от *арифметических простых дивизиров* поля $^*K$, будем называть *функциональными простыми дивизорами* (в случае алгебраически замкнутого поля K функциональные простые дивизоры поля F находятся во взаимно однозначном соответствии с точками кривой X).

Каждый нестандартный арифметический простой дивизор $\mathfrak{p}$ поля $^*K$ тривиален на K и, следовательно, индуцирует на поле F нормирование, которое, в случае его нетривиальности, определяет некоторый функциональный простой дивизор P поля F. Будем говорить, что дивизор P индуцирован простым дивизором $\mathfrak{p}$ и писать при этом $\mathfrak{p} \mid P$.

Если каждый функциональный простой дивизор P индуцирован некоторым нестандартным арифметическим простым дивизором $\mathfrak{p}$ поля $^*K$, тогда справедливо утверждение теоремы А. Действительно, каждая непостоянная функция $x \in F$ имеет по меньшей мере один полюс, скажем P, представляющий собой функциональный простой дивизор. Если этот дивизор индуцирован нестандартным арифметическим простым дивизором $\mathfrak{p}$ поля $^*K$, то $\mathfrak{p}$ делит знаменатель рациональной функции x.

Обратно, из теоремы A следует, что каждый функциональный простой дивизор P поля F индуцирован некоторым нестандартным арифметическим простым дивизором $\mathfrak{p}$ поля $^*K$. Действительно, в соответствии с теоремой Римана — Роха существует функция $x \in F$, имеющая P в качестве единственного своего полюса. Из теоремы A следует, что имеется нестандартный простой дивизор $\mathfrak{p}$ поля $^*K$, делящий знаменатель рациональной функции x и, следовательно, индуцирующий полюс P функции x. Так как это единственный полюс рассматриваемой функции, то $\mathfrak{p} \mid P$.

Из сказанного получаем, что теорема A эквивалентна следующему утверждению.

Теорема B. *В условиях и обозначениях теоремы* A *каждый функциональный простой дивизор P поля F индуцируется некоторым нестандартным арифметическим простым дивизором $\mathfrak{p}$ поля $^*K$.*

Для полей рода $g = 0$ утверждения теорем A и B перестают быть справедливыми, например, пусть $F = K(x)$, где x — некоторый нестандартный целый элемент в $^*K$. Тогда $g = 0$ и знаменатель элемента x не делится ни на один неархимедов простой дивизор. Значит, теорема A не справедлива для функции $x \in F$, а теорема B не справедлива для полюса функции x. Однако нестандартный подход позволяет получить некоторую информацию и в случае $g = 0$. Оказывается, что в этом случае существует не более двух исключительных в смысле теоремы B функциональных простых дивизоров, т. е. простых дивизоров поля F, которые не индуцируются никакими нестандартными арифметическими простыми дивизорами поля $^*K$ (см. задачу 11). Это приводит к параметризации тех функций $u \in F$, знаменатели которых не содержат нестандартные арифметически простые дивизоры (см. задачу 12). Указанный результат можно рассматривать как нестандартную версию зигелевской параметризации кривых рода 0, обладающих бесконечным числом целых точек [54d]).

Среди всех нормирований поля F (обязательно неархимедовых), определяющих функциональный простой дивизор P, имеется ровно одно каноническое нормирование, для которого группа значений совпадает с $\mathbb{Z}$. Назовем это нормирование *P-адической порядковой функцией поля F* и обозначим ее v_P. Поле вычетов дивизора P является расширением конечной степени $n = \deg P$ поля K (см. задачу 2). Если

$$w_P(x) = v_P(x) \deg P,$$

то имеет место соотношение

$$\sum_P w_P(x) = 0, \tag{1}$$

выражающее тот факт, что каждый ненулевой элемент $x \in F$

имеет одинаковое число нулей и полюсов (в этом соотношении P пробегает все функциональные простые дивизоры поля F, включая простой дивизор, соответствующий бесконечно удаленной точке кривой X).

Определение 1. Свободный $\mathbb{Z}$-модуль, порожденный функциональными простыми дивизорами P поля F, называется *группой функциональных дивизоров* поля F.

Обозначим эту группу $\mathrm{Div}(F)$ и заметим, что каждый функциональный дивизор $A \in \mathrm{Div}(F)$ однозначно представляется в виде

$$A = \sum_P \alpha_P \cdot P,$$

где α_P — целые числа, равные нулю для почти всех P. Положим

$$v_P(A) = \alpha_P$$

и

$$w_P(A) = v_P(A) \deg P.$$

Число

$$\deg A = \sum_P w_P(A)$$

назовем *степенью функционального дивизора* A.

Определение 2. Ядро степенного гомоморфизма $\deg\colon \mathrm{Div}(F) \to \mathbb{Z}$ называется *группой функциональных дивизоров степени ноль*.

Обозначим эту группу $\mathrm{Div}^0(F)$. Каждый ненулевой элемент $x \in F$ определяет *главный дивизор*

$$[x] = \sum_P v_P(x) \cdot P$$

(мы используем квадратные скобки, чтобы отличить функциональные главные дивизоры от арифметических главных дивизоров $(x) \in {}^*\mathfrak{D}$). Сопоставление $x \mapsto [x]$ задает отображение $F \to \mathrm{Div}(F)$, ядром которого является мультипликативная группа поля констант K. Другими словами, последовательность

$$1 \to K \to F \to \mathrm{Div}(F)$$

точна. Ввиду соотношения (1) образ $\mathfrak{P}(F)$ мультипликативной группы поля F при отображении $F \to \mathrm{Div}(F)$ содержится в группе $\mathrm{Div}^0(F)$.

Определение 3. Факторгруппы $\mathrm{Cl}(F) = \mathrm{Div}(F)/\mathfrak{P}(F)$ и $\mathrm{Cl}^0(F) = \mathrm{Div}^0(F)/\mathfrak{P}(F)$ называются соответственно *группой классов функциональных дивизоров* и *группой классов функциональных дивизоров нулевой степени*.

Установим связь между функциональными и арифметическими простыми дивизорами. Пусть $\mathfrak{p} \in {}^*V$ — арифметический простой дивизор и $w_{\mathfrak{p}}(x) = -\log \|x\|_{\mathfrak{p}}$ — логарифмическое значе-

ние нормы $\|x\|_{\mathfrak{p}}$. В общем случае функция $w_{\mathfrak{p}}(x)$ либо вовсе не является нормированием поля $^*K$ (в случае, когда $\mathfrak{p}$ — архимедов простой дивизор), либо она не тривиальна на K (в случае, когда $\mathfrak{p}$ — стандартный простой дивизор). Однако модифицированная функция $\overset{\circ}{w}_{\mathfrak{p}}$, задающая порядок значимости величины $w_{\mathfrak{p}}(x)$, представляет собой нормирование поля $^*K$, тривиальное на K. Следовательно, ограничение функции $\overset{\circ}{w}_{\mathfrak{p}}$ на подполе F поля $^*K$ задает, в случае его нетривиальности на F, нормирование поля F над K, определяющее некоторый функциональный простой дивизор P. В этом случае назовем арифметический простой дивизор $\mathfrak{p}$ *эффективным на* F и скажем, что дивизор P *индуцирован* дивизором $\mathfrak{p}$. Если функциональный простой дивизор P индуцирован арифметическим простым дивизором $\mathfrak{p}$ поля $^*K$, то будем писать $\mathfrak{p}|P$. Построенное нами нормирование w_P поля F эквивалентно функции $w_{\mathfrak{p}}$ на F в том смысле, что существует гипердействительное число $n_{\mathfrak{p}} \overset{\circ}{>} 0$, для которого

$$w_{\mathfrak{p}}(x) \overset{\circ}{=} n_{\mathfrak{p}} w_P(x) \tag{2}$$

при всех $0 \neq x \in F$. Порядок значимости числа $n_{\mathfrak{p}}$ определяется этим соотношением единственным образом.

Пусть $\pi \in F$ — униформизирующий параметр простого дивизора P, т. е. $v_P(\pi) = 1$. Если положим $e_{\mathfrak{p}} = v_{\mathfrak{p}}(\pi)$ и $f_{\mathfrak{p}} = \log(N_{\mathfrak{p}})/\deg P$, то из соотношения (2) получим

$$n_{\mathfrak{p}} \overset{\circ}{=} e_{\mathfrak{p}} f_{\mathfrak{p}}.$$

Число $e_{\mathfrak{p}}$ можно рассматривать как $\mathfrak{p}$-адический индекс ветвления, а число $f_{\mathfrak{p}}$ как $\mathfrak{p}$-адическую степень поля вычетов расширения $^*K$ поля F. В свою очередь, инвариант $n_{\mathfrak{p}}$ можно рассматривать как локальную степень поля $^*K$ над F.

Лемма 1. *Каждый функциональный простой дивизор P поля F индуцируется некоторым арифметическим простым дивизором $\mathfrak{p}$ поля $^*K$.*

Доказательство. По теореме Римана — Роха существует элемент $x \in F$, имеющий P своим единственным полюсом, т. е. $w_P(x) < 0$ для единственного функционального простого дивизора P поля F. Так как $x \notin K$, то из леммы 2 из § 3 гл. VI следует, что существует арифметический простой дивизор $\mathfrak{p}$, такой, что $w_{\mathfrak{p}}(x) \overset{\circ}{<} 0$. Последнее неравенство означает, во-первых, что $\mathfrak{p}$ эффективен на F и, во-вторых, что $\mathfrak{p}$ индуцирует в поле F функциональный простой дивизор, который является полюсом элемента x. Поскольку элемент x имеет единственный полюс P, отсюда следует, что $\mathfrak{p}|P$. Лемма доказана.

Покажем теперь, что существует вложение $i: \mathrm{Div}(F) \to \overset{\circ}{\mathfrak{D}}$ группы функциональных дивизоров $\mathrm{Div}(F)$ в группу дивизорных порядков значимости $\overset{\circ}{\mathfrak{D}}$. Для существования такого вложения необходимо, чтобы образ iA каждого функционального дивизора A имел следующие $\mathfrak{p}$-адические значения:

$$w_{\mathfrak{p}}(iA) = \begin{cases} n_{\mathfrak{p}} w_P(A), & \text{если } \mathfrak{p} \mid P, \\ 0, & \text{если } \mathfrak{p} \text{ не эффективен на } F. \end{cases} \tag{3}$$

Далее, если дивизор $iA \in {}^*\mathfrak{D}$ с указанными свойствами существует, то в соответствии с леммой 3 из § 3 гл. VI он определяется однозначно.

Лемма 2. *Для каждого функционального дивизора $A \in \mathrm{Div}(F)$ существует арифметический дивизор $iA \in {}^*\mathfrak{D}$, удовлетворяющий условиям* (3). *Этот дивизор однозначно определен в своем порядке значимости и составное отображение*

$$i: \mathrm{Div}(F) \to {}^*\mathfrak{D} \to \overset{\circ}{\mathfrak{D}}$$

является инъективным гомоморфизмом, обладающим следующими свойствами:

1) $A \leqslant B \Leftrightarrow iA \overset{\circ}{\leqslant} iB$;
2) $i(A, B) \overset{\circ}{=} (iA, iB)$;
3) $i\{A, B\} \overset{\circ}{=} \{iA, iB\}$;
4) $i[x] \overset{\circ}{=} (x)$.

Доказательство. Установим сначала существование дивизора $iA \in {}^*\mathfrak{D}$, удовлетворяющего условиям (3). Если $A = [x]$ — главный дивизор некоторого элемента $x \in F$, то можем положить $iA = (x)$. В этом случае справедливость (3) гарантирована соотношениями (2). В общем случае попытаемся выразить A через главные дивизоры, и затем воспользуемся полученным только что результатом.

Покажем сначала, что можно ограничиться рассмотрением случая, когда $A \geqslant 0$. В самом деле, если A не положителен, то представим A в виде $A = B - C$, где $B = \{0, A\} \geqslant 0$ и $C = (0, -A) \geqslant 0$. Тогда, если установлено существование iB и iC, то мы можем положить $iA = iB - iC$ (заметим, что условия (3) носят аддитивный характер).

Итак, пусть $A \geqslant 0$, т. е. $w_P(A) \geqslant 0$ для всех функциональных простых дивизоров P. Среди них имеется лишь конечное число таких, что $w_P(A) > 0$. Используя теорему об аппроксимации (теорема 3 из § 2 гл. IV), можно найти такой элемент $x \in F$, что

$$w_P(x) = w_P(A)$$

для всех P с условием $w_P(A) > 0$.

Далее, имеется лишь конечное число простых дивизоров P с условием $w_P(x) > 0$ и, следовательно, можно найти такой

ненулевой элемент $y \in F$, для которого

$$w_P(y) = \begin{cases} w_P(A), & \text{если } w_P(A) > 0, \\ 0, & \text{если } w_P(A) = 0 \text{ и } w_P(x) > 0. \end{cases}$$

В таком случае

$$\min(w_P(x), w_P(y)) = \begin{cases} w_P(A), & \text{если } w_P(A) > 0, \\ 0, & \text{если } w_P(A) = 0 \text{ и } w_P(x) > 0 \end{cases}$$

и

$$\min(w_P(x),\ w_P(y)) \leqslant 0, \text{ если } w_P(x) \leqslant 0.$$

Отсюда следует, что

$$\max(0,\ \min(w_P(x),\ w_P(y))) = w_P(A)$$

для каждого функционального простого дивизора P и, значит,

$$A = \{0,\ ([x],\ [y])\}.$$

Таким образом, нам удалось выразить дивизор A через главные дивизоры $[x]$ и $[y]$.

Положим теперь

$$iA = \{0,\ ((x),\ (y))\}$$

и заметим, что для каждого арифметического простого дивизора $\mathfrak{p}$

$$w_{\mathfrak{p}}(iA) = \max\big(0, \min\big(w_{\mathfrak{p}}(x), w_{\mathfrak{p}}(y)\big)\big).$$

Если $\mathfrak{p}$ — эффективен на F, то, используя соотношение (2), получаем

$$w_{\mathfrak{p}}(iA) \mathrel{\mathring{=}} n_{\mathfrak{p}} \max(0, \min(w_P(x), w_P(y))) = n_{\mathfrak{p}} w_P(A).$$

Если же $\mathfrak{p}$ не эффективен на F, то имеем $w_{\mathfrak{p}}(x) \mathrel{\mathring{=}} 0 \mathrel{\mathring{=}} w_{\mathfrak{p}}(y)$, и тогда $w_{\mathfrak{p}}(iA) \mathrel{\mathring{=}} 0$. Тем самым мы установим существование дивизора $iA \in {}^*\mathfrak{D}$, удовлетворяющего условиям (3).

В лемме 3 из § 3 гл. VI было показано, что каждый дивизор в $\mathring{\mathfrak{D}}$ однозначно определяется его $\mathfrak{p}$-адическими значениями в $\mathring{\mathbb{R}}$. Следовательно, дивизор iA однозначно определен в $\mathring{\mathfrak{D}}$ условиями (3) независимо от выбора элементов $x, y \in F$, участвовавших в построении этого дивизора. Таким образом, мы получили отображение i: $\mathrm{Div}(F) \to \mathring{\mathfrak{D}}$, которое, как легко видеть, является гомоморфизмом групп, сохраняющим отношение частичного порядка, а также операции взятия наибольшего общего делителя и наименьшего общего кратного. Остается показать, что

$$iA \mathrel{\mathring{\leqslant}} iB \Rightarrow A \leqslant B$$

и установить, тем самым, инъективность отображения i.

Пусть P — функциональный простой дивизор. Из леммы 1 следует, что существует арифметический простой дивизор $\mathfrak{p} | P$. Так как $iA \mathrel{\mathring{\leqslant}} iB$, имеем $w_{\mathfrak{p}}(iA) \mathrel{\mathring{\leqslant}} w_{\mathfrak{p}}(iB)$. Ввиду (3) это означает, что

$$n_{\mathfrak{p}} w_P(A) \mathrel{\mathring{\leqslant}} n_{\mathfrak{p}} w_P(B)$$

или, что

$$n_{\mathfrak{p}} w_P(A) \leqslant n_{\mathfrak{p}} w_P(B) + \gamma,$$

где γ — некоторое конечное гипердействительное число. Стало быть,

$$w_P(A) \leqslant w_P(B) + \delta,$$

где $\delta = \gamma / n_{\mathfrak{p}}$.

Поскольку $n_{\mathfrak{p}} \mathrel{\mathring{>}} 0$, то $n_{\mathfrak{p}}$ — бесконечно большое число и, значит, δ — бесконечно малое число. В частности, $\delta < 1$ и, следовательно,

$$w_P(A) < w_P(B) + 1.$$

Так как $w_P(A)$ и $w_P(B)$ — стандартные целые числа, то

$$w_P(A) \leqslant w_P(B),$$

а так как P — произвольный функциональный простой дивизор, то $A \leqslant B$. Лемма доказана.

Ввиду полученного нами вложения i: $\mathrm{Div}(F) \to \mathring{\mathfrak{D}}$ можно отождествить группу $\mathrm{Div}(F)$ с ее образом в $\mathring{\mathfrak{D}}$. В соответствии с этим вложением будем рассматривать функциональные дивизоры $A \in \mathrm{Div}(F)$ как арифметические внутренние дивизоры с той лишь оговоркой, что для них вместо знака $=$ используется знак $\mathring{=}$. При этом формула (3) и свойство 4) из леммы 2 перепишутся в виде

$$w_{\mathfrak{p}}(A) \mathrel{\mathring{=}} \begin{cases} n_{\mathfrak{p}} w_P(A), & \text{если } \mathfrak{p} | P, \\ 0, & \text{если } \mathfrak{p} \text{ не эффективен на } F, \end{cases} \tag{4}$$

$$[x] \mathrel{\mathring{=}} (x) \tag{5}$$

соответственно.

Каждый функциональный дивизор $A \in \mathrm{Div}(F)$, рассматриваемый как элемент группы $\mathring{\mathfrak{D}}$, имеет однозначно определенный размер $\sigma(A) \in \mathring{\mathbb{R}}$. Поэтому получаем отображение

$$\sigma\colon\ \mathrm{Div}(F) \to \mathring{\mathbb{R}}.$$

С другой стороны, имеем отображение $\deg\colon \mathrm{Div}(F) \to \mathbb{Z}$, ставящее в соответствие дивизору $A \in \mathrm{Div}(F)$ его степень

$$\deg A = \sum_P w_P(A) = \sum_P v_P(A) \deg P.$$

Возникает естественный вопрос о том, каким образом связаны между собой инварианты σ и deg на группе $\mathrm{Div}(F)$.

Рассмотрим сначала этот вопрос для случая конечного расширения E степени n поля F. Пусть $e_{\mathfrak{P}}$ — *индекс ветвления* простого дивизора $\mathfrak{P}$ поля E, лежащего над простым дивизором P поля F ($\mathfrak{P}|P$), относительно P (см. задачу 2). Если F и E имеют одно и то же поле констант и если

$$\mathrm{con}\colon \mathrm{Div}(F) \to \mathrm{Div}(E)$$

— отображение, ставящее в соответствие каждому дивизору

$$A = \sum_P v_P(A) \cdot P$$

группы $\mathrm{Div}(F)$ дивизор

$$\mathrm{con}_{F/E} A = \sum_{\mathfrak{P}} v_P(A)\, e_{\mathfrak{P}} \cdot \mathfrak{P}$$

группы $\mathrm{Div}(E)$ (называемый *конормой* дивизора A), то для всех $A \in \mathrm{Div}(F)$ имеет место (см. задачу 5) соотношение

$$\deg(\mathrm{con}_{F/E} A) = n \deg A.$$

Введенное выше отображение

$$i\colon \mathrm{Div}(F) \to \mathring{\mathfrak{D}}$$

вполне аналогично отображению con.

Кроме того, размер $\sigma(A)$ дивизора A, рассматриваемого как элемент группы $\mathring{\mathfrak{D}}$, играет роль степени этого дивизора. Поэтому, несмотря на то, что расширение $^*K$ поля F не является конечным, мы вправе надеяться на существование такого гипердействительного числа $\nu > \mathring{0}$, для которого при всех $A \in \mathrm{Div}(F)$ справедливо аналогичное соотношение

$$\sigma(A) \mathrel{\mathring{=}} \nu \deg A.$$

Однако, ввиду того, что $^*\mathbb{R}$ является неархимедовым упорядоченным полем, последнее соотношение в общем случае оказывается неверным. Тем не менее, справедливо весьма похожее, но более слабое, соотношение

$$\frac{\sigma(A)}{\nu} \approx \deg A, \tag{6}$$

где символ $\approx$ означает бесконечную близость соответствующих гипердействительных чисел.

Прежде чем перейти к доказательству справедливости последнего соотношения, остановимся на нем более детально. Напомним, что два гипердействительных числа $\alpha, \beta \in {}^*\mathbb{R}$ называются бесконечно близкими, если $\alpha = \beta + \delta$ для некоторого

бесконечно малого числа δ. Как и в случае конечных гипердействительных чисел, бесконечно малые числа образуют изолированную аддитивную подгруппу $^*\mathbb{R}_{\mathrm{inf}}$ группы $^*\mathbb{R}$. Поэтому факторгруппа $^*\mathbb{R}/{}^*\mathbb{R}_{\mathrm{inf}}$ наследует отношение порядка, имеющегося на $^*\mathbb{R}$. В соответствии с этим, если $\alpha \leqslant \beta + \delta$ при некотором бесконечно малом δ, то будем писать $\alpha \mathrel{\mathring{\leqslant}} \beta$. Заметим, что оба отношения $\alpha \mathrel{\mathring{\leqslant}} \beta$ и $\alpha \leqslant \beta$ имеют аддитивный характер и не согласованы с операцией умножения. Тем не менее, множество $^*\mathbb{R}_{\mathrm{fin}}$ образует кольцо нормирования поля $^*\mathbb{R}$, а множество $^*\mathbb{R}_{\mathrm{inf}}$ является максимальным идеалом этого кольца.

Лемма 3. *Пусть ν — бесконечно большое гипердействительное число. Если $\alpha \mathrel{\mathring{\leqslant}} \beta$, тогда $\alpha/\nu \leqslant \beta/\nu$. В частности, если $\alpha \mathrel{\mathring{=}} \beta$, то $\alpha/\nu \approx \beta/\nu$. Другими словами, сопоставление $\alpha \mapsto \alpha/\nu$ задает сохраняющий отношение порядка гомоморфизм аддитивной группы $\mathring{\mathbb{R}} = {}^*\mathbb{R}/{}^*\mathbb{R}_{\mathrm{fin}}$ на группу $^*\mathbb{R}/{}^*\mathbb{R}_{\mathrm{inf}}$.*

Доказательство. Если $\alpha \mathrel{\mathring{\leqslant}} \beta$, то $\alpha \leqslant \beta + \gamma$, где γ — некоторое конечное число. Отсюда следует, что $\alpha/\nu \leqslant \beta/\nu + \delta$, где $\delta = \gamma/\nu$, а так как γ — конечное и ν — бесконечно большое, то δ — бесконечно малое число. Следовательно, $\alpha/\nu \leqslant \beta/\nu$ и лемма, тем самым, доказана.

Если $A \in \mathrm{Div}(F)$, то число $\sigma(A)$ определено по $\mathrm{mod}\ ^*\mathbb{R}_{\mathrm{fin}}$. Из предыдущей леммы следует, что отношение $\sigma(A)/\nu$ определено по $\mathrm{mod}\ ^*\mathbb{R}_{\mathrm{inf}}$. Поэтому соотношение (6) является лучшим, на что можно надеяться при наших рассмотрениях.

Теорема 1. *Существует бесконечно большое число $\nu \in {}^*\mathbb{R}$ такое, что*

$$\frac{\sigma(A)}{\nu} \approx \deg A$$

для всех функциональных дивизоров $A \in \mathrm{Div}(F)$. Число ν определено однозначно с точностью до бесконечно малых в следующем мультипликативном смысле: если $\mu \in {}^*\mathbb{R}$ — другое такое число, то $\nu/\mu \approx 1$.

Доказательство. Выясним сначала формальные свойства отображения σ.

1) *Отображение $\sigma\colon \mathrm{Div}(F) \to \mathring{\mathbb{R}}$ представляет собой сохраняющий отношение порядка гомоморфизм, который равен нулю на главных дивизорах $[x] \in \mathrm{Div}(F)$.*

Ввиду включения $\mathrm{Div}(F) \subset \mathring{\mathfrak{D}}$, справедливость первого утверждения следует из его справедливости для исходного отображения $\sigma\colon {}^*\mathfrak{D} \to {}^*\mathbb{R}$. Что касается второго утверждения, то ввиду формулы (3) из § 3 гл. VI, оно справедливо для отображения $\sigma\colon {}^*\mathfrak{D} \to {}^*\mathbb{R}$ и для главных дивизоров $(x) \in {}^*\mathfrak{D}$. Поскольку, ввиду соотношения (5), дивизоры $[x]$ и (x) можно отождествить, то оно справедливо также и для отображения $\sigma\colon \mathrm{Div}(F) \to \mathring{\mathbb{R}}$.

2) *Отображение* $\sigma\colon \mathrm{Div}(F)\to \mathring{\mathbb{R}}$ *не равно тождественно нулю. Более того,* $\sigma(A)\overset{\circ}{>}0$ *для каждого* $A>0$.

Если $A>0$ в группе $\mathrm{Div}(F)$, то $A\overset{\circ}{>}0$ в группе $\mathring{\mathfrak{D}}$ и, следовательно, достаточно показать, что для каждого внутреннего дивизора $\mathfrak{a}$ неравенство $\mathfrak{a}\overset{\circ}{>}0$ влечет за собой неравенство $\sigma(\mathfrak{a})\overset{\circ}{>}0$. Ввиду леммы 3 из § 3 гл. VI, если $\mathfrak{a}\overset{\circ}{>}0$, то существует $\mathfrak{p}\in {}^*V$, для которого $w_{\mathfrak{p}}(\mathfrak{a})\overset{\circ}{>}0$. В таком случае, достаточно доказать, что

$$\mathfrak{a}\overset{\circ}{\geqslant}0\Rightarrow\sigma(\mathfrak{a})\overset{\circ}{\geqslant}w_{\mathfrak{p}}(\mathfrak{a})$$

для любого внутреннего дивизора $\mathfrak{a}$ и любого внутреннего простого дивизора $\mathfrak{p}$. Это утверждение тривиальным образом справедливо в ${}^*\mathfrak{D}$, а именно

$$\mathfrak{a}\geqslant 0\Rightarrow\sigma(\mathfrak{a})\geqslant w_{\mathfrak{p}}(\mathfrak{a}).$$

Но тогда оно выполняется также и в $\mathring{\mathfrak{D}}$.

