Парадигма развития науки

Методологическое обеспечение

А. Е. Кононюк

ОБОБЩЕННАЯ ТЕОРИЯ МОДЕЛИРОВАНИЯ

Книга 2

Числа

количественные оценки параметров моделей

Киев
Освіта України
2012

УДК 51 (075.8)
ББК В161.я7
К 213

Рецензент: *Н.К.Печурин* - д-р техн. наук, проф. (Национальный авиационный университет).

Кононюк А. Е.
К65 Обобщенная теория моделирования. Числа (количественные оценки параметров моделей) К.2.
К.4:"Освіта України", 2012. - 548 с.
ISBN 978-966-7599-50-8

Настоящая работа является систематическим изложением обобщенной теории моделирования. Основное внимание уделяется идейным основам теории моделирования, их сравнительному анализу и примерам использования. Рассмотрен значительный круг задач моделирования — от общих задач моделирования до частных задач моделирования, а именно: моделирование объектов по выполняемым функциям, по составу, по структуре, по форме, по организации, по управлению. Обсуждается методика постановки и решения проблем моделирования. Рассматриваются средства математического описания объектов и процессов моделирования. Описываются системы автоматизированного моделирования.

Работа предназначена для магистров, аспирантов, докторантов, инженеров, экономистов, статистиков, вычислителей и всех тех, кто сталкивается с задачами моделирования, прежде всего, математического.

ББК В161.я7

ISBN 978-966-7599-50-8

Оглавление

Введение в теорию чисел как количественных оценок параметров моделей

Теория чисел, или **высшая арифметика** — раздел математики, изучающий целые числа и сходные объекты. В теории чисел в широком смысле рассматриваются как алгебраические, так и трансцендентные числа, а также функции различного происхождения, которые связаны с арифметикой целых чисел и их обобщений.

В исследованиях по теории чисел, наряду с элементарными и алгебраическими методами применяются геометрические и аналитические методы, а также метода теории вероятностей.

Элементарная теория чисел

В **элементарной теории чисел** целые числа изучаются без использования методов других разделов математики. Такие вопросы, как делимость целых чисел, алгоритм Евклида для вычисления наибольшего общего делителя и наименьшего общего кратного, разложение числа на простые множители, построение магических квадратов, совершенные числа, числа Фибоначчи, малая теорема Ферма, теорема Эйлера, задача о четырёх кубах относятся к этому разделу.

Аналитическая теория чисел

В **аналитической теории чисел** для вывода и доказательства утверждений о числах и числовых функциях используется мощный аппарат математического анализа. Первым шагом в этом направлении стал метод производящих функций, сформулированный Эйлером. Для определения количества целочисленных неотрицательных решений линейного уравнения вида

$$a_1 x_1 + ... + a_n x_n = N,$$

где $a_1, ..., a_n$ — натуральные числа,

Эйлер построил производяшую функцию, которая определяется как

$$F_i(z) = \sum_{k=0}^{\infty} z_i^a k$$

произведение сходящихся рядов (при $|z| < 1$) и является суммой членов геометрической прогрессии, при этом

$$F(z) = \sum_{N=0}^{\infty} l(N) z^N ,$$

где $l(N)$ — число решений изучаемого уравнения.

На основе этого метода был построен круговой метод Харди — Литлвуда.

В работе над квадратичным законом взаимности Гаусс рассмотрел

$$S(a) = \sum_{n=1}^{p} e^{2ian^2/p}$$

конечные суммы вида, которые могут быть представлены в виде суммы синусов и косинусов (по формуле Эйлера), из-за чего они являются частным случаем тригонометрических сумм. Метод тригонометрических сумм, позволяющий оценивать число решений тех или иных уравнений или систем уравнений в целых числах играет большую роль в аналитической теории чисел. Основы метода разработал и впервые применил к задачам теории чисел И. М. Виноградов.

Работая над доказательством теоремы Евклида о бесконечности простых чисел Эйлер рассмотрел произведение по всем простым числам и сформулировал тождество:

$$\Pi_p \left(1 - \frac{1}{p_s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

которое стало основанием для теорий дзета-функций. Наиболее известной и до сих пор не решённой проблемой аналитической теории чисел является доказательство гипотезы Римана о нулях дзета-функции, утверждающей, что все нетривиальные корни уравнения $\zeta(s) = 0$ лежат на так называемой *критической прямой* $\operatorname{Re} s = \frac{1}{2}$, где $\zeta(s)$ — дзета-функция Римана.

Для доказательства теоремы о бесконечности простых чисел в общем виде Дирихле использовал произведения по всем простым числам, аналогичные эйлерову произведению, и показал, что

$$\Pi_p \left(1 - \frac{\chi(p)}{p_s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

при этом функция $\chi(p)$, получившая название характер Дирихле, определена так, что удовлетворяет следующим условиям: она является периодической, вполне мультипликативной и не равна тождественно нулю. Характеры и ряды Дирихле нашли применение и в других разделах математики, в частности в алгебре, топологии и теории функций.

Чебышев показал, что число простых чисел, не превосходяших X, обозначенное как $\pi(X)$, стремится к бесконечности по следующему закону:

$$a\frac{X}{ln(X)} < \pi(X) < b\frac{X}{ln(X)},$$

где $a > 1/2ln2$ и $b < 2ln2$.

Другим направлением аналитической теории чисел является применение комплексного анализа в доказательстве теоремы о распределении простых чисел.

Алгебраическая теория чисел

В **алгебраической теории чисел** понятие числа расширяется, в качестве алгебраических чисел рассматривают корни многочленов с рациональными коэффициентами. При этом аналогом целых чисел выступают целые алгебраические числа, то есть корни унитарных многочленов с целыми коэффициентами. В отличие от целых чисел в кольце целых алгебраических чисел не обязательно выполняется свойство факториальности, то есть единственности разложения на простые множители.

Теория алгебаических чисел обязана своим появлением попыткам доказать теорему Ферма. Куммеру принадлежит равенство

$$x^n = z^n - y^n = \prod_{i=1}^{n}(z - a_i y),$$

где a_i — корни степени n из единицы.

Таким образом Куммер определил новые целые числа вида $z + a_i y$. Позднее Лиувилль показал, что если алгебраическое число является корнем уравнения степени n, то к нему нельзя подойти ближе чем на Q^{-n}, приближаясь дробями вида P/Q, где P и Q — целые взаимно простые числа.

После определения алгебраических и трансцендентных чисел в алгебраической теории чисел выделилось направление, которое занимается доказательством трансцендентности конкретных чисел, и направление, которое занимается алгебраическими числами и изучает степень их приближения рациональными и алгебраическими.

Алгебраическая теория чисел включает в себя такие разделы, как теорию дивизоров, теорию Галуа, теорию полей классов, дзета- и *L*-функции Дирихле, когомологии групп и многое другое.

Одним из основных приёмов является вложение поля алгебраических чисел в своё пополнение по какой-то из метрик — архимедовой (например, в поле вещественных или комплексных чисел) или неархимедовой (например, в поле *p*-адических чисел).

Теория чисел в древнем мире

В Древнем Египте математические операции проводились над целыми числами и аликвотными дробями. Математические папирусы содержат задачи с решениями и вспомогательные таблицы. Неизвестно ни одного бесспорного примера применения теории чисел в Древнем Египте, в отличие от более развитой алгебры. Ещё более широкое применение таблиц характерно для Вавилона, которые вслед за шумерами использовали шестидесятиричную систему счисления. Вавилонские клинописные математические тексты включают таблицы умножения и обратных чисел, квадратов и кубов чисел натурального ряда. В Вавилоне знали множество пифагоровых троек, для поиска которых, вероятно, пользовались неизвестным общим приёмом. Самой древней археологической находкой в истории арифметики является обломок глиняной таблички Плимптон, 322 (*англ.*), датируемый 1800 годами до нашей эры. Он содержит список Пифагоровых троек, то есть натуральных чисел (a, b, c) таких что $a^2 + b^2 = c^2$. В тройках встречаются пятизначные числа, да и их самих слишком много, чтобы предположить что они были получены механическим перебором вариантов.

Весомый вклад в становление теории чисел оказали пифагорейцы, Евклид и Диофант.

Пифагорейцы рассматривали только целые положительные числа и полагали число собранием единиц. Единицы были неделимы и расплогались в виде правильных геометрических тел. Пифагорейцам характерно определение «фигурных чисел» («треугольных», «квадратных» и других). Изучая свойства чисел, они разбили их на чётные и нечётные (как признак делимости на два), простые и составные. Вероятно именно пифагорейцы с помощью только признака делимости на два смолги доказать, что если $1 + 2 + ... + 2^n = p$ — простое число, то $2^n p$ — совершенное число. Доказательство изложено в Началах Евклида, только в 18 веке Эйлер доказал, что других чётных совершенных чисел не существует, а

вопрос о бесконечности числа совершенных чисел до сих пор не решён. Также пифагорейцы вывели формулу и нашли бесконечное множество целых решений уравнения $x^2 + y^2 = z^2$, так называемых пифагоровых троек.

Общая теория делимости появилась в 399 году до н. э. и принадлежит, по-видимому, Теэтету. Евклид посвятил ей книгу VII и часть книги IX Начал. В основе теории лежит алгоритм Евклида для нахождения общего наибольшего делителя двух чисел. Следствием алгоритма является возможность разложения любого числа на простые сомножители, а также единственность такого разложения. Закон однозначности разложения на простые множители является основой арифметики целых чисел.

VII, VIII и IX книги, входящие в Начала Евклида посвящены простым числам и делимости. В частности там описывается алгоритм нахождения наибольшего общего делителя двух чисел (алгоритм Евклида) и доказывается бесконечность множества простых чисел.

Диофант Александрийский, в отличие от предыдущих математиков Древней Греции, решал задачи классической алгебры описывая их геометрически. В своем труде «Арифметика», он перечисляет задачи по нахождению целочисленных решений для систем полиномальных уравнений (называемых сейчас диофантовыми). Работы Диофанта по решению неопределённых уравнений в рациональных числах стоят на стыке теории чисел и алгебраической геометрии. Он исследует уравнение второго порядка от двух переменных $F_2(x, y) = 0$, которое является уравнением конического сечения. Метод, с помощью которого Диофант находит рациональные точки кривой, если известна хоть одна такая, устанавливает, что кривая второго порядка либо содержит бесконечное множество точек, координаты которых выражаются как рациональные функции одного параметра, либо не содержит их вовсе. Для исследования уравнений третьего и четвёртого порядка применяются более сложные геометрические методы (построение касательной в рациональной точке, или прямой через две рациональные точки для поиска следующего пересечения).

Теория чисел в Средние века

Китайская теорема об остатках входила в качестве упражнения в трактат Сунь Цзы «Сунь Цзы Суань Цзин» (кит. упр. 孙子算经, пиньинь: *sūnzǐ suànjīng*). В его решении был опущен один из важных шагов, полное доказательство впервые получено Ариабхатой в VI веке н. э.

Индийские математики Ариабхата, Брахмагупта и Бхаскары решали диофантовы уравнения вида $ax + b = cy$ в целых числах. Кроме того, они решали в целых числах уравнения вида $ax^2 + b = y^2$, что было наивысшим достижением индийских математиков в области теории чисел. Впоследствии это уравнение и его частный случай при $b = 1$ привлекли внимание Ферма, Эйлера, Лагранжа. Предложенный Лагранжем метод нахождения решения был близок к индийскому.

Дальнейшее развитие теории чисел

Дальнейшее развитие теория чисел получила в работах Ферма, связанных с решением диофантовых уравнений и делимостью целых чисел. В частности, Ферма сформулировал теорему о том, что для любого простого p и целого a, $a^p - a$ делится на p, названную малой теоремой Ферма и, кроме того, сформулировал теорему о неразрешимости диофантового уравнения в целых числах, или Великую теорему Ферма. Обобщением малой теоремы и доказательством великой теоремы для частных случаев занимался в начале XVIII века Эйлер. Он же стал использовать для решения задач по теории чисел мощный аппарат математического анализа, сформулировав метод производяших функций, тождество Эйлера, а также задачи, связанные со сложением простых чисел.

В XIX веке над теорией чисел работали многие видные учёные. Гауссом была создана теория сравнений, с помощью которой доказан ряд теорем о простых числах, изучены свойства квадратичных вычетов и невычетов, включая квадратичный закон взаимности, в поисках доказательства которого Гаусс рассмотрел конечные ряды определённого вида, обобщённые впоследствии до тригонометрических сумм. Развивая работы Эйлера, Гаусс и Дирихле

создали теорию квадратичных форм. Кроме того, они сформулировали ряд задач о количестве целых точек в областях на плоскости, частные решения которых позволили доказать общую теорему о бесконечности числа простых точек в прогрессиях вида $nk + l$, где k и l взаимно просты. Дальнейшим изучением распределения простых чисел занимался Чебышев, который показал более точный, чем теорема Евклида, закон стремления к бесконечности числа простых чисел, доказал гипотезу Бертрана о существовании простого числа в интервале $(x, 2x), x \geq 2$, а также поставил задачу об оценке сверху наименьшего значения разности между соседними простыми числами (расширение вопроса о простых близнецах).

В начале XX века А. Н. Коркин, Е. И. Золотарёв и А. А. Марков продолжили работу над теорией квадратичных форм. Коркин и Золотарёв доказали теорему о переменных положительной кватернарной квадратичной формы, а Марков занимался изучением минимумов бинарных квадратичных форм положительного определителя. Формулы, сформулированные Дирихле для целых точек в областях на плоскости, нашли своё развитие в работах Г. Ф. Вороного, который в 1903 году определил порядок остаточного члена. В 1906 году метод был успешно перенесён на проблему Гаусса о числе целых точек в круге В. Серпиньским.

В 1909 году Д. Гильберт решил аддитивную проблему Варинга.

Э.Куммер, пытаясь доказать теорему Ферма, работал с алгебраическим числовым полем, для множества чисел которого он применил все четыре алгебраических операции и построил таким образом арифметику целых чисел алгебраического числового поля, порождённого a_i, ввёл понятие идеальных множителей и дал толчок к созданию алгебраической теории чисел. В 1844 году Ж.Лиувилль ввёл понятия алгебраических и трансцендентных чисел, сформулировав таким образом в математических терминах замечание Эйлера о том, что квадратные корни и логарифмы целых чисел имеют принципиальные различия. Лиувилль показал, что алгебраические числа плохо приближаются рациональными дробями. В конце XIX века над доказательством трансцендентности конкретных чисел работали такие математики как Шарль Эрмит, который в 1873 году доказал трансцендентность числа e, Ф.Линдеман, который в 1882 году доказал трансцендентность числа π. Другим направлением было изучение степени приближения алгебраических чисел рациональными

или алгебраическими. В нём работал Аксель Туэ, который в 1909 году доказал теорему, названную его именем.

Другим направлением работ явилось определение Риманом дзета-функции и доказательство того, что она аналитически продолжается на всю плоскость комплексного переменного и обладает рядом других свойств. Риман также высказал гипотезу о нулях дзета-функции. Работая над дзета-функциями, Ш. Ла Валле Пуссен и Жак Адамар сформулировали в 1896 году ассимптотический закон распределения простых чисел. Использованный ими метод получения ассимптотических формул, или метод комплексного интегрирования, стал широко использоваться в дальнейшем.

В первой половине XX века над проблемами теории чисел работали Герман Вейль, сформулировавший соотношение для равномерного распределения дробных долей целочисленных функций, Г.Харди и Дж. Литвуд, которые сформулировали круговой метод решения аддитивных задач, А. О. Гельфонд и Т. Гнейдер, которые решили 7-ю проблему Гильберта, К. Зигель, который доказал ряд теорем о трансцендентности значений функций, Б. Н. Делоне и Д. К. Фаддеев, которые занимались исследованием диофантова уравнения $x^3 - ay^3 = 1$, А.Сельберг, который работал в теории дзета-функции Римана.

Большой вклад в развитие теории чисел внёс И. М. Виноградов, доказавший неравенство о числе квадратичных вычетов и невычетов на отрезке, определивший метод тригонометрических сумм, который позволил упростить решение проблемы Варинга, а также решение ряда задач по распределению дробных долей функции, определению целых точек в области на плоскости и в пространстве, порядок роста дзета-функции в критической полосе. В задачах, связанных с тригонометрическими суммами, важным является как можно более точная оценка их модуля. Виноградов предложил два метода такой оценки. Кроме того, он вместе с учениками разработал ряд методов, которые позволяют решить задачи, выводимые из гипотезы Римана.

Многочисленные работы по теории чисел относятся ко второй половине XX века. Ю. В. Линник разработал дисперсионный метод, который позволил вывести ассимптотические формулы для проблемы Харди — Литлвуда и проблемы простых делителей Титчмарша.

Вместе с тем, в теории чисел существует большое количество открытых проблем.

1. Базовый класс чисел – натуральные числа

Объект любой природы можно охарактеризовать (описать) качественными и количественными признаками. Для количественной характеристики объектов используют числа.

— это абстракция, используемая для количественной характеристики и нумерации различных объектов, в том числе и объектов моделирования. Возникнув ещё в первобытном обществе из потребностей счёта, понятие числа изменялось и обогащалось и превратилось в важнейшее математическое понятие. Письменными знаками (символами) для записи чисел служат цифры.

1.1. Характеристика натуральных чисел

Начальным классом чисел является натуральный класс чисел. **Натуральные числа** — это числа, получаемые при естественном счёте. Множество натуральных чисел принято обозначать буквой $\mathbb{N}$. Т.е. $\mathbb{N} = \{1, 2, 3, ...\}$ (иногда к множеству натуральных чисел также относят ноль, т. е. $\mathbb{N} = \{0, 1, 2, 3, ...\}$). Натуральные числа замкнуты относительно сложения и умножения (но не вычитания или деления). Сложение и умножение натуральных чисел коммутативны и ассоциативны, а умножение натуральных чисел дистрибутивно относительно сложения и вычитания.

Как мы уже отмечали, натуральные числа можно использовать для счёта (одно яблоко, два яблока и т. п.).

Натуральные числа (естественные числа) — числа, возникающие естественным образом при счёте (как в смысле перечисления, так и в смысле исчисления).

Существуют два подхода к определению натуральных чисел — числа, используемые при:

- **перечислении (нумеровании) предметов** (*первый*, *второй*, *третий*, …);
- **обозначении количества предметов** (*нет предметов*, *один предмет*, *два предмета*, …). Данный подход принят в трудах Бурбаки, где натуральные числа определяются как мощности конечных множеств.

Отрицательные и нецелые (рациональные, вещественные, …) числа **натуральными не являются**.

Как мы уже говорили, множество всех натуральных чисел принято обозначать знаком $\mathbb{N}$. Множество натуральных чисел является бесконечным, так как для любого натурального числа найдётся большее его натуральное число.

1.1.1. Аксиомы Пеано

Множество $\mathbb{N}$ будем называть множеством натуральных чисел, если зафиксирован некоторый элемент $1 \in \mathbb{N}$ (единица) и функция $S\colon \mathbb{N} \to \mathbb{N}$ (функция следования) так, что выполнены следующие условия

1. $1 \in \mathbb{N}$ (1 является натуральным числом);
2. Если $x \in \mathbb{N}$, то $S(x) \in \mathbb{N}$ (число, следующее за натуральным, также является натуральным);
3. $\nexists x \in \mathbb{N}\ (S(x) = 1)$ (1 не следует ни за каким натуральным числом);
4. Если $S(b) = a$ и $S(c) = a$, тогда $b = c$ (если натуральное число *a* непосредственно следует как за числом *b*, так и за числом *c*, то *b*=*c*);
5. **Аксиома индукции**. Пусть $P(n)$ — некоторый одноместный предикат, зависящий от параметра — натурального числа *n*. Тогда:

если $P(1)$ и $\forall n\,(P(n) \Rightarrow P(S(n)))$, то $\forall n\ P(n)$ (если некоторое высказывание *P* верно для *n*=1 (*база индукции*) и для любого *n* при допущении, что верно $P(n)$, верно и $P(n+1)$ *(индукционное предположение)*, то $P(n)$ верно для любых натуральных *n*).

Перечисленные аксиомы отражают интуитивные представления о «натуральном ряде». Принципиальным фактом является то, что эти **аксиомы однозначно определяют натуральные числа** (категоричность системы аксиом Пеано). А именно, можно доказать, что если $(\mathbb{N}, 1, S)$ и $(\tilde{\mathbb{N}}, \tilde{1}, \tilde{S})$ — две модели для системы аксиом Пеано, то они необходимо изоморфны, то есть существует биекция $f: \mathbb{N} \to \tilde{\mathbb{N}}$ такая, что $f(1) = \tilde{1}$ и $f(S(x)) = \tilde{S}(f(x))$ для всех $x \in \mathbb{N}$. Поэтому, достаточно зафиксировать в качестве $\mathbb{N}$ какую-либо одну конкретную модель множества натуральных чисел, например, ту, что описана ниже.

1.1.2. Теоретико-множественное определение (Определение Фреге-Рассела)

Согласно теории множеств, единственным объектом конструирования любых математических систем является множество. Таким образом, и натуральные числа вводятся, исходя из понятия множества, по двум правилам:

- $0 = \varnothing$
- $S(n) = n \cup \{n\}$

Числа, заданные таким образом, называются **ординальными.**

Первые несколько ординальных чисел и соответствующие им натуральные числа:

- $0 = \varnothing$
- $1 = \{0\} = \{\varnothing\}$
- $2 = \{0, 1\} = \{\varnothing,\ \{\varnothing\}\}$

- $3 = \{0,1,2\} = \left\{\varnothing,\ \{\varnothing\},\ \left\{\varnothing,\ \{\varnothing\}\right\}\right\}$

Ноль как натуральное число

Иногда, в иностранной и переводной литературе, в первой и третьей аксиомах Пеано заменяют 1 на 0. В этом случае ноль считается натуральным числом. При определении через классы равномощных множеств 0 является натуральным числом по определению. Специально отбрасывать его было бы неестественно. Кроме того, это значительно усложнило бы дальнейшее построение и применение теории чисел, так как в большинстве конструкций ноль, как и пустое множество, не является чем-то выделенным. Одним из преимуществ натурального нуля является то, что при этом $\mathbb{N}$ образует полугруппу с единицей.

В русской литературе обычно ноль исключён из числа натуральных чисел $0 \notin \mathbb{N}$, а множество натуральных чисел с нулём обозначается как $\mathbb{N}_0$. Если в определение натуральных чисел включен ноль, то множество натуральных чисел записывается как $\mathbb{N}$, а без нуля как $\mathbb{N}^*$.

В международной математической литературе, с учётом сказанного выше и во избежание неоднозначностей, множество $\{1,2,\ldots\}$ обычно называют множеством положительных целых чисел и обозначают $\mathbb{Z}_+$. Множество $\{0,1,\ldots\}$ зачастую называют множеством неотрицательных целых чисел и обозначают $\mathbb{Z}_{\geqslant 0}$.

1.2. Операции над натуральными числами

1.2.1. Замкнутые операции над натуральными числами

К замкнутым операциям (операциям, не выводящим результат из множества натуральных чисел) над натуральными числами относятся следующие арифметические операции:

- **Сложение**. Слагаемое + Слагаемое = Сумма

- **Умножение**. Множитель * Множитель = Произведение
- **Возведение в степень** a^b, где a — основание степени и b — показатель степени. Если основание и показатель натуральны, то и результат будет являться натуральным числом.

Дополнительно рассматривают ещё две операции. С формальной точки зрения они не являются операциями над натуральными числами, так как не определены для **всех** пар чисел (иногда существуют, иногда нет).

- **Вычитание**. Уменьшаемое - Вычитаемое = Разность. При этом Уменьшаемое должно быть больше Вычитаемого (или равно ему, если считать 0 натуральным числом).
- **Деление**. Делимое / Делитель = (Частное, Остаток). Частное p и остаток r от деления a на b определяются так: $a = p * b + r$, причём $0 \leqslant r < b$. Заметим, что именно последнее условие запрещает деление на ноль, так как иначе a можно представить в виде $a = p * 0 + a$, то есть можно было бы считать частным 0, а остатком = a.

Следует заметить, что именно операции сложения и умножения являются основополагающими. В частности, **кольцо целых чисел определяется именно через бинарные операции сложения и умножения.**

1.2.2. Теоретико-множественные определения

Воспользуемся определением натуральных чисел как классов эквивалентности конечных множеств. Будем обозначать класс эквивалентности множества A относительно биекций как $[A]$. Тогда основные арифметические операции определяются следующим образом:

- $[A] + [B] = [A \sqcup B]$
- $[A] * [B] = [A \times B]$
- $[A]^{[B]} = [A^B]$

где $A \sqcup B$ — дизъюнктное объединение множеств, $B \times A$ — прямое произведение, A^B — множество отображений из B в A. Можно

показать, что полученные операции на классах введены корректно, то есть не зависят от выбора элементов классов, и совпадают с индуктивными определениями.

1.2.3. Основные свойства

1. Коммутативность сложения. $a+b=b+a$
2. Коммутативность умножения. $ab=ba$
3. Ассоциативность сложения. $(a+b)+c=a+(b+c)$
4. Ассоциативность умножения. $(ab)c=a(bc)$
5. Дистрибутивность умножения относительно сложения. $\begin{cases} a(b+c)=ab+ac \\ (b+c)a=ba+ca \end{cases}$

1.2.4. Алгебраическая структура

Сложение превращает множество натуральных чисел в полугруппу с единицей, роль единицы выполняет **0**. Умножение также превращает множество натуральных чисел в полугруппу с единицей, при этом единичным элементом является **1**. С помощью замыкания относительно операций сложения-вычитания и умножения-деления получаются группы целых чисел $\mathbb{Z}$ и рациональных положительных чисел $\mathbb{Q}_+^*$ соответственно.

1.3. Простые числа

Важным подмножеством натуральных чисел являются **простые числа** $\mathbb{P}$**.** Простое число — это натуральное число, имеющее ровно два различных натуральных делителя: **единицу и самого себя.** Все остальные натуральные числа, кроме единицы, называются составными. Ряд простых чисел начинается так: $2, 3, 5, 7, 11, 13, 17, ...$ Любое натуральное число, большее единицы, представимо в виде произведения простых чисел, причём

единственным способом с точностью до порядка следования сомножителей. Например, $121968=2^4 \cdot 3^2 \cdot 7 \cdot 11^2$.

Изучением свойств простых чисел занимается теория чисел. В теории колец простым числам соответствуют неприводимые элементы.

Последовательность простых чисел начинается так:

> 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, … (последовательность A000040 в OEIS)

1.3.1. Разложение натуральных чисел в произведение простых

Основная теорема арифметики утверждает, что каждое натуральное число, большее единицы, представимо в виде произведения простых чисел, причём единственным способом с точностью до порядка следования сомножителей. Таким образом, **простые числа — элементарные «строительные блоки» натуральных чисел**.

Представление натурального числа в виде произведения простых называется *разложением на простые* или *факторизацией* числа. На настоящий момент неизвестны полиномиальные алгоритмы факторизации чисел, хотя и не доказано, что таких алгоритмов не существует. На предполагаемой большой вычислительной сложности задачи факторизации базируется криптосистема RSA и некоторые другие. Факторизация с полиномиальной сложностью теоретически возможна на квантовом компьютере с помощью алгоритма Шора.

1.3.2. Алгоритмы поиска и распознавания простых чисел

Простые способы нахождения начального списка простых чисел вплоть до некоторого значения дают: решето Эратосфена, решето Сундарама и решето Аткина. Однако, на практике вместо получения списка простых чисел зачастую требуется проверить, является ли данное число простым. Алгоритмы, решающие эту задачу, называются тестами простоты. Существует множество полиномиальных тестов простоты, но большинство их являются вероятностными (например,

тест Миллера — Рабина) и используются для нужд криптографии. В 2002 году было доказано, что задача проверки на простоту в общем виде полиномиально разрешима, но предложенный детерминированный тест Агравала — Каяла — Саксены имеет довольно большую вычислительную сложность, что затрудняет его практическое применение.

Для некоторых классов чисел существуют специализированные эффективные тесты простоты (см. ниже).

1.3.3. Бесконечность множества простых чисел

Простых чисел бесконечно много. Самое старое известное доказательство этого факта было дано Евклидом в «Началах» (книга IX, утверждение 20). Его доказательство может быть кратко воспроизведено так:

> Представим, что количество простых чисел конечно. Перемножим их и прибавим единицу. Полученное число не делится ни на одно из конечного набора простых чисел, потому что остаток от деления на любое из них даёт единицу. Значит, число должно делиться на некоторое простое число, не включённое в этот набор. Противоречие.

Математики предлагали другие доказательства. Одно из них (приведённое Эйлером) показывает, что сумма величин, обратных к первым *n* простым числам, неограниченно растёт с ростом *n*.

Теорема о распределении простых чисел утверждает, что количество простых чисел меньших *n*, обозначаемое $\pi(n)$, растёт как $n/\ln(n)$.

1.3.4. Наибольшее известное простое

Издавна ведутся записи, отмечающие наибольшие известные на то время простые числа. Один из рекордов поставил в своё время Эйлер, найдя простое число $2^{31}-1=2147483647$. Наибольшим известным простым числом по состоянию на февраль 2011 года является $2^{43112609}-1$. Оно содержит 12 978 189 десятичных цифр и является простым числом Мерсенна ($M_{43112609}$). Его нашли 23 августа

2008 года на математическом факультете университета UCLA в рамках проекта по распределённому поиску простых чисел Мерсенна GIMPS.

Числа Мерсенна выгодно отличаются от остальных наличием эффективного теста простоты: теста Люка — Лемера. Благодаря ему простые числа Мерсенна давно удерживают рекорд как самые большие известные простые.

1.3.5. Простые числа специального вида

Существует ряд чисел, простота которых может быть установлена эффективно с использованием специализированных алгоритмов.

- Числа Мерсенна — числа вида $M_p = 2^p - 1$, где *p* — простое число (последовательность A001348 в OEIS). Как уже было отмечено выше, эффективным тестом простоты является тест Люка-Лемера. Простые числа Мерсенна образуют последовательность A000668 в OEIS.
- Числа Ферма — числа вида $F_n = 2^{2^n} + 1$, где *n* — неотрицательное целое число (последовательность A000215 в OEIS). Эффективным тестом простоты является тест Пепина. По состоянию на ноябрь 2011 года известно только 5 простых чисел Ферма (для *n* = 0, 1, 2, 3, 4), и высказана гипотеза, что других простых чисел Ферма нет.
- Числа Вудалла (*англ.*) — числа вида $W_n = n \cdot 2^n - 1$ (последовательность A003261 в OEIS). Эффективным тестом простоты является тест Люка-Лемера-Ризеля (*англ.*). Простые числа Вудалла образуют последовательность A050918 в OEIS.

С использованием теста Бриллхарта-Лемера-Селфриджа (*англ.*) может быть проверена простота следующих чисел:

- Числа Куллена (*англ.*) — числа вида $C_n = n \cdot 2^n + 1$ (последовательность A002064 в OEIS). Простые числа Куллена образуют последовательность A050920 в OEIS.
- Числа Прота — числа вида $P = k \cdot 2^n + 1$, причем *k* нечетно и $2^n > k$ (последовательность A080075 в OEIS). Числа Куллена являются частным случаем чисел Прота при *k* = *n*. Числа Ферма являются частным случаем чисел Прота при *k* = 1

и $n = 2^m$. Простые числа Прота образуют последовательность A080076 в OEIS.

Для поиска простых чисел обозначенных типов в настоящее время используются проекты распределенных вычислений GIMPS, PrimeGrid, Ramsey@Home, Seventeen or Bust, Riesel Sieve, Wieferich@Home.

1.3.6. Некоторые свойства простых чисел

- Если p — простое, и p делит ab, то p делит a или b. Доказательство этого факта было дано Евклидом и известно как лемма Евклида. Оно используется в доказательстве основной теоремы арифметики.
- Кольцо вычетов $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое.
- Характеристика каждого поля — это ноль или простое число.
- Если p — простое, а a — натуральное, то $a^p - a$ делится на p (малая теорема Ферма).
- Если G — конечная группа с p^n элементов, то Gсодержит элемент порядка p.
- Если G — конечная группа, и p^n — максимальная степень p, которая делит $|G|$, то G имеет подгруппу порядка p^n, называемую силовской подгруппой, более того, количество силовских подгрупп равно $pk + 1$ для некоторого целого k (теоремы Силова).
- Натуральное $p > 1$ является простым тогда и только тогда, когда $(p-1)! + 1$ делится на p (теорема Вильсона).
- Если $n > 1$ — натуральное, то существует простое p, такое, что $n < p < 2n$ (постулат Бертрана).
- Ряд чисел, обратных к простым, расходится. Более того, при $x \to \infty$

$$\sum_{p<x} \frac{1}{p} \sim \ln \ln x.$$

- Любая арифметическая прогрессия вида $a, a+q, a+2q, a+3q, ...$, где $a, q > 1$ — целые взаимнопростые числа, содержит бесконечно много простых чисел (Теорема Дирихле о простых числах в арифметической прогрессии).
- Всякое простое число, большее 3, представимо в виде $6k+1$ или $6k-1$, где k — некоторое натуральное число. Отсюда, если разность между последовательными простыми числами (при $k>1$) одинакова, то она обязательно кратна 6 — например (251-257-263-269; 199-211-223; 20183-20201-20219).
- Если $p > 3$ — простое, то $p^2 - 1$ кратно 24 (справедливо также для всех нечётных чисел, не делящихся на 3).
- Теорема Грина-Тао (*англ.*). Существуют сколь угодно длинные конечные арифметические прогрессии, состоящие из простых чисел.
- Никакое простое число не может иметь вид $n^k - 1$, где $n>2$, $k>1$. Иначе говоря, число, следующее за простым, не может быть квадратом

  имеет вид $2^k - 1$, то k — простое (см. числа Мерсенна).
- Никакое простое число не может иметь вид $n^{2k+1} + 1$, где $n>1$, $k>0$. Иначе говоря, число, предшествующее простому, не может быть кубом
- Множество положительных значений многочлена

$$(k+2)(1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2-[2n+p+q+z-e]^2-$$
$$[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2-$$
$$[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2-$$
$$[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2-$$
$$[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2)$$

при неотрицательных целых значениях переменных в точности совпадает со множеством простых чисел. Этот результат является частным случаем доказанной Юрием Матиясевичем диофантовости любого перечислимого множества.

1.4. Целое число

Целые числа, получаемые объединением натуральных чисел с множеством отрицательных чисел и нулём, обозначаются $\mathbb{Z} = \{... -2, -1, 0, 1, 2, ...\}$. Целые числа замкнуты относительно сложения, вычитания и умножения (но не деления).

Множество целых чисел (от ср.-лат. cifra от араб. (ṣifr) «пустой, нуль») — $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, определяется как замыкание множества натуральных чисел $\mathbb{N}$ относительно арифметических операций сложения (+) и вычитания (-). Таким образом, сумма, разность и произведение двух целых чисел дает снова целые числа. Оно состоит из натуральных чисел (1, 2, 3), чисел вида - *n* ($n \in \mathbb{N}$) и числа нуль. Необходимость рассмотрения целых чисел продиктована невозможностью (в общем случае) вычесть из одного натурального числа другое. Целые числа являются кольцом относительно операций сложения и умножения. Отрицательные числа ввели в математический обиход Михаэль Штифель (1487—1567) в книге «Полная арифметика» (1544), и Николя Шюке (1445—1500).

1.4.1. Алгебраические свойства целых чисел

$\mathbb{Z}$ не замкнуто относительно деления двух целых чисел (например, 1/2). Следующая таблица иллюстрирует несколько основных свойств сложения и умножения для любых целых *a*, *b* и *c*.

	сложение	умножение
замкнутость:	$a + b$ — целое	$a \times b$ — целое
ассоциативность:	$a + (b + c) = (a + b) + c$	$a \times (b \times c) = (a \times b) \times c$
коммутативность:	$a + b = b + a$	$a \times b = b \times a$
существование нейтрального элемента:	$a + 0 = a$	$a \times 1 = a$
существование противоположного элемента:	$a + (-a) = 0$	$a \neq \pm 1 \Rightarrow 1/a$ не является целым
дистрибутивность умножения	$a \times (b + c) = (a \times b) + (a \times c)$	

относительно сложения:	

На языке абстрактной алгебры первые пять вышеперечисленных свойств сложения говорят о том, что $\mathbb{Z}$ является абелевой группой относительно бинарной операции сложения, и, следовательно, также циклической группой, так как каждый ненулевой элемент $\mathbb{Z}$ может быть записан в виде конечной суммы 1 + 1 + … 1 или (−1) + (−1) + … + (−1). Фактически, $\mathbb{Z}$ является *единственной* бесконечной циклической группой по сложению в силу того, что любая бесконечная циклическая группа изоморфна группе $(\mathbb{Z}, +)$.

Первые четыре свойства умножения говорят о том, что $\mathbb{Z}$ — коммутативный моноид по умножению. Однако стоит заметить, что не каждое целое имеет противоположное по умножению, например, нет такого *x* из $\mathbb{Z}$, что 2*x* = 1, так как левая часть уравнения чётна, а правая нечётна. Из этого следует, что $\mathbb{Z}$ не является группой по умножению, а также не является полем. Наименьшее поле, содержащее целые числа, — множество рациональных чисел ($\mathbb{Q}$).

Совокупность всех свойств таблицы означает, что $\mathbb{Z}$ является коммутативным кольцом с единицей относительно сложения и умножения. Обычное деление не определено на множестве целых чисел, но определено так называемое **деление с остатком**: для любых целых *a* и *b*, $b \neq 0$, существует единственный набор целых чисел *q* и *r*, что $a = bq + r$ и $0 \leq r < |b|$, где |*b*| — абсолютная величина (модуль) числа *b*. Здесь *a* — делимое, *b* — делитель, *q* — частное, *r* — остаток. На этой операции основан алгоритм Евклида нахождения наибольшего общего делителя двух целых чисел.

1.4.2. Теоретико-множественные свойства

$\mathbb{Z}$ — линейно упорядоченное множество без верхней и нижней границ. Порядок в нём задаётся соотношениями:

… < −2 < −1 < 0 < 1 < 2 < …

Целое число называется **положительным**, если оно больше нуля, **отрицательным**, если меньше нуля. Нуль не является положительным или отрицательным.

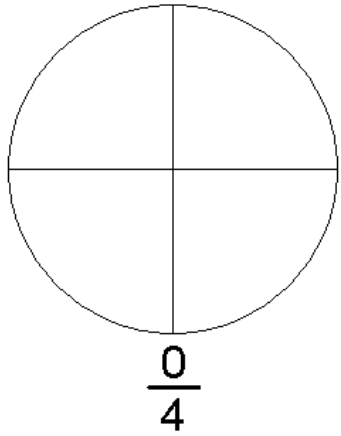
Для целых чисел справедливы следующие соотношения:

1. если $a < b$ и $c < d$, тогда $a + c < b + d$.
2. если $a < b$ и $0 < c$, тогда $ac < bc$. (Отсюда легко показать, что если $c < 0$, то $ac > bc$.)

Тип «целое число» — зачастую один из основных типов данных в языках программирования. Тем не менее эти «целые числа» — лишь имитация класса $\mathbb{Z}$ в математике, так как это множество бесконечно и всегда найдётся целое число, которое данный компьютер не сможет хранить в своей памяти. Целые типы данных обычно реализуются как фиксированный набор битов, но любые представления в конце концов приведут к тому, что свободное место на носителе (жёстком диске) закончится. С другой стороны, теоретические модели цифровых компьютеров имеют потенциально бесконечное (но счётное) пространство.

2. Рациональные числа

Рациональные числа — числа, представленные в виде дроби m/n ($n \neq 0$), где m — целое число, а n — натуральное число. Рациональные числа замкнуты уже относительно всех четырёх арифметических действий: сложения, вычитания, умножения и деления (кроме деления на ноль). Для обозначения рациональных чисел используется знак $\mathbb{Q}$.



Четверти

Рациональное число (лат. *ratio* — отношение, деление, дробь) — число, представляемое несократимой обыкновенной дробью $\frac{m}{n}$, m — целое число, а знаменатель n — натуральное число. Понятие дроби возникло несколько тысяч лет назад, когда, сталкиваясь с необходимостью измерять некоторые вещи (длину, вес, площадь и т.п.), люди поняли, что не удаётся обойтись целыми числами и необходимо ввести понятие доли: половины, трети и т.п. Дробями и операциями над ними пользовались, например, шумеры, древние египтяне и греки.

2.1. Множество рациональных чисел

Множество рациональных чисел обозначается $\mathbb{Q}$ и может быть записано таком в виде:

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

При этом оказывается, что разные записи могут представлять одну и ту же дробь, например, $\frac{3}{4}$ и $\frac{9}{12}$, (все дроби, которые можно получить друг

из друга умножением или делением на одно и то же натуральное число, представляют одно и то же рациональное число). Поскольку делением числителя и знаменателя дроби на их наибольший общий делитель можно получить единственное несократимое представление рационального числа, то можно говорить об их множестве как о множестве *несократимых* дробей со взаимно простыми целым числителем и натуральным знаменателем:

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}, \gcd(m,n) = 1 \right\}.$$

Здесь $\gcd(m,n)$ — наибольший общий делитель чисел *m* и *n*.

Множество рациональных чисел является естественным обобщением множества целых чисел. Легко видеть, что если у рационального числа $a = \frac{m}{n}$ знаменатель *n*=1, то *a*=*m* является целым числом. Множество рациональных чисел располагается на числовой оси всюду плотно: между любыми двумя различными рациональными числами расположено хотя бы одно рациональное число (а значит, и бесконечное множество рациональных чисел). Тем не менее, оказывается, что множество рациональных чисел имеет счётную мощность (т. е. все его элементы можно перенумеровать). Заметим, кстати, что ещё древние греки убедились в существовании чисел, не представимых в виде дроби (например, они доказали, что не существует рационального числа, квадрат которого равен 2).

2.2. Терминология

2.2.1. Формальное определение

Формально рациональные числа определяются как множество классов эквивалентности пар $\{(m,\ n) \mid m \in \mathbb{Z},\ n \in \mathbb{N}\}$ по отношению эквивалентности $(m,\ n) \sim (m',\ n')$, если $m \cdot n' = m' \cdot n$. При этом операции сложения и умножения определяются следующим образом:

- $(m_1,\ n_1) + (m_2,\ n_2) = (m_1 \cdot n_2 + m_2 \cdot n_1,\ n_1 \cdot n_2)$;

- $(m_1,\ n_1)\cdot(m_2,\ n_2)=(m_1\cdot m_2,\ n_1\cdot n_2)\,.$

2.2.2. Связанные определения

Правильные, неправильные и смешанные дроби

Правильной называется дробь, у которой модуль числителя меньше модуля знаменателя. Правильные дроби представляют рациональные числа, по модулю меньшие единицы. Дробь, не являющаяся правильной, называется *неправильной* и представляет рациональное число, большее или равное единице по модулю.

Неправильную дробь можно представить в виде суммы целого числа и правильной дроби, называемой ***смешанной дробью***. Например,

$$2\frac{3}{7}=2+\frac{3}{7}=\frac{14}{7}+\frac{3}{7}=\frac{17}{7}.$$

Подобная запись (с пропущенным знаком сложения), хотя и употребляется в элементарной арифметике, избегается в строгой математической литературе из-за схожести обозначения смешанной дроби с обозначением произведения целого числа на дробь.

Высота дроби

Высота обыкновенной дроби — это сумма модуля числителя и знаменателя этой дроби. ***Высота рационального числа*** — это сумма модуля числителя и знаменателя несократимой обыкновенной дроби, соответствующей этому числу.

Например, высота дроби $-\frac{15}{6}$ равна $15+6=21$. Высота же соответствующего рационального числа равна $5+2=7$, так как дробь сокращается на 3.

Термин **дробное число (дробь)** иногда используется как синоним к термину *рациональное число*, а иногда синоним любого нецелого числа. В последнем случае, дробные и рациональные числа являются

разными вещами, так как тогда нецелые рациональные числа — всего лишь частный случай дробных.

2.3. Свойства рациональных чисел

2.3.1. Основные свойства

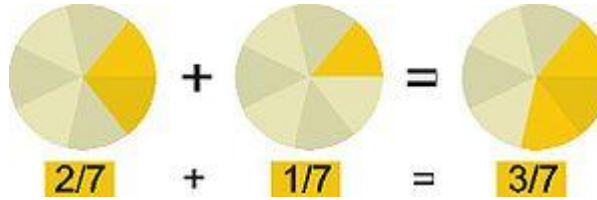
Множество рациональных чисел удовлетворяют шестнадцати основным свойствам, которые легко могут быть получены из свойств целых чисел.

1. **Упорядоченность.** Для любых рациональных чисел a и b существует правило, позволяющее однозначно идентифицировать между ними одно и только одно из трёх отношений: «$<$», «$>$» или «$=$». Это правило называется *правилом упорядочения* и формулируется следующим образом: два положительных числа $a = \frac{m_a}{n_a}$ и $b = \frac{m_b}{n_b}$ связаны тем же отношением, что и два целых числа $m_a \cdot n_b$ и $m_b \cdot n_a$; два неположительных числа a и b связаны тем же отношением, что и два неотрицательных числа $|b|$ и $|a|$; если же вдруг a неотрицательно, а b — отрицательно, то $a > b$.

$$\forall a, b \in \mathbb{Q} \ \ (a < b \vee a > b \vee a = b)$$

2. **Операция сложения.** Для любых рациональных чисел a и b существует так называемое *правило суммирования*, которое ставит им в соответствие некоторое рациональное число c. При этом само число c называется *суммой* чисел a и b и обозначается $(a + b)$, а процесс отыскания такого числа называется *суммированием*. Правило суммирования имеет следующий вид: $\frac{m_a}{n_a} + \frac{m_b}{n_b} = \frac{m_a \cdot n_b + m_b \cdot n_a}{n_a \cdot n_b}$.

$$\forall a, b \in \mathbb{Q} \ \exists (a + b) \in \mathbb{Q}$$



Суммирование дробей

3. **Операция умножения.** Для любых рациональных чисел a и b существует так называемое *правило умножения*, которое ставит им в соответствие некоторое рациональное число c. При этом само число c называется *произведением* чисел a и b и обозначается $(a \cdot b)$, а процесс отыскания такого числа также называется *умножением*. Правило умножения имеет следующий вид: $\frac{m_a}{n_a} \cdot \frac{m_b}{n_b} = \frac{m_a \cdot m_b}{n_a \cdot n_b}$.

$$\forall a, b \in \mathbb{Q}\ \exists (a \cdot b) \in \mathbb{Q}$$

4. **Транзитивность отношения порядка.** Для любой тройки рациональных чисел a, b и c если a меньше b и b меньше c, то a меньше c, а если a равно b и b равно c, то a равно c.

$$\forall a, b, c \in \mathbb{Q}\ \ (a < b \wedge b < c \Rightarrow a < c) \wedge (a = b \wedge b = c \Rightarrow a = c)$$

5. **Коммутативность сложения.** От перемены мест рациональных слагаемых сумма не меняется.

$$\forall a, b \in \mathbb{Q}\ \ a + b = b + a$$

6. **Ассоциативность сложения.** Порядок сложения трёх рациональных чисел не влияет на результат.

$$\forall a, b, c \in \mathbb{Q}\ \ (a + b) + c = a + (b + c)$$

7. **Наличие нуля.** Существует рациональное число 0, которое сохраняет любое другое рациональное число при суммировании.

$$\exists 0 \in \mathbb{Q}\ \forall a \in \mathbb{Q}\quad a + 0 = a$$

8. **Наличие противоположных чисел.** Любое рациональное число имеет противоположное рациональное число, при суммировании с которым даёт 0.

$$\forall a \in \mathbb{Q}\ \exists (-a) \in \mathbb{Q}\quad a + (-a) = 0$$

9. **Коммутативность умножения.** От перемены мест рациональных множителей произведение не меняется.

$$\forall a, b \in \mathbb{Q}\quad a \cdot b = b \cdot a$$

10. **Ассоциативность умножения.** Порядок перемножения трёх рациональных чисел не влияет на результат.

$$\forall a, b, c \in \mathbb{Q}\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

11. **Наличие единицы.** Существует рациональное число 1, которое сохраняет любое другое рациональное число при умножении.

$$\exists 1 \in \mathbb{Q}\ \forall a \in \mathbb{Q}\quad a \cdot 1 = a$$

12. **Наличие обратных чисел.** Любое ненулевое рациональное число имеет обратное рациональное число, умножение на которое даёт 1.

$$\forall a \in \mathbb{Q}\ \exists a^{-1} \in \mathbb{Q}\quad a \cdot a^{-1} = 1$$

13. **Дистрибутивность умножения относительно сложения.** Операция умножения согласована с операцией сложения посредством распределительного закона:

$$\forall a,b,c \in \mathbb{Q} \quad (a+b)\cdot c = a\cdot c + b\cdot c$$

14. **Связь отношения порядка с операцией сложения.** К левой и правой частям рационального неравенства можно прибавлять одно и то же рациональное число.

$$\forall a,b,c \in \mathbb{Q} \quad a < b \Rightarrow a + c < b + c$$

15. **Связь отношения порядка с операцией умножения.** Левую и правую части рационального неравенства можно умножать на одно и то же положительное рациональное число.

$$\forall a,b,c \in \mathbb{Q} \quad c > 0 \wedge a < b \Rightarrow a\cdot c < b\cdot c$$

16. **Аксиома Архимеда.** Каково бы ни было рациональное число *a*, можно взять столько единиц, что их сумма превзойдёт *a*.

$$\forall a \in \mathbb{Q}\ \exists n \in \mathbb{N} \quad \sum_{k=1}^{n} 1 > a$$

2.3.2. Дополнительные свойства

Все остальные свойства, присущие рациональным числам, не выделяют в основные, потому что они, вообще говоря, уже не опираются непосредственно на свойства целых чисел, а могут быть доказаны исходя из приведённых основных свойств или непосредственно по определению некоторого математического объекта. Таких дополнительных свойств очень много. Здесь имеет смысл привести лишь некоторые из них.

- Отношение порядка «>» (с противоположным порядком аргументов) также транзитивно.

$$\forall a,b,c \in \mathbb{Q} \quad a > b \wedge b > c \Rightarrow a > c$$

- Произведение любого рационального числа на ноль равно нулю.

$$\forall a \in \mathbb{Q} \quad a \cdot 0 = 0$$

- Рациональные неравенства одного знака можно почленно складывать.

$$\forall a, b, c, d \in \mathbb{Q} \quad a > b \wedge c > d \Rightarrow a + c > b + d$$

- Множество рациональных чисел $\mathbb{Q}$ является полем (а именно, полем частных кольца целых чисел $\mathbb{Z}$) относительно операций сложения и умножения дробей.

$$(\mathbb{Q}, +, \cdot) \text{ — поле}$$

- В позиционной системе счисления рациональное число представляется периодической дробью. Более того, наличие представления в виде периодической дроби является критерием рациональности вещественного числа.
- Каждое рациональное число является алгебраическим.

$$\mathbb{Q} \subset \mathbb{A}$$

2.4. Счётность множества рациональных чисел

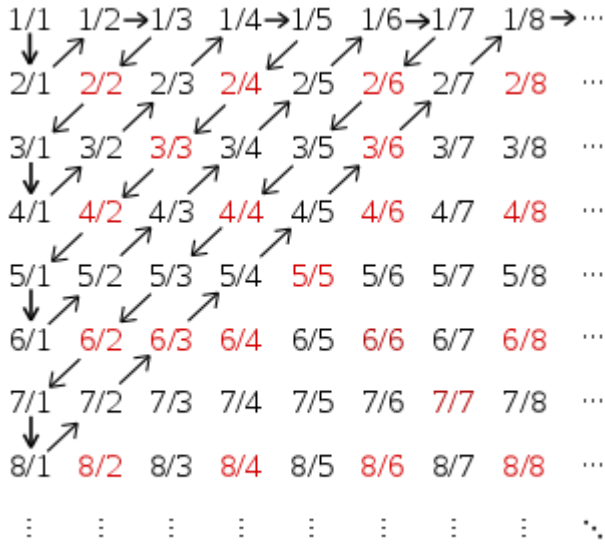
Чтобы оценить количество рациональных чисел, нужно найти мощность их множества. Легко доказать, что множество рациональных чисел счётно. Для этого достаточно привести алгоритм, который нумерует рациональные числа, т. е. устанавливает биекцию между множествами рациональных и натуральных чисел. Примером такого построения может служить следующий простой алгоритм. Составляется бесконечная таблица обыкновенных дробей, на каждой i-ой строке в каждом j-ом столбце которой располагается дробь $\frac{i}{j}$. Для определённости считается, что строки и столбцы этой таблицы нумеруются с единицы. Ячейки таблицы обозначаются (i, j), где i — номер строки таблицы, в которой располагается ячейка, а j — номер столбца. Полученная таблица обходится «змейкой» по следующему формальному алгоритму.

- Если текущее положение (i, j) таково, что i — нечётное, а $j = 1$, то следующим положением выбирается $(i + 1, j)$.
- Если текущее положение (i, j) таково, что $i = 1$, а j — чётное, то следующим положением выбирается $(i, j + 1)$.
- Если для текущего положения (i, j) сумма индексов $(i + j)$ нечётна, то следующее положение — $(i - 1, j + 1)$.
- Если для текущего положения (i, j) сумма индексов $(i + j)$ чётна, то следующее положение — $(i + 1, j - 1)$.

Эти правила просматриваются сверху вниз и следующее положение выбирается по первому совпадению.

В процессе такого обхода каждому новому рациональному числу ставится в соответствие очередное натуральное число. Т. е. дроби $1/1$ ставится в соответствие число 1, дроби $2/1$ — число 2, и т. д. Нужно отметить, что нумеруются только несократимые дроби. Формальным признаком несократимости является равенство единице наибольшего общего делителя числителя и знаменателя дроби.

Следуя этому алгоритму, можно занумеровать все положительные рациональные числа. Это значит, что множество положительных рациональных чисел $\mathbb{Q}_+$ счётно.



Нумерация положительных рациональных чисел

Легко установить биекцию между множествами положительных и отрицательных рациональных чисел, просто поставив в соответствие каждому рациональному числу противоположное ему. Т. о. множество отрицательных рациональных чисел $\mathbb{Q}_-$ тоже счётно. Их объединение $\mathbb{Q}_+ \cup \mathbb{Q}_-$ также счётно по свойству счётных множеств. Множество же рациональных чисел $\mathbb{Q} = \mathbb{Q}_+ \cup \mathbb{Q}_- \cup \{0\}$ тоже счётно как объединение счётного множества с конечным.

Существуют и другие способы занумеровать рациональные числа. Например, для этого можно воспользоваться такими структурами как дерево Калкина — Уилфа, дерево Штерна — Броко или ряд Фарея.

Утверждение о счётности множества рациональных чисел может вызывать некоторое недоумение, т. к. на первый взгляд складывается впечатление, что оно гораздо обширнее множества натуральных чисел. На самом деле это не так и натуральных чисел хватает, чтобы занумеровать все рациональные.

2.5. Недостаточность рациональных чисел

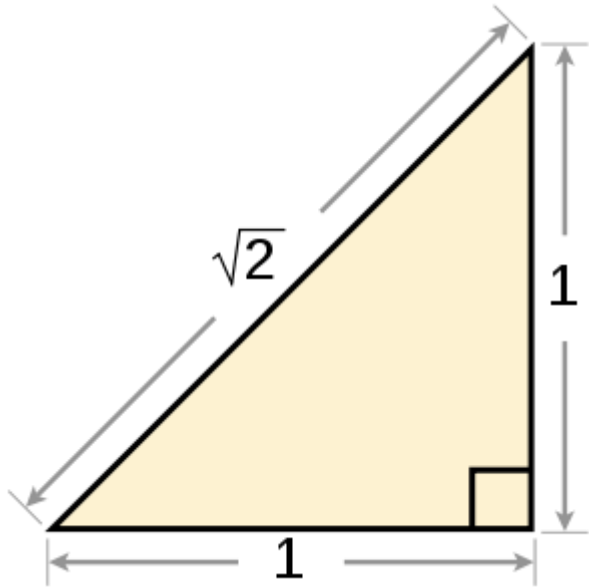
В геометрии следствием так называемой аксиомы Архимеда (в более общем понимании, чем упомянуто выше) является возможность построения сколь угодно малых (т. е., коротких) величин, выражаемых рациональными числами вида $1/n$. Этот факт создаёт обманчивое впечатление, что рациональными числами можно измерить вообще любые геометрические расстояния. Легко показать, что это не верно.

Из теоремы Пифагора известно, что гипотенуза прямоугольного треугольника выражается как квадратный корень суммы квадратов его катетов. Т. о. длина гипотенузы равнобедренного прямоугольного треугольника с единичным катетом равна $\sqrt{2}$, т. е. числу, квадрат которого равен 2.

Если допустить, что число $\sqrt{2}$ представляется некоторым рациональным числом, то найдётся такое целое число m и такое натуральное число n, что $\sqrt{2} = \frac{m}{n}$, причём дробь $\frac{m}{n}$ несократима, т. е. числа m и n — взаимно простые.

Если $\sqrt{2} = \frac{m}{n}$, то $2 = \sqrt{2} \cdot \sqrt{2} = \frac{m}{n} \cdot \frac{m}{n} = \frac{m^2}{n^2}$, т. е. $m^2 = 2n^2$. Следовательно, число m^2 чётно, но произведение двух нечётных чисел нечётно, что означает, что само число m также чётно. А значит найдётся натуральное число k, такое что число m можно представить в виде $m = 2k$. Квадрат числа m в этом смысле $m^2 = 4k^2$, но с другой стороны $m^2 = 2n^2$, значит $4k^2 = 2n^2$, или $n^2 = 2k^2$. Как уже показано ранее для числа m, это значит, что число n — чётно, как и m. Но тогда они не являются взаимно простыми, так как оба делятся пополам. Полученное противоречие доказывает, что $\sqrt{2}$ не есть рациональное число.

Из вышесказанного следует, что существуют отрезки на плоскости, а, значит, и на числовой прямой, которые не могут быть измерены рациональными числами. Это приводит к возможности расширения понятия рациональных чисел до вещественных.



Гипотенуза такого треугольника не выражается никаким рациональным числом

3. Действительные (вещественные) числа

3.1. Введение в действительные (вещественные) числа

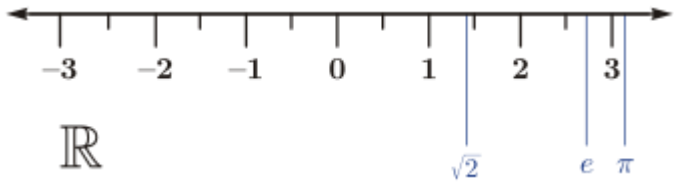
Действительные (вещественные) числа представляют собой расширение множества рациональных чисел, замкнутое относительно некоторых (важных для математического моделирования) операций предельного перехода. Множество вещественных чисел обозначается

$\mathbb{R}$. Его можно рассматривать как пополнение поля рациональных чисел $\mathbb{Q}$ при помощи нормы, являющейся обычной абсолютной величины. Кроме рациональных чисел, $\mathbb{R}$ включает множество иррациональных чисел $\mathbb{I}$, не представимых в виде отношения целых.

, или — математическая абстракция, возникшая из потребности измерения геометрических и физических величин окружающего мира, а также проведения таких операций как извлечение корня, вычисление логарифмов, решение алгебраических уравнений.

Если натуральные числа возникли в процессе счета, рациональные — из потребности оперировать частями целого, то **вещественные числа предназначены для измерения непрерывных величин**. Таким образом, расширение запаса рассматриваемых чисел привело к множеству вещественных чисел, которое помимо чисел рациональных включает также другие элементы, называемые *иррациональными числами*.

Наглядно понятие вещественного числа можно представить себе при помощи *числовой прямой*.



Числовая прямая

Если на прямой выбрать направление, начальную точку и единицу длины для измерения отрезков, то каждому вещественному числу можно поставить в соответствие определённую точку на этой прямой, и обратно, каждая точка будет представлять некоторое, и притом только одно, вещественное число. Вследствие этого соответствия термин числовая прямая обычно употребляется в качестве синонима множества вещественных чисел.

Понятие вещественного числа прошло долгий путь становления. Ещё в Древней Греции в школе Пифагора, которая в основу всего ставила целые числа и их отношения, было открыто существование *несоизмеримых величин* (несоизмеримость стороны и диагонали квадрата), то есть в современной терминологии — чисел, не являющихся рациональными. Вслед за этим Евдоксом Книдским была предпринята попытка построить общую теорию числа, включавшую несоизмеримые величины. После этого, на протяжении более двух тысяч лет, никто не ощущал необходимости в точном определении понятия вещественного числа, несмотря на постепенное расширение этого понятия. Лишь во второй половине XIX века, когда развитие математического анализа потребовало перестройки его основ на новом, более высоком уровне строгости, в работах К. Вейерштрасса, Р. Дедекинда, Г. Кантора, Э. Гейне, Ш. Мере была создана строгая теория вещественных чисел.

С точки зрения современной математики, **множество вещественных чисел — непрерывное упорядоченное поле**. Это определение, или эквивалентная система аксиом, в точности определяет понятие вещественного числа в том смысле, что существует только одно, с точностью до изоморфизма, непрерывное упорядоченное поле.

Множество вещественных чисел имеет стандартное обозначение — **R** («полужирное R»), или $\mathbb{R}$ (англ. *blackboard bold* «R») от лат. *realis* — действительный.

3.2. История становления понятия вещественного числа

3.2.1. Наивная теория вещественных чисел

Первая развитая числовая система, построенная в Древней Греции, включала только натуральные числа и их отношения (пропорции, в современном понимании — рациональные числа). Однако вскоре выяснилось, что для целей геометрии и астрономии этого недостаточно: например, отношение длины диагонали квадрата к длине его стороны не может быть представлено ни натуральным, ни

рациональным числом. Для выхода из положения Евдокс Книдский ввёл, в дополнение к числам, более широкое понятие *геометрической величины*, то есть длины отрезка, площади или объёма. Теория Евдокса дошла до нас в изложении Евклида («Начала», книга V). По существу, теория Евдокса — это геометрическая модель вещественных чисел. С современной точки зрения, число при таком подходе есть *отношение* двух однородных величин — например, исследуемой и единичного эталона. Следует, однако, подчеркнуть, что Евдокс остался верен прежней традиции — он не рассматривал такое отношение как число; из-за этого в «Началах» многие теоремы о свойствах чисел затем заново доказываются для величин. Классическая теория Дедекинда для построения вещественных чисел по своим принципам чрезвычайно похожа на изложение Евдокса. Однако модель Евдокса неполна во многих отношениях — например, она не содержит аксиомы непрерывности, нет общей теории арифметических операций для величин или их отношений и др.

Ситуация начала меняться в первые века н. э. Уже Диофант Александрийский, вопреки прежним традициям, рассматривает дроби так же, как и натуральные числа, а в IV книге своей «Арифметики» даже пишет об одном результате: «Число оказывается не рациональным». После гибели античной науки на передний план выдвинулись индийские и исламские математики, для которых любой результат измерения или вычисления считался числом. Эти взгляды постепенно взяли верх и в средневековой Европе, где поначалу разделяли рациональные и *иррациональные* (буквально: неразумные) числа (их называли также мнимыми, абсурдными, глухими и т. п.). Полное уравнение в правах иррациональных чисел связано с трудами Симона Стевина (конец XVI века), который провозгласил:

> *Мы приходим к выводу, что не существует никаких абсурдных, иррациональных, неправильных, необъяснимых или глухих чисел, но что среди чисел существует такое совершенство и согласие, что нам надо размышлять дни и ночи над их удивительной законченностью.*

Он же, с некоторыми оговорками, легализовал отрицательные числа, а также развил теорию и символику десятичных дробей, которые с этого момента начинают вытеснять неудобные шестидесятеричные.

Спустя столетие Ньютон в своей «Универсальной арифметике» (1707) даёт классическое определение (вещественного) числа как отношения результата измерения к единичному эталону:

> *Под числом мы понимаем не столько множество единиц, сколько отвлечённое отношение какой-нибудь величины к другой величине того же рода, принятой за единицу.*

Долгое время это прикладное определение считалось достаточным, так что практически важные свойства вещественных чисел и функций не доказывались, а считались интуитивно очевидными (из геометрических или кинематических соображений). Например, считался самоочевидным тот факт, что непрерывная кривая, точки которой расположены по разные стороны от некоторой прямой, пересекает эту прямую. Строгое определение понятия непрерывности также отсутствовало. Как следствие, немало теорем содержали ошибки, нечёткие или чрезмерно широкие формулировки.

Даже после того, как Коши разработал достаточно строгий фундамент анализа, положение не изменилось, поскольку теории вещественных чисел, на которую обязан был опираться анализ, не существовало. Из-за этого Коши сделал немало ошибок, положившись на интуицию там, где она приводила к неверным выводам: например, он полагал, что сумма ряда из непрерывных функций всегда непрерывна.

3.2.2. Создание строгой теории

Первую попытку заполнить пробел в основаниях математики сделал Бернард Больцано в своей статье «Чисто аналитическое доказательство теоремы, что между любыми двумя значениями, дающими результаты противоположного знака, лежит по меньшей мере один действительный корень уравнения» (1817). В этой пионерской работе ещё нет целостной системы вещественных чисел, но уже приводится современное определение непрерывности и показывается, что на этой основе теорема, упомянутая в заглавии, может быть строго доказана. В более поздней работе Больцано даёт набросок общей теории вещественных чисел, по идеям близкой к канторовской теории множеств, но эта его работа осталась неопубликованной при жизни автора и увидела свет только в 1851 году. Взгляды Больцано

значительно опередили своё время и не привлекли внимания математической общественности.

Современная теория вещественных чисел была построена во второй половине XIX века, в первую очередь трудами Вейерштрасса, Дедекинда и Кантора. Они предложили различные, но эквивалентные подходы к теории этой важнейшей математической структуры и окончательно отделили это понятие от геометрии и механики.

3.3. Конструктивные способы определения вещественного числа

При конструктивном определении понятия вещественного числа, на основе известных математических объектов (например, множества рациональных чисел $\mathbb{Q}$), которые принимают заданными, строят новые объекты, которые, в определённом смысле, отражают наше интуитивное понимание о понятии вещественного числа. Существенным отличием между вещественными числами и этими построенными объектами является то, что первые, в отличие от вторых, понимаются нами лишь интуитивно и *пока* не являются строго определённым математическим понятием.

Эти объекты и объявляют вещественными числами. Для них вводят основные арифметические операции, определяют отношение порядка и доказывают их свойства.

Исторически первыми строгими определениями вещественного числа были именно конструктивные определения. В 1872 году были опубликованы одновременно три работы: теория фундаментальных последовательностей Кантора, теория Вейерштрасса (в современном варианте — теория бесконечных десятичных дробей) и теория сечений в области рациональных чисел Дедекинда.

3.3.1. Теория фундаментальных последовательностей Кантора

В данном подходе вещественное число рассматривается как предел последовательности рациональных чисел. Чтобы последовательность рациональных чисел сходилась, на неё накладывается *условие Коши*:

$$\forall \varepsilon > 0 \; \exists N(\varepsilon) : \; \forall n > N(\varepsilon) \; \forall m > 0 \; |a_{n+m} - a_n| < \varepsilon$$

Смысл этого условия заключается в том, что члены последовательности, начиная с некоторого номера будут лежать сколь угодно близко друг от друга. Последовательности, удовлетворяющие условию Коши, называются *фундаментальными*. Вещественное число, определяемое фундаментальной последовательностью рациональных чисел $\{a_n\}$, обозначим $[a_n]$.

Два вещественных числа $\alpha = [a_n]$ и $\beta = [b_n]$, определённые соответственно фундаментальными последовательностями $\{a_n\}$ и $\{b_n\}$, называются *равными*, если

$$\lim_{n \to \infty} (a_n - b_n) = 0$$

Если даны два вещественных числа $\alpha = [a_n]$ и $\beta = [b_n]$, то их суммой и произведением называются числа, определённые соответственно суммой и произведением последовательностей $\{a_n\}$ и $\{b_n\}$:

$$\alpha + \beta \stackrel{\text{def}}{=} [a_n + b_n] \qquad \alpha \cdot \beta \stackrel{\text{def}}{=} [a_n \cdot b_n]$$

Отношение порядка на множестве вещественных чисел устанавливается посредством соглашения, в соответствии с которым число $\alpha = [a_n]$ *по определению* больше числа $\beta = [b_n]$, т. е. $\alpha > \beta$, если

$$\exists \varepsilon > 0 \; \exists N : \; \forall n > N \; a_n \geqslant b_n + \varepsilon$$

Способ построения множества вещественных чисел с помощью фундаментальных последовательностей рациональных чисел является частным случаем конструкции *пополнения* произвольного метрического пространства. Как и в общем случае, полученное в результате пополнения множество вещественных чисел само уже

является *полным*, то есть содержит пределы всех фундаментальных последовательностей своих элементов.

3.3.2. Теория бесконечных десятичных дробей

Вещественное число определяется как *бесконечная десятичная дробь*, то есть выражение вида

$$\pm a_0, a_1 a_2 \ldots a_n \ldots$$

где $\pm$ есть один из символов $+$ или $-$, называемый знаком числа, a_0 — целое неотрицательное число, $a_1, a_2, \ldots a_n, \ldots$ — последовательность десятичных знаков, т. е. элементов числового множества $\{0, 1, \ldots 9\}$.

Бесконечная десятичная дробь интерпретируется как такое число, которое на числовой прямой лежит между *рациональными* точками вида

$$\pm a_0, a_1 a_2 \ldots a_n$$

и

$$\pm \left(a_0, a_1 a_2 \ldots a_n + 10^{-n} \right)$$

для всех $n = 0, 1, 2, \ldots$

Сравнение вещественных чисел в форме бесконечных десятичных дробей производится поразрядно. Например, пусть даны два неотрицательных числа

$$\begin{aligned} \alpha &= +a_0, a_1 a_2 \ldots a_n \ldots \\ \beta &= +b_0, b_1 b_2 \ldots b_n \ldots \end{aligned}$$

Если $a_0 < b_0$, то $\alpha < \beta$; если $a_0 > b_0$ то $\alpha > \beta$. В случае равенства $a_0 = b_0$ переходят к сравнению следующего разряда. И

так далее. Если $\alpha \neq \beta$, то после конечного числа шагов встретится первый разряд n, такой что $a_n \neq b_n$. Если $a_n < b_n$, то $\alpha < \beta$; если $a_n > b_n$ то $\alpha > \beta$.

Однако, при этом следует учитывать, что число $a_0, a_1 a_2 \ldots a_n(9) = a_0, a_1 a_2 \ldots a_n + 10^{-n}$. Поэтому если запись одного из сравниваемых чисел, начиная с некоторого разряда, представляет собой периодическую десятичную дробь, у которой в периоде стоит 9, то её следует заменить на эквивалентную запись, с нулём в периоде.

Арифметические операции над бесконечными десятичными дробями определяются как *непрерывное продолжение* соответствующих операций над рациональными числами. Например, суммой вещественных чисел α и β называется вещественное число $\alpha + \beta$, удовлетворяющее следующему условию:

$$\forall a', a'', b', b'' \in \mathbb{Q}\ (a' \leqslant \alpha \leqslant a'') \wedge (b' \leqslant \beta \leqslant b'') \Rightarrow (a' + b' \leqslant \alpha + \beta \leqslant a'' + b'')$$

Аналогично определяет операция умножения бесконечных десятичных дробей.

3.3.3. Теория сечений в области рациональных чисел

В подходе Дедекинда вещественные числа определяются с помощью сечений в множестве рациональных чисел.

Сечением в множестве рациональных чисел $\mathbb{Q}$ называется всякое разбиение совокупности всех рациональных чисел на два непустых *класса — нижний* A и *верхний* A', так что каждое число из нижнего класса строго меньше всякого числа из верхнего:

$$\mathbb{Q} = A \cup A' \quad \wedge \quad A, A' \neq \varnothing \quad \wedge \quad \forall a \in A, \forall a' \in A'\ (a < a')$$

Если существует число α, которое является максимальным в нижнем классе, либо минимальным в верхнем классе, то это число *разделяет*

множества A и A': числа нижнего и верхнего классов лежат по разные стороны от α. Говорят также, что рациональное число α *производит* данное сечение множества рациональных чисел.

Если же в нижнем классе сечения нет максимального элемента, а в верхнем — минимального, то не существует никакого рационального числа, которое разделяло бы множества A и A'. В этом случае по определению полагают, что данное сечение *определяет* некоторое *иррациональное число* α, которое находится между нижним и верхним классами, и тем самым производит данное сечение. Иначе говоря, для всякого сечения, не производимого никаким *рациональным* числом, вводят новый объект — *иррациональное* число, которое по определению больше всякого числа из нижнего класса и меньше всякого числа из верхнего класса:

$$\forall a \in A, \forall a' \in A'\ a < \alpha < a'$$

Объединение всех рациональных и всех иррациональных чисел называют *множеством вещественных чисел*, а его элементы — *вещественными числами.*

Арифметические операции над вещественными числами определяются как *непрерывное продолжение* соответствующих операций над рациональными числами. Например, суммой вещественных чисел α и β называется вещественное число $\alpha + \beta$, удовлетворяющее следующему условию:

$$\forall a', a'', b', b'' \in \mathbb{Q}\ (a' \leqslant \alpha \leqslant a'') \wedge (b' \leqslant \beta \leqslant b'') \Rightarrow (a' + b' \leqslant \alpha + \beta \leqslant a'' + b'')$$

3.4. Аксиоматический подход

Построить множество вещественных чисел можно разными способами. В теории Кантора вещественные числа — классы эквивалентных фундаментальных последовательностей рациональных чисел, в теории Вейерштрасса — бесконечные десятичные дроби, в теории Дедекинда — сечения в области рациональных чисел. Во всех этих подходах в результате мы получаем некоторое множество объектов (вещественных чисел), обладающих определёнными свойствами: их можно складывать, умножать, сравнивать между собой.

Более того, коль скоро установлены свойства этих объектов, мы можем больше не апеллировать к тем конкретным конструкциям, с помощью которых они были построены.

В математике важна не конкретная природа объектов, а лишь математические соотношения, существующие между ними. Для человека, который исследует математическое понятие количество элементов, безразлично, о чём говорить — о трёх яблоках или о трёх камнях, и их съедобность или несъедобность значения не имеет. В процессе отвлечения от несущественных признаков, то есть абстрагирования (лат. *abstractio* — отвлечение), он приходит к тому общему, что есть у трёх яблок и трёх камней — количеству элементов. Так возникает абстрактное понятие натурального числа. С этой точки зрения три яблока и три камня — две конкретные реализации, *модели* абстрактного понятия «число три». Точно так же классы фундаментальных последовательностей рациональных чисел, бесконечные десятичные дроби, сечения в области рациональных чисел являются лишь конкретными реализациями, моделями вещественного числа. А само понятие вещественного числа определяется существующими для него математическими соотношениями. Коль скоро они установлены, определено и понятие вещественного числа. Здесь уместно привести знаменитое высказывание Д. Гильберта, основоположника системного аксиоматического метода в математике, который, имея в виду аксиоматизацию геометрии, как-то заметил:

> *Следует добиться того, чтобы с равным успехом можно было говорить вместо точек, прямых и плоскостей о столах, стульях и пивных кружках.*
>
> Давид Гильберт

3.4.1. Аксиоматика вещественных чисел

Множество $\mathbb{R}$ *называется множеством вещественных чисел, а его элементы — вещественными числами, если выполнен следующий комплекс условий, называемый аксиоматикой вещественных чисел:*

3.4.1.1. Аксиомы поля

На множестве $\mathbb{R}$ определено отображение (*операция сложения*)

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

сопоставляющее каждой упорядоченной паре элементов a, b из $\mathbb{R}$ некоторый элемент c из того же множества $\mathbb{R}$, называемый *суммой* a и b($a + b$ эквивалентная запись элемента c множества $\mathbb{R}$).

Также, на множестве $\mathbb{R}$ определено отображение (*операция умножения*)

$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

сопоставляющее каждой упорядоченной паре элементов a, b из $\mathbb{R}$ некоторый элемент $a \cdot b$, называемый *произведением* a и b.

При этом имеют место следующие свойства.

I_1. *Коммутативность сложения.* Для любых $a, b \in \mathbb{R}$

$$a + b = b + a$$

I_2. *Ассоциативность сложения.* Для любых $a, b \in \mathbb{R}$

$$a + (b + c) = (a + b) + c$$

I_3. *Существование нуля.* Существует элемент $0 \in \mathbb{R}$, называемый *нулём*, такой, что для любого $a \in \mathbb{R}$

$$a + 0 = a$$

I_4. *Существование противоположного элемента.* Для любого $a \in \mathbb{R}$ существует элемент $-a \in \mathbb{R}$, называемый *противоположным* к a, такой, что

$$a + (-a) = 0$$

I_5. *Коммутативность умножения.* Для любых $a, b \in \mathbb{R}$

$$a \cdot b = b \cdot a$$

I_6. *Ассоциативность умножения.* Для любых $a, b \in \mathbb{R}$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

I_7. *Существование единицы.* Существует элемент $1 \in R$, называемый *единицей*, такой, что для любого $a \in R$

$$a \cdot 1 = a$$

I_8. *Существование обратного элемента.* Для любого $a \in \mathbb{R}, a \neq 0$ существует элемент $a^{-1} \in \mathbb{R}$, обозначаемый также $1/a$ и называемый *обратным* к a, такой, что

$$a \cdot a^{-1} = 1$$

I_9. *Дистрибутивный закон умножения относительно сложения.* Для любых $a, b, c \in \mathbb{R}$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

I_{10}. *Нетривиальность поля. Единица* и *ноль* — различные элементы $\mathbb{R}$:

$$1 \neq 0$$

3.4.1.2. Аксиомы порядка

Между элементами $\mathbb{R}$ определено отношение $\leqslant$, то есть для любой упорядоченной пары элементов a, b из $\mathbb{R}$ установлено, выполняется соотношение $a \leqslant b$ или нет. При этом имеют место следующие свойства.

II_1. *Рефлексивность.* Для любого $a \in \mathbb{R}$

$$a \leqslant a$$

II_2. *Антисимметричность.* Для любых $a, b \in \mathbb{R}$

$$(a \leqslant b) \wedge (b \leqslant a) \Rightarrow (a = b)$$

II_3. *Транзитивность.* Для любых $a, b, c \in \mathbb{R}$

$$(a \leqslant b) \wedge (b \leqslant c) \Rightarrow (a \leqslant c)$$

II_4. *Линейная упорядоченность.* Для любых $a, b \in \mathbb{R}$

$$(a \leqslant b) \vee (b \leqslant a)$$

II_5. *Связь сложения и порядка.* Для любых $a, b, c \in \mathbb{R}$

$$(a \leqslant b) \Rightarrow (a + c \leqslant b + c)$$

II_6. *Связь умножения и порядка.* Для любых $a, b \in \mathbb{R}$

$$(0 \leqslant a) \wedge (0 \leqslant b) \Rightarrow (0 \leqslant a \cdot b)$$

3.4.2.3. Аксиомы непрерывности

III_1. Каковы бы ни были непустые множества $A \subset \mathbb{R}$ и $B \subset \mathbb{R}$, такие что для любых двух элементов $a \in A$ и $b \in B$ выполняется неравенство $a \leqslant b$, существует такое число $\xi \in \mathbb{R}$, что для всех $a \in A$ и $b \in B$ имеет место соотношение

$$a \leqslant \xi \leqslant b$$

Этих аксиом достаточно чтобы строго вывести все известные свойства вещественных чисел.

На языке современной алгебры аксиомы первой группы означают, что множество $\mathbb{R}$ является полем. Аксиомы второй группы — что множество $\mathbb{R}$является линейно упорядоченным множеством (II_1 — II_4), причём отношение порядка согласовано со структурой поля II_5 — II_6. Множества, удовлетворяющие аксиомам первой и второй группы, называются *упорядоченными полями*. Наконец, последняя группа, состоящая из одной аксиомы, утверждает, что множество вещественных чисел обладает свойством *непрерывности*, которое

также называют *полнотой*. Резюмируя, можно дать эквивалентное определение множества вещественных чисел.

Определение. *Множеством вещественных чисел называется непрерывное упорядоченное поле.*

3.4.2. Другие системы аксиом вещественных чисел

Существуют и другие способы аксиоматизации вещественных чисел. Например, вместо аксиомы непрерывности III_1 можно использовать любое другое эквивалентное ей условие, или группу условий. Например, в системе аксиом, предложенной Гильбертом, аксиомы групп I и II, по существу, те же, что и в приведённые выше, а вместо аксиомы III_1 используются следующие два условия:

III'_1. *Аксиома Архимеда.* Пусть $a > 0$ и $b > 0$. Тогда элемент a можно повторить слагаемым столько раз, чтобы образовавшаяся в результате сумма превзошла b:

$$a + a + \ldots + a > b$$

III'_2. *Аксиома полноты (в смысле Гильберта).* Систему $\mathbb{R}$ невозможно расширить ни до какой системы $\mathbb{R}^*$, так чтобы при сохранении прежних соотношений между элементами $\mathbb{R}$, для $\mathbb{R}^*$ выполнялись бы все аксиомы I—II, III'_1.

Таким образом, можно дать следующее эквивалентное определение:

Определение. *Множество вещественных чисел есть максимальное архимедово упорядоченное поле*

В качестве другого примера аксиоматизации вещественных чисел можно привести аксиоматику Тарского (*англ.*), состоящую всего из 8 аксиом.

3.5. Свойства

3.5.1. Связь с рациональными числами

Очевидно, что на числовой прямой рациональные числа располагаются вперемешку с вещественными, причём множество вещественных чисел в известном смысле «плотнее» множества рациональных. Возникает закономерный вопрос, насколько часто на числовой прямой попадаются рациональные и вещественные числа и можно ли одни числа приблизить другими. Ответ на этот вопрос дают три леммы, основанные, в основном, на аксиоме Архимеда.

Лемма 1. Для любого вещественного числа и любого наперёд взятого положительного рационального расстояния найдётся пара рациональных чисел, отстоящих друг от друга менее, чем на это расстояние, таких что вещественное число лежит на отрезке между этими рациональными числами.

$$\forall a \in \mathbb{R}\ \forall \varepsilon \in \mathbb{Q}_+\ \exists q_1, q_2 \in \mathbb{Q}:\ (q_1 \le a \le q_2) \wedge (q_2 - q_1 < \varepsilon)$$

Эта лемма говорит о том, что любое вещественное число можно с заданной точностью с двух сторон приблизить рациональными числами.

Лемма 2. Между любыми двумя различными вещественными числами содержится рациональное число.

$$\forall a, b \in \mathbb{R}:\ a \neq b\ \exists q \in \mathbb{Q} : a < q < b$$

Очевидным следствием из этой леммы является тот факт, что между любыми двумя несовпадающими вещественными числами содержится целое бесконечное множество рациональных. Кроме того, ещё более очевидно, что между любыми двумя различными рациональными числами содержится вещественное.

Лемма 3. Приближение вещественного числа рациональными, описанное в лемме 1, идентифицирует вещественное число единственным образом.

$$(\forall a,b\in\mathbb{R}\,\forall\varepsilon\in\mathbb{Q}_+\,\exists q_1,q_2\in\mathbb{Q}:\ (q_1\le a\le q_2)\wedge(q_1\le b\le q_2)\wedge(q_2-q_1<\varepsilon))\Rightarrow a=b$$

Эти леммы прежде всего говорят о том, что множество вещественных чисел не такое «плотное» по сравнению с множеством рациональных чисел, как может показаться. Особенно ярко это иллюстрирует лемма 2. Все три леммы активно используются для доказательства различных теорем, связанных с операциями сложения и умножения вещественных чисел.

3.5.2. Теоретико-множественные свойства

Изначально вещественные числа были естественным обобщением рациональных, но у них впервые было обнаружено свойство несчётности, которое говорит о том, что множество вещественных чисел нельзя занумеровать, т. е. не существует биекции между множествами вещественных и натуральных чисел. Чтобы показать несчётность всего множества вещественных чисел, достаточно показать несчётность интервала $(0,1)$.

Пусть все числа указанного промежутка уже занумерованы некоторым образом. Тогда их можно выписать в следующем виде:

$$\begin{aligned} x_1 &= 0, a_{11}a_{12}\cdots a_{1m}\cdots \\ x_2 &= 0, a_{21}a_{22}\cdots a_{2m}\cdots \\ &\cdots \\ x_k &= 0, a_{k1}a_{k2}\cdots a_{km}\cdots \\ &\cdots \end{aligned}$$

Здесь a_{ij} — j-я цифра i-ого числа. Очевидно, что все числа указанного вида действительно принадлежат рассматриваемому промежутку, если только в каждом числе не все цифры сразу являются нулями или девятками.

Далее предлагается рассмотреть следующее число:

$$x = 0, d_1 d_2 \cdots d_m \cdots$$

Пусть каждая цифра d_i этого числа удовлетворяет следующим трём свойствам:

- $d_i \neq 0$
- $d_i \neq 9$
- $d_i \neq a_{ii}$

Такое число действительно существует на указанном промежутке, так как оно является вещественным, не совпадает ни с нулём, ни с единицей, а десятичных цифр достаточно, чтобы третье свойство выполнялось. Кроме этого, x интересно тем фактом, что оно не совпадает ни с одним из чисел x_j, выписанных выше, ведь иначе j-я цифра числа x совпала бы с j-ой цифрой числа x_j. Пришли к противоречию, заключающемуся в том, что как бы числа рассматриваемого промежутка ни были занумерованы, всё равно найдётся число из этого же промежутка, которому не присвоен номер. Это свидетельствует о том, что *множество вещественных чисел не является счётным*. Его мощность называется *мощностью континуума*.

Обобщение вещественных чисел

Поле вещественных чисел $\mathbb{R}$ постоянно служило в математике источником обобщений, причём в различных практически важных направлениях. Непосредственно к полю $\mathbb{R}$ примыкают следующие варианты обобщённых числовых систем.

1. **Комплексные числа**. Особенно плодотворны в алгебре и анализе.
2. **Интервальные числа**. Используются преимущественно в теории приближённых вычислений и в теории вероятностей.
3. Нестандартный анализ, который добавляет к вещественным числам **бесконечно малые и бесконечно большие числа** (разных порядков).

Прикладные применения

Математическая модель вещественных чисел повсеместно применяется в науке и технике для измерения непрерывно меняющихся величин. Однако это не главное её применение, потому что реально измеренные величины всегда имеют конечное число десятичных знаков, то есть являются рациональными числами. Основное назначение этой модели — служить **базой** для **аналитических методов исследования**. Огромный успех этих методов за последние три века показал, что модель вещественных чисел в большинстве случаев достаточно адекватно отражает **структуру непрерывных физических величин**.

Сказанное, конечно, не означает, что вещественная числовая прямая есть точный образ реальной непрерывной величины. Например, современной науке пока не известно, дискретны ли пространство и время или делимы неограниченно; однако даже во втором случае модель вещественных чисел для этих величин должна рассматриваться как приближённая, поскольку **понятия точки пространства и момента времени представляют собой идеализации, не имеющие реального аналога**. Этот фундаментальный вопрос широко обсуждается в науке, начиная с апорий Зенона. Приближённой эта модель является и в применении к величинам, которые в классической физике рассматривались как непрерывные, но в действительности оказались дискретными (квантуемыми).

4. Комплексные числа

4.1. Определения

Комплексные числа $\mathbb{C}$, являющиеся расширением множества действительных чисел. Они могут быть записаны в виде $z = x + iy$, где i — т. н. мнимая единица, для которой выполняется равенство $i^2 = -1$. Комплексные числа подразделяются на алгебраические и трансцендентные. При этом каждое действительное трансцендентное является иррациональным, а каждое рациональное число — действительным алгебраическим. Более общими (но всё ещё счётными) классами чисел, чем алгебраические,

являются периоды, вычислимые и арифметические числа (где каждый последующий класс шире, чем предыдущий).

Комплексные числа образуют алгебраически замкнутое поле — это означает, что многочлен степени n с комплексными коэффициентами имеет ровно nкомплексных корней (основная теорема алгебры). Это одна из главных причин широкого применения комплексных чисел в математических исследованиях. Кроме того, применение комплексных чисел позволяет удобно и компактно сформулировать многие математические модели, применяемые в математической физике и в естественных науках — электротехнике, гидродинамике, картографии, квантовой механике, теории колебаний и многих других.

Поле комплексных чисел можно понимать как расширение поля вещественных чисел, в котором многочлен $z^2 + 1$ имеет корень. Следующие две элементарные модели показывают, что непротиворечивое построение такой системы чисел возможно. Оба приведенных определения приводят к изоморфным расширениям поля вещественных чисел $\mathbb{R}$, как и любые другие конструкции поля разложения многочлена $z^2 + 1$.

4. 1.1. Стандартная модель

Комплексное число z можно определить как упорядоченную пару вещественных чисел (x, y). Введём операции сложения и умножения таких пар следующим образом:

- $(x,\ y) + (x',\ y') = (x + x',\ y + y')$;
- $(x,\ y) \cdot (x',\ y') = (xx' - yy',\ xy' + yx')$.

Вещественные числа являются в этой модели подмножеством множества комплексных чисел и представлены парами вида $(x,\ 0)$, причём операции с такими парами согласованы с обычными сложением и умножением вещественных чисел. Ноль представляется парой $0 = (0,\ 0)$, единица — $1 = (1,\ 0)$, а мнимая единица — $i = (0,\ 1)$. На множестве комплексных чисел ноль и единица

обладают теми же свойствами, что и на множестве вещественных, а квадрат мнимой единицы, как легко проверить, равен $(-1,\ 0)$, т. е. -1.

Несложно показать, что определённые выше операции имеют те же свойства, что и аналогичные операции с вещественными числами. Исключением являются только свойства, связанные с отношением порядка (*больше-меньше*), потому что расширить порядок вещественных чисел, включив в него все комплексные числа так, чтобы операции по-прежнему были согласованы с порядком, невозможно.

4.1.2. Матричная модель

Комплексные числа можно также определить как семейство вещественных матриц вида

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

с обычным матричным сложением и умножением. Действительной единице будет соответствовать

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

мнимой единице —

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Замечания

Ошибочно определение числа i как единственного числа, удовлетворяющего уравнению $x^2 = -1$, так как число $(-i)$ также удовлетворяет этому уравнению.

Следует также заметить, что выражение $\sqrt{-1}$, ранее часто использовавшееся вместо i, не вполне корректно, так как алгебраический корень определяется над множеством неотрицательных чисел. Вплоть до конца XIX века запись вроде $5+\sqrt{-3}$ считалась допустимой, но в настоящее время, во избежание ошибок, принято записывать это выражение как $5+i\sqrt{3}$. Пример возможной ошибки при неосторожном использовании устаревшей записи:

$$\sqrt{-3}\cdot\sqrt{-3}=\sqrt{(-3)\cdot(-3)}=\sqrt{9}=3,$$

в то время как правильная запись приводит к иному ответу:

$$\left(i\sqrt{3}\right)\cdot\left(i\sqrt{3}\right)=i\cdot i\cdot\sqrt{9}=-3.$$

4.2. Действия над комплексными числами

- Сравнение

  $a+bi=c+di$ означает, что $a=c$ и $b=d$ (два комплексных числа равны между собой тогда и только тогда, когда равны их действительные и мнимые части).

- Сложение

$$(a+bi)+(c+di)=(a+c)+(b+d)i.$$

- Вычитание

$$(a+bi)-(c+di)=(a-c)+(b-d)i.$$

- Умножение

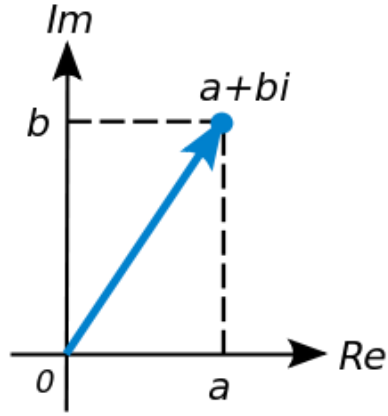
$$(a+bi)\cdot(c+di)=ac+bci+adi+bdi^2=(ac-bd)+(bc+ad)i.$$

- Деление

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \left(\frac{bc-ad}{c^2+d^2}\right)i.$$

4.3. Геометрическая модель

Рассмотрим плоскость с прямоугольной системой координат. Каждому комплексному числу $z = x + iy$ сопоставим точку плоскости с координатами $\{x, y\}$ (а также радиус-вектор, соединяющий начало координат с этой точкой). Такая плоскость называется комплексной. Вещественные числа на ней занимают горизонтальную ось, мнимая единица изображается единицей на вертикальной оси; по этой причине горизонтальная и вертикальная оси называются соответственно *вещественной* и *мнимой* осями.



Геометрическое представление комплексного числа

Часто бывает удобно рассматривать на комплексной плоскости также полярную систему координат, в которой координатами точки являются расстояние до начала координат (*модуль*) и угол радиус-вектора точки (показанного синей стрелкой на рисунке) с горизонтальной осью (*аргумент*). Подробнее см. ниже.

В этом наглядном представлении сумма комплексных чисел соответствует векторной сумме соответствующих радиус-векторов. При перемножении комплексных чисел их модули перемножаются, а аргументы складываются. Если модуль второго сомножителя равен 1, то умножение на него геометрически означает поворот радиус-вектора первого числа на угол, равный аргументу второго числа. Этот факт объясняет широкое использование комплексного представления в теории колебаний, где вместо терминов «модуль» и «аргумент» используются термины «амплитуда» и «фаза».

Геометрическая модель комплексных чисел широко используется в планиметрии: многие планиметрические теоремы можно доказать как некоторые комплексные тождества. Часто этот метод даёт наиболее простое доказательство.

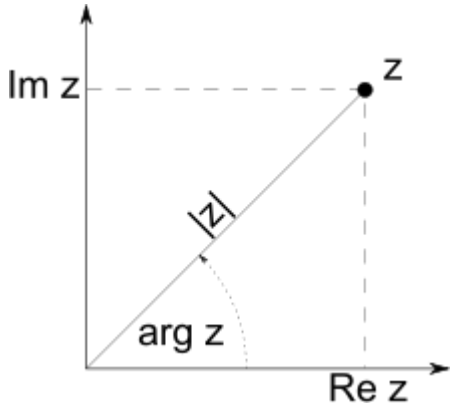
4.4. Связанные определения

Пусть $z = x + iy$ — комплексное число, где x и y — вещественные числа. Числа $x = \Re(z)$ или $\mathrm{Re}\ z$ и $y = \Im(z)$ или $\mathrm{Im}\ z$ называются соответственно вещественной и мнимой (аналогично англ. *real, imaginary*) частями z.

- Если $x = 0$, то z называется мнимым или чисто мнимым числом.
- Если $y = 0$, то z является действительным (вещественным) числом.

4.4.1. Модуль и аргумент

Модулем (абсолютной величиной) комплексного числа называется длина радиус-вектора соответствующей точки комплексной плоскости (или, что то же, расстояние между точкой комплексной плоскости, соответствующей этому числу, и началом координат).



Модуль, аргумент, вещественная и мнимая части

Модуль комплексного числа z обозначается $|z|$ и определяется выражением $|z| = \sqrt{x^2 + y^2}$. Часто обозначается буквами r или ρ. Если z является вещественным числом, то $|z|$ совпадает с абсолютной величиной этого вещественного числа.

Для любых $z, z_1, z_2 \in \mathbb{C}$ имеют место следующие свойства модуля. :

1) $|z| \geqslant 0$, причём $|z| = 0$ тогда и только тогда, когда $z = 0$;;
2) $|z_1 + z_2| \leqslant |z_1| + |z_2|$ (неравенство треугольника);
3) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$;
4) $|z_1/z_2| = |z_1|/|z_2|$.

Из третьего свойства следует $|a \cdot z| = |a| \cdot |z|$, где $a \in \mathbb{R}$. Данное свойство модуля вместе с первыми двумя свойствами вводят на множестве комплексных чисел структуру двумерного нормированного пространства над полем $\mathbb{R}$.

5) Для пары комплексных чисел z_1 и z_2 модуль их разности $|z_1 - z_2|$ равен расстоянию между соответствующими точками комплексной плоскости.

Угол φ(в радианах) радиус-вектора точки, соответствующей числу z, называется аргументом числа z и обозначается $\mathrm{Arg}(z)$.

- Из этого определения следует, что

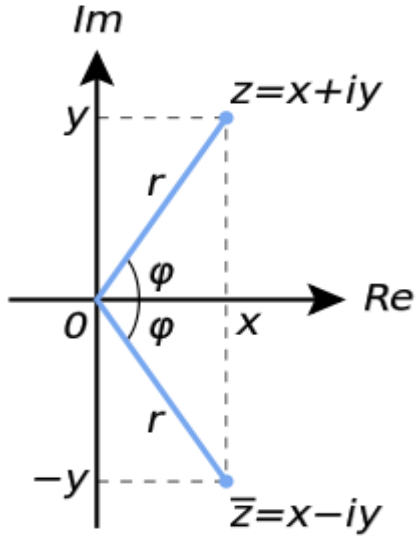
$$\mathrm{tg}\ \varphi = \frac{y}{x};\ \cos\varphi = \frac{x}{|z|};\ \sin\varphi = \frac{y}{|z|}.$$

- Для комплексного нуля значение аргумента не определено, для ненулевого числа z аргумент определяется с точностью до $2k\pi$, где k — любое целое число.
- Главным значением аргумента называется такое значение φ, что $-\pi < \varphi \leqslant \pi$. Часто главное значение обозначается $\arg(z)$. Главное значение аргумента обратного числа отличается знаком от аргумента исходного:

$$\arg\left(\frac{1}{z}\right) = -\arg(z)$$

4.4.2. Сопряжённые числа

Если комплексное число $z = x + iy$, то число $\bar{z} = x - iy$ называется сопряжённым (или комплексно сопряжённым) к z (обозначается также z^*). На комплексной плоскости сопряжённые числа получаются зеркальным отражением друг друга относительно вещественной оси. Модуль сопряжённого числа такой же, как у исходного, а их аргументы отличаются знаком.



Геометрическое представление сопряжённых чисел

Переход к сопряжённому числу можно рассматривать как одноместную операцию; перечислим её свойства.

- $\bar{\bar{z}} = z$ (сопряжённое к сопряжённому есть исходное).
- $z \cdot \bar{z} = |z|^2$.
- $\overline{z_1 \pm z_2} = \bar{z}_1 \pm \bar{z}_2$.
- $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$.
- $z_1 / z_2 = \bar{z}_1 / \bar{z}_2$.

Обобщение: $\overline{p(z)} = p(\bar{z})$, где $p(z)$ — произвольный многочлен с вещественными коэффициентами.

- $|\bar{z}| = |z|$
- $\operatorname{Re} z = \dfrac{z + \bar{z}}{2}; \quad \operatorname{Im} z = \dfrac{z - \bar{z}}{2i}.$

Значимость сопряжения объясняется тем, что оно является образующей группы Галуа $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2$.

4.5. Представление комплексных чисел

4.5.1. Алгебраическая форма

Запись комплексного числа z в виде $x + iy,\ x,\ y \in \mathbb{R}$, называется *алгебраической формой* комплексного числа.

Сумма и произведение комплексных чисел могут быть вычислены непосредственным суммированием и перемножением таких выражений, как обычно раскрывая скобки и приводя подобные, чтобы представить результат тоже в стандартной форме (при этом надо учесть, что $i^2 = -1$):

$$(a + ib) + (c + id) = (a + c) + i(b + d);$$
$$(a+ib)\cdot(c+id) = ac+iad+ibc+i^2bd = ac+iad+ibc-bd = (ac-bd)+i(ad+bc).$$

4.5.2. Тригонометрическая и показательная формы

Если вещественную x и мнимую y части комплексного числа выразить через модуль $r = |z|$ и аргумент φ ($x = r\cos\varphi$, $y = r\sin\varphi$), то всякое комплексное число z, кроме нуля, можно записать в *тригонометрической форме*

$$z = r(\cos\varphi + i\sin\varphi).$$

Также может быть полезна *показательная* форма записи комплексных чисел, тесно связанная с тригонометрической через формулу Эйлера:

$$z = re^{i\varphi},$$

где $e^{i\varphi}$ — расширение экспоненты для случая комплексного показателя степени.

Отсюда вытекают следующие широко используемые равенства:

$$\cos\varphi = \frac{(e^{i\varphi} + e^{-i\varphi})}{2}; \quad \sin\varphi = \frac{(e^{i\varphi} - e^{-i\varphi})}{2i}.$$

4.5.3. Формула Муавра и извлечение корней из комплексных чисел

Эта формула позволяет возводить в целую степень ненулевое комплексное число, представленное в тригонометрической форме. Формула Муавра имеет вид:

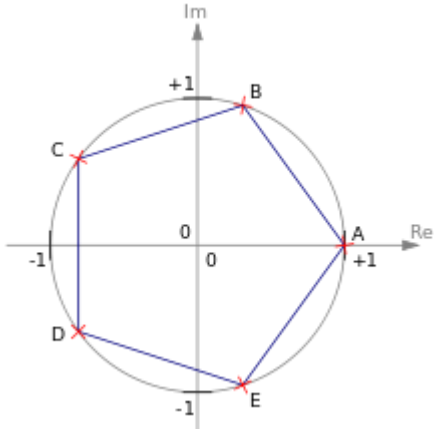
$$z^n = [r(\cos\varphi + i\sin\varphi)]^n = r^n(\cos n\varphi + i\sin n\varphi),$$

где r — модуль, а φ — аргумент комплексного числа. В современной символике она опубликована Эйлером в 1722 году. Приведенная формуле справедлива при любом целом *n*, не обязательно положительном.

Аналогичная формула применима также и при вычислении корней n-ой степени из ненулевого комплексного числа:

$$z^{1/n} = [r(\cos(\varphi + 2\pi k) + i\sin(\varphi + 2\pi k))]^{1/n} =$$
$$= r^{1/n}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right),$$
$$n > 1, k = 0,\ 1,\ \ldots,\ n-1.$$

Отметим, что корни n-й степени из ненулевого комплексного числа всегда существуют, и их количество равно n. На комплексной плоскости, как видно из формулы, все эти корни являются вершинами правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{r}$ с центром в начале координат (см. рисунок).



Корни пятой степени из единицы (вершины пятиугольника)

4.6. Историческая справка

Впервые, по-видимому, мнимые величины появились в известном труде «Великое искусство, или об алгебраических правилах» Кардано (1545), который счёл их непригодными к употреблению. Пользу мнимых величин, в частности, при решении кубического уравнения, в так называемом неприводимом случае (когда вещественные корни многочлена выражаются через кубические корни из мнимых величин), впервые оценил Бомбелли (1572). Он же дал некоторые простейшие правила действий с комплексными числами.

Выражения вида $a + b\sqrt{-1}$, появляющиеся при решении квадратных и кубических уравнений, стали называть «мнимыми» в XVI—XVII веках, однако даже для многих крупных ученых XVII века алгебраическая и геометрическая сущность мнимых величин представлялась неясной. Лейбниц, например, писал: «Дух божий нашёл тончайшую отдушину в этом чуде анализа, уроде из мира идей, двойственной сущности, находящейся между бытием и небытием, которую мы называем мнимым корнем из отрицательной единицы».

Долгое время было неясно, все ли операции над комплексными числами приводят к комплексным результатам, или, например, извлечение корня может привести к открытию какого-то нового типа чисел. Задача о выражении корней степени n из данного числа была решена в работах Муавра (1707) и Котса (1722).

Символ $i = \sqrt{-1}$ предложил Эйлер (1777, опубл. 1794), взявший для этого первую букву слова лат. *imaginarius*. Он же распространил все стандартные функции, включая логарифм, на комплексную область. Эйлер также высказал в 1751 году мысль об алгебраической замкнутости поля комплексных чисел. К такому же выводу пришел д'Аламбер (1747), но первое строгое доказательство этого факта принадлежит Гауссу (1799). Гаусс и ввёл в широкое употребление термин «комплексное число» в 1831 году, хотя этот термин ранее использовал в том же смысле французский математик Лазар Карно в 1803 году.

Геометрическое истолкование комплексных чисел и действий над ними появилось впервые в работе Весселя (1799). Первые шаги в этом направлении были сделаны Валлисом (Англия) в 1685 году. Современное геометрическое представление, иногда называемое «диаграммой Аргана», вошло в обиход после опубликования в 1806-м и 1814-м годах работы Ж. Р. Аргана, повторявшей независимо выводы Весселя. Термины «модуль», «аргумент» и «сопряжённое число» ввёл Коши.

Арифметическая модель комплексных чисел как пар вещественных чисел была построена Гамильтоном (1837); это доказало непротиворечивость их свойств. Гамильтон предложил и обобщение комплексных чисел — кватернионы, алгебра которых некоммутативна.

5. Функции комплексного переменного

5.1. Понятие функции комплексного переменного

Понятие комплексного числа было рассмотрено в разделе 1. Как известно, существуют так же многочлены $Q_n(z)$ от комплексного переменного. Многочлен является простейшим примером функции комплексного переменного.

Как мы уже говорили, комплексные числа мы условились изображать точками плоскости, где задана прямоугольная система координат.

Дадим понятие функции от комплексного переменного.

Пусть даны две плоскости комплексных чисел $z = x + iy$ и $w = u + iv$ (рис. 1).

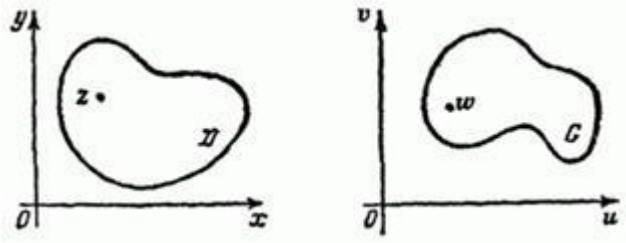


Рис. 1

Рассмотрим некоторое множество точек D в плоскости z и множество G в плоскости w. Если каждому числу $z \in D$ по некоторому закону поставлено в соответствие определенное комплексное число $w \in G$, то говорят, что на множестве D задана однозначная функция комплексного переменного, отображающая множество D в множество G. Символически это обозначают так:

$$w = f(z)$$

Множество D называют областью определения функции $f(z)$. Если каждая точка множества G является значением функции, то говорят, что G - область значений этой функции или образ множества D при помощи функции $f(G) = f(D)$. В этом случае говорят еще, что функция f отображает D на G.

Функцию $f(z)$ можно записать в виде

$$f(z)=u(x,y)+iv(x,y) \qquad ((x,y)\in D),$$

где

$$u(x,y)=\operatorname{Re} f(z),\ v(x,t)=\operatorname{Im} f(z) \qquad ((x,y)\in D),$$

- действительные функции от переменных x,y.

Если каждому $z\in D$ соответствует несколько разных значений w, то функция $w=f(z)$ называется многозначной.

Понятия предела и непрерывности функции комплексного переменного вводятся аналогично, как это делается для функции действительного переменного, необходимо лишь всюду вместо абсолютной величины писать модуль комплексного числа.

Говорят, что функция

$$w=f(z)=u(x,y)+iv(x,y)$$

имеет предел в точке z_0, равный числу $A=a+ib$, если

$$\lim_{|z-z_0|\to 0}|f(z)-A|=0. \qquad (1)$$

В этом случае пишут

$$\lim_{z\to z_0} f(z)=A.$$

На языке функций u и v свойство (1) записывается в виде равенства

$$\lim_{|z-z_0|\to 0}\sqrt{(u-a)^2+(v-b)^2}=0 \tag{2}$$

или, что все равно, в виде двух равенств

$$\lim_{(x,y)\to(x_0,y_0)}u(x,y)=a\,,\qquad \lim_{(x,y)\to(x_0,y_0)}v(x,y)=b\,. \tag{3}$$

Для комплексных функций $f(z)$ и $g(z)$ имеют место свойства, аналогичные соответствующим свойствам действительных функций:

$$\left.\begin{aligned}
&\lim_{z\to z_0}\left[f(z)\pm g(z)\right]=\lim_{z\to z_0}f(z)\pm\lim_{z\to z_0}g(z),\\
&\lim_{z\to z_0}\left[f(z)g(z)\right]=\lim_{z\to z_0}f(z)\lim_{z\to z_0}g(z),\\
&\lim_{z\to z_0}\frac{f(z)}{g(z)}=\frac{\lim\limits_{z\to z_0}f(z)}{\lim\limits_{z\to z_0}g(z)}\quad\left(\lim_{z\to z_0}g(z)\neq 0\right).
\end{aligned}\right\} \tag{4}$$

Как обычно, формулы (4) надо понимать в том смысле, что если пределы, стоящие в их правых частях, существуют, то существуют также пределы, стоящие в их левых частях, и выполняется соответствующее равенство.

Функция $w=f(z)=u(x,y)+iv(x,y)$ называется непрерывной в точке z_0, если для нее выполняется свойство

$$\lim_{z\to z_0}f(z)=f(z_0)\,,\quad f(z+\Delta z)-f(z_0)\to 0\,,\ \Delta z\to 0\,. \tag{5}$$

Таким образом, непрерывная в точке z_0 функция должна быть определена в окрестности этой точки, в том числе и в ней самой и должно выполняться равенство (5). Равенство (5) эквивалентно двум равенствам:

$$\lim_{(x,y)\to(x_0,y_0)} u(x,y) = u(x_0,y_0), \quad \lim_{(x,y)\to(x_0,y_0)} v(x,y) = v(x_0,y_0).$$

Следовательно, непрерывность f в точке z_0 эквивалентна непрерывности функций u и v в точке (x_0,y_0).

Из свойств (4) следует, что сумма, разность, произведение и частное непрерывных в точке z_0 комплексных функций $f(z)$ и $g(z)$ есть непрерывная функция в этой точке. В случае частного надо в этой формулировке считать, что $g(z_0)\neq 0$.

Пример 1. Функция $w=|z|=\sqrt{x^2+y^2}$ задана на всей комплексной плоскости. Ее значения – неотрицательные числа. Эта функция непрерывна во всех точках комплексной плоскости:

$$\big||z+\Delta z|-|z|\big|\le|\Delta z|\to 0 \quad (\Delta z\to 0).$$

Пример 2.

$$w=\arg z=\arg z+2k\pi \quad (k=0,\pm1,\ldots). \tag{6}$$

Эта функция многозначная (бесконечнозначная); $\varphi=\arg z$ - главное значение аргумента $(0\le\varphi\le 2\pi)$.

Пример 3. Функция $w=z$. Она непрерывна:

$$|z+\Delta z-z|=|\Delta z|\to 0 \quad (\Delta z\to 0).$$

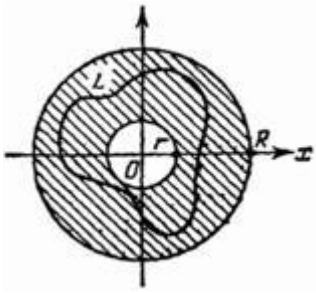


Рис. 2

Но тогда и функция $z^n \ (n=2,3,...)$ непрерывна как произведение конечного числа непрерывных функций.

Множество комплексных чисел D будем называть областью, если D, как множество точек плоскости, открыто и связно.

Область D называется односвязной, если любая непрерывная замкнутая самонепересекающаяся кривая, проведенная в D, ограничивает некоторую область G, целиком принадлежащую D. Область, не обладающую этим свойством, будем называть многосвязной.

Пример 4. Кольцо $r<|z|<R$ - многосвязная (двусвязная) область. Кривая L (рис. 2) принадлежит кольцу, но ограничивает область, не входящую целиком в него.

Термин **комплексная функция** может относиться к двум видам функций:

Комплекснозначная функция — функция вещественного переменного, имеющая комплексные значения:

$$f: \mathbb{R} \to \mathbb{C}.$$

Как мы говорили, такая функция может быть представлена в виде

$$f(x) = u(x) + iv(x),$$

где $u(x)$ и $v(x)$ — вещественные функции. Функция $u(x)$ называется *вещественной частью* функции $f(x)$, а $v(x)$ — её *мнимой частью*.

Функция комплексного переменного

Это понятие — обобщение предыдущего варианта:

$$f: \mathbb{C} \to \mathbb{C}.$$

Такими функциями занимается отдельная область математического анализа — теория функций комплексного переменного, или комплексный анализ.

Функция также может быть представлена в виде

$$f(z) = u(z) + iv(z),$$

однако имеется более глубокая связь между *u* и *v*. Например, для того, чтобы функция $f(z)$ была дифференцируема, должны выполняться условия Коши — Римана:

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y},$$
$$\frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

5.2. Комплексный анализ

5.2.1. Общие понятия

Каждая комплексная функция $w = f(z) = f(x + iy)$ может рассматриваться как пара вещественных функций от двух переменных: $f(z) = u(x,\ y) + iv(x,\ y)$, определяющих её вещественную и мнимую часть соответственно. Функции u, v называются *компонентами* комплексной функции $f(z)$.

Понятие предела для последовательности и функции вводится так же, как и в вещественном случае, с заменой абсолютной величины на комплексный модуль. Если $\lim\limits_{z \to a+bi} f(z) = A + Bi$, то $\lim\limits_{x \to a,\ y \to b} u(x,\ y) = A$ и $\lim\limits_{x \to a,\ y \to b} v(x,\ y) = B$. Верно и обратное: из существования пределов компонент вытекает существование предела самой функции, и компонентами предела будут пределы компонентов. Непрерывность комплексной функции тоже определяется так же, как в вещественном случае, и она равносильна непрерывности обеих её компонент.

Все основные теоремы о пределе и непрерывности вещественных функций имеют место и в комплексном случае, если это расширение не связано со сравнением комплексных величин на *больше-меньше*. Например, нет аналога теореме о промежуточных значениях непрерывной функции.

ε-окрестность числа z_0 определяется как множество точек z, удалённых от z_0 менее чем на ε: $|z - z_0| < \varepsilon$. На комплексной плоскости ε-окрестность представляет собой круг радиуса ε с центром в z_0.

5.2.2. Бесконечно удалённая точка

В комплексном анализе часто полезно рассматривать *полную комплексную плоскость*, дополненную по сравнению с обычной *бесконечно удалённой точкой*: $z = \infty$. При таком подходе

неограниченно возрастающая (по модулю) последовательность считается сходящейся к бесконечно удалённой точке. Алгебраические операции с бесконечностью не производятся, хотя несколько алгебраических соотношений имеют место:

- $\frac{z}{\infty} = 0; z + \infty = \infty (z \neq \infty)$
- $z \cdot \infty = \infty; \frac{z}{0} = \infty (z \neq 0)$

ε-окрестностью бесконечно удалённой точки считается множество точек z, модуль которых больше, чем ε, то есть внешняя часть ε-окрестностей начала координат.

5.2.3. Дифференцирование

Определение

Производная для комплексной функции одного аргумента $w = f(z)$ определяется так же, как и для вещественной:

$$f'(z) = \frac{df}{dz} = \lim_{h \to 0} \frac{f(z+h) - f(z)}{h}$$

(здесь h — комплексное число). Если этот предел существует, функция называется *дифференцируемой* или *голоморфной*. При этом

$$f(z+h) - f(z) = \frac{df}{dz} \cdot h + o(h).$$

Следует учитывать одну важную особенность: поскольку комплексная функция задана на плоскости, существование приведённого предела означает, что он одинаков при стремлении к z с любого направления. Этот факт накладывает существенные ограничения на вид функций-компонент u, v и определяет их жёсткую взаимосвязь (условия Коши — Римана):

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}; \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

Отсюда следует, что дифференцируемости компонент u и v недостаточно для дифференцируемости самой функции.

Более того, имеют место следующие свойства, отличающие комплексный анализ от вещественного:

- Всякая дифференцируемая в некоторой окрестности точки z комплексная функция дифференцируема неограниченное число раз и аналитична, то есть её ряд Тэйлора сходится к данной функции во всех точках этой окрестности (в литературе наряду с термином *аналитическая функция* используется также его синоним «голоморфная функция»).
- (Теорема Лиувилля): Если функция дифференцируема на всей комплексной плоскости и не является константой, то её модуль не может быть ограничен.
- Обе компоненты дифференцируемой комплексной функции являются гармоническими функциями, то есть удовлетворяют уравнению Лапласа:

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} = 0; \qquad \frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} = 0.$$

- Любая гармоническая функция может быть как вещественной, так и мнимой компонентой дифференцируемой функции. При этом другая компонента определяется однозначно (из условий Коши — Римана), с точностью до константы-слагаемого.

Таким образом, любая дифференцируемая комплексная функция — это функция вида $u + iv$, где u, v — взаимосвязанные гармонические функции двух аргументов.

Другие свойства

Пусть функции $f(z)$ и $g(z)$ дифференцируемы в области $G \subset \mathbb{C}$. Тогда $f(z) \pm g(z)$ и $f(z) \cdot g(z)$ также дифференцируемы в этой области. Если $g(z)$ в области G не обращается в ноль, то $\frac{f(z)}{g(z)}$ будет дифференцируема в G. Композиция функций $f(g(z))$ дифференцируема всюду, где она определена. Если производная функции $w = f(z)$ в области G не обращается в ноль, то существует обратная к ней функция $z = \varphi(w)$, и она будет дифференцируема.

Производные суммы, разности, произведения, частного от деления, композиции функций и обратной функции вычисляется по тем же формулам, что и в вещественном анализе.

Геометрический смысл производной

Каждая комплексная функция $w = f(z) = u(x,\ y) + iv(x,\ y)$ определяет некоторое отображение комплексной плоскости с координатами $(x,\ y)$ на другую комплексную плоскость с координатами $(u,\ v)$. При этом выражение:

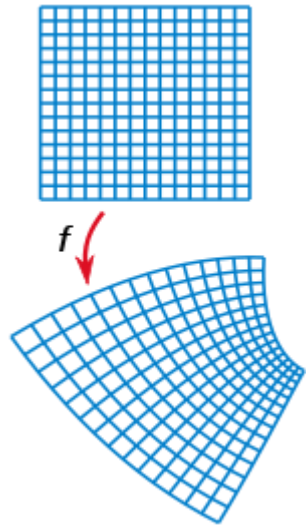
$$\left| \frac{f(z+h) - f(z)}{h} \right| = k(h)$$

при малом h геометрически можно истолковать как *коэффициент масштабирования*, которое выполняет данное отображение при переходе от точки z к точке $z + h$. Существование предела $\lim\limits_{h \to 0} k(h)$, то есть модуля производной $|f'(z)| = k$, означает, что коэффициент масштабирования одинаков в любом направлении от

точки z, т. е. не зависит от направления. Вообще говоря, коэффициент масштабирования меняется от точки к точке.

Если коэффициент масштабирования $k > 1$, то в окрестности точки z расстояния между точками увеличиваются, и коэффициент масштабирования называют *коэффициентом растяжения*. Если коэффициент масштабирования $k < 1$, то в окрестности точки z расстояния между точками уменьшаются, и коэффициент масштабирования называют *коэффициентом сжатия*.

Что касается аргумента производной, то он определяет угол поворота гладкой кривой, проходящей через точку z. Все гладкие кривые при таком отображении поворачиваются на один и тот же угол. Отображения, сохраняющие углы, называются *конформными*; таким образом, любая дифференцируемая комплексная функция определяет конформное отображение (в той области, где её производная не обращается в ноль).



Пример конформного отображения. Видно, что углы сохраняются.

С этим фактом связано широкое применение комплексных функций в картографии и гидродинамике.

5.2.4. Интегрирование

Понятие первообразной комплексной функции (неопределённого интеграла) вводится так же, как в вещественном случае. Однако аналог определённого интеграла в интервале от a до b на комплексной плоскости, вообще говоря, не существует, так как путь от начальной точки до конечной неоднозначен. Поэтому основным видом комплексного интеграла является криволинейный интеграл, зависящий от конкретного пути. Ниже будут указаны условия, при выполнении которых интеграл не зависит от пути, и тогда интеграл «от точки до точки» может быть определён корректно.

Пусть уравнение $z = z(t),\ a \leqslant t \leqslant b$ определяет некоторую кусочно-гладкую кривую γ в комплексной плоскости, а функция $f(z)$ определена в точках этой кривой. Разделим интервал задания параметра на n равных частей: $a = t_0 < t_1 < \ldots < t_n = b$ и рассмотрим интегральную сумму:

$$\sum_{1 \leqslant k \leqslant n} f(z(t_k))(z(t_k) - z(t_{k-1})).$$

Предел этой суммы при неограниченном возрастании n называется (комплексным) интегралом по кривой γ от данной функции $f(z)$; он обозначается:

$$\int_{\gamma} f(z)\, dz.$$

Для любой функции $f(z)$, непрерывной вдоль γ, этот интеграл существует и может быть вычислен через обычный вещественный интеграл по параметру:

$$\int_\gamma f(z)\,dz = \int_a^b f(z(t))z'(t)\,dt = \int_\gamma (u\,dx - v\,dy) + i\int_\gamma (v\,dx + u\,dy).$$

Здесь $u,\ v$— компоненты $f(z)$. Из этого представления сразу следует, что свойства комплексного интеграла аналогичны свойствам вещественного криволинейного интеграла.

Контурный интеграл

Особый практический интерес представляют интегралы по (замкнутому) контуру, то есть по кусочно-гладкой кривой без точек самопересечения, у которой начальная точка совпадает с конечной. Контур можно обходить в двух направлениях; положительным считается направление, при котором ограниченная контуром область располагается слева по ходу движения.

Если кривая γ образует замкнутый контур, употребляется особое обозначение интеграла:

$$\oint_\gamma f(z)\,dz.$$

Имеет место важная интегральная теорема Коши: для любой функции $f(z)$, аналитической в односвязной области $A \subset \mathbb{C}$ и для любого замкнутого контура $\gamma \subset A$ справедливо соотношение:

$$\oint_\gamma f(z)\,dz = 0$$

.

Следствие: пусть функция $f(z)$, аналитична в односвязной области $A \subset \mathbb{C}$, а точки z_1, z_2 из области A соединены некоторой кривой γ. Тогда интеграл $\int_\gamma f(z)\,dz$ зависит только от точек z_1, z_2, но не

от выбора соединяющей их кривой γ, так что можно обозначить его

$$\int_{z_1}^{z_2} f(z)\,dz$$

,

и имеет место теорема Ньютона — Лейбница:

$$\int_{z_1}^{z_2} f(z)\,dz = F(z_2) - F(z_1),$$

где *F(z)* — первообразная для $f(z)$.

Другие инструменты для исследования комплексных и вещественных интегралов:

- Интегральная формула Коши и её следствия: принцип максимума модуля, теоремы о среднем
- Основная теорема о вычетах

5.2.5. Теоремы единственности и аналитическое продолжение

Нулём функции $f(z)$ называется точка z_0, в которой функция обращается в ноль: $f(z_0) = 0$.

Теорема о нулях аналитической функции. Если нули функции $f(z)$, аналитической в области D, имеют предельную точку внутри D, то функция $f(z)$ всюду в D равна нулю.

Следствие: если функция $f(z)$ аналитическая в области D и не равна тождественно нулю, то в любой ограниченной замкнутой подобласти $C \subset D$ у неё может быть лишь конечное число нулей.

Теорема единственности аналитической функции. Пусть $\{z_n\}$— сходящаяся последовательность различных точек области D. Если две аналитические функции $f(z), g(z)$ совпадают во всех точках этой последовательности, то они тождественно равны в D.

В частности, если две аналитические функции совпадают на некоторой кусочно-гладкой кривой в D, то они совпадают всюду в D. Это значит, что значения аналитической функции даже на небольшом участке области полностью определяют поведение функции во всей области её определения. Задав аналитическую функцию на кривой (например, на вещественной оси), мы однозначно определяем её расширение (если оно возможно) на более широкую область, которое называется аналитическим продолжением исходной функции.

Все стандартные функции анализа — многочлен, дробно-линейная функция, степенная функция, экспонента, тригонометрические функции, обратные тригонометрические функции, логарифм — допускают аналитическое продолжение на комплексную плоскость. При этом для их аналитических продолжений будут иметь место те же алгебраические, дифференциальные и другие тождества, что и для вещественного оригинала, например:

$$\sin^2 z + \cos^2 z = 1; \qquad e^u \cdot e^v = e^{u+v}$$

5.2.6. Разложение в ряд

Степенной ряд

Определение суммы числового ряда и признаки сходимости в комплексном анализе практически такие же, как в вещественном, с заменой абсолютной величины на комплексный модуль; исключение составляют признаки сходимости, в которых происходит сравнение на больше-меньше самих элементов ряда, а не их модулей.

Всякая дифференцируемая в точке z_0 функция разлагается в окрестности этой точки в степенной ряд Тэйлора:

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

Коэффициенты ряда вычисляются по обычным формулам. Этот ряд сходится к функции $f(z)$ в некотором круге радиуса R с центром в точке z_0, который служит аналогом интервала сходимости вещественного ряда. В этом круге ряд абсолютно сходится, а вне его расходится. При этом возможны 3 случая.

1. Ряд сходится в круге конечного и ненулевого радиуса.
2. Ряд сходится во всей комплексной плоскости, то есть $R = \infty$. Такие функции называются **целыми.**
3. Ряд сходится только в точке z_0. Пример: $\sum_{n=0}^{\infty} n!(z - z_0)^n$

   Такие точки z_0 называются *особыми* для функции $f(z)$. Неособые точки называются *правильными.* Внутренность круга сходимости состоит из правильных точек.

Граница круга сходимости содержит хотя бы одну особую точку. Отсюда следует, что радиус круга сходимости в точке z_0 равен расстоянию от z_0 до ближайшей к ней особой точки.

Теорема Абеля: если R— радиус круга сходимости степенного ряда, то в любом круге с тем же центром, но меньшего радиуса, ряд сходится равномерно.

Ряд Лорана

Представляет большой интерес при моделированиии исследование поведения функции вблизи изолированной особой точки, т. е. точки, в окрестности которой функция аналитична, но в самой точке либо не аналитична, либо не определена. Степенной ряд здесь бесполезен, поэтому вводится более общий ряд Лорана:

$$\sum_{n=-\infty}^{\infty} c_n (z - z_0)^n = \sum_{n=0}^{\infty} c_n (z - z_0)^n + \sum_{n=1}^{\infty} \frac{c_{-n}}{(z - z_0)^n}$$

Если область сходимости ряда Лорана не пуста, она представляет собой круговое кольцо: $r < |z - z_0| < R$.

Основная теорема: если функция $f(z)$ аналитична в круговом кольце, то она может быть представлена в этом кольце сходящимся рядом Лорана, причём однозначно.

Как и для степенного ряда, границы кольца сходимости определяются распределением особых точек функции. По виду ряда Лорана можно сделать некоторые выводы о поведении функции вблизи точки z_0.

1. Устранимая особая точка: если ряд Лорана не содержит элементов с отрицательными степенями $z - z_0$. Тогда это просто степенной ряд, определяющий функцию в некотором круге, окружающем z_0. Сумма ряда в этом круге конечна и может отличаться от $f(z)$ только в точке z_0, так что достаточно переопределить $f(z_0)$, чтобы функция стала аналитичной во всём круге. Имеет место следующий признак: если функция вблизи z_0 аналитична и ограничена, то z_0 — устранимая особая точка.
2. Полюс: если ряд Лорана содержит конечное число элементов с отрицательными степенями $z - z_0$. В этом случае функция в точке z_0 бесконечна (по модулю).
3. Существенно особая точка: если ряд Лорана содержит бесконечное число элементов с отрицательными степенями $z - z_0$. В этом случае функция в точке z_0 не может быть корректно определена так, чтобы быть непрерывной.

5.2.7. Приложения в вещественном анализе

С помощью теории вычетов, являющейся частью ТФКП, вычисляются многие сложные интегралы по замкнутым контурам.

Средствами комплексного анализа объясняются некоторые моменты, не поддающиеся простой интерпретации в терминах вещественного анализа. Приведем классический пример: функция

$$f(x) = \frac{1}{1+x^2}$$

непрерывна и бесконечно дифференцируема на всей вещественной прямой. Рассмотрим её ряд Тейлора

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + \dots$$

Этот ряд сходится только в интервале $(-1;\ 1)$, хотя точки ± 1 не являются какими-то особенными для $f(x)$.

Положение проясняется при переходе к функции комплексного переменного $f(z) = \frac{1}{1+z^2}$, у которой обнаруживаются две особые точки: $\pm i$. Соответственно, эту функцию можно разложить в ряд Тейлора только в круге $\Delta = \{z: |z| < 1\}$.

Примеры функций комплексной переменной (ФКП)

$$w = f(z),\ z \in D,\ D \subset C,$$

$$w = u(x,\ y) + iv(x,\ y),\ z = x + iy.$$

Экспонента

$$w = e^z = e^x(\cos y + i \sin y),$$

$$e^x = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \dots + \frac{z^n}{n!} + \dots,\ z \in C.$$

Свойства:

$$e^{z_1+z_2}=e^{z_1}e^{z_2},\ e^{z+2\pi i}=e^{z}$$

(периодичность),

$$\left|e^{z}\right|=e^{x},\ Arg\,e^{z}=y+2\pi k,\ k\in Z,$$

$$e^{2k\pi i}=1,\ k\in Z,\ e^{\pi i}=-1,\ e^{-\pi i}=-1,\ e^{\pi i/2}=i,\ e^{-\pi i/2}=-i.$$

Тригонометрические функции

$$\cos z=\frac{e^{iz}+e^{-iz}}{2},\quad \sin z=\frac{e^{iz}-e^{-iz}}{2i},$$

$$tgz=\frac{\sin z}{\cos z}=\frac{e^{iz}-e^{-iz}}{i\left(e^{iz}+e^{-iz}\right)},$$

$$ctgz=\frac{\cos z}{\sin z}=\frac{i\left(e^{iz}+e^{-iz}\right)}{e^{iz}-e^{-iz}},$$

$$\cos z=1-\frac{z^2}{2!}+\frac{z^4}{4!}-\ldots+(-1)^n\frac{z^{2n}}{(2n)!}+\ldots,\ z\in C,$$

$$\sin z=z-\frac{z^3}{3!}+\frac{z^5}{5!}-\ldots+(-1)^n\frac{z^{2n+1}}{(2n+1)!}+\ldots,\ z\in C,$$

$$\cos^2 z+\sin^2 z=1,\quad \cos(z+2\pi)=\cos z,\quad \sin(z+2\pi)=\sin z,$$

$$\cos^2 z-\sin^2 z=\cos 2z,\quad 2\sin z\cos z-\sin 2z,$$

$$\sin(z_1+z_2)=\sin z_1\cos z_2+\cos z_1\sin z_2,$$

$$\cos(z_1+z_2)=\cos z_1\cos z_2-\sin z_1\sin z_2,$$

$$\mathrm{Re}\cos z=\cos x\,\mathrm{ch}y,\quad \mathrm{Im}\cos z=-\sin x\,\mathrm{sh}y,$$

$$\operatorname{Re}\sin z = \sin x \operatorname{ch} y, \quad \operatorname{Im}\sin z = \cos x \operatorname{sh} y,$$

$$\cos z = \operatorname{ch} iz, \quad \sin z = -i \operatorname{sh} iz,$$

$$tgz = -i\, th\, iz, \quad ctgz = i\, cth\, iz.$$

Гиперболические функции

$$chz = \frac{e^z + e^{-z}}{2}, \quad shz = \frac{e^z - e^{-z}}{2},$$

$$thz = \frac{shz}{chz} = \frac{e^z - e^{-z}}{e^z + e^{-z}}, \quad cthz = \frac{chz}{shz} = \frac{e^z + e^{-z}}{e^z - e^{-z}},$$

$$chz = 1 + \frac{z^2}{2!} + \frac{z^4}{4!} + \ldots + \frac{z^{2n}}{(2n)!} + \ldots, \; z \in C,$$

$$shz = z + \frac{z^3}{3!} + \frac{z^5}{5!} + \ldots + \frac{z^{2n+1}}{(2n+1)!} + \ldots, \; z \in C,$$

$$chz = \cos iz, \quad thz = -i\, tg\, iz,$$

$$shz = -i \sin iz, \quad cthz = i\, ctg\, iz,$$

$$\operatorname{Re} chz = chx \cos y, \quad \operatorname{Im} chz = -shx \sin y,$$

$$\operatorname{Re} shz = shx \cos y, \quad \operatorname{Im} shz = chx \sin y.$$

Логарифм

$$Lnz = \ln z + 2\pi k i, \quad \ln z = \ln|z| + i \arg z,$$

$$Ln(z_1 z_2) = Lnz_1 + Lnz_2, \quad Ln(z_1 / z_2) = Lnz_1 - Lnz_2,$$

$$Ln\,z^n = n\,Ln\,z, \quad \mathrm{Re}\,Ln\,z = \ln|z|, \quad \mathrm{Im}\,Ln\,z = Arg\,z.$$

Обратные тригонометрические и обратные гиперболические функции

$$Arcsin z = -i\,Ln\left(iz + \sqrt{1-z^2}\right),$$

$$Arccos z = -i\,Ln\left(z + \sqrt{z^2-1}\right),$$

$$Arctg\,z = \frac{i}{2}\,Ln\frac{i+z}{i-z}, \quad Arcctg\,z = \frac{i}{2}\,Ln\frac{z-i}{z+i},$$

$$Arsh\,z = Ln\left(z + \sqrt{z^2+1}\right), \quad Arch\,z = Ln\left(z + \sqrt{z^2-1}\right),$$

$$Arth\,z = \frac{1}{2}\,Ln\frac{1+z}{1-z}, \quad Arcth\,z = \frac{1}{2}\,Ln\frac{z+1}{z-1}.$$

Производная ФКП

Определение:

$$f'(z) = \lim_{\Delta z \to 0} \frac{f(z+\Delta z) - f(z)}{\Delta z}.$$

Условия Коши-Римана существования производной функции $f(z) = u(x,\ y) + iv(x,\ y)$:

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial v}{\partial x} = -\frac{\partial u}{\partial y}.$$

В этом случае

$$f'(z) = \frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x} = \frac{\partial v}{\partial y} - i\frac{\partial u}{\partial y}.$$

Условия Коши-Римана в полярных координатах $\left(z = re^{i\varphi},\ \omega = u(r,\ \varphi) + iv(r,\ \varphi)\right)$:

$$\frac{\partial u}{\partial r} = \frac{1}{r}\frac{\partial v}{\partial \varphi},\quad \frac{\partial u}{\partial \varphi} = -r\frac{\partial v}{\partial r}.$$

Интеграл ФКП

$$\int_{\gamma} f(z)dz.$$

Связь интеграла ФКП и Кри-2

$$\int_{\gamma} f(z)dz = \int_{\gamma} u(x,\ y)dx - v(x,\ y)dy + i\int_{\gamma} v(x,\ y)dx + u(x,\ y)dy$$

$$\left(f(z) = u(x,\ y) + iv(x,\ y)\right).$$

Сведение интеграла ФКП к интегралу от комплекснозначной функции действительной переменной

Если

$$\gamma:\ z = \sigma(t),\ t \in [\alpha;\ \beta],$$

то

$$\int_{\gamma} f(z)dz = \int_{\alpha}^{\beta} f(\sigma(t))\sigma'(t)dt.$$

Формула Ньютона-Лейбница

Если f аналитическая в области D, F - первообразная для $f,\ z_1,\ z_2 \in D,$ то

$$\int_{z_1}^{z_2} f(z)dz = F(z_2) - F(z_1) = F(z)\Big|_{z_1}^{z_2}.$$

Свойства интеграла

1.

$$\int_{\gamma}\left(af(z)+bg(z)\right)dz = a\int_{\gamma} f(z)dz + b\int_{\gamma} g(z)dz, \quad a,\ b \in C.$$

2.

$$\int_{\gamma} f(z)dz = \int_{\gamma_1} f(z)dz + \int_{\gamma_2} f(z)dz, \quad \gamma = \gamma_1 \cup \gamma_2,\ \gamma_1 \cap \gamma_2 = \varnothing.$$

3.

$$\int_{\gamma} f(z)dz = -\int_{\gamma^-} f(z)dz.$$

4.

$$\left|\int_{\gamma} f(z)dz\right| \le \int_{\gamma} |f(z)|ds \le Ml,\ M = \max_{z\in\gamma}|f(z)|,\ l = \partial л.\gamma.$$

Если *f(z)* аналитическая в области *D* и непрерывная в $D \cup \partial D,$ где ∂D - граница области *D*, то имеют место:

1) интегральная теорема Коши:

$$\int_{\partial D} f(\zeta)d\zeta = 0;$$

2) интегральная формула Коши:

$$\frac{1}{2\pi i}\int_{\partial D}\frac{f(\zeta)}{\zeta - z}d\zeta = f(z) \quad \forall z \in D;$$

3) интегральное представление для производных:

$$\frac{n!}{2\pi i}\int_{\partial D}\frac{f(\zeta)}{(\zeta - z)^{n+1}}d\zeta = f^{(n)}(z) \quad \forall z \in D.$$

Степенные ряды

$$\sum_{k=0}^{\infty} c_k (z - z_0)^k, \ c_k, \ z_0, \ z \in C.$$

Радиус сходимости степенного ряда

$$R = \frac{1}{\overline{\lim\limits_{n\to\infty}}\sqrt[n]{|c_n|}}$$ (формула Коши-Адамара),

$$R = \frac{1}{\lim\limits_{n\to\infty}\sqrt[n]{|c_n|}}, \quad R = \lim_{n\to\infty}\left|\frac{c_n}{c_{n+1}}\right|.$$

Круг сходимости:

$$\{z| \ |z - z_0| < R\}.$$

Ряд Тейлора

Если *f(z)* аналитическая в области *D* и $z_0 \in D$, то

$$f(z)=\sum_{k=0}^{\infty}\frac{f^{(k)}(z_0)}{k!}(z-z_0)^k, \quad |z-z_0|<R,$$

R равно расстоянию от точки z_0 до границы области *D*.

Нули аналитической функции

Для того чтобы точка z_0 была нулем кратности *k* функции *f*, необходимо и достаточно выполнение одного из следующих условий:

1) $$f(z_0)=f'(z_0)=\ldots=f^{(n)}(z_0)=0, \quad f^{(k)}(z_0)\neq 0;$$

2) $$f(z)=(z-z_0)^k\varphi(z), \quad \varphi(z_0)\neq 0;$$

3) $$f(z)=c_k(z-z_0)^k+c_{k+1}(z-z_0)^{k+1}+\ldots, \quad c_k\neq 0.$$

Если $z_0=\infty$ - нуль порядка *k* функции *f(z)*, то
$f(z)=z^{-k}\varphi(z), \ \varphi(\infty)\neq 0.$

Ряд Лорана

Если функция *f(z)* - аналитическая в кольце $r < |z - z_0| < R,$ то

$$f(z) = \sum_{k=-\infty}^{+\infty} c_k (z - z_0)^k,$$

$$c_k = \frac{1}{2\pi i} \int_{|z-z_0|=\rho} \frac{f(\zeta) d\zeta}{(\zeta - z_0)^{k+1}}, \quad k \in Z, \; r < \rho < R.$$

Изолированные особые точки однозначного характера

Тип особой точки z_0 функции определяется видом разложения *f(z)* в ряд Лорана в окрестности точки z_0:

1) $f(z) = \sum_{k=0}^{\infty} c_k (z - z_0)^k, \quad 0 < |z - z_0| < R,$ тогда z_0 - устранимая особая точка;

2) $f(z) = \sum_{k=-m}^{\infty} c_k (z - z_0)^k, \quad 0 < |z - z_0| < R, \; c_{-m} \neq 0,$ тогда z_0 - полюс порядка m;

3) $f(z) = \sum_{k=-\infty}^{+\infty} c_k (z - z_0)^k, \quad 0 < |z - z_0| < R,$

и бесконечное число коэффициентов $c_{-k}, \; k \in N,$ отлично от нуля, тогда z_0 - существенно особая точка.

Если z_0 - полюс порядка m, то $f(z) = \varphi(z)/(z - z_0)^m, \; \varphi(z)$ - аналитическая, $\varphi(z_0) \neq 0.$

Вычеты и их применение

$\operatorname*{res}_{z=z_0} f(z)$ - вычет функции *f(z)* относительно изолированной особой точки z_0:

$$\operatorname*{res}_{z=z_0} f(z)=\frac{1}{2\pi i}\int_{|z-z_0|=\rho} f(z)dz$$

(в круге $|z-z_0|\le\rho$ нет других особых точек).

Если $f(z)=\sum_{k=-\infty}^{+\infty} c_k(z-z_0)^k,\ 0<|z-z_0|<R,$ то

$$\operatorname*{res}_{z=z_0} f(z)=c_{-1}.$$

Вычисление вычетов

1. z_0 - устранимая особая точка:

$$\operatorname*{res}_{z=z_0} f(z)=0.$$

2. z_0 - полюс:

а) z_0 - простой полюс:

$$\operatorname*{res}_{z=z_0} f(z)=\lim_{z\to z_0}\left((z-z_0)f(z)\right).$$

В частности, если $f(z)=\varphi(z)/\psi(z),\ \psi(z_0)=0,\ \psi'(z_0)\ne 0,\ \varphi(z_0)\ne 0,$ то

$$\operatorname*{res}_{z=z_0}\frac{\varphi(z)}{\psi(z)}=\frac{\varphi(z_0)}{\psi'(z_0)};$$

б) z_0 - полюс порядка m:

$$\operatorname*{res}_{z=z_0} f(z) = \frac{1}{(m-1)!} \lim_{z \to z_0} \frac{d^{m-1}}{dz^{m-1}} \left((z - z_0)^m f(z) \right)$$

(формула также верна, если z_0 - полюс порядка не выше m).

3. z_0 - существенно особая точка. Вычет находится по разложению в ряд Лорана.