Приступим теперь к доказательству теоремы. Пусть g — род поля F. Если $\deg A\geqslant g$, то из теоремы Римана — Роха следует, что существует положительный дивизор $A'\geqslant 0$, который линейно эквивалентен дивизору A. Тогда из свойства 1) выводим, что

$$\sigma(A)\overset{\circ}{=}\sigma(A')\overset{\circ}{\geqslant}0.$$

Если $\deg A>0$, тогда существует положительное целое $n\in\mathbb{Z}$ такое, что $\deg(nA)\geqslant g$. В таком случае $\sigma(nA)=n\sigma(A)\overset{\circ}{\geqslant}0$ и, следовательно, $\sigma(A)\overset{\circ}{\geqslant}0$. Заменяя теперь дивизор A на дивизор $A-B$, получаем

$$\deg A\geqslant\deg B\Rightarrow\sigma(A)\overset{\circ}{\geqslant}\sigma(B).$$

Далее, заменяя A и B соответственно на mA и nB, где $m,\ n\in\mathbb{Z}$, выводим, что

$$m\deg A>n\deg B\Rightarrow m\sigma(A)\overset{\circ}{>}n\sigma(B). \tag{7}$$

Последнее утверждение остается справедливым и для рациональных m, n (этот случай сводится к случаю целых m, n умножением на наименьший общий знаменатель).

Выберем фиксированный положительный дивизор $B>0$. Тогда $\deg B>0$ и по свойству 2) $\sigma(B)\overset{\circ}{>}0$. Пусть $\nu\in{}^*\mathbb{R}$ таково, что $\nu\overset{\circ}{=}\sigma(B)/\deg B$. Ясно, что ν — бесконечно большое гипердействительное число. Полагая в (7) $m=1$, $n=r/\deg B$, где $r\in\mathbb{Q}$, и используя результат леммы 3, получаем

$$\deg A>r\Rightarrow\sigma(A)\overset{\circ}{>}r\nu\Rightarrow\sigma(A)/\nu\gtrsim r.$$

Данное утверждение справедливо для любых рациональных $r<\deg A$. Поэтому, устремляя r к $\deg A$, приходим к неравенству

$$\frac{\sigma(A)}{\nu}\gtrsim\deg A.$$

С другой стороны, проведя в (7) замены $A\leftrightarrow B$ и повторяя рассуждения, получаем противоположное неравенство

$$\frac{\sigma(A)}{\nu}\lesssim\deg A.$$

Следовательно,

$$\frac{\sigma(A)}{\nu}\approx\deg A$$

и остается лишь доказать единственность числа ν.

Заметим, что если $\alpha,\beta\notin{}^*\mathbb{R}_{\mathrm{inf}}$, тогда $\alpha\approx\beta\Rightarrow\alpha/\beta\approx 1$. Пусть A — произвольный дивизор положительной степени. Тогда в соотношении

$$\frac{\sigma(A)}{\nu}\approx\deg A\approx\frac{\sigma(A)}{\mu}$$

числа $\sigma(A)/\nu$ и $\sigma(A)/\mu$ не являются бесконечно малыми и, стало быть, $\nu/\mu\approx 1$. Теорема доказана.

Следствие 1. *Пусть* $A,\ B\in\mathrm{Div}(F)$. *Если* $\deg A>0$, *то* $\sigma(A)\overset{\circ}{>}0$ *и*

$$\frac{\sigma(B)}{\sigma(A)}\approx\frac{\deg B}{\deg A}.$$

Рассмотрим теперь непостоянный элемент $x\in F$ и возьмем в качестве A дивизор полюсов элемента x:

$$A=-(0,\ [x])=\{0,\ -[x]\}.$$

Мы знаем, что (см. теорему 7 из § 2, гл. IV) $\deg A=[F\colon K(x)]$. С другой стороны, если рассмотрим A как внутренний дивизор, то получим, что

$$A\overset{\circ}{=}\{0,-(x)\},$$

где $\{0,\ -(x)\}$ является знаменателем элемента $x\in{}^*K$ в арифметическом смысле. Чтобы вычислить размер этого знаменателя, заметим, что

$$w_{\mathfrak{p}}\{0,-(x)\}=\max\big(0,-w_{\mathfrak{p}}(x)\big)=\log\max\big(1,\|x\|_{\mathfrak{p}}\big),$$

и введем в рассмотрение *высоту Хассе*

$$H(x)=\prod_{\mathfrak{p}}\max\big(1,\|x\|_{\mathfrak{p}}\big)$$

элемента x. Тогда получаем соотношение

$$\sigma(A) \overset{\circ}{=} \log H(x)$$

и приходим к следующему результату.

Следствие 2. *Пусть x — непостоянный элемент поля F. Тогда для каждого дивизора $B \in \mathrm{Div}(F)$ справедливо соотношение*

$$\frac{\sigma(B)}{\log H(x)} \approx \frac{\deg B}{[F\colon K(x)]}.$$

В частности, взяв в качестве B дивизор полюсов другого непостоянного элемента $y \in F$, получаем следующий результат.

Следствие 3. *Для любых двух непостоянных элементов имеет место соотношение*

$$\frac{\log H(y)}{\log H(x)} \approx \frac{[F\colon K(y)]}{[F\colon K(x)]}.$$

2. Исключительные функциональные дивизоры. Пусть P — функциональный простой дивизор поля F. Из леммы 1 следует, что существует по меньшей мере один арифметический простой дивизор $\mathfrak{p}$ поля $^*K$, такой, что $\mathfrak{p}|P$. С другой стороны, теорема B утверждает, что среди таких арифметических простых дивизоров $\mathfrak{p}$ имеется нестандартный простой дивизор, если только род g поля F больше нуля. Следовательно, необходимо изучить те функциональные простые дивизоры P, которые не индуцируются нестандартными простыми дивизорами $\mathfrak{p}$. Такие простые дивизоры назовем *исключительными* и покажем, что исключительные простые дивизоры существуют только в случае $g = 0$.

Расширим понятие исключительных простых дивизоров и назовем функциональный дивизор $A \in \mathrm{Div}(F)$ *исключительным*, если

$$A = P_1 + P_2 + \ldots + P_r,$$

где P_i — различные исключительные простые дивизоры. Таким образом, исключительные дивизоры положительны и не имеют кратных компонент.

Наша ближайшая цель будет состоять в том, чтобы получить оценку для степени исключительного дивизора A, которая одновременно даст нам верхнюю оценку для числа исключительных простых дивизоров поля F (если только они существуют). Как мы знаем из теоремы 1, степень дивизора A тесно связана с его размером. В силу этого приходим к необходимости изучения размера $\sigma(A)$ исключительного дивизора A.

Скажем, что арифметический простой дивизор $\mathfrak{p}$ *эффективен на* A (обозначение: $\mathfrak{p}|A$), если $\mathfrak{p}$ индуцирует некоторую компоненту P дивизора A.

Лемма 4. *Пусть $A \in \mathrm{Div}(F)$ — исключительный дивизор поля F. Тогда существует лишь конечное число арифметических простых дивизоров $\mathfrak{p}$ поля $^*K$, эффективных на A. Простые дивизоры $\mathfrak{p}|A$ характеризуются условием $w_{\mathfrak{p}}(A) \overset{\circ}{>} 0$ и имеет место соотношение*

$$\sigma(A) \overset{\circ}{=} \sum_{\mathfrak{p}|A} w_{\mathfrak{p}}(A).$$

Доказательство. Если $\mathfrak{p}|A$, то существует некоторая компонента P дивизора A, такая, что $\mathfrak{p}|P$. Отсюда, ввиду (4) получаем

$$w_{\mathfrak{p}}(A) \overset{\circ}{=} n_{\mathfrak{p}} w_P(A) \overset{\circ}{\geqslant} n_{\mathfrak{p}} \overset{\circ}{>} 0.$$

Обратно, предположим, что $w_{\mathfrak{p}}(A) \overset{\circ}{>} 0$. Тогда из формулы (4) следует ,что простой дивизор $\mathfrak{p}$ эффективен на F, т. е. существует некоторый функциональный простой дивизор P, такой, что $\mathfrak{p}|P$. Более того, эта формула показывает, что $w_P(A) > 0$ для простого дивизора P. Значит, P является компонентой дивизора A и, следовательно, $\mathfrak{p}|A$. Таким образом, мы установили, что

$$\mathfrak{p}\,|\,A \Leftrightarrow w_{\mathfrak{p}}(A) \overset{\circ}{>} 0.$$

Рассмотрим теперь A как элемент группы $\mathring{\mathfrak{D}}$ в соответствии с вложением

$$i\colon \mathrm{Div}(F) \to \mathring{\mathfrak{D}}.$$

Пусть $\mathfrak{a} \in {}^*\mathfrak{D}$ — внутренний дивизор, представляющий A в $\mathring{\mathfrak{D}}$ $(\mathfrak{a} \overset{\circ}{=} A)$. Тогда для каждого $\mathfrak{p}$ имеем $w_{\mathfrak{p}}(\mathfrak{a}) \overset{\circ}{=} w_{\mathfrak{p}}(A)$. Это означает, что гипердействительное число $w_{\mathfrak{p}}(\mathfrak{a})$ представляет $w_{\mathfrak{p}}(A)$ в $\mathring{\mathbb{R}}$. Обозначим S множество тех арифметических простых дивизоров $\mathfrak{p}$, для которых $w_{\mathfrak{p}}(\mathfrak{a}) \overset{\circ}{>} 0$. Тогда S — внутреннее множество и, как было показано выше, S содержит каждый простой дивизор $\mathfrak{p}$, эффективный на A. Более того, если простой дивизор $\mathfrak{p} \in S$ не эффективен на A, то $w_{\mathfrak{p}}(\mathfrak{a}) \overset{\circ}{=} 0$.

Покажем, что S не содержит нестандартных простых дивизоров. Пусть, например, $\mathfrak{p} \in S$ — нестандартный простой дивизор. Тогда $\mathfrak{p} \nmid A$ (так как A — исключительный дивизор) и, следовательно, $w_{\mathfrak{p}}(\mathfrak{a}) \overset{\circ}{=} 0$. Это означает, что гипердействительное число $w_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{a}) \log(N\mathfrak{p})$ положительно и конечно. В результате мы приходим к противоречию с тем, что $N\mathfrak{p}$ — бесконечно большое число (см. лемму 1 из § 3 гл. VI).

Так как S — внутреннее множество, не содержащее нестандартных элементов, то оно необходимо конечно. В частности, имеется лишь конечное число арифметических простых дивизоров $\mathfrak{p}$, которые эффективны на A.

Положим

$$\mathfrak{a}' = \sum_{\mathfrak{p}|A} v_{\mathfrak{p}}(\mathfrak{a})\cdot\mathfrak{p}.$$

Поскольку сумма справа конечна, то $\mathfrak{a}'$ — внутренний дивизор. По построению, дивизор $\mathfrak{a}'$ совпадает с $\mathfrak{a}$ в простых $\mathfrak{p}|A$ и равен нулю в других простых $\mathfrak{p}|\mathfrak{a}$. Следовательно,

$$w_{\mathfrak{p}}(\mathfrak{a}') \overset{\circ}{=} w_{\mathfrak{p}}(A) \overset{\circ}{>} 0, \quad \text{если} \quad \mathfrak{p}\,|\,A$$

и

$$w_{\mathfrak{p}}(\mathfrak{a}') = 0 \overset{\circ}{=} w_{\mathfrak{p}}(A), \quad \text{если} \quad \mathfrak{p} \nmid A.$$

Отсюда следует, что $\mathfrak{a}' \overset{\circ}{=} A$, т. е. $\mathfrak{a}' \in {}^*D$ также является представителем дивизора $A \in \mathfrak{D}$. Стало быть,

$$\sigma(A) \overset{\circ}{=} \sigma(\mathfrak{a}') = \sum_{\mathfrak{p}|A} w_{\mathfrak{p}}(\mathfrak{a}) \overset{\circ}{=} \sum_{\mathfrak{p}|A} w_{\mathfrak{p}}(A).$$

Лемма доказана.

Элемент $x \in F$ назовем *A-целым*, если ни один из полюсов этого элемента не является компонентой дивизора A, т. е. если $w_P(x) \geqslant 0$ для каждой компоненты P дивизора A.

Следствие. *Пусть A — исключительный дивизор поля F, каждая компонента которого имеет степень 1. Тогда для каждого A-целого непостоянного элемента $x \in F$ найдутся такие элементы $a_{\mathfrak{p}} \in K$, $\mathfrak{p}\,|\,A$, что*

$$\sigma(A) \overset{\circ}{\leqslant} \sum_{\mathfrak{p}|A} w_{\mathfrak{p}}(x - a_{\mathfrak{p}}).$$

Доказательство. Пусть P — компонента дивизора A, индуцированная арифметическим простым дивизором $\mathfrak{p}|A$ и $a_{\mathfrak{p}}$ — вычет элемента x по $\bmod P$. Так как $\deg P = 1$, то $a_{\mathfrak{p}} \in K$, и элемент $x - a_{\mathfrak{p}}$ поля F имеет ноль в P, т. е. $v_P(x - a_{\mathfrak{p}}) \geqslant 1$. С другой стороны, P — простая компонента дивизора A (компонента кратности 1) и, стало быть, $w_P(A) = 1 \leqslant v_P(x - a_{\mathfrak{p}})$. Значит, $w_P(A) \leqslant w_P(x - a_{\mathfrak{p}})$ и тогда, ввиду (4),

$$w_{\mathfrak{p}}(A) \overset{\circ}{\leqslant} w_{\mathfrak{p}}(x - a_{\mathfrak{p}}).$$

Утверждение следует теперь из леммы 4. Следствие доказано.

Наша задача по нахождению верхней оценки размеров исключительных дивизоров редуцируется, таким образом, к задаче об отыскании верхней оценки для конечных сумм вида

$$\sum_{\mathfrak{p}|A} w_{\mathfrak{p}}(x - a_{\mathfrak{p}}).$$

Для решения последней задачи воспользуемся теоремой Туэ — Зигеля — Рота, которую можно сформулировать следующим образом.

Теорема 2. *Пусть S — конечное множество простых дивизоров $\mathfrak{p}$ поля K, $a_{\mathfrak{p}}$ — заданные элементы алгебраического замыкания $\overline{K}$ поля K и $\varkappa > 2$ — произвольное действительное число. Тогда существует лишь конечное число элементов $x \in K$, удовлетворяющих неравенству*

$$\prod_{\mathfrak{p}\in S} \|x - a_{\mathfrak{p}}\|_{\mathfrak{p}}^{*} \leqslant H(x)^{-\varkappa}, \tag{8}$$

где $\|\ \|_{\mathfrak{p}}^{*}$ — продолжение нормы $\|\ \|_{\mathfrak{p}}$ на $\overline{K}$.

Туэ, Зигель и Рот рассматривали случай $K = \mathbb{Q}$ и $S = \{\mathfrak{p}\}$, где $\mathfrak{p}$ — единственный архимедов простой дивизор поля рациональных чисел $\mathbb{Q}$, который, как оказалось, содержит в себе все принципиальные трудности. При этом Туэ [122] установил справедливость сформулированного выше результата при $\varkappa > \nu/2 + 1$, а Зигель [54a] — при $\varkappa > 2\sqrt{\nu}$, где ν — степень $a^{\mathfrak{p}}$ над полем $\mathbb{Q}$. Наконец, Рот [107] доказал конечность числа решений неравенства (8) в элементах $x \in \mathbb{Q}$ для всякого заданного $\varkappa > 2$.

Обобщение теоремы Туэ — Зигеля — Рота на случай произвольного конечного расширения K поля $\mathbb{Q}$ и $S = \{\mathfrak{p}\}$, где $\mathfrak{p}$ — произвольный архимедов простой дивизор поля K, было предложено Левеком [68a].

Риду [102] распространил теорему Туэ — Зигеля — Рота на случай $K = \mathbb{Q}$ и $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Аналогичный результат для равных между собой чисел $a_{\mathfrak{p}}$ был получен автором [117a] в случае произвольного расширения K поля $\mathbb{Q}$. Сформулированная выше теорема является частным случаем более общих результатов, полученных Малером [79c, приложение C] и Ленгом (см. [70h, гл. 7]).

По теореме Туэ — Зигеля — Рота множество элементов $x \in K$, удовлетворяющих неравенству (8), конечно. Следовательно, оно не расширяется при переходе к полю ${}^*K$. Это означает, что каждый элемент $x \in {}^*K$, который удовлетворяет этому неравенству, является стандартным и, значит, если $x \in {}^*K$ — нестандартный элемент, то он не удовлетворяет указанному неравенству. В результате мы получаем следующую нестандартную версию теоремы Туэ — Зигеля — Рота.

Теорема 3. *Пусть S — конечное множество стандартных простых дивизоров поля $^*K$, $a_\mathfrak{p}$ — заданные стандартные элементы этого поля и $\varkappa > 2$ — стандартное гипердействительное число. Тогда для каждого нестандартного элемента $x \in {}^*K$ выполняется неравенство*

$$\prod_{\mathfrak{p}\in S} \|x - a_\mathfrak{p}\|_\mathfrak{p} > H(x)^{-\varkappa}.$$

Логарифмируя обе части этого неравенства, получаем

$$\sum_{\mathfrak{p}\in S} w_\mathfrak{p}(x - a_\mathfrak{p}) < \varkappa \log H(x).$$

Выбирая затем элементы $a_\mathfrak{p} \in K$ в соответствие с утверждением следствия леммы 4, приходим к неравенству

$$\sigma(A) \overset{\circ}{\leqslant} \varkappa \log H(x).$$

Так как $\log H(x)$ — бесконечно большое число, то (ввиду леммы 3)

$$\frac{\sigma(A)}{\log H(x)} \leqslant \varkappa,$$

а так как $\varkappa > 2$ — произвольное стандартное число, то

$$\frac{\sigma(A)}{\log H(x)} \leqslant 2.$$

С другой стороны, согласно следствию 2 теоремы 1 имеем

$$\frac{\sigma(A)}{\log H(x)} \approx \frac{\deg A}{[F\colon K(x)]}.$$

В таком случае

$$\frac{\deg A}{[F\colon K(x)]} \leqslant 2$$

и, следовательно,

$$\deg A \leqslant 2[F\colon K(x)]. \tag{9}$$

Неравенство (9) получено для всякого непостоянного элемента $x \in F$ и для каждого исключительного дивизора A при дополнительных условиях, что x является A-целым элементом и что каждая компонента дивизора A имеет степень 1. Покажем, что эти дополнительные условия можно исключить. Другими словами, неравенство (9) справедливо для каждого исключительного дивизора A и для всех непостоянных элементов x поля F.

Чтобы исключить первое дополнительное условие, заметим, что формула (9) зависит лишь от поля $K(x)$ и не зависит от выбора порождающего элемента x этого поля. Поэтому, если x не является A-целым, то выберем другой порождающий элемент y поля $K(x)$, который будет A-целым. Тогда справедливость неравенства (9) для y влечет, ввиду равенства $K(x) = K(y)$, его справедливость для x. Например, можно взять $y = (x - c)^{-1}$, где элемент $c \in K$ выбран таким образом, что он отличен от вычетов элемента x по $\bmod P$ для каждой компоненты P дивизора A, не являющейся полюсом для x.

Чтобы исключить второе дополнительное условие, воспользуемся методом расширения поля констант. Если K' — конечное расширение поля K, то обозначим $F' = FK'$ соответствующее ему расширение поля F (которое можно трактовать как поле частных кольца $F \otimes_K K'$, либо как композит полей F и K'). Группа $\mathrm{Div}(F)$ естественным образом вкладывается в группу $\mathrm{Div}(F')$, и такое вложение не изменяет степени дивизоров (см. задачи 5, 9). Это означает, что если рассматривать дивизор $A \in \mathrm{Div}(F)$ как элемент группы $\mathrm{Div}(F')$, то его степень (над новым полем констант K') равна степени дивизора A как элемента группы $\mathrm{Div}(F)$. Кроме того, для любого непостоянного элемента $x \in F$ имеет место равенство $[F\colon K(x)] = [F'\colon K'(x)]$ (см. задачу 8). Следовательно, справедливость неравенства (9) в поле F' над K' влечет за собой его справедливость в поле F над K. Хорошо известно (см. задачи 4, 6), что поле K' можно выбрать таким образом, что каждая компонента дивизора $A \in \mathrm{Div}(F)$ распадается в группе $\mathrm{Div}(F')$ на простые компоненты степени 1. Такое поле F' называется *полем разложения дивизора* A. Таким образом, если мы покажем, что исключительный дивизор A поля остается исключительным в его поле разложения F', то из справедливости неравенства (9) в поле F' получим справедливость этого неравенства в поле F.

Напомним, что понятие исключительного дивизора поля F связано с вложением $F \subset {}^*K$ этого поля в нестандартное расширение $^*K$ поля K. Поэтому, чтобы говорить об исключительных дивизорах поля $F' = FK'$, необходимо вложить его в нестандартное расширение $^*K'$ поля K'. Поле F' естественным образом вкладывается в композит $^*KK'$ полей $^*K$ и K'. Покажем, что этот композит совпадает с нестандартным расширением $^*K'$ поля K'. Действительно, пусть $\omega_1, \ldots, \omega_n$ — базис поля K' над K. Утверждение о том, что элементы $\omega_1, \ldots, \omega_n$ составляют базис K' над K остается истинным в нестандартном расширении и, значит, элементы $\omega_1, \ldots, \omega_n$ образуют базис поля $^*K'$ над $^*K$. Следовательно, $^*KK' = {}^*K'$ и поля $^*K$, K' линейно разделены над K. Отсюда получаем, что поле F' естественным образом вкладывается в поле $^*K'$. Это вложение $F' \subset {}^*K'$ дает возможность рассматривать свойство исключительности дивизора A поля F'. Пусть $\mathfrak{p}'$ — арифметический простой дивизор поля $^*K'$, эффективный на A. Чтобы установить исключительность дивизора $A \in \mathrm{Div}(F')$, мы должны показать, что $\mathfrak{p}'$ — стандартный простой дивизор. Пусть P' — функциональный простой дивизор поля F', индуцированный простым дивизором $\mathfrak{p}'$. Тогда P' является компонентой дивизора

$A \in \mathrm{Div}(F')$. Пусть, далее, P — функциональный простой дивизор поля F, индуцированный простым дивизором P'. Тогда P является компонентой дивизора $A \in \mathrm{Div}(F)$. Пусть, кроме того, $\mathfrak{p}$ — арифметический простой дивизор поля $^*K$, индуцированный простым дивизором $\mathfrak{p}'$. В результате мы имеем ситуацию, изображенную на рис. 3 в виде диаграммы полей и соответствующих простых дивизоров. Из построения следует, что P индуцирован арифметическим простым дивизором $\mathfrak{p}$. Стало быть, поскольку A — исключительный дивизор поля F, то $\mathfrak{p}$ — стандартный простой дивизор. В частности, простой дивизор $\mathfrak{p}$ не тривиален на K и тогда $\mathfrak{p}'$ не тривиален на K'. Отсюда получаем, что $\mathfrak{p}'$ является стандартным простым дивизором поля K'.

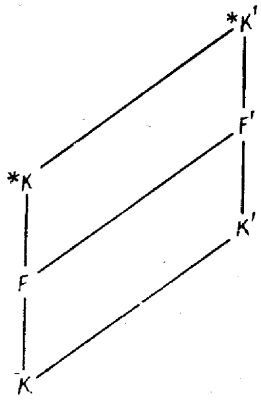


Рис. 3

Отметим также, что расширение $F' = FK'$ поля F *не разветвлено* (см. задачи 2, 6). Это означает, что каждый функциональный простой дивизор P поля F при его рассмотрении в качестве дивизора поля F' **не содержит кратных компонент.** Отсюда следует, что исключительный дивизор A не имеет кратных компонент не только в группе $\mathrm{Div}(F)$, но также и в группе $\mathrm{Div}(F')$.

Из сказанного выше заключаем, что каждый исключительный дивизор A поля F остается исключительным и в поле $F' = FK'$. Следовательно, если возьмем в качестве F поле разложения дивизора A, то получим, что неравенство (9) справедливо для поля K без всяких дополнительных условий на x и на исключительный дивизор A.

Положим

$$d = \min_{\substack{x \in F \\ x \notin K}} [F:\ K(x)] \tag{10}$$

и назовем d *минимальной степенью поля* F над подполем рациональных функций. Эта величина является инвариантом поля F. Из неравенства (9) выводим, что

$$\deg A \leqslant 2d$$

для каждого исключительного дивизора A поля F. В частности, мы видим, что число компонент дивизора A ограничено величиной $2d$. Отсюда следует, что имеется не более $2d$ исключительных простых дивизоров поля F.

Резюмируя изложенное выше, получаем следующий результат.

Теорема 4. *Пусть d — минимальная степень поля F. Имеется лишь конечное число $r \leqslant 2d$ исключительных простых дивизоров $P_1, \ldots, P_r$ поля F и, если*

$$A = P_1 + \ldots + P_r,$$

то

$$\deg A \leqslant 2d.$$

Следствие. *Справедливо неравенство*

$$\deg A \leqslant 2g + 2,$$

где g — род поля F над K.

Доказательство. Достаточно показать, что $d \leqslant g + 1$. Пусть B — произвольный дивизор поля F степени $g + 1$. Тогда, по теореме Римана — Роха, $\dim_K L(-B) \geqslant 2$ и, следовательно, существуют по меньшей мере два различных положительных дивизора B' и B'', линейно эквивалентных дивизору B. Для этих дивизоров имеем $B' - B'' = [x]$, где x — непостоянный элемент поля F, $[F:\ K(x)] \leqslant \deg B'' = \deg B = g + 1$. Следствие доказано.