Вычет относительно бесконечно удаленной точки

$$\operatorname*{res}_{z=\infty} f(z) = \frac{1}{2\pi i} \int_{|z|=\rho} f(z) dz$$

($f(z)$ - аналитическая в области $\rho \le |z| < +\infty$; обход контура - по часовой стрелке).

$$\operatorname*{res}_{z=\infty} f(z) = -c_{-1},$$

c_{-1} - коэффициент при z^{-1} в разложении $f(z)$ в ряд Лорана в окрестности точки $z_0 = \infty$.

Вычисление вычета в бесконечно удаленной точке

1. $z = \infty$ - правильная точка:

$$\operatorname*{res}_{z=\infty} f(z) = \lim_{z \to \infty} z \left(f(\infty) - f(z) \right),$$

$z = \infty$ - нуль:

$$\operatorname*{res}_{z=\infty} f(z) = -\lim_{z\to\infty} z f(z).$$

В частности, если $f(z) \sim A/z^m$ при $z \to \infty$, то

$$\operatorname*{res}_{z=\infty} f(z) = \begin{cases} -A, & если \quad m = 1, \\ 0, & если \quad m > 1. \end{cases}$$

2. $z = \infty$ - полюс порядка не выше *m*:

$$\operatorname*{res}_{z=\infty} f(z) = \frac{(-1)^m}{(m+1)!} \lim_{z\to\infty} z^{m+2} f^{(m+1)}(z).$$

3. Если *f(z)* представима в виде $f(z) = \varphi\left(\frac{1}{z}\right)$, где $\varphi(\zeta)$ - аналитическая в точке $\zeta = 0$, то

$$\operatorname*{res}_{z=\infty} f(z) = -\varphi'(0).$$

Если *f(z)* имеет конечное число особых точек z_k, *k = 1, 2, ..., n,* в конечной части плоскости, то

$$\operatorname*{res}_{z=\infty} f(z) = -\sum_{k=1}^{n} \operatorname*{res}_{z=z_k} f(z).$$

Основная теорема о вычетах

Если *f(z)* - аналитическая на границе ∂D области *D* и внутри области, за исключением конечного числа особых точек z_1, z_2, ..., z_n, лежащих в *D*, то

$$\int_{\partial D} f(z)dz = 2\pi i \sum_{k=1}^{n} res f(z)$$

(обход контура положительный).

Вычисление интегралов от функций действительной переменной

1. $$\int_0^{2\pi} R(\cos t,\ \sin t)dt = \frac{1}{i}\int_{|z|=1} R\left(\frac{z^2+1}{2z},\ \frac{z^2-1}{2iz}\right)\frac{dz}{z}$$

(*R* - рациональная функция двух переменных).

2. Если *R(x)* - рациональная функция, а $\int_{-\infty}^{+\infty} R(x)dx$ сходится, то

$$\int_{-\infty}^{+\infty} R(x)dx = 2\pi i \sum_{k=1}^{n} res\, R(z),$$

где z_k - все особые точки функции *R(z)*, лежащие в верхней полуплоскости (Im $z_k > 0$).

Если $\zeta_1,\ \zeta_2,\ \ldots,\zeta_m$ - особые точки функции *R(z)*, лежащие в нижней полуплоскости, то

$$\int_{-\infty}^{+\infty} R(x)dx = -2\pi i \sum_{k=1}^{m} res R(z).$$

3. Если *R(x)* - рациональная функция, не обращающаяся в нуль на действительной оси,

$$R(x) \sim c/x^k\ (x \to \infty,\ c \neq 0,\ k \geq 1),$$

то

$$\int_{-\infty}^{+\infty} e^{i\alpha x} R(x)dx = 2\pi i \sum_{k=1}^{n} res\left(e^{i\alpha z} R(z)\right), \quad \alpha > 0$$

(z_k - все особые точки, лежащие в верхней полуплоскости);

$$\int_{-\infty}^{+\infty} e^{i\beta x} R(x)dx = -2\pi i \sum_{k=1}^{m} res\left(e^{-i\beta z} R(z)\right), \quad \beta > 0$$

(ζ_k - все особые точки, лежащие в нижней полуплоскости).

Замечание.

$$\int_{-\infty}^{+\infty} R(x)\sin \alpha x dx = \mathrm{Im} \int_{-\infty}^{+\infty} R(x) e^{i\alpha x} dx,$$
$$\int_{-\infty}^{+\infty} R(x)\cos \alpha x dx = \mathrm{Re} \int_{-\infty}^{+\infty} R(x) e^{i\alpha x} dx$$

4. Если *R(x)* - рациональная функция, аналитическая в верхней полуплоскости, за исключением конечного числа изолированных особых точек $z_1, z_2, ..., z_n$ ($\mathrm{Im}\, z_k > 0$), имеет на действительной оси простые полюса $x_1, x_2, ..., x_m$ и $|R(z)| \to 0,\ z \to \infty (\mathrm{Im} z \geq 0)$, то

$$\text{v. p.} \int_{-\infty}^{+\infty} e^{i\alpha x} R(x)dx = 2\pi i \sum_{k=1}^{n} res\left(e^{i\alpha z} R(z)\right) + \pi i \sum_{k=1}^{m} res\left(e^{i\alpha z} R(z)\right).$$

конформные отображения некоторых областей на единичный круг $|\omega| < 1$

1. Верхней полуплоскости $\mathrm{Im}\, z > 0$:

$$\omega = e^{i\alpha}\frac{z-z_0}{z-\bar{z}_0},\ \alpha \in R,\ \mathrm{Im} z_0 > 0.$$

2. Единичного круга $|z| < 1$:

$$\omega = e^{i\alpha}\frac{z-z_0}{1-\bar{z}_0 z},\ \alpha \in R,\ |z_0| < 1.$$

3. Полосы $0 < \mathrm{Re}\, z < \pi,\ -\infty < \mathrm{Im}\, z < +\infty$:

$$(\omega - 1)/(\omega + 1) = ie^{iz}.$$

4. Полукруга $|z| < R$, $\mathrm{Re}\, z > 0$:

$$\omega = i\frac{z^2 + 2Rz - R^2}{z^2 - 2Rz - R^2}.$$

6. Алгебраическое число

6.1. Общие сведения об алгебраических числах

Алгеб над полем k — элемент алгебраического замыкания поля k, то есть корень многочлена (не равного тождественно нулю) с коэффициентами из k.

Если поле не указывается, то предполагается поле рациональных чисел, то есть $k = \mathbb{Q}$, в этом случае поле алгебраических чисел обычно обозначается $\mathbb{A}$. Поле $\mathbb{A}$ является подполем поля комплексных чисел.

Этот раздел посвящен именно этим «рациональным алгебраическим числам».

Связанные определения

- Комплексное число, не являющееся алгебраическим, называется трансцендентным.

- Целыми алгебраическими числами называются корни многочленов с целыми коэффициентами и со старшим коэффициентом единица.
- Если α — алгебраическое число, то среди всех многочленов с рациональными коэффициентами, имеющих α своим корнем, существует единственный многочлен наименьшей степени со старшим коэффициентом, равным 1. Такой многочлен автоматически является неприводимым, он называется **каноническим**, или **минимальным**, многочленом алгебраического числа α. (Иногда **каноническим** называют многочлен, получающийся из минимального домножением на наименьший общий знаменатель его коэффициентов, то есть многочлен с целыми коэффициентами)
    - Степень канонического многочлена α называется **степенью** алгебраического числа α.
    - Другие корни канонического многочлена α называются **сопряжёнными** к α.
    - **Высотой** алгебраического числа α называется наибольшая из абсолютных величин коэффициентов в неприводимом и примитивном многочлене с целыми коэффициентами, имеющем α своим корнем.

Примеры

- Рациональные числа, и только они, являются алгебраическими числами 1-й степени.
- Мнимая единица *i* и $\sqrt{2}$ являются алгебраическими числами 2-й степени. Сопряжёнными к ним являются соответственно -*i* и $-\sqrt{2}$.
- При любом натуральном числе *n* число $\sqrt[n]{2}$ является алгебраическим степени *n*.

Свойства

- Множество алгебраических чисел счётно, а следовательно, имеет меру нуль.
- Множество алгебраических чисел плотно в комплексной плоскости.

- Сумма, разность, произведение и частное двух алгебраических чисел (кроме деления на нуль) суть алгебраические числа, т. е. множество всех алгебраических чисел образует поле.
- Корень многочлена с алгебраическими коэффициентами есть алгебраическое число, т. е. поле алгебраических чисел алгебраически замкнуто.
- Для всякого алгебраического числа α существует такое натуральное N, что $N\alpha$ — целое алгебраическое число.
- Алгебраическое число α степени n имеет n различных сопряжённых чисел (включая себя).
- α и β сопряжены тогда и только тогда, когда существует автоморфизм поля $\mathbb{A}$, переводящий α в β.
- Любое алгебраическое число вычислимо, а следовательно, арифметично.
- Порядок на множестве действительных алгебраических чисел изоморфен порядку на множестве рациональных чисел.

Первоначальные элементы математики связаны с появлением навыков счета, возникающих в примитивной форме на сравнительно ранних ступенях развития человеческого общества, в процессе трудовой деятельности.

Исторически теория чисел возникла как непосредственное развитие арифметики. В настоящее время в теорию чисел включают значительно более широкий круг вопросов, выходящих за рамки изучения натуральных чисел. В теории чисел рассматриваются не только натуральные числа, но и множество всех целых чисел, а так же множество рациональных чисел.

Если рассматривать корни многочленов: $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$ с целыми коэффициентами, то обычные целые числа соответствуют случаю, когда этот многочлен имеет степень n=1. Во множестве комплексных чисел естественно выделить так называемые целые алгебраические числа, представляющие собой корни многочленов с целыми коэффициентами.

Изучение свойств таких чисел составляет содержание одного из важнейших разделов современной теории чисел, называемого

алгебраической теорией чисел. Она связана с изучением различных классов алгебраических чисел.

6.2. Краткий исторический очерк

Впервые алгебраические поля стал рассматривать Гаусс. Его исследования положили начала алгебраической теории чисел. При обосновании теории биквадратичных вычетов он развил арифметику целых гауссовых чисел, то есть чисел вида $a + bi$, где a и b — целые числа. Далее, изучая теорию кубических вычетов, Якоби и Эйзенштейн создали арифметику чисел вида $a + b\rho$, где $\rho = (-1 + i\sqrt{3})/2$ — кубический корень из единицы, а a и b — целые числа. В 1844 году Лиувилль доказал теорему о невозможности слишком хорошего приближения корней многочленов с рациональными коэффициентами рациональными дробями, и, как следствие, ввёл формальные понятия алгебраических и трансцендентных (то есть всех прочих вещественных) чисел. Попытки доказать великую теорему Ферма привели Куммера к изучению полей деления круга, введению понятия идеала и созданию элементов теории алгебраических чисел. В работах Дирихле, Кронекера, Гильберта и других теория алгебраических чисел получила свое дальнейшее развитие. Большой вклад в неё внесли русские математики Золотарев (теория идеалов), Вороной (кубические иррациональности, единицы кубических полей), Марков (кубическое поле), Сохоцкий (теория идеалов) и другие.

Теория алгебраических чисел была построена в работах Куммера (1810-1893) и Дирихле (1805-1859) и развита затем Кронекером (1823-1891), Дедекиндом (1831-1916) и Е.И. Золотаревым (1847-1878). Работы Лиувилля (1809-1882) и Эрмита (1822-1901) явились основой трансцендентных чисел.

Вопросы аппроксимации алгебраических чисел рациональными были существенно продвинуты в начале XX века А. Туэ, а затем в пятидесятых годах XX века в работах К. Рота.

Внимание специалистов по теории чисел привлекает алгебраическая теория чисел.

Здесь надо назвать работы Г. Хассе, Е. Гекке, а в особенности французского математика А. Вейля, результаты которого были использованы во многих теорико-числовых исследованиях, как например Д. Берджессом в проблеме о наименьшем квадратичном вычете.

К алгебраической теории чисел относятся и интересные работы математика И.Р. Шафаревича, а так же работы Б.Н. Делонга по теории кубических форм.

6.3. Поле алгебраических чисел.

6.3.1 Понятие числового поля

Естественный и важный подход к выделению и изучению тех или иных множеств чисел связан с замкнутостью множеств чисел относительно тех или иных действий.

Определение 1: Мы говорим, что некоторое множество чисел M замкнуто относительно некоторого действия, если для всяких двух чисел их M, для которых определен результат данного действия над ним, число, является этим результатом, всегда принадлежащим M.

Пример:

1) N Множество натуральных чисел замкнуто относительно сложения, т.к. a, bÎN $\Rightarrow$ (a+b) ÎN.

В отношении умножения множество N так же замкнуто. Но оно не является замкнутым относительно вычитания и деления. Действительно:

5, 7 ÎN, но 5-7=-2 ÎN,

3, 2ÎN, но 3:2=1,5 ÎN

2) Множество целых чисел Z замкнуто относительно сложения, вычитания и умножения.

3) Множество чисел вида $2^к$, кÎN, замкнуто относительно умножения и деления.

2к*2l=2k+l

2к:2l=2k-l

В связи с замкнутостью действий на множестве выделились классы числовых множеств.

Рассмотрим один их классов, называемых полем.

Определение 2: Множество чисел М, содержащие не менее двух чисел, называется числовым полем, если оно замкнуто относительно действий сложения, вычитания, умножения и деления.

Последнее означает, что для любых a, b ÎM, должно иметь место a+b, a-b, a*b ÎM. Так же для любого aÎM и любого b¹0 из М, должно выполняться a:bÎM.

Пример:

Среди важнейших числовых полей наиболее важными являются:

1) поле всех рациональных чисел;

2) поле всех вещественных чисел;

3) поле всех комплексных чисел.

Что касается **множества всех целых чисел, то оно не является числовым полем, ибо не замкнуто относительно деления.**

Существует бесконечно много числовых полей. Нас, в данном случае интересует поле алгебраических чисел.

6.3.2 Определение алгебраического числа.

Существуют различные признаки, по которым из общего множества Z выделяют те или иные подмножества, подвергаемые специальному изучению. С точки зрения важного для алгебры понятия алгебраического уравнения, естественным представляется выделение классов чисел, являющихся корнями алгебраических уравнений, коэффициенты которых принадлежат тому или иному классу чисел.

Определение 3: Число Z называется алгебраическим, если оно является корнем какого-нибудь алгебраического уравнения с целыми коэффициентами:

$a_n x^n+a_{n-1}x^{n-1}+\ldots+a_1 x+a_0=0$

($a_0, a_1, \ldots, a_n$ÎZ; a_n¹0),

т.е. выполняется:

$a_n z^n+a_{n-1}z^{n-1}+\ldots+a_1 z+a_0=0$

Числа, не являющиеся алгебраическими называются трансцендентными.

В определении алгебраического числа можно допустить, чтобы коэффициенты $a_0, a_1, \ldots, a_{n-1}, a_n$ были любыми рациональными числами, поскольку, умножив левую и правую части уравнения на целое число, являющиеся общим кратным знаменателем всех коэффициентов, мы получили уравнение с целыми коэффициентами, корнем которого будет наше число.

К алгебраическим числам принадлежат, в частности, и все рациональные числа. Действительно, рациональное число z=p/q (p, qÎN) очевидно является корнем уравнения: qx-p=0.

Также всякое значение корня любой степени из рационального числа является алгебраическим числом. Действительно, число $z=\sqrt[n]{\frac{p}{q}}$ (p, qÎN) является корнем уравнения:

$qx^n-p=0$.

Существуют и другие алгебраические числа, нежели указанное выше.

Пример:

1) Число $z=\sqrt{2}+\sqrt{3}$ является алгебраическим. Действительно, возводя в квадрат обе части равенства, определяющего число z, получим: $z^2=2+2\sqrt{2}\sqrt{3}^2-5=2\sqrt{6}^4-10z^2+25=24$. Отсюда следует, что число z является корнем следующего уравнения:

$x^4-10x^2+1=0$

2) Всякое число z=a+bi, у которого компоненты a и b – рациональные числа, являются алгебраическими. Докажем это.

$a=\frac{p}{q}\ b=\frac{p'}{q'}$ (p, q, p′,q′ÎN).

Из равенства

$$z=\frac{p}{q}+\frac{p'}{q'}i\ \ pq'z-pq'=qp'i$$

.

Отсюда, возводя в квадрат, получим:

$$q^2q'^2z^2-2pqq'^2z+p^2q'^2=-q^2p'^2$$

Следовательно, z является корнем уравнения:

$$(q^2q'^2)x^2-(2pqq'^2)x+(p^2q'^2+q^2p'^2)=0$$

все коэффициенты которого целые числа.

В дальнейшем нас будут интересовать только действительные алгебраические числа, не оговаривая этого каждый раз.

Из f(x)=0 следует f(z)j(x)=0, где в качестве j(x) можно взять любой многочлен с целыми коэффициентами. Таким образом для любого алгебраического числа z, из всех этих многочленов обычно рассматривают многочлен наименьшей степени.

Определение 4: Число n называется степенью алгебраического числа z, если z есть корень некоторого многочлена n-ой степени с рациональными коэффициентами и не существует тождественно не равного нулю многочлена с рациональными коэффициентами степени, меньшей чем n, корнем которого является z.

Если корень многочлена n-ой степени с целыми рациональными коэффициентами z не является корнем ни одного тождественно неравного нулю многочлена с целыми коэффициентами степени меньшей чем n, то z не может быть корнем и тождественно неравного нулю многочлена с рациональными коэффициентами степени меньшей чем n, т.е. z – алгебраическое число степени n.

Рациональные числа являются алгебраическими числами первой степени. Любая квадратическая иррациональность представляет собой алгебраическое число 2-й степени, так как, являясь корнем квадратичного уравнения с целыми коэффициентами, она не является корнем какого-либо уравнения 1-й степени с целыми коэффициентами. Алгебраические числа 3-й степени часто называют кубическими иррациональностями, а 4-й степени биквадратическими иррациональностями.

Пример:

1) $\sqrt[3]{2}$ - алгебраическое число 3-й степени, т.е. кубическая иррациональность. Действительно, это число есть корень многочлена 3-й степени с целыми коэффициентами $x^3-2=0$ и $\sqrt[3]{2}$ не является корнем какого-либо многочлена 1-й или 2-й степени с целыми коэффициентами.

Определение 5: Если алгебраическое число n-й степени z является корнем многочлена

$$f(x)=x^n+b_1x^{n-1}+ \dots +b_n \ (n^3 1) \qquad (1)$$

с рациональными коэффициентами, то f(x) называется минимальным многочленом для z. Таким образом, минимальным многочленом для z называется многочлен наименьшей степени с рациональными коэффициентами и старшим коэффициентом, равном единице, корнем которого является z.

Если вместо многочлена (1) взять какой-либо другой многочлен с рациональными коэффициентами степени n, корнем которого является z, то многочлен (1) может быть получен из него делением всех коэффициентов на старший член.

Пример:

1) Минимальным многочленом для $\sqrt[3]{2}$ является x^3-2, так как корень этого многочлена $\sqrt[3]{2}$ не является корнем какого-либо многочлена степени с рациональными коэффициентами.

Теорема 1: Если f(x) минимальный многочлен алгебраического числа z и f(x) многочлен с рациональными коэффициентами, такой, что F(z)=0, то f(x) делитель F(x), т.е. F(x)=f(x)g(x), где g(x) также многочлен с рациональными коэффициентами.

Доказательство: Согласно известной теореме алгебры F(x) можно представить в виде:

$$F(x)=f(x)g(x)+r(x)$$

где g(x) и r(x) – многочлены с рациональными коэффициентами, причем степень r(x) меньше степени f(x). Поскольку F(x)=0 и f(z)=0, то придавая x значение z, получаем r(z)=0; z – корень многочлена r(x) с рациональными коэффициентами степени, меньшей чем у минимального для z многочлена, т.е. меньшей чем степень z. Это может быть только если r(x) тождественно равен нулю, а значит F(x)=f(x)g(x). Теорема доказана.

Теорема 2: Для любого алгебраического числа z минимальный многочлен неприводим над полем рациональных чисел.

Доказательство: Пусть f(x) – минимальный многочлен для z. Предположим, что f(x) приводим над полем рациональных чисел, т.е., что f(x)=w(x)j(x), w(x)j(x) – многочлены с рациональными коэффициентами, степени меньшей, чем n.

Из равенства w(x)j(x)=f(x)=0 следует, что из двух чисел w(x) и j(x), по крайней мере одно равно нулю. Пусть например w(x)=0, тогда z – корень тождественно не равного нулю многочлена w(x) с рациональными коэффициентами, степени меньшей, чем n, т.е. меньшей чем у f(x). А это противоречит тому, что f(x) – минимальный многочлен для z. Предположение, что f(x) приводим над полем рациональных чисел, оказалось неверным, т.е. f(x) неприводим над этим полем. Теорема доказана.

Теорема 3: Если z корень неприводимого над полем рациональных чисел многочлена F(x) с рациональными коэффициентами степени n, то z – алгебраическое число степени n.

Доказательство: Обозначим минимальный многочлен для z через f(x). Согласно теоремы 1: F(x)=f(x)g(x); где g(x) – многочлен с рациональными коэффициентами. Поскольку F(x) неприводим над полем рациональных чисел и f(x) отлично от постоянного, то g(x)=c, где c – рационально. F(x)=cf(x), т.е. z – алгебраическое число n-й степени. Теорема доказана.

Пример:

Пусть p – простое число.

$\sqrt[p]{a}$ при любом простом целом a (a>1), не равном p-ой степени другого целого, представляет собой алгебраическое число степени p. Действительно, это число есть корень неприводимого над полем рациональных чисел многочлена.

$$x^p-a=0$$

Если z – алгебраическое число степени n и f(x) – минимальный многочлен для z, то все корни z_1, z_2, … z_n уравнения f(x)=0, отличные от z, называют сопряженным с z.

Один из корней совпадает с z, будем ставить его на первое место, т.е. $z=z_1$.

6.3.3. Поле алгебраических чисел

Теорема 4: Множество всех действительных алгебраических чисел представляет собой поле, т.е. сумма, разность, произведение и частное двух алгебраических чисел a и b (для частного при b'0) являются алгебраическими числами.

Доказательство:

1) Пусть a - корень многочлена f(x) степени n с целыми коэффициентами, корни которого a_1, a_2, … ,a_n, a и b - корень многочлена j(x) степени m с целыми коэффициентами, корни которого b_1, b_2, … b_m ($b=b_1$). Рассмотрим многочлен:

$$F(x)= \left(\prod_{i=1}^{n}\prod_{j=1}^{m}(a_i+b_i)\right)=$$

$$= (x-a_1-b_1)\,(x-a_1-b_2)\,\ldots\,(x-a_1-b_m)$$

$$(x-a_2-b_1)\,(x-a_2-b_2)\,\ldots\,(x-a_2-b_m)$$

$$- -$$

$$(x-a_n-b_1)\,(x-a_n-b_2)\,\ldots\,(x-a_n-b_m) \qquad (2)$$

Если в этом произведении сделать какую угодно подстановку величин a_1, a_2, … ,a_n, то некоторые строки переставляются местами, но произведение в целом не изменится. Это значит, что F(x) – симметрический многочлен по отношению b_1, b_2, … b_m. В целом F(x) – симметрический многочлен от двух систем аргументов: a_1, a_2, … ,a_n и b_1, b_2, … b_m.

Согласно известным теоремам о симметрических многочленах, коэффициенты многочлена F(x) могут быть выражены рационально через элементарные симметрические функции от a_1, a_2, … ,a_n и b_1, b_2, … b_m, т.е. через целые коэффициенты, f(x) и j(x). Это значит, что коэффициенты F(x) рациональны, и, следовательно, число $a+b=a_1+b_1$, являющегося, как это непосредственно видно из формулы (2), корнем F(x), есть алгебраическое число.

2) Для доказательства того, что произведение двух алгебраических чисел a и b есть алгебраическое число, достаточно, аналогично тому, как это было только что сделано для многочлена (2), рассмотреть многочлен:

$$F(x)=(\prod_{i=1}^{n}\prod_{j=1}^{m} a_i b_i) \qquad (3)$$

Этот многочлен имеет в качестве одного из своих корней $a_1b_1=ab$.

3) Пусть b - корень многочлена $j(x)=b_0x^n+ b_1x^{n-1}+ \dots b_n$, ($b_i$ – целые числа). Тогда -b является корнем многочлена с целыми коэффициентами.

$j(-x)=(-1)^n b_0x^n+(-1)^{n-1}b_1x^{n-1}+ \dots b^n$, а при $b^1 0$ корень многочлена $x^n j(\frac{1}{x_0}+b_1x+ \dots b_nx^n$. Таким образом, вместе с b алгебраическими числами являются -b и $\frac{1}{\beta}$

Разность может быть представлена в виде a+(-b), т.е. в виде суммы двух алгебраических чисел. При $b^1 0$ частное $\frac{a}{\beta}=a\frac{1}{\beta}$

Если степени алгебраических чисел a и b равны m и n, то, взяв в качестве f(x) и j(x) соответствующие минимальные многочлены будем в (2) и (3) иметь многочлены степени mn, и ab алгебраические числа степени, не большей, чем mn. Многочлены j(x), j(-x), и

$x^n\varphi\frac{1}{x}$ одинаковой степени, а, следовательно, b, -b, $\frac{1}{\beta}$ a-b и $\frac{a}{\beta}$ имеют степени не больше, чем mn. Теорема доказана.

Пример:

1) $\sqrt{2}$ и $\sqrt{3}$ алгебраические числа 2-й степени, а $\sqrt{2}+\sqrt{3}$ - алгебраическое число 4 степени. Действительно, если a=$\sqrt{2}+\sqrt{3}$ $a^2=5+2\sqrt{6}$ ^{4}-$10a^2$+1=0, т.е. a корень многочлена f(x)=x^4-$10x^2$+1 с целыми коэффициентами, и

$$f(x)=(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3}) \qquad (4)$$

Из теоремы единственности над полем рациональных чисел множители f(x) должны являться произведением каких-то множителей правой части равенства (4). Легко видеть, что из этих множителей нельзя составить многочлен с рациональными коэффициентами степени меньшей, чем 4, т.е. f(x) – неприводимый над полем рациональных чисел многочлен, а, следовательно, согласно теореме 3, $\sqrt{2}+\sqrt{3}$ - алгебраическое число 4-й степени.

2) a=$\sqrt[6]{3}$ и b=$\sqrt[6]{12}$ ab=$\sqrt[3]{6}$ - алгебраическое число 3-й степени.

6.4. Рациональные приближения алгебраических чисел.

6.4.1. Теорема Лиувилля

Алгебраические числа не могут иметь слишком хороших рациональных приближений: погрешность при замене алгебраического числа рациональной дробью не может быть достаточно мала по порядку в сравнении с величиной, обратной знаменателю рациональной дроби.

Для алгебраического числа 1-й степени существует постоянная c>0, такая, что для любой рациональной дроби $\frac{a}{b}$ a, будет выполняться неравенство:

$$\left|\alpha-\frac{a}{b}\right|\geq\frac{c}{b} \tag{5}$$

Для алгебраического числа 2-й степени можно подобрать c>0, такое, что для любой рациональной дроби, будет иметь место неравенство:

$$\left|\alpha-\frac{a}{b}\right|\geq\frac{c}{b^2} \tag{6}$$

В 1844 г., французским математиком Лиувиллем, впервые была доказана общая теорема:

Теорема 5: Для любого действительного алгебраического числа a степени n можно подобрать положительноес, зависящее только от a, такое, что для всех рациональных чисел $\frac{a}{b}$ ($\frac{a}{b}$ ¹a) будет иметь место неравенство:

$$\left|\alpha-\frac{a}{b}\right|\geq\frac{c}{b^n} \tag{7}$$

Доказательство: Пусть $f(x)=A_0x^n+A_1x^{n-1}+A_n$ неприводимый многочлен с целыми коэффициентами, корнем которого является a. В качестве f(x) можно, например, взять многочлен, получающийся из минимального для a многочлена после умножения всех коэффициентов на наименьшее кратное их знаменателей.

Согласно теореме Безу, имеем:

$$f(x)=(x-a)g(x), \tag{8}$$

где g(x) – многочлен с действительными коэффициентами.

Возьмем произвольное d>0. |g(x)| - непрерывная, а следовательно, ограниченная функция от x в сегменте [a-d; a+d], т.е. существует положительное число M, такое, что |g(x)|≤M, для всех x из этого сегмента. Обозначим через c=min $(\frac{1}{M}, \delta)$ $c \le \frac{1}{M}$ и $c \le \delta^n$

Для произвольного рационального числа $\frac{a}{b}$ могут представиться две возможности:

1) $\frac{a}{b}$ лежит вне сегмента |a-d^m; a+d^m|, тогда

$$\left|a-\frac{a}{b}\right| > \delta \ge c \ge \frac{c}{b^n}$$

2) $\frac{a}{b}$ удовлетворяет неравенствам:

a-d≤$\frac{a}{b}$≤a+d, тогда |g($\frac{a}{b}$)|≤M и, подставляя в (8) вместо x значение $\frac{a}{b}$

$$\left|f(\frac{a}{b})\right| = \left|\frac{a}{b}-a\right| \cdot \left|g(\frac{a}{b})\right| \le M\left|a-\frac{a}{b}\right| \le \frac{1}{c}\left|a-\frac{a}{b}\right| \quad (9)$$

Неприводимый над полем рациональных чисел многочлен f(x) степени n³2 не имеет рациональных корней, а при n=1 не имеет корней, отличных от a, так что:

$$f(\frac{a}{b})=\frac{\left|A_0a^n+A_1a^{n-1}b+\_+A_nb^n\right|}{b^n}\neq 0$$

Поскольку числитель $\left|A_0a^n+A_1a^{n-1}b+\_+A_nb^n\right|$ - целое неотрицательное, отличное от нуля, т.е. число большее или равное 1, то

$$\left|f(\frac{a}{b})\right|\geq\frac{1}{b^n} \qquad (10).$$

Сравнивая неравенства (9) и (10) получаем $\frac{1}{b}\left|\alpha-\frac{a}{b}\right|\geq\frac{1}{b^n}$, так что и в этом случае имеем: $\left|\alpha-\frac{a}{b}\right|\geq\frac{c}{b^n}$. Теорема доказана.

Пример:

Пусть z – неквадратное целое число. Найти c>0, такое, что для всех рациональных чисел $\frac{a}{b}$ имело бы место неравенство:

$$\left|\sqrt{D}-\frac{a}{b}\right|\geq\frac{c}{b^n}.$$

$\sqrt{D}$ - корень многочлена x^a-D. Деля x^2-D на $x-\sqrt{D}$, находим $g(x)=x+\sqrt{D}$.

При $\sqrt{D}$ d<x<$\sqrt{D}$ </x<d имеем $|g(x)| < 2\sqrt{D} + \delta$, т.е. M=$2\sqrt{D}$ +d.

В качестве c берем $\min(\frac{1}{2\sqrt{D}+\delta}, \delta)$, при этом выгодней всего взять d так, что $\delta = \frac{1}{2\sqrt{D+\delta}}$, $d^2+2\sqrt{D}$ d-1=0, т.е. d=$-\sqrt{D}+\sqrt{D+1}$.

При таком d получаем $c = \sqrt{D+1} - \sqrt{D}$, так что при любых целых a и b имеем:

$$\left|\sqrt{D} - \frac{a}{b}\right| \geq \frac{\sqrt{D+1}-\sqrt{D}}{b^2}.$$

6.4.2. Трансцендентные числа Лиувилля.

Числа, являющиеся корнями уравнений с целыми коэффициентами, не исчерпывают все множество действительных чисел, т.е. существуют действительные числа отличные от алгебраических.

Определение 6: Любое неалгебраическое число называется трансцендентным.

Впервые существование трансцендентных чисел доказано Лиувиллем. Доказательство существования трансцендентных чисел у Лаувилля эффективно; на основе следующей теоремы, являющейся непосредственным следствием теоремы 5, строятся конкретные примеры трансцендентных чисел.

Теорема 6: Пусть a – действительное число. Если для любого натурального n³1 и любого действительного c>0 существует хотя бы одна рациональная дробь $\frac{a}{b}, (\frac{a}{b} \neq a)$, такая, что

$$\left|\alpha-\frac{a}{b}\right|<\frac{c}{b^n} \qquad (11),$$

то а – трансцендентное число.

Доказательство: Если бы а было алгебраическим, то нашлось бы (теорема 5) целое положительное n и действительное c>0 такие, что для любой дроби $\frac{a}{b}$ было бы $\left|\alpha-\frac{a}{b}\right|\geq\frac{c}{b^n}$, а это противоречит тому, что имеет место (11). Предположение, что а алгебраическое число, т.е. трансцендентное число. Теорема доказана.

Числа а, для которых при любых n³1 и c>0 неравенство (11) имеет решение в целых числах а и b называются трансцендентными числами Лиувилля.

Пример:

1) $$\alpha=\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\ldots=0{,}1100010\ldots$$

а – трансцендентное число.

Возьмем произвольные действительные n³1 и c>0. Пусть $\alpha=10^{k!}\cdot\left(\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\ldots+\frac{1}{10^{k!}}\right), b=10^{k!}$, где k выбрано настолько большим, что $10^{k!}\geq\frac{2}{c}$ и k³n, тогда

$$\left|\alpha-\frac{a}{b}\right|=\frac{1}{10^{(k+1)!}}+\frac{1}{10^{(k+2)!}}+\ldots<\left(1+\frac{1}{2}+\frac{1}{2^2}+\ldots\right)=\frac{2}{10^{k!}}\cdot\frac{1}{10^{k!}}\leq c\frac{1}{b^n}$$

Поскольку для произвольных n³1 и c>0 можно найти дробь $\frac{a}{b}$ такую, что $\left|\alpha-\frac{a}{b}\right|\le\frac{c}{b^n}$, то a – трансцендентное число.

Алгебраические числа имеют широкое применение в теории чисел, алгебре, геометрии, теории моделирования и других разделах наук. Они позволяют раскрыть вариантности алгебры для приложений в области моделирования.

Изучение свойств таких чисел составляет содержание одного из важнейших разделов современной теории чисел, называемого алгебраической теорией чисел.

К этому разделу относятся вопросы, связанные с изучением различных классов алгебраических чисел.

7. Гиперкомплексные числа

Для перечисленных множеств чисел справедливо следующее выражение: $\mathbb{P}\subset\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$.

7.1. Кватернионы

(от лат. *quaterni*, *по четыре*) — система гиперкомплексных чисел, образующее **векторное пространство размерностью четыре над полем вещественных чисел**. Кватернионы — минимальное расширением комплексных чисел, образующее тело, но их умножение некоммутативно. Предложена Гамильтоном в 1843 году, обычно обозначается $\mathbb{H}$. Кватернионы в отличие от комплексных чисел не коммутативны относительно умножения.

Кватернионы удобны для описания изометрий трёх- и четырёхмерного Евклидовых пространств, и поэтому получили широкое распространение в механике. Также их используют в вычислительной математике, например при создании трёхмерной графики.

7.1.1. Определения

7.1.1.1. Стандартное

Кватернионы можно определить как формальную сумму $a + bi + cj + dk$, где a, b, c, d — вещественные числа, а i, j, k — *мнимые единицы* со следующим свойством: $i^2 = j^2 = k^2 = ijk = -1$. Таким образом, таблица умножения *базисных кватернионов* — $1, i, j, k$ — выглядит так:

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

например, $ij = k$, а $ji = -k$.

7.1.1.2. Как вектор&скаляр

Кватернион представляет собой пару $(a, \vec{u})$, где $\vec{u}$ — вектор трёхмерного пространства, а a — скаляр, то есть вещественное число. Операции сложения определены следующим образом:

$$(a, \vec{u}) + (b, \vec{v}) = (a + b, \vec{u} + \vec{v})$$

Произведение определяется следующим образом:

$$(a,\vec{u})\,(b,\vec{v}) = (ab - \vec{u}\cdot\vec{v},\, a\vec{v} + b\vec{u} + \vec{u}\times\vec{v})$$

где $\cdot$ обозначает скалярное произведение, а $\times$— векторное произведение.

В частности,

$$\begin{aligned}(a,0)\,(0,\vec{v}) &= (0,\vec{v})\,(a,0) = (0,a\vec{v})\\ (a,0)\,(b,0) &= (ab,0)\\ (0,\vec{u})\,(0,\vec{v}) &= (-\vec{u}\cdot\vec{v},\,\vec{u}\times\vec{v})\end{aligned}$$

Заметим, что

- Алгебраические операции в кватернионах обладают свойством дистрибутивности.
- Антикоммутативность векторного произведения влечёт некоммутативность произведения кватернионов.

7.1.1.4. Через комплексные числа

Кватернион можно представить как пару комплексных чисел. Пусть $j^2 = -1,\ j \neq \pm i$и $z, w \in \mathbb{C}$. Тогда кватернион можно записать в виде $q = z + wj = a + bi + cj + dij$.

7.1.1.5. Через матричные представления

Вещественными матрицами

Кватернионы также можно определить как вещественные матрицы следующего вида с обычными матричными произведением и суммой:

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}.$$

При такой записи:

- сопряжённому кватерниону соответствует транспонированная матрица:

$$\bar{q} \mapsto Q^T;$$

- четвёртая степень модуля кватерниона равна определителю соответствующей матрицы:

$$|q|^4 = \det Q.$$

Комплексными матрицами

Альтернативно, кватернионы можно определить как комплексные матрицы следующего вида с обычными матричными произведением и суммой:

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix},$$

здесь $\bar{\alpha}$ и $\bar{\beta}$ обозначают комплексно-сопряжённые числа к α и β.

Такое представление имеет несколько важных свойств:

- комплексному числу соответствует диагональная матрица;
- сопряжённому кватерниону соответствует сопряжённая транспонированная матрица:

$$\bar{q} \mapsto \bar{Q}^T;$$

- квадрат модуля кватерниона равен определителю соответствующей матрицы:

$$|q|^2 = \det Q.$$

7.1.1.6. Связанные объекты и операции

Для кватерниона

$$q = a + bi + cj + dk$$

кватернион a называется *скалярной частью* q, а кватернион $u = bi + cj + dk$ — *векторной частью*. Если $u = 0$, то кватернион называется *чисто скалярным*, а при $a = 0$ — *чисто векторным*.

Сопряжение

Для кватерниона q *сопряжённым* называется:

$$\bar{q} = a - bi - cj - dk$$

Сопряжённое произведение есть произведение сопряжённых в обратном порядке:

$$\overline{pq} = \bar{q}\bar{p}$$

Для кватернионов справедливо равенство

$$\overline{p} = -\frac{1}{2}(p + ipi + jpj + kpk)$$

Модуль

Так же, как и для комплексных чисел,

$$|q| = \sqrt{q\bar{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$$

называется *модулем* q. Если $|q| = 1$, то q называется *единичным кватернионом*.

В качестве нормы кватерниона обычно рассматривают его модуль:

$$\|z\| = |z|.$$

Таким образом, на множестве кватернионов можно ввести метрику. Кватернионы образуют метрическое пространство, изоморфное $\mathbb{R}^4$ с евклидовой метрикой.

Кватернионы с модулем в качестве нормы образуют банахову алгебру.

Из тождества четырёх квадратов вытекает, что $|p \cdot q| = |p| \cdot |q|$, иными словами, кватернионы обладают мультипликативной нормой и образуют ассоциативную алгебру с делением.

Обращение умножения (деление)

Кватернион, обратный по умножению к q, вычисляется так:

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

7.1.2. Алгебраические свойства

Четыре базисных кватерниона и четыре противоположных им по знаку образуют по умножению группу кватернионов (порядка 8). Обозначается:

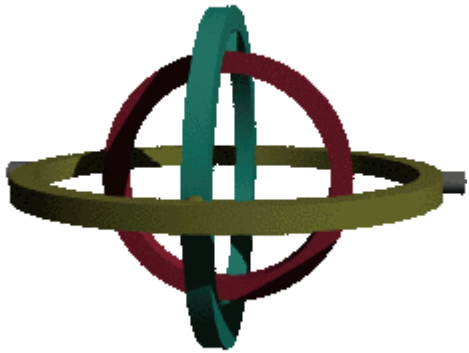
$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Множество кватернионов является примером кольца с делением.

Множество кватернионов образует четырёхмерную ассоциативную алгебру с делением над полем вещественных (но не комплексных) чисел. Вообще $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ являются единственными конечномерными ассоциативными алгебрами с делением над полем вещественных чисел.

Некоммутативность умножения кватернионов приводит к неожиданным последствиям. Например, количество различных корней полиномиального уравнения над множеством кватернионов может быть больше, чем степень уравнения. В частности, уравнение $q^2 + 1 = 0$ имеет бесконечно много решений — это все единичные чисто векторные кватернионы.

7.1.3. Кватернионы и повороты пространства



Организация трёх степеней свободы, но окончательная свобода меньших колец зависит от положения больших колец

Кватернионы, рассматриваемые как алгебра над $\mathbb{R}$, образуют четырёхмерное вещественное векторное пространство. Любой поворот этого пространства относительно 0 может быть записан в виде $q \mapsto \xi q \zeta$, где ξ и ζ — пара единичных кватернионов, при этом пара (ξ, ζ) определяется с точностью до знака, то есть один поворот определяют в точности две пары — (ξ, ζ) и $(-\xi, -\zeta)$. Из этого следует, что группа Ли $SO(\mathbb{R}, 4)$ поворотов $\mathbb{R}^4$ есть факторгруппа $S^3 \times S^3 / \mathbb{Z}_2$, где S^3 обозначает мультипликативную группу единичных кватернионов.

Чисто векторные кватернионы образуют трёхмерное вещественно векторное пространство. Любой поворот пространства чисто векторных кватернионов относительно 0 может быть записан в виде $u \mapsto \xi u \bar{\xi}$, где ξ — некоторый единичный кватернион. Соответственно, $SO(\mathbb{R},3) = S^3/\mathbb{Z}_2$, в частности, $SO(\mathbb{R},3)$ диффеоморфно $\mathbb{R}\mathrm{P}^3$.

7.1.4. «Целые» кватернионы

В качестве нормы кватерниона выберем квадрат его модуля:

$$\|z\| = |z|^2.$$

Целыми по Гурвицу (также engl) принято называть кватернионы $a + bi + cj + dk$ такие, что все $2a, 2b, 2c, 2d$ — целые и одинаковой чётности.

Целый кватернион называется

- *чётным*
- *нечётным*
- *простым*

если таким же свойством обладает его норма.

Целый кватернион называется *примитивным*, если он не делится ни на какое натуральное число, кроме 1, *нацело* (иными словами, $\gcd(2a, 2b, 2c, 2d) \leq 2$).

7.1.4.1. Целые единичные кватернионы

Существует 24 целых единичных кватерниона:

$$\pm 1, \pm i, \pm j, \pm k,$$
$$\frac{\pm 1 \pm i \pm j \pm k}{2}.$$

Они образуют группу по умножению и лежат в вершинах правильного четырёхмерного многогранника — кубооктаэдра (не путать с трёхмерным многогранником-кубооктаэдром).

7.1.4.2. Разложение на простые сомножители

Для примитивных кватернионов верен аналог основной теоремы арифметики.

Теорема. Для любого фиксированного порядка множителей в разложении нормы кватерниона $N(q)$ в произведение простых целых положительных чисел $N(q) = p_1 p_2 ... p_n$ существует разложение кватерниона q в произведение простых кватернионов $q = q_1 q_2 ... q_n$ такое, что $N(q_i) = p_i$. Причём данное разложение единственно по модулю домножения на единицы — это значит, что любое другое разложение будет иметь вид

$$q = (q_1 \epsilon_1)\,(\bar{\epsilon}_1 q_2 \epsilon_2)\,(\bar{\epsilon}_2 q_3 \epsilon_3)\,...\,(\bar{\epsilon}_{n-1} q_n),$$

где ϵ_1, ϵ_2, ϵ_3, … ϵ_{n-1} — целые единичные кватернионы.

Например, примитивный кватернион $q = (1+i)^2(1+i+j)(2+i)$ имеет норму 60, значит, по модулю домножения на единицы он имеет ровно 12 разложений в произведение простых кватернионов, отвечающих 12 разложениям числа 60 в произведений простых:

$60 = 2{\cdot}2{\cdot}3{\cdot}5$ $60 = 2{\cdot}2{\cdot}5{\cdot}3$ $60 = 2{\cdot}3{\cdot}2{\cdot}5$ $60 = 2{\cdot}5{\cdot}2{\cdot}3$ $60 = 2{\cdot}3{\cdot}5{\cdot}2$ $60 = 2{\cdot}5{\cdot}3{\cdot}2$

$60 = 3{\cdot}2{\cdot}2{\cdot}5$ $60 = 5{\cdot}2{\cdot}2{\cdot}3$ $60 = 3{\cdot}2{\cdot}5{\cdot}2$ $60 = 5{\cdot}2{\cdot}3{\cdot}2$ $60 = 3{\cdot}5{\cdot}2{\cdot}2$ $60 = 5{\cdot}3{\cdot}2{\cdot}2$

Общее число разложений такого кватерниона равно

$$24^3 \cdot 12 = 165888$$

7.1.5. Функции кватернионного переменного

7.1.5.1. Вспомогательные функции

Знак кватерниона вычисляется так:

$$\operatorname{sgn} q = \frac{q}{|q|}.$$

Аргумент кватерниона — это угол поворота четырёхмерного вектора, который отсчитывается от вещественной единицы:

$$\arg q = \arccos \frac{a}{|q|}.$$

В дальнейшем используется представление заданного кватерниона q в виде

$$q = a + |\mathbf{u}|\,\mathrm{i} = |q|\,\mathrm{e}^{\mathrm{i}\arg q}$$

Здесь a — вещественная часть кватерниона, $\mathrm{i} = |\mathbf{u}|^{-1}\,\mathbf{u}$. При этом $\mathrm{i}^2 = -1$, поэтому проходящая через q и вещественную прямую плоскость имеет структуру алгебры комплексных чисел, что позволяет перенести на случай кватернионов произвольные аналитические функции. Они удовлетворяют стандартным соотношениям, если все аргументы имеют вид $a + b\mathrm{i}$ для фиксированного единичного вектора i. В случае если требуется рассматривать кватернионы с разным направлением, формулы значительно усложняются, в силу некоммутативности алгебры кватернионов.

7.1.5.2. Элементарные функции

Стандартное определение аналитических функций на ассоциативной нормированной алгебре основано на разложении этих функций в степенные ряды. Рассуждения, доказывающие корректность определения таких функций, полностью аналогичны комплексному

случаю и основаны на вычислении радиуса сходимости соответствующих степенных рядов. Учитывая указанное выше «комплексное» представление для заданного кватерниона, соответствующие ряды можно привести к указанной ниже компактной форме. Здесь приведены лишь некоторые наиболее употребительные аналитические функции, аналогично можно вычислить любую аналитическую функцию. Общее правило таково: если $f(a+b\mathrm{i}) = c + d\mathrm{i}$ для комплексных чисел, то $f(q) = c + d\mathbf{i}$, где кватернион q рассматривается в «комплексном» представлении $q = a + b\mathbf{i}$.

Степень и логарифм

$$\exp q = \exp a\,(\cos|\mathbf{u}| + \sin|\mathbf{u}|\,\hat{\mathbf{u}})$$
$$\ln q = \ln|q| + \arg q\,\hat{\mathbf{u}}$$

Отметим, что, как обычно в комплексном анализе, логарифм оказывается определён лишь с точностью до $2\pi\hat{\mathbf{u}}$.

Тригонометрические функции

$$\sin q = \sin a\ \mathrm{ch}\,|\mathbf{u}| + \cos a\ \mathrm{sh}\,|\mathbf{u}|\,\hat{\mathbf{u}}$$
$$\cos q = \cos a\ \mathrm{ch}\,|\mathbf{u}| - \sin a\ \mathrm{sh}\,|\mathbf{u}|\,\hat{\mathbf{u}}$$
$$\mathrm{tg}\ q = \frac{\sin q}{\cos q}$$

7.1.5.3. Регулярные функции

Существуют разные способы определения регулярных функций кватернионного переменного. Самый явный — рассмотрение кватернионно дифференцируемых функций, при этом можно рассматривать *праводифференцируемые* и *леводифференцируемые* функции, не совпадающие в силу некоммутативности умножения кватернионов. Очевидно, что их теория полностью аналогична. Определим кватернионно леводифференцируемую функцию f как имеющую предел

$$\frac{df}{dq} = \lim_{h \to 0} \left[h^{-1} \left(f\left(q + h\right) - f\left(q\right) \right) \right]$$

Оказывается, что все такие функции имеют в некоторой окрестности точки q вид

$$f = a + qb$$

где a, b — постоянные кватернионы. Другой способ основан на использовании операторов

$$\frac{\partial}{\partial \bar{q}} = \frac{\partial}{\partial t} + \vec{i}\frac{\partial}{\partial x} + \vec{j}\frac{\partial}{\partial y} + \vec{k}\frac{\partial}{\partial z}$$
$$\frac{\partial}{\partial q} = \frac{\partial}{\partial t} - \vec{i}\frac{\partial}{\partial x} - \vec{j}\frac{\partial}{\partial y} - \vec{k}\frac{\partial}{\partial z}$$

и рассмотрении таких кватернионных функций f, для которых

$$\frac{\partial f}{\partial \bar{q}} = 0$$

что полностью аналогично использованию операторов $\frac{\partial}{\partial \bar{z}}$ и $\frac{\partial}{\partial z}$ в комплексном случае. При этом получаются аналоги интегральной теоремы Коши, теории вычетов, гармонических функций и рядов Лорана для кватернионных функций.

7.1.5.4. Производная Гато

Производная Гато функции кватернионного переменного определена согласно формуле

$$\partial f(x)(a) = \lim_{t \to 0} (t^{-1}(f(x + ta) - f(x)))$$

Производная Гато является аддитивным отображением приращения аргумента и может быть представлена в виде

$$\partial f(x)(dx) = \frac{{}_{(s)0}\partial f(x)}{\partial x} dx \frac{{}_{(s)1}\partial f(x)}{\partial x}$$

Здесь предполагается суммирование по индексу s. Число слагаемых зависит от выбора функции f. Выражения $\frac{{}_{(s)0}\partial f(x)}{\partial x}$ и $\frac{{}_{(s)1}\partial f(x)}{\partial x}$ называются компонентами производной.

7.1.6. Виды умножений

Умножение Грассмана

Так по-другому называется общепринятое умножение кватернионов (pq).

Евклидово умножение

Отличается от общепринятого тем, что вместо первого сомножителя берется сопряжённый к нему: $\bar{p}q$. Оно также некоммутативно.

Скалярное произведение

Аналогично одноимённой операции для векторов:

$$p \cdot q = \frac{\bar{p}q + \bar{q}p}{2}.$$

Эту операцию можно использовать для выделения одного из коэффициентов, например, $(a + bi + cj + dk) \cdot i = b$.

Определение модуля кватерниона можно видоизменить:

$$|p| = \sqrt{p \cdot p}.$$

Внешнее произведение

$$\mathrm{Outer}\,(p,q) = \frac{\bar{p}q - \bar{q}p}{2}.$$

Используется не очень часто, тем не менее рассматривается в дополнение к скалярному произведению.

Векторное произведение

Аналогично одноимённой операции для векторов. Результатом является тоже вектор:

$$p \times q = \frac{pq - qp}{2}.$$

7.1.7. Из истории

Система кватернионов была впервые опубликована Гамильтоном в 1843 году. Историки науки также обнаружили наброски по этой теме в неопубликованных рукописях Гаусса, относящихся к 1819—1820 годам.

Бурное и чрезвычайно плодотворное развитие комплексного анализа в XIX веке стимулировало у математиков интерес к следующей задаче: **найти новый вид чисел, аналогичный по свойствам комплексным, но содержащий не одну, а <u>две мнимые единицы</u>.** Предполагалось, что такая модель будет полезна при решении пространственных задач математической физики. Однако работа в этом направлении оказалась безуспешной.

Новый вид чисел был обнаружен ирландским математиком Уильямом Гамильтоном в 1843 году, и он содержал не две, как ожидалось, а **<u>три мнимые единицы</u>**. Гамильтон назвал эти числа *кватернионами*. Позднее Фробениус строго доказал (1877) теорему, согласно которой расширить комплексное поле до поля или тела с двумя мнимыми единицами невозможно.

Несмотря на необычные свойства новых чисел (их некоммутативность), эта модель довольно быстро принесла практическую пользу. **Максвелл использовал компактную кватернионную запись для формулировки своих уравнений электромагнитного поля**. Позднее на основе алгебры кватернионов был создан **трёхмерный векторный анализ** (Гиббс, Хевисайд).

Новые результаты и направления исследований

Кватернионы и метрика Минковского

Как алгебра над $\mathbb{R}$, кватернионы образуют вещественное векторное пространство $\mathbb{H}$, снабжённое тензором третьего ранга S типа (1,2), иногда называемого *структурным тензором*. Как всякий тензор такого типа, S отображает каждую 1-форму t на $\mathbb{H}$ и пару векторов (a, b) из $\mathbb{H}$ в вещественное число $S(t, a, b)$. Для любой фиксированной 1-формы tS превращается в ковариантный тензор второго ранга, который, в случае его симметрии, становится скалярным произведением на $\mathbb{H}$. Поскольку каждое вещественное векторное пространство является также вещественным линейным многообразием, такое скалярное произведение порождает тензорное поле, которое, при условии его невырожденности, становится (псевдо- или собственно-) евклидовой метрикой на $\mathbb{H}$. В случае кватернионов это скалярное произведение индефинитно, его сигнатура не зависит от 1-формы t, а соответствующая псевдоевклидова метрика есть метрика Минковского. Эта метрика автоматически продолжается на группу Ли ненулевых кватернионов вдоль её левоинвариантных векторных полей, образуя так называемую закрытую ФЛРУ (Фридман — Леметр — Робертсон — Уолкер) метрику — важное решение уравнений Эйнштейна. Эти результаты проясняют некоторые аспекты проблемы совместимости квантовой механики и общей теории относительности в рамках теории квантовой гравитации.

7.2. Октавы (алгебра Кэли)

— система гиперкомплексных чисел, 8-мерная алгебра над полем вещественных чисел. Обычно обозначается $\mathbb{O}$, поскольку её элементы (**числа Кэли**) называются иногда

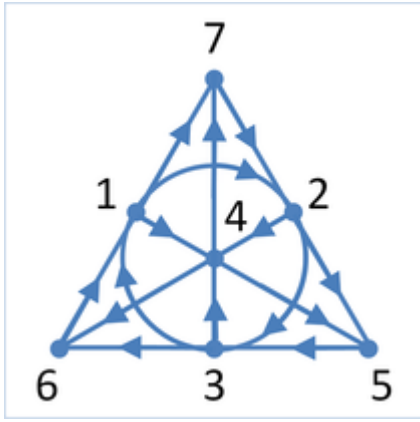
октонионами или **октавами**. **Октавы** $\mathbb{O}$, являющиеся расширением кватернионов, теряют свойство ассоциативности.

Число Кэли — это линейная комбинация элементов $\{1, i, j, k, l, il, jl, kl\}$. Каждая октава *x* может быть записана в форме

$$x = x_0 + x_1\, i + x_2\, j + x_3\, k + x_4\, l + x_5\, il + x_6\, jl + x_7\, kl.$$

с вещественными коэффициентами x_i. Октонионы находят применение в физике: например, в СТО и теории струн. Таблица умножения элементов октавы:

1	***i* (*e1*)**	***j* (*e2*)**	***k* (*e3*)**	***l* (*e4*)**	***il* (*e5*)**	***jl* (*e6*)**	***kl* (*e7*)**
***i* (*e1*)**	−1	*k*	−*j*	*il*	−*l*	−*kl*	*jl*
***j* (*e2*)**	−*k*	−1	*i*	*jl*	*kl*	−*l*	−*il*
***k* (*e3*)**	*j*	−*i*	−1	*kl*	−*jl*	*il*	−*l*
***l* (*e4*)**	−*il*	−*jl*	−*kl*	−1	*i*	*j*	*k*
***il* (*e5*)**	*l*	−*kl*	*jl*	−*i*	−1	−*k*	*j*
***jl* (*e6*)**	*kl*	*l*	−*il*	−*j*	*k*	−1	−*i*
***kl* (*e7*)**	−*jl*	*il*	*l*	−*k*	−*j*	*i*	−1



Плоскость Фано для мнемонического запоминания таблицы умножения

Таблица (Кэли) умножения октонионов

e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1

Часто числа могут заменяться буквенным обозначением:

Число	1	2	3	4	5	6	7
Буквы	*i*	*j*	*k*	*l*	*il*	*jl*	*kl*
Замена	*i*	*j*	*k*	*l*	*m*	*n*	*o*

7.2.1. Свойства

- По теореме Фробениуса, алгебра Кэли является единственной 8-мерной вещественной альтернативной алгеброй без делителей нуля.
- Алгебра Кэли является алгеброй с однозначным делением и с единицей, альтернативной, но неассоциативной и некоммутативной.

7.2.2. Сопряжение и норма

Пусть дан октонион

$$x = x_0 + x_1\, i + x_2\, j + x_3\, k + x_4\, l + x_5\, il + x_6\, jl + x_7\, kl$$

Операция сопряжения октониона x определена равенством

$$x^* = x_0 - x_1\, i - x_2\, j - x_3\, k - x_4\, l - x_5\, il - x_6\, jl - x_7\, kl.$$

Операция сопряжения удовлетворяет равенствам

$$(xy)^* = y^* x^*$$

$$x^* = -\frac{1}{6}(x+(ix)i+(jx)j+(kx)k+(lx)l+((il)x)(il)+((jl)x)(jl)+((kl)x)(kl))$$

Вещественная часть октониона x определена равенством

$$\frac{1}{2}(x + x^*) = x_0$$

и мнимая часть октониона x определена равенством

$$\frac{1}{2}(x - x^*)$$

Норма октониона x определена равенством

$$\|x\| = \sqrt{x^* x}.$$

Легко убедиться, что норма неотрицательное вещественное число

$$\|x\|^2 = x^* x = x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2.$$

Следовательно, $\|x\| = 0$ тогда и только тогда, когда $x = 0$.

Из определения нормы следует, что октонион $x \neq 0$ обратим и

$$x^{-1} = \frac{x^*}{\|x\|^2}.$$

7.3. Седенионы

Седенионы — элементы 16-мерной алгебры. Каждый седенион — это линейная комбинация элементов 1, e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}, e_{12}, e_{13}, e_{14} и e_{15}, которая формирует базис векторного пространства седенионов. (Аналогично комплексным числам, двумерной алгебре, где каждое число является комбинацией двух элементов и имеет вид: $a + bi$). В отличие от октав, седенионы $\mathbb{S}$ не обладают свойством альтернативности, но сохраняют свойство степенной ассоциативности

Как и в случае октонионов, умножение седенионов не является ни коммутативным, ни ассоциативным. В отличие от октонионов, седенионы не обладают свойством альтернативности. Тем не менее седенионы обладают свойством степенной ассоциативности. Есть единичный элемент, есть обратные элементы, но нет алгебры деления. Это происходит из-за того, что есть делители нуля, т. е. два ненулевых элемента могут быть перемножены и получится нулевой результат: например, $(e_3 + e_{10}) \times (e_6 - e_{15})$.

Множество седенионов обозначается как $\mathbb{S}$.

Таблица умножения элементов приведена ниже:

$\times$	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6	e_9	$-e_8$	$-e_{11}$	e_{10}	$-e_{13}$	e_{12}	e_{15}	$-e_{14}$
e_2	e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$	e_{10}	e_{11}	$-e_8$	$-e_9$	$-e_{14}$	$-e_{15}$	e_{12}	e_{13}
e_3	e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$	e_{11}	$-e_{10}$	e_9	$-e_8$	$-e_{15}$	e_{14}	$-e_{13}$	e_{12}
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3	e_{12}	e_{13}	e_{14}	e_{15}	$-e_8$	$-e_9$	$-e_{10}$	$-e_{11}$
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2	e_{13}	$-e_{12}$	e_{15}	$-e_{14}$	e_9	$-e_8$	e_{11}	$-e_{10}$

									3	2		4				0
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$	e_{14}	$-e_{15}$	$-e_{12}$	e_{13}	e_{10}	$-e_{11}$	$-e_8$	e_9
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1	e_{15}	e_{14}	$-e_{13}$	$-e_{12}$	e_{11}	e_{10}	$-e_9$	$-e_8$
e_8	e_8	$-e_9$	$-e_{10}$	$-e_{11}$	$-e_{12}$	$-e_{13}$	$-e_{14}$	$-e_{15}$	-1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_9	e_9	e_8	$-e_{11}$	e_{10}	$-e_{13}$	e_{12}	e_{15}	$-e_{14}$	$-e_{11}$	-1	$-e_3$	e_2	$-e_5$	e_4	e_7	$-e_6$
e_{10}	e_{10}	e_{11}	e_8	$-e_9$	$-e_{14}$	$-e_{15}$	e_{12}	e_{13}	$-e_{22}$	e_3	-1	$-e_{11}$	$-e_6$	$-e_7$	e_4	e_5
e_{11}	e_{11}	$-e_{10}$	e_9	e_8	$-e_{15}$	e_{14}	$-e_{13}$	e_{12}	$-e_{33}$	$-e_2$	e_{11}	-1	$-e_7$	e_6	$-e_5$	e_4
e_{12}	e_{12}	e_{13}	e_{14}	e_{15}	e_8	$-e_9$	$-e_{10}$	$-e_{11}$	$-e_{44}$	e_5	e_6	e_7	-1	$-e_{11}$	$-e_2$	$-e_3$
e_{13}	e_{13}	$-e_{12}$	e_{15}	$-e_{14}$	e_9	e_8	e_{11}	$-e_{10}$	$-e_{55}$	$-e_4$	e_7	$-e_6$	e_{11}	-1	e_3	$-e_2$
e_{14}	e_{14}	$-e_{15}$	$-e_{12}$	e_{13}	e_{10}	$-e_{11}$	e_8	e_9	$-e_{66}$	$-e_7$	$-e_4$	e_5	e_2	$-e_3$	-1	e_1
e_{15}	e_{15}	$-e_{14}$	$-e_{13}$	e_{12}	e_{11}	e_{10}	$-e_9$	e_8	$-e_{77}$	e_6	$-e_5$	$-e_4$	e_3	e_2	$-e_1$	-1

Для этих множеств обобщённых чисел справедливо следующее выражение: $\mathbb{C} \subset \mathbb{H} \subset \mathbb{O} \subset \mathbb{S}$

8. Дуальные числа

Дуальные числа или (гипер)**комплексные числа параболического типа** — гиперкомплексные числа вида $a + \varepsilon * b$, где a и b — вещественные числа, и $\varepsilon^2 = 0$. Любое дуальное число однозначно определяется такой парой чисел a и b. Множество всех дуальных чисел образует двумерную коммутативную ассоциативную алгебру с единицей относительно мультипликативной операции над полем

вещественных чисел $\mathbb{R}$. В отличие от поля обычных комплексных чисел, эта алгебра содержит делители нуля, причём все они имеют вид $a * \varepsilon$. Плоскость всех дуальных чисел представляет собой «альтернативную комплексную плоскость». Аналогичным образом строятся алгебры комплексных и двойных чисел.

Замечание. Иногда дуальные числа называют двойными числами, хотя обычно под двойными числами понимается иная система гиперкомплексных чисел.

8.1. Определение

8.1.1. Алгебраическое определение

Дуальные числа — это пары вещественных чисел вида $(a,\ b)$, для которых определены операции умножения и сложения по правилам:

$$(a_1,\ b_1) + (a_2,\ b_2) = (a_1 + a_2,\ b_1 + b_2)$$
$$(a_1,\ b_1) * (a_2,\ b_2) = (a_1 a_2,\ a_1 b_2 + a_2 b_1)$$

Числа вида $(a,\ 0)$ отождествляются при этом с вещественными числами, а число $(0,\ 1)$ обозначается ε, после чего определяющие тождества примут вид:

$$\varepsilon^2 = 0, \quad (a,\ b) = a + b\varepsilon$$
$$(a_1 + \varepsilon b_1) + (a_2 + \varepsilon b_2) = (a_1 + a_2) + \varepsilon(b_1 + b_2),$$
$$(a_1 + \varepsilon b_1)(a_2 + \varepsilon b_2) = (a_1 a_2) + \varepsilon(a_1 b_2 + a_2 b_1).$$

Более кратко, кольцо дуальных чисел есть факторкольцо $\mathbb{R}[x]/(x^2)$ кольца вещественных многочленов по идеалу, порождённому многочленом x^2.

8.1.2. Линейное представление

Дуальные числа можно представить как матрицы из вещественных чисел, при этом сложению дуальных чисел соответствует сложение матриц, а умножению чисел — умножение матриц. Положим $\varepsilon = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

Тогда произвольное дуальное число примет вид

$$a + b\varepsilon = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}.$$

8.1.3. Показательная форма

Для экспоненты с дуальным показателем верно следующее равенство:

$$\mathrm{e}^{\varepsilon x} = 1 + \varepsilon x$$

Данная формула позволяет представить любое дуальное число в показательной форме и найти его логарифм по вещественному основанию. Она может быть доказана разложением экспоненты в ряд Тейлора:

$$\mathrm{e}^{\varepsilon x} = 1 + \varepsilon x + \frac{(\varepsilon x)^2}{2!} + \frac{(\varepsilon x)^3}{3!} + \cdots$$

При этом все члены выше первого порядка равны нулю. Как следствие:

$$\sinh \varepsilon x = \sin \varepsilon x = \varepsilon x$$
$$\cosh \varepsilon x = \cos \varepsilon x = 1$$

8.2. Арифметические операции

- Сложение

$$(a+b\varepsilon)+(c+d\varepsilon)=(a+c)+(b+d)\varepsilon$$

- Вычитание

$$(a+b\varepsilon)-(c+d\varepsilon)=(a-c)+(b-d)\varepsilon$$

- Умножение

$$(a+b\varepsilon)*(c+d\varepsilon)=(ac)+(bc+ad)\varepsilon$$

- Деление

$$\frac{a+b\varepsilon}{c+d\varepsilon}=\frac{a}{c}+\frac{bc-ad}{c^2}\varepsilon$$

8.3. Корни

Корень n-й степени из числа вида $a+\varepsilon b$ определяется как:

$$\sqrt[n]{a}+\frac{\varepsilon b}{n\sqrt[n]{a^{n-1}}}$$

8.4. Дифференцирование

Дуальные числа тесно связаны с дифференцированием функций. Рассмотрим аналитическую функцию $f(x)$, область определения которой можно естественным образом продолжить до кольца дуальных чисел. Можно легко показать, что

$$f(x+y\varepsilon)=f(x)+y\varepsilon f'(x)$$

Таким образом, производя вычисления не над вещественными, а над дуальными числами, можно автоматически получать значение производной функции в точке. Особенно удобно рассматривать таким образом композиции функций.

Можно провести аналогию между дуальными числами и числами **нестандартного анализа.** Мнимая единица ε кольца дуальных чисел подобна бесконечно малому числу нестандартного анализа: любая степень (выше первой) ε в точности равна 0, в то время как любая степень бесконечно малого числа *приблизительно* равна 0 (является бесконечно малой более высокого порядка). Значит, если δ — бесконечно малое число, то с точностью до $o(\delta)$ кольцо гипердействительных чисел вида $\mathbb{R} + \mathbb{R}\delta$ изоморфно кольцу дуальных чисел.

9. p-адическое число

p-адические числа $\mathbb{Q}_p$ можно рассматривать как элементы поля, являющегося пополнением поля рациональных чисел $\mathbb{Q}$ при помощи т. н. p-адического нормирования, аналогично тому, как поле действительных чисел $\mathbb{R}$ определяется как его пополнение при помощи обычной абсолютной величины.

Для заданного фиксированного простого числа *p* ***p***- (произносится: *пэ-адическое*; соответственно: *два-адическое*, *три-адическое* и т.п.) — элемент расширения поля рациональных чисел, являющегося пополнением поля рациональных чисел относительно *p*-адической нормы, определяемой на основе свойств делимости целых чисел на *p*.

p-адические числа были введены Гензелем (*нем.*) в 1897 году.

Поле *p*-адических чисел обычно обозначается $\mathbb{Q}_p$ или $\mathbf{Q}_p$.

9.1. Алгебраическое построение

9.1.1. Целые *p*-адические числа

9.1.1.1. Стандартное определение

Целым *p*-адическим числом для заданного простого p называется бесконечная последовательность $x = \{x_1, x_2, \ldots\}$ вычетов x_n по модулю p^n, удовлетворяющих условию:

$$x_n \equiv x_{n+1} \pmod{p^n}.$$

Сложение и умножение целых *p*-адических чисел определяется как почленное сложение и умножение таких последовательностей. Для них непосредственно проверяются все аксиомы кольца.

9.1.1.2. Определение через проективный предел

В терминах проективных пределов кольцо целых p-адических чисел определяется как предел

$$\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$$

колец $\mathbb{Z}/p^n\mathbb{Z}$ вычетов по модулю p^n относительно естественных проекций $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$.

Эти рассмотрения можно провести в случае не только простого числа p, но и любого составного числа m — получится т. н. кольцо m-адических чисел, но это кольцо в отличие от $\mathbb{Z}_p$ обладает делителями нуля, поэтому дальнейшие построения, рассматриваемые ниже, к нему неприменимы.

9.1.1.3. Свойства

Кольцо целых *p*-адических чисел обычно обозначается $\mathbb{Z}_p$. Обычные целые числа вкладываются в $\mathbb{Z}_p$ очевидным образом: $x = \{x, x, \ldots\}$ и являются подкольцом.

```
  ...10424      ...30021        ...013
+ ...21242    - ...12433      x ...442
-----------   -----------     ---------
  ...32221      ...12033        ...031
                              + ...12
                                ...2
                              ---------
                                ...401
```

Пример выполнения арифметических операций над 5-адическими числами.

Беря в качестве элемента класса вычетов число $a_n = x_n \bmod p^n$ (таким образом, $0 \le a_n < p^n$), мы можем записать каждое целое *p*-адическое число в виде $x = \{a_1, a_2, \ldots\}$ однозначным образом. Такое представление называется *каноническим*. Записывая каждое a_n в *p*-ичной системе счисления $a_n = b_n \ldots b_2 b_1$ и, учитывая, что $a_n \equiv a_{n+1} \pmod{p^n}$, мы можем всякое *p*-адическое число в каноническом виде представить в виде $x = \{b_1, b_2 b_1, b_3 b_2 b_1, \ldots\}$ или записать в виде бесконечной последовательности цифр в *p*-ичной системе счисления $x = \{\ldots b_n \ldots b_2 b_1\}$. Действия над такими последовательностями производятся по обыкновенными правилами сложения, вычитания и умножения «столбиком» в *p*-ичной системе счисления.

В такой форме записи натуральным числам и нулю соответствуют *p*-адические числа с конечным числом ненулевых цифр, совпадающих

с цифрами исходного числа. Отрицательным числам соответствуют *p*-адические числа с бесконечным числом ненулевых цифр, например в пятеричной системе −1=…4444=(4).