При доказательстве следствия был использован тот факт, что существует по меньшей мере один функциональный дивизор степени $g + 1$. Для полноты изложения покажем, что каждое стандартное целое является степенью некоторого функционального дивизора поля F. Для этого достаточно, очевидно, установить существование хотя бы одного функционального дивизора степени 1. Справедливо следующее утверждение (ср. его с соответствующим утверждением из § 1 гл. V).

Предложение. *Каждое поле алгебраических функций F над K, вложенное в $^*K$, имеет бесконечно много простых дивизоров степени 1.*

Доказательство. Пусть x_1 — непостоянный элемент поля F и R — целое замыкание кольца $K[x_1]$ в поле F. Тогда R является конечно порожденной K-алгеброй и, если $R = K[x_1, \ldots, x_m]$, то пусть

$$f_i(x_1, \ldots, x_m) = 0, \quad 1 \leqslant i \leqslant r,$$

— система определяющих соотношений для $x_1, \ldots, x_m$ над полем K. Так как эта система имеет нестандартное решение $x_1, \ldots, x_m$, то в соответствии с принципом нестандартного расширения для множества она имеет бесконечно много решений $(a_1, \ldots, a_m) \in K^m$. Каждое такое решение задает K-гомоморфизм $R \to K$, отображающий x_j на a_j. Ядром этого гомоморфизма является максимальный идеал кольца R. Отсюда следует, что имеется бесконечно много максимальных идеалов $\mathfrak{m}$ кольца R таких, что $R/\mathfrak{m} = K$. С другой стороны, поскольку R является дедекиндовым кольцом, то его максимальные идеалы $\mathfrak{m}$ находятся во взаимно однозначном соответствии с теми простыми дивизорами P поля F, чьи кольца нормирований содержат R. При таком соответствии кольцо нормирования простого диви-

зора P совпадает с локализацией кольца R относительно $\mathfrak{m}$ и поле вычетов простого дивизора P изоморфно полю $R/\mathfrak{m}$. Из сказанного следует, что имеется бесконечно много функциональных простых дивизоров P поля F с полем вычетов K, т. е. простых дивизоров степени 1. Предложение доказано.

Отметим, что справедливо и обратное утверждение: *если абстрактное поле функций F над K от одной переменной имеет бесконечно много простых дивизоров степени 1, то существует K — изоморфизм этого поля в $^*K$.* Это утверждение получается из принципа нестандартного расширения для множеств обращением приведенных выше рассуждений.

Задачи

1. Пусть F/K — поле алгебраических функций от одной переменной с полем констант K, вложенное в $^*K$, и пусть $\varphi\colon \mathrm{Div}(F) \to \overset{\circ}{\mathbb{R}}$ — произвольный нетривиальный гомоморфизм, сохраняющий отношение порядка и обращающийся в ноль на главных дивизорах.

Доказать, что существует бесконечно большое число $\nu \in {}^*\mathbb{R}$, такое, что $\varphi(A)/\nu \approx \deg A$ для каждого дивизора $A \in \mathrm{Div}(F)$.

2. Пусть F/K и E/L — поля алгебраических функций от одной переменной с полями констант K и L. В дальнейшем будем считать, что E/L — алгебраическое расширение поля F/K и что $F \cap L = K$. Каждый простой дивизор $\mathfrak{P}$ поля E/L индуцирует некоторый простой дивизор P поля F/K. В этом случае будем говорить, что $\mathfrak{P}$ лежит над P и писать $\mathfrak{P}|P$. Если v_P — P-адическая порядковая функция поля F/K, так что $v_P(F^*) = \mathbb{Z}$ и $v_{\mathfrak{P}}$ — индуцирующее функцию v_P нормирование поля E/L с группой значений $v_{\mathfrak{P}}(F^*) = \Gamma_{\mathfrak{P}} \subset \subset \mathbb{Z}$, то индекс $e_{\mathfrak{P}} = (\mathbb{Z}\colon \Gamma_{\mathfrak{P}})$ назовем *индексом ветвления* дивизора $\mathfrak{P}$ относительно P. Если $e_{\mathfrak{P}} > 1$, то простой дивизор $\mathfrak{P}$ называется *разветвленным* относительно P; если же $e_{\mathfrak{P}} = 1$, то $\mathfrak{P}$ называется *неразветвленным*.

Пусть $\mathfrak{o}_P$, $\mathfrak{m}_P$ и $\mathfrak{o}_{\mathfrak{P}}$, $\mathfrak{m}_{\mathfrak{P}}$ — локальные кольца и их максимальные идеалы нормирований v_P и $v_{\mathfrak{P}}$ соответственно. Поля $\Sigma_P = \mathfrak{o}_P/\mathfrak{m}_P$ и $\Sigma_{\mathfrak{P}} = \mathfrak{o}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}$ называются *полями вычетов простых дивизоров* P и $\mathfrak{P}$. Поле Σ_P канонически вкладывается в поле $\Sigma_{\mathfrak{P}}$ и степень $f_{\mathfrak{P}}$ поля $\Sigma_{\mathfrak{P}}$ над Σ_P называется *степенью простого дивизора* $\mathfrak{P}$ относительно P.

Пусть простой дивизор $\mathfrak{P}$ поля E/L лежит над простым дивизором P поля $F/K \subset E/L$.

Доказать следующие утверждения:

а) Справедливы равенства

$$[\Sigma_{\mathfrak{P}}\colon K] = [\Sigma_{\mathfrak{P}}\colon \Sigma_P]\cdot[\Sigma_P\colon K] = [\Sigma_{\mathfrak{P}}\colon L]\cdot[L\colon K].$$

б) Если x — произвольный трансцендентный над K элемент поля F, то $[F : K(x)] < \infty$, $[E : L(x)] < \infty$ и

$$[E : K(x)] = [E : F] \cdot [F : K(x)] = [E : L(x)] \cdot [L(x) : K(x)].$$

в) Для всякого трансцендентного над K элемента $x \in F$ выполняется неравенство

$$[L(x) : K(x)] = [L : K].$$

г) Следующие предложения эквивалентны между собой:

1) $[L : K] < \infty$,

2) $[E : F] < \infty$,

3) $[\Sigma_{\mathfrak{P}}\colon \Sigma_P] < \infty$.

(Указание. Воспользовавшись результатами предыдущих пунктов, доказать, что 1) $\Leftrightarrow$ 3) и 1) $\Leftrightarrow$ 2).)

д) Следующие предложения эквивалентны между собой:

1) поле L алгебраично над K,

2) поле E алгебраично над F,

3) поле $\Sigma_{\mathfrak{P}}$ алгебраично над Σ_P.

е) Если E — конечное расширение поля F и $\deg P$, $\deg \mathfrak{P}$ — *степени простых дивизоров* P, $\mathfrak{P}$ (равные степеням Σ_P над K и $\Sigma_{\mathfrak{P}}$ над L соответственно), то имеет место соотношение

$$\deg \mathfrak{P} = \frac{f_{\mathfrak{P}} \deg P}{[L\colon K]}.$$

ж) Для каждого простого дивизора P поля F существует по меньшей мере один простой дивизор поля E, лежащий над P, и число таких простых дивизоров поля E конечно.

(Указание. Пусть g — род поля F и C — класс дивизора $(g+1)P$ в группе $\mathrm{Cl}(F)$. Используя теорему Римана — Роха, показать, что в C существует по меньшей мере один положительный дивизор Q. Вывести отсюда, что

$$(g+1)P - Q = [x],$$

где $[x] \in \mathrm{Div}(F)$ — главный дивизор некоторого трансцендентного над K элемента $x \in F$, и что главный дивизор (x) поля E имеет вид

$$(x) = \sum_{i=1}^{r} \alpha_i \mathfrak{P}_i - (q),$$

где $r \geqslant 1$, α_i — положительные целые числа, $\mathfrak{P}_i$ — различные простые дивизоры поля E и q — знаменатель элемента x в поле E. Показать, что $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ исчерпывают все простые дивизоры поля E, лежащие над P.)

з) Имеет место равенство

$$[E\colon F] = \sum_{\mathfrak{P}|P} e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

(Указание. Рассмотреть элемент $x \in F$ из предыдущего пункта и воспользоваться тем, что степень дивизора нулей элемента x равна $[F : K(x)]$, а степень дивизора нулей того же элемента, рассмотренного в поле E, равна $[E : L(x)]$. Кроме того, воспользоваться результатом п. б).)

3. Пусть E — конечное расширение поля F и E_s — подполе всех *сепарабельных элементов* поля E над F (минимальные многочлены которых над полем F не имеют кратных корней). Степень $[E_s : F]$ называется *сепарабельной степенью поля* E поля F и обозначается $[E : F]_s$. Поле E является чисто несепарабельным расширением поля E_s и степень $[E : F_s]$ называется *несепарабельной степенью поля* E над F (обозначение: $[E : F]_n$).

Пусть E/L — конечное расширение поля алгебраических функций F/K и пусть $\mathfrak{P}$ — простой дивизор поля E/L, лежащий над простым дивизором P поля F/K. Степени

$$[\Sigma_{\mathfrak{P}}\colon \Sigma_P]_s \quad \text{и} \quad [\Sigma_{\mathfrak{P}}\colon \Sigma_P]_n$$

называется соответственно *сепарабельными* и *несепарабельными степенями простого дивизора* $\mathfrak{p}$ относительно P. Обозначим их $f_{\mathfrak{p},s}$ и $f_{\mathfrak{p},n}$. Простой дивизор $\mathfrak{p}$ называется *сепарабельным*, *несепарабельным* или *чисто несепарабельным* в соответствии с тем, будет ли число $f_{\mathfrak{p},n}$ равно 1, больше 1 или равно $f_{\mathfrak{p}}$.

Пусть E/L и E'/L' — два конечных расширения поля алгебраических функций F/K и σ — изоморфизм полей E и E', отображающий L на L' и оставляющий неподвижным поле F. Для каждого простого дивизора $\mathfrak{p}$ поля E с порядковой функцией $v_{\mathfrak{p}}$ определим простой дивизор $\sigma\mathfrak{p}$ поля E', положив

$$v_{\sigma\mathfrak{p}}(x)=v_{\mathfrak{p}}(\sigma^{-1}x)$$

для всех $x\in E'$. Легко видеть, что сопоставление $\mathfrak{p}\mapsto\sigma\mathfrak{p}$ задает взаимно однозначное соответствие между простыми дивизорами $\mathfrak{p}$ поля E и простыми дивизорами $\mathfrak{p}'$ поля E'.

Доказать справедливость следующих утверждений:

а) Пусть $F/K\subset E/L\subset E'/L'$ — башня полей алгебраических функций, $[E':F]<\infty$ и $\mathfrak{p}'$ — простой дивизор поля E', лежащий над простым дивизором $\mathfrak{p}$ поля E, который лежит над простым дивизором P поля F. Если $e_{\mathfrak{p}'}$, $f_{\mathfrak{p}'}$ — индекс ветвления и степень простого дивизора $\mathfrak{p}'$ относительно P; $e_{\mathfrak{p}'}$, $f_{\mathfrak{p}'}$ — индекс ветвления и степень того же простого дивизора относительно $\mathfrak{p}$ и $e_{\mathfrak{p}}$, $f_{\mathfrak{p}}$ — индекс ветвления и степень простого дивизора $\mathfrak{p}$ относительно P, то справедливы соотношения

$$e_{\mathfrak{p}'}=e_{\mathfrak{p}'}\cdot e_{\mathfrak{p}} \text{ и } f_{\mathfrak{p}'}=f_{\mathfrak{p}'}\cdot f_{\mathfrak{p}}.$$

б) Если σ — указанный выше изоморфизм конечных расширений E/L и E'/L' поля алгебраических функций F/K, то имеют место равенства $e_{\sigma\mathfrak{p}}=e_{\mathfrak{p}}$ и $f_{\sigma\mathfrak{p}}=f_{\mathfrak{p}}$.

в) Пусть E/L — конечное нормальное расширение поля алгебраических функций F/K, G — группа Галуа этого расширения и $\mathfrak{p}$ — простой дивизор поля E, лежащий над простым дивизором P поля F. Тогда каждый простой дивизор поля E, лежащий над P, имеет вид $\sigma\mathfrak{p}$ для некоторого $\sigma\in G$.

(Указание. Пусть $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ — все простые дивизоры поля E, лежащие над P и $\mathfrak{p}=\mathfrak{p}_1$. Найти такой элемент $x\in E$, для которого $v_{\mathfrak{p}}(x)>0$, $v_{\mathfrak{p}_i}(x)=0$ при $2\leqslant i\leqslant r$, и показать, что $v_{\mathfrak{p}}(\mathrm{norm}_{E/F}x)>0$ (см. [70d, гл. VIII, § 5]). Вывести отсюда, что $v_P(\mathrm{norm}_{E/F}x)>0$, а затем, что $v_{\mathfrak{p}_i}(\mathrm{norm}_{E/F}x)>0$ для каждого $i=2,3,\ldots,r$. Используя последние неравенства, показать, что для каждого $i=2,3,\ldots,r$ существует такой автоморфизм $\sigma_i\in G$, что $\mathfrak{p}_i=\sigma_i\mathfrak{p}$.)

4. Пусть E/L — нормальное расширение поля F/K с группой Галуа G. Если $\mathfrak{p}$ — простой дивизор поля E, то подгруппа $D_{\mathfrak{p}}$ группы G, состоящая из тех элементов $\sigma\in G$, для которых $\sigma\mathfrak{p}=\mathfrak{p}$, называется *группой разложения простого дивизора* $\mathfrak{p}$.

Поле $\Sigma_{\mathfrak{p}}$ является (см. ниже п. в)) нормальным расширением поля Σ_P. Каждый элемент $\sigma_{\mathfrak{p}}$ группы Галуа $G_{\mathfrak{p}}$ этого расширения индуцируется некоторым элементом σ группы $D_{\mathfrak{p}}$. Подгруппа $I_{\mathfrak{p}}$ элементов $\sigma\in D_{\mathfrak{p}}$, для которых индуцированный автоморфизм $\sigma_{\mathfrak{p}}\in G_{\mathfrak{p}}$ тривиален на $\Sigma_{\mathfrak{p}}$, называется *группой инерции простого дивизора* $\mathfrak{p}$.

Доказать справедливость следующих утверждений:

а) Число простых дивизоров поля E, лежащих над P, равно индексу $(G: D_{\mathfrak{p}})$ подгруппы $D_{\mathfrak{p}}$ в группе G.

б) Для любого автоморфизма $\sigma\in G$ имеет место равенство

$$D_{\sigma\mathfrak{p}}=\sigma D_{\mathfrak{p}}\sigma^{-1}.$$

в) Поле $\Sigma_{\mathfrak{p}}$ является нормальным расширением поля Σ_P и каждый элемент группы Галуа $G_{\mathfrak{p}}$ этого расширения индуцируется некоторым элементом σ группы $D_{\mathfrak{p}}$.

(Указание. Пусть $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ — все простые дивизоры поля E, лежащие над P и $\mathfrak{p}=\mathfrak{p}_1$. Показать, что для каждого элемента $x_{\mathfrak{p}}\in\Sigma_{\mathfrak{p}}$ можно найти такой представитель x кольца $\mathfrak{o}_{\mathfrak{p}}$, для которого $v_{\mathfrak{p}_i}(x)>0$ при всех $i=2,3,\ldots,r$. Показать, далее, что редукция по $\mathrm{mod}\,\mathfrak{p}$ минимального многочлена

$$f(t)=\{\prod_{\sigma\in G}(t-\sigma x)\}^{[E:F]_n}$$

элемента x над F является многочленом над Σ_P вида

$$f_{\mathfrak{p}}(t)=\{\prod_{\sigma\in D_{\mathfrak{p}}}(t-\sigma_{\mathfrak{p}}x_{\mathfrak{p}})\}^{[E:F]_n}t^N$$

при некотором целом $N\geqslant 0$. Вывести отсюда, что $\Sigma_{\mathfrak{p}}$ — нормальное расширение поля Σ_P и что $\sigma_{\mathfrak{p}}\in G_{\mathfrak{p}}$ индуцирован автоморфизмом $\sigma\in D_{\mathfrak{p}}$. Для доказательства того факта, что все автоморфизмы поля $\Sigma_{\mathfrak{p}}$ над Σ_P исчерпываются автоморфизмами $\sigma_{\mathfrak{p}}$, применить те же рассуждения к *примитивному элементу* $x_{\mathfrak{p}}$ поля $\Sigma_{\mathfrak{p}}$ (порождающему поле $\Sigma_{\mathfrak{p}}$ над Σ_P).)

г) Имеет место изоморфизм

$$G_{\mathfrak{p}}\simeq D_{\mathfrak{p}}/I_{\mathfrak{p}}.$$

д) Справедливы соотношения

$$(G:1)=[E:F]_s=r(D_{\mathfrak{p}}:1),$$

$$(D_{\mathfrak{p}}:I_{\mathfrak{p}})=[\Sigma_{\mathfrak{p}}:\Sigma_P]_s=f_{\mathfrak{p},s},$$

$$[E:F]=re_{\mathfrak{p}}f_{\mathfrak{p}},$$

$$(D_{\mathfrak{p}}:1)=\frac{e_{\mathfrak{p}}f_{\mathfrak{p}}}{[E:F]_n},$$

$$(I_{\mathfrak{p}}:1)=\frac{e_{\mathfrak{p}}f_{\mathfrak{p},n}}{[E:F]_n}.$$

5*. Пусть E/L — конечное расширение поля алгебраических функций от одной переменной F/K,

$$A=\sum_P v_P(A)\cdot P$$

— произвольный дивизор поля F и $e_{\mathfrak{p}}$ — индекс ветвления простого

дивизора $\mathfrak{p}$ поля E, лежащего над P. Дивизор

$$\mathrm{con}_{F/E}A = \sum_{\mathfrak{p}} v_P(A)\, e_{\mathfrak{p}} \cdot \mathfrak{p}$$

поля E называется *конормой дивизора* A. Положим

$$d(A) = \deg_E(A) = \deg(\mathrm{con}_{F/E}A).$$

Пусть E' — наименьшее нормальное расширение поля F, содержащее E, и L' — алгебраическое замыкание поля L в E'. Тогда E'/L' — поле алгебраических функций с полем констант L'. Пусть G' — группа Галуа поля E' над F и H' — ее подгруппа, оставляющая неподвижным поле E. Пусть G'/H' — множество левых классов смежности группы G' по подгруппе H'. Если

$$\mathfrak{a} = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{a}) \cdot \mathfrak{p}$$

— произвольный дивизор поля E, то дивизор

$$\mathrm{norm}_{E/F}\mathfrak{a} = [E\colon F]_n \sum_{\bar{\sigma}' \in G'/H'} \sigma'\mathfrak{a}$$

поля F называется *нормой дивизора* $\mathfrak{a}$ (легко видеть, что это определение не зависит от выбора представителя $\sigma' \in G'$ класса $\bar{\sigma}'$).

Установить справедливость следующих утверждений:

а) Отображение

$$\mathrm{con}\colon \mathrm{Div}(F) \to \mathrm{Div}(E),$$

ставящее в соответствие каждому дивизору $A \in \mathrm{Div}(F)$ дивизор $\mathrm{con}_{F/E}A$, является вложением группы $\mathrm{Div}(F)$ в группу $\mathrm{Div}(E)$ и задает гомоморфизм группы $\mathrm{Cl}(F)$ в группу $\mathrm{Cl}(E)$.

б) Для каждого дивизора A поля F справедливо соотношение

$$d(A) = \frac{[E\colon F]}{[L\colon K]} \deg A.$$

(Указание. Доказать сначала, что для любых двух простых дивизоров P и Q поля F выполняется соотношение

$$\frac{d(P)}{\deg P} = \frac{d(Q)}{\deg Q}.$$

Для этого предположить, что

$$\frac{d(P)}{\deg P} < \frac{d(Q)}{\deg Q}$$

и выбрать затем положительные целые m, n и t таким образом, чтобы выполнялись неравенства

$$d(P)/\deg P < m/n < d(Q)/\deg Q,$$
$$\deg(ntP - mtQ) > 2g - 1$$

и

$$d(ntP - mtQ) < 0,$$

где g — род поля F. Воспользовавшись теоремой Римана — Роха вывести отсюда, что существует такой главный дивизор $[x]$ поля F, для которого $d([x]) > 0$, и прийти к противоречию.

Используя полученный результат, установить, что

$$d(A) = \lambda \deg A$$

для всякого дивизора $A \in \mathrm{Div}(F)$, и затем, воспользовавшись результатом п. е) задачи 2, показать, что $\lambda = [E:F]/[L:K]$.)

в) Сопоставление $\mathfrak{a} \mapsto \mathrm{norm}_{E/F}\mathfrak{a}$ задает гомоморфизм

$$\mathrm{norm}\colon \mathrm{Div}(E) \to \mathrm{Div}(F)$$

группы $\mathrm{Div}(E)$ в группу $\mathrm{Div}(F)$.

г) Если $\mathfrak{p}$ — простой дивизор поля E, лежащий над простым дивизором P поля F, то

$$\mathrm{norm}_{E/F}\mathfrak{p} = f_{\mathfrak{p}} \cdot P.$$

д) Если $x \in E$, то

$$\mathrm{norm}_{E/F}(x) = [\mathrm{norm}_{E/F}x].$$

е) Если $A \in \mathrm{Div}(F)$, то

$$\mathrm{norm}_{E/F}A = [E:F] \cdot A.$$

6*. Доказать справедливость следующих утверждений:

а) Если E/L — чисто несепарабельное алгебраическое расширение поля F/K характеристики $p > 0$, то имеется ровно один простой дивизор $\mathfrak{p}$ поля E, лежащий над данным простым дивизором P поля F, и $P = p^n\mathfrak{p}$ при некотором неотрицательном целом n.

б) Если E/L — поле алгебраических функций, сепарабельное над F/K и такое, что $E = FL$, то в поле E нет разветвленных или несепарабельных над F простых дивизоров.

(Указание. Пусть $\mathfrak{p}$ — разветвленный (несепарабельный) над F простой дивизор поля E. Найти такой элемент $x \in E$, для которого $v_{\mathfrak{p}}(x) = 1$, и показать, что x лежит в некотором нормальном расширении $E' = F(\theta_1, \ldots, \theta_m)$ поля F, где $\theta_i \in L$. Пусть $\mathfrak{p}'$ — простой дивизор поля $E' \subset E$, над которым лежит $\mathfrak{p}$. Показать, что $\mathfrak{p}'$ разветвлен (несепарабелен) над F и что существует нетривиальный автоморфизм $\sigma \in I_{\mathfrak{p}'}$ поля E' над F, для которого

$$v_{\mathfrak{p}'}(\theta_i - \sigma\theta_i) > 0$$

при всех $i = 1, 2, \ldots, m$. Вывести отсюда, что $\theta_i = \sigma\theta_i$ и прийти к противоречию.)

в) Если E/L — сепарабельное алгебраическое расширение поля F/K, то имеется лишь конечное число простых дивизоров поля E, разветвленных или несепарабельных над F.

(Указание. Доказать утверждение сначала для конечных расширений поля F/K, затем для конечных сепарабельных расширений и, наконец, для общего случая.

Пусть $\mathfrak{p}$ — разветвленный или несепарабельный над F простой дивизор конечного расширения Галуа E поля F. Рассмотреть примитивный элемент x поля E над F и автоморфизм $\sigma \in I_{\mathfrak{p}}$ такой, что $\sigma x \neq x$. Показать, что либо $v_{\mathfrak{p}}(x - \sigma x) > 0$, либо $v_{\mathfrak{p}}(x^{-1} - (\sigma x)^{-1}) > 0$, и что имеется лишь конечное число простых дивизоров $\mathfrak{p}$ поля E, для которых выполняется каждое из указанных неравенств. Для случая конечного сепарабельного расширения E поля F рассмотреть наименьшее нормальное расширение поля F, содержащее E.

В общем случае воспользоваться тем, что поле E/L является конечным сепарабельным расширением композита FL, и затем результатом п. б).)

7* (Дойринг [46b, §36]). Пусть K' — расширение поля констант K поля алгебраических функций F и FK' — композит полей F и K'.

Установить справедливость следующих утверждений:

а) Существует единственное с точностью до F-изоморфизма поле алгебраических функций E/L, являющееся расширением поля F/K и обладающее свойствами:

1) поле K' K-изоморфно некоторому подполю L' поля L;

2) $E = FL'$.

(Указание. Пусть $\{x_i\}$ — базис трансцендентности поля K' над K, $\{y_i\}$ — множество алгебраически независимых элементов над F, находящихся во взаимно однозначном соответствии с элементами x_i и Ω — алгебраическое замыкание поля $F(\{y_i\})$. Показать, что изоморфизм $\lambda\colon K(x_i) \to K(y_i)$, тривиальный на K, может быть расширен до изоморфизма поля K' на некоторое подполе L' поля Ω, и что Ω содержит композит $E = FL'$ полей F и L'.

Пусть L — алгебраическое замыкание поля L' в E и x — трансцендентный над K элемент поля F. Показать, что x трансцендентен над L', и вывести отсюда, что $[E : L'(x)] \leqslant [F : K(x)] < \infty$ и $[L : L'] < \infty$.

Для доказательства того факта, что поле E/L определяется свойствами 1) и 2) однозначно с точностью до F-изоморфизма, показать сначала, что достаточно ограничиться рассмотрением случая, когда L' — конечно порожденное расширение поля K.

Пусть $L' = K(z_1, \ldots, z_m)$ — чисто трансцендентное расширение поля K. Показать, что в этом случае требуемый F-изоморфизм определяется заданием образов элементов $z_1, \ldots, z_m$. Для этого воспользоваться следующим результатом: *если поле A алгебраически замкнуто в поле B и если элементы $z_1, \ldots, z_m$ алгебраически независимы над B, то поле $A(z_1, \ldots, z_m)$ алгебраически замкнуто в $B(z_1, \ldots, z_m)$*. Вывести отсюда, что $L = K(z_1, \ldots, z_m)$.

Пусть $L' = K(\theta_1, \ldots, \theta_m)$ — конечное расширение поля K. В этом случае доказательство единственности поля E/L с точностью до F-изоморфизма провести индукцией по числу $m \geqslant 0$ порождающих элементов $\theta_1, \ldots, \theta_m$ поля L').

б) Поле констант L построенного в пункте а) расширения E/L поля F/K является чисто несепарабельным конечным расширением поля L'.