9.1.2. *p*-адические числа

9.1.2.2. Определение как поля частных $\mathbb{Q}_p$

p-адическим числом называется элемент поля частных $\mathbb{Q}_p$ кольца $\mathbb{Z}_p$ целых *p*-адических чисел. Это поле называется полем *p*-адических чисел.

9.1.2.3. Свойства

Поле *p*-адических чисел содержит в себе поле рациональных чисел.

```
...40,1:...01,3=...401:...013

  ...401   | ...013
- ...031   | ...442
  ...32
- ...12
  ...2
- ...2
  ...
```

Пример выполнения деления 5-адических чисел.

Нетрудно доказать, что любое целое *p*-адическое число некратное *p* обратимо в кольце $\mathbb{Z}_p$, а кратное *p* однозначно записывается в виде xp^n, где *x* не кратно *p* и поэтому обратимо, а $n > 0$. Поэтому любой ненулевой элемент поля $\mathbb{Q}_p$ может быть записан в виде xp^n, где *x* не кратно *p*, а *n* любое; если *n* отрицательно, то, исходя из

представления целых *p*-адических чисел в виде последовательности цифр в *p*-ичной системе счисления, мы можем записать такое *p*-адическое число в виде последовательности $x = \{\dots b_k \dots b_2 b_1, b_0 b_{-1} \dots b_{n+1}\}$, то есть, формально представить в виде *p*-ичной дроби с конечным числом цифр после запятой и, возможно, бесконечным числом ненулевых цифр до запятой. Деление таких чисел можно также производить аналогично «школьному» правилу, но начиная с младших, а не старших разрядов числа.

9.2. Метрическое построение

Любое рациональное число r можно представить как $r = p^n \frac{a}{b}$ где a и b целые числа, не делящиеся на p, а n — целое. Тогда $|r|_p$ — p-адическая норма r — определяется как p^{-n}. Если $r = 0$, то $|r|_p = 0$.

Поле p-адических чисел есть пополнение поля рациональных чисел с метрикой d_p, определённой p-адической нормой: $d_p(x, y) = |x - y|_p$. Это построение аналогично построению поля вещественных чисел как пополнения поля рациональных чисел при помощи нормы, являющейся обычной абсолютной величиной.

Норма $|r|_p$ продолжается по непрерывности до нормы на $\mathbb{Q}_p$.

9.3. Свойства

- Каждый элемент *x* поля *p*-адических чисел может быть представлен в виде сходящегося ряда

$$x = \sum_{i=n_0}^{\infty} a_i p^i$$

где n_0 — некоторое целое число, а a_i — целые неотрицательные числа, не превосходящие $p-1$. А именно, в качестве a_i здесь выступают цифры из записи *x* в системе счисления с основанием *p*. Такая сумма всегда сходится в метрике d_p к самому x.

- *p*-адическая норма $|x|_p$ удовлетворяет сильному неравенству треугольника

$$|x-z|_p \le \max\{|x-y|_p, |y-z|_p\}.$$

  - Числа $x \in \mathbb{Q}_p$ с условием $|x|_p \le 1$ образуют кольцо $\mathbb{Z}_p$ целых *p*-адических чисел, являющееся пополнением кольца целых чисел $\mathbb{Z} \subset \mathbb{Q}$ в норме $|x|_p$.
  - Числа $x \in \mathbb{Q}_p$ с условием $|x|_p = 1$ образуют мультипликативную группу и называются *p*-адическими единицами.
  - Совокупность чисел $x \in \mathbb{Q}_p$ с условием $|x|_p < 1$ является главным идеалом в $\mathbb{Z}_p$ с образующим элементом *p*.

- метрическое пространство $(\mathbb{Q}_p, d_p)$ гомеоморфно Канторову множеству, а пространство $(\mathbb{Q}_p, d_p)$ гомеоморфно Канторову множеству с вырезанной точкой.
- Для различных *p* нормы $|x|_p$ независимы, а поля $\mathbb{Q}_p$ неизоморфны.
- Для любых элементов r_∞, r_2, r_3, r_5, r_7, … таких, что $r_\infty \in \mathbb{R}$ и $r_p \in \mathbb{Q}_p$, можно найти последовательность рациональных чисел x_n таких, что для любого *p* $|x_i - r_p|_p \to 0$ и $|x_i - r_\infty| \to 0$.

Применения

- Если $F(x_1, x_2, \ldots, x_n)$ — многочлен с целыми коэффициентами, то разрешимость при всех *k* сравнения

$$F(x_1, x_2, \cdots, x_n) \equiv 0 \pmod{p^k}$$

эквивалентна разрешимости уравнения

$$F(x_1, x_2, \cdots, x_n) = 0$$

в целых *p*-адических числах. Необходимым условием разрешимости этого уравнения в целых или рациональных числах является его разрешимость в кольцах или, соответственно, полях *p*-адических чисел при всех *p*, а также в поле вещественных чисел. Для некоторых классов многочленов (например, для квадратичных форм) это условие является также достаточным.

На практике для проверки разрешимости уравнения в целых *p*-адических числах достаточно проверить разрешимость указанного сравнения для определенного конечного числа значений *k*. Например, согласно лемме Гензеля (*англ.*), при $n = 1$ достаточным условием для разрешимости сравнения при всех натуральных *k* служит наличие простого решения у сравнения по модулю *p* (т. е., простого корня у соответствующего уравнения в поле вычетов по модулю *p*). Иначе говоря, при $n = 1$ для проверки наличия корня у уравнения в целых *p*-адических числах, как правило, достаточно решить соответствующее сравнение при $k = 1$.

10. Адели

определяются как бесконечные последовательности $\{a_\infty, a_2, a_3, \ldots a_p \ldots\}$, где a_∞ — любое действительное число, а a_p — *p*-адическое, причём все a_p, кроме, может быть, конечного их числа, являются целыми *p*-адическими. Складываются и умножаются адели покомпонентно и образуют кольцо. Поле рациональных чисел вкладывается в это кольцо обычным образом $r \to \{r, r, \ldots r, \ldots\}$. Обратимые элементы этого кольца образуют группу и называются

.

АДЕЛЬ - элемент группы аделей, т. е. топологического прямого произведения

$$\Pi_{v \in V} G_{k_v}(G_{O_v})$$

групп G_{k_v} с отмеченными открытыми подгруппами GQ Здесь G_k-линейная алгебраическая группа, определенная над глобальным полем k, V - множество всех неэквивалентных нормирований поля k, k_v - пополнение к относительно $v \in V$, O_v - кольцо целых элементов в k_v . Группа аделей алгебраической группы G обозначается через G_A . Так как все группы G_{kr} локально компактны, а G_{Ov} компактны, то G_A - локально компактная группа.

Примеры.

1) Если G_k - аддитивная группа k^+ поля k, то G_A обладает естественной структурой кольца, которое называют кольцом аделей поля k и обозначается A_k .

2) Если G_k - мультипликативная группа k^* поля k, то G_k называется группой иделей поля k (группа иделей является группой единиц в кольце аделей A_k).

3) Если $G_k = GL(n, k)$ - полная линейная группа над k, то G_A состоит из таких элементов $g = (g_v) \in \Pi_{v \in V} G_v$, что $g_v \in GL(n, O_v)$ для почти всех нормирований v.

Понятие группы аделей было впервые введено К. Шевалле (C. Chevalley) в 30-х гг. 20 в. для полей алгебраических чисел в связи с потребностями теории полей классов. Спустя 20 лет оно было обобщено М. Кнезером (M. Kneser) и Ц. Тамагава (T. Tamagawa) на алгебраич. группы. Последние заметили, что основные результаты об арифметике квадратичных форм над числовыми полями удобно переформулировать на языке группы аделей.

Образ диагонального вложения G_k в G_A является дискретной подгруппой в G_A и называется подгруппой главных аделей. Если ∞ - множество всех архимедовых нормирований k, то

$$G_{A(\infty)} = \Pi_{v \in \infty} G_{k_v} \times \Pi_{v \in \infty} G_{O_v}$$

называется подгруппой целых аделей. Если $G_k = k^*$, то число различных двойных классов смежности вида $G_k \times GA_{(\infty)}$ группы аделей G_A конечно и равно числу классов идеалов поля k. Естественно возникающий вопрос о конечности числа таких двойных классов для произвольной алгебраической группы G связан с теорией приведения для подгруппы главных аделей, т. е. с конструкцией фундаментальной области для факторпространства G_A / G_k . Доказано, что G_A / G_k тогда и только тогда компактно, когда группа G является k-анизотропной. Более того, решен вопрос о том, когда над полем алгебраических чисел факторпространство G_A / G_k имеет конечный объем в Хаара мере. Так как G_A локально компактна, то такая мера всегда существует и объем G_A / G_k в мере Хаара конечен тогда и только тогда, когда группа G не имеет рациональных k-характеров. Величина $\tau(G)$ объема G_A / G_k представляет важный арифметический инвариант алгебраической группы G. Опираясь на эти результаты, доказано, что для произвольной алгебраической группы G имеет место разложение

$$G_A = \bigcup_{i=1}^{m} G_k x_i G_{A(\infty)}.$$

Для случая, когда k-функциональное поле, также доказана конечность числа двойных классов смежности указанного вида для группы аделей алгебраической группы и построен аналог теории приведения.

11. Интервальная арифметика

Практически важным обобщением числовой системы является интервальная арифметика.

Интервальная арифметика — математическая структура, которая для вещественных интервалов определяет операции, аналогичные обычным арифметическим. Эту область математики называют также **интервальным анализом** или **интервальными вычислениями.** Данная математическая модель удобна для исследования различных объектов, которые представлены матем атическими моделями:

- Величины, значения которых известны только приближённо, то есть определён конечный интервал, в котором эти значения содержатся.
- Величины, значения которых в ходе вычислений искажены ошибками округления.
- Случайные величины.

Объекты и операции интервальной арифметики можно рассматривать как обобщение модели вещественных чисел, поэтому интервалы в ряде источников называются **интервальными числами**. Практическая важность этой модели связана с тем, что результаты измерений и вычислений почти всегда имеет некоторую погрешность, которую необходимо учесть и оценить.

11.1. Операции над интервалами

Мы будем рассматривать всевозможные конечные вещественные интервалы $[a, b]\ (a \leqslant b)$. Операции над ними определяются следующим образом:

- Сложение: $[a,b] + [c,d] = [a + c, b + d]$
- Вычитание: $[a,b] - [c,d] = [a - d, b - c]$
- Умножение: $[a,b] \times [c,d] = [\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)]$
- Деление: $[a,b] / [c,d] = [\min(a/c, a/d, b/c, b/d), \max(a/c, a/d, b/c, b/d)]$

Из определения видно, что интервал-сумма содержит всевозможные суммы чисел из интервалов-слагаемых и определяет границы множества таких сумм. Аналогично трактуются прочие действия. Отметим, что операция деления определена только в том случае, когда интервал-делитель не содержит нуля.

Вырожденные интервалы, у которых начало и конец совпадают, можно отождествить с обычными вещественными числами. Для них данные выше определения совпадают с классическими арифметическими действиями.

11.2. Свойства операций

Сложение и умножение интервалов коммутативны и ассоциативны. Дистрибутивное свойство имеет место в ослабленном виде:

$$X(Y+Z) \subset XY + XZ$$

12. Поличисла (n-числа)

Алгебра поличисел P_n реализуется элементами $A \in P_n$ вида:

$$A = A_1 e_1 + \ldots + A_n e_n,$$

где $A_i \in P_n$, e_i – набор образующих P_n, подчиняющихся следующим правилам умножения (умножение коммутативно и ассоциативно):

$$e_i e_j = 0 \quad (i \neq j), \quad e_i^2 = 1.$$

Нетрудно проверить, что умножение в алгебре поличисел в выбранном базисе сводится к умножению соответствующих компонент, а деление определено только для поличисел, у которых все $A_i \neq 0$ (по этой причине поличисла не образуют числового поля). Алгебраическая единица имеет в выбранном базисе следующее представление:

$$I = e_1 + \ldots + e_n.$$

На алгебре P_n существует n-1 операция комплексного сопряжения. Одну из них можно определить следующим правилом:

$$A^{(1)} = A^* = A_n e_1 + A_1 e_2 + \ldots + A_{n-1} e_n,$$

которое сводится к циклической перестановке компонент поличисла A. k-ое комплексное сопряжение можно определить формулой:

$$A^{(k)} = A^{k(1)} = ((A^*)^*)^{\cdots})^* (k \text{ - раз})$$

Очевидно, что $A^{(n)} = A$.

Рассмотрим поличисло вида

$$N(A) = AA^{(1)}A^{(2)} \dots A^{(n-1)}, \qquad (1)$$

где $A \in P_n$.

Нетрудно проверить, что $N(A)$ вещественно в том смысле, что

$$N(A) = r^n I,$$

где $r^n \in R$.

Число r называется *(квази)нормой* поличисла A. Квазинорма r выражается через координаты поличисла A по формуле :

$$r^n = A_1 A_2 \dots A_n = G(A, A, \dots, A), \qquad (2)$$

где G– n-форма

$$G = \hat{S}\left(dx^1 \otimes \cdots \otimes dx^n\right), \qquad (3)$$

$\hat{S}$ – оператор симметризации. Эта форма является (финслеровой) метрикой в пространствах Бервальда-Моора. Формулы (1)-(3) проясняют связь алгебры поличисел с пространствами Бервальда-Моора: *метрическая n-форма (3) индуцирована вещественной алгебраической формой* $N(A)$*, являющейся многомерным аналогом евклидовой квадратичной формы* $|z|^2 = zz^*$ *на комплексной плоскости.*

По аналогии с комплексной билинейной формой:

$$(\zeta, \xi) = Re(\zeta\xi),$$

где $\zeta, \xi \in C$, можно рассмотреть n-линейную форму

$$(A, B, \ldots, Z) = \mathrm{Re}(AB \ldots Z) = \sum_{\sigma(A,B,\ldots,Z)} AB^{(1)}C^{(2)} \ldots Z^{(n-1)} = n!G(A, B, \ldots, Z). \quad (4)$$

Здесь суммирование производится по множеству $\sigma(A, B, \ldots, Z)$ всех перестановок элементов $A, B, \ldots, Z \in P_n$. Последний знак равенства в (4) (он устанавливается непосредственной проверкой) также выявляет генетическую связь алгебр поличисел и геометрий соответствующих пространств Бервальда-Моора.

Можно показать, что описанная выше алгебра поличисел P_n является прямой суммой n экземпляров алгебры вещественных чисел R. Среди всех ассоциативно-коммутативных алгебр она, в определенном смысле, максимально симметрична (содержит n гиперболических мнимых единиц). Более общей конструкцией будет поличисловая алгебра $P_{n,m}$, представляющая собой прямую сумму n экземпляров алгебры вещественных чисел R и m экземпляров алгебры комплексных чисел C.

13. Еще раз о цепочке чисел

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$$

Об этой цепочке последовательных расширений понятия числа (или по крайней мере первые 4—6 членов ее) мы уже говорили. Символы, составляющие цепочку, являются практически стандартными обозначениями соответственно для множеств натуральных, целых, рациональных, вещественных, комплексных чисел, кватернионов и октонионов (последние, как мы знаем, называются также октавами или числами Кэли).

Мы обсудим здесь переходы от одного звена цепочки к следующему и покажем, что идеи, лежащие в основе этих переходов, работают и в теориях математического моделирования.

13.1. От N к Z и от Z к Q: группа Гротендика, тела Ли и производные категории

Напомним, что натуральные числа можно складывать, но не всегда можно вычитать; целые числа можно умножать, но не всегда можно делить. Стремление обойти эти неудобства, по существу, и вызвало переход от натуральных чисел к целым и от целых к рациональным.

Напомним, как совершаются эти переходы. Если мы хотим вычесть натуральное число m из натурального числа n, то в случае $m \geqslant n$ ответ не может быть натуральным числом. Обозначим его временно символом $n \ominus m$. Если мы хотим, чтобы в расширенном множестве чисел выполнялись привычные нам аксиомы сложения, то мы должны будем отождествить $n \ominus m$ со всеми выражениями $(n + k) \ominus (m + k)$, $k \in \mathbf{N}$, а также с выражениями вида $(n - k) \ominus (m - k)$, $1 \leqslant k < \min(m, n)$. Другими словами, символы $n_1 \ominus m_1$ и $n_2 \ominus m_2$ отождествляются, если $n_1 + m_2 = n_2 + m_1$.

Рассмотрим теперь всевозможные выражения вида $n \ominus m$, $n, m \in \mathbf{N}$, с указанным законом отождествления. Их можно не только складывать (покомпонентно), но и вычитать по правилу

$$n_1 \ominus m_1 - n_2 \ominus m_2 = (n_1 + m_2) \ominus (n_2 + m_1).$$

Например, $0 \ominus 0 - m \ominus n = n \ominus m$. Можно проверить, что классы эквивалентности образуют группу по сложению. Сделайте это самостоятельно (это упражнение предназначается тем, кто только начинает осваивать понятие группы). Довольно просто установить, что полученная группа изоморфна Z: при $m>n$ символы $(m + k) \ominus (n + k)$ отождествляются с натуральным числом m — n, при $m = n$ — с нулем, а при $m < n$ — с отрицательным числом m — n.

Процедура построения мультипликативной группы Q* ненулевых рациональных чисел исходя из полугруппы $\mathbf{Z} \setminus \{0\}$ полностью аналогична: мы рассматриваем формальные символы $m:n$, где $m, n \in \mathbf{Z} \setminus \{0\}$, и отождествляем $m_1 : n_1$ с $m_2 : n_2$, если $m_1 n_2 = m_2 n_1$. Ясно, что класс эквивалентности символа $m : n$ можно отождествить с рациональным числом $r = m/n$.

Более интересный пример. Рассмотрим совокупность всех конечных групп Г. Если Γ_1 — нормальный делитель в Г и Γ_2 — факторгруппа Γ/Γ_1, то естественно считать, что Г «делится» па Γ_1 и «частное» равно Γ_2. Попробуем из этого материала построить коммутативную группу $\mathfrak{G}$.

Групповой закон в $\mathfrak{G}$ мы обозначим знаком «+» (аддитивная запись). Пусть [Г] обозначает класс конечных групп, изоморфных группе Г. По определению $\mathfrak{G}$ порождается всеми символами [Г] с соотношениями

$$[\Gamma] = [\Gamma_1] + [\Gamma_2],$$

если Γ_1 — нормальный делитель в Г, а $\Gamma_2 = \Gamma/\Gamma_1$.

Это значит, что элементом группы $\mathfrak{G}$ является класс эквивалентности выражений вида

$$n_1 \cdot [\Gamma_1] + n_2 \cdot [\Gamma_2] + \ldots + n_h \cdot [\Gamma_h], \qquad (1)$$

где $n_i \in Z$, а Γ_i — конечные группы. Справедлива

Теорема 1. *Группа* $\mathfrak{G}$ *— свободная абелева группа со счетным числом образующих. В качестве этих образующих можно выбрать классы* [Г], *где* Г *— либо циклическая группа* $Ц_p$ *простого порядка p, либо простая конечная группа.*

Таким образом, каждое выражение вида (1) можно заменить ровно одним эквивалентным ему выражением того же вида, в котором Γ_i принадлежат списку групп, указанному в теореме.

Во всех рассмотренных случаях мы строили группу по одному и тому же принципу, вводя дополнительные элементы (отрицательные числа, дроби, формальные линейные комбинации и т. п.) и разбивая полученное множество на классы эквивалентности.

Наиболее общим выражением описанного принципа считалось понятие *группы Гротендика,* $\mathfrak{G}(\mathcal{K})$, определенное для любой малой аддитивной категории $\mathcal{K}$. Эта группа по определению коммутативна и порождается классами эквивалентности объектов категории с соотношениями [*A*] = [*B*] + [*C*], где *B* — подобъект *A,* а *C* — соответствующий фактор-объект. Например, построенная выше группа $\mathfrak{G}$ является группой Гротендика категории конечных групп.

Известно, что для категории всех счетных абелевых групп с конечным числом образующих группа Гротенднка $\mathfrak{G}$ изоморфна Z.

Одно из самых ярких применений этой конструкции — так называемая *К*-теория, где исходным материалом для построения группы служит категория векторных расслоений над заданным гладким многообразием. Возможно, однако, дальнейшее обобщение, в котором вводимая операция некоммутативна.

Пример. Пусть $\mathcal{A}$ означает алгебру с единицей над полем С, порожденную элементами *p* и *q* с соотношением $pq - qp = 1$. Эту алгебру удобно реализовать в виде алгебры дифференциальных операторов на прямой с полиномиальными коэффициентами: образующим *p* и *q* соответствуют операторы дифференцирования $\frac{d}{dx}$ и умножения на *x*.

Отметим, что в $\mathscr{A}$ нет делителей нуля, т. е. из $ab = 0$ следует, что или $a = 0$ или $b = 0$.

Назовем правой дробью выражение вида ab^{-1} и левой дробью выражение вида $b^{-1}a$, где $a,\ b \in \mathscr{A}$ и $b \neq 0$.

Скажем, что левая дробь $c^{-1}d$ эквивалентна правой дроби ab^{-1}, если $ca = db$. Две левые (соответственно правые) дроби будем считать эквивалентными, если они эквивалентны в указанном выше смысле одной и той же правой (соответственно левой) дроби. Имеет место

Теорема 2. *В каждом классе эквивалентности есть и правые и левые дроби. В любых двух классах найдутся левые (соответственно правые) дроби с общим знаменателем.*

Доказательство теоремы выводится из следующего факта, представляющего самостоятельный интерес.

Лемма. *Для любых двух ненулевых элементов из $\mathscr{A}$ существует ненулевое общее левое (правое) кратное.*

Доказательство. Пусть L_n означает подпространство в $\mathscr{A}$, состоящее из всех элементов, которые можно записать в виде многочлена степени $\leq n$ от образующих p и q. Легко проверить, что $\dim L_n = \frac{1}{2}(n+1)(n+2)$.

Пусть a и b принадлежат L_m. Тогда пространства $L_n a$ и $L_n b$ содержатся в L_{n+m} (Мы обозначаем $L_n a$ множество всех элементов вида $xa,\ x \in L_n$. Вообще, если A и B — множества, а $*$ — некоторая операция над элементами этих множеств, то символом $A * B$ означают множество всех элементов вида $a * b$, где $a \in A,\ b \in B$.) При достаточно большом n будет справедливо неравенство $\dim L_n a + \dim L_n b > \dim L_{n+m}$. Поэтому $L_n a$ и $L_n b$ имеют общий ненулевой элемент, который и будет общим левым кратным a и b.

Теорема 1 позволяет определить для алгебры $\mathscr{A}$ *тело отношений D*. А именно, классы эквивалентности дробей можно складывать, вычитать и делить по правилам

$$a_1 b^{-1} \pm a_2 b^{-1} = (a_1 \pm a_2) b^{-1};\ a_1 b^{-1} : a_2 b^{-1} = a_1 a_2^{-1}.$$

Умножение на дробь ab^{-1} можно определить как деление на обратную дробь ba^{-1}.

Построение тела D, описанное здесь, допускает обобщения.

Прежде всего, можно в качестве исходной алгебры взять алгебру $\mathscr{A}_n$, порожденную n парами образующих $p_i,\ q_i$, с соотношениями

$$p_i q_j - q_j p_i = \delta_{ij},\ p_i p_j - p_j p_i = q_i q_j - q_j q_i = 0. \qquad (2)$$

Соответствующее тело отношешш обозначается D_n.

Более существенное обобщение получается следующим образом. Рассмотрим ассоциативную алгебру $\mathcal{A}$, порожденную образующими $x_1, x_2, \ldots, x_n$, которые удовлетворяют соотношениям специального вида

$$x_i x_j - x_j x_i = \sum_k c_{ij}^k x_k, \quad 1 \leqslant i, j \leqslant n, \tag{3}$$

где c_{ij}^k — некоторые константы.

Левая часть равенства (3) называется *коммутатором* элементов x_i и x_j и обозначается $[x_i, x_j]$.

Отметим, что в ассоциативной алгебре операция коммутирования удовлетворяет тождеству

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0,$$

которое называется *тождеством Якоби.*

Здесь уместно сообщить (или напомнить) читателю, что линейное пространство, снабженное билинейной кососимметричной операцией, удовлетворяющей тождеству Якоби, называется *алгеброй Ли.* Название это связано с группами Ли, о которых еще пойдет речь ниже.

Вернемся к нашей ассоциативной алгебре $\mathcal{A}$. Предположим, что образующие $x_1, x_2, \ldots, x_n$ линейно независимы. Тогда константы c_{ij}^k обладают свойством

$$\sum_s \left(c_{ij}^s c_{sk}^m + c_{jk}^s c_{si}^m + c_{ki}^s c_{sj}^m \right) = 0. \tag{5}$$

В этом случае линейное пространство g, натянутое на образующие $x_1, x_2, \ldots, x_n$, будет алгеброй Ли, а ассоциативная алгебра $\mathcal{A}$ - ее так называемой *универсалъной обертывающей алгеброй* или *ассоциативной оболочкой.* Обычно она обозначается $U(\mathfrak{g})$. Утверждения леммы и теоремы 1 остаются в силе для алгебры $U(\mathfrak{g})$. Тем самым они дают возможность определить тело отношений этой алгебры, которое называется *телом Ли* и обозначается $D(\mathfrak{g})$.

Изучение тел D_n и $D(\mathfrak{g})$ составляет один из интересных разделов направления в математике, которое можно назвать *некоммутативной алгебраической геометрией*.

В заключение этого раздела приведем здесь два простых с виду вопроса о структуре алгебры $\mathcal{A}$, ответ на которые до сих пор неизвестен.

1. Разрешимо ли в алгебре $\mathcal{A}$ *уравнение Ферма*

$$X^n + Y^n = Z^n? \tag{6}$$

(Имеются в виду нетривиальные решения, когда *X, Y* и *Z* не пропорциональны одному мпогочлену *P.)*

Известно, что в алгебре $\operatorname{gr} \mathcal{A} = \bigoplus_{n=0} L_n / L_{n-1} \cong \mathbf{C}[p, q]$

уравнение (6) не имеет нетривиальных решений при $n>2$. Существует пример нетривиального решения уравнения (6) при $n = 3$.

2. Пусть $P \in \mathcal{A}$ и $Q \in \mathcal{A}$ обладают свойством

$$PQ - QP = 1. \tag{7}$$

Тогда отображение $\varphi\colon p \mapsto P,\ q \mapsto Q$ задает эндоморфизм алгебры $\mathcal{A}$ в себя. Верно ли, что это — изоморфизм? (Другими словами, верно ли, что φ обратимо?)

«Коммутативный аналог» этого вопроса также не решен. Это так называемая *проблема детерминанта.* Ее точная формулировка такова.

Пусть $P(x, y)$ и $Q(x, y)$ — два многочлена со свойством

$$\begin{vmatrix} \partial P/\partial x & \partial Q/\partial x \\ \partial P/\partial y & \partial Q/\partial y \end{vmatrix} = 1.$$

Верно ли, что полиномиальное отображение $\varphi\colon (x, y) \mapsto (P, Q)$ допускает полиномиальное обратное отображение?

В этом же русле идей находится понятие *производной категории,* которое оказалось эффективным средством решения трудных конкретных задач из разных областей математики. Идея перехода к производной категории довольно проста и напоминает одновременно построение группы Гротендика и построение тела частных некоммутативной алгебры.

13.2. От Q к R: идея пополнения, *p*-адическне числа и адели

1. Вещественные числа получаются из рациональных с помощью процедуры *пополнения.* Эта процедура применима к любому *метрическому пространству,* т. е. множеству, в котором определены расстояния между точками.

Зададимся «крамольным» вопросом: а насколько естественно определено обычное расстояние между рациональными числами

$$d(r_1, r_2) = |r_1 - r_2|; \tag{1}$$

нет ли других способов описания «близости» между ними? Оказывается есть! Вот пример. Выберем простое число p. Как известно, любое рациональное число r однозначно записывается в виде $r = p^k \cdot \frac{m}{n}$, где $k \in \mathbf{Z}$, а $\frac{m}{n}$ — несократимая дробь, числитель и знаменатель которой взаимно просты с p. Величина p^{-k} называется *p-адической нормой* числа r и обозначается $\|r\|_p$. Можно проверить, что расстояние, определенное формулой

$$d_p(r_1, r_2) = \|r_1 - r_2\|_p, \tag{2}$$

обладает многими привычными нам свойствами обычного расстояния (1), например, оно удовлетворяет аксиоме треугольника:

$$d_p(r_1, r_2) + d_p(r_2, r_3) \geqslant d_p(r_1, r_3).$$

В то же время есть и отличия. Так, в смысле расстояния d_p все треугольники равнобедренны, причем длина основания не превосходит длины боковой стороны (проверьте!). Пространства с таким свойством называют *ультраметрическими.*

В ультраметрическом пространстве справедлив следующий простой признак сходимости: ряд $\sum x_n$ сходится тогда и только тогда, когда его общий член x_n стремится к нулю.

Еще одно отличие p-адического расстояния от обычного состоит в том, что целые числа образуют ограниченное множество диаметра 1. Если применить к этому множеству процедуру пополнения, мы получим компакт, который обозначается $\mathbf{O}_p$. Элементы $\mathbf{O}_p$ называются *целыми p-адическими числами.* Они допускают удобную запись в виде бесконечнозначных чисел в p-ичной системе счисления. А именно, целое p-адическое число a однозначно записывается в виде бесконечной влево последовательности

$$\ldots a_n \ldots a_2 a_1 a_0, \; 0 \leqslant a \leqslant p-1. \tag{3}$$

Эту запись можно понимать как сумму сходящегося ряда

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots \tag{4}$$

В самом деле, $\|a_n p^n\| \leqslant p^{-n}$, так что члены ряда (4) стремятся к нулю и согласно критерию из задачи 1 ряд сходится.

Целые p-адические числа образуют кольцо: их можно складывать, вычитать и перемножать. Однако в отличие от $\mathbf{Z}$ в $\mathbf{O}_p$ нет никакого естественного порядка. Понятия положительного и отрицательного числа в $\mathbf{O}_p$ не имеют смысла. Это видно, например, из того, что множество $\mathbf{N}$ натуральных чисел плотно в $\mathbf{O}_p$. (Проверьте, что $-1 = \lim (p^n - 1)$ при $n \to \infty$.)

Тем не менее для целых p-адических чисел можно определить аналог функции «сигнум», принимающий p различных значений.

Напомним, что обычный сигнум

$$\operatorname{sgn} x = \begin{cases} 1, & \text{если } x \geqslant 0, \\ 0, & \text{если } x = 0, \\ -1, & \text{если } x \leqslant 0, \end{cases}$$

можно на отрезке [—1, 1] приблизить функцией x^{ε}, где ε — малое рациональное число (с нечетным знаменателем, чтобы обеспечить вещественность x^{ε} при отрицательных x). В p-адической ситуации нужно вместо малого ε взять p^n с большим n.

Теорема. *Для любого* $a \in \mathbf{O}_p$ *существует предел* $\lim a^{p^n}$ *при* $n \to \infty$. *Он обозначается* $\operatorname{sgn}_p a$ *и обладает свойствами:*

a) $\operatorname{sgn}_p (ab) = \operatorname{sgn}_p a \cdot \operatorname{sgn}_p b$;

b) $\operatorname{sgn}_p a$ *зависит лишь от последней цифры* a_0 *числа* a *в записи* (3);

c) $\operatorname{sgn}_p a = 0$, *если* $a_0 = 0$, *и является корнем* (p — 1)-*й степени из* 1, *если* $a_0 \neq 0$.

Таким образом, на p-адической прямой можно двигаться в p — 1 различных направлениях. Для доказательства теоремы полезна

Лемма. *Если* $0 < d_p(a, b) < 1$, *то* $d_p(a^p, b^p) < d_p(a, b)$.

В отличие от обычных целых чисел многие целые p-адические числа обратимы. А именно, если $\operatorname{sgn}_p a \neq 0$, то a^{-1} — также целое p-адическое число. В частности, все рациональные числа со знаменателем, взаимно простым с p, являются целыми p-адическими числами.

Отметим, число вида (3) рационально тогда и только тогда, когда последовательность $\{a_n\}$ периодична, начиная с некоторого места.

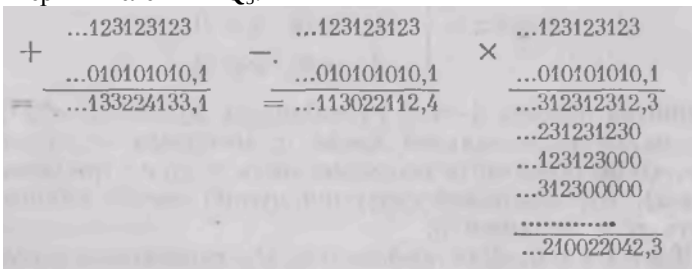
Если процедуру пополнения по расстоянию (2) применить не к **Z**, а к **Q**, то мы получим множество всех (не обязательно целых) p-адических чисел. Оно обозначается $\mathbf{Q}_p$. Его элементы удобно записывать в виде бесконечных влево p-ичных дробей:

$$a = \ldots a_n \ldots a_2 a_1 a_0, a_{-1} \ldots a_{-k}. \qquad (5)$$

Мы видим, что всякое p-адическое число имеет вид $a \cdot p^{-k}$, где $a \in \mathbf{Q}_p$.

Правила арифметических действий с p-адическими числами очень похожи на правила действий с обычными десятичными дробями, но с одним дополнительным принципом: все вычисления надо проводить, начиная с последней цифры.

Пример вычислений в $\mathbf{Q}_5$:



Фактически, здесь записаны некоторые соотношения между рациональными числами. Вот более сложный пример

$$\sqrt{-1} = \sqrt{\ldots 44444} = \operatorname{sgn} 2 = \lim_{n\to\infty} 2^{5^n} = \ldots 212.$$

2. В множестве $\mathbf{Q}_p$ *p*-адических чисел определены все операции алгебры и анализа — 4 арифметических действия и предельный переход. Это позволяет перенести на *p*-адический случай почти весь материал, изучаемый на младших курсах университетов. Некоторые теоремы при этом переносятся дословно, другие приходится корректировать, а третьи заменять совсем непохожими (и даже противоположными) утверждениями.

Например, естественным аналогом отрезка [0, 1], излюбленного объекта веществешюго анализа, служит множество $\mathbf{O}_p$. Этот «*p*-адический отрезок» так же, как и обычный, является шаром, т. е. множеством точек, удаленных от некоторой точки с (центра шара) на расстояние не более *r* (радиус шара) (однако, в отличие от обычного отрезка, роль центра в $\mathbf{O}_p$ играет любая его точка.) Кроме того, он является компактом и, следовательно, обладает всеми свойствами обычного отрезка, вытекающими из его компактности.

Отметим, что всякая непрерывная функция на $\mathbf{O}_p$ со значениями в $\mathbf{O}_p$, равномерно приближается многочленами с коэффициентами из $\mathbf{O}_p$.

Рассмотрим отображение $\varphi\colon\ \mathbf{O}_p \to \mathbf{R}$, которое переводит *p*-адическое число *a* вида (5) в вещественное число $\varphi(a) = \sum a_k p^{-k}$. (Таким образом, *p*-ичная запись числа $\varphi(a)$ получается из *p*-ичной записи числа *a* операцией «отражения относительно запятой».) Тогда можно доказать , что φ непрерывно, отображает $\mathbf{Q}_p$ на множество $\mathbf{R}_+$ неотрицательных вещественных чисел, а множество $\mathbf{O}_p$ — на отрезок [0, 1].

Может показаться, что отображение $\varphi\colon\ \mathbf{Q}_p \to \mathbf{R}_+$ взаимно однозначно и взаимно непрерывно. Однако это не так ввиду неоднозначности *p*-ичной записи вещественных чисел! Заметим также, что ограничение φ на $\mathbf{O}_p$ тесно связано с так называемой «канторовой лестницей».

Основные приложения *p*-адпческого анализа до сих пор относились к теории чисел. На этом языке удобно формулировать разные вопросы делимости и сравнений по целому модулю. Однако в последнее время все более многочисленны попытки использовать *p*-адическнй анализ в математической физике. Некоторые из этих попыток основаны лишь на принципе, что **любая математическая конструкция должна иметь физический смысл (причем чем проще и красивее конструкция, тем фундаментальнее ее физический смысл).** Другие, по существу, идут «от противного»: если обычного анализа недостаточно для современной физики, попробуем *p*-адический. Наконец, есть еще одно

важное соображение, для которого можно искать физическую интерпретацию. Оно состоит в том, что обычное вещественное поле **R** вместе с полями $\mathbf{Q}_p$ для всех простых чисел p можно объединить вместе в один красивый объект: **кольцо *аделей* А.**

Элементами А являются по определению последовательности вида

$$a = (a_\infty, a_2, a_3, a_5, \ldots, a_p, \ldots), \qquad (6)$$

где $a_\infty \in \mathbf{R}$, $a_p \in \mathbf{Q}_p$, причем для почти всех p (т. е. всех, за исключением конечного числа) $a_p \in \mathbf{O}_p$. Арифметические операции и предельный переход для аделей определяются покомпонентно. На адели переносится весь аппарат алгебры и анализа. При этом «адельные» теоремы связывают воедино вещественные и p-адические факты. Например, многие элементарные и специальные функции, встречающиеся в математике и в математической физике, имеют интересные p-адические и адельные аналоги. Рассмотрим здесь лишь о двух примерах таких аналогов.

3. Числа Тамагавы. Обратимые элементы кольца А называются *иделями.* Нормой иделя $a \in \mathbf{A}^*$ называется число

$$\|a\| = \prod_p \|a_p\|_p.$$

Это бесконечное произведение на самом деле сводится к конечному, так как почти все сомножители равны 1. Заметим теперь, что поле **Q** вкладывается в кольцо А: рациональному числу r соответствует адель $\underline{r} = (r, r, r, \ldots)$, где r на первом месте рассматривается как вещественное число, на втором — как 2-адическое, на третьем — как 3-адическое и т. д.

Адели вида $\underline{r}$, $r \in \mathbf{Q}$, называются *главными.* Ясно, что если $r \neq 0$, то главный адель $\underline{r}$ обратим. Более того, имеет место замечательное соотношение : адельная норма главного аделя $\underline{r}$ при $r \neq 0$ равна 1.

Пусть теперь M — гладкое алгебраическое многообразие, определенное над полем **Q** (т. е. задаваемое системой алгебраических уравнений с коэффициентами из **Q**). Тогда имеет смысл говорить о точках M над любым кольцом K, содержащим **Q.** Обозначим M_K множество точек M над K. Если K = **R**, то, как известно из курса анализа, по каждой дифференциальной форме старшей степени на M можио определить меру μ_K на M_K. При этом если форма умножается на рациональное число r, то мера $\mu_{\mathbf{R}}$ умножается на $|r|$.

Оказывается, эту конструкцию можно обобщить и на случай $K = \mathbf{Q}_p$ или A. При этом если форма умножается на *r*, то мера $\mu_{\mathbf{Q}_p}$ умножается на $\|r\|_p$, а мера— $\mu_{\mathbf{A}}$ на

$$\|r\| = 1.$$

Предположим теперь, что на *M* естественно выделяется класс форм старшей степени, определенных с точностью до рационального множителя. Например, если многообразие *M* однородно (т. е. на нем действует достаточно большая группа преобразований, способная перевести любую точку *M* в любую другую), то инвариантная рациональная дифференциальная форма старшей степени, если она существует, определяется однозначно с точностью до умножепия на рациональное число. Таким образом, соответствующая адельная инвариантная мера $\mu_{\mathbf{A}}$ определена однозначпо. Она называется *мерой Тамагавы.*

Важным примером описанной ситуации являются многообразия $M = G_{\mathbf{A}}/G_{\mathbf{Q}}$, где *G* — алгебраическая группа. Интеграл меры $\mu_{\mathbf{A}}$ по многообразию *M* в этом случае называется *числом Тамагавы* группы *G* и является характеристикой этой группы. Можно показать, что число Тамагавы $\tau(G)$ для широкого класса групп *G* равно произведению вещественного объема многообразия $G_{\mathbf{R}}/G_{\mathbf{Z}}$ и *p*-адическик объемов многообразий $G_{\mathbf{O}_p}$.

Обычно $\tau(G)$ оказывается очень простой константой, чаще всего единицей. Разберем для иллюстрации два простейших примера.

Пусть сначала *G* — аддитивная группа поля, так что $G_K = K$. Инвариантная форма равна *dx,* а соответствующая мера μ — это обычная мера Лебега $\mu_{\mathbf{R}}$ на **R**, или мера μ_p на $\mathbf{Q}_p$, принимающая значение *r* на шаре радиуса *r*, или мера $\mu_{\mathbf{A}}$ на A, которая является произведением меры $\mu_{\mathbf{R}}$ и всех мер μ_p. В этом случае все объемы, о которых говорилось выше, равны 1. В самом деле, $G_{\mathbf{R}}/G_{\mathbf{Z}}$ отождествляется с единичным отрезком, а $G_{\mathbf{O}_p}$ — с *p*-адическнм отрезком $\mathbf{O}_p$.

Теперь в качестве *G* возьмем окружность на плоскости, задаваемую уравнением $x^2+y^2=1$. Групповая операция определяется отождествлением точки *(x, y)* либо с комплексным числом $x + iy$, либо с матрицей

$$\begin{Vmatrix} x & y \\ -y & x \end{Vmatrix}.$$

Инвариантная форма имеет вид $dx/y = -dy/x$. Пространство $G_{\mathbf{R}}/G_{\mathbf{Z}}$ в этом случае потучается факторизацией вещественной окружности со стандартной мерой

$$\frac{dx}{\sqrt{1-x^2}}$$

по подгруппе $Ц_4$. Его объем равен $2\pi : 4 = \pi/2$.

Пространство $G_{\mathbf{O}_p}$ — «*p*-адическая окружность» — устроено по-разному в зависимости от вычета *p* mod 4.

Доказано, что *p*-адическая окружность состоит из:

a) четырех непересекающихся шаров радпуса 1/4, если $p = 2$;

b) p — 1 шаров радпуса p^{-1}, если $p \equiv 1 \bmod 4$;

c) $p + 1$ шаров радиуса p^{-1}, если $p \equiv -1 \bmod 4$.

Таким образом, число Тамагавы и в этом случае равно 1, так как

$$\prod_{p=4k+1} (1-p^{-1})^{-1} \cdot \prod_{p=4k-1} (1+p^{-1})^{-1} = \\ = 1 - 1/3 + 1/5 - 1/7 + \ldots = \pi/4.$$

(Первое равенство проверяется непосредственно с помощью тождества $(1-p^{-1})^{-1} = \sum_{k=0}^{\infty} p^{-k}$, а второе доказывается в курсе анализа.)

4. *p*-адическая ζ-функция. Классическая ζ-функция Римана определяется как сумма ряда

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \qquad (7)$$

который сходится при $\operatorname{Re} s > 1$. Мы увидпм сейчас, что эта функция может быть аналитически продолжена на всю комплексную плоскость и что ее значения в целых отрицательных точках имеют очень интересные арифметические свойства. Для этого нам понадобятся элементы комплексного анализа (понятие голоморфной функции и аналитического продолжения, теорема Коши о вычетах, свойства элементарных функций). Рассмотрим интеграл

$$I(s) = \int \frac{z^s}{e^z - 1} \cdot \frac{dz}{z}$$

по контуру C, показанному на рис. 1.

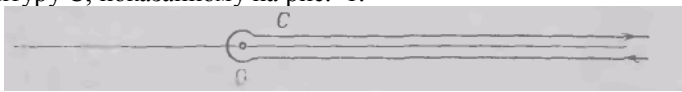


Рис. 1

Здесь под z^s понимается величина $\exp\,(s(\ln|z| + i\arg z))$, где $0 < \arg z < 2\pi$. Таким образом, подынтегральное выражение голоморфно по *s* и по *z* при всех s и при всех z, кроме точек луча [0, ∞]. Интеграл сходится при всех $s \in \mathbf{C}$ и определяет голоморфную функцию ***I***(s) на всей плоскости **C**.

Вычислим этот интеграл двумя способами. Во-первых, стягивая контур *C* к дважды проходимому лучу [0, ∞), мы получаем, что при Re s > 1 (при этом условии сходится интеграл в правой части)

$$I(s) = \left(1 - e^{2\pi i s}\right) \int_0^\infty \frac{x^s}{e^x - 1} \frac{dx}{x}.$$

Далее, так как

$$\frac{1}{e^x - 1} = \sum_{n=1}^{\infty} e^{-nx}$$

(формула суммы геометрической прогрессии) и

$$\int_0^\infty x^{s-1} e^{-nx} dx = n^{-s}\Gamma(s)$$

(заменой *y=nx* сводится к определению Г-фупкции), мы получаем

$$I(s) = (1 - e^{2\pi i s})\Gamma(s)\zeta(s) \quad \text{при } \operatorname{Re} s > 1. \tag{8}$$

Это равенство показывает, что $\zeta(s)$ голоморфно продолжается на всю комплексную плоскость, за исключением точки *s* = 1.

Во-вторых, при $\operatorname{Re} s < 0$ мы можем дополнить контур *C* контуром C_N (рис. 2), интеграл по которому стремится к 0 при $N \to \infty$, и вычислить полученный интеграл с помощью вычетов. Получим

$$I(s) = 2\pi i \sum_{n \neq 0} (2\pi i n)^{s-1}.$$

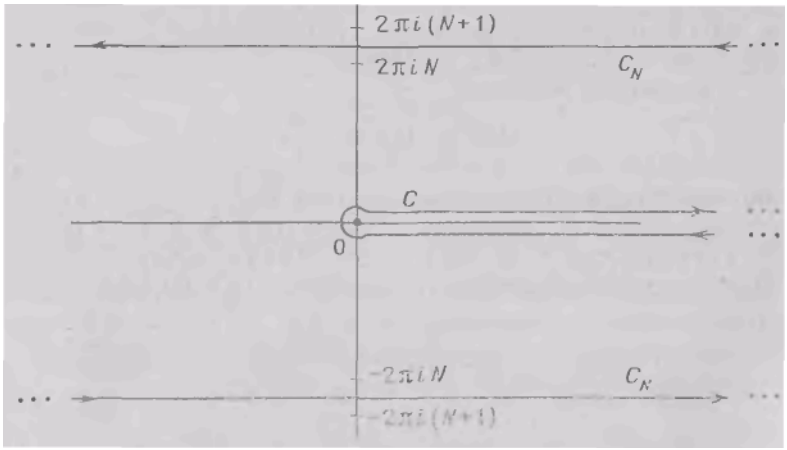


Рис. 2

Вспоминая определение z^s и $\zeta(s)$, имеем

$$I(s) = (2\pi)^s e^{\pi i s/2}(1 - e^{\pi i s})\zeta(1 - s) \text{ при } \operatorname{Re} s < 1. \quad (9)$$

Наконец, сравнивая (8) и (9), приходим к равенству

$$2\cos(\pi s/2)\Gamma(s)\zeta(s) = (2\pi)^s \zeta(1 - s),$$

откуда, в частности, при $s = 2k,\ k \in \mathbf{N}$ следует, что

$$\zeta(1 - 2k) = (-1)^k (2k - 1)! 2^{1-2k} \pi^{-2k} \zeta(2k). \quad (10)$$

Оказывается, правая часть в (10) — рациональное число! Чтобы убедиться в этом, нам понадобятся некоторые элементарные сведения о многочленах и числах Бернулли.

Рассмотрим функцию $f_k(x)$, задаваемую суммой ряда

$$f_k(x) = \sum_{n \neq 0} \frac{e^{2\pi i n x}}{(2\pi i n)^k}. \quad (11)$$

Этот ряд сходится в обычном смысле при $k \geq 2$ и его сумма является периодической функцией x с периодом 1. (При $k = 1$ ряд сходится условно, если x — не целое число.) Эта функция на интервале (0, 1) совпадает с некоторым многочленом степени k:

$$f_k(x) = -B_k(x)/k! \quad (12)$$

Многочлены $B_k(x)$ называются *многочленами Бернулли.*
Их можно определить условиями:

a) $B_0(x) \equiv 1$;
b) $B_h'(x) = kB_{h-1}(x)$;
c) $\int_0^1 B_k(x)\,dx = 0$ при $k \geqslant 1$

(Доказательство равенства (12) проще всего получить с помощью теории обобщенпых функций).

Величины $B_k(0)$ обозначаются просто B_k и называются *числами Бернулли.* Легко убедиться, что все они рациональны и что $B_{2k-1} = 0$ при $k > 1$. Из (11) и (12) вытекает, что

$$\zeta(2k) = (2\pi i)^{2k} f_{2k}(0) = -(2\pi i)^{2k} B_{2k}/(2k)!$$

п, следовательно, в силу (10)

$$\zeta(1-2k) = -B_{2k}/2k. \tag{13}$$

Имеет место

Теорема *(сравнения Куммера). Если p* — 1 *не делит k, то:*

a) $\|B_k\|_p \leqslant 1$;

b) при $k \equiv m \bmod (p-1)p^N$ справедливо сравнение

$$(1-p^h)B_h/k \equiv (1-p^m)B_m/m \bmod p^{N+1}. \tag{14}$$

Определим *p*-адическую ζ-функцию $\zeta_p(k)$ формулой

$$\zeta_p(k) = (1-p^{k-1})\zeta(1-k). \tag{15}$$

Из сравнений Куммера вытекает, что функция $\zeta_p(k)$ равномерно непрерывна на каждом множестве M_a вида $a + (p-1)\mathbf{N}$, $a = 1, 2, \ldots, p-2$. Поэтому она продолжается по непрерывности на пополнение M_a, совпадающее с $\mathbf{O}_p$. Кульминацией всей этой теории Куботы — Леопольдта является интегральное представление продолженной функции, которое является *p*-адическим аналогом формулы (8)

$$\zeta(k) = \int_{\mathbf{O}_p} x^{-k} d\mu(x),$$

где μ — некоторая мера на $\mathbf{O}_м$ сосредоточенная на множестве обратимых чисел.

Помимо теоретико-числовых и возможных физических приложений, наличие полей $\mathbf{Q}_p$ существенно расширяет построение методов математического моделирования. В принципе для любого определения, теоремы, формулы можно поставить вопрос: а какой у этого факта *p*-адическнй аналог? Нередко сама возможность постановки такого вопроса позволяет лучше понять исходную ситуацию. Стоит также отметить, что все больший интерес к *p*-адическому анализу проявляют специалисты по математическому моделированию.

13.3. От Q к R: идея порядка; нестандартный анализ

Есть еще один способ перейти от рациональных чисел к вещественным. Он не использует понятия расстояния, а опирается на естественный порядок в множестве **Q**. В этом подходе вещественное число *c* определяется как сечение в множество рациональных чисел, т. е. разбиение **Q** на два подмножества *A* и *B* так, что все числа $a \in A$ меньше всех чисел $b \in B.$ Если в *A* есть максимальныйэлемент $a_{\max}$ или в *B* есть минимальный элемент $b_{\min}$, то *c* отождествляется с одним из этих элементов (оба случая сразу осуществиться не могут, так как между $a_{\max}$, и $b_{\min}$ нашлись бы другие рациональные числа, которые не входили бы ни в *A,* ни в *B).* Если же ни $a_{\max}$, ни $b_{\min}$ не существуют, то *c* — новое число, не входящее в **Q**. Оно по определению считается большим, чем все числа нз *A,* и меньшим, чем все числа из *B.* Для введенных таким образом сечений можно определить все арифметические действия и получить поле, изоморфное **R**.

Однако здесь также есть повод для размышления. А именно, почему теперь нельзя пойти дальше и рассматривать сечения поля **R** как элементы еще большего поля? Формально этому мешает известная теорема о верхней грани, утверждающая, что для любого сечения $\mathbf{R} = A \cup B$ существует либо $a_{\max} \in A,$ либо $b_{\min} \in B.$

Но остается вопрос, нельзя ли все-таки вставить между *A* и *B* еще одно число *c*? Например, нельзя ли символ ε в анализе считать реально существующей бесконечно малой величиной, удовлетворяющей неравенству

$$0 < \varepsilon < 1/n \text{ для всех } n \in \mathbf{N}? \qquad (1)$$

Оказывается, это возможно, если отказаться от одной из аксиом, входящих в описание поля **R**. Речь идет об аксиоме Архимеда, утверждающей, что «как бы ни было мало положительное число ε и как бы пи было велико число *N*, складывая много раз величину ε саму с собой, мы получим число, превосходящее *N*».

Ясно, что неравенства (1) несовместимы с аксиомой Архимеда. Если же пожертвовать этой аксиомой, то можно построить много «неархимедовых» полей, содержащих **R**. До некоторого времени эти поля рассматривались как примеры, а соответствующий «нестандартный анализ» — как не имеющий существенных приложений в математике. Однако в 1966 году с помощью нестандартного анализа А. Робинсону и А. Р. Беристейну удалось решить трудную проблему функционального анализа — доказать

существование нетривиального инвариантного замкнутого подпространства для полиномиально компактного оператора в гильбертовом пространстве. Хотя вскоре это решение было переведено на обычный математический язык П. Халмошем (а более общий результат проще доказан В. И. Ломоносовым), уже нельзя отрицать плодотворность применения «нестандартного» подхода к классическим задачам. Появилось много популярных изложений этого подхода. Рассмотрим один оригинальный подход к построению неархимедова расширения поля **R**. Этот подход принадлежит англнйскому математику Дж. Конвею. Конвей называет построенные им числа сюрреальными (сверхвещественными), а мы будем их называть К-числами или *числами Конвея.*

Прежде всего — о записи чисел. В арифметике Конвея используются только два знака: $\uparrow$ и $\downarrow$ (по-английски — «up» и «down»). Вполне упорядоченный набор из этих знаков и есть К-число. Наборы могут быть любой мощности (чтобы избежать теоретико-множественных трудностей, нужно ограничить сверху мощность допустимых наборов. Уже счетные наборы включают в себя все обычные вещественные числа и много «нестандартных».) Например, пустой набор, как мы увидим ниже, играет роль нуля, и мы будем обозначать его 0.

На множестве всех К-чисел есть два отношения порядка. Одно задается обычным лексикографическим упорядочением. Для него используются термины «больше» и «меньше» и знаки > и <. Тот факт, что наборы вполне упорядочены, гарантирует сравнимость любых двух К-чисел.

Для другого отношения Конвей предлагает термины «раньше» и «позже». По определению более раннее число *a* получается из более позднего *b* «обрезанием хвоста», т. е. отбрасыванием всех знаков, начиная с некоторого места. Это записывается символом $a \prec\!\!\!\leftarrow b.$

При определении арифметических действий над К-числами используется.

Основная лемма. *Если A и B — два множества К-чисел, такие что все* $a \in A$ *меньше всех* $b \in B,$ *то существует единственное К-число c, обладающее свойствами:*

1) *c разделяет A и B (т. е. a <c <b для всех* $a \in A,$ $b \in B$);

2) *c —самое раннее из всех К-чисел, разделяющих A и B. В дальнейшем это число будет обозначаться (A : B).*

Конвей задает правила действия над К-числамп, руководствуясь двумя принципами: очередности и простоты. Согласно первому принципу правила действий определяются не сразу для всех К-чисел, а постепенно, начиная с более ранних. Согласно второму принципу

результат действия должен быть самым простым из возможных (т. е. самым ранним числом из тех, которые не противоречат ранее полученным результатам).

Пример. Найдем сумму 0 + 0. Поскольку 0 является самым ранним числом, никаких более ранних результатов у нас нет. Значит, ответ может быть любым К-числом; из всех возможностей мы должны выбрать самую раннюю, а это число 0. Значит, 0 + 0=0.

Конечно, этот пример любопытен, но читателю, привыкшему к строгим определениям анализа, он может показаться легкомысленным. Мы покажем сейчас, что можно строго определить сумму любых К-чисел, следуя принципам Копвея. Для этого введем некоторые обозначения.

Назовем *верхним срезом x* и обозначим $x\urcorner$ множество чисел, более ранних, чем x и больших x; аналогично определяется *нижний срез* $x\llcorner$.

Например, если $x = \uparrow\downarrow\uparrow\uparrow$, то

$$x\urcorner = \{\uparrow\}, \quad x\llcorner = \{\uparrow\downarrow\uparrow, \uparrow\downarrow, 0\},$$

а если $x = 0$, то $x\llcorner = x\urcorner = \varnothing$.

Определим теперь сумму двух К-чисел формулой

$$x + y = \{(x\llcorner + y) \cup (x + y\llcorner) : (x\urcorner + y) \cup (x + y\urcorner)\}. \quad (2)$$

Здесь $x\llcorner + y$ означает множество всех чисел вида $a+y$, где $a \in x\llcorner$; аналогичный смысл имеют выражения

$$x + y\llcorner, x\urcorner + y \text{ и } x + y\urcorner.$$

Формула (2) определяет $x + y$ при условии, что уже известны суммы всех более ранних слагаемых (принцип очередности), и делает это наиболее простым способом (см. основную лемму).

Утверждение 1. Пусть $\uparrow^n$ и $\downarrow^n$, $n \in \mathbb{N}$ означает К-число, записываемое n символами $\uparrow$ или $\downarrow$. Существуют равенства:

a) $\uparrow^m + \uparrow^n = \uparrow^{m+n}$;

b) $\downarrow^m + \downarrow^n = \downarrow^{m+n}$;

c) $$\uparrow^m + \downarrow^n = \begin{cases} \uparrow^{m-n} & \text{при } m > n, \\ 0 & \text{при } m = n, \\ \downarrow^{n-m} & \text{при } m < n. \end{cases}$$

Утверждение 1 показывает, что совокупность К-чисел содержит аддитивную подгруппу, изоморфную Z.

Существует равенство $\uparrow\downarrow + \uparrow\downarrow = \uparrow$.

Таким образом, К-число $\uparrow\downarrow$ играет роль «половинки» К-числа $\uparrow$. Аналогично можно установить, что $\uparrow\downarrow\downarrow$ — это «четвертинка», $\uparrow\downarrow\downarrow\downarrow$ — «восьмушка» и т. д.

После этих простейших примеров можно догадаться, что все конечные К-числа образуют аддитивную группу, изоморфную группе $\mathbf{Z}[1/2]$ двоично-рациональных чисел.

При этом запись двоично-рационального числа r в виде последовательности ↑ и ↓ есть не что иное, как «протокол поиска» этого числа в следующем смысле. Мы стартуем из точки 0 на вещественной оси (удобно считать ее расположенной вертикально, так чтобы числа возрастали снизу вверх) и двигаемся вверх или вниз шагами единичной длины. Каждый такой шаг отмечается в протоколе символом ↑ или ↓. Так продолжается до тех пор, пока мы не «перешагнем» r. После этого каждый новый шаг по длине делается вдвое короче предыдущего, а его направление по-прежнему отмечается в протоколе символом ↑ или ↓. Например, для числа $r = 2\frac{3}{16}$ процесс поиска равносилен записи $r = 3 - 1/2 - 1/4 - 1/8 + 1/16$ и дает К-число $\uparrow\uparrow\uparrow\downarrow\downarrow\downarrow\uparrow$.

Тот же принцип применим ко всем вещественным числам и приводит к их записи в виде бесконечных К-чисел.

Утверждение. Рациональные, но не двоично-рациональные числа соответствуют периодическим (начиная с некоторого места) К-числам.

Для записи периодических К-чнсел удобно использовать знак $\overset{\frown}{\ }$ для обозначения периода. Например, запись $\uparrow\uparrow\overset{\frown}{\downarrow}$ означает К-число $\uparrow\uparrow\downarrow\uparrow\downarrow\uparrow\downarrow\uparrow\downarrow\uparrow\downarrow\ldots$, что соответствует вещественному числу 5/3.

Все встреченные до сих пор К-числа можно было рассматривать как некоторый своеобразный способ записывать обычные вещественные числа. Этот способ хотя и отличается некоторой наглядностью, но менее удобен для вычислений по сравнению с обычной записью. Преимущества его выявляются при переходе к нестандартным числам, которые записываются не сложнее обычных.

Рассмотрим, например, К-числа $\omega = \overset{\frown}{\uparrow}$ и $\varepsilon = \uparrow\overset{\frown}{\downarrow}$.

Утверждение. Для любого $n \in \mathbf{N}$ справедливы неравенстка

$$\omega > n, \quad 0 < n\varepsilon < 1.$$

Таким образом, ω — «бесконечно большое», а ε — «бесконечно малое» число. Можно проверить, определив умножение положительных К-чисел формулой

$$x \cdot y = \{(x \cdot y\rfloor) \cup (x\rfloor \cdot y) : (x \cdot y\rceil) \cup (x\rceil \cdot y)\}, \tag{3}$$

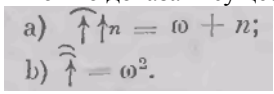
что произведение ω и ε равно ↑.

К сожалению, зга проверка довольно громоздка, так как в ходе ее придется вычислить произведение всех более ранних чисел. Однако это полезно для того, чтобы освоиться с К-числамн.

Вспомним, что в определении К-чисел говорилось о *вполне упорядоченном* множестве символов ↑ и ↓. Напомним, что упорядоченное множество называется вполне упорядоченным, если в любом его подмножестве есть минимальный элемент. Например, множество **N** с естественным порядком вполне упорядочено (принцип математической индукции), а множества **Q** и **R** — нет. Счетное множество может быть вполне упорядочении разными способами (возникает вопрос, а что это значит «разные способы»? Проще всего ответить так: упорядоченные множества образуют категорию (морфизмы — монотонные отображения), а в любой категории есть понятие эквивалентных объектов.) Более того, этих способов несчетное множество!

Отметим, что все до сих пор встречавшиеся нам К-числа соответствовали вполне упорядоченному множеству типа **N**. Вот пример другого типа: число $\overbrace{\uparrow\uparrow}$. Казалось бы, это то же самое, что и $\overbrace{\uparrow:}$ и там, и там — счетное множество символов ↑. Однако эти множества по-разному упорядочены: первое имеет максимальный элемент, а второе — пет.

Можно доказать существование равенств:



13.4. От R к C, H и O: алгебры Клиффорда, уравнение Дирака и проективная плоскость над полем из двух элементов

1. Комплексные числа играют в теории моделирования важную роль. Во-первых, это простейший пример *алгебраически замкнутого поля.* Это значит, что любой многочлен с комплексными коэффициентами от одного неизвестного имеет комплексный корень и, следовательно, разлагается на линейные множители (алгебраические замыкания других полей устроены более сложно. Например, алгебраическое замыкание $\mathbf{Q}_p$ не является полным относительно естественного продолжения *p*-адического расстояния. Его пополнение C_p описано в литературе. Это поле все чаще используется в алгебраической теории чисел, но его роль не сравнима с полем комплексных чисел. Сравнительно просто устроено алгебраическое замыкание конечного поля $\mathbf{F}_p$ из *p* элементов. Это объединение полей $\mathbf{F}_q$, $q=p^n$, $n \in \mathrm{N}$.

Однако в этом поле нет никакой естественной топологии, кроме дискретной.)

Во-вторых, комплексный анализ, т. е. теория комплексно-значных функций одной или нескольких комплексных переменных, это естественная область изучения аналитических функций. Многие «чисто вещественные» факты теории аналитических функций невозможно понять без рассмотрения их продолжения в комплексную область. Например, почему ряды для sin *x* и cos *x* сходятся для всех *x,* а ряд для $\operatorname{arctg} x$ — только для $|x| < 1$? Или почему неопределенный интеграл

$$\int (1 - x^2)^{\alpha} dx$$

вычисляется явно при $\alpha = 1/2,$ но не вычисляется при $\alpha = 1/3,\ 1/4$ и т. д.?

Наконец, переход от вещественных чисел к комплексным числам и кватернионам допускает обобщения, одно из которых — общая теория *алгебр Клиффорда.*

Изобретатель кватернионов знаменитый ирландский математик У. Гамильтон потратил много лет, пытаясь построить закон умножения трехмерных векторов по образцу умножения комплексных чисел, изображаемых двумерными векторами. Эти попытки, как мы теперь знаем, были обречены на неудачу. И только когда Гамильтон решился отбросить гипотезу о трехмерности новых чисел, ему удалось найти их реализацию. Она оказалась четырехмерной, и поэтому новые числа получили название *кватернионов.* Алгебра кватернионов **H** порождается как вещественное пространство обычной единицей 1 и тремя мнимыми единицами *i, j, k,* связанными соотношениями

$$i^2 = j^2 = k^2 = ijk = -1. \qquad (1)$$

Именно эти соотношения Гамильтон, говорят, вырезал на перилах моста, через который он переходил во время своих математических прогулок-размышлений.

Однако алгебраическое строение **H**, пожалуй, лучше отражает другая система соотношений, эквивалентная (1):

$$i^2 = j^2 = k^2 = -1, \quad ij + ji = jk + kj = ki + ik = 0. \qquad (2)$$

Эта система в свою очередь эквивалентна тождеству

$$(ai + bj + ck)^2 = -(a^2 + b^2 + c^2) \text{ для всех } a,\ b,\ c \in \mathbf{R}. \qquad (3)$$

Гамильтон выделял в кватернионе $q = x_0 + x_1 i + x_2 j + x_3 k$ *скалярную* часть $x_0 \in \mathbf{R}$ и *векторную* часть $\mathbf{x} = (x_1,\ x_2,\ x_3) \in \mathbf{R}^3.$

Произведение двух векторных кватернионов распадалось при этом на два слагаемых: *скалярное произведение*

$$(\mathbf{x}, \mathbf{y}) = x_1y_1 + x_2y_2 + x_3y_3$$

и *векторное произведение*

$$\mathbf{x} \times \mathbf{y} = \det \begin{Vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ i & j & k \end{Vmatrix}.$$

Эти операции нашли применения далеко за пределами теории кватернионов. Скалярное произведение вошло в структуру евклидовых и гильбертовых пространств, а векторное произведение явилось первым примером *операции коммутирования в алгебре Ли*.

2. Тождество (3) подсказывает общее определение *алгебры Клиффорда* $\mathrm{Cl}\ (V, Q)$, связанной с линейным пространством V над полем K и квадратичной формой Q в этом пространстве. По определению, $\mathrm{Cl}\ (V, Q)$ — алгебра над K, порожденная единицей 1 и пространством V с соотношениями

$$v^2 = Q(v) \cdot 1 \quad \text{для всех } v \in V. \tag{4}$$

Отметим, что алгебры **C** и **H** являются алгебрами Клиффорда соответственно для $V = \mathbf{R}$, $Q(x) = -x^2$ и $V = \mathbf{R}^2$, $Q(x, y) = -x^2 - y^2$.

Можно показать, что комплексная алгебра Клиффорда, соответствующая пространству $\mathbf{C}^n$ и невырожденной квадратичной форме Q, изоморфна при $n=2k$ алгебре матриц порядка 2^k с комплексными коэффициентами, а прн $n = 2k+1$ — прямой сумме двух таких алгебр.

Вещественные алгебры Клиффорда более разнообразны. Приведем таблицу алгебр $C_{p,q} = \mathrm{Cl}(\mathbf{R}^{p+q}, Q_{p,q})$, где $Q_{p,q}$ — квадратичная форма вида

$$Q_{p,q}(x_1, \ldots, x_{p+q}) = \sum_{i=1}^{p} x_i^2 - \sum_{j=p+1}^{p+q} x_j^2:$$

q/p	0	1	2	3	4	5	6	7
0	R	2R	R(2)	C(2)	H(2)	2H(2)	H(4)	C(8)
1	C	R(2)	2R(2)	R(4)	C(4)	H(4)	2H(4)	H(8)
2	H	C(2)	R(4)	2R(4)	R(8)	C(8)	H(8)	2H(8)
3	2H	H(2)	C(4)	R(8)	2R(8)	R(16)	C(16)	H(16)
4	H(2)	2H(2)	H(4)	C(8)	R(16)	2R(16)	R(32)	C(32)
5	C(4)	H(4)	2H(4)	H(8)	C(16)	R(32)	2R(32)	R(64)
6	R(8)	C(8)	H(8)	2H(8)	H(16)	C(32)	R(64)	2R(64)
7	2R(8)	R(16)	C(16)	H(16)	2H(16)	H(32)	C(64)	R(128)
8	R(16)	2R(16)	R(32)	C(32)	H(32)	2H(32)	H(64)	C(128)

Здесь для краткости алгебра матриц порядка n над полем или телом K обозначена символом $K(n)$, а прямая сумма двух таких алгебр — символом $2K(n)$.

До сих пор мы рассматривали лишь алгебры Клиффорда, связанные с невырожденными квадратичными формами. Представляет интерес и другой крайний случай — нулевой формы Q. Соответствующая алгебра — это так называемая *внешняя* или *грассманова* алгебра, о которой пойдет речь далее.

3. Одна из алгебр Клиффорда была использована замечательным английским физиком Дираком в квантовой теории электромагнетизма. Пытаясь заменить волновое уравнение

$$\Box f := (\partial^2/\partial t^2 - \partial^2/\partial x^2 - \partial^2/\partial y^2 - \partial^2/\partial z^2)f = 0 \qquad (5)$$

эквивалентным ему уравнением первого порядка по времени (именно такими уравнениями описываются квантовые системы), Дирак предположил, что оператор (5) можно записать в виде квадрата оператора первого порядка:

$$\Box = (\gamma_0\partial/\partial t + \gamma_1\partial/\partial x + \gamma_2\partial/\partial y + \gamma_3\partial/\partial z)^2. \qquad (6)$$

(Знак $=:$ или $:=$ показывает, что равенство является определением той части, к которой направлено двоеточие. В нашем случае — определением символа $\Box f(a_1, a_2, \ldots, a_n)$.

Коэффициенты γ_i в этом равенстве не могут быть обычными числами. Они являются образующими алгебры Клиффорда $C_{1,3}$ (см. выше п. 2) или ее комплексной оболочки.

Уравнение Дирака, описывающее элементарные частицы фермионного типа (электроны, мюоны, нейтрино), имеет вид

$$(\gamma_0\partial/\partial t + \gamma_1\partial/\partial x + \gamma_2\partial/\partial y + \gamma_3\partial/\partial z)\upsilon = \mu\upsilon. \qquad (7)$$

Обычно в физической интерпретации предполагается, что γ_i — комплексные матрицы четвертого порядка, а υ — комплексный 4-вектор (так называемый *дираковский спинор).*

4. Среди вещественных алгебр Клиффорда лишь три являются телами: **R, C** и **H**. Теорема Фробенпуса утверждает, что других ассоциативных алгебр, с делением над **R** нет. Однако если отказаться от ассоциативности, то можно построить пример алгебры с делением размерности-8 над **R.**

Это алгебра **O** так называемых *чисел Кэли,* или октав, или октонионов. Как линейное пространство над К, эта алгебра порождена обычной единицей 1 и семью мнимыми единицами $e_1, \ldots, e_7$ с соотношениями

$$e_i^2 = -1, \quad 1 \leqslant i \leqslant 7; \quad e_i e_j = \pm e_{k(i,j)}. \qquad (8)$$

Таким образом, произведение двух базисных единиц с точностью до знака снова является базисной единицей. Выбор знаков и значений *k(i, j)* изображаются таблицей (рис. 3).

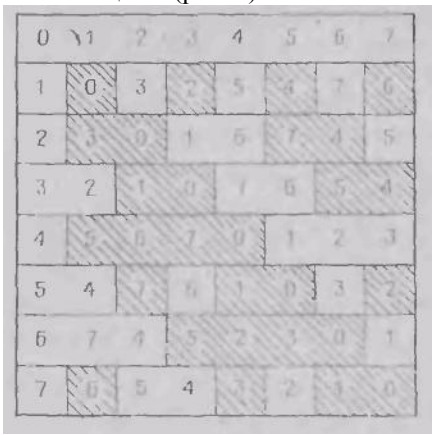


Рис. 3

Эта таблица обладает свойствами симметрии (позволяющими ее почти однозначно восстановить по первой строке и первому столбцу):

1) В каждой строке и в каждом столбце встречаются по одному разу все цифры 0, 1,2, 3, 4, 5, 6, 7.

2) В каждой строке и в каждом столбце, кроме первых, половина чисел заштрихована, половина — не заштрихована.

3) В каждом фрагменте вида

$$\begin{matrix} a & b \\ b & a \end{matrix}$$

количество заштрихованных и незаштрихованных чисел нечетно (т. е. заштрихованные числа встречаются три раза, незаштриховашше один или наоборот).

Геометрическую интерпретацию этой таблицы мы обсудим ниже, а пока приведем еще одну реализацию алгебры **O**. В ней элемент **O** изображается парой кватернионов, сложение покомпонентно, а умножение задается формулой

$$(q_1,\ r_1)(q_2,\ r_2) = (q_1q_2 - \bar{r}_2r_1,\ r_2q_1 + r_1\bar{q}_2). \qquad (9)$$

Здесь черта означает кватернионное сопряжение: если

$$q = (x_0,\ \mathbf{x}),\ \text{то}\ \bar{q} = (x_0,\ -\mathbf{x}).$$

Распределение знаков и индексов в формуле (8) связано с геометрической конфигурацией — проективной плоскостью над полем $\mathbf{F}_2$ из двух элементов. Напомним, что проективная плоскость над полем

K — это совокупность $P^2(K)$ всех прямых (= одномерных подпространств) в трехмерном пространстве над *K*. Обычно точку $x \in P^2(K)$ задают набором трех однородных координат $(x_0 : x_1 : x_2)$, определенных с точностью до умножения на элемент из $K^* = K \setminus \{0\}$. В нашем случае *K** состоит из одной единицы, так что $P^2(\mathbf{F}_2)$ отождествляется с $\mathbf{F}_2^3 \setminus \{0\}$ и, стало быть, состоит из семи точек.

Прямой на $P^2(\mathbf{F}_2)$ называется совокупность α точек *x,* однородные координаты которых удовлетворяют линейному соотношению

$$a_1x_1 + a_2x_2 + a_3x_3 = 0.$$

Коэффициенты a_1, a_2, a_3 в этой формуле можно считать координатами точки *a* из другой проективной плоскости, дуальной к исходной. Итак, мы имеем 7 точек и 7 прямых. Взаимное расположение их можно изобразить схемой (рис. 4).

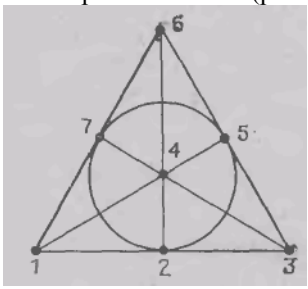


Рис. 4

Таблица умножения в алгебре **O** связана со схемой рис. 4 таким образом: точки (i), (j) и $(k(i, j))$ лежат на одной прямой в $P^2(\mathbf{F}_2)$, а знак ± определяется взаимным расположением этих точек. А именно, назовем *ориентацией* прямой *l* циклический порядок ее точек (т. е. порядок с точностью до циклической перестановки). Будем изображать этот порядок стрелкой на отрезке или окружности, изображающей эту прямую. Зададим ориентацию как на рис. 5.

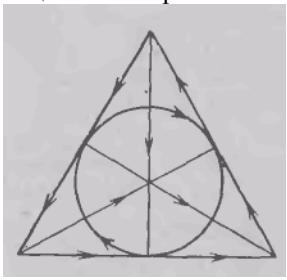


Рис. 5

Правило знаков формулируется так: $e_i e_j = +e_{k(i,j)}$ тогда и только тогда, когда точки (i), (j) и $(k(i, j))$ определяют ориентацию соответствующей прямой.

В заключение предлагаем следующую тему для размышления. На проективной плоскости лежат проективные пространства меньшей размерности: прямые и точки. Заметим, что подалгебра в **O**, порожденная мнимыми единицами, соответствующими точками некоторой прямой $l \subset P^2(\mathbf{F}_2)$, изоморфна **H**, а подалгебра, порожденная одной мнимой единицей, изоморфна **C**. Следует выяснить, какие алгебры соответствуют проективным пространствам более высоких размерностей.

Введем обозначение

$$\binom{n}{k}_q = \frac{(q^n-1)(q^{n-1}-1)\ldots(q-1)}{(q^k-1)\ldots(q-1)\cdot(q^{n-k}-1)\ldots(q-1)}.$$

Эта величина является так называемым *q-аналогом* биномиального коэффициента C_n^k (и превращается в него при $q \to 1$).

Можно доказать, что число *k*-мерных пространств в $p^n(\mathbf{F}_q)$ равно $\binom{n}{k}_q$.

14. Другие варианты чисел

Роль чисел могут играть не только элементы поля или тела. В этом разделе речь пойдет о других математических объектах, также выступающих в роли чисел. Все они возникли сначала в «чистой» математике, а потом были использованы как заменители чисел в математической физике.

14.1. Матрицы в роли чисел

1. Обобщением понятия числа являются матрицы. Мы будем обозначать $\mathrm{Mat}_n(K)$ множество квадратных матриц размера $n \times n$ с элементами из поля K. Элементы матрицы A обозначаются A_{ij} (или a_{ij}), где i — номер строки, а j — номер столбца, в котором стоит элемент. Как известно, $\mathrm{Mat}_n(K)$ — алгебра над полем K: сложение, вычитание и умножение на число производятся поэлементно:

$$(A \pm B)_{ij} = A_{ij} \pm B_{ij}, \quad (\lambda \cdot A)_{ij} = \lambda \cdot A_{ij},$$

а произведение двух матриц задается формулой

$$(AB)_{ij} = \sum_{k=0}^{n} A_{ik} B_{kj}. \qquad (1)$$

Формула (1) задает гораздо более важную алгебру, чем прямое произведение n^2 экземпляров поля K. Дело в том, что правило (1) вытекает из геометрической интерпретации матрицы $A \in \mathrm{Mat}_n(K)$ как линейного преобразования n-мерного пространства V над полем K.

(Отметим, что это не единственный способ придать матрицам геометрический смысл. Можно, например, рассматривать матрицу $A \in \mathrm{Mat}_n(K)$ как билинейную форму на V (т. е. отображение $V \times V$ в K, линейное по обоим аргументам). При замене базиса в V матрица A преобразуется по-разному, в зависимости от того, какой ей придается смысл. Матрица линейного оператора меняется по правилу $A \mapsto Q^{-1}AQ$, а матрица билинейной формы — по правилу $A \mapsto Q'AQ$, где Q — матрица замены базиса, Q^{-1} — обратная, а Q' — транспонированная матрица (т. е. $Q'_{ij} = Q_{ji}$). У нас матрица всегда будет отождествляться с линейным оператором.)

В самом деле, если $\{v_i\}$ — координаты вектора $\mathbf{v} \in V$, то матрица A задает преобразование $\mathbf{v} \mapsto A\mathbf{v}$, где

$$(A\mathbf{v})_i = \sum_j A_{ij} v_j, \qquad (2)$$

и непосредственное вычисление показывает, что произведению (т. е. последовательному выполнению) преобразований (2) соответствует произведение матриц по формуле (1).

Итак, матрицы, подобно числам, можно складывать, вычитать и умножать. Что касается деления, то здесь положение более сложное, чем для чисел. Известно, что деление на матрицу A возможно и однозначно лишь в том случае, если она не вырождена, т. е. ее определитель $\det A$ не равен нулю.

Главное же отличие матриц от обычных чисел состоит в том, что операция умножения некоммутативна: AB, как правило, не равно BA. По этой причине использование матриц в роли чисел стало популярным лишь сравнительно недавно, после того как к этому пришли физики в процессе построения квантовой теории.

Сейчас мы поговорим о другом важном свойстве чисел. А именно, числа можно подставлять в функции в качестве аргумента. Посмотрим, насколько матрицы способны выполнять эту роль чисел.

2. Простейшие функции — это многочлены. Пусть

$$P(x) = \sum_{k=0}^{n} c_k x^k$$

— многочлен с вещественными коэффициентами. Ясно, как придать смысл выражению *P(A),* где $A \in \mathrm{Mat}_n(\mathbf{R})$. Надо положить

$$P(A) = \sum_{k=0}^{n} c_k A^k,$$

где A^0 по определению равно единичной матрице, которую мы будем обозначать просто 1 (или 1_n, если важно указать размер матрицы).

Одна из самых старых задач математики — отыскание корней мпогочленов, т. е. решение уравнений вида *P(x)* = 0. С течением времени выяснилось, что не менее интересна **обратная задача**: **описать те многочлены, для которых данное число является корнем**. Ответ дается известной теоремой Безу: искомое множество многочленов является идеалом в алгебре $\mathscr{P}$, порожденным $x - a$.

Посмотрим, какие условия на многочлен $P \in \mathscr{P}$ налагает равенство

$$P(A) = 0. \tag{4}$$

Ответ довольно прост, если матрица A диагональна:

$$A = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix} =: \mathrm{diag}\,(a_1, a_2, \dots, a_n).$$

В этом случае $P(A) = \mathrm{diag}\,(P(a_1),\ P(a_2),\ \dots,\ P(a_n))$. Поэтому равенство (4) равносильно системе уравнений

$$P(a_i) = 0, \quad 1 \leqslant i \leqslant n. \tag{5}$$

Таким образом, одна матрица A заменяет собой целый набор чисел $\{a_1,\ a_2,\ \dots,\ a_n\}$.

Пусть теперь матрица A не диагональна, но приводится к диагональпому виду: $A = Q^{-1}\Lambda Q$, где $\Lambda = \mathrm{diag}\,(\lambda_1,\ \lambda_2,\ \dots,\ \lambda_n)$. Легко проверить (но еще важнее понять), что справедливо тождество

$$P(Q^{-1}AQ) = Q^{-1}P(A)Q. \tag{6}$$

Поэтому условие (4) равносильно системе уравнений $P(\lambda_i) = 0,\ 1 \leqslant i \leqslant n.$ Опять мы видим, что матрица A заменяет набор из n чисел. Из курса линейной алгебры мы знаем, что эти числа суть *собственные значения* матрицы A (т. е. корни *характеристического уравнения* $\det(A - \lambda \cdot 1) = 0$), а их совокупность составляет *спектр* матрицы A. Если все собственные значения A различны, то говорят, что A имеет *простой спектр.* Известно, что если $A \in \mathrm{Mat}_n(K)$ имеет простой спектр, содержащийся в K, то A приводится к диагональному виду. Из всего сказанного вытекает

Теорема 1. *Для того чтобы многочлен* $P \in K[x]$ *обращался в нуль на матрице A с простым спектром, содержащимся в K, необходимо и достаточно, чтобы он обращался в нуль на спектре A.*

Доказано, что теорема 1 верна и в том случае, когда спектр A не содержится в K.

Утверждение теоремы 1 является одним из проявлений общего принципа: *матричные элементы составляют лишь бренное тело преобразования A, в то время как спектр выражает его бессмертную душу.*

С другими проявлениями этого принципа мы встретимся ниже, а пока предлагается следующая тема для размышления.

3. Рассмотрим теперь для $A \in \mathrm{Mat}_n(K)$ совокупность $K[A]$ всех матриц вида $P(A)$, $P \in K[x]$. Ясно, что $K[A]$ — подалгебра в $\mathrm{Mat}_n(K)$, порожденная A, как алгебра с единицей. С другой стороны, $K[A]$ — фактор-алгебра $K[x]$ по идеалу $\boldsymbol{I}(A)$, задаваемому условием (4).

Теорема 2. *Если A — матрица с простым спектром, лежащим в K, то алгебра* $K[A]$ *изоморфна алгебре всех функций на спектре A со значениями в K.*

В самом деле, из (6) следует, что искомый изоморфизм можно задать соответствием

$$K[A] \ni P(A) \mapsto (P(\lambda_1),\ P(\lambda_2),\ \ldots,\ P(\lambda_n)) \in K^n.$$

Более существенная ситуация возникает, когда спектр матрицы A не прост или не содержится в K.

Модельный пример матрицы с непростым спектром — это «жорданова клетка»:

$$J_n(\lambda) := \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & \lambda \end{pmatrix}$$

Доказано, что для $A = J_n(\lambda)$ *идеал* $\boldsymbol{I}(A)$ *состоит из тех многочленов P, для которых*

$$P(\lambda) = P'(\lambda) = \ldots = P^{(n-1)}(\lambda) = 0. \tag{7}$$

Как известно (и легко проверить), спектр $J_n(\lambda)$ состоит из одной точки λ. Это значит, что аналоги теорем 1 и 2 для этой матрицы неверны. Однако с интуитивной точки зрения удобно считать, что эти теоремы верны всегда, если только правильно понимать, что такое спектр матрицы и какие функции на спектре нужно рассматривать. Например, будем считать, что спектр $J_n(\lambda)$ состоит не из одной точки

λ, а включает и ее *бесконечно малую окрестность порядка n* — 1, которую мы обозначим $U_{n-1}(\lambda)$.

Теорема 2 подсказывает, что нужно называть ограничением многочлена *P* на $U_{n-1}(\lambda)$: надо разложить *P* по степеням *x* — λ и оборвать это разложение на члене *(n* — 1)-й степени. Равенства (7) будут тогда условием того, что многочлен *P* обращается в нуль на $U_{n-1}(\lambda)$. В случае *K* = **R** эта конструкция хорошо известна в анализе и применима к любым гладким функциям, определенным в (обычной) окрестности точки λ. А именно, *n-струей функции f в точке* λ называется выражение

$$\sum_{k=0}^{n} f^{(k)}(\lambda) \cdot \frac{(x-\lambda)^k}{k!},$$

которое мы и предлагаем считать ограничением функции *f* на $U_n(\lambda)$. Разумеется, $U_n(\lambda)$ нельзя рассматривать как обычную окрестность. Например, многочлен $(x-\lambda)^{n+1}$ обращается в нуль на этой окрестности, но не имеет других «обычных» нулей, кроме $x = \lambda$.

Разберем теперь ситуацию, когда спектр *A* не содержится в *K*. Так будет, если характеристический многочлен этой матрицы *A*

$$\chi_A(\lambda) = \det(A - \lambda \cdot 1) \tag{8}$$

не разлагается на линейные множители. Пусть, например, χ_A непрпводим, т. е. вообще не разлагается на множители меньшей степени в $K[\lambda]$. В этом случае идеал ***I(A)*** прост и порождается элементом χ_A. Поэтому алгебра $K[A]$ не имеет делителей нуля и, следовательно, является полем, содержащим *K*. Обозначим это поле $\tilde{K}$. Его размерность над *K* равна *n,* так как, с одной стороны, элементы $1, A, A^2, \ldots, A^{n-1}$ независимы над *K* (в ***I(A)*** нет элементов степени меньше *n*), а с другой стороны, в силу *тождества Кэли*

$$\chi_A(A) = 0 \tag{9}$$

каждый элемент алгебры $\tilde{K}$ записывается в виде

$$a_0 \cdot 1 + a_1 \cdot A + \ldots + a_{n-1} \cdot A^{n-1}, \tag{10}$$

где $a_i \in K$. Таким образом, алгебра $K[A]$ и в этом случае конечномерна над *K*. Чтобы теорема 2 была справедлива, можно поступить двояко.

Во-первых, можно считать, что спектр *A* состоит из одной точки, не принадлежащей *K,* алгебра $K[A]$ состоит из всех функций на спектре со значениями в *K*.

Во-вторых, можно считать, что спектр *A* состоит из всех собственных значений *A,* лежащих в $\tilde{K}$, а алгебра $K[A]$ состоит из $\tilde{K}$-значных функций на спектре, обладающих свойством

$$f(\gamma(\lambda)) = \gamma(f(\lambda)),$$

где γ пробегает *группу Галуа* $\mathrm{Gal}\,(\tilde{K}/K)$ поля $\tilde{K}$ над K (т. е. совокупность автоморфизмов поля $\tilde{K}$, оставляющих на месте каждый элемепт из K).

Пример 1. Если $K = \mathbf{R},\ A = \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}$, то $I(A)$ порождается неприводимым над **R** многочленом $x^2 + 1$, а поле K изоморфно **C**. Мы получили хорошо известную реализацию поля **C** вещественными матрицами вида

$$a_0 \cdot 1 + a_1 \cdot A = \begin{Vmatrix} a_0 & a_1 \\ -a_1 & a_0 \end{Vmatrix}.$$

Пример 2. Если $K = \mathbf{F}_2,\quad A = \begin{Vmatrix} 0 & 1 \\ 1 & 1 \end{Vmatrix}$, то $I(A)$ порождается неприводимым над $\mathbf{F}_2$ многочленом $x^2 + x + 1$, а поле K изоморфно $\mathbf{F}_4$. Таким образом, мы получаем простейшую реализацию поля $\mathbf{F}_4$ с помощью четырех матриц второго порядка с элементами из $\mathbf{F}_2$:

$$0 = \begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix},\quad 1 = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix},\quad x = \begin{Vmatrix} 0 & 1 \\ 1 & 1 \end{Vmatrix},\quad x + 1 = \begin{Vmatrix} 1 & 1 \\ 1 & 0 \end{Vmatrix}.$$

4. Мы разобрались более или менее с полиномиальными функциями матриц. Посмотрим, можно ли определить более общие функции матричного аргумента? Для этого вспомним, что в анализе помимо арифметических действий есть еще операция предельного перехода. Как известно, многие функции в том или ином смысле приближаются многочленами. Так, аналитическая функция на прямой приближается частичными суммами своего ряда Тейлора, любая непрерывная функция на отрезке равномерно приближаестя многочленами, а непрерывная функция на окружности $x^2 + y^2 = 1$ — многочленами от x и y (или, что то же, тригонометрическими многочленами от $\alpha = \mathrm{arctg}\,\frac{y}{x}$).

Выберем теперь класс функций F, приближаемых многочленами в каком-нибудь смысле и попробуем определить $f(A)$ для $f \in F$ следующим образом. Пусть $\{P_n\}$ — последовательность многочленов, сходящаяся к f. Если последовательность матриц $\{P_n(A)\}$ имеет предел, то этот предел мы и примем за значение $f(A)$. Чтобы это определение было корректным (т. е. не зависело от выбора приближающей последовательности $\{P_n\}$), нужно, чтобы для любой последовательности многочленов P_n, стремящейся к нулю в выбранном нами смысле, последовательность матриц $P_n(A)$ также стремилась к нулю. Разумеется, это зависит и от матрицы A, и от понятия предельного перехода.

Пример 3. Назовем последовательность многочленов сходящейся, если она сходится в каждой точке некоторого конечного множества $M \subset \mathbf{R}$. Из сказанного в п. 3 следует, что выражение $f(A)$ имеет смысл для любой функции f на M и для любой матрицы A с простым спектром, содержащимся в M. При этом если $A = Q^{-1}\Lambda Q$, $\Lambda = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$, то $f(A) = Q^{-1} \operatorname{diag}(f(\lambda_1), (f(\lambda_1), \ldots, f(\lambda_n))Q$.

Пример 4. Назовем последовательность многочленов сходящейся, если сами многочлены и все их производные до порядка n имеют предел в каждой точке множества $M \subset \mathbf{C}$. Тогда выражение $f(A)$ имеет смысл для любой гладкой функции f на M и для любой матрицы A порядка $\leq n + 1$, спектр которой лежит в M.

Пример 5. Функция $f(x) = \frac{1}{1+x^2}$ может быть приближена многочленами на любом отрезке вещественной оси равномерно вместе с любым числом производных.

Однако для матрицы

$$A = \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}$$

выражение $f(A)$ не определено, так как $1+ A^2 = 0$.

Эти примеры показывают, что понятие функции от матрицы довольно деликатно и требует осторожного обращения. В то же время есть класс матриц A, для которых выражение $f(A)$ имеет смысл практически для всех функций f на R. Это класс *эрмитовых матриц,* т. е. таких $A \in \operatorname{Mat}_n(\mathbf{C})$, для которых $A = A^*$. (Напомним, что символ * означает эрмитово сопряжение: $(A^*)_{ij} = A_{ij}$.) В частности, эрмитовыми являются все вещественные симметрические матрицы.

Пусть последовательность многочленов $\{P_n\}$ стремится к нулю в каждой точке вещественной оси. Доказано, что $P_n(A) \to 0$ для любой эрмитовой матрицы A.

5. Описанное выше свойство функций от эрмитовых матриц переносится на матрицы бесконечного порядка. Этот факт играет первостепенную роль в построении математической модели квантовой механики, поскольку физические величины в этой модели изображаются эрмитовыми матрицами бесконечного порядка.

Нужно, однако, уточнить, что мы называем матрицами бесконечного порядка и как определяются действия над ними. Поскольку матрица для нас — это форма записи линейного оператора над векторами, то сначала надо выяснить, что такое бесконечномерный вектор. По аналогии с конечномерным случаем можно было бы назвать бесконечномерным вещественным (соответственно комплексным)

вектором любую бесконечную последовательность $\mathbf{x} = (x_1, x_2, \ldots, x_n, \ldots)$, где x_j — вещественные (соответственно комплексные) числа. Такие векторы действительно образуют бесконечномерное линейное пространство. Однако если мы хотим сохранить и в бесконечномерной ситуации такие геометрические понятия, как длина, перпендикулярность, скалярное произведение векторов, то придется ограничить класс рассматриваемых последовательностей. А именно, назовем *допустимой* последовательность $\mathbf{x} = \{x_i\}$, если конечна сумма ряда $\sum_{i=1}^{\infty} |x_i|^2$.

Основные свойства допустимых последовательностей изложены ниже

Доказано, что

a) Для любых допустимых $\mathbf{x} = \{x_i\}$ и $\mathbf{y} = \{y_i\}$ сходится ряд $\sum_{i=1}^{\infty} x_i \bar{y}_i$.

b) Допустимые последовательности образуют линейное пространство относительно покомпонентного сложения и умножения на число.

c) Справедливо *неравенство Коши — Буняковского — Шварца*

$$|(\mathbf{x}, \mathbf{y})| \leqslant |\mathbf{x}| \cdot |\mathbf{y}|, \tag{11}$$

где символом $(\mathbf{x}, \mathbf{y})$ обозначено *скалярное произведение* **x** и **y,** задаваемое рядом из a), а символом $|\mathbf{x}|$ — *длина* вектора **x**, равная $(\mathbf{x}, \mathbf{x})^{1/2}$.

Пространство всех допустимых последовательностей обычно обозначается *H* и называется *гильбертовым пространством* в честь знаменитого немецкого математика Давида Гильберта, который ввел это пространство для решения интегральных уравнений математнческой физики.

Теперь можно сказать, какие бесконечные матрицы мы будем рассматривать: те, которые задают непрерывные линейные операторы в гильбертовом пространстве. К сожалению, этот класс матриц не так легко описать в терминах матричных элементов. Достаточным, но не необходимым условием является сходимость двойного ряда $\sum_{i,j} |A|_{ij}^2$, а необходимым, но не достаточным условием — сходимость рядов $\sum_i |A|_{ij}^2$ и $\sum_j |A|_{ij}^2$ при всех *j* и *i* соответственно.

Каким же может быть спектр бесконечной эрмитовой матрицы. Легко привести пример (диагональной) матрицы, имеющей счетное множество собственных значений. Более поучителен следующий

пример, показывающий, что спектр может заполнять целый отрезок вещественной оси.

Пример 6. Рассмотрим матрицу A с элементами

$$a_{ij} = \begin{cases} 1, & \text{если } |i-j| = 1, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Для выяснения свойств оператора, задаваемого этой матрицей, установим соответствие между допустимыми последовательностями $\mathbf{x} = \{x_i\}$ и нечетными 2π-периодическими функциями на прямой, полагая

$$\{x_n\} \Leftrightarrow \sum_{n=1}^{\infty} x_n \sin(nt). \qquad (12)$$

Можно показать, что образом пространства H при этом соответствии будет совокупность $\widetilde{H}$ всех нечетных 2π-периодических функций φ на прямой, для которых конечен интеграл (в смысле Лебега)

$$\int_0^{\pi} |\varphi(t)|^2 \, dt.$$

При этом скалярное произведение в пространстве H переходит в скалярное произведение в $\widetilde{H}$, задаваемое формулой

$$(\varphi, \vartheta) = \frac{2}{\pi} \int_0^{\pi} \varphi(t)\overline{\vartheta(t)} \, dt.$$

Можно доказать утверждение, что линейный оператор, задаваемый матрицей A в пространстве H, переходит при соответствии (12) в оператор умножения на $2\cos t$ в пространстве $\widetilde{H}$. Из этого утверждения, что выражение $f(A)$ имеет смысл для всех непрерывных функций на отрезке $[-2, 2]$ и что соответствующий оператор в пространстве $\widetilde{H}$ является оператором умножения на $f(2\cos t)$.

Можно доказать, что матрица A не имеет ни одного допустимого собственного вектора.

Мы видим, что в бесконечномерном случае плохо определять спектр как совокупность собственных значений. «Правильное» определение спектра, пригодное и в конечномерной и в бесконечномерной ситуации, а также обеспечивающее справедливость аналогов теорем 1 и 2 (для эрмитовых матриц), можно найти в литературе по функциональному анализу.

14. 2. Непрерывные матрицы и факторы фон Неймана

Понятие матрицы допускает несколько вариантов перехода к бесконечности. Один из них мы разобрали в 14.4; в нем элементы матрицы нумеруются индексами *I* и *j,* пробегающими все натуральные значения. Разумеется, вместо множества **N** можно использовать и любое другое счетное множество. Часто бывает удобно вместо **N** взять множество $\mathbf{Z}_+$ всех неотрицательных целых чисел, или множество **Z** всех целых чисел, или *n*-мерную решетку $\mathbf{Z}^n$ и т. п.

Другой вариант — считать индекс непрерывным, например пробегающим вещественные числа. Тогда векторы превращаются в функции φ вещественной переменной *t,* матрицы — в функции *A* двух вещественных переменных *t* и *s,* суммирование по дискретному индексу — в интегрирование по непрерывному индексу, а соответствующие линейные преобразования — в интегральные операторы вида

$$A\varphi(t) = \int A(t, s)\,\varphi(s)\,ds. \qquad (1)$$

Чтобы все это имело смысл, нужно уточнить, какие функции φ и *A* мы рассматриваем и как понимаем сам интеграл. Оказывается, что при самом удобном и естественном выборе всех уточнений мы приходим к той же самой теории гильбертовых пространств, о которой говорилось выше. Дело в том, что между пространствами функций и пространствами последовательностей иногда можно установить взаимно однозначное соответствие, сохраняющее все операции гильбертова пространства: сложение, умножение на число, скалярное произведение и переход к пределу. Пример такого соответствия приведен в 14.1 (см. формулу (12) в примере 6).

Несмотря на простоту формулировки, это соответствие является очень сильным и глубоким результатом, имеющим важные математические и физические следствия. Примером первых является тождество

$$\sum_{n \geq 1} n^{-2} = \pi^2/6$$

примером вторых — так называемый дуализм «волна — частица» в квантовой механике.

Наконец, есть еще один способ построения бесконечных аналогов матриц. Этот способ принадлежит Дж. фон Нейману, одному из создателей математических основ квантовой теории. Он приводит к обобщениям линейных пространств, в которых размерность может

принимать не натуральные, как обычно, а любые вещественные значения. При жизни фон Неймана это его открытие не получило дальнейшего развития и рассматривалось скорее как математический курьез, вроде неизмеримых по Лебегу множеств. Сейчас теория факторов Неймана стала рабочим аппаратом функционального анализа н математической физики.

Остановимся на этой теории немного подробнее

Пример 1. *Непрерывные матрицы.* Мы будем рассматривать матрицы размера $n \times n$ при увеличивающемся n. Попробуем записать их в виде таблиц фиксированного размера (но со все более мелкими строчками и столбцами). Удобно при этом полагать $n = 2^k$, так как алгебра $\mathrm{Mat}_{2^k}(\mathbf{C})$ вкладывается в $\mathrm{Mat}_{2^l}(\mathbf{C})$ при $k \leqslant l$. Мы естественно придем к следующей интерпретации получающихся объектов.

Проведем в стандартном единичном квадрате главную диагональ (из левого верхнего в правый нижний угол), а также параллельные линии, делящие горизонтальные стороны квадрата на 2^k равных частей. Полученное множество обозначим X_k. Каждую из линий, составляющих X_k, разделим на равные части так, чтобы их горизонтальные проекции имели длину 2^{-k}. Множество X_k разделится при этом на 2^{2k} частей (см. рис. 6 для $k = 2$).

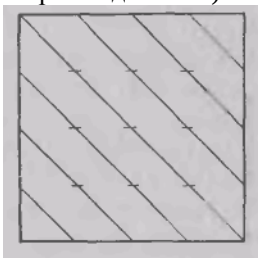


Рис. 6

Каждую матрицу $A \in \mathrm{Mat}_{2^k}(\mathbf{C})$ можно рассматривать как кусочно постоянную функцию на множестве X_k. Совокупность этих функций обозначим F_k. Это комплексное линейное пространство размерности 2^{2k}. Пусть $X = \bigcup_k X_k$. Продолжим функции, заданные на X_k, на все мпожество X нулевыми значениями. Мы получим реализацию объединения $\bigcup_k \mathrm{Mat}_{2^k}(\mathbf{C})$ всех матричных алгебр порядка 2^k в виде пространства $F = \bigcup_k F_k$ кусочно постоянных функций на X. Иногда удобно вместо множества X рассматривать его модификацию $\tilde{X}$, которая получается, если расщепить на две точки каждую «двоично-

рациональную» точку X . Эта операция расщепления выглядит естественно, если записывать вещественное число $x \in [0, 1]$ с помощью бесконечной двоичной дроби:

$$x=0,\ x_1x_2x_3\ldots = \sum_{k\geqslant 1} 2^{-k}\cdot x_k.$$

Как хорошо известно, такая запись неоднозначна, любое двоично-рациональное число допускает ровно две записи. Например, $\frac{1}{2}=0{,}1=0{,}01111\ldots$. Если считать, что разным записям соответствуют различные точки, то это и приведет к искомому расщеплению.

Преимущество $\widetilde{X}$ состоит в том, что все функции из F становятся непрерывными. Кроме того, множество $\widetilde{X}$ само естественно превращается в абелеву группу. А именно, пусть Г означает полное, а Γ_0 — ограниченное произведение счетного множества групп $\mathbf{Z}_2$. По определению элементы Г — произвольные последовательности нулей и единиц, а элементы Γ_0 — финитные последовательности (содержащие лишь конечное число единиц). Групповой закон задается компонентным сложением по модулю 2. Множество $\widetilde{X}$ отождествляется с $\Gamma \times \Gamma_0$ (элемент Γ_0 задает «диагональ», а элемент Г фиксирует точку на этой диагонали).

Описываемая ниже конструкция допускает многочисленные обобщения, в которых роль Г и Γ_0 могут играть другие группы.

Вернемся к пространству F. В нем можно определить несколько естественных понятий сходимости.

1. Введем в F скалярное произведение по формуле

$$(f, g) = \int_X f(x)\cdot\overline{g(x)}\,dx \qquad (2)$$

где dx означает меру на X, которая на каждом интервале равна длине горизонтальной проекции этого интервала.

Доказано, что на подпространстве $F_k \approx \mathrm{Mat}_{2^k}(\mathbf{C})$ скалярное произведение (2) можно задать формулой

$$(A, B) = 2^{-k}\,\mathrm{tr}\,(AB^*) = \frac{\mathrm{tr}\,(AB^*)}{\mathrm{tr}\,(1)}, \qquad (3)$$

где tr означает след матрицы (сумму ее диагональных элементов), а * — переход к эрмитово сопряженной матрице (см. 14.1).

Как всегда, имея скалярное произведение, можно определить длину вектора $|f| = (f, f)^{1/2}$, расстояние между векторами $d(f, g) = |f - g|$ и, наконец, понятие предела, считая, что $f_n \to f$, если $|f_n - f| \to 0$.

Пополнение F относительно этой сходимости мы обозначим H. Можно показать, что H — гильбертово пространство, состоящее из функций f на X, квадратично интегрируемых по Лебегу, точнее, из классов эквивалентности таких фупкций: две функции считаются эквивалентными, если они совпадают всюду, кроме точек некоторого множества нулевой меры Лебега. По традиции это уточнение лишь молчаливо подразумевают, а точки H называют просто функциями.

Скалярное произведение в H задается той же формулой (2), только интеграл в ней надо понимать в смысле Лебега.

2. Вспомним теперь, что пространство F является алгеброй: любые два элемента $f,\ g \in F$ принадлежат некоторому F_k и поэтому их можно перемножить как матрицы из $\mathrm{Mat}_{2^k}(\mathbb{C})$. Этот закон умножения допускает наглядную интерпретацию. Будем рассматривать элементы F как функции на всем единичном квадрате, равные нулю вне множества X. Тогда правило умножения запишется так:

$$AB = C, \quad \text{где} \quad C(x, y) = \sum_t A(x, t)\, B(t, y). \tag{4}$$

Суммирование в (4) идет по всем вещественным t из отрезка $[0, 1]$. Чтобы понять осмысленность этой процедуры, нужно заметить, что выражение под знаком суммы отлично от нуля лишь для тех t, для которых $x - t$ и $t - y$ имеют вид $n \cdot 2^{-k}$ (так как A и B принадлежат некоторому F_k). Поэтому фактически в сумме (4) лишь конечное число ненулевых слагаемых. Обратите внимание на сходство формулы (4) с обычным правилом матричного умножения!

Определим теперь в F норму $\|\cdot\|$, полагая

$$\|A\| = \sup_{B \neq 0} \frac{\|AB\|}{|B|}, \tag{5}$$

где $|\cdot|$ — длина, определенная выше через скалярное произведение (3). Из этого определения ясно, что $\|A\| \geqslant |A|$.

Доказано, что для матриц второго порядка

$$\|A\|^2 = |A|^2 + \sqrt{|A|^4 - |\det A|^2}.$$

Доказано, что для матриц любого порядка N

$$|A| \leqslant \|A\| \leqslant |A| \cdot \sqrt{N}. \tag{6}$$

Пополнение F по норме $\|\cdot\|$ обозначим C. Это некоторая алгебра операторов в H, *симметричная* (т. е. вместе с любым оператором A в C входит и сопряженный оператор A^*) и замкнутая по норме. Поскольку сходимость в C сильнее, чем в H, мы можем рассматривать C как подпространство в H. Пространство C содержится в пространстве $C_0(\tilde{X})$ всех непрерывных функций на $\tilde{X}$, стремящихся к нулю на

бесконечности. (В самом деле, функции из F_k обладают обоими указанными свойствами, а равномерный предельный переход их ие нарушает.)

3. Введем в F еще одно понятие сходимости. А именно, будем считать, что последовательность $\{A_n\}$ стремится к пределу A (лежащему в некотором пополнении F), если для любого $B \in H$ последовательность $\{A_n B\}$ сходится в H к элементу, который мы обозначим AB. Можно показать, что в этом случае нормы всех матриц A_n ограничены в совокупности и предельный оператор A также ограничен (т. е. имеет конечную норму) в H. Пополняя F в смысле этой сходимости, мы получим некоторую алгебру операторов в H, которую обозначим M.

Сходимость, которую мы только что ввели, называется *сильной операторной сходимостью*. Она слабее, чем сходимость по норме, но сильнее, чем сходимость в H. Поэтому имеют место непрерывные вложения

$$C \subset M \subset H.$$

Все три пространства естественно реализуются как пространства функций на X (или на $\tilde{X}$). Самое широкое пространство H мы уже описали выше как пространство функций с интегрируемым квадратом в смысле Лебега, а самое узкое — как часть пространства непрерывных функций, равных нулю на бесконечности.

К сожалению, пространство M до сих пор не получило прозрачного описания, а именно это пространстно (вернее, алгебра) представляет для нас интерес при построении математических моделей.

Лемма 1. *Пространство M состоит из всех элементов $A \in H$, для которых*

$$\|A\| = \sup_{B \in C} \frac{|AB|}{|B|} \leqslant \infty. \tag{7}$$

Следствие. *Для $A \in M$ и $B \in H$ определены произведения AB и BA, причем*

$$|AB| \leqslant \|A\| \cdot |B|, \quad |BA| \leqslant \|A\| \cdot |B|. \tag{8}$$

Теперь мы изготовим из M две алгебры операторов в пространстве H. Первая алгебра $L(M)$ состоит из операторов левого умножения $L(A)$: $B \mapsto AB$, а вторая $R(M)$ — из операторов правого умножения $R(A)$: $B \mapsto \mapsto BA$. Здесь A пробегает M, а $B \in H$.

Для любого множества S операторов в гильбертовом пространстве условимся символом S^1 обозначать *коммутант* S, т. е. множество операторов в H, перестановочных со всеми операторами из S. Справедлива

Теорема (фон Нейман). *Если S симметрично (т. е. вместе с любым оператором A содержит и сопряженный оператор A*), то* $S^{\mathrm{I}} = S^{\mathrm{III}}$, а S^{II} *совпадает с замыканием алгебры операторов, порожденной множеством S, в смысле сильной операторной сходимости.*

Первое основное свойство нашей конструкции описывает

Л е м м а 2. $L(M)^{\mathrm{I}} = R(M),\ R(M)^{\mathrm{I}} = L(M).$

Доказательство. Пусть *C* — оператор в *H* и $C \in L(M)^{\mathrm{I}}$. Тогда для любого $B \in M \subset H$ имеем

$$C(B) = C(B \cdot 1) = CL(B)(1) = L(B)C(1) = BC(1) = \\ = R(C(1))(B) \qquad (9)$$

и лемма доказана, если только $C(1) \in M$. Последнее можно установить, пользуясь леммой 1.

Итак, алгебры *L(M)* и *R(M)* являются взаимными коммутантами. Второе основное свойство состопт в том, что пересечение алгебр *L(M)* и *R(M).* которое, как легко видеть, совпадает с центром каждой из них, состоит из *скалярных* операторов (т. е. операторов умножения на число). Такие алгебры фон Нейман назвал *факторами.* Это название происходит из свойства факторов, напоминающего свойство простых чисел или простых групп. А именно, можно показать, что всякая симметричная алгебра операторов, содержащая единицу и замкнутая в сильной операторной топологии, в определенном смысле разлагается на факторы.

Доказано, что если *M* — фактор в конечномером гильбертовом пространстве *H*, а M^{I} — его коммутант, то *H* можно реализовать в виде пространства матриц размера $k \times l$ так, что *M* будет состоять из операторов умножения слева на квадратные матрицы размера $k \times k$, а M^{I} — из операторов умножения справа на квадратные матрицы размера $l \times l$.

Этот результат допускает лишь частичное обобщение на случай бесконечномерных пространств. А именно, можно показать, что если *M* — фактор в гильбертовом пространстве *H* и если *M* как топологическая алгебра с инволюцией изоморфен алгебре $L(H_1)$ всех ограниченных операторов в гильбертоволг пространстве H_1, то двойственный фактор M^{I} изоморфен алгебре $L(H_2)$, а пространство *H* отождествляется с гильбертовым тензорным произведением $H_1 \boxtimes H_2$. Такие факторы получили название факторов *типа* I.

Заслуга фон Неймана состоит в том, что он открыл новый тип факторов, которые не изоморфны *L(II)* ни для какого *H.* Примерами таких факторов являются как раз построенные выше алгебры *L(M)* и *R(M).*

Чтобы показать, что они не принадлежат типу I, введем понятие *относительной размерности* двух подпространств V_1 и V_2 в гильбертовом пространстве H, где действует некоторый фактор M. Это понятие вводится только для подпространств, инвариантных относительно всех операторов $A \in M$. Будем называть такие пространства *допустимыми.*

Доказано, что пространство PH инварнантно относительно M тогда и только тогда, когда ортопроектор P принадлежит $M^!$.

В дальнейшем мы часто будем отождествлять допустимые пространства с соответствующими ортопроекторами.

Назовем два допустимых подпространства V_1 и V_2 *эквивалентными,* если существует такой элемент $u \in M^!$ для которого

$$u^*u = P_1, \quad uu^* = P_2, \tag{10}$$

где P_i — ортопроектор на V_i.

Доказано, что равенства (10) равносильны утверждению, что оператор u отображает V_1 изометрично на V_2, а на $V_1^{\perp}$ обращается в нуль.

Будем говорить, что допустимое пространство V_1 *больше* V_2, если в V_1 есть собственное подпространство, эквивалентное V_2.

Теорема (Меррей — фон Нейман). *Для пары допустимых подпространств V_1 и V_2 имеет место одна из трех возможностей:*

a) *V_1 эквивалентно V_2;*

b) *V_1 больше V_2;*

c) *V_2 больше V_1.*

Доказательство этой теоремы использует рассуждение, аналогичное тому, с помощью которого доказывается теорема Кантора — Бернштейна о сравнении мощности двух множеств. А именно, таким образом устанавливается, что если для V_1 и V_2 справедливы и b) и c), то верно a). Кроме того, оно опирается на следующий факт.

Лемма 3. *Любые два ненулевых допустимых пространства содержат ненулевые эквивалентные части.*

Доказательство. Пусть V_1 и V_2 — ненулевые допустимые пространства. Для любого унитарного оператора $u \in M^!$ рассмотрим пространства $H_2 = uV_1 \cap V_2$ и $H_1 = u^{-1}H_2$. Ясно, что $H_i \subseteq V_i$ и что H_1 и H_2 эквивалентны. Однако они могут быть нулевыми. Если $uV_1 \cap V_2 = 0$ для всех $u \in M^!$, то пространство $M^! \cdot V_1$ будет нетривиальным (т. е. отличным от 0 и H) пространством, инвариантным относительно и M п $M^!$. Но тогда соответствующий проектор P принадлежит пересечению $M \cap M^!$ и, следовательно, равен 0 или 1. Полученное противоречие доказывает лемму.

Перейдем к определению относительной размерности. Для этого понадобится еще одно определение: допустимое пространство V называется *конечным,* если оно не эквивалентно своему собственному подпространству (сравните это с определением бесконечных множеств).

Пусть теперь V_1 и V_2 — два конечных допустимых пространства. Будем сравнивать их по аналогии с тем, как это делается с отрезками на вещественной прямой. А именно, если V_1 больше, чем V_2, то выделим в V_1 часть V'_2, эквивалентную V_2, и пусть V_3 — ортогональное дополнение к V'_2 в V_1. Тогда V_3 — также допустимое конечное подпространство и мы можем с парой V_2, V_3 повторить ту же процедуру. Этот процесс может за конечное число шагов привести к нулевому пространству. В этом случае наши исходные пространства «соизмеримы» в следующем смысле:

$$V_1 = \bigoplus_{i=1}^{k} V_{1i}, \quad V_2 = \bigoplus_{i=1}^{l} V_{2i}$$

и все V_{ij} попарно эквивалентны. Назовем относительной размерностью пары V_1, V_2 число k/l и обозначим его $V_1 : V_2$. Если же процесс сравнения исходных пространств продолжается до бесконечности, то мы определим величину $V_1 : V_2$ как иррациональное число, равное отношению длин таких двух отрезков, сравнение которых приводит к тому же «протоколу», что и сравнение наших пространств.

Доказано, что $V_1 : V_2$ равно нижней грани множества чисел m/n, для которых

$$V_1 \subseteq \bigoplus_{i=1}^{m} H, \quad V_2 \supseteq \bigoplus_{i=1}^{n} H'_i$$

и все H_i и H'_i эквивалентны друг другу.

Наиболее интересен случай, когда все пространство H конечно (и бесконечномерно в обычном смысле). Такпо факторы M получили название факторов *типа* II_1. Для них все допустимые подпространства конечны и можно определить *факторную размерность* $\dim_M V = V : H$, принимающую значения в отрезке [0, 1]. Далее, для любого оператора $A \in M$ можно определить его *факторный след* $\mathrm{tr}_M A$, полагая для ортопроектора P

$$\mathrm{tr}_M P = \dim_M PH \tag{11}$$

и распространяя его па остальные операторы по комплексной линейности и сильной непрерывности. Этот «след» сохраняет основное свойство обычного следа

$$\mathrm{tr}_M AB = \mathrm{tr}_M BA. \tag{12}$$

В случае, когда A — частичная изометрия, а $B = A^*$, это следует из определения эквивалентности и относительной размерности допустимых пространств; общий случай выводится из этого.

Теперь вернемся к нашему примеру фактора.

Доказано, что для $A \in M$ справедливо равенство

$$\mathrm{tr}_M A = \int_X A(x, x)\, dx. \tag{13}$$

Пример 2. *Квантовый тор* $\mathbf{T}^2$. Название этого примера отражает общую тенденцию связывать с квантовой теорией всякий переход от коммутативных объектов к некоммутативным. Хорошо известно, что каждый компакт X характеризуется алгеброй $C(X)$ непрерывных функций на нем, а гладкое компактное многообразие M — алгеброй $C^\infty(M)$ гладких функций, например, точки M восстанавливаются как максимальные идеалы в $C^\infty(M)$, векторные поля на M — как дифференцирования $C^\infty(M)$ и т. п. Соответствующие квантовые объекты получаются, если перейти к некоммутативным алгебрам.

В случае тора алгебра $C^\infty(\mathbf{T}^2)$ состоит из функций вида

$$\sum c_{k,l} \exp 2\pi i\,(kx + ly), \tag{14}$$

где суммирование идет по двумерной решетке $\mathbf{Z}^2$, а коэффициенты удовлетворяют для любого $N \in \mathbf{N}$ условиям

$$|c_{k,l}| \leqslant \mathrm{const} \cdot (1 + k^2 + l^2)^{-N}. \tag{15}$$

Рассмотрим теперь алгебру с инволюцией A_q, порожденную единицей и двумя элементами u и v с соотношениями

$$u^*u = uu^* = 1,\ v^*v = vv^* = 1,\ uv = qvu, \tag{16}$$

где $q = e^{2\pi i\tau}$ — комплексное число с $|q| = 1$.

Общий элемент этой алгебры имеет вид

$$\sum_{k,l \in \mathbf{Z}} c_{k,l} u^k v^l, \tag{17}$$

где лишь конечное число коэффициентов отлично от нуля. Обычно рассматривают несколько большую алгебру, состоящую из сумм вида (17), где коэффициенты подчинены условиям (15), и называют ее «алгеброй гладких функций на квантовом торе $\mathbf{T}^2_q$. Ясно, что при $q = 1$ определенный таким образом квантовый тор совпадает с обычным.

Оказывается, из алгебры A_q можно, как и в примере 1, изготовить гильбертово пространство H, алгебру M и два ее представления L и R в пространстве H, причем в случае иррационального τ (т. е. в случае, когда q не является корнем из 1) $L(M)$ и $R(M)$ будут факторами типа II_1.

Доказано, что факторы примера 1 и 2 изоморфны.

Пример 3. *Квантовые сферы* S^2 *и* S^3. Как известно, сфера S^3 является группой, а сфера S^2 — однородным пространством для этой группы.

Все эти факты можно сформулировать в терминах гладких функций на них. Например, тот факт, что S^3 действует на S^2, описывается гладким отображением $S^3 \times S^2 \to S^2$, а это отображение, в свою очередь, определяется гомоморфизмом алгебры $C^\infty(S^2)$ в алгебру $C^\infty(S^3 \times S^2) \cong C^\infty(S^3) \otimes C^\infty(S^2)$. Оказывается, существуют такие некоммутативные деформации A_q п B_q алгебр $C^\infty(S^3)$ и $C^\infty(S^2)$, зависящие от параметра q, что для них по-прежнему имеют смысл все нужные гомоморфизмы. Это позволяет рассматривать A_q и B_q как «алгебры функций» на квантовой группе S^3_q и ее квантовом однородном пространстве S^2_q.

14.3. О понятии суперсимметрии

1. В математике, как и во всех науках, большую роль играет понятие симметрии. Чаще всего свойства симметрии выражаются на языке групп, однородных пространств и представлений. Однако в математике и математической физике все большую роль приобрел тип симметрии, который получил название *суперсимметрии.* В математике суперсимметрия означает в каком-то смысле равноправие между плюсом и минусом, четным и нечетным, симметрическим и антисимметрическим и т. д. В физике — это равноправие между фермионами и бозонами.

Идеология суперсимметрии состоит в следующем. Каждому «обычному», или «четному», понятию (определению, теореме, конструкции и т. д.) должен соответствовать «нечетный» аналог, который вместе с исходным понятием объединяется в «суперобъект».

Формализм суперсимметрии требует чисел нового сорта, которые отличаются от обычных тем, что умножение не коммутативно, а *антикоммутативно:* $xy = -yx$. В частности, $x^2 = 0$. Эти числа могут использоваться так же широко и на тех же правах, как и обычные числа. Например, они могут играть роль локальных координат на многообразии, и таким образом возникает понятие *супермногообразия*.

Для некоторых математических понятий нечетные аналоги достаточно очевидны, для других — более сложны, а порой и неожиданны. Приведем несколько сравнительно элементарных примеров, предоставляя читателю самому продолжить этот список. Попробуйте, например, ответить на вопрос: что означает суперспмметрия в той задаче, над которой вы сейчас думаете (или думали недавно)?

2. Суперснмметрня в алгебре. Начнем с линейной алгебры. Супераналогом линейного пространства являетсятак называемое

$\mathbf{Z}_2$-градуированное линейное пространство, т. е. пространство V, разбитое в прямую сумму $V = V_0 \oplus V_1$, причем элементы V_0 считаются *четными,* а элементы V_1 — *нечетными.* Пару $(\dim V_0,\ \dim V_1)$ назовем *размерностью* V (точнее, суперразмерностью).

Назовем индексом $\mathbf{Z}_2$-градуированного пространства $V = V_0 \oplus V_1$ число $i(V) = \dim V_0 - \dim V_1$. Доказано, что

$$i(V \oplus W) = i(V) + i(W);$$
$$i(V \otimes W) = i(V)i(W).$$

Замечание 1. Иногда именно индекс считают правильным супераналогом понятия размерности линейного пространства. Единственным недостатком индекса в роли суперразмерности является нарушение принципа: два пространства изоморфны, если их размерности совпадают.

Замечание 2. Понятие индекса $\mathbf{Z}_2$-градуированного пространства давно употреблялось в алгебраической топологии. В самом деле, эйлерова характеристика, число Лефшеца и другие альтернированные суммы — все это примеры индексов.

Перейдем теперь к линейным операторам. Если V и W — $\mathbf{Z}_2$-градуированные пространства, то совокупность $L(V, W)$ линейных операторов из V в W также снабжается естественной $\mathbf{Z}_2$-градуированной. А именно, оператор $A \in L(V, W)$ записывается блочной матрицей

$$A = \begin{Vmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{Vmatrix}, \tag{1}$$

где A_{ij} — оператор из V_j в W_i. Блоки, стоящие на главной диагонали, буделм считать четными, а остальные — нечетными. Таким образом, если обозначить $p(x)$ *четность* объекта x (принимающую значения 0 и 1 mod 2), то для оператора A и вектора v будет справедливо соотношение

$$p(Ax) = p(A) + p(x). \tag{2}$$

Этот принцип принимается и для других мультипликативных операций: умножения операторов, тензорного умножения, скалярного умножения векторов и т. д.

Правило 1. *При умножении четности складываются.*

Кроме того, во всех определениях супералгебры, содержащих мультипликативные операции, появляются дополнительные множители ±1 согласно следующему принципу (нижеследующая формулировка заимствована из литературы по математике, а физики

предпочитают более сочную фразу: если что-то четности *a* течет мимо чего-то четности *b*, то возникает знак $(-1)^{ab}$.):

Правило 2. *Если в какой-то формуле обычной алгебры появляется несколько одночленов с переставленными членами, то в соответствующей формуле супералгебры каждая перестановка соседних членов, скажем x и y, сопровождается добавлением к этому одночлену множителя* $(-1)^{p(x)p(y)}$.

Важную роль в линейной алгебре играет понятие следа линейного оператора, действующего из *V* в *V*. Напомним, что с точностью до числового множителя след характеризуется свойством $\mathrm{tr}\,(AB) = \mathrm{tr}\,(BA)$, или $\mathrm{tr}\,[A, B] = 0$, где $[A, B] = AB - BA$. В супералгебре коммутатор задается формулой

$$[A, B] = AB - (-1)^{p(A)p(B)}BA. \tag{3}$$

Формула (3) применима лишь к однородным (четным или нечетным) операторам *A* и *B*. На общий случай она распространяется по линейности. Это замечание относится и к другим аналогичным формулам.

Определим *суперслед* оператора, записанного в виде (1), формулой

$$\mathrm{str}\,A = \mathrm{tr}\,A_{00} - \mathrm{tr}\,A_{11}. \tag{4}$$

Доказано, что $\mathrm{str}\,[A, B] = 0$ для всех *A* и *B*.

Доказано, что пространство *L(V, V)* с операцией суперкоммутпрования является *супералгеброй Ли* (проверьте выполнение тождества Якобн).

Результат задачи 5 можно сформулировать так: суперслед задает гомоморфизм супералгебры Ли *L(V, V)* в супералгебру **R** с нулевым коммутатором.

Далее определим супераналог определителя и установим тождество

$$\mathrm{sdet}\,(\exp A) = \exp\,(\mathrm{str}\,A), \tag{5}$$

хорошо известное в четном случае. Это можно сделать, однако далеко не так прямолинейно, как мы рассуждали до сих пор.

Дело в том, что свойства определителя естественно изучать на языке теории групп Ли, а эта теория существенно нелинейна. (Группой Ли напивается группа, являющаяся также гладким многообразием, причем структуры группы и многообразия согласованы естественным образом: групповые операции являются гладкими отображениями. Большинство групп, используемых в приложениях, — группы Ли.) Попробуйте, например, определить понятие супергруппы так, чтобы совокупность GL *(V)* обратимых операторов в суперпространстве *V* была примером такого объекта. Правильный ответ не прост и формулируется на языке

теории супермногообразий, которой посвящен последний раздел этого параграфа.

3. Суперсимметрпя в анализе. Назовем функцией четных переменных $x_1, x_2, \ldots, x_n$ и нечетных переменных $\xi_1, \xi_2, \ldots, \xi_m$ выражение

$$f(x, \xi) = \sum_I f_I(x_1, \ldots, x_n)\,\xi_I, \tag{6}$$

где суммирование ведется по всем наборам $I = \{i_1, i_2, \ldots, i_k\}$, $1 \le i_1 < i_2 < \ldots i_k \le n$, ξ_I означает $\xi_{i_1} \ldots \xi_{i_k}$, а $f_I(x_1, \ldots, x_n)$— обычные функции вещественных переменных $x_1, \ldots. x_n$. Мы будем считать их вещественными, гладкими и финитными (т. е. равными нулю вне некоторого компакта). Выражения (6) образуют алгебру относительно обычных операций сложения и умножения (с учетом соотношений антикоммутации $\xi_i\xi_j = -\xi_j\xi_i$). Обозначим эту алгебру $C_0^\infty(\mathbf{R}^{n,m})$. Как известно, основные операции анализа — дифференцирование и интегрирование — можно определить в чисто алгебраических терминах, используя структуру алгебры гладких функций. Этот способ легко поддается «суперизации».

Напомним, что *дифференцированием* алгебры $\mathcal{A}$ называется линейное отображение $\partial\colon \mathcal{A} \to \mathcal{A}$, обладающее свойством (правило Лейбница)

$$\partial(ab) = \partial(a)b + a\partial(b).$$

Доказано, что всякое дифференцирование алгебры $C_0^\infty(\mathbf{R}^n)$ имеет вид

$$\partial f = \sum_{k=1}^{n} a_k \partial_k f,$$

где $a_k \in C^\infty(\mathbf{R})$, а $\partial_k = \partial/\partial x_k$ — оператор частной производной по x_k.

Для супералгебры $\mathcal{A}$ естественно определить *супер-дифференцирование* как отображение $\partial\colon \mathcal{A} \to \mathcal{A}$, удовлетворяющее аналогичному условию («суперправнло Лейбница»)

$$\partial(ab) = \partial(a)b + (-1)^{p(a)p(\partial)}\, a\partial(b),$$

где $p(\partial)$— чепюсть супердифференцирования ∂.

В алгебре $C_0^\infty(\mathbf{R}^{n,m})$ можно определить операторы частных производных d_k (соответственно δ_k) как четные (соответственно нечетные) супердифференцирования, нормированные условиями

$$\partial_i x_j = \delta_{ij}, \quad \partial_i \xi_j = 0, \ \delta_i x_j = 0, \quad \delta_i \xi_j = \delta_{ij}.$$

Оставим читателям определение общих дифференциальных операторов в $C_0^\infty(\mathbf{R}^{n,m})$ и проверку того, что они образуют ассоциативную некоммутативную супералгебру.

Доказано, что любой линейный оператор в пространстве $C_0^\infty(\mathbf{R}^{0,m})$ может быть записан как дифференциальный:

$$A = \sum_{I,J} c_{I;J} \xi_I \cdot \delta_J, \tag{7}$$

где $I = \{i_i < \ldots < i_k\}$, $J = \{j_1 < \ldots < j_i\}$, а $c_{I;J}$— вещественные коэффициенты.

Перейдем к интегрированию по суперпространству $\mathbf{R}^{n,m}$. Обычный определенный интеграл по пространству $\mathbf{R}^n$ с точностью до числового множителя характеризуется свойствами:

1) интеграл является линейным функционалом на $C_0^\infty(\mathbf{R}^n)$;
2) интеграл обращается в нуль на образах операторов ∂_i, $1 \leqslant i \leqslant n$.

Поэтому естественно определить интеграл по суперпространству так, чтобы он обладал аналогичными свойствами. Мы приходим к формуле

$$\int\limits_{\mathbf{R}^{n,m}} f(x, \xi)\, d^n x\, d^m \xi = \int\limits_{\mathbf{R}^n} f_{12\ldots m}(x)\, d^n x. \tag{8}$$

Именно с этой формулы началась теория интегрирования на суперммогообразпях.

Доказано, что любой линейный оператор в пространстве $C_0^\infty(\mathbf{R}^{0,m})$ может быть записан как интегральный:

$$(Af)(\xi) = \int\limits_{\mathbf{R}^{0,m}} A(\xi, \eta)\, f(\eta)\, d^m \eta, \tag{9}$$

где $A(\xi, \eta)$— функция $2m$ нечетных переменных, а интеграл по переменным η предполагается перестановочным с умножением слева на переменные ξ.

Доказано, что след оператора *A,* заданного равенством (9), можно вычислять по формуле

$$\operatorname{tr} A = \int\limits_{\mathbf{R}^{0,m}} \overset{\vee}{A}(\xi, \xi)\, d^m \xi, \tag{10}$$

где операция $\vee$ переводит одночлен $\xi_I \eta_J$ в $\eta_J \xi_I$.

Важным свойством интеграла является его поведение при замене переменных. Для обычного четного интеграла это поведение по существу закодировано в форме записи (в случае одной переменной предложенной еще Лейбницем): интегрируется не функция *f(x),* а *дифференциальная форма* $f(x) d^n x$. Здесь $d^n x$ - краткое обозначение *n*-формы $dx^1 \wedge dx^2 \wedge \ldots \wedge dx^n$. Если переменные x^i выражены через другие переменные y^j, то форма $d^n x$ переходит в $\frac{D(x)}{D(y)} d^n y$, где

$\frac{D(x)}{D(y)}$ — якобиан замены переменных, т. е. определитель матрицы Якоби

$$\begin{Vmatrix} \partial x^1/\partial y^1 & \dots & \partial x^1/\partial y^n \\ \dots & \dots & \dots \\ \partial x^n/\partial y^1 & \dots & \partial x^n/\partial y^n \end{Vmatrix}$$

Заметим, что это правило замены переменных в интеграле (вспомните упражнения по анализу на вычисление кратных интегралов) является непосредственным следствием двух простых принципов:

1) правило замены для дифференциала:

$$dx^i = \sum_j \partial x^i/\partial y^j \cdot dy^j;$$

2) свойства внешнего произведения $\wedge: a \wedge b = -b \wedge a.$

В нечетном случае выражение $d^m\xi$ уле не является тензором! Это новый геометрический объект, который получил название *интегральной формы* или *формы Березина*. Общее определение интегральных форм естественно давать в контексте теории супермногообразий. Здесь следует отметить, что уже при линейных заменах переменных величина $d^m\xi$, в отличие от $d^m x$, *не умножается,* а *делится* на определитель соответствующей матрицы, как видно из простейшего примера:

$$\xi_i \to \eta_i = a_i \cdot \xi_i, \quad \int \xi_1 \dots \xi_m d^m\xi = \int \eta_1 \dots \eta_m d^m\eta = 1$$

Этот факт имеет принципиальное значение в квантовой теории поля, где с его помощью успешно борются с расходимостями.

Доказано, что определитель кососимметрической матрицы *A* размера *2m* × *2m* является квадратом некоторого многочлена *Pf(A)* степени *m* от коэффициентов этой матрицы.

4. О супергеометрии. Как мы видели выше, и алгебра и анализ подводят к необходимости определения понятия *супермногообразия*. Мы не будем здесь давать строгого определения супермногообразня, отсылая читателя к литературе по этому вопросу. Скажем лишь, что это можно сделать по аналогии с понятием алгебраического многообразия в его современной форме.

Наивное определение алгебраического многообразия *M* как множества в аффинном или проективном пространстве над полелг *К,* задаваемого системой алгебраических уравнений, в современной математике сменилось на функториалыюе. А именно, *M* определяется как функтор из категории коммутативных К-алгебр в категорию множеств: каждой алгебре $\mathcal{A}$ над *К* соответствует множество $M_{\mathcal{A}}$ $\mathcal{A}$*-точек* *M,* т. е. решений соответствующей системы уравнений с координатами из алгебры $\mathcal{A}$. Если в этом определении заменить

термин «коммутативная алгебра» на «суперкоммутативная супералгебра», мы получим определение супермногообразия.

Таким образом, мы отказываемся от теоретико-множественного подхода и описываем все свойства супермногообразий в терминах функций на них. В частности, вместо отображения $M \to N$ мы рассматриваем соответствующий гомоморфизм алгебр $C^\infty(N) \to C^\infty(M)$, а роль точки $m \in M$ играет максимальный идеал в алгебре функций на *M*. Отметим, что в отличие от обычных многообразий супермногообразие *не определяется* множеством своих точек.

Приведем один простой, по важный пример супермногообразня. Рассмотрим алгебру $\mathscr{A}$ гладких функций $f(t, \tau)$ одной четной переменной *t* и одной нечетной переменной τ. Эту алгебру можно рассматривать как алгебру гладких функций на супермногообразии *M* размерности (1, 1), которое является супераналогом обычной прямой. По аналогии с четным случаем назовем *векторным полем на M* дифференцирование алгебры $\mathscr{A}$.

Доказано, что каждое четное (соответственно нечетное) поле имеет вид

$$v = f(t)\partial/\partial t + g(t)\tau\partial/\partial\varepsilon \quad \text{(соответственно } \xi = \varphi(t)\tau\partial/\partial t + \vartheta(t)\partial/\partial\tau\text{).} \tag{11}$$

Совокупность векторных полей на *M* образует супералгебру Ли относительно операции суперкоммутирования

$$[v_1, v_2] = v_1 v_2 - (-1)^{p(v_1)p(v_2)}[v_1, v_2]. \tag{12}$$

Замечательно, что привычное нам четное поле $v_0 = \partial/\partial t$ является квадратом нечетного поля $\xi_0 = \partial/\partial\tau + \tau\partial/\partial t$. Это имеет принципиальное значение для теоретической физики. В самом деле, пусть переменная *t* означает время. Все законы изменения физических величин со временем формулируются в терминах поля v_0 и, следовательно, должны быть следствиями более фундаментальных законов, формулируемых в терминах поля ξ_0.

Изменение со временем — это специальный случай *действия группы* — в данном случае аддитивной группы **R** на многообразии, играющем роль фазового пространства (или пространства состояний) физической системы. Другие примеры возникают при наличии разного рода симметрии у рассматриваемой системы. Роль группы симметрии, как правило, играет некоторая группа Ли (группа параллельных переносов, группа вращений, группа Лоренца, группа Пуанкаре и т. д.). Идея *суперсимметрии в физике* состоит в том, что вместо этой группы Ли нужно рассматривать более широкую *супергруппу Ли.* При этом

оказалось, что большинство рассматривавшихся ранее групп симметрии (в частности, все перечисленные выше) обладают естественными расширениями до супергрупп.

Пример. Пусть $V = V_0 \oplus V_1 - \mathbf{Z}_2$-градуированное векторное пространство. Определим супергруппу GL(V) следующим образом. Для любой суперкоммутативной ассоциативной супералгебры $\mathscr{A}$ определим множество $\mathrm{GL}(V)_{\mathscr{A}}$ как совокупность обратимых матриц вида (1), у которых четные блоки состоят из четных элементов алгебры $\mathscr{A}$, а нечетные блоки — из нечетных. Тем самым мы определили супермногообразие GL(V). Чтобы ввести на нем структуру группы, нужно определить морфизмы $\mathrm{GL}(V)\times\mathrm{GL}(V)\to\mathrm{GL}(V)$ и $\mathrm{GL}(V)\to\mathrm{GL}(V),$ задающие закон умножения и переход к обратному элементу.

Доказано, что формула

$$\mathrm{sdet}\, A = \det\left(A_{00} - A_{01}A_{11}^{-1}A_{10}\right)\cdot\det\left(A_{11}^{-1}\right) \qquad (13)$$

задает гомоморфизм группы $\mathrm{GL}(V)_{\mathscr{A}}$ в группу $\mathrm{GL}(1)_{\mathscr{A}}$ обратимых элементов алгебры $\mathscr{A}$.

Этот гомоморфизм называют *супердетерминантом* или *березинианом* оператора $\mathscr{A}$ и обозначают также Вег $\mathscr{A}$.

Отметим, что Бег определяет гомоморфизм супергруппы GL(V) в супергруппу GL(1).

5. Суперсимметрия и арифметика. Это — сравнительно новое направление в математике, которому посвящено пока не так много работ. Примером является статья голландского математика Д. Спектора «Суперсимметрня и функция Мёбиуса», опубликованная в журнале «Сообщения математической фпзпкп» в 1980 г. В ней речь идет о физической интерпретации некоторых теоретико-числовых функций и, в частности, *функции Мёбиуса*

$$\mu(n) = \begin{cases} (-1)^n, & \text{если } n \text{ является произведением} \\ & k \text{ различных простых чисел,} \\ 0 & \text{в противном случае.} \end{cases}$$

Главным предметом изучения в статистической механике является так называемая *статистическая сумма* как функция температуры системы. В квантовой теории эта величина равна $\mathrm{tr}\, e^{-\beta P}$, где P — оператор энергии, а β — параметр, обратно пропорциональный температуре ($\beta^{-1} = kT$, где k — постоянная Больцмапа). В системе с суперсимметрией основное гильбертово пространство H является суперпространством, а оператор энергии P имеет вид Q^2, где Q — нечетный антиэрмитов оператор. В такой ситуации справедлива *формула Виттена*

$$\operatorname{str} e^{-\beta P} = \operatorname{ind} \ker P, \tag{14}$$

где $\ker P = \{x \in H | Px = 0\}$, а ind означает разность размерностей четной и нечетной компоненты (см. п. 1). В частности, левая часть на самом деле не зависит от β! Переходя в (14) к пределу при $\beta \to 0$ или $\beta \to \infty$, можно получить много важных соотношений (которые, разумеется, зависят от рассматриваемой системы). В статье Спектора рассматривается модельная система, в которой участвуют бозонные и фермионные частицы, нумеруемые простыми числами. Каждое чистое состояние системы (такие состояния соответствуют векторам ортонормированного базиса в *H)* определяется наличием заданного числа частиц каждого сорта. Пусть, например, имеется k_i бозонных и ε_i фермионных частиц сорта p_i (напомним, что сорта частиц соответствуют простым числом). Здесь k_i — целое неотрицательное число, а ε_i — либо 0, либо 1 в силу *принципа Паули.* Это состояние удобно нумеровать парой *(N, d),* где

$$N = \prod_i p_i^{k_i}, \quad d = \prod_i p_i^{\varepsilon_i}.$$

Приведем математическую формулировку того, что физики называют статистикой Бозе — Эйнштейна плп Ферми — Дирака. Пусть $L_\pm$ — пространство одночастичных (соответственно бозонных нлп фермионных состояний). Тогда полное пространство *H* имеет вид $S(L_+) \otimes \Lambda(L_-)$, где *S* означает симметрическую, а Λ — внешнюю алгебру.

Ясно, что *N* может быть любым натуральным числом, а *d* — любым делителем *N,* свободным от квадратов (т. е. не делящимся ни на какой квадрат, отличный от 1). Четность состояния *(N, d)* определяется числом простых сомножителей в *d.* А именно, $(-1)^{p(N,d)} = \mu(d)$.

14.4. Решеточное дифференциальное и интегральное исчисление

1. Физики до спх пор спорят о том, как устроено наше пространство на очень малых расстояниях: является ли оно безгранично делимым, или существует некоторая «элементарная длина». В последнем случае роль числовой прямой должно играть некоторое дискретное (т. е. состоящее из изолированных точек) множество. По разным соображениям в качестве такого множества удобно взять бесконечную в обе стороны арифметическую прогрессию с разностью $h > 0$ или геометрическую прогрессию со знаменателем $q > 1$.

Оказывается, на такой «дискретной прямой» или «решетке» существует аналог классического математического анализа.