(Указание. Воспользоваться рассуждениями предыдущего пункта. В случае, когда L' — чисто трансцендентное расширение поля K, утверждение очевидно. В случае, когда $L' = K(\theta_1, \ldots, \theta_m)$ — конечное расширение поля K, воспользоваться индукцией по числу $m \geqslant 0$ порождающих элементов $\theta_1, \ldots, \theta_m$ поля L'.)

в) Существует поле алгебраических функций F/K и расширение K' поля K, для которых поле констант L композита FL' отлично от L'.

(Указание. Рассмотреть поле k характеристики $p > 0$, поле $K = k(u, v)$, где u, v — алгебраически независимые над k элементы и поле $F = K(x, y)$, где x, y удовлетворяют уравнению $y^p = ux^p + v$. Установить, что K является полем констант для F. Взять затем $L' = K(v^{1/p})$ и показать, что поле $E = FL'$ содержит элемент $(y - v^{1/p})x^{-1} = u^{1/p}$. Вывести отсюда, что $L = K(u^{1/p}, v^{1/p})$ и что $[L : L'] = p$.)

8*. Пусть B и C — расширения поля A. Назовем поля B и C *линейно (алгебраически) разделенными* над A, если всякое конечное множество элементов из B, линейно (алгебраически) независимых над A, линейно (алгебраически) независимы и над C.

Доказать справедливость следующих утверждений.

а) Если A, B, C — подполя некоторого поля и C — конечное расширение степени n поля A, то композит BC является алгебраическим расширением поля B степени не выше n. Если же поля B и C линейно разделены над A, то $[BC : B] = n$.

б) Если поля B и C линейно разделены над A, то они алгебраически разделены над A.

в) Если B — чисто трансцендентное расширение поля A и поля B, C алгебраически разделены над A, то B и C линейно разделены над A.

г) Если A алгебраически замкнуто в поле B и $C = A(\alpha)$ — алгебраическое расширение поля A, то поля B и C линейно разделены над A.

д) Если $A \subset C \subset D$ и $B \supset A$ — подполя некоторого поля, то B и D линейно разделены над A тогда и только тогда, когда B, C линейно разделены над A и BC, D линейно разделены над C.

е) Пусть K' — расширение поля K и $E = E/L = FL'$ — соответствующее ему расширение поля алгебраических функций F/K. Пусть, далее, L'' — произвольное подполе поля L' и L_0 — поле констант расширения $E' = FL''$. Тогда, если поля F и L линейно разделены над K, то для любого трансцендентного над K элемента $x \in F$ имеет место равенство

$$[E' : L_0(x)] = [F : K(x)].$$

(Указание. Воспользоваться результатами п. а), в) и д).)

ж) В обозначениях предыдущего пункта следующие предложения эквивалентны между собой:

1) поля F и L линейно разделены над K;

2) для каждого конечно порожденного над K подполя L'' поля L' поле констант L_0 поля $E' = FL''$ совпадает с L''.

(Указание. Воспользоваться результатом предыдущего пункта.)

з) Если в обозначениях п. е) поля F и L линейно разделены над K, то для каждого подполя L'' поля L' поле констант L_0 поля $E' = FL''$ совпадает с L''.

и) Если в обозначениях п. е) хотя бы одно из полей F или L'' *сепарабельно порождено* над K (является сепарабельным алгебраическим расширением чисто трансцендентного расширения $K(x_1, \ldots, x_m)$ поля K), то $L = L'$.

(Указание. Ввиду результатов предыдущего пункта и предыдущей задачи можно считать, что L' — конечное расширение поля K. Показать, что в этом случае L является сепарабельным расширением поля L', и сравнить полученный результат с результатом предыдущей задачи о том, что поле L чисто несепарабельно над L'.)

9*. Пусть K' — расширение поля K и $E = E/L = FL'$ — соответствующее ему расширение поля алгебраических функций F/K.

Установить справедливость следующих утверждений:

а) Если рациональное число λ таково, что

$$d(A) = \lambda \deg A$$

для всех $A \in \mathrm{Div}\,(F)$, то

$$\lambda^{-1} = \begin{cases} p^\tau, \ \tau \in \mathbb{Z}, \ \tau \geqslant 0, & \text{если } \operatorname{char} K = p > 0, \\ 1, & \text{если } \operatorname{char} K = 0. \end{cases}$$

Равенство $\lambda = 1$ имеет место тогда и только тогда, когда поля F и L линейно разделены над K.

(Указание. Пусть x — трансцендентный над K элемент поля F и A — знаменатель главного дивизора $[x]$. Используя равенства $\deg A = [F : K(x)]$ и $d(A) = [E : L(x)]$, показать, что $\lambda = 1 \Leftrightarrow d(A) = \deg A \Leftrightarrow [E : L(x)] = [F : K(x)]$. Показать, далее, что $[E : L(x)] = [F : K(x)]$ в том и только в том случае, если поля F и L линейно разделены над K.

В случае характеристики $p = 0$ воспользоваться сепарабельностью F над K и результатом п. д) предыдущей задачи.

В случае характеристики $p > 0$ рассмотреть наибольшее сепарабельное расширение $\widetilde{F}_s$ поля $K(x)$, содержащееся в F, и поле $\widetilde{E}_s = \widetilde{F}_s L'$. Поля $\widetilde{F}_s$ и L' линейно разделены над K и тогда

$$[\widetilde{F}_s : K(x)] = [\widetilde{E}_s : L'(x)].$$

Показать, что $F/\widetilde{F}_s$ — чисто несепарабельное расширение степени p^μ, $\mu \geqslant 0$, и что $E = FL'$ — несепарабельное расширение степени p^ν, $0 \leqslant \nu \leqslant \mu$, поля $\widetilde{E}_s = \widetilde{F}_s L'$. Вывести отсюда, что

$$\lambda^{-1} = p^{\mu-\nu}[L : L']$$

и воспользоваться тем, что L — чисто несепарабельное расширение поля L'.)

б) Если $E = FL'$, где L' — сепарабельно порожденное расширение поля констант K поля алгебраических функций F/K, и если $\mathfrak{p}$ — простой дивизор поля E, лежащий над простым дивизором P поля F, то $\Sigma_{\mathfrak{p}} = \Sigma_P L'$.

(Указание. Рассмотреть вначале случаи, когда L' — чисто трансцендентное расширение и когда L' — конечное расширение поля K.)

10* (Дойринг [46b, § 38]). Пусть K' — расширение поля K и $E/L = FL'$ — соответствующее ему расширение поля алгебраических функций F/K. Обозначим g_F род поля F и g_E — род поля E. Пусть A — некоторый дивизор поля F и

$$F(A) = \{x \in F \mid x \equiv 0 \pmod{A}\}$$

линейное векторное пространство над K. Аналогичным образом определим линейное векторное пространство $E(A)$ над L и положим

$$l_F(A) = \dim_K F(A), \quad l_E(A) = \dim_L E(A).$$

Доказать справедливость следующих утверждений:

а) Если поля F и L линейно разделены над K, то $g_E \leqslant g_F$ и для каждого дивизора A поля F имеет место неравенство

$$l_F(A) \leqslant l_E(A).$$

(Указание. Второе утверждение следует из включения $F(A) \subset E(A)$. Для доказательства первого утверждения рассмотреть дивизор $-A$, для которого $d(-A) > 2g_E - 2$, $\deg(-A) > 2g_F - 2$ и воспользоваться теоремой Римана — Роха.)

б) Если поле L' сепарабельно порождено над K, то $g_E = g_F$ и для любого дивизора $A \in \mathrm{Div}(F)$ базис пространства $F(A)$ является также базисом пространства $E(A)$.

(Указание. Рассмотреть сначала случай чисто трансцендентного расширения $L = L' = K(x)$ поля K и показать, что в этом случае каждый элемент $y \in E(A)$ представляется в виде многочлена от x с коэффициентами из $F(A)$. Используя линейную разделенность полей F и L, вывести отсюда, что $l_E(A) = l_F(A)$.

В случае когда $L = L' = K(\alpha)$ — конечное сепарабельное расширение поля K, показать, что каждый элемент $y \in E(A)$ можно представить в виде

$$y = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}, \quad a_i \in F,$$

где n — степень α над K или над F. Затем рассмотреть наименьшее нормальное расширение поля E над K и доказать, что $a_i \in F(A)$. Вывести отсюда, что $l_E(A) = l_F(A)$.

Наконец, выбрав дивизор $-A$ таким, что $d(-A) > 2g_E - 2$ и $\deg(-A) > 2g_F - 2$, установить справедливость равенства $g_E = g_F$.)

11*. Пусть $F = K(t)$ — поле алгебраических функций рода $g = 0$ и $P_1, \ldots, P_r$ — все исключительные простые дивизоры этого поля. Назовем элемент $x \in F \subset {}^*K$ *исключительным*, если его знаменатель не содержит нестандартные простые дивизоры поля $^*K$. Исключительные элементы образуют подкольцо R поля F, содержащее поле K. Согласно теореме 4 степень дивизора

$$A = P_1 + \ldots + P_r$$

не превосходит 2.

Доказать справедливость следующих утверждений:

а) если $\deg A = 0$, то $R = K$;

б) если $\deg A = 1$, то можно выбрать порождающий элемент t поля F/K таким образом, что $R = K[t]$;

в) если $\deg A = 2$ и $r = 2$, то порождающий элемент t поля F/K можно выбрать таким образом, что $R = K[t, t^{-1}]$;

г) если $\deg A = 2$ и $r = 1$, то порождающий элемент t поля F/K можно выбрать таким образом, что $R = K[f^{-1}, tf^{-1}]$, где $f(t) = t^2 - a$ — неприводимый в кольце $K[t]$ многочлен. Далее, если $K' = K(\sqrt{a})$ — квадратичное расширение поля K и σ: $\sqrt{a} \mapsto -\sqrt{a}$ — нетривиальный автоморфизм поля K' над K, то кольцо R совпадает с неподвижным относительно σ подкольцом кольца $R' = K'[t', t'^{-1}]$, где

$$t' = \frac{t + \sqrt{a}}{t - \sqrt{a}};$$

д) каждый из случаев а) — г) реализуется на некотором подполе F рода $g = 0$ поля $^*K$.

(Указание. Достаточно в каждом из указанных случаев построить подходящий элемент t поля $F = K(t)$.

Пусть u — отличный от нуля элемент поля K, не являющийся корнем из 1, и $t_2 = u^v$, где v — бесконечно большой элемент из $^*\mathbb{N}$. Показать, что t_2 — нестандартный элемент и что случай в) реализуется на поле $F_2 = K(t_2)$. Пусть, далее,

$$t_1 = t_2 + t_2^{-1} \quad \text{и} \quad t_0 = t_1 + t_1^{-1}.$$

Показать, что случаи а) и б) реализуются на полях $F_0 = K(t_0)$ и $F_1 = K(t_1)$ соответственно. Пусть, наконец,

$$u' = \frac{u + \sqrt{a}}{u - \sqrt{a}}$$

— отличный от нуля элемент поля $K' = K(\sqrt{a})$, не являющийся корнем из 1; σ — нетривиальный автоморфизм поля K' над K и $^*\sigma$ — его продолжение на поле $^*K'$ над $^*K$, так что, если $t_2' = u'^v$, то $^*\sigma t_2' = t_2'^{-1}$. Показать, что

$$t_3 = \sqrt{a}\,\frac{t_2' + 1}{t_2' - 1}$$

является элементом поля $^*K$ и что случай г) реализуется на поле $F_3 = K(t_3)$.)

12. Пусть X — кривая рода $g = 0$, определенная над полем K уравнением $f(x, y) = 0$. Предположим, что кривая X *исключительна* в том смысле, что для нее не выполняется утверждение теоремы Зигеля — Малера. Тогда на X имеется нестандартная точка (x, y) с квазицелыми в $^*K$ координатами относительно конечного множества S простых дивизоров поля K. Стало быть, x и y являются исключительными элементами поля $F = K(x, y) \subset {}^*K$.

Используя результаты предыдущей задачи, дать следующую *классификацию Зигеля* исключительных кривых рода 0:

а) если $\deg A = 1$, то $x = \eta(t)$, $y = \theta(t)$, где η, θ — многочлены из кольца $K[t]$;

б) если $\deg A = 2$ и $r = 2$, то $x = \eta(t)$, $y = \theta(t)$, где η, θ — конечные ряды Лорана с коэффициентами из K;

в) если $\deg A = 2$ и $r = 1$, то $x = \eta(t')$, $y = \theta(t')$, где η, θ — конечные ряды Лорана с коэффициентами из поля $K' = K\sqrt{a}$, удовлетворяющие условиям $\eta(t') = {}^{\sigma}\eta(t'^{-1})$, $\theta(t') = {}^{\sigma}\theta(t'^{-1})$. Здесь σ — нетривиальный автоморфизм поля K' над K и ${}^{\sigma}\eta$, ${}^{\sigma}\theta$ — конечные ряды Лорана, получающиеся из η, θ применением σ к их коэффициентам;

г) указанная в п. а) — в) параметризация не только необходима, но и достаточна для того, чтобы кривая X была исключительной.

§ 2. Доказательство теоремы Зигеля — Малера

1. Гиперэллиптический случай. Пусть A — исключительный дивизор поля F. Покажем, что если род g поля F положителен, то $A = 0$. Для этого, применяя теорему 4 из § 1 к подходящему неразветвленному расширению поля F в $^*K$, усилим полученное нами неравенство

$$\deg A \leqslant 2d \leqslant 2g + 2$$

и докажем, что

$$\deg A < 1.$$

Пусть E — такое расширение поля F, что

$$K \subset F \subset E \subset {}^*K.$$

Предположим, что степень $[E : F]$ поля E над F конечна. Тогда E — поле алгебраических функций от одной переменной с полем констант K.

Лемма 1. *Функциональный простой дивизор P поля F исключителен в том и только в том случае, если таковым является каждый функциональный простой дивизор Q поля E, лежащий над P.*

Доказательство. Пусть P исключительный простой дивизор поля F. По определению он индуцирован некоторым стандартным простым дивизором $\mathfrak{p} \in {}^*V$. Если Q — простой дивизор поля E, лежащий над P, то всякий простой дивизор $\mathfrak{p} \in {}^*V$, индуцирующий Q, индуцирует также и P. Следовательно, $\mathfrak{p}$ — стандартный дивизор и, значит, Q — исключительный простой дивизор поля E.

Обратно, пусть каждый простой дивизор поля E, лежащий над P, исключителен. Всякий простой дивизор $\mathfrak{p} \in {}^*V$, индуцирующий P, индуцирует также и некоторый простой дивизор Q поля E, лежащий над P. Следовательно, $\mathfrak{p}$ — стандартный простой дивизор и, значит, P — исключительный дивизор поля F. Лемма доказана.

Пусть $Q_1, \ldots, Q_s$ — все функциональные простые дивизоры поля E, лежащие над исключительными простыми дивизорами $P_1, \ldots, P_r$, являющимися компонентами дивизора

$$A = P_1 + \ldots + P_r.$$

Из леммы 1 следует, что каждый простой дивизор Q_i является исключительным. Если A рассматривается как дивизор поля E, то он имеет вид

$$A = e_1 Q_1 + \ldots + e_s Q_s,$$

где e_i — индекс ветвления простого дивизора Q_i над полем F.

Предположим теперь, что E — неразветвленное расширение поля F. Тогда $A = Q_1 + \ldots + Q_s$ и, значит, A является исключительным дивизором поля E. Другими словами, дивизор A остается исключительным в неразветвленном расширении E поля F. В таком случае, если $\deg_E A$ — степень дивизора $A \in \mathrm{Div}(E)$ и

$$d_E = \min_{\substack{x \in E \\ x \notin K}} [E\colon K(x)]$$

— минимальная степень поля E, то в соответствии с теоремой 4 из § 1

$$\deg_E A \leqslant 2d_E.$$

Кроме того, имеет место (см. задачу 5 предыдущего параграфа) соотношение

$$\deg_E A = [E : F] \deg_F A$$

и, в результате, приходим к следующему утверждению.

Следствие. *Пусть E — неразветвленное расширение поля F. Тогда каждый исключительный дивизор A поля F остается исключительным в поле E и для степени $\deg A$ дивизора $A \in \mathrm{Div}(F)$ имеет место оценка*

$$\deg A \leqslant \frac{2d_E}{[E\colon F]}.$$

Отсюда выводим, что если только

$$[E : F] > 2d_E, \tag{1}$$

то $\deg A = 0$ и, следовательно, $A = 0$.

Таким образом, задача свелась к построению неразветвленных расширений E поля F в $^*K$ достаточно высокой степени $[E : F]$. Такое построение вполне элементарно в случае $d_F = 2$, т. е. в случае, когда поле F является квадратичным расширением поля рациональных функций $K(x)$. Остановимся здесь на рассмотрении именно этого частного случая. Общий случай будет разобран ниже.

Сделаем предварительно несколько замечаний. Если K' — конечное расширение поля K, то поле $F' = FK'$ является подполем нестандартного расширения $^*K' = {}^*K K'$. Таким образом, имеется цепочка вложений

$$K' \subset F' \subset {}^*K'.$$

Исключительный дивизор

$$A = P_1 + \ldots + P_r$$

поля F остается исключительным в поле F' и степень дивизора $A \in \mathrm{Div}(F)$ не изменяется при его рассмотрении как элемента группы $\mathrm{Div}(F')$. Кроме того, поля F и F' имеют (см. задачу 10 предыдущего параграфа) один и тот же род g. Из этих замечаний следует, что, чтобы установить отсутствие исключительных дивизоров в группе $\mathrm{Div}(F)$, достаточно установить их отсутствие в группе $\mathrm{Div}(F')$. Поэтому в дальнейшем вместо поля F можно использовать поле $F' = FK'$, полученное из исходного поля F расширением его поля констант K.

Пусть F — квадратичное расширение поля $K(x)$. Тогда существует такой порождающий элемент y поля F над $K(x)$, что $y^2 = f(x)$, где $f \in K[x]$ — многочлен без кратных корней. Если степень многочлена f равна m, то род g поля F вычисляется (см. задачу 12 из § 3 гл. IV) по формулам

$$g = \begin{cases} (m-1)/2, & \text{если } m = 2k-1, \\ (m-2)/2, & \text{если } m = 2k. \end{cases}$$

Поскольку по предположению $g > 0$, то $m \geqslant 3$. При $m = 3$ или $m = 4$ мы имеем дело с эллиптическим, а при $m \geqslant 5$ с гиперэллиптическим полем F.

Расширяя, в случае необходимости, поле констант K поля F, можем считать, что многочлен $f(x)$ имеет в поле K по меньшей мере два корня a и b, так что

$$f(x) = (x-a)(x-b)g(x),$$

где $g(x)$ — многочлен из кольца $K[x]$ степени $m-2$. Пусть P_a — функциональный простой дивизор, в котором $x-a$ имеет ноль. Тогда из уравнения

$$y^2 = (x-a)(x-b)g(x)$$

следует, что P_a является двойным нулем элемента $x-a$ $\left(v_{P_a}(x-a) = 2\right)$ и что в поле F элемент $x-a$ не имеет других нулей. Другими словами, простой дивизор P_a разветвлен над полем $K(x)$. Отсюда следует, что главный дивизор элемента $x-a$ имеет вид

$$[x-a] = 2P_a - P_\infty,$$

где P_∞ — полюс элемента x. Аналогичным образом

$$[x-b] = 2P_b - P_\infty,$$

причем, поскольку $a \neq b$, то $P_a \neq P_b$. Следовательно, элемент

$$z = \frac{x-a}{x-b} \tag{2}$$

имеет главный дивизор

$$[z] = 2P_a - 2P_b, \tag{3}$$

делящийся на 2.

Лемма 2. *Существует такая ненулевая константа $c \in K$, для которой $\sqrt{cz} \in {}^*K$.*

Доказательство. Рассмотрим P_a и P_b как дивизоры группы $\mathfrak{D}$. Тогда $(z) \overset{\circ}{=} 2P_a - 2P_b$. Так как отображение $\sigma\colon \mathrm{Div}(F) \to \mathbb{R}$ равно нулю на главных дивизорах, получаем, что $0 \overset{\circ}{=} \sigma(2P_a - 2P_b) \overset{\circ}{=} 2\sigma(P_a - P_b)$. Далее, поскольку группа $\mathbb{R}$ вполне упорядочена, то она не имеет кручения и, следовательно,

$$\sigma(P_a - P_b) \overset{\circ}{=} 0.$$

Таким образом, дивизор $P_a - P_b$ группы $\mathfrak{D}$ имеет нулевой размер, и тогда из теоремы 2 из § 3 гл. VI следует, что он является главным дивизором этой группы. Это означает, что существует такой элемент $t \in {}^*K$, что $(t) \overset{\circ}{=} P_a - P_b$. В таком случае

$$(t^2) = 2(t) \overset{\circ}{=} 2P_a - 2P_b \overset{\circ}{=} (z)$$

и, стало быть, ввиду той же теоремы 2, $t^2 = cz$ для некоторого элемента $c \in K$. Лемма доказана.

Из соотношения (2) следует, что $K(x) = K(z) = K(cz)$. Отсюда, учитывая, что $t = \sqrt{cz}$, получаем

$$K(x) \subset K(t) \quad \text{и} \quad [K(t) : K(x)] = 2.$$

С другой стороны, $[F : K(x)] = 2$. Если допустим, что $t \in F$, то получим равенство $F = K(t)$ и придем в противоречие с предположением о том, что род g поля F больше нуля. Следовательно, t — квадратичная иррациональность над F и, если положить $E = F(t)$, то $[E : F] = 2$. Тем самым нами построено некоторое квадратичное расширение $E \subset {}^*K$ поля F. Покажем, что оно не разветвлено над F. В самом деле, поле E порождено над F элементом $t = \sqrt{cz}$ и, в таком случае, каждый простой дивизор поля F, который разветвляется в E, входит в главный дивизор $[cz] = [z]$ с нечетной кратностью. Но из равенства (3) видно, что всякий простой дивизор, входящий в $[z]$, имеет кратность 2 и, значит, каждый простой дивизор поля F не разветвлен в E.

В построении неразветвленного расширения E поля F мы использовали то обстоятельство, что F квадратичное расширение поля $K(x)$. Точно такая же ситуация возникает и для поля E. Действительно, $E = F(t) = K(x, y, t) = K(y, t)$ и $y^2 \in K(x) \subset K(t)$. Следовательно, E представляет собой квадратичное расширение поля $K(t)$ и можно применить ту же конструкцию к полю E.

Итерируя указанный процесс, на n-м шаге получаем неразветвленное расширение $E_n \subset {}^*K$ поля F такое, что

$$[E_n\colon F] = 2^n \quad \text{и} \quad d_{E_n} = 2.$$

При $n = 3$ приходим к справедливости неравенства (1) и, тем самым, к справедливости утверждения о том, что группа $\mathrm{Div}(F)$ не содержит исключительных простых дивизоров. Отсюда заключаем, что теорема B справедлива для эллиптических и гиперэллиптических полей.

2. Общий случай кривых рода $g \geqslant 1$. Перейдем к рассмотрению общего случая поля алгебраических функций F рода $g > 0$. Как и в п. 1, нашей целью будет построение неразветвленного расширения $E \subset {}^*K$ поля F достаточно высокой степени $[E : F]$.

Пусть n — стандартное положительное целое число. Основой для дальнейших конструкций служит следующий результат.

Лемма 3. *Пусть T — такой функциональный дивизор поля F, для которого nT — главный дивизор этого поля. Тогда существует элемент $t \in {}^*K$ такой, что $T \overset{\circ}{=} (t)$ и $t^n \in F$. Расширение $F(t)$ не разветвлено над полем F.*

Доказательство. По условию леммы существует элемент $u \in F$ такой, что $nT = [u]$. Рассмотрим дивизор T как элемент группы $\mathfrak{D}$. Тогда $nT \overset{\circ}{=} (u)$, и поскольку отображение $\sigma\colon \mathfrak{D} \to \mathbb{R}$ равно нулю на главных дивизорах, то для размера $\sigma(nT)$ дивизора nT выполняется соотношение $\sigma(nT) = n\sigma(T) \overset{\circ}{=} 0$. Отсюда, ввиду того, что группа $\mathbb{R}$ не имеет кручения, получаем соотношение $\sigma(T) \overset{\circ}{=} 0$. Из теоремы 2 из § 3 гл. VI следует, что всякий дивизор группы $\mathfrak{D}$, имеющий нулевой размер, является главным дивизором. В таком случае $T \overset{\circ}{=} (t)$ для некоторого $t \in {}^*K$ и, значит, $(u) \overset{\circ}{=} nT = (t^n)$. Отсюда заключаем, что $t^n = cu$ при некотором $c \in K$. Следовательно, t является корнем n-й степени над полем F.

Если функциональный простой дивизор P поля F не содержится в главном дивизоре $[u] = [cu]$, то P не разветвлен в поле $E = F(t)$. Это следует из того факта, что многочлен $z^n - cu$, корнем которого является элемент t, имеет дискриминант $\pm n(cu)^{n-1}$, не делящийся на P. С другой стороны, если P содержится в $[u]$, то имеет место равенство $v_P(u) = nv_P(T)$. В таком случае, если x — элемент поля F, для которого $v_P(x) = v_P(T)$, и если $u' = ux^{-n}$, то P не входит в главный дивизор $[u']$. Кроме того, элемент $t' = tx^{-1}$ порождает поле E над F и удовлетворяет соотношению $t'^n = cu'$. Поэтому, если мы заменим в предыдущих рассуждениях t на t' и u на u', то получим, что P не разветвлен в E. Стало быть, E — неразветвленное расширение поля F и лемма, тем самым, доказана.

Для каждого стандартного целого $n \geqslant 1$ обозначим $\mathrm{Cl}_n(F)$ ядро отображения

$$\mathrm{Cl}(F) \to n\,\mathrm{Cl}(F)$$

и назовем $\mathrm{Cl}_n(F)$ *группой классов дивизоров порядка n*. Заметим, что в условиях предыдущей леммы дивизор T является представителем некоторого класса из $\mathrm{Cl}_n(F)$. Рассмотрим все корни n-й степени $t \in {}^*K$ такие, что $(t) \overset{\circ}{=} T$ для некоторого функционального дивизора $T \in \mathrm{Div}(F)$, представляющего некоторый класс группы $\mathrm{Cl}_n(F)$. Ясно, что такие элементы t образуют мультипликативную группу W_n, содержащую все ненулевые элементы поля F. Если мы сопоставим каждому элементу $t \in W_n$ класс соответствующего ему дивизора $T \in \mathrm{Div}(F)$, то получим гомоморфизм

$$W_n \to \mathrm{Cl}_n(F),$$

который, ввиду леммы 3, сюръективен. Ядром этого гомоморфизма является мультипликативная группа F^* поля F и, следовательно, имеет место изоморфизм

$$W_n/F^* \simeq \mathrm{Cl}_n(F).$$

Поле $F(W_n)$ является неразветвленным расширением поля F, так как оно порождается неразветвленными расширениями $F(t)$, $t \in W_n$. Если поле K содержит все корни n-й степени из 1, то из теории Куммера (см. [70d, гл. VIII, § 8]) следует, что поле $F(W_n)$, порожденное корнями n-й степени, является абелевым расширением показателя n поля F. Кроме того, из той же теории следует, что степень $[F(W_n) : F]$ равна порядку факторгруппы W_n/F^*. Отсюда, ввиду конечности группы $\mathrm{Cl}_n(F)$, получаем соотношение

$$[F(W_n) : F] = |\mathrm{Cl}_n(F)|,$$

где $|\mathrm{Cl}_n(F)|$ — порядок группы $\mathrm{Cl}_n(F)$.

Предполагая снова, что K содержат все корни n-й степени из 1, покажем, что поле $F(W_n) \subset {}^*K$ является максимальным неразветвленным абелевым расширением показателя n поля F. Согласно теории Куммера, каждое такое расширение порождается корнями n-й степени. Следовательно, достаточно показать, что всякий корень n-й степени из произвольного элемента u поля F содержится в W_n.

Пусть $t \in {}^*K$ — корень n-й степени над F и пусть поле $F(t)$ не разветвлено над F. Положим $t^n = u \in F$. Так как $F(t)$ — неразветвленное расширение поля F, то имеем, что $v_P(u) \equiv 0 \pmod n$ для каждого функционального простого дивизора P поля F. Следовательно, главный дивизор $[u]$ делится на n в группе

$\mathrm{Div}(F):[u]=nT$ для некоторого $T\in\mathrm{Div}(F)$. Это означает, что T является представителем некоторого класса из группы $\mathrm{Cl}_n(F)$ и что $nT\overset{\circ}{=}(u)\overset{\circ}{=}(t^n)$. В таком случае $T\overset{\circ}{=}(t)$ и, стало быть, $t\in W_n$.

Таким образом, нами установлен следующий результат.

Следствие 1. *Пусть поле K содержит все корни n-й степени из 1. Тогда все корни n-й степени $t\in{}^*K$ над F из леммы 3 порождают в ${}^*K$ максимальное неразветвленное абелево расширение показателя n поля F. Степень этого максимального расширения равна порядку группы* $\mathrm{Cl}_n(F)$.

Пусть K' — алгебраическое расширение поля K и $F'=FK'$ — соответствующее ему расширение поля F. Включение $F\subset F'$ естественным образом индуцирует инъективное отображение

$$\mathrm{Cl}(F)\to\mathrm{Cl}(F').$$

Следовательно, можно рассматривать $\mathrm{Cl}(F)$ как подгруппу группы $\mathrm{Cl}(F')$, и тогда $\mathrm{Cl}_n(F)=\mathrm{Cl}(F)\cap\mathrm{Cl}_n(F')$. Возьмем теперь в качестве K' алгебраическое замыкание поля K. В этом случае имеем (см. задачу 4)

$$|\mathrm{Cl}(F')|=n^{2g}$$

и, стало быть,

$$|\mathrm{Cl}_n(F)|\leqslant n^{2g}.$$

Если выполняется равенство $|\mathrm{Cl}_n(F)|=n^{2g}$, то все классы дивизоров порядка n называются *рациональными* над K. При этом все корни n-й степени из 1 лежат в K. Таким образом, справедлив следующий результат.

Следствие 2. *Пусть все классы дивизоров порядка n поля F рациональны над K. Если E_n — максимальное неразветвленное абелево расширение показателя n поля F в поле ${}^*K$, то*

$$[E_n:F]=n^{2g}.$$

Если K' — конечное расширение поля K и E_n' — его максимальное неразветвленное абелево расширение показателя n в ${}^*K'$, то легко видеть, что $E_n'=E_nK'$.

Чтобы определить E_n в общем случае, без предположения о рациональности классов дивизоров порядка n, введем понятие полуабелева расширения. Пусть E — конечное расширение поля F в ${}^*K$. Оно называется *полуабелевым расширением показателя n* поля F, если существует такое конечное расширение K' поля K, для которого $E'=EK'$ является абелевым расширением показателя n поля $F'=FK'$. Если E не разветвлено над F, то E' не разветвлено над K' и, стало быть, ввиду следствия 1 леммы 3,

$$[E:F]=[E':F']\leqslant|\mathrm{Cl}_n(F')|\leqslant n^{2g}.$$

Последнее соотношение выполняется для всякого расширения E поля F, обладающего свойствами:

1) E содержится в ${}^*K$;

2) E не разветвлено над F;

3) E является полуабелевым расширением показателя n поля F.

Каждое из этих свойств сохраняется при переходе к композиту и поэтому существует максимальное расширение поля F с указанными свойствами. Пусть E_n — такое максимальное расширение. Имеем

$$[E_n:F]\leqslant n^{2g} \tag{4}$$

и, если классы дивизоров порядка n поля F рациональны над K, то это расширение E_n совпадает с расширением E_n из следствия 2 леммы 3. В частности, в этом случае

$$[E_n:F]=n^{2g}.$$

Покажем, что последнее равенство имеет место в общем случае.

Теорема 1. *Пусть E_n — максимальное неразветвленное полуабелево расширение показателя n поля F в ${}^*K$. Тогда*

$$[E_n:F]=n^{2g}.$$

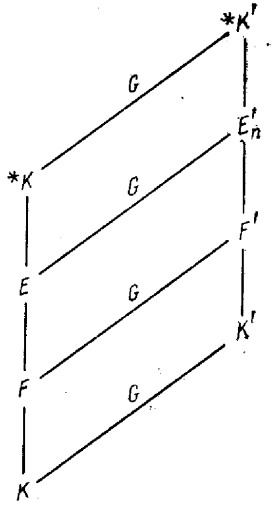


Рис. 4

Доказательство. Пусть K' — такое конечное расширение Галуа поля K, что все классы дивизоров порядка n поля F рациональны над K'. Рассмотрим расширение $F'=FK'$, которое вложено в поле ${}^*K'$, и обозначим E_n' максимальное неразветвленное абелево расширение показателя n поля F' в ${}^*K'$. Имеем $[E_n':F']=n^{2g}$. Кроме того, из определения E_n' следует, что каждый автоморфизм поля ${}^*K'$, отображающий F' на себя, отображает поле E_n' на себя.

Пусть G — группа Галуа поля K' над K. Каждый автоморфизм группы G имеет стандартное расширение на поле ${}^*K'$ и, следовательно, можно рассматривать G как группу Галуа поля ${}^*K'$ над ${}^*K$. Группа G отображает $F'=FK'$ на себя и тогда она отображает E_n' также на себя. Поэтому G индуцирует группу автоморфизмов поля E_n'. Обозначим E неподвижное поле этой группы (подполе поля E_n'). Оно обладает следующими свойствами (см. рис. 4):

1) *E содержится в ${}^*K$.*

В самом деле, так как ${}^*K$ — неподвижное поле группы G в поле ${}^*K'$, то $E={}^*K\cap E_n'$.

2) *E не разветвлено над F.*

Действительно, E_n' — неразветвленное расширение поля F'; F' — неразветвленное расширение поля F и, так как $E \subset E_n'$, то E — неразветвленное расширение поля F.

3) *Справедливо равенство $E_n' = EK'$.*

Справедливость указанного равенства следует из теории Галуа, так как каждый нетривиальный автоморфизм поля K' определяет нетривиальный автоморфизм поля EK'. Поскольку E_n' — абелево расширение показателя n поля F', отсюда следует, что E — полуабелево расширение показателя n поля F.

Из свойств 1)—3) поля E следует, что $E \subset E_n$. В таком случае, ввиду (4)

$$[E:F] \leqslant [E_n:F] \leqslant n^{2g}.$$

С другой стороны, из свойства 3) выводим, что

$$[E\colon F] = [EK'\colon FK'] = \left[E_n'\colon F'\right] = n^{2g}.$$

Отсюда заключаем, что $E_n = E$ и что $[E_n:F] = n^{2g}$. Теорема доказана.

Теорема 1 устанавливает существование в $^*K$ неразветвленного расширения E_n поля F произвольно большой степени n^{2g}. Для доказательства теоремы B необходимо оценить теперь инвариант

$$d_n = d_{E_n} = \min_{\substack{x \in E_n \\ x \notin K}} [E_n\colon K(x)]$$

поля E_n. Положим, как и прежде, $d_F = d$. Справедливо следующее утверждение.

Лемма 4. *Имеет место неравенство*

$$d_n \leqslant g^3 d n^{2g-2}.$$

Доказательство леммы 4, данное Зигелем [54d], основано на аналитической теории тета-функций. Так как эта теория не рассматривается в данной книге, мы изложим доказательство леммы 4 в виде задач (см. ниже задачи 1—4). В доказательстве теоремы Зигеля — Малера, предложенном Ленгом (см. [70h, гл. 8, § 8]) вместо тета-функций использован якобиан кривой X. Алгебраическое доказательство леммы 4, основанное на неравенстве Кастельнуово — Севери и справедливое в любой характеристике p, дано Рокеттом [106b].

Докажем теперь теорему B в общем случае. Из теоремы 1 и из леммы 4 имеем

$$d_n \leqslant \frac{g^3 d}{n^2} [E_n\colon F].$$

Отсюда, взяв n достаточно большим, получаем неравенство

$$d_n < \frac{1}{2} [E_n\colon F],$$

из которого (как было показано выше) следует, что группа $\mathrm{Div}(F)$ не содержит исключительных дивизоров. Теорема B доказана.

Задачи

1*. Пусть R — компактная связная риманова поверхность над расширенной комплексной плоскостью $\overline{\mathbb{C}}$ (см. [114, гл. 1, 5, 10; 128]). Если t — локальный (униформизирующий) параметр точки $P \in R$ и $\omega = \varphi dt$ — дифференциал, определенный в окрестности точки P, то ω называется *голоморфным* или *мероморфным* в точке P соответственно тому будет ли таковой функция $\varphi = \varphi(t)$ для каждого локального параметра t. Дифференциал ω на R называется дифференциалом *первого, второго или третьего* рода в соответствии с тем, будет ли он голоморфным всюду на R, мероморфным на R и имеющим нулевые вычеты в каждом полюсе или же мероморфным на R и имеющим полюса порядка не выше 1.

Доказать справедливость следующих утверждений:

а) Если γ — замкнутая кривая на R и ω — дифференциал первого или второго рода, то значение интеграла $\int_\gamma \omega$ зависит только от класса гомологий кривой γ. Это значение называется *периодом дифференциала* ω относительно γ.

б) Риманова поверхность R гомеоморфна сфере с g ручками при некотором $g \geqslant 0$ и ее первая группа гомологий $H_1(R, \mathbb{Z})$ является абелевой группой с $2g$ образующими.

в) Если ω — мероморфный дифференциал на R, то он имеет лишь конечное число полюсов $P_1, \ldots, P_r$ и справедливо равенство

$$\sum_{i=1}^{r} \mathrm{Res}_{P_i}(\omega) = 0.$$

г) Каждая непостоянная мероморфная функция φ на римановой поверхности R принимает любое значение $c \in \overline{\mathbb{C}}$ одно и то же число раз (это число называется *валентностью* функции φ).

д) Если φ и ψ — непостоянные мероморфные функции на R валентности m и n соответственно, то существует такой неприводимый многочлен $f \in \mathbb{C}[x, y]$ степени $\leqslant n$ по x и $\leqslant m$ по y, что $f(\varphi, \psi) = 0$.

(Указание. Пусть комплексное число c отлично от нулей и полюсов функции ψ, и пусть $P_1, \ldots, P_n$ — все точки поверхности R, в которых $\psi = c$. Показать, что для каждого целого $r \geqslant 0$ дифференциал $\omega = \varphi^r \frac{d\psi}{\psi - c}$ имеет в каждой точке P_i простой полюс с вычетом $\varphi^r(P_i)$ и что его вычеты во всех других полюсах являются рациональными функциями от c. Вывести отсюда, что суммы

$$\sum_{i=1}^{n} \varphi^r(P_i)$$

являются рациональными функциями от c и что таковыми являются элементарные симметрические функции от $\varphi(P_1), \ldots, \varphi(P_n)$.)

е) Мероморфные функции на R порождают конечное расширение поля рациональных функций $\mathbb{C}(x)$.

ж) Всякая компактная связная риманова поверхность R конформно эквивалентна неособой алгебраической кривой, определенной над полем $\mathbb{C}$.

(Указание. Воспользоваться результатом п. д) и установить существование взаимно однозначного и конформного отображения R на риманову поверхность алгебраической функции $y = y(x)$, удовлетворяющей уравнению $f(x, y) = 0$ (см. [114, гл. 10, п. 9]).)

2*. Пусть R — компактная связная риманова поверхность. Свободную абелеву группу, порожденную точками поверхности R, назовем *группой дивизоров* на R и обозначим ее $\mathrm{Div}(R)$. Если $P_1, \ldots, P_n$ и $Q_1, \ldots, Q_n$ — нули и полюса мероморфной на R функции φ, то дивизор

$$(\varphi) = P_1 + \ldots + P_n - Q_1 \ldots - Q_n$$

назовем *дивизором функции* φ или *главным дивизором*. Аналогичным образом определяется дивизор (ω) отличного от нуля дифференциала ω на R. Задание дивизора (φ) определяет мероморфную функцию φ на R с точностью до постоянного множителя. Дивизоры функций φ образуют *подгруппу* $P(R)$ *главных дивизоров* группы $\mathrm{Div}(R)$. Факторгруппа $\mathrm{Cl}(R) = \mathrm{Div}(R)/P(R)$ называется *группой классов дивизоров* на R. Каждый класс группы $\mathrm{Cl}(R)$ состоит из *линейно эквивалентных* между собой дивизоров. Дивизор

$$A = \sum a_i \cdot P_i, \quad a_i \in \mathbb{Z},$$

называется *положительным* (символическая запись $A \geqslant 0$), если $a_i \geqslant 0$ для всех i. Целое число

$$\sum a_i$$

называется *степенью* $\deg A$ *дивизора* A.

Дивизоры степени 0 образуют подгруппу $\mathrm{Div}^0(R)$ группы $\mathrm{Div}(R)$, содержащую в себе группу $P(R)$. Факторгруппа $\mathrm{Cl}^0(R) = \mathrm{Div}^0(R)/P(R)$ называется *группой классов дивизоров степени* 0.

Пусть R и S — две компактные связные римановы поверхности. Отображение $f\colon R \to S$ называется *голоморфным*, если для каждой точки $P \in R$ и любого локального параметра τ в точке $f(P) \in S$ функция $\tau \circ f$ голоморфна в P. Точка $P \in R$ называется *точкой ветвления индекса* e для f, если функция $\tau \circ f - \tau \circ f(P)$ имеет в точке P нуль порядка $e > 1$. Степень n дивизора $f^{-1}(Q)$ не зависит от выбора точки $Q \in S$ (при условии, что точка ветвления $f^{-1}(Q)$ берется с кратностью, равной ее порядку ветвления) и называется *степенью отображения* f.

Обозначим $L(-A)$ векторное пространство над полем $\mathbb{C}$, состоящее из мероморфных на R функций φ, таких, что $(\varphi) + A \geqslant 0$, и положим $l(-A) = \dim_{\mathbb{C}} L(-A)$. Пусть W — класс дивизоров отличных от нуля дифференциалов ω на римановой поверхности R. Класс W называется *каноническим классом*, и его элементы — *каноническими дивизорами*.

Доказать справедливость следующих утверждений:

а) Теорема Римана — Роха. *Существует целое число* $g \geqslant 0$, *зависящее лишь от* R *и называемое родом римановой поверхности* R, *такое, что*

$$l(-A) = \deg A - g + 1 + l(A - (\omega))$$

для каждого дивизора $A \in \mathrm{Div}(R)$ *и для любого канонического дивизора* (ω).

б) Для каждого $(\omega) \in W$ справедливы соотношения $\deg(\omega) = 2g - 2$ и $l(-(\omega)) = g$.

в) Дифференциалы первого рода образуют $\mathbb{C}$-векторное пространство размерности g.

г) Если $\deg A > 2g - 2$, то $l(-A) = \deg A - g + 1$.

д) Пусть R и S — две компактные связные римановы поверхности родов $g(R)$ и $g(S)$ соответственно. Если $f\colon R \to S$ — непостоянное голоморфное отображение R на S степени n и $P_1, \ldots, P_r$ — все точки ветвления, то

$$2g(R) - 2 = n(2g(S) - 2) + \sum_{i=1}^{r} (e_i - 1),$$

где e_i — индекс ветвления точки P_i.

е) Пусть φ — непостоянная мероморфная функция валентности n на римановой поверхности R рода g и $P_1, \ldots, P_r$ — все точки ветвления этой функции. Тогда

$$g = 2 - 2n + \sum_{i=1}^{r} (e_i - 1),$$

где e_i — индекс ветвления точки P_i.

ж) Если первая группа гомологий $H_1(R, \mathbb{Z})$ имеет $2g$ образующих, то род римановой поверхности R равен g.

з) Если триангуляция римановой поверхности R рода g содержит n вершин, m ребер и r граней, то

$$2g - 2 = m - n - r.$$

(Указание. См. [114, гл. 5; 70е, гл. II].)

3*. Пусть Ω — векторное над полем $\mathbb{C}$ пространство дифференциалов первого рода на компактной связной римановой поверхности R рода $g > 0$. Ввиду результата п. а) задачи 1 спаривание

$$(\omega, \gamma) \mapsto \int_{\gamma} \omega$$

индуцирует отображение

$$\Omega \times H_1(R, \mathbb{Z}) \to \mathbb{C},$$

которое $\mathbb{C}$-линейно по первому аргументу и аддитивно по второму. Поэтому это отображение индуцирует канонический гомоморфизм

$$H_1(R, \mathbb{Z}) \to \Omega^* = \mathrm{Hom}(\Omega, \mathbb{C}).$$

Образ Λ этого гомоморфизма является абелевой группой (*группой периодов*) с $k \leqslant 2g$ образующими. Пусть P_0 — фиксированная и P — произвольная точки поверхности R. Тогда дуге P_0P соответствует элемент $\omega \mapsto \int_{P_0}^{P} \omega$ группы Ω^*. Изменение дуги P_0P, соединяющей P_0 и P, приводит к изменению интеграла $\int_{P_0}^{P} \omega$ на некоторый элемент группы Λ. Поэтому точке P соответствует некоторый элемент факторгруппы Ω^*/Λ (называемой *якобианом* римановой поверхности R). По аддитивности это соответствие можно расширить до гомоморфизма

$$u\colon \mathrm{Div}(R) \to \Omega^*/\Lambda.$$

Если теперь ограничить этот гомоморфизм на группу дивизоров $\mathrm{Div}^0(R)$ степени 0, то он не будет зависеть от выбора точки P_0.

Пусть $\gamma_1, \ldots, \gamma_g, \gamma_1', \ldots, \gamma_g'$ — система замкнутых кривых на R, составляющая *канонический базис* группы $H_1(R, \mathbb{Z})$ (кривая γ_i пересекается лишь с γ_i' в единственной точке и ориентация кривых γ_i и γ_i' положительна по направлению от γ_i к γ_i'). Разрезав риманову поверхность R по кривым γ_i, γ_i', получаем ее представление в виде многоугольника R^* с $4g$ сторонами

$$\gamma_1, \gamma_1', -\gamma_1, -\gamma_1', \ldots, \gamma_g, \gamma_g', -\gamma_g, -\gamma_g'.$$

Если $\omega_1, \ldots, \omega_g$ — базис пространства дифференциалов первого рода на R, то интегралы

$$\alpha_{ij} = \int_{\gamma_i} \omega_j, \quad \alpha_{ij}' = \int_{\gamma_i'} \omega_j$$

называются *периодами дифференциалов* $\omega_1, \ldots, \omega_g$.

Доказать справедливость следующих утверждений:

а) Пусть P_0 — фиксированная внутренняя точка и P — произвольная точка многоугольника R^*. Если ω — любой дифференциал первого рода на R^*, то интеграл

$$f(P) = \int_{P_0}^{P} \omega$$

представляет собой однозначную голоморфную функцию на R^*.

(Указание. Показать, что интеграл от ω по любому замкнутому пути в R^* равен нулю.)

б) Для любых двух дифференциалов ω_1, ω_2 первого рода на R их периоды

$$\alpha_{ij} = \int_{\gamma_i} \omega_j \quad \text{и} \quad \alpha_{ij}' = \int_{\gamma_i'} \omega_j$$

связаны *билинейным соотношением Римана*

$$\sum_{i=1}^{g} (\alpha_{i1}\alpha_{i2}' - \alpha_{i1}'\alpha_{i2}) = 0.$$

(Указание. Воспользовавшись тем, что ω_1 обладает на R^* неопределенным интегралом f_1, представляющим собой однозначную голоморфную функцию, показать, что интеграл от дифференциала первого рода $\omega^* = f_1\omega_2$ по границе γ многоугольника R^* равен нулю. Затем, воспользовавшись тем, что каждой точке разреза γ_i соответствуют две точки границы γ, которые соединены путем, гомологичным γ_i', показать, что значения функции f_1 в этих двух точках различаются на α_{i1}'. Принимая во внимание ориентацию сторон многоугольника R^*, вывести отсюда, что

$$\int_{\gamma_i} \omega^* + \int_{-\gamma_i} \omega^* = -\alpha_{i1}' \int_{\gamma_i} \omega_2 = -\alpha_{i1}'\alpha_{i2}$$

и что

$$\int_{\gamma_i'} \omega^* + \int_{-\gamma_i'} \omega^* = \alpha_{i1} \int_{\gamma_i'} \omega_2 = \alpha_{i1}\alpha_{i2}'.$$

Суммируя эти равенства по $i = 1, 2, \ldots, g$, получить билинейное соотношение Римана.)

в) Группа периодов Λ является решеткой в Ω^* ранга $2g$ (свободной абелевой группой с $2g$ образующими, которые порождают Ω^*, рассматриваемое как действительное векторное пространство).

(Указание. Установить, что векторы периодов

$$\alpha_i = (\alpha_{i1}, \ldots, \alpha_{ig}), \quad \alpha_i' = (\alpha_{i1}', \ldots, \alpha_{ig}'), \quad 1 \leqslant i \leqslant g,$$

базисных элементов $\omega_1, \ldots, \omega_g$ пространства Ω порождают решетку Λ.)

г) Теорема Абеля. *Ядром гомоморфизма*

$$u\colon \mathrm{Div}^0(R) \to \Omega^*/\Lambda$$

служит группа $P(R)$ главных дивизоров римановой поверхности R.

(Указание. Показать сначала, что дивизор любой мероморфной на R функции t содержится в ядре рассматриваемого гомоморфизма. Для этого выбрать представление поверхности в виде многоугольника R^*, гданица которого γ не содержит ни нулей, ни полюсов функции t, и рассмотреть голоморфный на γ дифференциал $\omega = dt/t$, а также вектор

$$f(P) = (f_1(P), \ldots, f_g(P)),$$

где

$$f_i(P) = \int_{P_0}^{P} \omega_i$$

— однозначные голоморфные на R^* функции. Пусть

$$(t) = \sum_{j=1}^{r} a_j \cdot P_j$$

— дивизор функции t. Показать, что

$$\mathrm{Res}_{P_j}(f\omega) = a_j f(P_j).$$

Затем, воспользовавшись теоремой Коши о вычетах, а также рассуждениями п. б), показать, что

$$\int_{\gamma} f\omega = 2\pi\sqrt{-1} \sum_{j=1}^{r} \mathrm{Res}_{P_j}(f\omega) = 2\pi\sqrt{-1} \sum_{j=1}^{r} a_j f(P_j) = \sum_{i=1}^{g} (u_i'\alpha_i - u_i\alpha_i'),$$

где

$$u_i = \int_{\gamma_i} \omega = 2\pi\sqrt{-1}\, m_i, \quad m_i \in \mathbb{Z},$$

и

$$u_i' = \int_{\gamma_i'} \omega = 2\pi\sqrt{-1}\, m_i', \quad m_i' \in \mathbb{Z}.$$

Для доказательства обратного утверждения установить индукцией по $r \geqslant 2$ и с помощью теоремы Римана — Роха, что для каждого дивизора

$$A = \sum_{j=1}^{r} a_j \cdot P_j$$

степени 0 существует такой дифференциал третьего рода ω, что $\operatorname{Res}_{P_j}(\omega) = a_j$ для всех $j = 1, 2, \ldots, r$. Показать затем, что дифференциал ω может быть выбран таким образом, что, кроме того,

$$\int_{\gamma_i} \omega = 2\pi\sqrt{-1}\, n_i, \quad \int_{\gamma_i'} \omega = 2\pi\sqrt{-1}\, n_i',$$

где n_i, n_i' — некоторые целые числа.

Вывести отсюда, что A является дивизором некоторой мероморфной на R функции t. См. также [70e, гл. III, § 2; 33, т. 1, гл. 2, § 2 и 114, гл. 10, п. 7].)

д) Теорема Якоби. *Гомоморфизм*

$$u\colon \operatorname{Div}^0(R) \to \Omega^*/\Lambda$$

является эпиморфизмом.