2. Рассмотрим сначала случай арифметической прогрессии и предположим для упрощения формул, что $h = 1$. Другими словами, вместо обычной прямой **R** мы будем рассматривать «дискретную прямую» **Z**. Пусть f — вещественная функция на **Z** (т. е. бесконечная в обе стороны последовательность вещественных чисел). Все такие функции автоматически непрерывны. Более того, все они дифференцируемы, если определить *решеточную производную* Δf функции f формулой

$$\Delta f(n) = f(n+1) - f(n). \tag{1}$$

Решеточным интегралом функции f назовем величину

$$\int_m^n f(k)\,\Delta k =: \sum_{k=m}^{n-1} f(k). \tag{2}$$

Из этих определений вытекает решеточный аналог формулы Ньютона — Лейбница: если $\Delta f = F$, то

$$\int_m^n f(k)\,\Delta k = F(n) - F(m). \tag{3}$$

Далее, в обычном анализе важную роль играют многочлены

$$P_n(x) = x^n/n!.$$

Они характеризуются следующими свойствами:

$$DP_0 = 0,$$
$$DP_n = P_{n-1} \text{ при } n \geqslant 1$$

и

$$P_n(0) = \begin{cases} 1 & \text{при } n = 0, \\ 0 & \text{при } n \geqslant 1, \end{cases} \tag{4}$$

где $D = d/dx$ — оператор дифференцирования. Решеточным аналогом этих многочленов являются многочлены $\Pi_n(x)$, характеризуемые условиями:

$$\Delta\Pi_0 = 0,$$
$$\Delta\Pi_n = \Pi_{n-1} \text{ при } n \geqslant 1$$

и

$$\Pi_n(0) = \begin{cases} 1 & \text{при } n = 0, \\ 0 & \text{при } n \geqslant 1, \end{cases} \tag{4'}$$

где Δ — оператор решеточного дифференцирования.

Пусть $f(x)$—многочлен степени n, который принимает целые значения при всех целых x. Доказано, что

$$f(x) = \sum_{k=0}^{n} c_k \Pi_k(x), \tag{5}$$

где c_k — целые числа, вычисляемые по формуле

$$c_k = \Delta^k f(0).$$

Формула (5)—решеточный аналог формулы Тейлора.

С помощью многочленов Π_k можно вывести полезные формулы суммирования. Например, чтобы вычислить сумму $S_2(n) = 1^2 + 2^2 + \ldots + n^2$, достаточно заметить, что $x^2 = 2\Pi_2(x) + \Pi_1(x)$ и поэтому

$$\begin{aligned} S_2(n) = \sum_1^{n+1} k^2 \Delta k = \sum_1^{n+1} (2\Pi_2(k) + \Pi_1(k))\,\Delta k = \\ = 2(\Pi_3(n+1) - \Pi_3(1)) + \Pi_2(n+1) - \Pi_2(1) = \\ = 1/3 \cdot (n+1)n(n-1) + 1/2 \cdot (n+1)n = \\ = 1/6 \cdot n(n+1)(2n+1). \end{aligned}$$

Для вычисления более общих сумм $S_k(n) = 1^k + 2^k + \ldots + n^k$ нужно уметь выражать многочлены $P_m(x)$ через $\Pi_n(x)$ и обратно. Из (5) вытекает, что для каждого n набор $\{\Pi_k(x)\}_{0 \leqslant k \leqslant n}$ как и $\{P_k(x)\}_{0 \leqslant k \leqslant n}$ является базисом в пространстве всех многочленов степени $\leq n$. Поэтому существуют такие коэффициенты $\{a_{ni}\}$ и $\{b_{nj}\}$, что

$$\begin{aligned} \Pi_n(x) &= \sum_{i=0}^{n} a_{ni} P_i(x), \\ P_n(x) &= \sum_{j=0}^{n} b_{nj} \Pi_j(x). \end{aligned} \qquad (6)$$

Доказано, что при $n \geq 1$

$$\begin{aligned} a_{n1} &= (-1)^{n-1}/n, \\ b_{n1} &= 1/n!. \end{aligned}$$

Чтобы полностью вычислить коэффициенты $\{a_{ni}\}$ и $\{b_{nj}\}$, воспользуемся тем, что операторы обычного к решеточного дифференцирования связаны формулой

$$\Delta = e^D - 1. \qquad (7)$$

Надеемся, что у читателя, который хотя бы бегло просмотрел 14.5, не возникнет недоумения по поводу смысла выражения e^D (экспоненты от оператора) в правой части равенства (7). Прежде чем доказывать это равенство, уместно вспомнить о шаге решетки h, который мы положили равным 1. В общем случае решеточная производная определяется формулой

$$\Delta_h f(x) = (f(x+h) - f(x))/h. \qquad (1')$$

Доказано, что формула Тейлора для многочленов эквивалентна равенству

$$\Delta_h = (e^{hD} - 1)/h, \tag{7'}$$

которое при $h = 1$ превращается в (7).

Вместо того чтобы вычислять отдельно каждый коэффициент a_{ni} и b_{nj}, мы вычислим их все сразу, найдя так называемые *производящие функции*

$$A(x, y) = \sum_{n \geqslant k \geqslant 0} a_{nk} x^n y^k$$

и

$$B(x, y) = \sum_{n \geqslant k \geqslant 0} b_{nk} x^n y^k.$$

Доказано, что

$$A(x, y) = (1 - y(e^x - 1))^{-1},$$
$$B(x, y) = (1 - \ln(1 + x))^{-1}.$$

Вернемся теперь к формулам суммирования. Нас интересуют суммы вида (2), т. е. решеточные интегралы. Поскольку при $h \to 0$ формулы решеточного анализа переходят в формулы обычного анализа, естественно попытаться выразить сумму (2) через обычную первообразную $\mathcal{F}(x)$ функции f. Такое выражение было найдено Маклореном и, повидимому, еще раньше было известно Эйлеру. Оно называется формулой суммирования Эйлера — Маклорена. Идея его вывода (по Эйлеру) чрезвычайно проста. Пусть $F(x)$— решеточная первообразная функции f. Тогда $\Delta F = f = D\mathcal{F}$, откуда $F = D/(e^D - 1)\mathcal{F}$. Используя числа Бернулли (см. 14.2). можно показать, что $x/(e^x - 1) = \sum_{n \geqslant 0} B_n x^n/n!$, и поэтому $F = \sum_{n \geqslant 0} B_n \mathcal{F}^{(n)}/n!$. Отсюда следует искомое равенство:

$$\sum_{k=m}^{n-1} f(k) = \sum_{s \geqslant 0} B_s \left(\mathcal{F}^{(s)}(n) - \mathcal{F}^{(s)}(m)\right)/s!. \tag{8}$$

Из формулы Эйлера — Маклорена (8) следуют символические равенства:

$$S_k(n) = ((B + n + 1)^{k+1} - (B + 1)^{k+1})/(k + 1), \tag{9}$$

$$(B + 1)^k = B^k \text{ при } k \geqslant 2. \tag{10}$$

Понимать эти равенства надо так: после раскрытия скобок все выражения B^k надо заменить на B_k. Заметим, что (10) удобно использовать для рекуррентного вычисления чисел Бернулли. Например, при k=2 мы имеем $B_2 + 2B_1 + 1 = B_2$, откуда $B_1 = -1/2$.

Доказаны формулы:

$$\operatorname{ctg} x = 1/x - \sum_{k \geqslant 1} |B_{2k}| \cdot 2^{2k} \cdot x^{2k-1}/(2k)!,$$

$$\operatorname{tg} x = \sum_{k \geqslant 1} |B_{2k}| \cdot 2^{2k} \left(2^{2k} - 1\right) \cdot x^{2k-1}/(2k)!.$$

Рассмотрим решеточный аналог экспоненты $e^{\lambda x}$. В обычном анализе эту функцию можно определить либо как сумму ряда $\sum_{n \geqslant 0} \lambda^n P_n(x)$, либо как решение дифференциального уравнения $Df(x) = \lambda \cdot f(x)$ с начальным условием $f(0) = 1$.

Существуют x для которых ряд

$$E(x) = \sum_{n \geqslant 0} \lambda^n \Pi_n(x)$$

сходится

Можно показать,что $E(x)$ удовлетворяет разностному уравнению

$$\Delta E = \lambda \cdot E.$$

3. Перейдем к случаю геометрической прогрессии. Теперь переменная x пробегает множество

$$q^{\mathbf{Z}} = \{q^n \mid n \in \mathbf{Z}\}$$

Буква q в различных приложениях имеет разный смысл. Можно, например, считать ее еще одним независимым переменным, пробегающим вещественные или комплексные ненулевые значения; в другом коптексте q озпачает число элементов конечного поля. Есть теории, в которых q — корень из единицы. Наконец, можно считать q просто буквой и рассматривать многочлены, рациональные функции или формальные степенные ряды от q и q^{-1}.

Обозначим через D_q решеточную производную:

$$D_q f(x) := \frac{f(qx) - f(x)}{qx - x}. \qquad (1'')$$

Продолжая аналогию с п. 2, определим семейство многочленов $\{Q_n(x)\}_{n \geqslant 0}$ условиями:

$$DQ_0 = 0,$$
$$DQ_n = Q_{n-1} \text{ при } n \geqslant 1$$

и

$$Q_n(1) = \begin{cases} 1 & \text{при } n = 0, \\ 0 & \text{при } n \geqslant 1. \end{cases} \qquad (4'')$$

Можно показать, что

$$Q_n(x) = x^n/(n_q)!,$$

где $(n_q)! = 1_q \cdot 2_q \cdot \ldots \cdot n_q$, а

$$n_q = 1 + q + q^2 + \ldots + q^{n-1} = (q^n - 1)/(q - 1).$$

Таким образом, многочлены $Q_n(x)$ получаются из $P_n(x)$ заменой знаменателя $n!$ на его «квантовый аналог» (или q -аналог») $(n_q)!$, в то время как $\Pi_n(x)$ получались из $P_n(x)$ заменой числителя x^n на его решеточный аналог $x(x-h)(x-2h)\ldots(x-(n-1)h)$.

Рассмотрим теперь q -экспоненту

$$\exp_q(\lambda x) = \sum_{n\geqslant 0} \lambda^n \cdot Q_n(x). \tag{11}$$

Из определения $Q_n(x)$ легко выводится, что $\exp_q(\lambda x)$ удовлетворяет разностному уравнению

$$D_q \exp_q(\lambda x) = \lambda \cdot \exp_q(\lambda x). \tag{12}$$

которое можно переписать так:

$$\exp_q(qx) = \exp_q(x) \cdot (1 + (q-1)x).$$

Заменяя здесь x последовательно на $qx,\ q^2x,\ \ldots,\ q^{n-1}x$ и перемножая эти равенства, мы приходим к соотношению

$$\exp_q(q^n x) = \exp_q(x) \cdot \prod_{k=0}^{n-1} (1 + (q-1)q^k x).$$

Заметим, что в кольце формальных степенных рядов от q (а также, при малых q, в кольце аналитических функции от x) бесконечное произведение

$$\prod_{k=0}^{\infty} (1 + (q-1)\, q^k x)^{-1}$$

сходится и удовлетворяет тому же уравнению (12), что и $\exp_q(x)$, с тем же начальным условием $f(0)=1$. (Это рассуждение не вполне корректно, так как точка $x=0$ не лежит в множестве $q^{\mathbf{Z}}$. Однако этот пробел можно устранить.)

Поэтому

$$\exp_q(x) = \prod_{k=0}^{\infty} (1 + (q-1)\, q^k x)^{-1}.$$

Подставляя вместо x величину $x/(1-q)$, мы получаем тождество

$$\exp_q\left(\frac{x}{1-q}\right) = \prod_{k=0}^{\infty} (1 - q^k x)^{-1},$$

которое, если вспомнить определение $\exp_q(x)$, записывается в виде

$$\prod_{k=0}^{\infty} (1 - q^k x)^{-1} = \sum_{n\geqslant 0} \frac{x^n/(1-q)^n}{(n_q)!} = \sum_{n\geqslant 0} \frac{x^n}{(1-q)\ldots(1-q^{n-1})}. \tag{13}$$

Для многих элементарных и специальных функций обнаружены нетривиальные q-аналоги. Они естественно появляются в связи с квантовыми группами, теорией чисел, комбинаторикой и топологией. К сожалению, весь этот материал разбросан по многим статьям и препринтам, а частично существует в виде фольклора. Мы приведем

здесь лишь три интерпретации q-аналога биномиальных коэффициентов

$$\binom{n}{k}_q := \frac{(n_q)!}{(k_q)!\,(n-k)_q)!}.$$

1. Если q — число элементов конечного поля $\mathbf{F}_q$, то $\binom{n}{k}_q$ — число k-мерных пространств в n-мерном пространственад $\mathbf{F}_q$.
2. Если q — комплексное число, $|q|=1$, а u, v координатные функции квантового тора (см. 14.7), связанные соотношением $vu = quv$, то $\binom{n}{k}_q$ —коэффициент в разложении «квантового бинома»:

$$(u+v)^n = \sum_{k=0}^{n} \binom{n}{k}_q u^k \cdot v^{n-k}.$$

3. Пусть q — формальная переменная. Величина $\binom{n}{k}_q$ является многочленом степени $k(n-k)$ от q:

$$\binom{n}{k}_q = \sum_{s=0}^{k(n-k)} m^s_{n,k} \cdot q^s.$$

Оказывается, коэффициенты $m^s_{n,k}$ допускают следующую интерпретацию. Рассмотрим два пространства, в которых естественно действует симметрическая группа S_n: пространство $L^- = \Lambda^k(\xi_1, \xi_2, \ldots, \xi_n)$ однородных гармонических многочленов степени k от антикоммутирующщх переменных $\xi_1, \xi_2, \ldots, \xi_n$ и пространство $L^+ = \mathcal{H}^s_n(x_1, x_2, \ldots, x_n)$ однородных гармонических мпогочлепов степени s от обычных переменных $x_i, x_2, \ldots, x_n$. Термин «гармонический» здесь означает, что рассматриваемый многочлен аннулируется всеми S_n-инвариантными дифференциальными операторами вида

$$\Delta_k = \partial_1^k + \partial_2^k + \ldots + \partial_n^k,$$

где ∂_i означает оператор дифференцирования по i-й переменной, а в качестве k достаточно взять значения 1, 2, ..., n в случае L^+ и значение 1 в случае L^-. Пусть $\mathrm{Hom}_{S_n}(L^+, L^-)$ означает пространство линейных операторов из L^+ в L^-, перестановочных с действием S_n. Тогда

$$\dim \mathrm{Hom}_{S_n}(L^+, L^-) = m^s_{n,k}.$$

15. Классификатор гиперкомплексных чисел

Ниже будет приведена классификация гиперкомплексных чисел, предложенная Е.А.Каратаевым.

15.1. Принцип классификации. Введение.

Рассмотрим один из возможных вариантов классификации всего многообразия алгебр гиперкомплексных чисел и один из вариантов именования алгебр, предложенный Е.А.Каратаевым.

Классификатор разработан в качестве справочника по гиперкомплексным числам, в котором сделана попытка дать перечень наиболее часто встречающихся гиперкомплексных алгебр и их свойств.

В основу классификации положено строение алгебр на основе их образования путем удвоения по Кэли. Приводится не полный список алгебр, поскольку алгебр бесконечно много, а лишь некоторые из них, которые при этом имеют “удобные” свойства, такие как коммутативность, ассоциативность или альтернативность.

Для каждой алгебры приводится механизм ее образования, строение чисел алгебры, таблица произведений мнимых единиц и основные свойства. Для тех алгебр, которые хорошо изучены, приводятся дополнительные понятия, такие как выражение модуля числа через компоненты числа.

Классификатор может быть использован для выбора подходящей алгебры на основе известных свойств или на основе некоторых известных или требуемых свойств чисел. Классификатор не затрагивает вопросов функционального, дифференциального и интегрального анализов.

Часть терминов автор ввел самостоятельно ввиду того, что не встретил соответствующего термина ранее. К таким терминам относятся, в частности, термины “бикватернион”, “биоктава”, “паракватернион”.

При описании гиперкомплексных чисел даются обозначения мнимых единиц в виде латинских букв, повторяющиеся для различных алгебр. Следует иметь в виду, что смысл мнимых единиц для различных алгебр различен несмотря на схожесть их написания. Так, например, символы *i* для комплексных и паракомплексных чисел являются разными символами. Надеемся, что читатель не столкнется с разночтениями.

При знакомстве с приводимым классификатором у читателя может возникнуть недоумение, вызванное довольно большим количеством рассматриваемых алгебр и отсутствием упоминания большинства из них в теоремах Фробениуса и Гурвица. Дело в том, что Фробениус в своих работах сознательно сузил круг рассматриваемых им алгебр алгебрами без делителей нуля. И в начале доказательства теоремы о четырех алгебрах и в ходе ее он неоднократно указывал на этот факт. Алгебр же, не содержащих делителей нуля, действительно четыре - действительные числа, комплексные числа, кватернионы и октавы.

15.2. Комплексные числа.

Комплексным числом называется число алгебры, полученной удвоением по Кэли алгебры действительных чисел:

$$Q = D_1 + E \cdot D_2$$

с мнимой единицей удвоения $E^2 = -1$.

Здесь обозначены: D_1, D_2 - представители алгебры действительных чисел, E - мнимая единица удвоения алгебр, Q - представитель алгебры комплексных чисел.

Алгебра комплексных чисел отличается широкой применимостью в математике и моделировании благодаря своим свойствам. Эта алгебра, одновременно с тем и благодаря тому, очень хорошо изучена.

Комплексное число представимо в виде набора из двух действительных чисел (x, y). Для комплексных чисел определены операции сложения, вычитания, умножения и деления.

Сложение и вычитание комплексных чисел определены покомпонентно:

суммой чисел (x_1,y_1) и (x_2,y_2) является комплексное число (x_1+x_2, y_1+y_2), а разностью - комплексное число (x_1-x_2, y_1-y_2).

Следует отметить, что определение сложения и вычитания как покомпонентных операций относится ко всем без исключения гиперкомплексным числам.

Для того, чтобы было удобнее оперировать компонентами гиперкомплексных чисел и не путать их запись с записью векторов, используются так называемые покомпонентные формы записи в мнимом базисе. За единицы базиса принимаются мнимые единицы, соответствующие компонентам. Так, комплексные числа обычно записывают в виде:

$$z = a + i \cdot b$$

Здесь через *i* обозначена мнимая единица, a и b - значения компонент. При этом часть a называют действительной частью, а часть b - мнимой. Эти названия сложились исторически. И, хотя они не совсем точно отражают понятия, мы по-прежнему будем ими пользоваться.

Для гиперкомплексных чисел умножение одного числа на другое задается таблицей произведений базисных единиц. Для комплексных чисел такая таблица имеет вид:

	1	i
1	1	i
i	i	-1

Для комплексных чисел определена операция сопряжения. В отличие от иных гиперкомплексных чисел сопряжение комплексных чисел имеет единственную форму, поэтому вид сопряжения не указывается. То же самое относится к паракомплексным и дуальным числам. Мы будем полагать, что это сопряжение является одновременно и

скалярным и алгебраическим. К сожалению, тот факт, что для этих чисел сопряжения совпадают, может вносить как терминологическую, так и идеологическую путаницу при использовании в формулах и иногда может приводить к неверным выводам, например когда начальная посылка вывода опирается на сопряжение как алгебраическое, но в ходе вывода алгебраическое сопряжение может быть трактовано как скалярное.

Комплексное число z_2, сопряженное заданному комплексному числу z_1, выражается покомпонентно как:

если

$$z_1 = a + i \cdot b,$$

то

$$z_2 = a - i \cdot b.$$

Операция сопряжения обозначается как:

$$z_2 = \overline{z_1}$$

Произведение комплексного числа на сопряженное ему дает комплексное число, имеющее ненулевой только действительную часть. Если сопряжение считать алгебраическим, то результат такого произведения называют квадратом модуля комплексного числа. Модуль комплексного числа обозначается как:

$$|z|^2 = z \cdot \bar{z} = \bar{z} \cdot z$$

Модуль комплексного числа обладает свойством мультипликативности - модуль произведения чисел равен произведению их модулей.

В компонентах комплексного числа модуль выражается как:

$$|z| = \sqrt{a^2 + b^2}$$

Таким образом, модуль существует для любого комплексного числа.

Свойства комплексных чисел:

1) комплексные числа коммутативны по сложению и по умножению.

$$z_1 + z_2 = z_2 + z_1$$

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

2) комплексные числа ассоциативны по сложению и по умножению.

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

3) комплексные числа дистрибутивны.

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$$

Для комплексных чисел операция деления определена как операция обратная операции умножения. Если $z = \frac{z_1}{z_2}$, то z является решением уравнения $z \cdot z_2 = z_1$. Решим это уравнение, домножив левую и правую часть на $\overline{z_2}$ и разделив обе части на квадрат модуля. Получим, что

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}} = \frac{z_1 \cdot \overline{z_2}}{|z_2|^2}$$

Дополнительные замечания.

Для комплексных чисел широко известна формула Эйлера, представляющая собой операцию возведения действительного числа в степень комплексное число:

$$e^{a+i\cdot b} = e^{a}\cdot\left(\cos(b)+i\cdot\sin(b)\right)$$

Данное выражение широко используется при представлении комплексного числа в виде вектора на комплексной плоскости.

Тот факт, что представление комплексных чисел при возведении в степень тригонометрично, широко используется в интегральном и дифференциальном исчислении в теме “конформные отображения”.

При использовании в качестве операторов преобразования пространства комплексных чисел с величиной $a = 0$ такая форма оператора эквивалентна пространственному повороту на угол b:

$$e^{i\cdot\varphi}\cdot(x+i\cdot y) = \left(\cos(\varphi)+i\cdot\sin(\varphi)\right)\cdot(x+i\cdot y) =$$

$$= \cos(\varphi)\cdot x - \sin(\varphi)\cdot y + i\cdot\left(\sin(\varphi)\cdot x + \cos(\varphi)\cdot y\right)$$

15.3. Паракомплексные числа.

Паракомплексным числом называется число алгебры, полученной удвоением по Кэли алгебры действительных чисел:

$$Q = D_1 + E\cdot D_2$$

с мнимой единицей удвоения $E^2 = 1$.

Здесь обозначены: D_1, D_2 - представители алгебры действительных чисел, E - мнимая единица удвоения алгебр, Q - представитель алгебры паракомплексных чисел.

Мнимые единицы удвоения алгебр $E^2 = 1$ и $E^2 = 0$, в отличие от "классической" мнимой единицы $E^2 = -1$, применяются очень редко и считаются экзотическими, хотя все три, с точки зрения алгебры, имеют равное "право на жизнь".

Обозначим через *i* мнимую единицу паракомплексных чисел. Не следует ее путать с мнимой единицей комплексных чисел. Тогда по аналогии с комплексными числами паракомплексное число может быть записано покомпонентно:

$$z = a + i \cdot b$$

Точно также, как и для комплексных чисел, часть a называется действительной, а часть b - мнимой.

Таблица умножения паракомплексных чисел имеет вид:

	1	i
1	1	i
i	i	1

Для паракомплексных чисел, также как и для комплексных, определена операция сопряжения, которая одновременно является и алгебраическим и скалярным сопряжением.

Паракомплексное число z_2, сопряженное заданному паракомплексному числу z_1, выражается покомпонентно как:

если

$$z_1 = a + i \cdot b,$$

то

$$z_2 = a - i \cdot b .$$

Операция сопряжения обозначается как:

$$z_2 = \overline{z_1}$$

Произведение паракомплексного числа на сопряженное ему дает паракомплексное число, состоящее из только действительной части. Если сопряжение считать алгебраическим, то результат такого произведения называют квадратом модуля паракомплексного числа. Модуль паракомплексного числа обозначается как:

$$|z|^2 = z \cdot \bar{z} = \bar{z} \cdot z$$

Модуль паракомплексного числа обладает свойством мультипликативности - модуль произведения чисел равен произведению их модулей. В компонентах паракомплексного числа модуль выражается как:

$$|z| = \sqrt{a^2 - b^2}$$

Таким образом, модуль может быть вычислен для любого паракомплексного числа.

Свойства паракомплексных чисел:

1) паракомплексные числа коммутативны по сложению и по умножению.

$$z_1 + z_2 = z_2 + z_1$$

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

2) паракомплексные числа ассоциативны по сложению и по умножению.

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

3) паракомплексные числа дистрибутивны.

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$$

Алгебра паракомплексных чисел есть алгебра с делителями нуля. А именно - существуют такие паракомплексные числа, для которых не существует обратных, если обратное число определено как:

$$z\, z_{обр} = 1$$

В силу того, что для некоторого подмножества паракомплексных чисел, не равных 0, их модуль равен нулю, при вычислении обратного возникает операция деления на 0. В подмножество таких чисел входят паракомплексные числа, для которых

$$a^2 - b^2 = 0,$$

или

$$a = \pm b$$

Таким образом, подмножество делителей нуля в паракомплексных числах состоит из двух непересекающихся подмножеств:

$$z = a + i \cdot a$$

и

$$z = a - i \cdot a$$

где a - действительное число.

Данные два подмножества обладают весьма интересными особенностями, в которых несложно убедиться самостоятельно:

1) любое число из этих подмножеств представимо в нормализованном виде:

$$z = a \cdot \left(\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2} i \right)$$

Таким образом, делитель нуля в паракомплексных числах состоит из некоторой действительной константы и “ядра”.

2) эти два подмножества аналогичны по своему проявлению квантовым спиновым состояниям - существует естественное разделение на два изоморфных подмножества, различающиеся только знаком условной величины: + или -.

3) квадрат “ядра” есть само это “ядро”, то есть “ядра” делителей нуля в паракомплексных числах являются идемпотентами.

Идемпотентом называется такое число *p*, что существует натуральное число *n*, начиная с которого справедливо равенство $p^n = p$. Нильпотентом называется такое число *p*, что существует такое натуральное число *n*, начиная с которого справедливо равенство $p^n = 0$.

4) Результат произведения двух паракомплексных чисел, одно из которых входит в положительное или отрицательное подмножество делителей нуля, также входит в это положительное или отрицательное подмножество делителей нуля.

5) Результат произведения чисел, одно из которых принадлежит положительному подмножеству делителей нуля, а другое - отрицательному, есть ноль.

6) любое паракомплексное число представимо в виде линейной суперпозиции в базисе ядер делителей нуля:

$$z = x \cdot \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i \right) + y \cdot \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i \right)$$

Если же паракомплексное число не является делителем нуля, то операция деления на него определена так же, как и для комплексных чисел:

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}} = \frac{z_1 \cdot \overline{z_2}}{|z_2|^2}$$

Дополнительные замечания.

Для паракомплексных чисел, также как и для комплексных, можно составить аналог формулы Эйлера. Разложив экспоненциальный ряд и приведя подобные, получим, что:

$$e^{a+i \cdot b} = e^a \cdot \left(ch(b) + i \cdot sh(b) \right)$$

Поскольку $ch(x) \neq sh(x)$ при любом действительном *x*, результат взятия экспоненты от любого паракомплексного числа не является идемпотентом. Откуда следует, что для любого паракомплексного числа - неидемпотента существует его логарифм как решение формулы Эйлера для паракомплексных чисел.

При использовании паракомплексных чисел в качестве операторов преобразования пространства при $a = 0$ умножение на такой оператор эквивалентен гиперболическому повороту в условном двумерном “пространстве - времени Минковского”, сохраняющему величину $a^2 - b^2$:

$$e^{i \cdot \psi} \cdot (a + i \cdot b) = \left(ch(\psi) + i \cdot sh(\psi) \right) \cdot (a + i \cdot b) =$$

$$= ch(\psi) \cdot a + sh(\psi) \cdot b + i \cdot \left(sh(\psi) \cdot a + ch(\psi) \cdot b \right)$$

15.4. Дуальные числа.

Дуальным числом называется число алгебры, полученной удвоением по Кэли алгебры действительных чисел:

$$Q = D_1 + E \cdot D_2$$

с мнимой единицей удвоения $E^2 = 0$.

Здесь обозначены: D_1, D_2 - представители алгебры действительных чисел, E - мнимая единица удвоения алгебр, Q - представитель алгебры дуальных чисел.

Часто в литературе, использующей дуальные числа, мнимая единица дуальных чисел обозначается символом ε. Мы так же будем следовать этому соглашению.

Таким образом, дуальное число может быть записано покомпонентно следующим образом:

$$z = a + \varepsilon \cdot b$$

Таблица умножения дуальных чисел имеет вид:

	1	ε
1	1	ε
ε	ε	0

Дуальная мнимая единица выглядит еще более экзотичнее чем мнимая единица паракомплексных чисел - сама не равная нулю, в квадрате дает ноль. Таким образом, она должна быть в соответствии с ее определением отнесена к нильпотентам.

Для дуальных чисел определена операция сопряжения, которая одновременно является и алгебраическим и скалярным сопряжением.

Дуальное число z_2, сопряженное заданному дуальному числу z_1, выражается покомпонентно как:

если

$$z_1 = a + \varepsilon \cdot b,$$

то

$$z_2 = a - \varepsilon \cdot b.$$

Операция сопряжения обозначается как:

$$z_2 = \overline{z_1}$$

Для дуальных чисел дополнительно алгебраическому, скалярному и векторному сопряжениям, определено дуальное сопряжение. Для дуальных чисел дуальное сопряжение совпадает по форме с алгебраическим.

Произведение дуального числа на сопряженное ему дает дуальное число, имеющее ненулевой только действительную часть. Если сопряжение считать алгебраическим, то результат такого произведения называют квадратом модуля дуального числа. Модуль дуального числа обозначается как:

$$|z|^2 = z \cdot \bar{z} = \bar{z} \cdot z$$

Модуль дуального числа обладает свойством мультипликативности - модуль произведения чисел равен произведению их модулей. В компонентах дуального числа модуль выражается как:

$$|z| = \sqrt{a^2}$$

Таким образом, модуль существует для любого дуального числа.

Свойства дуальных чисел:

1) дуальные числа коммутативны по сложению и по умножению.

$$z_1 + z_2 = z_2 + z_1$$

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

2) дуальные числа ассоциативны по сложению и по умножению.

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

3) дуальные числа дистрибутивны.

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$$

Для дуальных чисел операция деления определена как операция обратная операции умножения. Если $z = \frac{z_1}{z_2}$, то z является решением уравнения $z \cdot z_2 = z_1$. Решим это уравнение, домножив левую и правую часть на $\overline{z_2}$ и разделив обе части на квадрат модуля. Получим, что

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}} = \frac{z_1 \cdot \overline{z_2}}{|z_2|^2}$$

Таким образом, любое дуальное число с ненулевой действительной частью имеет обратное себе. Приведенное правило вычисления деления требует, чтобы делитель обязательно имел ненулевую недуальную часть.

Дополнительные замечания.

Для дуальных чисел, как и для комплексных и для паракомплексных, можно составить аналог формулы Эйлера. Разложив в экспоненциальный ряд и приведя подобные, получим что:

$$e^{a+\omega\cdot b} = e^{a}\cdot\left(1+\omega\cdot b\right)$$

Частным случаем дуального числа является число с $a = 0$. При этом

$$e^{\omega\cdot b} = 1+\omega\cdot b$$

что при использовании дуальных чисел в качестве операторов преобразования пространства реализует сдвиг пространства на величину b:

$$e^{\omega\cdot b}\cdot\left(x+\omega\cdot y\right) = \left(1+\omega\cdot b\right)\cdot\left(x+\omega\cdot y\right) = x+\omega\cdot\left(b\cdot x+y\right)$$

15.5. Бикомплексные числа.

Бикомплексным числом называется число алгебры, полученной удвоением по Кэли алгебры комплексных чисел:

$$B = Q_1 + E\cdot Q_2$$

с мнимой единицей удвоения $E^2 = -1$.

Здесь обозначены: Q_1, Q_2 - представители алгебры комплексных чисел, E - мнимая единица удвоения алгебр, B - представитель алгебры бикомплексных чисел. При этом мнимая единица удвоения при образовании бикомплексных чисел определена как коммутирующая по умножению с мнимой единицей, входящей в исходные комплексные числа.

Для различения двух мнимых единиц обозначим одну как i, а вторую как $\dot{i}$. Тогда бикомплексное число может быть записано в виде:

$$B = q_0 + \dot{i}\cdot i\cdot q_1 + i\cdot q_2 + \dot{i}\cdot q_3$$

В этом обозначении компонента q_0 называется действительной частью, а компоненты q_1, q_2, q_3 - мнимыми.

Сложение и вычитание бикомплексных чисел определено покомпонентно. В силу того, что при удвоении алгебры комплексных чисел мнимая единица удвоения коммутирует с мнимой единицей комплексных чисел, таблица произведений бикомплексных чисел определяется как:

	1	$\dot{i}\,i$	i	$\dot{i}$
1	1	$\dot{i}\,i$	i	$\dot{i}$
$\dot{i}\,i$	$\dot{i}\,i$	1	$-\dot{i}$	$-i$
i	i	$-\dot{i}$	-1	$\dot{i}\,i$
$\dot{i}$	$\dot{i}$	$-i$	$\dot{i}\,i$	-1

Для бикомплексных чисел существует три вида сопряжения - алгебраическое, скалярное и векторное. Но в силу того, что скалярное и векторное сопряжения для бикомплексных чисел совпадают с точностью до перестановки компонент, выбор формы скалярного и векторного произведения может показаться необоснованным и содержащим произвол выбора.

Правило построения сопряжений:

1) для образования бикомплексного числа, алгебраически сопряженного заданному, следует решить уравнение вида:

$$B \cdot \overline{B} = M$$

Где *M* - квадрат модуля этого числа.

Алгебраическое сопряжение обозначается как $\overline{q}$.

Замечание:

Для определения алгебраически сопряженного числа используется определение модуля, в то время как для определения модуля используется алгебраическое сопряжение. Формально эти определения логически зациклены, но пока не найдено ничего лучшего. В случае, если будет найдено более удачное построение определений, будет осуществлена корректировка данного классификатора. В классических курсах аглебр используется применение скалярного произведения для определения модуля. Но само понятие скалярного произведения для гиперкомплексных чисел пока не определено убедительным и вообще возможным к какому либо использованию.

2) для образования бикомплексного числа, скалярно сопряженного заданному бикомплексному числу, следует сменить знаки у компонент, в образовании которых использовалась мнимая единица $\dot{i}$, считая мнимую единицу $\dot{i}\,i$ “составной” мнимой единицей.

Так, для бикомплексного числа $q_0 + \dot{i} \cdot i \cdot q_1 + i \cdot q_2 + \dot{i} \cdot q_3$ скалярно сопряженное ему число будет $q_0 - \dot{i} \cdot i \cdot q_1 + i \cdot q_2 - \dot{i} \cdot q_3$.

Скалярное сопряжение обозначается штрихом: q'.

3) для образования бикомплексного числа, векторно сопряженного заданному бикомплексному числу, следует сменить знаки у компонент, в образовании которых использовалась мнимая единица *i*, считая мнимую единицу $\dot{i}\,i$ “составной” мнимой единицей.

Так, для бикомплексного числа $q_0 + \dot{i} \cdot i \cdot q_1 + i \cdot q_2 + \dot{i} \cdot q_3$ векторно сопряженное ему число будет $q_0 - \dot{i} \cdot i \cdot q_1 - i \cdot q_2 + \dot{i} \cdot q_3$.

Векторное сопряжение обозначается тильдой: $\tilde{q}$.

Применение сопряжений перестановочно. Не важен порядок, в котором применяется одновременно несколько разных сопряжений.

Четное применение сопряжений одного вида не изменяет результат.

Наиболее сложным в сопряжениях бикомплексных чисел является определение алгебраически сопряженного числа, поскольку эта функция существенно нелинейна относительно компонент. Правило определения алгебраического сопряжения будет приведено ниже после определения необходимых свойств бикомплексных чисел.

Сложение и вычитание бикомплексных чисел определено покомпонентно. Также покомпонентно определено умножение и деление бикомплексного числа на действительное число.

Свойства бикомплексных чисел:

1) бикомплексные числа коммутативны по сложению и по умножению.

$$q_1 + q_2 = q_2 + q_1$$

$$q_1 \cdot q_2 = q_2 \cdot q_1$$

2) бикомплексные числа ассоциативны по сложению и по умножению.

$$(q_1 + q_2) + q_3 = q_1 + (q_2 + q_3)$$

$$(q_1 \cdot q_2) \cdot q_3 = q_1 \cdot (q_2 \cdot q_3)$$

3) бикомплексные числа дистрибутивны.

$$q_1 \cdot (q_2 + q_3) = q_1 \cdot q_2 + q_1 \cdot q_3$$

Далее мы используем тот факт, что $e^{A+B} = e^A \cdot e^B = e^B \cdot e^A$, если *A* и *B* коммутируют по сложению и умножению.

Для определения правила получения алгебраического сопряжения найдем экспоненту от бикомплексного числа:

$$\exp(q_0 + \dot{i} \cdot i \cdot q_1 + i \cdot q_2 + \dot{i} \cdot q_3)$$

$$= \exp(q_0) \cdot \exp\left(\dot{i} \cdot i \cdot q_1\right) \cdot \exp(i \cdot q_2) \cdot \exp\left(\dot{i} \cdot q_3\right)$$

$$\exp\left(\dot{i} \cdot i \cdot q_1\right) = ch(q_1) + \dot{i} \cdot i \cdot sh(q_1),$$

$$\exp(i \cdot q_2) = \cos(q_2) + i \cdot \sin(q_2),$$

$$\exp\left(\dot{i} \cdot q_3\right) = \cos(q_3) + \dot{i} \cdot \sin(q_3)$$

После решения уравнения $e^q = Q$ относительно *q* получаем логарифм бикомплексного числа. У полученного логарифма меняем знаки у всех компонент при мнимых единицах и вычисляем экспоненту от полученного результата.

Несложно видеть, что

$$\exp(q_0 + \dot{i} \cdot i \cdot q_1 + i \cdot q_2 + \dot{i} \cdot q_3) \cdot \exp(q_0 - \dot{i} \cdot i \cdot q_1 - i \cdot q_2 - \dot{i} \cdot q_3) = \exp(2 \cdot q_0)$$

В такой записи $\exp(q_0)$ будет являться модулем бикомплексного числа. Или, приняв обозначение функции взятия действительной части как Re, получим выражение для модуля бикомплексного числа:

$$|Q| = \exp\left(\mathrm{Re}\left(\ln(Q)\right)\right)$$

Это выражение и будем в дальнейшем считать концептуальным определением модуля гиперкомплексного числа.

Найдем выражение для модуля бикомплексного числа. Умножим число на векторно сопряженное ему:

$$\exp(q_0 + i\cdot i\cdot q_1 + i\cdot q_2 + i\cdot q_3)\cdot\exp(q_0 - i\cdot i\cdot q_1 + i\cdot q_2 - i\cdot q_3) = \exp(2\cdot q_0 - 2\cdot i\cdot q_2)$$

Результат умножим на скалярно сопряженный ему:

$$\exp(2\cdot q_0 + 2\cdot i\cdot q_2)\cdot\exp(2\cdot q_0 - 2\cdot i\cdot q_2) = \exp(4\cdot q_0)$$

В результате получим модуль исходного числа в четвертой степени. Проведя те же операции не в экспоненциальной форме, а в компонентной, получим:

$$|q|^4 = x_0^4 + x_1^4 + x_2^4 + x_3^4 - 2\cdot x_0^2\cdot x_1^2 + 2\cdot x_0^2\cdot x_3^2 + 2\cdot x_0^2\cdot x_2^2 +$$
$$+2\cdot x_1^2\cdot x_2^2 + 2\cdot x_1^2\cdot x_3^2 - 2\cdot x_2^2\cdot x_3^2 + 8\cdot x_0\cdot x_1\cdot x_2\cdot x_3$$

Выводы:

1) Модуль бикомплексного числа существует и может быть вычислен для любого бикомплексного числа.

2) В гиперкомплексных алгебрах, в которых векторное, скалярное и алгебраическое сопряжения не совпадают, модуль числа определяется не квадратичной формой компонент, а формой четвертой степени.

3) Для гиперкомплексных алгебр, в которых векторное, скалярное и алгебраическое сопряжения не совпадают, число, алгебраически сопряженное заданному, выражается через компоненты исходного числа существенно нелинейно.

Алгебра бикомплексных чисел, как и алгебра паракомплексных чисел, содержит делители нуля. Поэтому не для любого бикомплексного числа может быть вычислено число, обратное ему. Как и для паракомплексных чисел, делители нуля в бикомплексных числах образуют два подмножества:

$$Q = a \cdot \left(\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2} \cdot \dot{i} \cdot i \right),$$

где a - бикомплексное число. И, также как для паракомплексных чисел, бикомплексное число может быть представлено в виде линейной комбинации делителей нуля:

$$Q = a \cdot \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} \cdot \dot{i} \cdot i \right) + b \cdot \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} \cdot \dot{i} \cdot i \right),$$

где a и b - бикомплексные числа.

Операция деления бикомплексного числа на бикомплексное число определена так же как и для комплексных чисел: операция деления определена как операция, обратная операции умножения. Если $q = \frac{q_1}{q_2}$, то q является решением уравнения $q \cdot q_2 = q_1$. Решим это уравнение, домножив левую и правую часть на $\overline{q_2}$ и разделив обе части на квадрат модуля. Получим, что

$$\frac{q_1}{q_2} = \frac{q_1 \cdot \overline{q_2}}{q_2 \cdot \overline{q_2}} = \frac{q_1 \cdot \overline{q_2}}{|q_2|^2}$$

Отметим, что эта формула накладывает естественное ограничение на делитель - он не должен быть делителем нуля.

15.6. Дуальные комплексные числа.

Дуальным комплексным числом называется число алгебры, полученной удвоением по Кэли алгебры комплексных чисел:

$$D = C_1 + E \cdot C_2$$

с мнимой единицей удвоения $E^2 = 0$.

Здесь обозначены: C_1, C_2 - представители алгебры комплексных чисел, E - мнимая единица удвоения алгебр, D - представитель алгебры дуальных комплексных чисел.

Дуальное комплексное число может быть записано покомпонентно следующим образом:

$$q = q_0 + i \cdot \omega \cdot q_1 + i \cdot q_2 + \omega \cdot q_3$$

где через $i \cdot \omega$ обозначена составная мнимая единица.

Таблица умножения единиц дуальных комплексных чисел имеет вид:

	1	$i \cdot \omega$	i	ω
1	1	$i \cdot \omega$	i	ω
$i \cdot \omega$	$i \cdot \omega$	0	$-\omega$	0
i	i	$-\omega$	-1	$i \cdot \omega$
ω	ω	0	$i \cdot \omega$	0

Для дуальных комплексных чисел применимы три вида сопряжения - алгебраическое, скалярное и дуальное. Для числа $q = q_0 + i \cdot \varpi \cdot q_1 + i \cdot q_2 + \varpi \cdot q_3$ сопряженные ему числа будут иметь вид:

1) скалярное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых использована единица *i*:

$$q' = q_0 - i \cdot \varpi \cdot q_1 - i \cdot q_2 + \varpi \cdot q_3$$

2) дуальное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых использована единица ϖ:

$$\hat{q} = q_0 - i \cdot \varpi \cdot q_1 + i \cdot q_2 - \varpi \cdot q_3$$

3) алгебраическое сопряжение, образованное сменой знаков у компонент при всех мнимых единицах:

$$\bar{q} = q_0 - i \cdot \varpi \cdot q_1 - i \cdot q_2 - \varpi \cdot q_3$$

Квадрат модуля дуального комплексного числа образуется как:

$$|q|^2 = q \cdot \bar{q} = \bar{q} \cdot q = q_0^2 + q_2^2$$

Таким образом, модуль существует для любого дуального комплексного числа.

Свойства дуальных комплексных чисел:

1) дуальные комплексные числа коммутативны по сложению и по умножению.

$$z_1 + z_2 = z_2 + z_1$$

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

2) дуальные комплексные числа ассоциативны по сложению и по умножению.

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

3) дуальные комплексные числа дистрибутивны.

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$$

Для дуальных комплексных чисел операция деления определена как операция обратная операции умножения. Если $z = \frac{z_1}{z_2}$, то z является решением уравнения $z \cdot z_2 = z_1$. Решим это уравнение, домножив левую и правую часть на $\overline{z_2}$ и разделив обе части на квадрат модуля. Получим, что

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}} = \frac{z_1 \cdot \overline{z_2}}{|z_2|^2}$$

Таким образом, любое дуальное комплексное число с хотя бы одной ненулевой компонентой q_0, q_2 имеет обратное себе.

Дополнительные замечания.

Для дуальных комплексных чисел можно составить аналог формулы Эйлера. Разложив в экспоненциальный ряд и приведя подобные, получим:

$$\exp(q_0 + i \cdot \varpi \cdot q_1 + i \cdot q_2 + \varpi \cdot q_3) = \exp(q_0) \cdot (\cos(q_2) + i \cdot \sin(q_2)) \cdot (1 + \varpi \cdot (q_3 + i \cdot q_1))$$

15.7. Дуальные бикомплексные числа.

Дуальным бикомплексным числом называется число алгебры, полученной удвоением по Кэли алгебры бикомплексных чисел:

$$B = C_1 + \varpi \cdot B_2$$

с мнимой единицей удвоения $\varpi^2 = 0$.

Здесь обозначены: C_1, C_2 - представители алгебры бикомплексных чисел, ϖ- мнимая единица удвоения алгебр, B - представитель алгебры дуальных бикомплексных чисел.

Дуальное комплексное число может быть записано покомпонентно следующим образом:

$$q = q_0 + i \cdot \dot{i} \cdot q_1 + i \cdot q_2 + \dot{i} \cdot q_3 + \omega \cdot q_4 + i \cdot \dot{i} \cdot \omega \cdot q_5 + i \cdot \omega \cdot q_6 + \dot{i} \cdot \omega \cdot q_7$$

где через $i \cdot \omega$, $i \cdot \dot{i}$, $i \cdot \dot{i} \cdot \omega$ и др. при компонентах q_i обозначены составные мнимые единицы.

Таблица умножения мнимых единиц дуальных бикомплексных чисел является аналогом таблицы умножения мнимых единиц бикомплексных чисел с тем отличием, что произведение любых мнимых единиц, в образовании которых участвовала мнимая единица ϖ, равно нулю.

Свойства дуальных бикомплексных чисел повторяют свойства бикомплексных чисел. Для них также определены скалярное, векторное, алгебраическое и дуальное сопряжения, образующиеся сменой знаков у соответствующих мнимых единиц. В силу громоздкости и очевидности формул они не приводятся.

1) скалярное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых использована единица $\dot{i}$.

2) векторное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых использована единица *i*.

3) дуальное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых использована мнимая единица ε.

4) алгебраическое сопряжение, образованное сменой знаков у всех мнимых единиц.

Квадрат модуля дуального комплексного числа вычисляется по тем же правилам, что и любого другого дуального гиперкомплексного числа - вычисляется модуль числа с отброшенной дуальной частью, частью, в образовании мнимых единиц которой использовалась мнимая единица ε.

Свойства дуальных бикомплексных чисел:

1) дуальные бикомплексные числа коммутативны по сложению и по умножению.

$$z_1 + z_2 = z_2 + z_1$$

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

2) дуальные бикомплексные числа ассоциативны по сложению и по умножению.

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

3) дуальные бикомплексные числа дистрибутивны.

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$$

Для дуальных бикомплексных чисел операция деления определена как операция обратная операции умножения. Если $z = \frac{z_1}{z_2}$, то z является решением уравнения $z \cdot z_2 = z_1$. Решим это уравнение, домножив левую и правую часть на $\overline{z_2}$ и разделив обе части на квадрат модуля. Получим, что

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}} = \frac{z_1 \cdot \overline{z_2}}{|z_2|^2}$$

Дополнительные замечания.

Дуальные бикомплексные числа являются наиболее размерной коммутативной алгеброй из рассматриваемых в этом классификаторе. Дальнейшие операции удвоения этой алгебры дают либо некоммутативную алгебру, либо алгебру, изоморфную алгебре дуальных бикомплексных чисел.

15.8. Дуальные паракомплексные числа.

Дуальным паракомплексным числом называется число алгебры, полученной удвоением по Кэли алгебры паракомплексных чисел с мнимой единицей удвоения $\varpi^2 = 0$:

$$D = P_1 + \varpi \cdot P_2$$

Здесь обозначены: P_1, P_2 - представители алгебры паракомплексных чисел, ϖ- мнимая единица удвоения, D - представитель алгебры дуальных паракомплексных чисел.

Дуальное паракомплексное число может быть записано покомпонентно следующим образом:

$$q = q_0 + i \cdot \varpi \cdot q_1 + i \cdot q_2 + \varpi \cdot q_3$$

где через $i \cdot \omega$ обозначена составная мнимая единица.

Таблица умножения единиц дуальных паракомплексных чисел имеет вид:

	1	$i \cdot \omega$	i	ω
1	1	$i \cdot \omega$	i	ω
$i \cdot \omega$	$i \cdot \omega$	0	ω	0
i	i	ω	1	$i \cdot \omega$
ω	ω	0	$i \cdot \omega$	0

Для дуальных паракомплексных чисел применимы три вида сопряжения - алгебраическое, скалярное и дуальное. Для числа $q = q_0 + i \cdot \omega \cdot q_1 + i \cdot q_2 + \omega \cdot q_3$ сопряженные ему паракомплексные числа будут иметь вид:

1) скалярное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых использована единица *i*:

$$q' = q_0 - i \cdot \omega \cdot q_1 - i \cdot q_2 + \omega \cdot q_3$$

2) дуальное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых использована единица ω:

$$\hat{q} = q_0 - i \cdot \omega \cdot q_1 + i \cdot q_2 - \omega \cdot q_3$$

3) алгебраическое сопряжение, образованное сменой знаков у компонент при всех мнимых единицах:

$$\bar{q} = q_0 - i \cdot \omega \cdot q_1 - i \cdot q_2 - \omega \cdot q_3$$

Квадрат модуля дуального паракомплексного числа образуется как:

$$|q|^2 = q \cdot \bar{q} = \bar{q} \cdot q = q_0^2 + q_2^2$$

Таким образом, модуль существует для любого дуального паракомплексного числа.

Свойства дуальных паракомплексных чисел:

1) дуальные паракомплексные числа коммутативны по сложению и по умножению.

$$z_1 + z_2 = z_2 + z_1$$

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

2) дуальные паракомплексные числа ассоциативны по сложению и по умножению.

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

3) дуальные паракомплексные числа дистрибутивны.

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$$

Для дуальных паракомплексных чисел операция деления определена как операция обратная операции умножения. Если $z = \frac{z_1}{z_2}$, то z является решением уравнения $z \cdot z_2 = z_1$. Решим это уравнение, домножив левую и правую часть на $\overline{z_2}$ и разделив обе части на квадрат модуля. Получим, что

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}} = \frac{z_1 \cdot \overline{z_2}}{|z_2|^2}$$

Таким образом, любое дуальное паракомплексное число с хотя бы одной ненулевой компонентой q_0, q_2 имеет обратное себе.

Дополнительные замечания.

Для дуальных паракомплексных чисел можно составить аналог формулы Эйлера. Разложив в экспоненциальный ряд и приведя подобные, получим:

$$\exp(q_0 + i \cdot \varpi \cdot q_1 + i \cdot q_2 + \varpi \cdot q_3) = \exp(q_0) \cdot (ch(q_2) + i \cdot sh(q_2)) \cdot (1 + \varpi \cdot (q_3 + i \cdot q_1))$$

Дуальные паракомплексные числа могут быть использованы в моделировании преобразований двумерного пространства. Если сопоставить одному из измерений условного пространства компоненту q_3, а другому - компоненту q_1, то умножение такого вектора на дуальное паракомплексное число может рассматриваться как умножение на оператор преобразования. При этом в таком операторе преобразования будет присутствовать гиперболический поворот и сдвиг в условном пространстве. Гиперболический поворот будет оставлять неизменной величину $q_3^2 - q_1^3$.

15.9. Кватернионы.

Кватернионом называется число гиперкомплексной алгебры, полученной некоммутативным удвоением по Кэли алгебры комплексных чисел:

$$Q = K_1 + j \cdot K_2$$

С мнимой единицей удвоения $j^2 = -1$.

Здесь обозначены: K_1, K_2 - представители алгебры комплексных чисел, *j* - мнимая единица удвоения алгебр, *Q* - представитель алгебры кватернионов. Мнимая единица удвоения *j* не коммутирует по умножению с мнимой единицей исходной комплексной алгебры *i* и при умножении на нее образует третью мнимую единицу, обозначаемую как *k*. Таблица произведений единиц кватернионов имеет вид:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Данный закон умножения определен как правый закон умножения. Так же можно определить кватернионы с левым законом умножения. Отличие левых кватернионов от правых кватернионов состоит в результате произведения мнимых частей. В большинстве случаев при рассмотрении алгебры кватернионов пользуются определением кватерниона как правого кватерниона. Мы так же будем следовать этому соглашению.

Исторически сложилось так, что в силу относительной простоты устройства чисел наиболее известными представителями гиперкомплексых алгебр являются комплексные числа и кватернионы. При этом многие математики рассматривают кватернионы не столько как гиперкомплексные числа как таковые, сколько как самостоятельные объекты с законом умножения, определенным так же как и закон умножения кватернионов. При этом зачастую определяются кватернионы не только над полем действительных чисел, но и над другими полями.

Для кватернионов, как и для других гиперкомплексных чисел, определены операции сложения, вычитания, умножения и деления. Операции сложения и вычитания кватернионов определены покомпонентно. Умножение кватернионов полностью определяется

законом умножения их мнимых единиц, заданным таблицей произведения единиц кватернионов, приведенной выше.

Операций сопряжения для кватернионов определено три - скалярное сопряжение, векторное сопряжение и алгебраическое сопряжение. При этом в силу особенностей строения кватернионов эти сопряжения полностью совпадают. Кватернион, сопряженный заданному, образуется сменой знаков у компонент при мнимых единицах.

Если обозначить кватернион покомпонентно как

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3,$$

то сопряженный ему кватернион будет:

$$\bar{q} = q_0 - i \cdot q_1 - j \cdot q_2 - k \cdot q_3$$

К сожалению, тот факт, что для кватернионов сопряжения совпадают, может вносить как терминологическую, так и идеологическую путаницу при использовании в формулах и иногда может приводить к неверным выводам, например когда начальная посылка вывода опирается на сопряжение как алгебраическое, но в ходе вывода алгебраическое сопряжение может быть трактовано как скалярное и наоборот.

Произведение кватерниона на сопряженный ему дает кватернион, состоящий из только действительной части. Если используемое для умножения сопряжение считать алгебраическим, то результат такого произведения называют квадратом модуля кватерниона:

$$|q|^2 = q \cdot \bar{q} = \bar{q} \cdot q$$

Модуль кватерниона обладает свойством мультипликативности - модуль произведения кватернионов равен произведению их модулей. В компонентах кватерниона его модуль выражается как:

$$|q| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$$

Таким образом, модуль существует для любого кватерниона и для любого ненулевого кватерниона модуль ненулевой.

Для кватернионов вполне разумно выглядит определение скалярного произведения кватернионов:

$$(a,b) = a_0 \cdot b_0 + a_1 \cdot b_1 + a_2 \cdot b_2 + a_3 \cdot b_3 = |a| \cdot |b| \cdot \cos(\varphi)$$

Здесь через φ обозначен гиперугол между кватернионами *a* и *b*. Во многих источниках факт достаточно корректного определения скалярного произведения используется для дачи определения модуля. К сожалению, этот метод для произвольной гиперкомплексной алгебры не работает.

Свойства кватернионов:

1) кватернионы коммутативны и ассоциативны по сложению:

$$q + p = p + q$$

$$(q + p) + r = p + (q + r)$$

2) кватернионы некоммутативны по умножению:

$$q \cdot p \neq p \cdot q$$

3) кватернионы ассоциативны по умножению:

$$(q \cdot p) \cdot r = p \cdot (q \cdot r)$$

4) кватернионы дистрибутивны:

$$p \cdot (q + r) = p \cdot q + p \cdot r$$

Для кватернионов операция деления определена как операция обратная

$$r = \frac{p}{q}$$

операции умножения. Если $\frac{p}{q}$, то r является решением уравнения $r \cdot q = p$. Решим это уравнение, домножив левую и правую часть на $\bar{q}$ и разделив обе части на квадрат модуля. Получим, что

$$r = \frac{p}{q} = \frac{p \cdot \bar{q}}{q \cdot \bar{q}} = \frac{p \cdot \bar{q}}{|q|^2}$$

В силу того, что модуль определен для любого кватерниона, делить можно на любой кватернион и, соответственно, для любого кватерниона существует обратный ему. В силу того, что при определении деления использовано умножение, а кватернионы некоммутативны по умножению, делитель для кватернионов может быть как правым, так и левым. При этом также существуют два кватерниона, являющиеся обратными заданному.

Из высшей алгебры известно, что если некая алгебра ассоциативна, то левый и правый делитель для числа этой алгебры совпадают. Поэтому для кватернионов левый и правый делители совпадают.

Дополнительные замечания.

Для кватернионов можно составить аналог формулы Эйлера, возведение основания натуральных логарифмов в степень кватернион:

$$e^{q_0+iq_1+jq_2+kq_3} = e^{q_0} \cdot \left(\cos\left(\sqrt{q_1^2+q_2^2+q_3^3}\right) + \frac{iq_1+jq_2+kq_3}{\sqrt{q_1^2+q_2^2+q_3^3}} \cdot \sin\left(\sqrt{q_1^2+q_2^2+q_3^3}\right) \right)$$

Данное выражение удобно использовать при оперировании трехмерными поворотами и, как следствие, в задачах ориентации тела в трехмерном пространстве. Например, при расчете траекторий космических аппаратов.

Трехмерное преобразование поворота вектора вокруг заданного направления на заданный угол $\vec{\varphi}$ определяется как:

$$q' = e^{\frac{\hat{\vec{P}}}{2}} \cdot q \cdot e^{-\frac{\hat{\vec{P}}}{2}}$$

Данное выражение приводится как справочное дополнительное замечание и для детального рассмотрения вопроса применения кватернионов в задачах моделирования трехмерных поворотов следует использовать соответствующую литературу.

15.10. Бикватернионы.

Бикватернионом называется число гиперкомплексной алгебры, полученной коммутативным удвоением по Кэли алгебры кватернионов:

$$B = Q_1 + \dot{i} \cdot Q_2$$

С мнимой единицей удвоения $\dot{i}^2 = -1$.

Здесь обозначены: Q - представители алгебры кватернионов, $\dot{i}$ - мнимая единица удвоения алгебр, B - представитель алгебры бикватернионов. Мнимая единица удвоения коммутирует по умножению с мнимыми единицами исходного кватерниона и при умножении на мнимые единицы i, j, k дает три новых мнимых единицы, которые обозначим как $\dot{i} \cdot i, \dot{i} \cdot j, \dot{i} \cdot k$. Таблица произведений мнимых единиц бикватернионов имеет вид:

	1	$\dot{i}$	$\dot{j}$	$\dot{k}$	$\dot{1}$	i	j	k
1	1	$\dot{i}$	$\dot{j}$	$\dot{k}$	$\dot{1}$	i	j	k
$\dot{i}$	$\dot{i}$	1	$-k$	j	$-i$	$-\dot{1}$	$\dot{k}$	$-\dot{j}$
$\dot{j}$	$\dot{j}$	$-\dot{j}$	1	$-i$	$-j$	$-\dot{k}$	$-\dot{1}$	$\dot{i}$
$\dot{k}$	$\dot{k}$	$-j$	i	1	$-k$	$\dot{j}$	$-\dot{i}$	$-\dot{1}$
$\dot{1}$	$\dot{1}$	$-i$	$-j$	$-k$	-1	$\dot{i}$	$\dot{j}$	$\dot{k}$
i	i	$-\dot{1}$	$\dot{k}$	$-\dot{j}$	$\dot{i}$	-1	k	$-j$
j	j	$-\dot{k}$	$-\dot{1}$	$\dot{i}$	$\dot{j}$	$-k$	-1	i
k	k	$\dot{j}$	$-\dot{i}$	$-\dot{1}$	$\dot{k}$	j	$-i$	-1

При получении данной таблицы произведений мнимых единиц бикватернионов мы полагали правый закон произведения мнимых единиц исходных кватернионов, взятых при удвоении. Так же можно привести таблицу произведений для левых бикватернионов. В дальнейшем будем полагать, что операции будут производиться с правыми бикватернионами в соответствии с приведенной таблицей.

Бикватернионы в некоторых случаях можно рассматривать как кватернионы над полем комплексных чисел, при этом набор мнимых единиц i, j, k и $\dot{1}$ перемножается прозрачно - тройка мнимых единиц кватерниона сохраняет структуру кватерниона, а мнимая единица $\dot{1}$ сохраняет структуру поля комплексных чисел. Так же следует помнить, что **бикватернионы являются алгеброй с делителями**

нуля и не следует слепо копировать на них соотношения, полученные для кватернионов и комплексных чисел.

Для бикватернионов, как и для кватернионов, определены операции сложения, вычитания, умножения и деления. Операции сложения и вычитания бикватернионов определены покомпонентно. Умножение бикватернионов полностью определяется приведенной выше таблицей произведений мнимых единиц бикватернионов.

Для бикватернионов определены три операции сопряжения - скалярное сопряжение, векторное сопряжение и алгебраическое сопряжение. При этом все три сопряжения абсолютно различны, более того, алгебраическое сопряжение определено существенно нелинейно.

Примем за покомпонентное обозначение бикватерниона следующее обозначение:

$$q = q_0 + \dot{i} \cdot i \cdot q_1 + \dot{i} \cdot j \cdot q_2 + \dot{i} \cdot k \cdot q_3 + \dot{i} \cdot q_4 + i \cdot q_5 + j \cdot q_6 + k \cdot q_7$$

1) Скалярное сопряжение бикватернионов образуется сменой знаков у компонент, в образовании мнимых единиц которых участвовала мнимая единица $\dot{i}$:

$$q' = q_0 - \dot{i} \cdot i \cdot q_1 - \dot{i} \cdot j \cdot q_2 - \dot{i} \cdot k \cdot q_3 - \dot{i} \cdot q_4 + i \cdot q_5 + j \cdot q_6 + k \cdot q_7$$

2) Векторное сопряжение бикватернионов образуется сменой знаков у компонент, в образовании мнимых единиц которых участвовали мнимые единицы *i*,*j*,*k*:

$$\tilde{q} = q_0 - \dot{i} \cdot i \cdot q_1 - \dot{i} \cdot j \cdot q_2 - \dot{i} \cdot k \cdot q_3 + \dot{i} \cdot q_4 - i \cdot q_5 - j \cdot q_6 - k \cdot q_7$$

3) алгебраическое сопряжение бикватерниона определено как решение уравнения

$$B \cdot \overline{B} = |B|^2$$

Способ получения бикватерниона, алгебраически сопряженного заданному бикватерниону, будет приведен ниже, после рассмотрения дополнительных, требующихся для этого вопросов.

Свойства бикватернионов.

1) бикватернионы коммутативны по сложению.

$$q_1 + q_2 = q_2 + q_1$$

2) бикватернионы ассоциативны по сложению.

$$(q_1 + q_2) + q_3 = q_1 + (q_2 + q_3)$$

3) бикватернионы дистрибутивны.

$$q_1 \cdot (q_2 + q_3) = q_1 \cdot q_2 + q_1 \cdot q_3$$

4) бикватернионы некоммутативны по умножению.

$$p \cdot q \neq q \cdot p$$

для произвольно выбранных бикватернионов.

5) бикватернионы ассоциативны по умножению

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

Для получения правила определения алгебраически сопряженного бикватерниона поступим так же, как и в случае с бикомплексными числами - найдем экспоненту от числа - бикватерниона. Для сокращения записи введем дополнительные функции от бикватернионов.

1) Скалярная функция.

$$Scl(q) = q_0 + i\,q_4$$

2) Полярная функция.

$$Pol(q) = i\,iq_1 + i\,jq_2 + i\,kq_3$$

3) Аксиальная функция.

$$Ax(q) = iq_5 + jq_6 + kq_7$$

4) Векторная функция.

$$Vec(q) = Pol(q) + Ax(q)$$

Для любого бикватерниона, таким образом, верно равенство:

$$q = Scl(q) + Vec(q)$$

5) Экспоненциальная функция.

$$e^q = \sum_{n=0}^{\infty} \frac{q^n}{n!}$$

где $q^0 = 1$ для любого бикватерниона.

Разложив ряд в приведенных обозначениях и приведя подобные члены, получим:

$$e^q = e^{Scl(q)} \left(ch\left(\sqrt{Vec^2(q)}\right) + Vec(q) \frac{sh\left(\sqrt{Vec^2(q)}\right)}{\sqrt{Vec^2(q)}} \right)$$

Решением уравнения $e^{P} = q$ относительно φ получаем логарифм бикватерниона, или, другими словами, его фазу.

Следующим шагом меняем знаки у всех мнимых компонент полученного логарифма и берем экспоненту от результата. Полученный бикватернион и будет алгебраически сопряженным исходному, поскольку

$$e^{A+B} \cdot e^{A-B} = e^{2 \cdot A}$$

для любых *A*, коммутирующих с *B* по умножению. Это утверждение в рамках данного классификатора алгебр не доказывается, а используется.

Как и для бикомплексной алгебры, для бикватернионов модуль бикватерниона определяется формой четвертой степени.

Алгебра бикватернионов содержит делители нуля. Поэтому не для любого бикватерниона может быть определен бикватернион, обратный ему.

Делители нуля в алгебре бикватернионов есть решение уравнения:

$$Scl^2(p) - Vec^2(p) = 0$$

Решения данного уравнения разбиваются на два подмножества - решения уравнения с

$$Scl^2(q) = 0$$

и

$$Scl^2(q) \neq 0.$$

Решения для первого случая представляют собой нильпотенты, решения для второго случая - идемпотенты. Как и для бикомплексных

чисел, делители нуля в бикватернионах имеют обратный себе, такой что их произведение дает ноль. Но, в отличие от бикомплексных чисел, делитель нуля в бикватернионах может быть получен из обратного себе умножением на бикватернион благодаря тому, что бикватернионы имеют большую размерность и в их пространстве существует операция вращения, отображающая любой бикватернион на векторно сопряженный ему. Для произвольно взятого делителя нуля таких операторов поворота будет бесконечное множество.

Дополнительные замечания.

Существует модель представления 4-х мерного пространства-времени в бикватернионном базисе таким образом, что компоненте q_0 сопоставляется координата времени, а компонентам q_1, q_2, q_3 соответственно пространственные координаты *x,y,z*. Остальные части бикватерниона отбрасываются из рассмотрения либо полагаются всегда равными нулю. Впрочем, всегда можно рассмотреть наше пространство-время как пространство с еще 4-мя координатами. При такой замене преобразование вида

$$q' = e^{\frac{P}{2}} \cdot q \cdot e^{\frac{-P}{2}}, \quad Scl(\varphi) = 0$$

содержит в себе группу преобразований Лоренца. При этом полярная часть φ представляет собой параметр преобразования движения одной системы отсчета относительно другой, а аксиальная часть φ - параметр преобразования поворота системы отсчета, а именно - вектор поворота.

15.11. Паракватернионы.

Паракватернионом называется **число гиперкомплексной алгебры**, полученной некоммутативным удвоением по Кэли алгебры паракомплексных чисел:

$$Q = P_1 + j \cdot P_2$$

С мнимой единицей удвоения $j^2=1$..

Здесь обозначены: P_1, P_2, - представители алгебры паракомплексных чисел, j - мнимая единица удвоения алгебр, Q - представитель алгебры паракватернионов. Мнимая единица удвоения j не коммутирует по умножению с мнимой единицей исходной паракомплексной алгебры i и при умножении на нее образует третью мнимую единицу, обозначаемую как k. Таблица произведений единиц паракватернионов имеет вид:

	1	i	j	k
1	1	i	j	k
i	i	1	k	$-j$
j	j	$-k$	1	i
k	k	j	$-i$	1

Данный закон умножения определен как правый закон умножения. Так же можно определить паракватернионы с левым законом умножения. Отличие левых паракватернионов от правых паракватернионов состоит в результате произведения мнимых частей. В большинстве случаев при рассмотрении алгебры паракватернионов пользуются определением паракватерниона как правого паракватерниона. Мы так же будем следовать этому соглашению.

По своему строению паракватернионы очень похожи на кватернионы, что иногда может вводить в заблуждение и приводить к реальным ошибкам при проведении вычислений с их применением.

Для паракватернионов определены операции сложения, вычитания, умножения и деления. Операции сложения и вычитания для паракватернионов определены покомпонентно. Умножение паракватернионов определяется таблицей произведений их мнимых единиц, приведенной выше.

Операций сопряжения для паракватернионов определено три - скалярное, векторное и алгебраическое. В силу строения паракватерниона эти сопряжения полностью совпадают.

Паракватернион, сопряженный заданному, образуется сменой знаков у компонент при мнимых единицах.

Если обозначить паракватернион покомпонентно как

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3,$$

то сопряженный ему паракватернион будет:

$$\bar{q} = q_0 - i \cdot q_1 - j \cdot q_2 - k \cdot q_3$$

Сопряжения для паракватернионов, как и для кватернионов, имеют свойство:

$$\overline{a \cdot b} = \bar{b} \cdot \bar{a}$$

Как и для кватернионов, для паракватернионов следует сделать оговорку, вызванную совпадением всех трех сопряжений - следует быть внимательным, и различать выражения, использующие сопряжения. Следует внимательно относиться к виду сопряжения.

Произведение паракватерниона на сопряженный ему дает паракватернион, состоящий из только действительной части. Если используемое для умножения сопряжение считать алгебраическим, то результат такого произведения называют квадратом модуля паракватерниона:

$$|q|^2 = q \cdot \bar{q} = \bar{q} \cdot q$$

Модуль паракватерниона обладает свойством мультипликативности - модуль произведения паракватернионов равен произведению их модулей. В компонентах паракватерниона его модуль выражается как:

$$|q| = \left| \sqrt{q_0^2 - q_1^2 - q_2^2 - q_3^2} \right|$$

Паракватернионы являются представителями алгебры с делителями нуля. Как и для паракомплексных чисел, для паракватернионов можно выделить подмножества делителей нуля. Делители нуля в паракватернионах удовлетворяют уравнению:

$$q_0^2 - q_1^2 - q_2^2 - q_3^2 = 0,$$

или

$$q_0^2 = q_1^2 + q_2^2 + q_3^2$$

Если проводить геометрическое толкование этого уравнения, то, сопоставив паракватерниону 4-х мерное пространство, получим семейство сфер с точкой, лежащей на оси q_0.

В силу того, что паракватернионы являются более общим случаем паракомплексных чисел, свойства делителей нуля для паракомплексных чисел применимы так же и для паракватернионов, а именно:

1) любой делитель нуля для паракватернионов представим в виде вектора, являющегося решением уравнения сферы с точкой, лежащей на оси q_0.

2) любой делитель нуля выразим в виде произведения действительного числа и идемпотента.

3) произведение делителя нуля на векторно сопряженный ему дает ноль.

4) любой паракватернион представим в виде линейной суперпозиции делителей нуля.

Если паракватернион не является делителем нуля, то операция деления на него определена как:

$$\frac{q_1}{q_2} = \frac{q_1 \cdot \overline{q_2}}{q_2 \cdot \overline{q_2}} = \frac{q_1 \cdot \overline{q_2}}{|q_2|^2}$$

Дополнительные замечания.