(Указание. Дивизор $A \in \operatorname{Div}(R)$ называется *неспециальным*, если $l(A - (\omega)) = 0$ для любого канонического дивизора (ω). Доказать, что существует g различных точек $Q_1, \ldots, Q_g$, для которых дивизор

$$A = Q_1 + \ldots + Q_g$$

неспециален. Пусть t_i — локальный параметр в точке Q_i и $\omega_1, \ldots, \omega_g$ — базис пространства Ω. Показать, что определитель

$$\det \left\| \frac{\omega_j}{dt_i}(Q_i) \right\|_{1 \leqslant i,j \leqslant g}$$

отличен от нуля и вывести отсюда, что отображение

$$(P_1, \ldots, P_g) \mapsto \sum_{i=1}^{g} \left(\int_{Q_i}^{P_i} \omega_1, \ldots, \int_{Q_i}^{P_i} \omega_g \right)$$

определяет аналитический изоморфизм произведения $V_1 \times \ldots \times V_g$ достаточно малых дисков $V_1, \ldots, V_g$ с центрами в точках $Q_1, \ldots, Q_g$ с некоторой окрестностью нуля пространства Ω^*. Показать, далее, что сюръективность отображения u достаточно установить для некоторой окрестности нуля в Ω^*. См. также [70e, гл. III, § 3; 33, т. 1, гл. 2, § 2; 114, гл. 10, п. 8 и 128, гл. II, § 21].)

е) Факторгруппа Ω^*/Λ является $2g$-мерным вещественным тором.

(Указание. Рассмотреть Ω^* как g-мерное комплексное пространство $\mathbb{C}^g$. Установить, что каждый комплексный вектор $(z_1, \ldots, z_g)$ сравним по mod Λ с вектором, длина которого ограничена абсолютной константой, и воспользоваться затем результатом п. в).)

ж) Если $A = P_1 + \ldots + P_r - Q_1 - \ldots - Q_r$ — дивизор степени 0 на R и $\omega_1, \ldots, \omega_g$ — базис пространства Ω, то сопоставление

$$u\colon A \mapsto \left(\sum_{i=1}^{g} \int_{Q_i}^{P_i} \omega_1, \ldots, \sum_{i=1}^{g} \int_{Q_i}^{P_i} \omega_g \right) \pmod{\Lambda}$$

задает изоморфизм группы классов дивизоров $\mathrm{Cl}^0(R)$ степени 0 на Ω^*/Λ.

з) Если P_0 — фиксированная точка римановой поверхности R, $A = P_1 + \ldots + P_g$ — дивизор на R степени g и $\omega_1, \ldots, \omega_g$ — базис пространства Ω, то соответствие

$$u\colon A \mapsto \left(\sum_{i=1}^{g} \int_{P_0}^{P_i} \omega_1, \ldots, \sum_{i=1}^{g} \int_{P_0}^{P_i} \omega_g \right) \pmod{\Lambda}$$

взаимно однозначно тогда и только тогда, когда дивизор A неспециален.

4*. Пусть R компактная связная риманова поверхность рода $g > 0$ и Ω — векторное над полем $\mathbb{C}$ пространство дифференциалов первого рода на R. Пусть, далее, $\omega_1, \ldots, \omega_g$ — базис пространства Ω, P_0 — фиксированная точка римановой поверхности R, $A = P_1 + \ldots + P_g$ — дивизор степени g на R и

$$u\colon A \mapsto \left(\sum_{i=1}^{g} \int_{P_0}^{P_i} \omega_1, \ldots, \sum_{i=1}^{g} \int_{P_0}^{P_i} \omega_g \right) \pmod{\Lambda}$$

— отображение дивизора A в Ω^*/Λ. Числа

$$u_j(A) = \sum_{i=1}^{g} \int_{P_0}^{P_i} \omega_j$$

называются *абелевыми координатами* дивизора A.

Пусть K — конечное расширение поля рациональных чисел $\mathbb{Q}$. Дивизор

$$A = P_1 + \ldots + P_g$$

называется *K-рациональным*, если все рациональные симметрические функции от координат точек $P_1, \ldots, P_g$ с коэффициентами из $\mathbb{Q}$ являются элементами поля K. Классическая *теорема сложения точек* на R утверждает, что если P_0 суть K-рациональная точка и A, B — положительные K-рациональные дивизоры степени g, то существует такой положительный K-рациональный дивизор C степени g, определяющий единственный класс дивизоров, что

$$u_j(A) + u_j(B) \equiv u_j(C) \pmod{\Lambda}, \quad 1 \leqslant j \leqslant g.$$

Указанная операция сложения, которая может быть переписана в виде

$$A + B = C,$$

превращает множество положительных K-рациональных дивизоров степени g в абелеву группу $\operatorname{Div}_K^g(R)$. В соответствии с *теоремой Морделла — Вейля* [89b, 23a] эта группа имеет конечное число образующих (см. также [70h, гл. 6]).

Пусть $u_1, \ldots, u_g$ и $v_1, \ldots, v_g$ — абелевы координаты дивизоров $A = P_1 + \ldots + P_g$ и $B = Q_1 + \ldots + Q_g$ соответственно. Если

$$\tau_j = \sum_{i=1}^{g} \left(a_i \alpha_{ij} + a_i' \alpha_{ij}' \right), \quad a_i, a_i' \in \mathbb{Z}, \quad 1 \leqslant j \leqslant g,$$

— элементы решетки Λ, то выражения

$$u_1 - v_1 + \tau_1, \ldots, u_g - v_g + \tau_g$$

задают в общем виде абелевы координаты дивизора $A - B$. Далее, если $n > 1$ — целое число, то n^{2g} векторов

$$\left(\frac{u_1 - v_1 + \tau_1}{n}, \ldots, \frac{u_g - v_g + \tau_g}{n} \right), \quad 0 \leqslant a_i, \ a_i' \leqslant n - 1,$$

не сравнимы между собой по mod Λ. Отсюда следует, что каждый дивизор $A = gP$ порождает n^{2g} дивизоров

$$A' = P_1' + \ldots + P_g'$$

таких, что

$$u(A) \equiv nu(A') + u(B) \pmod{\Lambda}.$$

Пусть $X \subset \overline{\mathbb{C}} \times \overline{\mathbb{C}}$ — алгебраическая кривая рода g, определенная над полем K уравнением $f(x, y) = 0$. Отождествим ее с римановой поверхностью R рода g, а поле рациональных функций F на X — с полем мероморфных на R функций. Если $(n, g) = 1$, то множество E_n всех симметрических функций от координат точек $P_1', \ldots, P_g' \in R$ является полем рациональных функций на соответствующей кривой Y и, более того, неразветвленным абелевым расширением поля F степени n^{2g}. Риманова поверхность R_n поля E_n представляет собой n^{2g}-листное накрытие поверхности R. Дивизоры

$$A' = P_1' + \ldots + P_g' \in \mathrm{Div}(R_n)$$

такие, что $nA' \equiv 0 \pmod{\Lambda}$ называются *дивизорами порядка* n на R_n. Если P_0 — алгебраическая точка, то такие дивизоры имеют алгебраические координаты.

Используя билинейные соотношения Римана

$$\sum_{i=1}^{g} \left(\alpha_{ij}\alpha'_{ik} - \alpha'_{ij}\alpha_{ik}\right) = 0, \quad j \neq k,$$

и

$$\mathrm{Im}\left(\sum_{i=1}^{g} \alpha_{ij}\alpha'_{ij}\right) > 0, \quad 1 \leqslant j \leqslant g,$$

можно выбрать каноническую систему разрезов $\widetilde{\gamma}_i, \widetilde{\gamma}_i'$, $1 \leqslant i \leqslant g$, римановой поверхности R таким образом, чтобы выполнялись соотношения

$$\alpha'_{ij} = \alpha'_{ji}, \quad \alpha_{ij} = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j, \end{cases}$$

и чтобы мнимая часть квадратичной формы

$$\psi(x_1, \ldots, x_g) = \sum_{i,j=1}^{g} \alpha'_{ij} x_i x_j$$

была положительна для каждого ненулевого целочисленного набора $(x_1, \ldots, x_g) = (n_1, \ldots, n_g)$. Пусть

$$\theta(z) = \theta(z_1, \ldots, z_g) = \sum_{n_1, \ldots, n_g = -\infty}^{\infty} \exp\left\{\pi\sqrt{-1}\left(\sum_{i,j=1}^{g} \alpha'_{ij} n_i n_j + 2\sum_{i=1}^{g} n_i z_i\right)\right\}$$

— *тета-функция Римана*. При выполнении указанных условий она является отличной от нуля целой функцией комплексных переменных $z_1, \ldots, z_g$, удовлетворяющей функциональным уравнениям

$$\theta(z + \alpha_i) = \theta(z), \quad 1 \leqslant i \leqslant g,$$

и

$$\theta\left(z + \alpha_i'\right) = \exp\left\{-\pi\sqrt{-1}\left(2z_i + \alpha'_{ii}\right)\right\}\theta(z), \quad 1 \leqslant i \leqslant g.$$

Доказать справедливость следующих результатов Зигеля [54d]:

а) Если целое число $n > 1$ достаточно велико и точка P_0 выбрана подходящим образом, то для всех точек $P \in R$, за исключением их конечного числа, и для каждого множества периодов $\{\tau_1, \ldots, \tau_g\}$ существует единственный дивизор $A' = P_1' + \ldots + P_g'$ с абелевыми координатами

$$\frac{u_1 - v_1 + \tau_1}{n}, \ \ldots, \ \frac{u_g - v_g + \tau_g}{n},$$

где $(u_1, \ldots, u_g) = u(gP)$.

(Указание. Пусть $\tau = (\tau_1, \ldots, \tau_g)$ — произвольный вектор периодов и Q — любая точка поверхности R. Доказать, что существует лишь конечное число точек $P \in R$, для которых функция

$$f(P, P') = \theta\left(\frac{gu(P) + \tau}{n} - u(P') + u(Q)\right)$$

равна тождественно нулю по переменной $P' \in R$. Для этого предположить, что таких точек P имеется бесконечно много, и, воспользовавшись регулярностью функции f по переменной P, вывести отсюда, что $f(P, P') \equiv 0$. Показать далее, что при надлежащем изменении точки P на R и при надлежащем выборе целого $n > 1$ аргумент

$$\frac{gu(P) + \tau}{n} + u(Q) = \left(\frac{g}{n}\widetilde{\tau}_1 + \eta_1, \ \ldots, \ \frac{g}{n}\widetilde{\tau}_g + \eta_g\right)$$

функции f может быть сделан как угодно близким к произвольной точке $z = (z_1, \ldots, z_g)$. После этого прийти к противоречию с тем, что функция $\theta(z - u(P'))$ не равна тождественно нулю.

Воспользоваться, наконец, следующим результатом Римана: *если при некотором* $Q \in R$ *функция*

$$\theta\left(\frac{gu(P) + \tau}{n} - u(P') + u(Q)\right)$$

не равна тождественно нулю по переменной P', *то она имеет на* R *ровно* g *нулей* $P_1', \ldots, P_g'$, *которые при подходящем* $B = Q_1 + \ldots + Q_g \in \mathrm{Div}(R)$ *однозначно определяются соотношением*

$$\sum_{i=1}^{g} u\left(P_i'\right) \equiv \frac{gu(P) - u(B) + \tau}{n} \pmod{\Lambda}$$

(см. также [33, т. 1, гл. 2, § 7].)

б) Если $\varphi(P)$ — мероморфная на R функция валентности d и $A' = P_1' + \ldots + P_g'$ — дивизор на R_n, определенный в предыдущем пункте, то функция

$$\Phi(P) = \varphi\left(P_1'\right) \ldots \varphi\left(P_g'\right)$$

есть элемент поля E_n валентности не выше $dg^3 n^{2g-2}$.

(Указание. Представить риманову поверхность R_n в виде многоугольника R_n^*, состоящим из n^{2g} экземпляров многоугольника R^*, а функцию $\Phi(P)$ — в виде

$$\Phi(P) = c\prod_{i=1}^{d} \frac{\theta\left(\frac{gu(P) + \tau}{n} - u(P_i) + u(Q)\right)}{\theta\left(\frac{gu(P) + \tau}{n} - u(Q_i) + u(Q)\right)},$$

где $P_1, \ldots, P_d$ — нули и $Q_1, \ldots, Q_d$ — полюса функции $\varphi(P)$. Показать, что

число нулей функции

$$\theta = \theta\left(\frac{gu(P)}{n} + e\right)$$

внутри многоугольника R_n^* равно интегралу

$$\frac{1}{2\pi\sqrt{-1}} \int_{\Gamma_n} d\log\theta,$$

взятому в положительном направлении по границе Γ_n многоугольника R_n^*. Воспользовавшись функциональными уравнениями

$$\theta\left(\frac{gz}{n} + g\alpha_i\right) = \theta(z)$$

и

$$\theta\left(\frac{gz}{n} + g\alpha_i'\right) = \exp\left\{-\pi\sqrt{-1}\left(\frac{g^2}{n}z_i + g\alpha_{ii}'\right)\right\}\theta(z),$$

установить, что стороны $\tilde{\gamma}_i'$, $-\tilde{\gamma}_i'$ многоугольника R_n^* не дают никакого вклада в рассматриваемый интеграл, в то время как каждые n^2 экземпляров сторон $\tilde{\gamma}_i$, $-\tilde{\gamma}_i$ дают вклад $\frac{g^2}{n}\cdot n$. Учитывая, что для каждого $i = 1, 2, \ldots, g$ граница Γ_n многоугольника R_n^* содержит в точности n^{2g} экземпляров $\tilde{\gamma}_i$, $-\tilde{\gamma}_i$, вывести отсюда, что число нулей функции

$$\theta\left(\frac{gu(P)}{n} + e\right)$$

внутри R_n^* равно g^3n^{2g-2}.)

в) Пусть x_i', y_i' — координаты точек P_i', $1 \leqslant i \leqslant g$, определенных в п. а). Тогда при выбранных подходящим образом параметрах t_1, t_2, a_1, a_2, b_1, b_2, c_1, c_2 функции

$$\Phi_j(P) = \prod_{i=1}^{g}\left(t_j - \frac{a_1x_i' + b_1y_i' + c_1}{a_2x_i' + b_2y_i' + c_2}\right), \quad 1 \leqslant j \leqslant 2,$$

порождают поле E_n и связаны между собой над полем K неприводимым уравнением $f_n(x, y) = 0$ степени не выше dg^3n^{2g-2}, где d — минимальная степень поля F над $K(x)$.

(Указание. Выбрать параметры t_1, t_2, a_1, a_2, b_1, b_2, c_1, c_2 таким образом, чтобы валентности функций

$$\varphi_j = t_j - \frac{a_1x + b_1y + c_1}{a_2x + b_2y + c_2}, \quad 1 \leqslant j \leqslant 2,$$

были равны d, и воспользоваться результатами предыдущего пункта и п. д) задачи 1.)

ЗАКЛЮЧЕНИЕ

ДЕСЯТАЯ ПРОБЛЕМА ГИЛЬБЕРТА

Основным недостатком теоремы Зигеля — Малера является ее неэффективность. Чтобы лучше понять возникающие в этом вопросе трудности, полезно рассмотреть общую ситуацию, касающуюся эффективного определения решений произвольно взятого диофантова уравнения. Здесь мы ограничимся лишь кратким обзором возникающих при этом проблем, отсылая читателя за подробностями к книгам [32b], [40a], [50c], [80], [81c, d], [113c] и к статье [41].

В 1900 г. на Международном математическом конгрессе в Париже Д. Гильберт выделил 23 проблемы, решение которых представляло по его мнению особый интерес для дальнейшего развития математики. В их число вошла 10-я проблема, касающаяся вопроса о разрешимости диофантовых уравнений. Эта проблема может быть сформулирована в следующем виде. Пусть $P(t, x_1, \ldots, x_n)$ — многочлен из кольца $\mathbb{Z}[t, x_1, \ldots, x_n]$. Требуется построить алгоритм, позволяющий определить, будет ли каждое из уравнений

$$P(t, x_1, \ldots, x_n) = 0, \quad t = 0, 1, 2, \ldots,$$

иметь решение $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ или нет.

Многочисленные безуспешные попытки установить существование такого алгоритма навели в конце концов на мысль, что 10-я проблема Гильберта алгоритмически не разрешима.

Заметим сразу же, что вопрос об алгоритмической неразрешимости той или иной проблемы с необходимостью приводит к задаче о точном определении понятия алгоритма. Впервые подозрения о существовании алгоритмически неразрешимых проблем зародились в связи с принципиальными трудностями, возникшими при реализации программы Гильберта по обоснованию математики и, в частности, при решении его Entscheidungsproblem. Эта проблема, алгоритмическая неразрешимость которой впервые была установлена Чёрчем (1936 г.) и Тьюрингом (1937 г.), состоит в том, чтобы для произвольного конечного множества высказываний T и любого высказывания φ логики первого порядка определить, будет ли φ выводимо из T на основе некоторой естественной системы аксиом и в соответствии с определенными правилами вывода. Entscheidungsproblem была провозглашена Гильбертом самой фундаментальной проблемой математической логики, так как процедура ее решения могла,

по мнению Гильберта, привести к возможности алгоритмического решения всех математических задач. Последующее развитие математической логики разрушило эти надежды.

1. Неформальная вычислимость. Целью данного пункта является формализация процесса вычисления специального класса функций, определенных на наборах неотрицательных целых чисел и принимающих неотрицательные целые значения.

Пусть $\mathbb{N}$ — множество неотрицательных целых чисел и $\mathbb{N}^n$ — прямое произведение n экземпляров множества $\mathbb{N}$. *Частичной числовой функцией* называется пара $(f, D(f))$, состоящая из отображения $f\colon \mathbb{N}^n \to \mathbb{N}$ и его области определения $D(f)$. Множество всех таких функций имеет мощность континуума, и из этого огромного количества мы хотим выбрать счетное число функций, которые являются вычислимыми.

Начнем с интуитивного описания понятия вычислимости. Назовем n-местную частичную числовую функцию f *эффективно (алгоритмически) вычислимой*, если существует эффективная процедура (алгоритм), которая правильно вычисляет f. Эффективная процедура должна удовлетворять следующим критериям:

1) для этой процедуры должны иметься точные инструкции (программа) конечной длины. Эти инструкции не должны предполагать никакой изобретательности или даже понимания со стороны человека или машины, которые следуют этим инструкциям. Исполнение инструкций должно состоять только в аккуратном следовании указаниям;

2) если задан упорядоченный набор $x=(x_1, \ldots, x_n)$ из $D(f)$, то после конечного числа дискретных шагов процедура вычисления должна закончиться, выдав значение $f(x)$;

3) если задан упорядоченный набор $x=(x_1, \ldots, x_n)$, не принадлежащий $D(f)$, то процедура вычисления $f(x)$ продолжается неограниченно.

Несмотря на то что нами дано лишь приблизительное описание, а не точное определение алгоритма, уже на этом неформальном уровне можно развить почти всю теорию эффективно вычислимых функций. Отметим, что при этом не налагается никаких ограничений на величину аргументов, на время вычисления $f(x)$ при $x \in D(f)$ и на объем памяти.

Таким образом, класс эффективно вычислимых функций — это класс частичных числовых функций, которые могут быть вычислены в идеале, когда снимаются все практические ограничения.

2. Машины Тьюринга. Отметим сразу же одно весьма существенное обстоятельство. Совокупность эффективных процедур, удовлетворяющих критериям 1)—3), очень обширна и мало обозрима. Напротив, совокупность эффективно вычислимых функций при всевозможных истолкованиях эффективных процедур, удовлетворяющих критериям 1)—3), оказывается одной и той же, причем легко описываемой в обычных математических терминах. Учитывая это обстоятельство, Пост и Тьюринг почти одновременно ввели в рассмотрение довольно узкие классы абстрактных машин, на которых оказалось возможным реализовать все эффективные процедуры, которые когда-либо встречались в математике. Машины, описанные Постом и Тьюрингом, различались весьма незначительно, и в дальнейшем стали называться машинами Тьюринга.

Машина Тьюринга представляет собой абстрактное устройство, состоящее из потенциально бесконечной в обе стороны ленты, разделенной на ячейки управляющего устройства с конечным множеством состояний $Q=\{q_1, \ldots, q_s\}$ и считывающей головки. Работа машины Тьюринга происходит следующим образом. В каждый дискретный момент времени головка обозревает одну вполне определенную ячейку и в зависимости от записанного в ней символа a_i из алфавита $A=\{0, 1\}$ и от текущего внутреннего состояния q_j управляющего устройства головка вписывает в обозреваемую ячейку новый символ из A, сдвигаясь после этого на одну ячейку влево или вправо, либо оставаясь на месте, а управляющее устройство переходит в новое состояние q_k. Работу машины можно описать тремя частичными функциями

$$F\colon A\times Q \to A, \quad G\colon A\times Q \to Q, \quad H\colon A\times Q \to \{L, S, R\},$$

где L, S и R обозначают соответственно сдвиг головки влево, отсутствие движения и сдвиг вправо, или же в виде программы, состоящей из команд

$$a_i q_j F(a_i, q_j) G(a_i, q_j) H(a_i, q_j).$$

Основным кодом набора $(x_1, \ldots, x_n) \in \mathbb{N}^n$ называется запись на ленте вида

$$\ldots 0\underbrace{1\ldots1}_{x_1+1}0\underbrace{1\ldots1}_{x_2+1}0\ldots0\underbrace{1\ldots1}_{x_n+1}0\ldots.$$

Частичная числовая функция $f(x_1, \ldots, x_n)$ с областью определения $D(f)$ называется *вычислимой* (по Тьюрингу), если существует такая машина Тьюринга T, что:

1) при ее применении к основному коду для набора $(x_1, \ldots, x_n) \in D(f)$ машина T выдает после конечного числа шагов код числа $f(x_1, \ldots, x_n)$ и останавливается;

2) при ее применении к основному коду для набора $(x_1, \ldots, x_n) \notin D(f)$ машина T не останавливается.

Класс вычислимых функций обозначим $P_в$.

3. Частично рекурсивные функции. Перейдем к математическому описанию класса числовых функций, представляющих собой адекватную формализацию класса $P_в$.

Суперпозицией частичных функций $f=(f_1, \ldots f_m)\colon \mathbb{N}^n \to \mathbb{N}^m$ и $g\colon \mathbb{N}^m \to \mathbb{N}$ называется функция $n = g \circ f\colon \mathbb{N}^n \to \mathbb{N}$, задаваемая

в виде

$$h(x_1, \ldots, x_n) = g(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$$

и имеющая область определения

$$D(h) = \{x \in \mathbb{N}^n \mid x \in D(f), \quad f(x) \in D(g)\}.$$

Операция примитивной рекурсии заключается в сопоставлении паре частичных функций $g\colon \mathbb{N}^n \to \mathbb{N}$ и $h\colon \mathbb{N}^{n+2} \to \mathbb{N}$ частичной функции $f\colon \mathbb{N}^{n+1} \to \mathbb{N}$, задаваемой схемой:

$$\begin{cases} f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n), \\ f(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)). \end{cases}$$

Область определения $D(f)$ функции f также описывается рекурсивно

$$(x_1, \ldots, x_n, 0) \in D(f) \Leftrightarrow (x_1, \ldots, x_n) \in D(g);$$

$$(x_1, \ldots, x_n, y+1) \in D(f) \Leftrightarrow (x_1, \ldots, x_n, y) \in D(f) \text{ и } (x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \in D(h).$$

Операция минимизации μ ставит в соответствие частичной функции $g\colon \mathbb{N}^n \to \mathbb{N}$ частичную функцию $f\colon \mathbb{N}^n \to \mathbb{N}$, задаваемую следующим образом:

$$f(x_1, \ldots, x_n) = \mu_y(g(x_1, \ldots, x_{n-1}, y) = x_n) = \min\{y \in \mathbb{N} \mid g(x_1, \ldots, x_{n-1}, y) = x_n)\},$$

$$D(f) = \{(x_1, \ldots, x_n) \in \mathbb{N}^n \mid \exists y \in \mathbb{N},\ g(x_1, \ldots, x_{n-1}, y) = x_n \text{ и } (x_1, \ldots, x_{n-1}, z) \in D(f) \text{ для всех } z \leqslant \mu_y\}.$$

Своеобразие области определения диктуется процессом машинного перебора при нахождении решения уравнения $g(x_1, \ldots, x_{n-1}, y) = x_n$.

Множество всех частичных числовых функций, которые можно получить из системы простейших функций:

$$O(x) \equiv 0, \quad S(x) = x + 1, \quad I_m^n(x_1, \ldots, x_n) = x_m, \quad 1 \leqslant m \leqslant n,$$

при помощи операций суперпозиции, примитивной рекурсии и минимизации, называется *классом частично рекурсивных функций* и обозначается $P_{\text{чр}}$.

Теорема 1 (Клини). *Имеет место соотношение*

$$P_{\text{в}} = P_{\text{чр}}.$$

4. Тезис Чёрча. Возникает естественный вопрос, а именно, не существует ли некоторая другая формализация понятия алгоритма, которая может вывести за пределы класса $P_{\text{чр}}$.

Фундаментальным открытием теории вычислимости явилось то, что на поставленный вопрос нужно дать отрицательный ответ.

Соответствующая гипотеза впервые была выдвинута и аргументирована Чёрчем. В настоящее время эта гипотеза — тезис Чёрча принимается почти всеми скорее как экспериментально установленный закон, характеризующий математические способности человека и дающий единственную и окончательную формализацию понятия алгоритма.

Тезис Чёрча. *Класс эффективно вычислимых функций совпадает с классом всех частично рекурсивных функций.*

Разъясним теперь практическую значимость тезиса Чёрча для математики. Наибольший интерес представляют следующие его аспекты.

Тезис Чёрча как определение алгоритмической неразрешимости.

Введем сначала некоторые новые понятия. *Характеристической функцией множества* $A \subset \mathbb{N}^n$ называется функция $\chi_A\colon \mathbb{N}^n \to \mathbb{N}$ такая, что

$$\chi_A(x) = \begin{cases} 0, & \text{если } x \in A, \\ 1, & \text{если } x \notin A. \end{cases}$$

Частичной характеристической функцией множества A называется функция

$$\tilde{\chi}_A(x) = \begin{cases} 0, & \text{если } x \in A, \\ \text{не определена}, & \text{если } x \notin A. \end{cases}$$

Множество $A \subset \mathbb{N}^n$ называется *разрешимым (рекурсивным)*, если его характеристическая функция χ_A эффективно вычислима (частично рекурсивна). В противном случае множество A называется *неразрешимым*.

Аналогичным образом определяются *характеристическая (частичная характеристическая) функция предиката* R и *рекурсивный предикат*.

Пусть имеется счетная последовательность математических задач $P_1, P_2, \ldots$, каждая из которых имеет ответ «да» или «нет». Предположим, что эта последовательность допускает задание в виде некоторого n-местного предиката $R \subset \mathbb{N}^n$. Это означает, что существует взаимно однозначное кодирование номеров и условий задач P_i наборами $(x_1, \ldots, x_n) \in \mathbb{N}^n$, при котором R истинен на $(x_1, \ldots, x_n)$ в том и только том случае, когда соответствующая набору $(x_1, \ldots, x_n)$ задача P_i имеет ответ «да». Такая последовательность $P = \{P_i\}$ называется массовой проблемой.

Массовая проблема P называется алгоритмически разрешимой, если соответствующий ей предикат R рекурсивен, и алгоритмически неразрешимой в противном случае.

Одним из наиболее известных примеров алгоритмически неразрешимой массовой проблемы, к которой сводится по суще-

ству все остальные известные к настоящему времени неразрешимые проблемы, является проблема остановки машины Тьюринга.

Теорема 2. *Не существует алгоритма, который по данной машине Тьюринга T и по данному $x \in \mathbb{N}$ позволяет определить, остановится ли со временем машина T, начав работать с левой единицы основного кода числа x.*

Тезис Чёрча как эвристический принцип.

Эффективная вычислимость многих частичных числовых функций интуитивно ясна из определенных неформальных рассмотрений. К таким функциям относится, например, функция $h(n)$, задающая n-й десятичный знак числа e, или же функция $p(n)$, задающая n-е простое число. Тезис Чёрча позволяет разбить процесс исследования таких функций на два этапа: 1) отыскание неформального решения с использованием любых интуитивных алгоритмов; 2) последующая формализация.

5. Рекурсивно перечислимые множества. Рассмотрим теперь множества (предикаты), являющиеся рекурсивными лишь наполовину.

Множество $A \subset \mathbb{N}^n$ называется *рекурсивно перечислимым*, если существует такая частично рекурсивная функция $f(x_1, \ldots, x_n)$, что $A = D(f)$. Предикат $R(x_1, \ldots, x_n)$ назовем *рекурсивно перечислимым*, если рекурсивно перечислимо множество наборов $(x_1, \ldots, x_n) \in \mathbb{N}^n$, на котором R истинен.

Легко видеть, что множество $A \subset \mathbb{N}^n$ рекурсивно перечислимо (предикат R рекурсивно перечислим) тогда и только тогда, когда частичная характеристическая функция множества A (предиката R) частично рекурсивна.

Из отрицательного решения проблемы остановки машины Тьюринга легко вытекает справедливость следующего утверждения.

Теорема 3. *Существуют рекурсивно перечислимые, но не рекурсивные множества (предикаты).*

6. Диофантовы множества и предикаты. Нетрудно видеть, что для установления алгоритмической неразрешимости 10-й проблемы Гильберта достаточно ограничиться рассмотрением решений $(x_1, \ldots, x_n)$ полиномиальных уравнений $P(x_1, \ldots, x_n) = 0$ с компонентами из $\mathbb{N}$.

Предикат $R(x_1, \ldots, x_n)$, определенный на наборах $(x_1, \ldots, x_n) \in \mathbb{N}$, называется *диофантовым*, если существует многочлен $P \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ такой, что

$$R(x_1, \ldots, x_n) \Leftrightarrow (\exists y_1, \ldots, y_m \in \mathbb{N})(P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0).$$

Множество A наборов $(x_1, \ldots, x_n) \in \mathbb{N}^n$ называется *диофантовым*, если диофантовым является n-местный предикат, истинный на $(x_1, \ldots, x_n) \in A$ и ложный на остальных наборах $(x_1, \ldots, x_n)$.

Из определения диофантова предиката и из тезиса Чёрча следует справедливость следующего факта.

Теорема 4. *Каждый диофантов предикат рекурсивно перечислим.*

Если бы 10-я проблема Гильберта решалась положительно, то каждое диофантово множество было бы рекурсивным. Поэтому для отрицательного решения этой проблемы достаточно показать, что существуют нерекурсивные диофантовы множества. Решение этой задачи было дано совместными усилиями М. Девиса, Х. Патнема, Дж. Робинсон и Ю. В. Матиясевича.

Теорема 5. *Класс диофантовых предикатов совпадает с классом рекурсивно перечислимых предикатов и класс диофантовых множеств совпадает с классом рекурсивно перечислимых множеств.*

7. Положительные аспекты отрицательного решения десятой проблемы Гильберта. Используя результат теоремы 5, легко установить существование диофантова уравнения $P(t, x, y_1, \ldots, y_m) = 0$, которое универсально в том смысле, что, полагая

$$A_t = \{x \in \mathbb{N} \mid (\exists y_1, \ldots y_m \in \mathbb{N})(P(t, x, y_1, \ldots, y_m) = 0\},$$

получаем последовательность $\{A_t\}$ всех рекурсивно перечислимых подмножеств множества $\mathbb{N}$.

Ю. В. Матиясевич установил существование универсального многочлена $P(t, x, y_1, \ldots, y_m)$ с $m = 9$. Степень этого многочлена по оценке Дж. Джоунза имеет порядок $1{,}6 \cdot 10^{45}$. Отсюда следует, что 10-я проблема Гильберта заведомо не разрешима для диофантовых уравнений с 9 и более неизвестными. Точный минимум для m неизвестен, хотя ввиду наших предыдущих рассмотрений чрезвычайно интересен.

Каждое диофантово множество $A \subset \mathbb{N}$ может быть представлено как множество неотрицательных значений некоторого многочлена. В частности, таким свойством обладает множество простых чисел, представимое многочленом степени 25 от 26 переменных, последовательность

$$1,\ 2^2,\ 3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}\ (n \text{ раз}),\ \ldots,$$

множество неполных частных чисел $\sqrt[3]{2}$, e, π и т. д. (заметим, что для $\sqrt[3]{2}$ до сих пор не известно, конечно это множество или нет).

Из отрицательного решения 10-й проблемы Гильберта легко следует неразрешимость Entscheidungsproblem Гильберта. Более того, поскольку введенная Геделем теория нумераций в принципе сводит синтаксис формальных языков к арифметике, то в некотором смысле «почти вся математика» сводится к теории диофантовых уравнений (см. [81d, гл. 4]).

СПИСОК ЛИТЕРАТУРЫ

1. Айерлэнд, Роузен (Ireland K., Rosen M.)
Классическое введение в современную теорию чисел.— М.: Мир, 1987.
2. Акс, Кочен (Ax J., Kochen S.)
I — Diophantine problems over local fields // Amer. J. Math.— 1965.— V. 87.— P. 605—630; II — A complete set of axioms for p-adic number theory // Amer. J. Math.— 1965.— V. 87.— P. 631—648; III — Decidable fields // Ann. Math.— 1966.— V. 83.— P. 437—456.
3. Аладов Н. С.
О распределении квадратичных вычетов и квадратичных невычетов простого числа p в ряду 1, 2, ..., $p-1$ // Мат. сб.— 1896.— Т. 18, вып. 1.— С. 61—75.
4. Аракелов С. Ю.
a) Теория пересечений дивизоров на арифметической поверхности // Изв. АН СССР. Сер. мат.— 1974.— Т. 38, № 6.— С. 1179—1192.
b) Theory of intersection in the arithmetic surface // Proc. Intern. Congress of Math.— Vancouver.— 1974.— P. 405—408.
5. Артин Е. (Artin E.)
a) Quadratische Körper im Gebiete der höhern Kongruenzen, I, II // Math. Zeitschr.— 1924.— Bd 19.— S. 153—246.
b) Über die Zerlegung definite Funktionen in Quadrate // Hamb. Abh.— 1927.— V. 5.— S. 100—115.
(Collected papers of Emil Artin.— Reading, Mass.; London: Addison-Wesley, 1965.— P. 273—288).
6. Артин М. (Artin M.)
Grothendieck topologies // Harvard Math. Dept. Lecture Notes.— 1962.
7. Артин М., Гротендик, Вердье (Artin M., Grothendiek A., Verdier J. L.)
Théorie des Topos et Cohomologie Étale des Schémas // Lecture Notes in Math.— Heidelberg: Springer-Verlag, 1972—1973.— V. 269, 270, 305.
8. Атья, Макдональд (Atiyah M. F., Macdonald I. G.)
Введение в коммутативную алгебру.— М.: Мир, 1972.
9. Башмакова И. Г.
Диофант и диофантовы уравнения.— М.: Наука, 1972.
10. Бейкер (Baker A.)
a) Linear form in the logarithms of algebraic numbers // Mathematika.— 1966.— V. 13.— P. 204—216; 1967.— V. 14.— P. 102—107, 220—228; 1968.— V. 15.— P. 204—216.
b) Simultaneous rational approximations to certain algebraic numbers // Proc. Cambr. Philos. Soc.— 1967.— V. 63.— P. 693—702.
c) Contributions to the theory of Diophantine equations. II. The Diophantine equation $y^2 = x^3 + k$ // Phil. Trans. Roy. Soc. London.— Ser. A.— 1967—1968.— V. 263, № 1139.— P. 193—208.
d) Bounds for the solutions of the hyperelliptic equation // Proc. Cambr. Philos. Soc.— 1969.— V. 65.— P. 439—444.
e) Transcendental number theory.— London: New York: Cambr. Univ. Press. 1975.
11. Бейкер, Коутес (Baker A., Coates J.)
Integer points on curves of genus 1 // Proc. Cambr. Philos. Soc.— 1970.— V. 67.— P. 592—602.
12. Белл, Сломсон (Bell J. L., Slomson A. B.)
Models and Ultraproducts.— Amsterdam: North-Holland, 1969.

13. Берджесс (Burgess D. A.)
The distribution of quadratic residues and non-residues // Mathematika.— 1957.— V. 4.— P. 106—112.
14. Берч (Birch B. J.)
Forms in many variables // Proc. Roy. Soc. London.— Ser. A.— 1962.— V. 265.— P. 245—264.
15. Берч, Суиннертон-Дайер (Birch B., Swinnerton-Dayer H. P. F.)
Notes on elliptic curves. II // J. reine und angew. Math.— 1965.— Bd 218.— S. 79—108.
16. Бомбьери (Bombieri E.)
a) On exponential sums in finite fields // Amer. J. Math.— 1966.— V. 88, № 1.— P. 71—105; перевод: // Математика: Сб. пер.— М.: Мир, 1968.— Т. 12 : 2.— С. 58—87.
b) Counting points on curves over finite fields (d'aprés S. A. Stepanov).— Sém. Bourbaki.— 1973.— № 403.— P. 1—8.
c) Hilbert's 8th problem: An analogue // Proc. Symp. Pure Math.— 1976.— V. 28, p. 1.— P. 269—274.
17. Бомбьери, Дэвенпорт (Bombieri E., Davenport H.)
On two problems of Mordell // Amer. J. Math.— 1966.— V. 88, № 1.— P. 61—70; перевод: // Математика: Сб. пер.— М.: Мир, 1968.— Т. 12 : 2.— С. 49—57.
18. Бомбьери, Шмидт (Bombieri E., Schmidt W. M.)
On Thue's equation // Invent. Math.— 1987.— V. 88, № 1.— P. 69—81.
19. Боревич З. И., Шафаревич И. Р.
Теория чисел.— М.: Наука, 1985.
20. Боуз, Чоула (Bose R. C., Chowla S.)
Theorems in the additive theory of numbers // Comment. Math. Helv.— 1962.— V. 37.— P. 141—147.
21. Бурбаки Н. (Bourbaki N.)
Алгебра. Многочлены и поля. Упорядоченные группы.— М.: Наука, 1965.
22. Варнинг (Warning E.)
Bemerkung zur vorstehenden Arbeit von Herrn Chevalley // Abh. Math. Sem. Univ. Hamburg.— 1935.— Bd 11.— S. 76—83.
23. Вейль А. (Weil A.)
a) L'arithmétique sur les courbes algébriques // Acta Math.— 1929.— T. 52.— P. 281—315.
b) Sur un théoréme de Mordell // Bull. Sci. Math. (2).— 1930.— T. 54.— P. 182—191.
c) Foundations of Algebraic Geometry.— New York: Amer. Math. Soc. Colloquium Publ., 1946.— № 29; revised and enlarged edition 1962.
d) Sur les courbes algébriques et les variétes qui s'en déduisent.— Paris: Hermann, 1948.— (Actualités de Sciences Industrielles. № 1041).
e) On some exponential sums // Proc. Nat. Acad. Sci. USA.— 1948.— V. 34.— P. 204—207.
f) Variétés Abéliennes et Courbes Algébriques.— Paris: Hermann, 1948.
g) Number of solutions of equations in finite fields // Bull. Amer. Math. Soc.— 1949.— V. 55.— P. 497—508.
h) Number theory.— Boston; Basel; Stuttgart: Birkhäuser, 1983.
24. Вейль Г. (Weyl H.)
Алгебраическая теория чисел.— М.: ИЛ, 1947.
25. Венков Б. А.
Элементарная теория чисел.— М.; Л.: ОНТИ, 1937.
26. Виноградов А. И., Линник Ю. В.
Гиперэллиптические кривые и наименьший простой квадратичный вычет // ДАН СССР.— 1966.— Т. 168, № 2.— С. 259—261.
27. Виноградов И. М.
a) Избранные труды.— М., Л.: Изд-во АН СССР, 1952.

b) К вопросу о верхней границе для $G(n)$ // Изв. АН СССР. Сер. мат.— 1959.— Т. 23, № 5.— С. 637—642.
c) Метод тригонометрических сумм в теории чисел.— М.: Наука, 1971.
d) Основы теории чисел.— М.: Наука, 1972.
28. Вон (Vaughan R. C.)
Метод Харди — Литтлвуда.— М.: Мир, 1985.
29. Вороной Г. Ф.
О целых алгебраических числах, зависящих от корня уравнения третьей степени // Собр. соч.— Киев: — Изд-во АН УССР, 1952.— Т. 1.— С. 25—195.
30. Гаусс (Gauss C. F.)
a) Disquisitiones Arithmeticae.— Leipzig: Verlag Fischer, 1801.
b) Werke.— Göttingen: Königlische Gesellschaft der Wissenshaft, 1863—1933, Bd X, Teil. 1.— C. 571.
c) Труды по теории чисел.— М.: Изд-во АН СССР, 1959.
31. Гельфонд А. О.
a) Аппроксимация алгебраических иррациональностей и их логарифмов // Вестн. МГУ. Сер. 1, Математика, механика.— 1948.— Т. 9.— С. 3—25.
b) Трансцендентные и алгебраические числа.— М.: Гостехиздат, 1952.
32. Гильберт (Hilbert D.)
a) Über die vollen Invariantensysteme // Math. Ann.— 1893.— Bd 42.— S. 313—373.
b) Mathematische Probleme // Nachr. Acad. Wiss. Göttingen, Math.— Phys. Kl.— 1900.— S. 253—297; перевод: Проблемы Гильберта.— М.: Наука, 1969.
33. Гриффитс, Харрис (Griffiths Ph., Harris J.)
Принципы алгебраической геометрии.— М.: Мир, 1982.— Т. 1, 2.
34. Гросс, Загье (Gross B. h., Zagier D. B.)
Heegner points and derivatives of L-series // Invent. Math.— 1986.— V. 84, № 2.— P. 225—320.
35. Гротендик (Grothendieck A.)
a) The cohomology theory of abstract algebraic varieties // Proc. Intern. Congress of Math.— Edinburgh.— 1958.— P. 103—118; перевод: Международный математический конгресс в Эдинбурге.— М.: Физматгиз, 1962.— С. 116—137.
b) Formule de Lefschetz et rationalité des fonctions L // Séminaire Bourbaki.— 1965.— № 279.
36. Грюневальд, Циммерт (Grunewald F. J., Zimmert R.)
Über einige rationale elliptische Kurven mit freiem Rang $\geqslant 8$ // J. reine und angew. Math.— 1977.— Bd 296.— S. 100—107.
37. Гупта (Gupta R.)
Fields of division points of elliptic curves related to Coates-Wiles.— Ph. D. Thesis.— M. I. T., 1983.
38. Гурвиц (Hurwitz A.)
Über ternäre diophantische Gleidhung dritten Grades // Vierteljahrschrift d. Naturf. Ges. Zürich.— 1917.— Bd 62.— S. 207—229.
39. Дворк (Dwork B.)
a) On the rationality of the zeta function of an algebraic variety // Amer. J. Math.— 1960.— V. 82.— P. 631—648; перевод: // Математика. Сб. пер.— М.: Мир, 1961.— Т. 5 : 6.— С. 55—72.
b) On the zeta function of a hypersurface // Publ. Math. I. H. E. S.— 1962.— V. 12.— P. 5—68.
c) On the zeta function of a hypersurface. II // Ann. of Math. Ser. 2.— 1964.— V. 80.— P. 227—299.
40. Девис (Davis M.)
a) Computability and Unsolvability.— New York: McGraw-Hill, 1958.

b) Прикладной нестандартный анализ.— М.: Мир, 1980.
41. Девис М., Матиясевич Ю. В., Робинсон Дж. (Davis M., Matijasevic Yu., Robinson J.)
Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution // Proc. Symp. Pure Math.— 1976.— V. 28.— P. 323—378.
42. Делинь (Deligne P.)
a) La conjecture de Weil. I // Publ. Math. I. H. E. S.— 1974.— V. 43.— P. 273—307; перевод: // УМН.— 1976.— Т. 30, вып. 5(135).— С. 159—190.
b) La conjecture de Weil. II // Publ. Math. I. H. E. S.— 1980.— V. 52.— P. 137—252.
c) Cohomologie Etale // Lecture Notes in Math.— Heidelberg: Springer-Verlag, 1977.— V. 569.
43. Делоне Б. Н., Фаддеев Д. К.
Теория иррациональностей третьей степени // Тр. МИАН СССР.— 1940.— Т. 11.— С. 1—340.
44. Диксон (Dickson L. E.)
History of the theory of numbers. I. Divisibility and primality; II. Diophantine analysis; III. Quadratic and higher forms.— New York: Chelsea Publ., 1966.
45. Диофант Александрийский
Арифметика и книга о многоугольных числах.— М.: Наука, 1974.
46. Дойринг (Deuring M.)
a) The zeta functions of algebraic curves and varieties // J. Indian Math. Soc. (N. S.).— 1956.— V. 20.— P. 89—101.
b) Lectures on the Theory of Algebraic Functions of one variable // Lecture Not. Math.— 1973.— № 314. Berlin; New York: Springer-Verlag.
47. Дубровин Б. А., Новиков С. П., Фоменко А. Т.
Современная геометрия. Методы теории гомологий.— М.: Наука, 1984.
48. Дэвенпорт (Davenport H.)
a) On the distribution of quadratic residues (mod p) // J. London Math. Soc.— 1931.— V. 6.— P. 49—54.
b) On the distribution l-th power residues (mod p). II // J. London Math. Soc.— 1932.— V. 7.— P. 117—121.
c) On the distribution of quadratic residues (mod p) // J. London Math. Soc.— 1933.— V. 8.— P. 46—52.
d) On some infinite series involving arithmetical functions. II // Quart. J. Math. Oxford. Ser. 8.— 1937.— V. 32.— P. 313—320.
e) Note on a result of Siegel // Acta Arithm.— 1937.— V. 2.— P. 262—265.
f) Мультипликативная теория чисел.— М.: Наука, 1971.
49. Дэвенпорт, Эрдеш (Davenport H., Erdös P.)
The distribution of quadratic and higher residues // Publ. Math., Debrecen.— 1952.— V. 2.— P. 252—265.
50. Ершов Ю. Л.
a) Об элементарных теориях максимальных нормированных полей. II, III // Алгебра и логика.— 1966.— Т. 5, № 1.— С. 8—40; 1967.— Т. 6, № 3.— С. 33—39.
b) Об элементарных теориях максимальных полей // ДАН СССР.— 1965.— Т. 165, № 1.— С. 24—26.
c) Теория нумераций.— М.: Наука, 1977.
51. Ершов Ю. Л., Палютин Е. А.
Математическая логика.— М.: Наука, 1987.
52. Зарисски, й, Самюэль (Zariski O., Samuel P.)
Коммутативная алгебра.— М.: ИЛ, 1963.
53. Зархин Ю. Г.
a) Изогении абелевых многообразий над полями конечной характеристики // Мат. сб.— 1974.— Т. 95, № 3.— С. 461—470.

b) Эндоморфизмы абелевых многообразий над полями конечной характеристики // Изв. АН СССР. Сер. мат.— 1975.— Т. 39, № 2.— С. 272—277.

54. Зигель (Siegel C. L.)
a) Approximation algebraischer Zahlen // Math. Zeitschr.— 1921.— Bd 10.— S. 173—213.
b) Über Näherungswerte algebraischer Zahlen // Math. Ann.— 1921.— Bd 84.— S. 80—89.
c) The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$ // J. London Math. Soc.— 1926.— V. 1.— P. 66—68.
d) Über einige Anwendungen Diophantischer Approximationen // Abhandl. Preuss Acad. Wiss. Phys.— Math. Kl.— 1929.— Bd 1.— S. 41—69; то же: // Ges. Abhandl.— Berlin; New York: Springer-Verlag, 1966.— Bd 1.— S. 209—266.
e) Zur Theorie der quadratischen Formen // Nachr. Akad. Wiss., Göttingen.— 1972.— S. 21—46; то же: // Ges. Abhandl.— Berlin; New York: Springer-Verlag.— 1966.— Bd 4.— S. 224—249.

55. Ихара (Ihara Y.)
a) Hecke polynomials as congruence zeta functions in elliptic modular case // Ann. of Math. Ser. 2.— 1967.— V. 85.— P. 267—295.
b) On congruence monodromy problems I. II // Lect. Notes; Univ. of Tokyo, 1968—1969; перевод: // Математика: Сб. пер.— М.: Мир, 1970.— Т. 14 : 3.— С. 40—48; Т. 14 : 4.— С. 48—77; Т. 14 : 5.— С. 62—101; 1972.— Т. 16 : 3.— С. 54—96; Т. 16 : 4.— С. 50—71; Т. 16 : 5.— С. 42—104.

56. Карацуба А. А.
Суммы характеров и первообразные корни в конечных полях // ДАН СССР.— 1968.—Т. 180, № 6.— С. 1287—1289.

57. Карлиц (Carlitz L.)
Kloosterman sums and finite field extensions // Acta Arithm.— 1969.— V. 16, № 2.— P. 179—193.

58. Карлиц, Учияма (Carlitz L., Uchiyama S.)
Bounds for exponential sums // Duke Math. J.— 1957.— V. 24.— P. 179—193.

59. Касселс (Cassels J. W. S.)
a) Введение в теорию диофантовых приближений.— М.: ИЛ, 1961.
b) Введение в геометрию чисел.— М.: Мир, 1965.
c) Diophantine equations with special reference to elliptic curves // J. London Math. Soc.— 1966.— V. 41.— P. 193—291; перевод: // Математика: Сб. пер.— М.: Мир, 1968.—Т. 12 : 1.— С. 113—160; Т. 12 : 2.— С. 3—48.

60. Катц (Katz N. M.)
a) Travaux de Dwork // Séminaire Bourbaki.— 1971—1972.— V. 24.— P. 167—200; Lecture Notes in Math.— Berlin: Springer, 1973.— V. 317; перевод: // Математика: Сб. пер.— М.: Мир, 1974.— Т. 18 : 6.— С. 3—19.
b) An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields // Proc. Symp. Pure Math.— 1976.— V. 28, p. 1.— P. 275—305.
c) Sommes exponentielles // Astérisque-79. Soc. Math. de France.— Paris, 1980.

61. Коблиц (Koblitz N.)
p-адические числа, p-адический анализ и дзета-функции.— М.: Мир, 1982.

62. Колывагин В. А.
a) Конечность $E(\mathbb{Q})$ и Ш$(E, \mathbb{Q})$ для подкласса кривых Вейля // Изв. АН СССР. Сер. мат.— 1988.— Т. 52, № 3.— С. 522—540.

b) О группах Морделла — Вейля и Шафаревича — Тейта для эллиптических кривых Вейля // Изв. АН СССР. Сер. мат.— 1988.— Т. 52, № 6.— С. 1154—1180.

63. Коробов Н. М.
Оценка суммы символов Лежандра.— ДАН СССР.— 1971.— Т. 196, № 4.— С. 764—767.

64. Коутес (Coates J.)
An effective p-adic analogue of a theorem of Thue. I; II. The greatest prime factor of a binary form; III. The Diophantine equation $y^2 = x^3 + k$ // Acta Arithmetica.— 1969.— V. 15.— P. 279—305; 1970.— V. 16.— P. 399—412, 425—435.

65. Коутес, Уайлс (Coates J., Wiles A.)
On the conjecture of Birch and Swinnerton — Dyer // Invent. Math.— 1977.— V. 39, № 3.— P. 223—251.

66. Куга, Шимура (Kuga M., Schimura G.)
On the zeta function of a fibre variety whose fibres are abelian varieties // Ann. of Math. Ser. 2.— 1965.— V. 82.— P. 478—539; перевод: // Математика. Сб. пер.— М.: Мир, 1969.— Т. 11 : 5.— С. 21—87.

67. Лагранж (Lagrange I. L.)
Démonstration d'un théoreme d'arithmétique // Oeuvres de Lagrange.— Paris: Ganthier-Villars, 1896.— T. 3.— P. 189.

68. Левек (Le Veque W. J.)
a) Topics in Number Theory.— Reading, Mass.: Addison-Wesley, 1956.— V. 1, 2.
b) Rational points on curves of genus greater than 1 // J. reine und angew. Math.— 1961.— Bd 206.— S. 45—52.

69. Лейбниц (Leibniz C. W.)
Избранные отрывки из математических сочинений // УМН.— 1948.— Т. 2, вып. 1(23).— С. 165—204.

70. Ленг (Lang S.)
a) Abelian varieties.— New York: Interscience Publishers, Inc., 1959.
b) Integral points on curves // Publ. Math. I. H. E. S.— 1960.— P. 27—43.
c) Report on diophantine approximations // Bull. Soc. Math. France.— 1965.— T. 93.— P. 117—192.
d) Алгебра.— М.: Мир, 1968.
e) Введение в алгебраические и абелевы функции.— М.: Мир, 1976.
f) Elliptic Curves and Diophantine Analysis.— Berlin; New York: Springer-Verlag, 1978.
g) Эллиптические функции.— М.: Наука, 1984.
h) Основы диофантовой геометрии.— М.: Мир, 1986.