Для паракватернионов, также как и для комплексных чисел, можно составить аналог формулы Эйлера. Разложив экспоненциальный ряд и приведя подобные, получим, что:

$$e^{q_0+iq_1+jq_2+kq_3} = e^{q_0} \cdot \left(ch\left(\sqrt{q_1^2+q_2^2+q_3^3}\right) + \frac{iq_1+jq_2+kq_3}{\sqrt{q_1^2+q_2^2+q_3^3}} \cdot sh\left(\sqrt{q_1^2+q_2^2+q_3^3}\right) \right)$$

Поскольку $ch(x) \neq sh(x)$ при любом действительном *x*, результат взятия экспоненты от любого паракватерниона не является идемпотентом.

Откуда следует, что для любого паракватерниона - неидемпотента существует его логарифм как решение формулы Эйлера для паракватернионов.

15.12. Дуальные кватернионы.

Дуальным кватернионом называется число алгебры, полученной удвоением по Кэли алгебры кватернионов:

$$D = C_1 + E \cdot C_2$$

с мнимой единицей удвоения $E^2=0$.

Здесь обозначены: C_1, C_2 - представители алгебры кватернионов, E - мнимая единица удвоения алгебр, D - представитель алгебры дуальных кватернионов.

Дуальный кватернион может быть записан покомпонентно следующим образом:

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3 + \varpi \cdot q_4 + \varpi \cdot i \cdot q_5 + \varpi \cdot j \cdot q_6 + \varpi \cdot k \cdot q_7$$

где через $i, j, k, \varpi, \varpi \cdot i, \varpi \cdot j, \varpi \cdot k$ обозначены мнимые единицы, а через q_n обозначены компоненты дуального кватерниона.

Таблица умножения мнимых единиц дуальных кватернионов имеет вид:

	1	i	j	k	ϖ	ϖ_i	ϖ_j	ϖ_k
1	1	i	j	k	ϖ	ϖ_i	ϖ_j	ϖ_k
i	i	-1	k	$-j$	ϖ_i	$-\varpi$	ϖ_k	$-\varpi_j$
j	j	$-k$	-1	i	ϖ_j	$-\varpi_k$	$-\varpi$	ϖ_i
k	k	j	$-i$	-1	ϖ_k	ϖ_j	$-\varpi_i$	$-\varpi$
ϖ	ϖ	ϖ_i	ϖ_j	ϖ_k	0	0	0	0
ϖ_i	ϖ_i	$-\varpi$	ϖ_k	$-\varpi_j$	0	0	0	0
ϖ_j	ϖ_j	$-\varpi_k$	$-\varpi$	ϖ_i	0	0	0	0
ϖ_k	ϖ_k	ϖ_j	$-\varpi_i$	$-\varpi$	0	0	0	0

Для дуальных кватернионов применимы три вида сопряжений - алгебраическое, векторное и дуальное. Для дуального кватерниона, заданного в форме

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3 + \varpi \cdot q_4 + \varpi \cdot i \cdot q_5 + \varpi \cdot j \cdot q_6 + \varpi \cdot k \cdot q_7$$

сопряженные ему числа будут иметь вид:

1) векторное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых участвовали единицы *i, j, k*:

$$q = q_0 - i \cdot q_1 - j \cdot q_2 - k \cdot q_3 + \omega \cdot q_4 - \omega \cdot i \cdot q_5 - \omega \cdot j \cdot q_6 - \omega \cdot k \cdot q_7$$

2) дуальное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых участвовала мнимая единица ω:

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3 - \omega \cdot q_4 - \omega \cdot i \cdot q_5 - \omega \cdot j \cdot q_6 - \omega \cdot k \cdot q_7$$

3) алгебраическое сопряжение, образованное сменой знаков у компонентов при всех мнимых единицах:

$$q = q_0 - i \cdot q_1 - j \cdot q_2 - k \cdot q_3 - \omega \cdot q_4 - \omega \cdot i \cdot q_5 - \omega \cdot j \cdot q_6 - \omega \cdot k \cdot q_7$$

Квадрат модуля образуется как:

$$|q|^2 = q \cdot \overline{q} = \overline{q} \cdot q = q_0^2 + q_1^2 + q_2^2 + q_3^2$$

Дуальная часть дуального кватерниона в образовании модуля не участвует. При этом в некоторых задачах в дуальном кватернионе разделяют недуальную и дуальную части и рассматривают отдельно модуль недуальной и дуальной части без множителя ω.

Свойства дуальных кватернионов:

1) дуальные кватернионы коммутативны по сложению:

$$q_a + q_b = q_b + q_a$$

в силу того, что операции сложения и вычитания для дуальных кватернионов определены покомпонентно:

$$a \pm b = (a_0 \pm b_0) + i \cdot (a_1 \pm b_1) + j \cdot (a_2 \pm b_2) + k \cdot (a_3 \pm b_3) +$$
$$+ \omega \cdot (a_4 \pm b_4) + \omega \cdot i \cdot (a_5 \pm b_5) + \omega \cdot j \cdot (a_6 \pm b_6) + \omega \cdot k \cdot (a_7 \pm b_7)$$

2) дуальные кватернионы ассоциативны по сложению и по умножению:

$$(a+b)+c=a+(b+c)$$

$$(a\cdot b)\cdot c=a\cdot(b\cdot c)$$

3) дуальные кватернионы дистрибутивны:

$$a\cdot(b+c)=a\cdot b+a\cdot c$$

4) дуальные кватернионы некоммутативны по умножению. В общем случае:

$$a\cdot b\neq b\cdot a$$

Операция деления для дуальных кватернионов определена как операция умножения на обратный кватернион, где обратный кватернион вычисляется как:

$$q^{-1}=\frac{\overline{q}}{|q|^2}$$

Дополнительные замечания.

Для дуальных кватернионов можно составить аналог формулы Эйлера. Разложив в экспоненциальный ряд и приведя подобные, получим:

$$\exp(q_0+i\cdot q_1+j\cdot q_2+k\cdot q_3+\varpi\cdot q_4+\varpi\cdot i\cdot q_5+\varpi\cdot j\cdot q_6+\varpi\cdot k\cdot q_7)=$$

$$=\exp(q_0)\cdot\left(\cos\left(\sqrt{q_1^2+q_2^2+q_3^2}\right)+\frac{i\cdot q_1+j\cdot q_2+k\cdot q_3}{\sqrt{q_1^2+q_2^2+q_3^2}}\cdot\sin\left(\sqrt{q_1^2+q_2^2+q_3^2}\right)\right)\cdot$$

$$\cdot(1+\varpi\cdot(q_4+i\cdot q_5+j\cdot q_6+k\cdot q_7))$$

Дуальные кватернионы, благодаря своему строению и свойствам дуального произведения, очень хорошо подходят **для моделирования задач сдвигов, задач 3-х мерных вращений и сдвигов с одновременным вращением.** На языке дуальных кватернионов

находят свое красивое решение как прямая задача вращения со сдвигом, так и обратная - нахождение параметров результирующего преобразования. Так же красивое решение имеет задача отыскания требуемых промежуточных преобразований при заданных одного из начальных и результирующего преобразования.

15.13. Дуальные паракватернионы

Дуальным паракватернионом называется число алгебры, полученной удвоением по Кэли алгебры паракватернионов:

$$D = C_1 + E \cdot C_2$$

с мнимой единицей удвоения $E^2 = 0$.

Здесь обозначены: C_1, C_2 - представители алгебры паракватернионов, E - мнимая единица удвоения алгебр, D - представитель алгебры дуальных паракватернионов.

Дуальный паракватернион может быть записан покомпонентно следующим образом:

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3 + \omega \cdot q_4 + \omega \cdot i \cdot q_5 + \omega \cdot j \cdot q_6 + \omega \cdot k \cdot q_7$$

где через $i, j, k, \omega, \omega \cdot i, \omega \cdot j, \omega \cdot k$ обозначены мнимые единицы, а через q_n обозначены компоненты дуального паракватерниона.

Таблица умножения мнимых единиц дуальных паракватернионов имеет вид:

	1	i	j	k	ω	ω_i	ω_j	ω_k
1	1	i	j	k	ω	ω_i	ω_j	ω_k
i	i	1	k	$-j$	ω_i	ω	ω_k	$-\omega_j$
j	j	$-k$	1	i	ω_j	$-\omega_k$	ω	ω_i
k	k	j	$-i$	1	ω_k	ω_j	$-\omega_i$	ω
ω	ω	ω_i	ω_j	ω_k	0	0	0	0
ω_i	ω_i	ω	ω_k	$-\omega_j$	0	0	0	0
ω_j	ω_j	$-\omega_k$	ω	ω_i	0	0	0	0
ω_k	ω_k	ω_j	$-\omega_i$	ω	0	0	0	0

Для дуальных паракватернионов применимы три вида сопряжений - алгебраическое, векторное и дуальное. Для дуального паракватерниона, заданного в форме

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3 + \omega \cdot q_4 + \omega \cdot i \cdot q_5 + \omega \cdot j \cdot q_6 + \omega \cdot k \cdot q_7$$

сопряженные ему числа будут иметь вид:

1) векторное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых участвовали единицы *i, j, k*:

$$q = q_0 - i \cdot q_1 - j \cdot q_2 - k \cdot q_3 + \omega \cdot q_4 - \omega \cdot i \cdot q_5 - \omega \cdot j \cdot q_6 - \omega \cdot k \cdot q_7$$

2) дуальное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых участвовала мнимая единица ω:

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3 - \omega \cdot q_4 - \omega \cdot i \cdot q_5 - \omega \cdot j \cdot q_6 - \omega \cdot k \cdot q_7$$

3) алгебраическое сопряжение, образованное сменой знаков у компонентов при всех мнимых единицах:

$$q = q_0 - i \cdot q_1 - j \cdot q_2 - k \cdot q_3 - \omega \cdot q_4 - \omega \cdot i \cdot q_5 - \omega \cdot j \cdot q_6 - \omega \cdot k \cdot q_7$$

Квадрат модуля образуется как:

$$|q|^2 = q \cdot \overline{q} = \overline{q} \cdot q = q_0^2 + q_1^2 + q_2^2 + q_3^2$$

Дуальная часть дуального паракватерниона в образовании модуля не участвует. При этом в некоторых задачах в дуальном паракватернионе разделяют недуальную и дуальную части и рассматривают отдельно модуль недуальной и дуальной части без множителя ω.

Свойства дуальных паракватернионов:

1) дуальные паракватернионы коммутативны по сложению:

$$q_a + q_b = q_b + q_a$$

в силу того, что операции сложения и вычитания для дуальных паракватернионов определены покомпонентно:

$$a \pm b = (a_0 \pm b_0) + i \cdot (a_1 \pm b_1) + j \cdot (a_2 \pm b_2) + k \cdot (a_3 \pm b_3) +$$
$$+ \omega \cdot (a_4 \pm b_4) + \omega \cdot i \cdot (a_5 \pm b_5) + \omega \cdot j \cdot (a_6 \pm b_6) + \omega \cdot k \cdot (a_7 \pm b_7)$$

2) дуальные паракватернионы ассоциативны по сложению и по умножению:

$$(a + b) + c = a + (b + c)$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3) дуальные паракватернионы дистрибутивны:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

4) дуальные паракватернионы некоммутативны по умножению. В общем случае:

$$a \cdot b \neq b \cdot a$$

Операция деления для дуальных паракватернионов определена как операция умножения на обратный дуальный паракватернион, где обратный дуальный паракватернион вычисляется как:

$$q^{-1} = \frac{\overline{q}}{|q|^2}$$

Дополнительные замечания.

Свойства дуальных паракватернионов очень похожи на свойства дуальных кватернионов и в большинстве случаев их повторяют. Исключением является то, что дуальные паракватернионы, содержа в себе паракватернионную часть, содержат и делители нуля.

Для дуальных паракватернионов можно составить аналог формулы Эйлера. Разложив в экспоненциальный ряд и приведя подобные, получим:

$$\exp(q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3 + \varpi \cdot q_4 + \varpi \cdot i \cdot q_5 + \varpi \cdot j \cdot q_6 + \varpi \cdot k \cdot q_7) =$$

$$= \exp(q_0) \cdot \left(ch\left(\sqrt{q_1^2 + q_2^2 + q_3^2}\right) + \frac{i \cdot q_1 + j \cdot q_2 + k \cdot q_3}{\sqrt{q_1^2 + q_2^2 + q_3^2}} \cdot sh\left(\sqrt{q_1^2 + q_2^2 + q_3^2}\right) \right) \cdot$$

$$\cdot \left(1 + \varpi \cdot (q_4 + i \cdot q_5 + j \cdot q_6 + k \cdot q_7)\right)$$

Очевидно, что если дуальный паракватернион может быть представлен в виде правой части приведенного уравнения, для него так же существует и обратный дуальный паракватернион.

15.14. Дуальные бикватернионы.

Дуальным бикватернионом называется число алгебры, полученной удвоением по Кэли алгебры паракватернионов:

$$D = C_1 + E \cdot C_2$$

с мнимой единицей удвоения $E^2 = 0$.

Здесь обозначены: C_1, C_2 - представители алгебры бикватернионов, E - мнимая единица удвоения алгебр, D - представитель алгебры дуальных бикватернионов.

Дуальный бикватернион может быть записан покомпонентно следующим образом:

$$q = q_0 + i' \cdot i \cdot q_1 + i' \cdot j \cdot q_2 + i' \cdot k \cdot q_3 + i' \cdot q_4 + i \cdot q_5 + j \cdot q_6 + k \cdot q_7 +$$

$$+\omega \cdot \left(q_8 + i' \cdot i \cdot q_9 + i' \cdot j \cdot q_{10} + i' \cdot k \cdot q_{11} + i' \cdot q_{12} + i \cdot q_{13} + j \cdot q_{14} + k \cdot q_{15}\right)$$

где через i, j, k, ω, i' обозначены простые и составные мнимые единицы, а через q_n обозначены компоненты дуального бикватерниона.

Таблица умножения мнимых единиц дуальных бикватернионов не приводится в силу того, что она может быть построена самостоятельно на основе таблицы произведений мнимых единиц бикватернионов и правила умножения на дуальную мнимую единицу. К этим двум основам она ничего более не добавляет и самостоятельного интереса не представляет.

Для дуальных бикватернионов применимы все четыре сопряжения - алгебраическое, векторное, скалярное и дуальное. Причем различия между ними проявляются со всей ясностью, чего иногда трудно было сказать об алгебрах с меньшей мерностью. Для дуального бикватерниона, заданного в форме

$$q = q_0 + \dot{i} \cdot i \cdot q_1 + \dot{i} \cdot j \cdot q_2 + \dot{i} \cdot k \cdot q_3 + \dot{i} \cdot q_4 + i \cdot q_5 + j \cdot q_6 + k \cdot q_7 +$$

$$+\omega \cdot \left(q_8 + \dot{i} \cdot i \cdot q_9 + \dot{i} \cdot j \cdot q_{10} + \dot{i} \cdot k \cdot q_{11} + \dot{i} \cdot q_{12} + i \cdot q_{13} + j \cdot q_{14} + k \cdot q_{15} \right)$$

сопряженные ему дуальные бикватернионы будут иметь вид:

1) векторно сопряженный, образованный сменой знаков у компонент при мнимых единицах, в образовании которых участвовали единицы *i*, *j*, *k*:

$$q = q_0 - \dot{i} \cdot i \cdot q_1 - \dot{i} \cdot j \cdot q_2 - \dot{i} \cdot k \cdot q_3 + \dot{i} \cdot q_4 - i \cdot q_5 - j \cdot q_6 - k \cdot q_7 +$$

$$+\omega \cdot \left(q_8 - \dot{i} \cdot i \cdot q_9 - \dot{i} \cdot j \cdot q_{10} - \dot{i} \cdot k \cdot q_{11} + \dot{i} \cdot q_{12} - i \cdot q_{13} - j \cdot q_{14} - k \cdot q_{15} \right)$$

2) скалярное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых участвовала мнимая единица $\dot{i}$:

$$q = q_0 - \dot{i} \cdot i \cdot q_1 - \dot{i} \cdot j \cdot q_2 - \dot{i} \cdot k \cdot q_3 - \dot{i} \cdot q_4 + i \cdot q_5 + j \cdot q_6 + k \cdot q_7 +$$

$$+\omega \cdot \left(q_8 - \dot{i} \cdot i \cdot q_9 - \dot{i} \cdot j \cdot q_{10} - \dot{i} \cdot k \cdot q_{11} - \dot{i} \cdot q_{12} + i \cdot q_{13} + j \cdot q_{14} + k \cdot q_{15} \right)$$

3) дуальное сопряжение, образованное сменой знаков у компонент при мнимых единицах, в образовании которых участвовала мнимая единица ω:

$$q = q_0 + \dot{i} \cdot i \cdot q_1 + \dot{i} \cdot j \cdot q_2 + \dot{i} \cdot k \cdot q_3 + \dot{i} \cdot q_4 + i \cdot q_5 + j \cdot q_6 + k \cdot q_7 -$$

$$-\omega \cdot \left(q_8 + \dot{i} \cdot i \cdot q_9 + \dot{i} \cdot j \cdot q_{10} + \dot{i} \cdot k \cdot q_{11} + \dot{i} \cdot q_{12} + i \cdot q_{13} + j \cdot q_{14} + k \cdot q_{15} \right)$$

4) Для образования алгебраического сопряжения введем дуальную функцию:

$$Dual(q) = q_8 + \dot{i} \cdot i \cdot q_9 + \dot{i} \cdot j \cdot q_{10} + \dot{i} \cdot k \cdot q_{11} + \dot{i} \cdot q_{12} + i \cdot q_{13} + j \cdot q_{14} + k \cdot q_{15}$$

таким образом, что результат дуальной функции есть бикватернион, образованный из дуальной части дуального кватерниона с отбрасыванием дуальной мнимой удиницы. Также введем прямую функцию:

$$Dir(q) = q_0 + \dot{i} \cdot i \cdot q_1 + \dot{i} \cdot j \cdot q_2 + \dot{i} \cdot k \cdot q_3 + \dot{i} \cdot q_4 + i \cdot q_5 + j \cdot q_6 + k \cdot q_7$$

таким образом, что результат прямой функции есть бикватернион, образованный из дуального бикватерниона отбрасыванием его дуальной части. В результате получим, что:

$$q = Dir(q) + \omega \cdot Dual(q) = Dir(q) \cdot \left(1 + \omega \cdot \frac{\overline{Dir(q)}}{\left| Dir(q) \right|^2} \cdot Dual(q) \right)$$

Второе равенство, естественно, справедливо только в том случае, если модуль прямой части не равен нулю. Далее именно этот случай и будем рассматривать.

Алгебраически сопряженный бикватернион образуется как комбинация алгебраически сопряженной прямой части в качестве прямой части и дуально сопряженной дуальной части в качестве дуальной части:

$$\bar{q} = \overline{Dir}(q) - \omega \cdot Dual(q) = \left(1 - \omega \cdot Dual(q) \cdot \frac{Dir(q)}{\left| Dir(q) \right|^2} \right) \cdot \overline{Dir}(q)$$

таким образом, что их произведение дает действительное число, не зависящее от дуальной части:

$$q \cdot \bar{q} = Dir(q) \cdot \left(1 + \omega \cdot \frac{\overline{Dir(q)}}{\left| Dir(q) \right|^2} \cdot Dual(q) \right) \cdot \left(1 - \omega \cdot Dual(q) \cdot \frac{Dir(q)}{\left| Dir(q) \right|^2} \right) \cdot \overline{Dir}(q)$$

$$q \cdot \bar{q} = Dir(q) \cdot \overline{Dir}(q) = \left| Dir(q) \right|^2$$

Для тех дуальных бикватернионов, для которых модуль прямой части равен нулю при ненулевой прямой части, модуль полагают равным нулю.

В целом же, такой подход справедлив и для других дуальных чисел. Как и для других дуальных чисел, для дуальных бикватернионов зачастую удобно рассматривать его прямую и дуальную части раздельно, в том числе преобразования с ними и взятие модуля.

Свойства дуальных бикватернионов:

1) дуальные бикватернионы коммутативны по сложению:

$$q_a + q_b = q_b + q_a$$

в силу того, что операции сложения и вычитания для дуальных бикватернионов определены покомпонентно:

$$\begin{aligned} a \pm b = {} & (a_0 \pm b_0) + \hat{i} \cdot i \cdot (a_1 \pm b_1) + \hat{i} \cdot j \cdot (a_2 \pm b_2) + \hat{i} \cdot k \cdot (a_3 \pm b_3) + \\ & + \hat{i} \cdot (a_4 \pm b_4) + i \cdot (a_5 \pm b_5) + j \cdot (a_6 \pm b_6) + k \cdot (a_7 \pm b_7) + \\ & + \varpi \cdot ((a_8 \pm b_8) + \hat{i} \cdot i \cdot (a_9 \pm b_9) + \hat{i} \cdot j \cdot (a_{10} \pm b_{10}) + \hat{i} \cdot k \cdot (a_{11} \pm b_{11}) + \\ & + \hat{i} \cdot (a_{12} \pm b_{12}) + i \cdot (a_{13} \pm b_{13}) + j \cdot (a_{14} \pm b_{14}) + k \cdot (a_{15} \pm b_{15})) \end{aligned}$$

2) дуальные бикватернионы ассоциативны по сложению и по умножению:

$$(a + b) + c = a + (b + c)$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3) дуальные бикватернионы дистрибутивны:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

4) дуальные бикватернионы некоммутативны по умножению. В общем случае:

$$a \cdot b \neq b \cdot a$$

Операция деления для дуальных паракватернионов определена как операция умножения на обратный кватернион, где обратный кватернион вычисляется как:

$$q^{-1} = \frac{\bar{q}}{|q|^2}$$

Обратный дуальный бикватернион существует не для любого дуального бикватерниона. Для того, чтобы иметь обратный себе, дуальный бикватернион должен иметь ненулевую прямую часть, которая не должна являться нильпотентом или идемпотентом. При этом дуальная часть может быть абсолютно любой, поскольку в образовании обратного дуального бикватерниона на нее не накладывается никаких условий для преобразований.

Дополнительные замечания.

Свойства дуальных бикватернионов практически полностью повторяют свойства бикватернионов, привнося в выражения дуальную часть. Бикватернионы, таким образом, могут рассматриваться как частный случай дуальных бикватернионов. Как и для бикватернионов, для дуальных бикватернионов можно составить аналог формулы Эйлера. От соответствующей функции для бикватернионов она отличается множителем с единицей плюс дуальная функция:

$$\exp(q) = \exp\left(Scl\left(Dir(q)\right)\right) \cdot \left(ch\left(\sqrt{Vec^2\left(Dir(q)\right)}\right) + Vec\left(Dir(q)\right) \frac{sh\left(\sqrt{Vec^2\left(Dir(q)\right)}\right)}{\sqrt{Vec^2\left(Dir(q)\right)}} \right) \cdot$$

$$\cdot\left(1 + \varpi \cdot Dual(q)\right)$$

В силу присутствия в дуальных бикватернионах как бикватернионной прямой части, так и дуальной части, они могут быть с легкостью использованы для представления полной группы преобразований

Пуанкаре. При этом векторной части преобразуемого вектора пространства сопоставляется полярная часть дуальной части, а скалярной части преобразуемого вектора пространства сопоставляется скалярная часть дуальной части. **Параметрам преобразования сопоставляются: преобразованию трехмерного поворота сопоставляется аксиальная часть прямой части логарифма оператора, преобразованию гиперболического поворота скоростей - полярная часть прямой части логарифма оператора, а сдвигу - соответственно полярная и скалярная части дуальной части логарифма оператора. Присутствие так сказать "не полностью использованной" аксиальной части дуальной части оператора соответствует сдвигу по дополнительным степеням свободы, которые, так же как и псевдоскаляры, могут рассматриваться как внутренний момент вращения вектора пространства или объекта, который этим вектором моделируется.**

Аппарат дуальных бикватернионов или нерассматриваемых в данном классификаторе дуальных бипаракватернионов с успехом может быть использован в качестве математического аппарата построения моделей эфиродинамики, получивший много приверженцев и экспериментальных подтверждений. В существующих математических описаниях эфиродинамики до сих пор, как, впрочем, и в релятивизме, есть некоторые неточности. Как, например, в релятивизме при постулировании относительности явлений постулируется так же и масса покоя (покоя абсолютного? или относительно чего?), так и в эфиродинамике до сих пор принимается к рассмотрению группа преобразований Лоренца, являющаяся фундаментом специальной теории относительности. При этом эфиродинамика органически (в силу оперирования частицами эфира) приписывает частицам эфира внутреннее вращение, участвующее во взаимодействии. Но полное рассмотрение применения гмперкомплексных чисел как в релятивизме, так и в эфиродинамике в данном классификторе не приводится, поскольку это рассмотрение не является его целью.

15.15. Октавы.

Неассоциативные алгебры покрыты мифами экзотики. На самом деле ничего особенного, кроме потери ассоциативности, в них нет. Впрочем, эта потеря существенна. Если можно выразиться образно, то в космосе алгебр за ассоциативными уже ничего "живого" нет. Среди

неассоциативных алгебр наиболее известной является простейшая из них - **алгебра октав**. Или, иначе, **четвертая алгебра Фробениуса**, она же **алгебра Кэли-Диксона**. По мере рассмотрения будем давать так же и общие свойства неассоциативных алгебр в целом.

Октавой называется число гиперкомплексной алгебры, полученной некоммутативным удвоением по Кэли алгебры кватернионов:

$$O = Q_1 + E \cdot Q_2$$

Здесь обозначены:

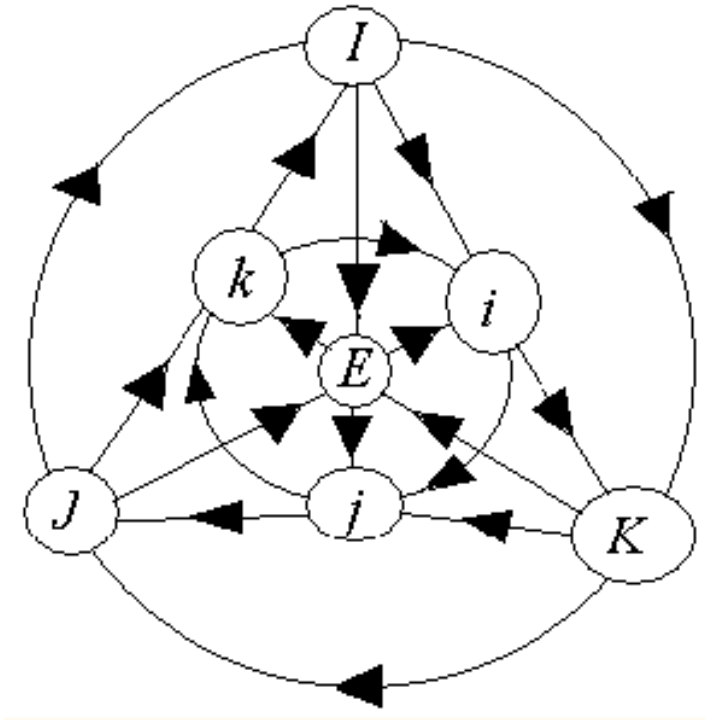
O - октава,

Q - кватернионы,

E - мнимая единица $E^2 = -1$. Эта мнимая единица умножается на мнимые единицы кватернионов *i, j, k* некоммутативно. При умножении на мнимые единицы кватернионов образуются дополнительно три несоставных мнимых единицы. Правило произведения мнимых единиц (*1,i,j,k,E,I,J,K*) может быть представлено таблицей:

	1	*i*	*j*	*k*	*E*	*I*	*J*	*K*
1	*1*	*i*	*j*	*k*	*E*	*I*	*J*	*K*
i	*i*	*-1*	*k*	*-j*	*-I*	*E*	*K*	*-J*
j	*j*	*-k*	*-1*	*i*	*-J*	*-K*	*E*	*I*
k	*k*	*j*	*-i*	*-1*	*-K*	*J*	*-I*	*E*
E	*E*	*I*	*J*	*K*	*-1*	*-i*	*-j*	*-k*
I	*I*	*-E*	*K*	*-J*	*i*	*-1*	*K*	*-J*
J	*J*	*-K*	*-E*	*I*	*j*	*-K*	*-1*	*I*
K	*K*	*J*	*-I*	*-E*	*K*	*J*	*-I*	*-1*

Или диаграммой взаимных произведений:



При получении вышеприведенной таблицы произведений мы исходили из правого закона произведения мнимых единиц кватернионов (внутренний круг диаграммы), правого закона произведения новых единиц (внешний круг диаграммы) и правого закона произведения мнимых единиц исходных кватернионов на мнимую единицу *E* (радиальные линии диаграммы). Так же можно использовать определение октав с левыми правилами произведения. В дальнейшем мы будем полагать, что используются правые правила.

Октавы во многих случаях уместно рассматривать как существенное расширение кватернионов. Так же как и кватернионы, октавы не имеют делителей нуля, и квадрат модуля так же выражается простой квадратичной формой. Для них, так же как и для кватернионов, можно определить условное скалярное произведение. Каковое и использовалось Фробениусом.

Для октав, как и для других гиперкомплексных чисел, определены операции сложения, вычитания, умножения и деления. Операции сложения и вычитания определены покомпонентно. Умножение октав определено таблицей произведения их мнимых единиц. Для выполнения деления производится замена операции деления на операцию умножения.

Для октав определены две операции сопряжения - алгебраическое и векторное. Два других сопряжения - дуальное и скалярное не применимы в силу отсутствия в строении октав скалярной и дуальной мнимых единиц. При этом векторное и алгебраическое сопряжения совпадают. Октава, сопряженная заданной, образуется сменой знаков у компонент при всех мнимых единицах. Или, если обозначить октаву покомпонентно как

$$q = q_0 + i \cdot q_1 + j \cdot q_2 + k \cdot q_3 + E \cdot q_4 + I \cdot q_5 + J \cdot q_6 + K \cdot q_7$$

то сопряженная ей октава будет иметь вид:

$$q = q_0 - i \cdot q_1 - j \cdot q_2 - k \cdot q_3 - E \cdot q_4 - I \cdot q_5 - J \cdot q_6 - K \cdot q_7$$

Так же как и для комплексных чисел и для кватернионов, тот факт, что для октав два различных сопряжения полностью совпадают, может приводить к путанице при оперировании октавами. Следует быть внимательным и следить, какой смысл вкладывается в сопряжение в каждом конкретном случае.

Произведение октавы на сопряженную ей дает октаву, имеющую только скалярную ненулевую часть. Если сопряжение в данном случае считать алгебраическим, то результат такого произведения есть квадрат модуля октавы:

$$|q|^2 = q \cdot \bar{q} = \bar{q} \cdot q$$

Модуль октавы обладает свойством мультипликативности - модуль произведения октав равен произведению их модулей. В компонентах модуль октавы выражается как:

$$|q| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2 + q_4^2 + q_5^2 + q_6^2 + q_7^2}$$

Как и для кватернионов, для октав вполне разумно выглядит определение скалярного произведения двух октав в виде:

$$(a,b) = a_0 \cdot b_0 + a_1 \cdot b_1 + a_2 \cdot b_2 + a_3 \cdot b_3 + a_4 \cdot b_4 + a_5 \cdot b_5 + a_6 \cdot b_6 + a_7 \cdot b_7 = |a| \cdot |b| \cdot \cos(\varphi)$$

Здесь через φ обозначен гиперугол между октавами *a* и *b*.

Свойства октав:

1) октавы коммутативны и ассоциативны по сложению:

$$a + b = b + a$$

$$a + (b + c) = (a + b) + c$$

в силу того, что операция сложения октав определена покомпонентно:

$$a \pm b = (a_0 \pm b_0) + i \cdot (a_1 \pm b_1) + j \cdot (a_2 \pm b_2) + k \cdot (a_3 \pm b_3) +$$
$$+ E \cdot (a_4 \pm b_4) + I \cdot (a_5 \pm b_5) + J \cdot (a_6 \pm b_6) + K \cdot (a_7 \pm b_7)$$

2) октавы некоммутативны по умножению:

$$a \cdot b \neq b \cdot a$$

данное равенство верно только для октав, где *b* зависит от *a*.

3) октавы дистрибутивны:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

4) октавы неассоциативны по умножению:

$$a \cdot (b \cdot c) \neq (a \cdot b) \cdot c$$

данное равенство выполняется только для октав *a, b* и *c* частного вида, зависящих друг от друга специальным образом.

5) алгебра октав есть алгебра с делением:

$$r = \frac{p}{q} = \frac{p \cdot \bar{q}}{q \cdot \bar{q}} = \frac{p \cdot \bar{q}}{|q|^2}$$

6) алгебра октав альтернативна:

$a \cdot (a \cdot b) = (a \cdot a) \cdot b$ - левая альтернативность

$a \cdot (b \cdot b) = (a \cdot b) \cdot b$ - правая альтернативность

Дополнительные замечания.

Приведем основные тождества, применимые к октавам. Тождества базируются на понятии ассоциатора, коммутатора и йорданова произведения.

$(x,y,z) = (x \cdot y) \cdot z - x \cdot (y \cdot z)$ - ассоциатор

$[x,y] = x \cdot y - y \cdot x$ - коммутатор

$x \circ y = x \cdot y + y \cdot x$ - йорданово произведение.

Линеаризуя тождества, несложно получить, что

$(x,z,y) + (z,x,y) = 0$ & $(x,y,z) + (x,z,y) = 0$

Таким образом, ассоциатор есть кососимметрическая функция от *x*, *y*, *z*. В частности, $(x,y,x)=0$:

$$(x,y,x)=(x\cdot y)\cdot x-x\cdot(y\cdot x),\ (x\cdot y)\cdot x=x\cdot(y\cdot x)$$

Алгебры, удовлетворяющие этому условию, называются **эластичными**. Таким образом, **алгебра октав эластична**. Покажем на основе эластичности тождество:

$$(x\cdot y)\cdot\bar{x}=x\cdot(y\cdot\bar{x})$$

$$\big((Scl(x)+Vec(x))\cdot y\big)\cdot\big(Scl(x)-Vec(x)\big)=\big(Scl(x)\cdot y\big)\cdot Scl(x)+$$
$$+\big(Vec(x)\cdot y\big)\cdot Scl(x)-\big(Scl(x)\cdot y\big)\cdot Vec(x)-\big(Vec(x)\cdot y\big)\cdot Vec(x)$$

В силу того, что $Scl(x)$ для октав всегда есть действительное число, а в силу эластичности $\big(Vec(x)\cdot y\big)\cdot Vec(x)=Vec(x)\cdot\big(y\cdot Vec(x)\big)$, получаем:

$$\big((Scl(x)+Vec(x))\cdot y\big)\cdot\big(Scl(x)-Vec(x)\big)=\big(Scl(x)-Vec(x)\big)\cdot\big(y\cdot\big(Scl(x)-Vec(x)\big)\big)$$

Таким образом, для эластичной алгебры справедливо:

$$x\cdot(y\cdot\bar{x})=(x\cdot y)\cdot\bar{x}$$

Функция Клейнфелда:

$$f(w,x,y,z)=(w\cdot x,y,z)-(x,y,z)\cdot w-x\cdot(w,y,z)$$

Лемма 1. $f(w,x,y,z)$ - кососимметрическая, для любой пары равных аргументов $f(w,x,y,z)=0$

В силу правой альтернативности $f(w,x,y,y)=0$

Во всякой алгебре справедливо тождество:

$$(w\cdot x,y,z)+(w,x,y\cdot z)-(w,x\cdot y,z)-w\cdot(x,y,z)-(w,x,y)\cdot z=0$$

Достаточно раскрыть все ассоциаторы. Обозначив левую часть этого равенства через $g(w,x,y,z)$, получим:

$$-f(z,w,x,y)=g(w,x,y,z)-f(z,w,x,y)=(w\cdot x,y,z)+(w,x,y\cdot z)-$$
$$-(w,x\cdot y,z)-w\cdot(x,y,z)-(w,x,y)\cdot z-(z\cdot w,x,y)+w\cdot(z,x,y)+(w,x,y)\cdot z=$$
$$=(w\cdot x,y,z)+(y\cdot z,w,x)-(x\cdot y,z,w)-(z\cdot w,x,y)$$

Поменяв местами: $w,x,y,z\rightarrow x,y,z,w$ получим: $f=-f$

Используя $f(w,x,y,y)=0$, получим, что $f(w,x,y,z)=0$ при любых одинаковых аргументах. Из этого следуют тождества:

1) $(x\cdot x,y,z)=x\circ(x,y,z)$

2) $(x,y\cdot x,z)=x\cdot(x,y,z)$

3) $(x,x\cdot y,z)=(x,y,z)\cdot x$

4) $(x\cdot x,y,z)=(x,x\circ y,z)$

Тождества Муфанг:

Правое тождество Муфанг: $z\cdot(x\cdot y\cdot x)=\left[(z\cdot x)\cdot y\right]\cdot x$

Левое тождество Муфанг: $(x \cdot y \cdot x) \cdot z = x \cdot [y \cdot (x \cdot z)]$

Центральное тождество Муфанг: $x \cdot (y \cdot z) \cdot x = (x \cdot y) \cdot (z \cdot x)$

Вопросы о строении простых алгебр в том или ином многообразии являются одними из главных вопросов теории колец. Мы уже знаем один пример простой неассоциативной альтернативной алгебры - это алгебра Кэли-Диксона. Оказывается, что других простых неассоциативных альтернативных алгебр не существует. Этот результат доказывался с нарастанием общности на протяжении нескольких десятков лет разными авторами: вначале для конечномерных алгебр (Цорн, Шафер), затем для алгебр с нетривиальным идемпотентом (Альберт), для альтернативных тел (Брак, Клейнфелд, Скорнаков), для коммутативных альтернативных алгебр (Жевлаков) и т. д. Наибольшее продвижение было получено Клейнфелдом, доказавшим, что всякая простая альтернативная неассоциативная алгебра, не являющаяся ниль-алгеброй характеристики 3, есть алгебра Кэли-Диксона. Окончательное описание простых альтернативных алгебр осуществилось после появления теоремы Ширшова о локальной нильпонентности альтернативных ниль-алгебр с тождественными соотношениями.

Заключение.

В классификаторе были рассмотрены основные ассоциативные алгебры и алгебра октав. Некоторые ассоциативные алгебры, такие как бипаракватернионы, могут быть построены и рассмотрены по аналогии самостоятельно. Так же не было рассмотрено расширений алгебры октав коммутативным и дуальным удвоением. При необходимости их построение делается так же по аналогии.

Данный классификатор окажется полезным для практического применения имеющихся алгебр, а так же для выбора подходящей алгебры в качестве базового математического аппарата построения моделей в каждом конкретном случае.

16. Основы терии чисел

В основе этого раздела по теории алгебраических числе лежит работа А.Вейля «Основы теории чисел». Автор настоящей работы считает, что изложение взглядов А.Вейля по рассматриваемому вопросу будут очень важны и полезны при построении математических моделей объектов исследования. Главная тема предлагаемой читателю раздела— изложение теории полей классов. Мы считаем, что эта теория действительно является основой современной алгебраической теории чисел.

Наиболее существенные части теории полей классов были созданы Гильбертом в конце XIX века. За прошедшее с тех пор время было найдено несколько вариантов изложения, существенно изменился ее язык, но ее роль как центрального комплекса идей и результатов алгебраической теории чисел стала еще более ясной, чем во времена Гильберта.

Ниже приведено довольно подробное изложение теории полей классов, как основы построения моделей объектов. Особенностью такого построения этой теории является использование аналитических соображений, основанных на понятии ζ-функции. В этом можно видеть возврат к идеям Гильберта и его непосредственных продолжателей — в их работах использование аналитических методов играло большую роль. В книге А. Вейля аналитические понятия появляются в другом виде, чем у основателей теории полей классов — они связаны с интегрированием в локально компактных группах, являющихся произведениями вещественных и *p*-адических групп Ли. В этом можно видеть только новый язык — другой вариант прежнего изложения. Однако этот язык уже показал свою плодотворность при изучении арифметических аспектов теории алгебраических групп.

Материал настоящего раздела подводит читателя к широкому кругу вопросов — арифметике алгебраических групп, в ее связи с алгебраической геометрией и теорией бесконечномерных представлений, широко используемых в различных приложения математики, в том числе и в обобщенной теории моделирования.

16.0. Предварительные сведения и обозначения

Излагаемый метериал предполагает знание теории чисел в объеме изложенном в предыдущих разделах настоящей работы. Полезно, но не обязательно знакомство с *p*-адическими нормированиями поля рациональных чисел **Q** и определяемыми этими нормированиями его

пополнениями $\mathbf{Q}_p$. Предполагается, что читатель знаком с основными понятиями алгебры (группы, кольца, поля) и линейной алгебры (векторные пространства, тензорные произведения).

На протяжении всего раздела существенно используются основные свойства локально компактных коммутативных групп, в частности существование и единственность меры Хаара. Прежде чем браться за изучение настоящего раздела, читатель должен хотя бы в общих чертах познакомиться с этими вопросами. В работе коротко освещаются основные факты из теории двойственности локально компактных коммутативных групп, основные факты из теории преобразования Фурье, играющие существенную роль в дальнейшем изложении.

Что касается терминологии и обозначений, то они обычно совпадают с терминологией и обозначениями Бурбаки. В частности, это относится к символам **N** (множество «конечных кардинальных», или «натуральных» чисел 0, 1, 2, . . .), **Z** (кольцо рациональных целых чисел), **Q** (поле рациональных чисел), **R** (поле вещественных чисел), **C** (поле комплексных чисел), **H** (поле «классических», «обыкновенных», или «гамильтоновых» кватернионов). Если p — простое число, то мы обозначаем через $\mathbf{F}_p$ простое поле из p элементов, через $\mathbf{Q}_p$ — поле p-адических чисел (пополнение поля **Q** по отношению к p-адическому нормированию), через $\mathbf{Z}_p$ — кольцо p-адических целых чисел (т. е. замыкание **Z** в $\mathbf{Q}_p$). Всегда подразумевается, что поля **R, C, H,** $\mathbf{Q}_p$, равно как и конечномерные векторные пространства над ними, снабжены их обычной («естественной») топологией. Под $\mathbf{F}_q$ понимается конечное поле из q элементов, если таковое существует, т. е. если q имеет вид p^n, где p — простое число, а n — целое ≥ 1. Символ $\mathbf{R}_+$ обозначает множество всех вещественных чисел ≥ 0.

Предполагается, что все кольца имеют единицу. Единица кольца R обозначается через 1_R или просто 1, если это не может вызвать недоразумений; мультипликативная группа обратимых элементов кольца R обозначается через $R^\times$. В частности, если K — поле (не обязательно коммутативное), $K^\times$ —это мультипликативная группа его ненулевых элементов. Мультипликативную группу вещественных чисел >0 мы обозначаем через $R^\times{}_+$. Пусть R — произвольное кольцо. Символ $M_n(R)$ обозначает кольцо матриц с n строками и n столбцами с элементами из **R**, a 1_n —единицу этого кольца, т. е. матрицу (δ_{ij}), где $\delta_{ij} = 1_R$ или 0, в соответствии с тем, $i = j$ или $i \neq j$; ${}^tX$ обозначает матрицу, транспонированную к матрице $X \in M_n(R)$, а tr (X) — ее след, т. е. сумму диагональных элементов. В случае когда кольцо R коммутативно, через det (X) обозначаем определитель матрицы X. Иногда мы будем писать $M_{m,\,n}(R)$ для обозначения множества матриц с элементами из **R**, имеющих m строк и n столбцов.

Если R — коммутативное кольцо и T — переменная, то мы обозначаем через $R[T]$ кольцо многочленов от T с коэффициентами в R. Многочлен называется *унитарным,* если его старший коэффициент равен 1. Если S — кольцо, содержащее R, и x—его элемент, коммутирующий со всеми элементами из R, то мы обозначаем через $R[x]$ подкольцо в S, порожденное R и x. Оно состоит из элементов кольца S, имеющих вид $F(x)$, где $F \in R[T]$. Если K — коммутативное поле, L — некоторое (не обязательно коммутативное) поле, содержащее K, и x — элемент поля L, коммутирующий со всеми элементами из K, то мы обозначаем через $K(x)$ подполе в L, порожденное K и x. Это подполе коммутативно. Мы называем поле L «расширением» поля K, только если оба они коммутативны; обычно этот термин используется в случае, когда поле L конечной степени над K, и тогда $[L : K]$ обозначает его степень, т. е. размерность L, рассматриваемого как векторное пространство над K (индекс группы g' в группе g также обозначается через $[g: g']$, если он конечен; это не приводит к путанице).

Все топологии предполагаются *хаусдорфовыми,* т. е. удовлетворяющими аксиоме отделимости Хаусдорфа *(отделимыми* в смысле Бурбаки). Слово *гомоморфизм* для групп, колец, модулей, векторных пространств употребляется в следующем смысле:

(a) в случае когда имеются топологии, *все гомоморфизмы предполагаются непрерывными;*

(b) гомоморфизмы колец предполагаются *унитарными;* это означает, что гомоморфизм кольца R в кольцо S переводит 1_R в 1_S.

С другой стороны, в случае групп гомоморфизмы *не предполагаются открытыми* (т. е. переводящими открытые множества в открытые). Поэтому в случае надобности мы говорим об *открытом гомоморфизме.* Слово *морфизм* используется как краткий синоним слова *гомоморфизм.* В некоторых ситуациях в качестве синонима слова гомоморфизм используется также слово *представление,* например для гомоморфизмов заданной группы в $\mathbf{C}^\times$ или для некоторых гомоморфизмов простых алгебр. Под *характером* (не обязательно коммутативной) группы G будем понимать, как обычно, гомоморфизм (или «представление») группы G в подгруппу группы $\mathbf{C}^\times$, определяемую условием $z\bar{z} = 1$. Как было сказано выше, он предполагается непрерывным, если G — топологическая группа. Употребление слов *эндоморфизм, автоморфизм, изоморфизм* подчиняется тем же ограничениям (a) и (b), что и для слова гомоморфизм. Следовательно, в топологическом случае автоморфизмы и изоморфизмы суть отображения биективные и бинепрерывные. Если f — отображение множества A в множество B, причем оба эти

множества снабжены некоторыми структурами (обычно структурами поля) и f определяет изоморфизм A на его образ в B, то иногда, допуская вольность речи, мы говорим, что f — изоморфизм из A в B.

Говорят, что элемент x группы G имеет *порядок* n, если n — наименьшее целое ≥ 1, для которого $x^n = e$, где e — единичный элемент группы G. Если K — поле, то элемент конечного порядка из $K^\times$ называется *корнем из единицы в K'*; в согласии с давней традицией корень из единицы порядка, делящего n, называют корнем степени n из единицы в K; его называют *примитивным* корнем n-й степени из единицы, если его порядок равен n. Таким образом, корни n-й степени из единицы в K являются корнями в K уравнения $X^n = 1$.

Если a, b — элементы из $\mathbf{Z}$, то (a, b) обозначает их наибольший общий делитель, т. е. элемент d из $\mathbf{N}$, такой, что $d\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z}$. Пусть R — произвольное кольцо. Отображение $n \to n \cdot 1_R$ из $\mathbf{Z}$ в R переводит $\mathbf{Z}$ в подкольцо $\mathbf{Z} \cdot 1_R$ кольца R, известное под названием *простого кольца в R*. Ядро морфизма $n \to n \cdot 1_R$ из $\mathbf{Z}$ на $\mathbf{Z} \cdot 1_R$ является подгруппой в $\mathbf{Z}$ и, следовательно, имеет вид $m\cdot\mathbf{Z}$, где $m \in \mathbf{N}$. Если R не равно $\{0\}$ и не имеет делителей нуля, число m либо равно 0, либо просто; его называют *характеристикой* кольца R. Если $m = 0$, то отображение $n \to n \cdot 1_R$ является изоморфизмом кольца $\mathbf{Z}$ на $\mathbf{Z} \cdot 1_R$, что позволяет их отождествлять. Если же характеристика кольца R есть простое число $p > 1$, то простое кольцо $\mathbf{Z} \cdot 1_R$ изоморфно простому полю $\mathbf{F}_p$.

Рассматривая левые и правые модули над некоммутативными кольцами, мы будем использовать следующие обозначения. Пусть R — кольцо, M и N — левые модули над ним. Тогда морфизмы из M в N, сохраняющие их структуры как левых R-модулей, можно рассматривать как *правые операторы* на M; иначе говоря, если α — такой морфизм, то можно записывать его в виде $m \to m\alpha$, где $m \in M$, и свойство быть морфизмом означает, помимо аддитивности, что для всех $r \in R$ и $m \in M$ $r\,(m\alpha) = (rm)\,\alpha$. Это относится, в частности, к эндоморфизмам модуля M. Аналогичным образом морфизмы правых R-модулей можно записывать как левые операторы. Эта запись будет постоянно использоваться.

Поскольку морфизмы полей, как указывалось выше, предполагаются унитарными, они всегда инъективны. Поэтому в согласии со сказанным выше морфизм поля K в поле L мы будем иногда называть изоморфизмом или *вложением* поля K в L. Для таких отображений с первом случае будет использоваться «функциональная» запись, а во втором, где на сцену выходит теория Галуа,—«экспоненциальная» запись. В первом случае отображение λ записывается в

виде $x \to \lambda(x)$, а во втором — в виде $x \to x^{\lambda}$. Пусть L — расширение Галуа поля K и λ, μ — два его автоморфизма над K. Определим закон композиции $(\lambda, \mu) \to \lambda\mu$ в группе Галуа $\mathfrak{g}$ поля L над K как закон $(\lambda, \mu) \to \lambda \circ \mu$ в первом случае и как противоположный закон во втором случае. Иначе говоря, он определяется соответственно условиями $(\lambda\mu)x = \lambda(\mu x)$ и $x^{\lambda\mu} = (x^{\lambda})^{\mu}$. Например, если K' — поле, промежуточное между K и L, и $\mathfrak{h}$ — соответствующая подгруппа в $\mathfrak{g}$, состоящая из автоморфизмов, которые оставляют на месте все элементы поля K', то автоморфизмы поля L над K, совпадающие на K' с заданным автоморфизмом λ, образуют правый класс смежности $\lambda\mathfrak{h}$ в функциональной записи и левый класс $\mathfrak{h}\lambda$ — в экспоненциальной.

Пусть A, B, C — аддитивно записанные коммутативные группы (как правило, с дополнительными структурами), и пусть задан *дистрибутивный* (или *биаддитивный,* или *билинейный)* морфизм $(a, b) \to ab$ из $A \times B$ в C. В этом случае для двух подгрупп X и Y соответственно в A и B принято через $X \cdot Y$ обозначать не образ произведения $X \times Y$ относительно этого отображения, а подгруппу в C, порожденную этим образом, т. е. подгруппу, состоящую из конечных сумм вида $\sum x_i y_i$, где $x_i \in X$ и $y_i \in Y$ для всех i.

Мы часто пишем $\exp(z)$ вместо e^z и $\mathbf{e}(z)$ вместо $\exp(2\pi i z) = e^{2\pi i z}$ для $z \in \mathbf{C}$; обозначение $\mathbf{e}(z)$ применяется, как правило, лишь для $z \in \mathrm{R}$.

16.1. Локально компактные поля

16.1.1. Конечные поля

Пусть F — конечное (не обязательно коммутативное) поле с единичным элементом 1. Его характеристика является, очевидно, простым числом $p>1$, а простое кольцо, содержащееся в F, изоморфно простому полю $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, с которым оно может быть отождествлено. Таким образом, F можно рассматривать как векторное пространство над $\mathbf{F}_p$; очевидно, оно имеет конечную размерность f, а число его элементов равно $q=p^f$. Если F — подполе поля F', состоящего из $q' = p^{f'}$ элементов, F' можно также рассматривать, как, скажем, левое векторное пространство над F, и если его размерность равна d, то $f' = df$ и $q' = q^d = p^{df}$.

Теорема 1. *Все конечные поля коммутативны.*

Эта теорема впервые была доказана Веддербарном, и мы воспроизведем здесь принадлежащий Витту вариант его первоначального

доказательства. Пусть F — конечное поле характеристики p, Z — его центр, $q = p^f$ — число элементов в Z; если размерность поля F как векторного пространства над Z равна n, то F имеет q^n элементов. Мультипликативную группу $F^\times$ ненулевых элементов поля F можно разбить на классы «сопряженных» элементов, называя два элемента x, x' из $F^\times$ сопряженными, если существует элемент $y \in F^\times$, такой, что $x' = y^{-1}xy$. Для каждого $x \in F^\times$ обозначим через $N(x)$ множество элементов поля F, коммутирующих с x; это — подполе в F, содержащее Z; если $\delta(x)$ — его размерность над Z, то в нем имеется $q^{\delta(x)}$ элементов. Как мы видели выше, n кратно $\delta(x)$ и $\delta(x) < n$ при $x \notin Z$. Поскольку число элементов группы $F^\times$, сопряженных с x, равно индексу группы $N(x)^\times$ в $F^\times$, т. е. $(q^n - 1)/(q^{\delta(x)} - 1)$, получаем

$$q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{\delta(x)} - 1}, \qquad (1)$$

где сумма распространяется на полное множество представителей классов нецентральных сопряженных элементов из $F^\times$. Предположим теперь, что $n>1$, и обозначим через P «круговой» многочлен $\prod (T - \zeta)$, где произведение берется по всем примитивным корням n-й степени из 1 в поле **C** комплексных чисел. По хорошо известной элементарной теореме (легко доказываемой индукцией по n) этот многочлен имеет целые рациональные коэффициенты; ясно, что P делит $(T^n - 1)/(T^\delta - 1)$ для любых δ, делящих n и отличных от n. Следовательно, в (1) все члены, кроме q— 1, кратны $P(q)$, так что $P(q)$ должно делить q — 1. С другой стороны, каждый множитель в произведении $P(q) = \prod (q - \zeta)$ по абсолютной величине больше q — 1. Мы пришли к противоречию, значит n = 1, а F = Z.

Таким образом, к каждому конечному полю применим следующий элементарный результат.

Лемма 1. *Если K — коммутативное поле, то всякая конечная подгруппа в $K^\times$ циклична.*

Действительно, пусть Г — такая группа, или, что то же самое, конечная подгруппа группы всех корней из 1 в поле K. Для каждого $n \geq 1$ существует не более n корней уравнения $X^n = 1$ в поле K и, следовательно, в Г; покажем, что всякая конечная коммутативная группа с подобным свойством циклична. Пусть α — элемент группы Г, имеющий максимальный порядок N. Обозначим через β какой-нибудь элемент из Г и через n его порядок. Если n не делит N, то для некоторого простого числа p существует такая его степень $q = p^\nu$, что q делит n, но не N. Сразу проверяется, что порядок элемента $\alpha\beta^{n/q}$ есть наименьшее общее кратное N и q, так что он больше N, что противоречит определению N. Следовательно, n делит N. Поэтому

уравнение $X^n=1$ имеет в Г и различных корней $\alpha^{iN/n}$ с $0 \leqslant i < n$; поскольку β — корень этого уравнения, он обязан быть одним из них. Значит, α порождает группу Г.

Теорема 2. *Пусть К — алгебраически замкнутое поле характеристики p* > 1. *Тогда для каждого f*≥1 *поле К содержит одно и только одно поле F* =$\mathbf{F}_q$ *из q* = p^f *элементов; поле F состоит из корней уравнения* $X^q = X$ *в поле К; группа* $F^\times$ *состоит из корней уравнения* $X^{q-1} = 1$ *в поле К и является циклической группой порядка q* — 1.

Пусть F — произвольное поле из q элементов. Лемма 1 показывает, что $F^\times$ — циклическая группа порядка q—1. Поэтому, если K содержит поле F, группа $F^\times$ должна состоять из корней уравнения $X^{q-1} = 1$, а поле F — из корней уравнения $X^q - X = 0$, так что оба они однозначно определены. Обратно, если $q = p^f$, то $x \to x^q$ есть автоморфизм поля K, инвариантные элементы которого образуют поле F, состоящее из корней уравнения $X^q - X = 0$; так как, очевидно, многочлен $X^q - X$ имеет в поле K только простые корни, поле F состоит из q элементов.

Следствие 1. *С точностью до изоморфизма существует только одно поле из* $q = p^f$ *элементов.*

Это сразу следует из теоремы 2 и того факта, что все алгебраические замыкания простого поля $\mathbf{F}_q$ изоморфны. Этим оправдывается обозначение $\mathbf{F}_q$ для рассматриваемого поля.

Следствие 2. *Положим* $q = p^f$, $q' = p^{f'}$, *где* $f \geqslant 1$, $f' \geqslant 1$. *Поле* $\mathbf{F}_{q'}$ *содержит поле* $\mathbf{F}_q$ *из q элементов в том и только в том случае, когда f делит f'; если это так, то* $\mathbf{F}_{q'}$ *является циклическим расширением поля* $\mathbf{F}_q$ *степени* f'/f *и его группа Галуа над* $\mathbf{F}_q$ *порождается автоморфизмом* $x \to x^q$.

Как мы уже говорили, если поле $\mathbf{F}_{q'}$ содержит $\mathbf{F}_q$, то оно должно иметь над ним конечную степень d и $q' = q^d$, $f' = df$. Обратно, предположим, что $f' = df$, так что $q' = q^d$, и обозначим через K алгебраическое замыкание поля $\mathbf{F}_{q'}$. В силу теоремы 2 поля $\mathbf{F}_q$ и $\mathbf{F}_{q'}$, содержащиеся в K, состоят из элементов поля K, инвариантных соответственно относительно автоморфизмов α и β, определяемых формулами $x \to x^q$ и $x \to x^{q'}$; поскольку $\beta = \alpha^q$, поле $\mathbf{F}_{q'}$ содержит $\mathbf{F}_q$. Ясно, что α отображает поле $\mathbf{F}_{q'}$ на себя; если φ — автоморфизм поля $\mathbf{F}_{q'}$ индуцированный α, то $\mathbf{F}_q$ состоит из элементов, инвариантных относительно φ и, следовательно, относительно группы автоморфизмов поля $\mathbf{F}_{q'}$, порожденной φ; эта группа конечна, так как φ^d — тождественное отображение; используя теорию Галуа, получаем, что эта группа является группой Галуа поля $\mathbf{F}_{q'}$ над $\mathbf{F}_q$ и имеет порядок d.

Следствие 3. *В тех же обозначениях, что и в следствии* 2, *предположим, что f' = df. Тогда для каждого n*≥1 *элементы поля* $\mathbf{F}_{q'}$, *инвариантные относительно отображения* $x \to x^{q^n}$, *образуют подполе, состоящее из* q^r *элементов поля* $\mathbf{F}_{q'}$, *где r = (d, n).*

Пусть *K* — то же, что и в доказательстве следствия 2. Элементы поля *K,* инвариантные относительно отображения $x \to x^{q^n}$, образуют подполе *F'* поля *K* из q^n элементов; поэтому $F' \cap \mathbf{F}_{q'}$ будет наибольшим подполем, содержащимся как в *F',* так и в $\mathbf{F}_{q'}$, и поскольку оно содержит $\mathbf{F}_q$, число его элементов должно иметь вид q^r, где *r* равно, как показывает следствие 2, *(d, n).*

16.1.2. Модуль в локально компактном поле

Любое поле, снабженное дискретной топологией, становится локально компактным. Поэтому задача описания и изучения локально компактных полей становится содержательной лишь при условии недискретности рассматриваемого поля.

Напомним определение модуля автоморфизма, которое является основным для дальнейшего. Для наших целей достаточно рассматривать автоморфизмы локально компактных коммутативных групп. Пусть *G* — такая группа (записываемая аддитивно), λ — автоморфизм группы *G* и α — мера Хаара на *G.* Так как мера Хаара определена однозначно с точностью до константы, λ переводит α в меру *c*α, где $c \in \mathbf{R}_+^\times$; постоянный множитель *c,* который, очевидно, не зависит от выбора меры α, называется *модулем* автоморфизма λ и обозначается символом $\mathrm{mod}_G(\lambda)$. Иначе говоря, он определяется одной из следующих эквивалентных формул:

$$\alpha(\lambda(X)) = \mathrm{mod}_G(\lambda)\,\alpha(X),$$
$$\int f(\lambda^{-1}(x))\,d\alpha(x) = \mathrm{mod}_G(\lambda)\int f(x)\,d\alpha(x), \tag{2}$$

где *X* — произвольное измеримое множество, *f* — интегрируемая функция и

$$0 < \alpha(X) < +\infty, \quad \int f\,d\alpha \neq 0.$$

Вторую формулу символически можно записать так: $d\alpha(\lambda(x)) = \mathrm{mod}_G(\lambda)\,d\alpha(x)$. Если группа *G* дискретна или компактна, первая формула (примененная соответственно к $X = \{0\}$ и к $X = G$) показывает, что модуль равен 1. Ясно, что если λ, λ′ — автоморфизмы группы *G,* то модуль автоморфизма $\lambda \circ \lambda'$ равен произведению модулей λ и λ′. Нам понадобится следующая лемма:

Лемма 2. *Пусть G' — замкнутая подгруппа группы G и λ — автоморфизм группы G, индуцирующий на G' автоморфизм λ'. Положим $G'' = G/G'$ и обозначим через λ'' автоморфизм группы G'', определяемый λ по модулю G'. Тогда*

$$\mathrm{mod}_G(\lambda) = \mathrm{mod}_{G'}(\lambda')\,\mathrm{mod}_{G''}(\lambda'').$$

В самом деле, как хорошо известно, можно выбрать меры Хаара α, α', α'' на группах G, G', G'' так, чтобы для любой непрерывной функции f на G с компактным носителем выполнялось равенство

$$\int_G f(x)\,d\alpha(x) = \int_{G''}\left(\int_{G'} f(x+y)\,d\alpha'(y)\right) d\alpha''(\dot{x});$$

здесь $\dot{x}$ обозначает образ x в G'', а функция $\int f(x+y)\,d\alpha'(y)$, которая записана как функция от $x \in G$, но фактически постоянна на классах смежности по подгруппе G', рассматривается очевидным образом как функция от $\dot{x}$ на группе G''. Применяя к обеим частям автоморфизм λ, получаем утверждение леммы.

Пусть теперь K—произвольное топологическое поле и $a \in K^\times$. Тогда $x \to ax$ и $x \to xa$ — автоморфизмы его аддитивной группы, и если поле K локально компактно, то можно рассматривать их модули. Точно так же если V — топологическое левое векторное пространство над K, то $v \to av$ есть его автоморфизм для любого $a \in K^\times$, и если V локально компактно, можно определить модуль этого автоморфизма. Мы будем обозначать его через $\mathrm{mod}_V(a)$ и считать, что $\mathrm{mod}_V(0)$ равен 0. Иными словами, если μ — мера Хаара на V и X — произвольное измеримое подмножество в V, для которого $0 < \mu(X) < +\infty$ (например, компактная окрестность нуля), то для каждого $a \in K$ модуль $\mathrm{mod}_V(a)$ определяется соотношением

$$\mathrm{mod}_V(a) = \frac{\mu(aX)}{\mu(X)}.$$

В частности, для любого локально компактного поля K мы полагаем $\mathrm{mod}_K(a)$ равным модулю автоморфизма $x \to ax$, если $a \neq 0$, и равным 0, если $a = 0$. Позднее будет показано, что модуль автоморфизма $x \to xa$ тот же самый, что и у автоморфизма $x \to ax$. Ясно, что если $K = \mathbf{R}, \mathbf{C}$ или $\mathbf{H}$, то $\mathrm{mod}_K(a)$ равен соответственно $|a|$, $|a|^2 = a\bar{a}$ или $|a|^4 = (a\bar{a})^2$.

Вплоть до конца этого параграфа обозначим через K недискретное локально компактное поле (коммутативное или нет), а через α — меру Хаара его аддитивной группы.

Предложение 1. *Функция mod_K непрерывна на K, и $\mathrm{mod}_K(ab) = \mathrm{mod}_K(a)\,\mathrm{mod}_K(b)$ для всех $a, b \in K$.*

Последнее утверждение очевидно. Пусть X — компактная окрестность нуля в поле K. Для каждого $a \in K$ и каждого $\varepsilon > 0$ существует открытая окрестность U компактного множества aX, такая, что $\alpha(U) \leqslant \alpha(aX) + \varepsilon$; пусть W — окрестность точки a, для которой $WX \subset U$. Тогда для всех $x \in W$ имеем

$$\mathrm{mod}_K(x) \leqslant \mathrm{mod}_K(a) + \alpha(X)^{-1}\varepsilon.$$

Отсюда видно, что функция mod_K полунепрерывна сверху. В частности, она непрерывна в нуле. А поскольку $\mathrm{mod}_K(x) = \mathrm{mod}_K(x^{-1})^{-1}$ для $x \neq 0$, она также полунепрерывна снизу всюду на $K^\times$ и, следовательно, непрерывна.

Так как поле K недискретно, из предложения 1 следует, что для любого $\varepsilon > 0$ существует такое $a \in K$, что $0 < \mathrm{mod}_K(a) \leqslant \varepsilon$, а для любого $M > 0$ — такое $b \in K$, что $\mathrm{mod}_K(b) \geqslant M$. Поскольку mod_K — неограниченная функция, K не может быть компактно.

Предложение 2. *Для всех $m > 0$ множество B_m элементов $x \in K$, таких, что $\mathrm{mod}_K(x) \leqslant m$, компактно.*

Пусть V — компактная окрестность нуля в K, W — окрестность нуля, для которой $WV \subset V$. Как и выше, можно выбрать $r \in V \cap W$ так, чтобы $0 < \mathrm{mod}_K(r) < 1$; индукцией по n получаем, что $r^n \in V$ для всех $n \geq 1$. Если r' — какая-нибудь предельная точка последовательности $\{r^n\}_{n \geqslant 1}$, то $\mathrm{mod}_K(r')$ должен быть равен нулю, ибо $\mathrm{mod}_K(r^n)$ стремится к нулю при $n \to +\infty$. Таким образом, эта последовательность не имеет других предельных точек, кроме нуля, а так как она содержится в компактном множестве V, ее предел равен нулю. Возьмем теперь $m > 0$ и $a \in B_m$; поскольку $r^n a$ стремится к нулю, существует наименьшее целое $\nu \geqslant 0$, такое, что $r^\nu a \in V$; если a не принадлежит V, то $r^{\nu-1}a \notin V$ и, следовательно, $r^\nu a \in V - (rV)$. Обозначим через X замыкание множества $V - (rV)$. Ясно, что X компактно и 0 не принадлежит X; поэтому если положить $\mu = \inf_{x \in X} \mathrm{mod}_K(x)$, то $\mu > 0$. Пусть N — целое число, для которого $\mathrm{mod}_K(r)^N \leqslant \mu/m$. Тогда для

$$a \in B_m, \quad a \notin V$$

и ν, определенного, как выше, имеем

$$\mathrm{mod}_K(r)^N m \leqslant \mu \leqslant \mathrm{mod}_K(r^\nu a) = \mathrm{mod}_K(r)^\nu \mathrm{mod}_K(a) \leqslant \mathrm{mod}_K(r)^\nu m$$

и, следовательно, $\nu \leq N$. Таким образом, B_m содержится в объединении компактных множеств $V, r^{-1}V, \ldots, r^{-N}V$. Так как из предложения 1 следует, что B_m замкнуто, этим и завершается доказательство.

Следствие 1. *Множества B_m, $m > 0$, образуют фундаментальную систему окрестностей нуля в К.*

Пусть V — произвольная компактная окрестность нуля в поле K. Возьмем

$$m > \sup_{x \in V} \operatorname{mod}_K (x)$$

так, чтобы $B_m \supset V$, обозначим через X замыкание множества $B_m - V$ и положим

$$m' = \inf_{x \in X} \operatorname{mod}_K (x).$$

Тогда $0 \notin X$ и $X \subset B_m$. В силу предложения 2 X компактно, следовательно, $0 < m' \leqslant m$. Если $0 < \mu < m'$, то $B_\mu \subset B_m$, $B_\mu \cap X = \varnothing$ и потому $B_\mu \subset V$.

Следствие 2. *Для* $a \in K$ $\lim_{n \to +\infty} a^n = 0$ *в том и только в том случае, когда* $\operatorname{mod}_K (a) < 1$.

Следствие 3. *Дискретное подполе поля К конечно.*

Пусть L — такое поле. Если $a \in L$, то непременно $\operatorname{mod}_K (a) \leqslant 1$, ибо в противном случае последовательность $\{a^{-n}\}_{n \geqslant 0}$ содержалась бы в L в силу предложения 2 и не была бы дискретной. Значит, L есть дискретное подмножество компактного множества B_1 и, следовательно, конечно. Но ясно, что этого не может быть, если K — поле характеристики 0.

Теорема 3. *Пусть V — топологическое левое векторное пространство над полем К и V' — его конечномерное подпространство с базисом $\{v_1, \ldots, v_n\}$. Тогда отображение*

$$(x_1, \ldots, x_n) \longrightarrow \sum_{i=1}^{n} x_i v_i$$

пространства K^n в V' является изморфизмом структур топологических левых векторных пространств на K^n и V'; при этом V' замкнуто в V и локально компактно.

Пусть f — указанное выше отображение. Оно биективно, K-линейно и непрерывно по определению топологического векторного пространства. Чтобы показать, что оно изоморфизм, достаточно доказать, что отображение f^{-1} непрерывно, т. е. что f — открытое отображение; ввиду следствия 1 предл. 2 и линейности f нам нужно только показать, что образ множества $(B_m)^n$ относительно отображения f содержит окрестность нуля в V' для всех $m > 0$. Пусть S — подмножество пространства K^n, определенное условием

$$\sup_i \operatorname{mod}_K (x_i) = 1.$$

Тогда $0 \notin S$; множество S замкнуто в силу предложения 1 и содержится в $(B_1)^n$, а потому компактно согласно предложению 2. Поэтому $0 \notin f(S)$ и $f(S)$ компактно. Следовательно, существуют окрестность нуля W в V и некоторая окрестность нуля в K, имеющая вид B_ε, где $\varepsilon > 0$, такие, что $B_\varepsilon W \subset V - f(S)$, т. е. $yW \cap f(S) = \varnothing$ при $\mathrm{mod}_K(y) \leqslant \varepsilon$. Выберем теперь $m > 0$ и $a \in K$ так, чтобы $0 < \mathrm{mod}_K(a) \leqslant m\varepsilon$. Пусть $v = \sum x_i b_i$ — произвольная отличная от нуля точка в $V' \cap aW$. Подберем h так, чтобы

$$\sup_i \mathrm{mod}_K(x_i) = \mathrm{mod}_K(x_h).$$

Тогда $x_h \neq 0$. Положим

$$x_i^n = x_h^{-1} x_i,$$

где $1 \leq i \leq n$, и

$$v' = \sum_1^n x_i' v_i = x_h^{-1} v.$$

Поскольку $(x_1', \ldots, x_n')$ находится в S, имеем $v' \in f(S)$, а так как $v \in aW$, получаем, что $v' \in yW$, где $y = x_h^{-1} a$. По определению W и ε отсюда следует, что $\mathrm{mod}_K(y) > \varepsilon$ и, следовательно, $\mathrm{mod}_K(x_h) < \varepsilon^{-1} \mathrm{mod}_K(a) \leqslant m$. Поэтому $(x_1, \ldots, x_n)$ принадлежит множеству $(B_m)^n$ и v находится в образе этого множества относительно отображения f. Итак, мы показали, что этот образ содержит множество $V' \cap aW'$, являющееся окрестностью нуля в V'. Пусть теперь w принадлежит замыканию V' в пространстве V. Применяя только что доказанное к конечномерному подпространству V'', порожденному V' и w, видим, что V' должно быть замкнуто в V''. А так как отсюда вытекает, что $w \in V'$, доказательство теоремы завершено.