71. Ленг, Вейль (Lang S., Weil A.)
Number of points of varieties in finite fields // Amer. J. Math.— 1954.— V. 76, № 4.— P. 819—827.

72. Лидл, Нидеррейтер (Lidl R., Hiederreiter H.)
Конечные поля. I; II.— М.: Мир, 1988.

73. Линник Ю. В.
a) Большое решето.— ДАН СССР.— 1941.— Т. 30, № 4.— С. 290—292; см. также: // Избранные труды: Теория чисел. Эргодический метод и L-функции.— М.; Л.: Наука, 1979.— С. 293—296.
b) Замечание о наименьшем квадратичном невычете // ДАН СССР.— 1942.— Т. 30, № 4—5.— С. 131—132; см. также: // Избранные труды: Теория чисел. Эргодический метод и L-функции.— М.; Л.: Наука, 1979.— С. 296—297.
c) On the least prime in an arithmetic progession. I. The basic theorem // Мат. сб.— 1944.— Т. 15, № 2.— С. 139—178; II. The Deuring — Heilbronn phenomenon // Мат. сб.— 1944.— Т. 15, № 3.— С. 347—368.

см. также: // Избранные труды: Теория чисел. Эргодический метод и L-функции.— М.; Л.: Наука, 1979.— С. 336—399.

74. Линник Ю. В., Реньи А.
О некоторых гипотезах теории характеров Дирихле // Изв. АН СССР. Сер. мат.— 1947.— Т. 11.— С. 539—546; см. также: Линник Ю. В. Избранные труды: Теория чисел. L-функции и дисперсионный метод.— М.; Л.: Наука, 1980.— С. 30—37.
75. Лиувилль (Liouville J.)
Sur des classes tres étendues de quantités dont la valeur n'est ni algébrique, ni même reducible à des irrationneles algébriques // C. R. Acad. Sci. Paris.— 1844.— T. 18.— P. 883—885, 910—911.
76. Лось (Łoś J.)
Quelques remarques, théoreme et problém sur les classes définisable d'algébres // Mathematical Interpretation of Formal System.— Amsterdam: North-Holland, 1955.— P. 98—113.
77. Мазур (Mazur B.)
a) Rational points on modular curves // Lecture Notes in Math.— Berlin: Springer, 1977.— V. 601.
b) Modular curves and Eisenstein ideal // Publ. Math. I. H. E. S.— 1977.— V. 47.— P. 33—186.
c) Rational isogenies of prime degree // Invent. Math.— 1978.— V. 2.— P. 129—162.
d) Modular Curves and Arithmetic // Proc. Intern. Congr. of Math.— Warszawa.— 1983.— V. 1.— P. 185—211.
e) Arithmetic on curves // Bull. Amer. Math. Soc.— 1986.— V. 14, № 2.— P. 207—259.
78. Майерсон (Myerson G.)
The distribution of rational points on varieties defined over a finite field // Mathematika.— 1981.— V. 28, № 2.— P. 153—159.
79. Малер (Mahler K.)
a) Über die rationalen Punkte auf Kurven von Geschlecht Eins // J. reine und angew. Math.— 1934.— Bd 170.— S. 168—178.
b) A remark on Siegel's theorem on algebraic curves // Mathematika.— 1955.— V. 2.— P. 116—127.
c) Lectures on diophantine approximation.— Notre Dame: Notre Dame Univ. Press.— 1961.
80. Мальцев А. И.
Алгоритмы и рекурсивные функции.— М. Наука, 1986.
81. Манин Ю. И.
a) О сравнениях третьей степени по простому модулю // Изв. АН СССР. Сер. мат.— 1956.— Т. 20, № 5.— С. 673—678.
b) A course in mathematical logic.— New York; Springer-Verlag, 1977.
c) Доказуемое и недоказуемое.— М.: Сов. радио, 1979.
d) Вычислимое и невычислимое.— М.: Сов. радио, 1980.
82. Матиясевич Ю. В.
a) Диофантовость перечислимых множеств // ДАН СССР.— 1970.— Т. 191, № 2.— С. 279—282.
b) Диофантовы множества // УМН.— 1972.— Т. 27, вып. 5.— С. 185—222.
83. Маттук А., Тейт Дж. (Mattuck A., Tate J. T.)
On the inequality of Castelnuovo — Severi // Abhandl. Math. Sem. Univ. Hamburg.— 1958.— Bd 22.— P. 295—299; перевод: // Математика: Сб. пер.— М.: Мир, 1960.— Т. 4 : 2.— С. 25—29.
84. Мацумура (Matsumura H.)
Commutative Algebra.— New York: W. A. Benjamin Co., 1970.
85. Местр (Mestre J.— F.)
Formules explicites et minorations de conducteurs de variétés algébriques // Compositio Math.— 1986.— V. 58, № 2.— P. 209—232.

86. Милн (Milne J. S.)
a) The Tate — Šafarevič group of a constant abelian variety // Invent. Math.— 1968.— V. 6.— P. 91—105.
b) Этальные когомологии.— М.: Мир, 1983.
87. Митькин Д. А.
Об элементарном доказательстве оценки А. Вейля для рациональных тригонометрических сумм с простым знаменателем. // Изв. вузов. Математика.— 1986.— Т. 6.— С. 14—17.
88. Монтгомери (Montgomery H. L.)
Мультипликативная теория чисел.— М.: Мир, 1974.
89. Морделл (Mordell L. J.)
a) Indeterminate equations of the third and fourth degrees // Quart. J. Pure and Appl. Math.— 1914.— V. 45.— P. 170—186.
b) On the rational solutions of the indeterminate equations of the 3rd and 4th degrees // Proc. Cambr. Phil. Soc.— 1922.— V. 21.— P. 179—192.
c) On a sum analogous to a Gauss's sum // Quart. J. Math.— 1932.— V. 1.— P. 161—167.
d) The number of solutions of some congruences in two variables // Math. Zeitschr.— 1933.— Bd 37.— P. 193—209.
e) On some arithmetical results in the geometry of numbers // Compositio Math.— 1934.— V. 1.— P. 248—253.
f) A chapter in the theory of numbers.— Cambr.: Univ. Press, 1947.
g) The infinity of rational solutions of $y^2 = x^3 + k$ // J. London Math. Soc.— 1966.— V. 41.— P. 523—525.
h) On the magnitude of the integer solutions of the equation $ax^2 + by^2 + cz^2 = 0$ // J. Number Theory.— 1968.— V. 1.— P. 1—3.
i) Diophantine equations.— London; New York: Academic Press, 1969.
90. Нагелль (Nagell T.)
Solution de quelques problém dans la théorie arithmetique des cubiques planes du premier genre // Vid. Akad. Skrifter Oslo.— 1935.— V. 1.
91. Неron (Neron A.)
Problémes arithmétiques et géometriques rattachés à la notion de rang d'une courbe algébriques dans un corps // Bull. Soc. Math. France.— 1952.— T. 80.— P. 101—166.
92. Нисневич Л. Б.
О числе точек алгебраического многообразия в простом конечном поле // ДАН СССР.— 1954.— Т. 99, № 1.— С. 17—20.
93. Новиков П. С.
a) Об алгоритмической неразрешимости проблемы тождества слов в теории групп // Тр. МИАН СССР.— 1955.— Т. 44.— С. 1—144.
b) Элементы математической логики.— М.: Наука, 1973.
94. Огг (Ogg A. P.)
Diophantine equations and modular forms // Bull. Amer. Math. Soc.— 1975.— V. 81.— P. 14—27.
95. Паршин А. Н.
a) Алгебраические кривые над функциональными полями. I // Изв. АН СССР. Сер. мат. 1968.— Т. 32, № 5.— С. 1191—1219.
b) Quelques conjectures de finitude en Géométrie Diophantine // Actes Congr. Intern. Math.— 1970.— Т. 1.— P. 467—471.
c) Модулярные соответствия, высоты и изогении абелевых многообразий // Тр. МИАН СССР.— 1973.— Т. 122.— С. 211—236.
96. Перельмутер Г. И.
a) О некоторых суммах с характерами // УМН.— 1963.— Т. 18, вып. 2.— С. 145—149.
b) Оценка суммы вдоль алгебраической кривой // Мат. заметки 1969.— Т. 5.— С. 373—380.

c) Оценка многократной суммы с символом Лежандра // Мат. заметки.— 1975.— Т. 18, № 3.— С. 421—427.
d) Оценка многократной суммы с символом Лежандра для многочлена нечетной степени // Мат. заметки.— 1976.— Т. 20, № 6.— С. 815—824.

97. Полиа (Polya G.)
a) Über die Verteilung der quadratischen Reste und Nichtreste // Nachr. Akad. Wiss. Göttingen. Math.— Phys. Kl.— 1918.— S. 21—29.
b) Zur arithmetischen Untersuchung der Polynome // Math. Zeitschr.— 1918.— Bd 1.— S. 143—148.

98. Постников А. Г.
Эргодические вопросы теории сравнений и теории диофантовых приближений // Тр. МИАН СССР.— 1966.— Т. 82.— С. 3—112.

99. Постникова Л. П.
Тригонометрические суммы и теория сравнений по простому модулю.— М. Изд-во МГПИ им. В. И. Ленина, 1973.

100. Пуанкаре (Poincaré H.)
Oeuvres de Henri Poincaré. T. 2.— Paris: Gauthier-Villars, 1916.

101. Раджвад (Rajwade A. R.)
Arithmetic on curves with complex multiplication *by* $\sqrt{-2}$ // Proc. Cambr. Phil. Soc.— 1968.— V. 64.— P. 659—672.

102. Риду (Ridout D.)
The *p*-adic generalization of the Thue — Siegel — Roth theorem // Mathematika.— 1958.— V. 5.— P. 40—48.

103. Риордан (Riordan J.)
Введение в комбинаторный анализ.— М.: ИЛ, 1963.

104. Робинсон (Robinson A.)
a) On ordered fields and definite functions // Math. Ann.— 1955.— V. 130.— P. 257—271.
b) Non-standard analysis // Proc. Roy. Acad. Amsterdam, Ser. A.— 1961.— V. 64.— P. 432—440.
c) Non-Standard Analysis.— Amsterdam: North-Holland, 1966. (Study in Logic and the Foundations of Math.)
d) Nonstandard theory of Dedekind rings // Indaq. Math.— 1967.— V. 29.— P. 444—452.

105. Робинсон А., Рокетт П. (Robinson A., Roquette P.)
On the finiteness theorem of Siegel and Mahler concerning Diophantine equations // J. Number Theory.— 1975.— V. 7.— P. 121—176.

106. Рокетт (Roquette P.)
a) Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkörpern beliebigen Geschlechts // J. reine und angew. Math.— 1953.— Bd 191.— S. 199—252.
b) On the division fields of an algebraic function field of one variable. An estimate for their degree of irrationality // Houston J. Math.— 1976.— V. 2, № 2.— P. 251—287.

107. Рот (Roth K. F.)
Rational approximations to algebraic numbers // Mathematika.— 1955.— V. 2.— P. 102—168.

108. Рубин (Rubin K.)
a) Congruences for special values of *L*-functions of elliptic curves with complex multiplication // Invent. Math.— 1983.— V. 71.— P. 339—364.
b) Tate — Schafarevich groups and *L*-functions of elliptic curves with complex multiplication // Invent. Math.— 1987.— V. 89, № 3.— P. 527—560.

109. Салье (Salié.)
Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl // Math. Nachr.— 1949.— Bd 3.— S. 7—8.

110. Серр (Serre J. P.)
a) Sur la topologie des variétés algébriques en caractéristique *p* // Symp. Intern. Topol. Algebr. Mexico.— 1958.— P. 24—53.
b) Rationalité des fonctions ζ des variétés algébriques (d'aprés B. Dwork) // Séminaire Bourbaki.— 1960.— T. 198.
c) Алгебраические группы и поля классов.— М.: Мир, 1968.
d) Majoration de sommes exponentielles // J. Arithm. de Caen.— 1976.— P. 111—126; Astérisque 41—42, Paris; Soc. Math. France, 1977.

111. Сильверман (Silverman J. H.)
a) Representation of integers by binary forms and the rank of the Mordell — Weil group // Invent. Math.— 1983.— V. 74.— P. 218—292.
b) The arithmetic of elliptic curves.— New York: Springer-Verlag.— 1986.

112. Сколем (Skolem T.)
a) Einige Sätze über *p*-adische Potenzreiben mit Anwendung auf gewisse exponentielle Gleihungen // Math. Ann.— 1935.— Bd 111.— S. 399—424.
b) Diophantische Gleichungen.— Berlin: Springer, 1938.— (Ergebniss d. Math u. Ihrer Grenzgebiete. Bd 5).

113. Справочная книга по математической логике/Под ред. Дж. Барвайса
a) Теория моделей.— М.: Наука, 1982.
b) Теория множеств.— М.: Наука, 1982.
c) Теория рекурсий.— М.: Наука, 1982.
d) Теория доказательств и конструктивная математика.— М.: Наука, 1983.

114. Спрингер (Springer G.)
Введение в теорию римановых поверхностей.— М.: ИЛ, 1960.

115. Спринджук В. Г.
a) Гиперэллиптическое диофантово уравнение и числа классов идеалов // Acta Arithm.— 1976.— V. 30, № 1.— P. 95—108.
b) Арифметическая структура целочисленных многочленов и числа классов идеалов // Тр. МИАН СССР.— 1977.— Т. 143.— С. 152—174.
c) Классические диофантовы уравнения от двух неизвестных.— М.: Наука, 1982.

116. Старк (Stark H.)
a) On the Riemann hypothesis in hyperelliptic function fields // Proc. Symp. Pure Math.— 1973.— V. 24.— P. 285—302.
b) Effective estimates of solutions of some Diophantine equations // Acta Arithm.— 1973.— V. 24, № 3.— P. 251—259.
c) The Coates — Wiles theorem revisited. Number theory related to Fermat's last theorem // Progres in Mathematics. Boston; Basel; Stuttgart: Birkhäuser, 1982.— V. 26.— P. 349—362.

117. Степанов С. А.
a) Аппроксимация алгебраического числа алгебраическими числами специального вида // Вестн. МГУ. Сер. 1, Математика, механика.— 1967.— № 6.— С. 78—86.
b) О числе точек гиперэллиптической кривой над простым конечным полем // Изв. АН СССР. Сер. мат.— 1969.— Т. 33, № 5.— С. 1171—1181.
c) Elementary method in the theory of congruences for a prime modulus // Acta Arithm.— 1970.— V. 17.— P. 231—247.
d) Об оценке рациональных тригонометрических сумм с простым знаменателем // Тр. МИАН СССР.— 1971.— Т. 112.— С. 346—371.
e) An elementary proof of the Hasse — Weil theorem for hyperelliptic curves // J. Number Theory.— 1972.— V. 4, № 2.— P. 118—143.
f) Сравнения с двумя неизвестными // Изв. АН СССР. Сер. мат.— 1972.— Т. 36, № 4.— С. 683—711.

g) Конструктивный метод в теории уравнений над конечными полями // Тр. МИАН СССР.— 1973.— Т. 132.— С. 237—246.
h) Рациональные точки алгебраических кривых над конечными полями // Актуальные проблемы аналитической теории чисел.— Минск: Наука и техника, 1974.— С. 223—243.
i) Elementary method in the theory of equations over finite fields // Proc. Intern. Congress of Math.— Vancouver, 1974.— P. 383—391.
j) Уравнения над конечными полями // Мат. заметки.— 1977.— Т. 21, № 2.— С. 271—279.
k) Об оценках снизу неполных сумм характеров от многочленов // Тр. МИАН СССР.— 1977.— Т. 143.— С. 175—177.
l) Диофантовы уравнения // Тр. МИАН СССР.— 1984.— Т. 168.— С. 31—45.

118. Стор, Волох (Stöhr K. O., Voloch J. F.)
Weierstrass points and curves over finite fields // Proc. London Math. Soc. (3).— 1986.— V. 52.— P. 1—19.

119. Суиннертон-Дайер (Swinnerton-Dyer H. P. F.)
a) Применение вычисления в теории полей классов.— Алгебраическая теория чисел/Под ред. Дж. Касселса, А. Фрёлиха.— М.: Мир: 1969.— С. 417—432.
b) Analytic theory of abelian varieties.— London; New York: Cambr. Univ. Press, 1974.

120. Тейт (Tate J.)
a) Алгебраические классы когомологий // УМН.— 1965.— Т. 20, вып. 6.— С. 27—40.
b) Endomorphisms of abelian varieties over finite fields // Invent. Math.— 1966.— V. 2.— P. 134—144; перевод: // Математика: Сб. пер.— М.: Мир.— Т. 12 : 6.— С. 31—40.
c) The arithmetic of elliptic curves // Invent. Math.— 1974.— V. 23.— P. 179—206.

121. Тейхмюллер (Teichmûller O.)
Differentialrechung bei Charakteristik p // J. reine und angew. Math.— 1936.— Bd 175.— S. 89—99.

122. Туэ (Thue A.)
Über Annäherungswerte algebraischer Zahlen // J. reine und angew. Math.— 1909.— Bd 135.— S. 284—305.

123. Уайтмен (Whiteman A. L.)
Cyclotomy and Jacobsthal sums // Amer. J. Math.— 1952.— V. 84.— P. 89—99.

124. Успенский В. А.
Что такое нестандартный анализ? — М.: Наука, 1987.

125. Фалтингс (Faltings G.)
Endlichkeitssätze fûr abelsche Varietäten ûber Zahlkörpern // Invent. Math.— 1983.— V. 73, № 3.— P. 349—366.

126. Фейс (Faith C.)
Алгебра: кольца, модули и категории.— М.: Мир, 1977.— Т. 1; 1979.— Т. 2.

127. Фельдман Н. И.
a) Оценка неполной линейной формы от некоторых алгебраических чисел // Мат. заметки.— 1970.— Т. 7, № 5.— С. 569—580.
b) Эффективное степенное усиление теоремы Лиувилля // Изв. АН СССР. Сер. мат.— 1971.— Т. 35, № 5.— С. 973—990.
c) Effective bounds of the solutions of certain Diophantine equations // J. Austral. Math. Soc. Ser. A.— 1979.— V. 28, № 2.— P. 129—135.
d) Приближения алгебраических чисел.— М.: Изд-во МГУ, 1981.
e) Седьмая проблема Гильберта.— М.: Изд-во МГУ, 1982.

128. Форстер (Forster O.)
Римановы поверхности.— М.: Мир, 1980.

129. Фрид, Джарден (Fried M. D., Jarden M.)
Field Arithmetic.— Berlin; Heidelberg; New York: Springer Verlag, 1986. (Ergebniss d. Math. u. Ihrer Grenzegebiete, 3 Folge. Bd 11).

130. Фридлендер В. Р.
О наименьших степенных невычетах // ДАН СССР.— 1949.— Т. 66.— С. 351—352.

131. Харди (Hardy G. H.)
Collected papers of G. H. Hardy (including joint papers with J. E. Littlewood and others).— Oxford: Clarendon Press, 1966.— V. 1.

132. Хартсхорн (Hartshorne R.)
Алгебраическая геометрия.— М.: Мир, 1981.

133. Хассе (Hasse H.)
a) Theorie der höheren Differentiable in einem algebraischen Funktionenkörper mit vollkommem Konstantenkörper bei beliebiger Charakteristik // J. reine und angew. Math.— 1936.— Bd 175.— S. 50—54.
b) Zur Theorie der abstrakten elliptischen Funktionenkörper I—III // J. reine und angew, Math.— 1936.— Bd 175.— S. 55—62; 69—88; 193—208.
c) Лекции по теории чисел.— М.: ИЛ, 1953.
d) La conjectura de Riemann para cuerpos de Functiones sobre cuerpos de constantes finitos.— Madrid: Univ. Madrid Publ. Fac. Ciencia, 1957.

134. Херглотц (Herglotz G.)
Zur letzten Eintragung im Gausschen Tagebuch // Ber. Math.— Ph. Kl.— Leipzig: Sächsischen Akad. Wiss, 1921.— Bd 73.— S. 271—276.

135. Хиз-Браун (Heath-Brown D. R.)
Fermat's last theorem for «almost all» exponents // Bull. London Math. Soc.— 1985.— V. 17, pt. 1, № 64.— P. 15—16.

136. Холл (Hall M.)
Теория групп.— М.: ИЛ, 1962.

137. Хольцер (Holzer L.)
Minimal solutions of diophantine equations // Can. J. Math.— 19[illegible]— V. 11.— P. 238—244.

138. Хопф (Hopf H.)
Über die Verteilung quadratischer Reste // Math. Zeitschr.— 1930.— Bd 32.— S. 222—231.

139. Хуа Ло-ген (Hua Loo-Keng)
Метод тригонометрических сумм и его применения в теории чисел.— М.: Мир, 1964.

140. Цейтен (Zeuthen H. G.)
История математики в древности и в средние века.— М.: ГОНТИ, 1938.

141. Циммер (Zimmer H. G.)
Computational Problems, Methods and Results in Algebraic Number Theory // Lecture Notes in Math.— V. 262.— Berlin; Heidelberg; New York: Springer-Verlag, 1972; перевод: // Математика: Сб. пер.— М.: Мир, 1976.— Т. 2.— С. 221—298.

142. Чандрасекхаран (Chandrasekharan K.)
a) Введение в аналитическую теорию чисел.— М.: Мир, 1974.
b) Арифметические функции.— М.: Наука, 1975.

143. Чебышев П. Л.
Теория сравнений.— С.-Питербург: Обществ. польза, 1879.

144. Шафаревич И. Р.
a) Поля алгебраических чисел // Proc. Intern. Congress of Math.— Stockholm, 1962.— P. 163—176.
b) Основы алгебраической геометрии.— М.: Наука, 1988.

145. Шевалле (Chevalley C.)
a) Démonstration d'une hypothèse de E. Artin // Abhandl. Math. Sem. Univ. Hamburg, 1935.— Bd 11.— S. 73—75.

b) Введение в теорию алгебраических функций от одной переменной.— М.: Физматгиз, 1959.
146. Шмидт (Schmidt W. M.)
a) Simultaneous approximation to algebraic numbers by rationals // Acta Math.— 1970.— V. 125.— P. 189—201.
b) Linear forms with algebraic coefficients. I // J. Number Theory.— 1971.— V. 3.— P. 253—277.
c) Linearformen mit algebraischen Koeffizienten. II // Math. Ann.— 1971.— Bd 191.— S. 1—20.
d) Approximation to algebraic numbers // L'Enseignement Math.— 1971.— T. 17, № 3—4.— P. 187—253.
e) Norm form equations // Ann. Math.— 1972.— V. 96.— P. 526—551.
f) Zur Methode von Stepanov // Acta Arithm.— 1973.— Bd 24, № 4.— S. 347—368.
g) A lower bound for the number of solutions of equations over finite fields // J. Number Theory.— 174.— V. 6.— P. 448—480.
h) Equations over finite fields. An elementary approach // Lecture Notes in Math. Berlin; Heidelberg; New York: Springer-Verlag, 1976.— V. 536.
i) Диофантовы приближения.— М.: Мир, 1983.
j) The density of integer points on homogeneous varieties // Acta Math.— 1985.— V. 154, № 3—4.— P. 243—296.
147. Шори, Тайдеман (Shorey T. N., Tijdeman R.)
Exponential Diophantine Equations.— Cambridge; New York: Cambr. Univ. Press, 1986.
148. Штикельбергер (Stickelberger L.)
Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper // Verhandl. Ersten Intern. Math. Kongress, Zûrich, 1897.— S. 182—193.
149. Эвертс (Evertse J.— H.)
Upper bounds for the number of solutions of diophantine equations // Math. Centrum Amsterdam.— 1983.— P. 173—196.
150. Эйхлер (Eichler M.)
a) Quadratische Formen und orthogonale Gruppen.— Berlin: Springer-Verlag, 1952.
b) Einfuhrung in die Theorie der algebraischen Zahlen und Funktionen.— Basel; Stuttgart: Birkhäuser, 1963.
151. Эллиот (Elliott P. D. T. A.)
a) Some notes on k-th power residues // Acta Arithm.— 1967—1968.— V. 14.— P. 153—162.
b) The distribution of primitive roots // Can. J. Math.— 1969.— V. 21.— P. 822—841.
152. Энкени (Ankeny N. C.)
The least quadratic non-residues // Ann. of Math.— 1952.— V. 55.— P. 65—72.
153. Эрдёш (Erdös P.)
Remarks on number theory. I // Mat. Lapok.— 1961.— V. 12.— P. 10—17.
154. Якобсталь (Jakobsthal E.)
Über die Darstellung der Primzahlen der Form $4n+1$ als Summe zweier Quadrate // J. reine und angew. Math.— 1907.— Bd 132.— S. 238—245.
155. Ясумото (Yasumoto M.)
Hilbert irreducibility sequences and nonstandard arithmetic // J. Number Theory.— 1987.— V. 26.— P. 274—285.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

S. A. STEPANOV

ARITHMETIC OF ALGEBRAIC CURVES

Monograph
Moscow, Nauka, Main Editorial Board
for Literature on Physics and Mathematics,
1991

Readership: Researches in the number theory, algebraic geometry and mathematical logic; undergraduates and students.

The book: This is a systematic presentation of the modern state, basic concepts and methods of the theory of diophantine equations.

Main attention is focused on the consideration of the case of equations in two variables.

The monograph may serve as an introduction to the theory of equations over finite and number fields, arithmetic theory of algebraic curves and nonstandard arithmetic.

Contents: Equations over finite fields. Distribution of quadratic residues and nonresidues. Algebraic functions and Riemann — Roch theorem. Rational points on algebraic curves. Integral points on curves and nonstandard arithmetic.

The author: Professor Sergei Stepanov. D. Sc. (Phys. & Math.), Winner of the USSR State Prize, Steklov Institute of Mathematics, USSR Academy of Sciences.

S. A. STEPANOV

ARITHMETIC OF ALGEBRAIC CURVES

The book contains a detailed exposition of the theory of Diophantine equations in two variables over finite and arbitrary number fields.

CONTENTS