Следствие 1. *Каждое конечномерное левое векторное пространство над полем K можно снабдить одной и только одной структурой топологического левого векторного пространства над K.*

Действительно, если V имеет размерность n, то подобную структуру на V можно определить с помощью любого K-линейного биективного отображения K^n на V; единственность следует из теоремы 3, примененной к пространству V.

Начиная с этого места, мы будем без оговорок предполагать, что каждое такое векторное пространство снабжено структурой, определяемой этим следствием.

Следствие 2. *Если V — локально компактное топологическое левое векторное пространство над полем K, то оно имеет над K конечную размерность d и* $\mathrm{mod}_V(a) = \mathrm{mod}_K(a)^d$ *для любого* $a \in K$.

Для пространства размерности d последнее утверждение является следствием теоремы Фубини и того факта, что ввиду следствия 1 каждое такое пространство изоморфно пространству K^d. Предположим теперь лишь, что V локально компактно, и выберем $a \in K$ так, чтобы $0 < \mathrm{mod}_K(a) < 1$. Тогда в силу следствия 2 предл. 2 $\lim a^n = 0$ и потому $\mathrm{mod}_V(a) < 1$. Пусть V' — подпространство в V конечной размерности δ; по теореме 3 оно замкнуто. Положим $V'' = V/V'$. Ввиду леммы 2 получаем

$$\mathrm{mod}_V(a) = \mathrm{mod}_{V'}(a)\,\mathrm{mod}_{V''}(a) = \mathrm{mod}_K(a)^\delta\,\mathrm{mod}_{V''}(a)$$

и, следовательно,

$$\mathrm{mod}_V(a) \leqslant \mathrm{mod}_K(a)^\delta,$$

ибо $\mathrm{mod}_{V''}(a)$ должен быть меньше 1, если $V'' \neq \{0\}$, и равен 1, если $V'' = \{0\}$. Это дает оценку сверху для δ, верную для всех конечномерных подпространств пространства V, следовательно, V само имеет конечную размерность.

Если V — левое векторное пространство над K конечной размерности n, топологизированное так, как было сказано выше, то из теоремы Фубини следует, что каждое подпространство размерности $n' < n$ в V имеет меру 0. Пусть теперь A — произвольное K-линейное отображение пространства V в себя; если оно ранга n, то оно является автоморфизмом пространства V также и в топологическом смысле, и мы можем рассмотреть его модуль $\mathrm{mod}_V(A)$. Если же его ранг $n' < n$, то оно отображает V на подмножество меры 0, и мы положим $\mathrm{mod}_V(A)$ равным 0.

Следствие 3. *Пусть A — эндоморфизм левого векторного пространства V конечной размерности над K. Если поле K коммутативно, то* $\mathrm{mod}_V(A) = \mathrm{mod}_K(\det A)$.

Пусть n — размерность пространства V. Если ранг A меньше n, утверждение очевидно. Если нет, то, выбрав в V некоторый базис, отождествим V с пространством K^n. Как хорошо известно, каждый автоморфизм пространства K^n можно записать в виде произведения автоморфизмов следующих трех типов:

(a) перестановки координат,

(b) отображения вида

$$(x_1, \ldots, x_n) \to (ax_1, x_2, \ldots, x_n),$$

где $a \in K^\times$,

(c) отображения вида

$$(x_1, \ldots, x_n) \to \left(x_1 + \sum_{i=2}^{n} a_i x_i,\ x_2,\ \ldots,\ x_n\right).$$

Для автоморфизмов типа (a) утверждение очевидно; для автоморфизмов типов (b) и (c) оно получается непосредственным применением теоремы Фубини так же, как и в классическом анализе (где эта теорема доказывается для случая $K = \mathbf{R}$).

Предложение 3. *Функция* mod_K *индуцирует на группе* $K^\times$ *открытый гомоморфизм на замкнутую подгруппу* Γ *группы* $\mathbf{R}_+^\times$.

Обозначим через Γ, Γ' образы групп $K^\times$ и K относительно отображения mod_K. Ясно, что Γ — подгруппа в $\mathbf{R}_+^\times$ и что $\Gamma' = \Gamma \cup \{0\}$. Для каждого $m > 0$ пересечение группы Γ' с замкнутым интервалом $[0, m]$ является образом множества B_m относительно отображения mod_K; в силу предложений 1 и 2 оно компактно и, следовательно, группа Γ' замкнута в $\mathbf{R}_+$, а Γ в $\mathbf{R}_+^\times$. Пусть теперь U — ядро отображения mod_K в $K^\times$, т. е. множество $\{x \in K \mid \mathrm{mod}_K(x) = 1\}$. Обозначим через V произвольную окрестность единицы в $K^\times$ и через V' — ее образ относительно отображения mod_K; чтобы доказать открытость гомоморфизма mod_K из $K^\times$ на Γ, нужно показать, что V' — окрестность единицы в группе Γ. Предположим, что это не так. Тогда существует последовательность (γ_n) в Γ — V', такая, что $\lim \gamma_n = 1$. Для каждого n пусть $a_n \in K^\times$ таково, что $\gamma_n = \mathrm{mod}_K(a_n)$. По предложению 2 последовательность (a_n) имеет по меньшей мере одну предельную точку a; ясно, что $\mathrm{mod}_K(a) = 1$, т. е. $a \in U$. Но UV — окрестность множества U, поэтому существует n, для которого $a_n \in UV$ и, следовательно, $\gamma_n \in V'$. Но это противоречит условию.

Теорема 4. *Существует константа* $A > 0$, *такая, что*

$$\mathrm{mod}_K(x + y) \leqslant A \sup(\mathrm{mod}_K(x),\ \mathrm{mod}_K(y)) \tag{3}$$

для всех $x \in K$, $y \in K$. *Если неравенство* (3) *выполняется для* $A = 1$, *то образ подгруппы* Γ *в* $K^\times$ *относительно отображения* mod_K *дискретен в* $\mathbf{R}_+^\times$. *Более того, неравенство* (3) *выполняется для*

$$A = \sup_{x \in K,\ \mathrm{mod}_K(x) \leqslant 1} \mathrm{mod}_K(1 + x),$$

и это наименьшее значение A, для которого оно имеет место.

Определим A последней формулой; ясно, что $1 \leqslant A < +\infty$. Для $x = y = 0$ неравенство (3) очевидно. Поэтому можно считать, поменяв в случае необходимости x и y, что $x \neq 0$ и $\mathrm{mod}_K(y) \leqslant \mathrm{mod}_K(x)$. Положим $z = yx^{-1}$. Тогда $\mathrm{mod}_K(z) \leqslant 1$, $\mathrm{mod}_K(1 + z) \leqslant A$ и, следовательно,

$$\mathrm{mod}_K(x + y) = \mathrm{mod}_K(1 + z)\,\mathrm{mod}_K(x) \leqslant A\,\mathrm{mod}_K(x).$$

Неравенство (3) доказано. Полагая в формуле (3) $y = 1$ и $x \in B_1$, где B_1 такое же, как и в предложении 2, видим, что выбранное нами значение для A является наименьшим из всех, для которых выполняется (3). Предположим теперь, что A=1. Тогда образ множества $1 + B_t$ относительно отображения mod_K содержится в интервале [0, 1], а так как он в силу предложений 2 и 3 должен содержать окрестность единицы в Г, подгруппа Г должна быть дискретной.

Следствие. *Пусть неравенство* (3) *выполняется для* $A = 1$. *Тогда* $\mathrm{mod}_K (x + y) = \mathrm{mod}_K (y)$, *если* $\mathrm{mod}_K (y) < \mathrm{mod}_K (x)$.

Из равенства $(-1)^2 = 1$ вытекает, что $\mathrm{mod}_K (-1) = 1$ и, значит, $\mathrm{mod}_K (-y) = \mathrm{mod}_K (y)$. Так как $x = (x + y) + (-y)$, из наших предположений следует, что

$$\mathrm{mod}_K (x) \leqslant \sup (\mathrm{mod}_K (x + y), \mathrm{mod}_K (y)) \leqslant \mathrm{mod}_K (x),$$

чем наше утверждение и доказано.

Определение 1. *Неравенство* (3) *с* A=1 *называется ультраметрическим неравенством. Если оно выполняется, то говорят, что отображение* mod_K *и само поле К ультраметричны.*

16.1.3. Классификация локально компактных полей

Нам понадобится следующая элементарная лемма:

Лемма 3. *Пусть F — функция на множестве натуральных чисел* **N** *со значениями в* $\mathbf{R}_+$. *Предположим, что для всех m, n имеет место равенство* $F (mn) = F (m) F (n)$ *и что существует* $A>0$, *для которого*

$$F (m + n) \leqslant A \sup (F (m), F (n))$$

для всех m, n. Тогда или $F (m) \leq 1$ *для всех m, или для всех m выполняется равенство* $F (m) = m^{\lambda}$, *где* $\lambda > 0$.

Из первого предположения относительно F следует, для m — 0, что если функция F не равна тождественно 1, то $F (0) = 0$, а для $m = 1$, что $F (1) = 1$, если F не равна тождественно 0. Из него следует также, что $F (m^k) = F (m)^k$ для всех целых $k \geq 1$. Оставляя в стороне тривиальные случаи, когда F — константа, равная 0 или 1, мы можем считать, что $F (0) = 0$ и $F (m^k) = F (m)^k$ для всех целых $k \geq 0$. Положим $f (m) = \sup (0, \log F (m))$; подразумевается, что $f(m) = 0$ при $F (m) = 0$. Наша лемма равносильна теперь утверждению, что $f (m) = \lambda \log m$ для всех $m \geq 2$, где $\lambda \geqslant 0$ — некоторая константа. Пусть $a = \sup (0, \log A)$. Тогда для всех m, n, k имеем

$$f(m^k) = kf(m);\ f(mn) \leqslant f(m) + f(n),$$
$$f(m+n) \leqslant a + \sup(f(m),\ f(n)).$$

Из последнего соотношения индукцией по r получаем

$$f\left(\sum_{i=0}^{r} m_i\right) \leqslant ra + \sup_i (f(m_i)). \tag{4}$$

Если m, n — целые числа ≥ 2, то m можно представить в форме

$$m = \sum_{i=0}^{r} e_i n^i,$$

где $n^r \leqslant m < n^{r+1}$ и $0 \leqslant e_i < n$, $0 \leqslant i \leqslant r$. Положим

$$b = \sup(f(0),\ f(1),\ \ldots,\ f(n-1)).$$

Тогда для каждого i

$$f(e_i n^i) \leqslant b + if(n)$$

и, следовательно, ввиду (4)

$$f(m) \leqslant ra + b + rf(n).$$

Поскольку $n^r \leqslant m$, т. е. $r \log n \leqslant \log m$, отсюда вытекает, что

$$\frac{f(m)}{\log m} \leqslant \frac{a + f(n)}{\log n} + \frac{b}{\log m}.$$

Заменим в этом неравенстве m на m^k; это не изменит левой части. При $k \to +\infty$ получаем

$$\frac{f(m)}{\log m} \leqslant \frac{ra + f(n)}{\log n}.$$

Заменим теперь m на n^k. Устремляя k к $+\infty$, получаем

$$\frac{f(m)}{\log m} \leqslant \frac{f(n)}{\log n}.$$

Переставляя m и n, видим, что $f(m)/\log m$ есть константа при $m \geq 2$. Как было отмечено выше, отсюда следует утверждение леммы.

Рассмотрим теперь снова недискретное локально компактное поле K. Для большей ясности в оставшейся части этого параграфа единичный элемент поля K мы будем обозначать через 1_K (а не через 1). Простое кольцо в K состоит из элементов вида $m \cdot 1_K$, где $m \in \mathbf{Z}$, и если K — поле характеристики $p > 1$, то $p \cdot 1_K = 0$. Для $m \in \mathbf{N}$ положим $F(m) = \mathrm{mod}_K (m \cdot 1_K)$. Тогда для всех $m \in \mathbf{Z}$ и $x \in K$ имеем $\mathrm{mod}_K (mx) = F(|m|)\, \mathrm{mod}_K (x)$.

Лемма 4. *Предположим, что функция F ограничена, т. е. что отображение* mod_K *ограничено на простом кольце в K. Тогда* $F \leqslant 1$ *и отображение* mod_K *ультраметрично на K.*

Так как $F(mn) = F(m)\,F(n)$, первое утверждение очевидно. Пусть A такое же, как и в теореме 4 п.16.1.2, $n \geqslant 1$, $N = 2^n$ и $x_1, \ldots, x_N$ — какие-нибудь N элементов поля K. Индукцией по n получаем неравенство

$$\mathrm{mod}_K\left(\sum_{i=1}^{N} x_i\right) \leqslant A^n \sup_i \left(\mathrm{mod}_K(x_i)\right).$$

Заменяя некоторые из x_i нулями, видим, что это неравенство справедливо и при $N \leqslant 2^n$. Применяя его к соотношению

$$(x+y)^{2^n} = \sum_{i=0}^{2^n} \binom{2^n}{i} x^i y^{2^n-i},$$

находим

$$\mathrm{mod}_K(x+y)^{2^n} \leqslant A^{n+1} \sup_i \left(F\left(\binom{2^n}{i}\right) \mathrm{mod}_K(x)^i\, \mathrm{mod}_K(y)^{2^n-i}\right).$$

Предположим для определенности, что $\mathrm{mod}_K(y) \leqslant \mathrm{mod}_K(x)$. Поскольку $F \leqslant 1$, приходим к неравенству

$$\mathrm{mod}_K(x+y)^{2^n} \leqslant A^{n+1}\, \mathrm{mod}_K(x)^{2^n}.$$

Оно верно для всех $n \geqslant 1$; при $n \to +\infty$ получаем

$$\mathrm{mod}_K(x+y) \leqslant \mathrm{mod}_K(x),$$

т. е. ультраметрическое неравенство.

Напомним теперь определение обычных нормирований поля рациональных чисел $\mathbf{Q}$. Пусть сначала p — простое число. Каждое $x \in \mathbf{Q}^\times$ можно одним и только одним способом записать в виде $p^n a/b$, где n, a, b —целые числа, причем $b > 0$, а a и b взаимно просты друг с другом и с p. Положим $|x|_p = p^{-n}$, а также $|0|_p = 0$. Определенная таким образом на $\mathbf{Q}$ функция $x \to |x|_p$ называется *p-адическим нормированием* поля $\mathbf{Q}$. Оно, очевидно, удовлетворяет ультраметрическому неравенству и задает на $\mathbf{Q}$ некоторую топологию, а именно топологию, определяемую расстоянием

$$\delta(x, y) = |x - y|_p.$$

Пополнение поля $\mathbf{Q}$ по этой метрике называется *полем p-адических чисел.* Это поле обозначается через $\mathbf{Q}_p$. Замыкание множества $\mathbf{Z}$ в этом поле называется *кольцом p-адических целых чисел* и обозначается через $\mathbf{Z}_p$. Ясно, что p-адическое нормирование поля $\mathbf{Q}$ продолжается по непрерывности на $\mathbf{Q}_p$ и остается там ультраметричным; это продолжение обозначается также через $|x|_p$. Легко видеть, что $\mathbf{Z}_p$ компактно (по той причине, что $\mathbf{Z}_p$ есть, так сказать, «проективный предел» конечных групп $\mathbf{Z}/p^n\mathbf{Z}$ при $n \to +\infty$). Поскольку $\mathbf{Z}_p$ —

окрестность нуля в $\mathbf{Q}_p$, поле $\mathbf{Q}_p$ локально компактно и, очевидно, недискретно.

В тех случаях, когда это будет удобно, мы будем писать $|x|_\infty$ вместо $|x|$ для обозначения «обычного» абсолютного значения в полях **Q** и **R**. А так как **R** — не что иное, как пополнение поля **Q** по метрике $|x-y|_\infty$, мы будем иногда писать $\mathbf{Q}_\infty$ вместо **R**. Таким образом, символом $\mathbf{Q}_p$, где v может быть равно ∞ или простому числу, обозначается любое из пополнений $\mathbf{Q}_\infty = \mathbf{R}$ или $\mathbf{Q}_p$ поля **Q**.

Теорема 5. *Пусть K — недискретное локально компактное поле; положим $F(m) = \mathrm{mod}_K(m \cdot 1_K)$, $m \in \mathbf{N}$. Тогда либо* (a) *K, — поле характеристики $p > 1$ и $F(m) = 0$ при $m \equiv 0 \pmod p$ и $F(m) = 1$ при $(m, p) = 1$, либо* (b) *K — алгебра с делением конечной размерности δ над полем $\mathbf{Q}_v$ и $F(m) = |m|_v^\delta$.*

В силу предложения 1 и теоремы 4 п.16.1.2 F удовлетворяет условиям леммы 3 и, следовательно, либо имеет вид $m \to m^\lambda$, где $\lambda > 0$, либо всюду меньше 1. Предположим, что имеет место последнее; это означает, что последовательность $(m \cdot 1_K)$, $m \in \mathbf{N}$, содержится в B_1, где B_1 — множество из предложения 2 п.16.1.2; так как множество B_1 компактно, оно должно иметь по крайней мере одну предельную точку, скажем a. Но тогда, согласно следствию 1 предл. 2, для каждого $\varepsilon > 0$ существует бесконечно много чисел $m \in \mathbf{N}$, таких, что $\mathrm{mod}_K(m \cdot 1_K - a) \leqslant \varepsilon$. Пусть m, m' — два таких числа, $m < m'$. Поскольку из неравенства $F \leqslant 1$ следует, по лемме 4, что отображение mod_K ультраметрично, то мы имеем

$$\mathrm{mod}_K(m' \cdot 1_K - m \cdot 1_K) \leqslant \varepsilon,$$

т. е. $F(m' - m) \leqslant \varepsilon$. Отсюда видно, в частности, что существуют целые числа $n \geq 1$, для которых $F(n) < 1$.

Пусть p — наименьшее из таких чисел. Поскольку $F(mn)=F(m)F(n)$, ясно, что p должно быть простым. Для каждого $x \in \mathbf{N}$ имеем $F(px) < 1$ и, значит, $F(1 + px) = 1$ по следствию теор. 4 п.16.1. 2. Для любого целого $m \geqslant 1$, взаимно простого с p, имеем $m^{p-1} \equiv 1\ (p)$, следовательно, по только что доказанному $F(m^{p-1}) = 1$, откуда $F(m) = 1$. Если K — поле характеристики $p' > 1$, то $F(p^1) = 0$, так что p' не может быть отлично от p, и функция F такова, как утверждалось в (a). Если K — поле характеристики 0, то $F(p)$ не может равняться нулю и можно считать, что $F(p) = p^\lambda$, где $\lambda > 0$. Поэтому $F(m) = |m|_p^\lambda$ для всех m, что сразу видно, если записать m в виде $m = p^n m'$, где $(m', p) = 1$. Таким образом, если K — поле характеристики 0, то функция F должна иметь вид $m \to |m|_v^\lambda$, где $\lambda > 0$. Отображение $n \to n \cdot 1_K$ кольца $\mathbf{Z}$ в простое кольцо $\mathbf{Z} \cdot 1_K$ поля K

является в этом случае алгебраическим (но не обязательно топологическим) изоморфизмом, который можно продолжить до изоморфизма поля **Q** на простое подполе в *K*. Мы будем для простоты отождествлять последнее с полем **Q** при помощи этого изоморфизма. Из установленных свойств функции *F* следует, что отображение mod к индуцирует на поле **Q** функцию $x \to |x|_v^{\lambda}$. Следовательно, структура топологической группы, индуцированная полем *K* на поле **Q**, определяется метрикой $|x - y|_v$. А так как замыкание поля **Q** в *K* локально компактно и, следовательно, полно в этой структуре, мы видим, что оно изоморфно пополнению $\mathbf{Q}_v$ поля **Q** по нормированию *v*. Поскольку простое кольцо, а значит, и простое поле содержатся, очевидно, в центре поля *K,* то же самое справедливо и для поля $\mathbf{Q}_v$. Поле *K* можно рассматривать поэтому как векторное пространство над $\mathbf{Q}_v$, имеющее ввиду следствия 2 теор. 3 п.16.1.2 конечную размерность δ. Для всех $x \in \mathbf{Q}_v$ имеем $\mathrm{mod}_K(x) = \mathrm{mod}_{\mathbf{Q}_v}(x)^{\delta}$. Чтобы завершить доказательство, остается только показать, что в случае $v = \infty$ $\mathrm{mod}_{\mathbf{R}}(m) = m$ для $m \in \mathbf{N}$, но это очевидно, а в случае $v = p$ $\mathrm{mod}_{\mathbf{Q}_p}(p) = p^{-1}$. Это следует из того факта, что кольцо $\mathbf{Z}_p$ есть компактная окрестность нуля в $\mathbf{Q}_p$, а его образ $p \cdot \mathbf{Z}_p$ относительно отображения $x \to px$ является компактной подгруппой в $\mathbf{Z}_p$ индекса *p,* так что его мера равна $p^{-1}\alpha(\mathbf{Z}_p)$ для любой хааровокой меры α на $\mathbf{Q}_p$. Нам будет удобно сформулировать отдельно только что доказанное утверждение.

Следствие. *В случае* (b) *теоремы* 5 $\mathrm{mod}_K(x) = |x|_v^{\delta}$ *для* $x \in \mathbf{Q}_v$.

Определение 2. *Недискретное локально компактное поле K называется p-полем, если p — простое число и* $\mathrm{mod}_K(p \cdot 1_K) < 1$, *и* **R***-полем, если оно является алгеброй над полем* **R**.

В силу лемм 3 и 4 и теоремы 4 п.16.1. 2, если *K* есть *p*-поле, то образ Γ группы $K^{\times}$ относительно mod_K дискретен, поэтому такое поле не может быть связным; это показывает, что топологическое поле является **R**-полем в том и только том случае, когда оно связно и локально компактно. Как хорошо известно, не существует других **R**-полей, кроме **R, C** и поля **H** «обычных» (или «классических») кватернионов.

16.1.4. Структура *p*-полей

В этом параграфе *p* будет простым числом, а *K* — некоторым *p*-полем с единичным элементом 1.

Теорема 6. *Пусть K — некоторое p-поле, а R,* $R^{\times}$ *и P —*

подмножества в К, определяемые соответственно формулами

$$R = \{x \in K \mid \mathrm{mod}_K(x) \leqslant 1\},$$
$$R^\times = \{x \in K \mid \mathrm{mod}_K(x) = 1\},$$
$$P = \{x \in K \mid \mathrm{mod}_K(x) < 1\}.$$

Тогда поле К ультраметрично; R — единственное максимальное компактное подкольцо в К; $R^\times$ — группа обратимых элементов кольца R; P—единственный максимальный левый, правый или двусторонний идеал кольца R. Существует элемент $\pi \in P$, *такой, что* $P = \pi R = R\pi$. *Более того, поле вычетов* $k = R/P$ *есть поле характеристики p, и если q — число его элементов, то образ* Γ *группы* $K^\times$ *относительно отображения* mod_K *является подгруппой в* $\mathbf{R}_+^\times$, *порожденной q, и* $\mathrm{mod}_K(\pi) = q^{-1}$.

Множество R совпадает с введенным ранее множеством B_1; оно компактно, как и $R^\times$. По теореме 5 п.16.1.3 $\mathrm{mod}_K \leqslant 1$на простом кольце поля K; следовательно, по лемме 4 п.16.1.3 поле K, ультраметрично. В силу теоремы 4 п.16.1.2 последнее утверждение эквивалентно равенству $R + R = R$, а так как R, очевидно, замкнуто относительно умножения, мы видим, что R — кольцо. Ясно, что каждое относительно компактное замкнутое по умножению множество содержится в R; следовательно, R — максимальное компактное подкольцо поля K. Обратимые элементы в R — это как раз элементы из $R^\times$. По теореме 4 п.16.1.2 Γ — дискретная подгруппа в $\mathbf{R}_+^\times$; пусть γ — наибольший из меньших 1 элементов подгруппы Γ, и пусть $\pi \in K^\times$ таково, что $\mathrm{mod}_K(\pi) = \gamma$. Ясно, что γ порождает Γ; следовательно, для каждого $x \in K^\times$ существует одно и только одно целое n, для которого $\mathrm{mod}_K(x) = \gamma^n$, а тогда элементы $x\pi^{-n}$ и $\pi^{-n}x$ лежат в $R^\times$. Ясно, что $P = \pi R = R\pi$, откуда следует, что P компактно. Поскольку $R - P = R^\times$, P обладает свойствами максимальности, указанными в формулировке теоремы. Так как R — окрестность нуля и $R = R + R$, то R — открытое множество, как и P; а так как R компактно, поле $k = R/P$ конечно. Поскольку $p \cdot 1 \in P$, образ $p \cdot 1$ в поле k есть 0, так что это поле имеет характеристику p. Если в нем q элементов, то индекс $P = \pi R$ в аддитивной группе кольца R равен q. Следовательно, если α — мера Хаара поля K, то $\alpha(R) = q\alpha(\pi R)$ и потому $\mathrm{mod}_K(\pi) = q^{-1}$. Этим доказательство завершено.

Определение 3. *В обозначениях теоремы* 6 *будем называть q модулем поля К, а любой элемент* π *из* $K^\times$, *для которого* $P = \pi R = R\pi$, *— простым элементом поля К. Для каждого* $x \in K^\times$ *будем обозначать через* $\mathrm{ord}_K(x)$ *такое целое число, что* $\mathrm{mod}_K(x) = q^{-\mathrm{ord}_K(x)}$. *Для каждого* $n \in \mathbf{Z}$ *будем писать* $P^n = \pi^n R = R\pi^n$.

Мы будем писать ord (x) вместо $\mathrm{ord}_K(x)$, если это не может привести к недоразумению. Будем считать также, что ord $(0) = +\infty$; P^n будет тогда множеством элементов поля K, для которых $\mathrm{ord}\,(x) \geqslant n$. Пользуясь этими обозначениями, мы можем теперь сформулировать ряд следствий из теоремы 6.

Следствие 1. *Пусть $(x_0, x_1, \ldots)$ — произвольная, сходящаяся к нулю последовательность в поле К. Тогда ряд $\sum_0^{+\infty} x_i$ безусловно сходится в К.*

Для каждого $n \in \mathbf{N}$ положим

$$\varepsilon_n = \sup_{i>n} \mathrm{mod}_K (x_i).$$

Наше предположение означает, что $\lim \varepsilon_n = 0$. Пусть теперь S, S' — две конечные суммы членов ряда $\Sigma\, x_i$, содержащие каждая члены $x_0, x_1, \ldots, x_n$ и, возможно, другие члены. Ультраметрическое неравенство дает $\mathrm{mod}_K (S - S') \leqslant \varepsilon_n$. Отсюда следует требуемое утверждение («фильтр» конечных сумм ряда $\Sigma\, x_i$ является «фильтром Коши» относительно метрики mod_K $(x—y)$).

Следствие 2. *Пусть ξ — некоторый отличный от нуля элемент множества Р, $n = \mathrm{ord}\,(\xi)$ и А — полное множество представителей классов смежности по P^n в R. Тогда для всех $\nu \in \mathbf{Z}$ каждый элемент $x \in P^{n\nu}$ можно одним и только одним способом представить в виде*

$$x = \sum_{i=\nu}^{+\infty} a_i \xi^i,$$

где $a_i \in A$ для всех $i \geqslant \nu$.

Записывая x в виде $x = x'\xi^\nu$, где $x' \in R$, видим, что достаточно рассмотреть случай $\nu = 0$. В этом случае, используя индукцию по N, сразу видим, что можно одним и только одним способом определить элементы $a_i \in A$, удовлетворяющие условию

$$x \equiv \sum_{i=0}^{N} a_i \xi^i \quad (P^{n(N+1)})$$

$(N = 0, 1, \ldots)$. Это эквивалентно тому, что утверждается в нашем следствии.

Следствие 3. *Каждый автоморфизм поля К (как топологического поля) отображает R на R, Р на Р и имеет модуль* 1 *как автоморфизм аддитивной группы поля К.*

Следствие 4. *Для всех $a \in K^\times$ автоморфизмы $x \to ax$ и $x \to xa$ аддитивной группы поля К имеют одинаковый модуль.*

Это вытекает из следствия 3, примененного к автоморфизму $x \to a^{-1}xa$. Поскольку для поля **H** «обычных» кватернионов

аналогичный факт легко проверяется непосредственно, это следствие выполняется для всех локально компактных полей.

Следствие 5. *Пусть К — коммутативное р-поле, К′ — алгебра с делением над К. Тогда К′ есть р-поле; каждый автоморфизм (в алгебраическом смысле) алгебры К′ над К является топологическим автоморфизмом, и если R и R′—максимальные компактные подкольца полей К и К′, а Р и Р′ — максимальные идеалы колец R, R′, то* $R = K \cap R'$ *и* $P = K \cap P'$. Рассматривая K' как конечномерное векторное пространство над K, наделим его «естественной топологией» согласно следствию 1 теор. 3 п.16.1. 2. Из единственности топологии следует, что она инвариантна относительно всех K-линейных отображений алгебры K' на себя, и в частности относительно всех автоморфизмов K' над K. Отождествляя, как обычно, K с подполем $K \cdot 1_{R'}$ алгебры K', видим, что K' — недискретная алгебра. Остальные утверждения очевидны.

Следствие 6. *Пусть в условиях и обозначениях следствия* 5 q *и* q' *— модули полей К и К′ соответственно,* π *— простой элемент поля К и* $e = \mathrm{ord}_{K'}(\pi)$. *Тогда* $q' = q^f$, *где f — целое число* $\geqslant 1$ *и размерность поля К′ над К равна ef.*

Положим $k = R/P$ и $k' = R'/P'$; ввиду последнего утверждения следствия 5 можно отождествить поле k с образом кольца R в $k' = R'/P'$. Если f — степень поля k' над k, то $q' = q^f$. Применяя теперь следствие 2 теор. 3 п.16.1. 2 к $\mathrm{mod}_K(\pi)$ и $\mathrm{mod}_{K'}(\pi)$, получаем сформулированный выше результат.

Последнее следствие показывает, в частности, что число $\mathrm{ord}_{K'}(\pi)$ не меньше 1 и не зависит от выбора простого элемента π в поле K. Этим оправдано следующее определение.

Определение 4. В *условиях и обозначениях следствий* 5 *и* 6 *теор.* 6 *число e называется порядком ветвления поля К′ над К, а число f — модулярной степенью поля К′ над К. Говорят, что К′ неразветвлено над К, если e* = 1, *и вполне разветвлено, если f* = 1.

Предложение 4. *Пусть К — коммутативное р-поле; К′ — вполне разветвленная алгебра с делением конечной размерности над К; R, R′ — максимальные компактные подкольца полей К и К′ соответственно;* π' *— простой элемент поля К′. Тогда* $K' = K(\pi')$, $R' = R[\pi']$ *и алгебра К′ коммутативна.*

Пусть P, P' — максимальные идеалы колец R и R' соответственно, A — полное множество представителей классов смежности кольца R по идеалу P. Поскольку поле K' вполне разветвлено над K, следствия 5 и 6 теор. 6 показывают, что A является также полным множеством представителей классов смежности кольца R' по идеалу P'. Применяя

следствие 2 теор. 6 к K, R' и P', а также к A и $\xi = \pi'$, получаем, что элементы кольца R', имеющие вид $\sum_{i=0}^{e-1} a_i \pi'^i$, где $a_i \in A$ для $0 \leqslant i \leqslant e-1$, образуют полное множество A' представителей классов смежности по идеалу P'^e. Выберем теперь какой-нибудь простой элемент π поля K и положим $e = \operatorname{ord}_{R'}(\pi)$; e является порядком ветвления поля K' над K и, следовательно, размерностью поля K' над K (в силу следствия 6 теор. 6). Применяя снова следствие 2 теор. 6 к K', R', P'^e, A' и $\xi = \pi$, видим, что каждый элемент идеала P^{ev} можно записать одним и только одним способом в виде

$$\sum_{j=v}^{+\infty} a'_j \pi^j,$$

где $a'_j \in A'$ для всех $j \geqslant v$. Так как K содержится в центре алгебры K', то π' коммутирует с π, откуда в силу определения множества A' следует, что каждый рассматриваемый элемент записывается в виде

$$\sum_{i=0}^{e-1} \left(\sum_{j=v}^{+\infty} a_{ij} \pi^j \right) \pi'^i,$$

где $a_{ij} \in A$ для $0 \leqslant i \leqslant e-1$, $j \geqslant v$. Это равносильно, ввиду следствия 2 теор. 6, представлению в виде $\sum_{i=0}^{e-1} \alpha_i \pi'^i$, где $\alpha_i \in P^v$ для $0 \leqslant i \leqslant e-1$. Отсюда видно, что полагая $K' = K(\pi')$; $v = 0$, находим, что $R' = R[\pi']$. Поскольку K содержится в центре алгебры K', то π' коммутирует со всеми элементами поля K', следовательно, поле K' коммутативно.

Следствие 1. *Пусть K — коммутативное p-поле характеристики p. Обозначим через K^p его образ относительно эндоморфизма $x \to x^p$, и пусть π — какой-нибудь простой элемент в K. Тогда K — вполне разветвленное расширение степени p поля K^p и $K = K^p(\pi)$.*

Пусть $K' = K^p$; отображение $x \to x^p$ есть изоморфизм поля K на K', который можно использовать для перенесения топологии поля K на поле K'. Поэтому K можно рассматривать как топологическое векторное пространство над K', имеющее в силу следствия 2 теор. 3 п.16.1.2 конечную размерность. Это показывает, что K имеет конечную степень над K'. А так как поля K и K' изоморфны, они имеют одинаковый модуль, и модулярная степень поля K над K' равна 1. Это дает с учетом предложения 4 равенство $K = K'(\pi)$. Поскольку $\pi^p \in K'$, степень поля K над K' должна равняться p или 1. Но так как $\operatorname{ord}_K(\pi) = 1$, то π не принадлежит K^p и, значит, $K \neq K'$. Таким образом, поле K имеет над полем K' степень p.

Следствие 2. *Пусть К — то же, что и в следствии* 1, $\overline{K}$ *— его алгебраическое замыкание. Тогда для каждого* $n \geqslant 0$ *поле* $\overline{K}$ *содержит одно и только одно чисто несепарабельное расширение степени* p^n *поля К', оно является образом* $K^{p^{-n}}$ *поля относительно автоморфизма* $x \to x^{p^{-n}}$. Из следствия 1 вытекает, что поле $K^{p^{-1}}$ имеет над *К* степень *р;* индукцией по *n* получаем, что степень поля $K^{p^{-n}}$ над *К* равна p^n. С другой стороны, хорошо известен и легко доказывается тот факт, что если *К'* — чисто несепарабельное расширение степени $\leqslant p^n$ поля *К,* то оно содержится в поле $K^{p^{-n}}$. Отсюда следует наше утверждение.

Теорема 7. *Пусть К — некоторое р-поле, q — его модуль, R — максимальное компактное подкольцо и Р — максимальный идеал в R. Тогда группа* $K^\times$ *имеет по меньшей мере одну подгруппу порядка q*—1 *и каждая такая подгруппа циклична. Если* $M^\times$*— такая подгруппа, то* $M = M^\times \cup \{0\}$ *является полным множеством представителей классов смежности кольца R по идеалу Р и существует такой простой элемент* π *поля К, что* $\pi M^\times = M^\times \pi$. *Если поле К коммутативно, то существует только одна подобная группа* $M^\times$*, а именно группа корней из единицы в К степени, взаимно простой с р.*

Конструкция группы $M^\times$ основывается на следующей лемме.

Лемма 5. *Для всех* $n \geqslant 0$ *имеет место включение*

$$(1 + P)^{p^n} \subset 1 + P^{n+1}.$$

Это утверждение непосредственно проверяется индукцией по *n.* Его можно переформулировать еще так: $x^{p^n} \equiv 1 \ (P^{n+1})$, если $x \equiv 1 \ (P)$.

Обозначим теперь через ρ канонический гомоморфизм кольца *R* на поле $k = R/P$. По теореме 2 п.16.1.1 группа $k^\times$ циклична и ее порядок равен q — 1. В частности, для всех $x \in R^\times$ имеем $\rho(x)^{q-1} = 1$, т. е. $x^{q-1} \equiv 1 \ (P)$. Если $q = p^f$, то, согласно лемме 5, $x^{(q-1)q^n} \equiv 1 \ (P^{fn+1})$, что можно такжезаписать в виде

$$x^{q^{n+1}} \equiv x^{q^n} \quad (P^{fn+1}).$$

Снова, применяя следствие 1 теор. к ряду

$$x + (x^q - x) + (x^{q^2} - x^q) + \ldots,$$

видим, что он сходится при всех $x \in R^\times$, так что можно написать

$$\omega(x) = \lim_{n \to +\infty} x^{q^n}$$

для $x \in R^\times$ и, конечно, для $x \in P$, а значит, и для всех $x \in R$. Очевидно, $\omega(xy) = \omega(x)\,\omega(y)$, если $xy=yx;$ в частности, $\omega(x^\nu) = \omega(x)^\nu$ для всех $x \in R^\times$, $\nu \in \mathbf{Z}$. Как видно из написанного

выше ряда для $\omega(x)$, $\omega(x) \equiv x\ (P)$ для всех $x \in R$. Очевидно, $\omega(x) = 0$ для $x \in P$, и лемма 5 показывает, что $\omega(x) = 1$ для $x \in 1 + P$. Следовательно, $\omega^{-1}(0) = P$ и $\omega^{-1}(1) = 1 + P$. А так как $x^{q-1} \in 1 + P$ для всех $x \in R^\times$, то $\omega(x)^{q-1} = 1$ при $x \in R^\times$.

Выберем в группе $R^\times$ представитель x_1 образующей циклической группы $k^\times = (R/P)^\times$ и положим $\mu_1 = \omega(x_1)$. Равенство $\mu_1^n = 1$ имеет место для всех $n \in \mathbf{Z}$ в том и только в том случае, когда $\omega(x_1^n) = 1$; а так как последнее условие эквивалентно соотношению $x_1^n \equiv 1\ (P)$, а значит, ввиду выбора x_1, соотношению $n \equiv 0\ (q - 1)$, это показывает, что μ_1 порождает циклическую подгруппу в $R^\times$ порядка q— 1. Обратно, пусть Γ — произвольная конечная подгруппа группы $K^\times$, порядок которой взаимно прост с p; ясно, что она является подгруппой группы $R^\times$. Образ числа q в мультипликативной группе $(\mathbf{Z}/n\mathbf{Z})^\times$ целых чисел, взаимно простых с n и взятых по модулю n, должен иметь конечный порядок N; поэтому $q^N \equiv 1\ (n)$. Поскольку $z^n = 1$ при всех $z \in \Gamma$, мы получаем, что $z^{q^{Nv}} = z$ для всех $v \geqslant 0$ и всех $z \in \Gamma$, откуда $\omega(z) = z$. Таким образом, $z \equiv 1\ (P)$ влечет z=1. Полученный результат показывает, что ρ индуцирует инъективное отображение группы Γ в $k^\times = (R/P)^\times$; отсюда следует, что группа Γ циклична, что ее порядок делит q — 1 и что, если он равен q — 1, то множество $\Gamma \cup \{0\}$ образует полную систему представителей поля R/P в R. В частности, для коммутативного поля K получаем, что отображение ω индуцирует на $R^\times$ морфизм группы $R^\times$ на группу $M^\times$ корней из единицы в K степени q — 1, отображает кольцо R на множество $M = M^\times \cup \{0\}$ и определяет биекцию поля R/P на M. Кроме того, каждая подгруппа Γ группы $K^\times$, порядок которой взаимно прост с p, содержится в $M^\times$; в частности, $M^\times$ содержит все корни из единицы в K порядка взаимно простого с p. Что касается существования простого элемента поля K, удовлетворяющего требованиям нашей теоремы, то оно очевидно, если поле K коммутативно. Предположим, что это не так, и возьмем какой-нибудь простой элемент π поля K/ Для каждого $a \in K^\times$ отображение $x \to axa^{-1}$ есть автоморфизм поля K и, значит, согласно следствию 3 теор. 6, отображает R на R, P на P, определяя тем самым автоморфизм $\lambda(a)$ поля $k = R/P$. Отображение $a \to \lambda(a)$ есть, очевидно, гомоморфизм группы $K^\times$ в группу автоморфизмов поля k. Для $a \in R^\times$ $\lambda(a)$ есть отображение $\xi \to \rho(a)\,\xi\rho(a)^{-1}$, которое тождественно, ибо поле k коммутативно. Поэтому если a — элемент из $K^\times$ с $\operatorname{ord}(a) = n$, то $\lambda(a) = \lambda(\pi)^n$. В силу следствия 2 теор. 2 п.16.1.1, примененного к полю k и его простому подполю, $\lambda(\pi)$ имеет вид $\xi \to \xi^{p^r}$; это означает, что для всех $x \in R$

$$\pi x \pi^{-1} \equiv x^{p^r} (P),$$

или, что то же самое,

$$\pi x \equiv x^{p^r} \pi (P^2).$$

Выберем теперь $M^\times$ так же, как и выше, и положим

$$\pi' = -\sum_{\mu \in M^\times} \mu^{p^r} \pi \mu^{-1}.$$

Как следует из написанных выше сравнений, каждое из $q - 1$ слагаемых суммы в правой части сравнимо с π по модулю P^2. Поскольку $q \cdot 1 \in P$, получаем

$$\pi' \equiv (1 - q)\, \pi \equiv \pi (P^2),$$

откуда следует, что π' — простой элемент поля K. В то же время из определения π' видно, что

$$\pi' \mu = \mu^{p^r} \pi'$$

для всех $\mu \in M^\times$ и, следовательно, $\pi' M^\times = M^\times \pi'$, чем и завершается доказательство. Аналогичными рассуждениями можно доказать, что если $M^\times$ и $N^\times$ —две подгруппы порядка $q - 1$ группы $K^\times$, то существует простой элемент поля π, такой, что $\pi M^\times = N^\times \pi$.

Следствие 1. *Если K и M таковы, как в теореме 7, и K — поле характеристики p, то M — подполе поля K. Если при этом поле K коммутативно, то M является алгебраическим замыканием, простого поля в K.*

Пусть k_0 — простое поле в K и μ — образующая группы $M^\times$. Тогда $k_0(\mu)$ есть коммутативное поле характеристики p, в котором уравнение $X^q - X = 0$ имеет q корней, являющихся элементами группы M, откуда следует в силу теоремы 2 п.16.1.1, что M — поле. Если K коммутативно, то каждый отличный от нуля элемент алгебраического замыкания поля k_0 в K является корнем из единицы степени, взаимно простой с p (снова по теореме 2 п.16.1.1), и, значит, должен лежать в M (теорема 7).

Следствие 2. *Пусть K — коммутативное p-поле, q — его модуль, K′ — расширение конечной степени поля K, порожденное корнями из единицы степени, взаимно простой с p. Тогда K′ неразветвлено и циклично над K, а его группа Галуа над K порождена автоморфизмом* φ, *индуцирующим перестановку* $\mu \to \mu^q$ *на группе корней из единицы степени, взаимно простой с p.*

Из следствия 5 теор. 6 вытекает, что K' есть p-поле. Пусть $R, P, q, k, \rho, M^\times$ таковы, как в теореме 7 и ее доказательстве, а $R', P', q', k', \rho', M'^\times$— аналогичные объекты для поля K'. По теореме 7 K' порождается над K множеством $M'^\times$, т. е. корнями уравнения $X^{q'-1} = 1$; поэтому оно есть расширение Галуа поля K, а его автоморфизмы над K однозначно определяются теми перестановками,

которые они индуцируют в множестве M^κ. По следствию 5 теор. 6 $R = R' \cap K$, $P = P' \cap K$, и, следовательно, мы можем отождествить k с подполем поля k', причем ρ будет отображением, индуцируемым морфизмом ρ' на R. Пусть α — автоморфизм поля K' над K. Он отображает R' на R', P' на P' и оставляет на месте каждый элемент из R; следовательно, он определяет автоморфизм $\lambda(\alpha)$ поля k' над k. При этом λ, т. е. отображение $\alpha \to \lambda(\alpha)$, является морфизмом группы Галуа поля K' над K в группу Галуа поля k' над k. По следствию 2 теор. 2 п.16.1.1 $\lambda(\alpha)$ должно иметь вид $\xi \to \xi^{q^s}$. Отсюда получаем, что для всех $\mu \in M'^\times$

$$\rho'(\alpha(\mu)) = \rho'(\mu)^{q^s} = \rho'(\mu^{q^s}).$$

По теореме 7 ρ' индуцирует на M^κ изоморфизм группы M^κ на $k^{\prime\kappa}$; поэтому $\alpha(\mu) = \mu^{q^s}$. В частности, если $s = 0$, т. е. если $\lambda(\alpha)$ — тождественное отображение, то отображение α также тождественно; это показывает, что λ инъективно; поэтому если n — степень поля K' над K и f — степень k' над k, то $n \leqslant f$. А поскольку $q' = q^f$, из следствия 6 теор. 6 вытекает, что поле K' неразветвлено над K и $n = f$. Таким образом, λ является изоморфизмом группы Галуа поля K' над K на группу Галуа поля k' над k, чем ввиду следствия 2 теор. 2 п.16.1.1 и завершается наше доказательство.

Следствие 3. *Пусть K и q таковы, как в следствии* 2; *тогда алгебра с делением конечной размерности над K неразветвлена в том и только в том случае, когда она коммутативна и порождается над K корнями из единицы степени, взаимно простой с p. Для каждого $f \geqslant 1$ поле K имеет с точностью до изоморфизма одно и только одно неразветвленное расширение степени f; это расширение порождается над K, примитивным корнем $(q^f - 1)$-й степени из единицы.*

Пусть K' — неразветвленная алгебра с делением размерности f над K и q, q' — соответственно модули алгебр K и K'. Тогда по следствию 6 теор. 6 $q' = q^f$. Возьмем подгруппу M^κ порядка $q' - 1$ в $K'^\times$; по теореме 7 она циклична; взяв образующую μ в M^κ, получим поле $K'' = K(\mu)$. Ясно, что это поле коммутативно, а так как оно содержит $M'^\times$, то модуль его равен по меньшей мере q', так что по следствию 6 теор. 6 его степень над K не меньше f. Следовательно, $K'' = K'$, что вместе со следствием 2 доказывает первую часть нашего следствия. Возьмем теперь любое целое $f \geqslant 1$, положим $q' = q^f$ и обозначим через K' расширение поля K, порожденное примитивным корнем степени $q' - 1$ из единицы, или, что то же самое, множеством $M'^\times$ всех корней уравнения $X^{q'-1} = 1$. По теореме 7 модуль поля K' не меньше q', так что из следствия 6 теор. 6 вытекает, что степень K' над K равна по меньшей мере f. С другой стороны, в силу следствия 2

K' неразветвлено и циклично над K и его группа Галуа порождается определенным в этом следствии автоморфизмом φ. Так как автоморфизм φ^f индуцирует тождественный автоморфизм на $M'^{\times}$, то он тождествен и, следовательно, степень K' над K не больше f. Таким образом, она равна f. Из предыдущих результатов следует, что каждое неразветвленное расширение поля K, имеющее степень f, должно содержать расширение, изоморфное K'. Этим наше доказательство завершается.

Следствие 4. *Пусть K' — конечное расширение коммутативного p-поля K', обозначим через f его модулярную степень над K, а через e порядок ветвления над K. Тогда существует единственное максимальное неразветвленное расширение K_1 поля K, содержащееся в K'. Оно имеет степень f над K, и K' вполне разветвлено и имеет степень e над K_1.*

Это сразу следует из предыдущих результатов, если в качестве K_1 взять поле, порожденное содержащимися в K' корнями из единицы степени, взаимно простой с p.

Определение 5. *Пусть K — коммутативное p-поле и K' — его неразветвленное расширение. Образующая φ группы Галуа поля K' над K, определяемая следствием 2 теор. 7, называется автоморфизмом Фробениуса поля K' над K.*

В следствии 2 теор. 6 можно взять в качестве ξ простой элемент π поля K, а в качестве A —множество M, определенное в теореме 7. Для коммутативных полей характеристики p отсюда получается следующая

Теорема 8. *Каждое коммутативное p-поле характеристики p изоморфно полю формальных степенных рядов от одной переменной с коэффициентами из некоторого конечного поля.*

В обозначениях теоремы 7 следствие 1 из этой теоремы показывает, что M является полем из q элементов. Положив $\xi = \pi$ и $A = M$ в следствии 2 теор. 6, мы получим для каждого $x \in K$ с $\operatorname{ord}(x) \geqslant n$ единственное разложение в ряд

$$x = \sum_{i=n}^{+\infty} \mu_i \pi^i,$$

где $\mu_i \in M$ для всех $i \geqslant n$. Немедленно устанавливается, что эти ряды складываются и умножаются по обычным алгебраическим правилам для формальных степенных рядов (или для сходящихся степенных рядов в классическом анализе). Более того, полученное соответствие является также изоморфизмом и в топологическом смысле, если поле формальных степенных рядов снабдить обычной топологией, в которой фундаментальную систему окрестностей нуля образуют

кольцо R_0 «целых» степенных рядов (т. е. рядов, не содержащих степеней переменной с показателем <0) и идеалы в нем, порожденные степенями переменной. Напомним, что в этой топологии кольцо R_0 целых формальных степенных рядов от одной переменной над произвольным конечным полем F компактно, поскольку его аддитивная группа изоморфна, очевидно, произведению счетного числа групп, изоморфных F. Таким образом, соответствующее поле локально компактно. Поскольку в силу теоремы 8 все коммутативные p-поля характеристики p являются полями такого типа, получаем, что (с точностью до изоморфизма) существует взаимно однозначное соответствие между этими полями и конечными полями $\mathbf{F}_q$ с $q = p^n$, $n \geqslant 1$.

Под *локальным полем* будет пониматься в дальнейшем коммутативное недискретное локально компактное поле. Мы только что получили полный список локальных полей характеристики $p > 1$; что же касается полей характеристики 0, то все они даются теоремой 5 из п.16.1.3. Это **R, C** и конечные алгебраические расширения полей $\mathbf{Q}_p$ для всех p.

Используя ту же идею, что и в доказательстве теоремы 8, можно получить более общий результат для некоммутативного случая.

Предложение 5. *Пусть K — некоторое p-поле, коммутативное или нет, с максимальным компактным подкольцом R. Тогда центр K_0 поля K является p-полем, и если d — его модулярная степень над K_0, то порядок ветвления его над K_0 равен d, а размерность равна d^2. Поле K содержит максимальное коммутативное подполе K_1, которое неразветвлено и имеет степень d над K_0. Кроме того, если K_1 — такое подполе и R_1 — его максимальное компактное подкольцо, то в K существует простой элемент π со следующими свойствами:* (a) π^d *есть простой элемент поля K_0;* (b) $\{1, \ldots, \pi^{d-1}\}$ *есть базис поля K, рассматриваемого как левое векторное пространство над K_1, и порождает R как левый R_1-модуль;* (c) *внутренний автоморфизм $x \to \pi^{-1}x\pi$ поля K индуцирует в K_1 автоморфизм α, порождающий группу Галуа поля K_1 над K_0.*

Пусть обозначения таковы, как в теоремах 6 и 7; выберем M и π так же, как в теореме 7, и применим к ним следствие 2 теор. 6. Получим, что для всех $n \in \mathbf{Z}$ каждый элемент $x \in P^n$ может быть представлен единственным образом в виде

$$x = \sum_{i=n}^{+\infty} \mu_i \pi^i, \tag{5}$$

где $\mu_i \in M$ для всех $i \geqslant n$. Поэтому элемент поля K находится в центре K_0 этого поля в том и только в том случае, когда он ком-

мутирует с π и с каждым элементом из M (или, что то же самое, с какой-нибудь образующей циклической группы $M^\times$). Так как автоморфизм $x \to \pi^{-1}x\pi$ индуцирует перестановку множества M, то некоторая его степень тождественна на M. Иначе говоря, существует такое $\nu > 0$, что π^ν коммутирует с каждым элементом из M. Поэтому множество K_0 содержит $\pi^{\nu n}$ для всех $n \in \mathbf{Z}$, чем доказана его недискретность, а поскольку оно, очевидно, замкнуто в K, получаем, что поле K локально компактно. Если мы рассмотрим теперь K как векторное пространство и, следовательно, алгебру над K_0, то по следствию 2 теор. 3 п.16.1.2 оно имеет конечную размерность над K_0. Следствие 5 теор. 6 показывает теперь, что K_0 есть p-поле. Обозначим через q модуль поля K_0, через d — модулярную степень K над K_0 и через K_1— поле, порожденное над K_0 множеством M, или, что то же самое, любой образующей циклической группы $M^\times$. Поскольку $M^\times$ имеет порядок $q^d - 1$, такая образующая является примитивным корнем степени $q^d - 1$ из единицы, так что по следствию 3 теор, 7 K_1 неразветвлено и имеет степень d над K_0. Так как отображение $x \to \pi^{-1}x\pi$ индуцирует перестановку на M и тождественное отображение на K_0, оно определяет в K_1 автоморфизм α поля K_1 над K_0. Элементы из K_1 коммутируют со всеми элементами из M; с π они коммутируют в том и только в том случае, когда они инвариантны относительно α. Другими словами, элементы поля K_1, инвариантные относительно α, совпадают с K_0, так что α порождает группу Галуа поля K_1 над K_0. Следовательно, α имеет порядок d, откуда, как мы видели выше, следует, что π^d находится в K_0, а π^ν не принадлежит K_0, если ν не кратно d. Возьмем теперь $x \in K$ и $\mu \in M^\times$ и запишем x в виде (5). Мы получим

$$\mu^{-1}x\mu = \sum_{i=n}^{+\infty} \mu_i'\pi^i,$$

где

$$\mu_i' = \mu^{-1}\mu_i \cdot (\pi^i\mu\pi^{-i}).$$

В последней формуле последний множитель в правой части принадлежит группе $M^\times$, так что элементы μ_i' находятся в M. Ввиду единственности для $x \in K$ разложения (5) отсюда вытекает, что $x = \mu^{-1}x\mu$ (т. е. x коммутирует с μ) в том и только в том случае, когда $\mu_i' = \mu_i$ для всех i. Ясно, однако, что $\mu_i' = \mu_i$ тогда и только тогда, когда или $\mu_i = 0$, или π^i коммутирует с μ. Следовательно, x коммутирует со всеми элементами из $M^\times$ тогда и только тогда, когда π^i обладает этим свойством для всех i, для которых $\mu_i \neq 0$. В силу доказанного выше последнее имеет место в том и только в том случае,

когда $\mu_i = 0$ для всякого i, не являющегося кратным d. Мы можем поэтому написать

$$x = \sum_i \mu_{d_i} (\pi^d)^i.$$

Поскольку $\pi^a \in K_0$, элемент x принадлежит замыканию поля K_1, и, следовательно, ему самому, откуда видно, что K_1 — максимальное коммутативное подполе в K. Ввиду разложения (5) и единственности этого разложения ясно также, что $\{1, \pi, \ldots, \pi^{a-1}\}$ есть базис поля K, рассматриваемого как левое векторное пространство над K_1; что этот базис порождает R как левый R_1-модуль и что π^d есть простой элемент поля K_1 и, следовательно, поля K_0, поскольку он в нем лежит. Так как отсюда следует, что порядок ветвления K над K_0 есть d, доказательство окончено.

Пусть в обозначениях предложения 5 φ — автоморфизм Фробениуса поля K_1 над K_0. Так как он тоже порождает группу Галуа поля K_1 над K_0, то $\varphi = \alpha^r$, где r взаимно просто с d и определено однозначно по модулю d. Далее будет показано, что для данного K_0 числа d и rг, удовлетворяющие этим условиям, можно выбирать произвольно и что они однозначно определяют структуру алгебры с делением K. Другими словами, две алгебры с делением конечной размерности над K_0 и с центром K_0 изоморфны тогда и только тогда, когда они имеют одинаковую размерность d^2 над K_0 и целое число r для обеих алгебр одно и то же по модулю d.

Мы завершим эту главу одним результатом о максимальных компактных подкольцах p-полей. Напомним, что если R — произвольное коммутативное кольцо и x — элемент кольца, содержащего R, то этот элемент называется *целым над* R, если он является корнем некоторого унитарного многочлена над R, т. е. некоторого многочлена с коэффициентами из R, старший коэффициент которого равен 1.

Предложение 6. *Пусть K есть p-поле, K_0 — некоторое p-поле, содержащееся в его центре, R, R_0 — максимальные компактные подкольца полей K и K_0 соответственно. Тогда R состоит из элементов поля K, целых над R_0.*

Пусть элемент x принадлежит K и цел над R_0; это означает, что он удовлетворяет уравнению

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

в котором $a_i \in R_0$ для $1 \leqslant i \leqslant n$. Предположим, что x не лежит в R, т. е. что $\operatorname{ord}_K (x) < 0$. Тогда $x \neq 0$ и

$$1 = -a_1 x^{-1} - \ldots - a_n x^{-n};$$

все члены в правой части находятся в максимальном идеале P кольца R, так что $1 \in P$, что невозможно. Обратно, пусть x принадлежит R. По

следствию 2 теор. 3 п.16.1.2 K имеет конечную размерность над K_0; значит, коммутативное поле K', определяемое равенством $K' = K_0(x)$, является конечным расширением поля K_0. Обозначим через F неприводимый унитарный многочлен с коэффициентами из K_0, такой, что $F(x) = 0$. Пусть K'' — содержащееся в каком-нибудь алгебраическом замыкании поля K' поле, порожденное всеми корнями многочлена F, так что F разлагается в K'' на линейные множители. Поскольку K', K'' суть конечные расширения поля K_0, они являются p-полями; пусть R', R'' — их максимальные компактные подкольца. Тогда $R' = K' \cap R = K' \cap R''$, а так как элемент x лежит в R, он принадлежит как R', так и R''. Поскольку многочлен F неприводим, каждый его корень x' в K'' является образом корня x относительно некоторого автоморфизма поля K'' над K_0, а так как такой автоморфизм отображает R'' на R'', все эти корни лежат в R''. Таким образом, все коэффициенты многочлена F находятся в R'', а поскольку они принадлежат K_0, они лежат в R_0, чем доказательство и завершено.

Если поле K коммутативно, предложение 6 можно выразить, сказав, что R является целым замыканием кольца R_0 в K.

16.2. Решетки и двойственность над локальными полями

16.2.1. Нормы

В этом и следующем параграфах K будет обозначать p-поле, не обязательно коммутативное. Мы будем рассматривать большей частью левые векторные пространства над K; все, однако, может быть распространено очевидным образом и на правые векторные пространства. Все векторные пространства будут конечной размерности; кроме того, всегда будет предполагаться, что они снабжены «естественной» топологией согласно следствию 1 теор. 3 п. 16.1.2. По теореме 3 п. 16.1.2 каждое подпространство такого пространства V замкнуто в V. Используя координаты, легко доказать, что все линейные отображения таких пространств друг в друга непрерывны; в частности, непрерывны все линейные формы. Аналогичным образом каждое линейное инъективное отображение такого пространства V в некоторое другое является изоморфизмом V на его образ. Так как K некомпактно, то всякое подпространство в V, кроме $\{0\}$, некомпактно.

Определение 1. *Пусть V — левое векторное пространство над p-полем K. Под K-нормой на V понимается функция N со значениями в*

$\mathbf{R}_+$, *такая, что:* (i) $N(v) = 0$ *в том и только в том случае, когда* $v = 0$; (ii) $N(xv) = \mathrm{mod}_K(x)\, N(v)$ *для всех* $x \in K$ *и всех* $v \in V$; (iii) *для всех* v, w *выполняется ультраметрическое неравенство*

$$N(v + w) \leqslant \sup(N(v), N(w)). \tag{1}$$

На K^n можно определить K-норму N_0, положив $N_0(x) = \sup_{1 \leqslant i \leqslant n} (\mathrm{mod}_K(x_i))$ для всех $x = (x_1, \ldots, x_n)$ из K^n. Поскольку каждое векторное пространство конечной размерности над K изоморфно пространству K^n, получаем, что на всех таких пространствах существуют K-нормы.

Ясно, что с помощью произвольной K-нормы на V можно топологизировать V, взяв $N(v - w)$ в качестве метрики.

Предложение 1. *Пусть* V — *левое векторное пространство конечной размерности над* p-*полем* K. *Каждая* K-*норма* N *на* V *определяет на* V *естественную топологию. В частности, каждая такая норма* N *непрерывна, и для всех* $r > 0$ *подмножества* L_r *в* V, *определяемые условием* $N(v) \leqslant r$, *являются компактными окрестностями нуля.*

Что касается первого утверждения, то в силу следствия 1 теор. 3 п.16.1.2 нужно только показать, что топология, определяемая нормой N на V, превращает V в топологическое векторное пространство над K. Это сразу следует из неравенства

$$N(x'v' - xv) \leqslant \sup(\mathrm{mod}_K(x')\, N(v' - v),\ \mathrm{mod}_K(x' - x)\, N(v)),$$

которое является непосредственным следствием определения 1. Следовательно, норма N непрерывна, и множества L_r образуют фундаментальную систему замкнутых окрестностей нуля. В частности, для некоторого $r > 0$ множество L_r должно быть компактно. Выберем теперь для произвольного $s > 0$ элемент $a \in K^\times$ так, чтобы $\mathrm{mod}_K(a) \leqslant r/s$; сразу видно, что множество L_r содержится в $a^{-1}L_r$ и, следовательно, компактно.

Следствие 1. *В* $V - \{0\}$ *существует компактное подмножество* A, *которое содержит скалярное кратное любого элемента* v *из* $V - \{0\}$.

Обозначим через q модуль поля K и выберем какую-нибудь K-норму N на V. Если π — простой элемент поля K, то в силу теоремы 6 п. 16.4 $\mathrm{mod}_K(\pi) = q^{-1}$ и потому для всех $n \in \mathbf{Z}$ и всех $v \in V$ имеет место равенство $N(\pi^n v) = q^{-n} N(v)$. Пусть A — под множество в V, определенное условием $q^{-1} \leqslant N(v) \leqslant 1$; в силу предложения 1 оно компактно, и для каждого $v \neq 0$ можно найти $n \in \mathbf{Z}$, такое, что $\pi^n v \in A$.

Следствие 1 означает, что «проективное пространство», связанное с V, компактно.

Следствие 2. *Пусть* φ *— произвольная непрерывная функция на* $V - \{0\}$ *со значениями в* $\mathbf{R}$, *такая, что* $\varphi(av) = \varphi(v)$ *для всех* $a \in K^{\times}$ *и всех* $v \in V - \{0\}$. *Тогда* φ *достигает максимума в некоторой точке* v_1 *из* $V - \{0\}$.

В самом деле, достаточно взять множество A из следствия 1 и выбрать в качестве v_1 ту точку множества A, в которой φ достигает максимума на A.

Следствие 3. *Пусть* f *— произвольная линейная форма на* V *и* N *— некоторая* K*-норма на* V. *Тогда в* V *существует элемент* $v_1 \neq 0$, *такой, что для всех* $v \neq 0$ *из* V

$$N(v)^{-1} \bmod_K (f(v)) \leqslant N(v_1)^{-1} \bmod_K (f(v_1)). \qquad (2)$$

Это частный случай следствия 2, примененного к левой части неравенства (2). Если обозначить правую часть (2) через $N^*(f)$, то $N^*(f)$ будет наименьшим положительным числом, таким, что

$$\bmod_K (f(v)) \leqslant N^*(f)\, N(v)$$

для всех $v \in V$; соответствие $f \to N^*(f)$ будет K-нормой на пространстве, двойственном к V, т. е. на правом векторном пространстве линейных форм на V (сложение форм определяется очевидным образом, а умножение на скаляр производится по правилу $(fa)(v) = f(v)\, a$, где f— форма, а $a \in K$).

Под *гиперплоскостью* в V понимается подпространство коразмерности 1, т. е. подмножество H в V, определенное уравнением $f(v) = 0$, где f — линейная форма, отличная от нуля. Если H задано, то f определяется однозначно с точностью до отличного от нуля скалярного множителя. Далее, если формула (2) выполняется при всех $v \neq 0$, для заданных нормы N, линейной формы $f \neq 0$ и элемента $v_1 \neq 0$, то это же будет верно, если заменить f на fa, где $a \in K^{\times}$, и v_1 на bv_1 где $b \in K^{\times}$. Другими словами, справедливость неравенства (2) для всех $v \neq 0$ зависит лишь от свойств гиперплоскости H, определяемой уравнением $f = 0$, и подпространства W в V, порожденного вектором v_1. В случае когда (2) выполняется для всех $v \neq 0$, говорят, что H и W N*-ортогональны* друг другу.

Предложение 2. *Гиперплоскость* H *и подпространство* W *в* V *размерности* 1 N*-ортогональны тогда и только тогда, когда* V *является прямой суммой* H *и* W *и* $N(h + w) = \sup(N(h), N(w))$ *для всех* $h \in H$ *и* $w \in W$.

Пусть H определено уравнением $f(v) = 0$, и пусть H и W N-ортогональны. Тогда, если заменить в (2) v_1 на любое отличное от нуля $w \in W$, то (2) будет справедливо. Отсюда следует, что $f(w)$ не

равно нулю; следовательно, V есть прямая сумма H и W. Заменим теперь в (2) v на $h + w$, где $h \in H$; поскольку $f(h + w) = f(w) \neq 0$, из (2) вытекает, что $N(h + w) \geqslant N(w)$. Применяя ультраметрическое неравенство (1) к $h = (h + w) + (-w)$, получаем $N(h) \leqslant N(h + w)$; применение этого неравенства к $h + w$ дает доказываемую формулу при $w \neq 0$, а так как она тривиальна при $w = 0$, необходимость нашего условия доказана. Пусть теперь V есть прямая сумма H и W. Выберем какое-нибудь $v \neq 0$ и запишем его в виде $v = h + w$, где $h \in H$ и $w \in W$, так что $f(v) = f(w)$.

Если $w \neq 0$ и $N(h + w) \geqslant N(w)$, то

$$N(v)^{-1} \bmod_K (f(v)) \leqslant N(w)^{-1} \bmod_K (f(w)).$$

Поскольку правая часть неравенства не изменится, если заменить w любым вектором v_1, порождающим подпространство W, мы видим, что (2) выполняется для каждого такого v_1 и произвольного v, не лежащего в H. При $v \in H$, т. е. при $w = 0$, оно выполняется тривиальным образом, чем доказательство и завершено.

Аналогичным образом будем говорить, что два подпространства V', V'' из V *N-ортогональны* друг другу, если V является их прямой суммой и $N(v' + v'') = \sup(N(v'), N(v''))$ для всех $v' \in V'$ и $v'' \in V''$.

Предложение 3. *Пусть V имеет размерность n над K, и пусть N — некоторая K-норма на V. Тогда существует разложение $V = V_1 + \ldots + V_n$ пространства V в прямую сумму подпространств V_i размерности* 1, *для которого $N(\Sigma v_i) = \sup_i N(v_i)$ при $v_i \in V_i$, $1 \leqslant i \leqslant n$. Более того, если $W_1 = V$, $W_2, \ldots, W_n$ — последовательность подпространств в V, такая, что W_i есть подпространство в W_{i-1} коразмерности то 1, $2 \leqslant i \leqslant n$, подпространства V_i можно выбрать так, чтобы $W_i = V_i + \ldots + V_n$ для всех i.*

Это очевидно для $n = 1$. Если $n > 1$, то воспользуемся индукцией по n. В силу следствия 3 предл. 1 можно выбрать v_1 так, чтобы пространство V_1, порожденное v_1, было N -ортогонально к W_2; по предложению 2 тогда $N(v_1' + w_2) = \sup(N(v_1'), N(w_2))$, $v_1' \in V_1$, $w_2 \in W_2$. Применяя предположение индукции к K-норме, индуцированной на W_2 нормой N, и к последовательности $W_2, \ldots, W_n$, получаем наш результат.

Следствие. *Для каждого подпространства W в V существует подпространство W', N-ортогональное к W.*

Выберем последовательность подпространств $W_1, \ldots, W_n$, такую, как в предложении 3, для которой W является одним из ее членов, скажем

W_i. Возьмем V_i из предложения 3. Пространство $W' = V_1 + \ldots + V_{i-1}$ будет тогда N -ортогонально к W.

Предложение 4. *Пусть N и N' — две К-нормы на V. Тогда существует разложение $V = V_1 + \ldots + V_n$ пространства V в прямую сумму подпространств V_i размерности 1, такое, что*

$$N(\Sigma v_i) = \sup_i N(v_i) \quad и \quad N'(\Sigma v_i) = \sup_i N'(v_i)$$

при $v_i \in V_i \qquad 1 \leq i \leq n$.

Это очевидно для $n = 1$. Для $n > 1$ используем индукцию по n. Применяя следствие 2 предл. 1 к $\varphi = N/N'$, получаем вектор $v_1 \neq 0$, такой, что для всех $v \neq 0$

$$N(v)\, N'(v)^{-1} \leqslant N(v_1)\, N'(v_1)^{-1}.$$

Обозначим через V_1 пространство, порожденное вектором v_1. По следствию предл. 3 существует гиперплоскость W, которая N-ортогональна к V_1; если $f = 0$ — уравнение этой гиперплоскости, то

$$N(v)^{-1} \bmod_K (f(v)) \leqslant N(v_1)^{-1} \bmod_K (f(v_1))$$

для всех $v \neq 0$. Перемножая эти два неравенства, находим

$$N'(v)^{-1} \bmod_K (f(v)) \leqslant N'(v_1)^{-1} \bmod_K (f(v_1));$$

это означает, что W N'-ортогонально к V_1. Применяя теперь предложение 2 к N, V_1, W, а также к N', V_1, W, а предположение индукции к нормам, индуцированным на W нормами N и N', получаем утверждаемый результат.

Следует отметить тесную аналогию между предложениями 3 и 4 с их доказательствами и соответствующими результатами и доказательствами для норм, определяемых положительно определенными квадратичными формами в векторных пространствах над **R** или эрмитовыми формами в пространствах над **C** или **H**. Так, например, предложение 4 соответствует одновременному приведению двух квадратичных или эрмитовых форм к диагональному виду.

16.2.2. Решетки

В этом параграфе будут использоваться обозначения, введенные в п.16.1, и K снова будет обозначать p-поле. В частности, мы по-прежнему будем обозначать через R максимальное компактное подкольцо в K, через P — максимальный идеал в R, через q — модуль поля K и через π — его простой элемент. Для $n \in \mathbf{Z}$ полагаем $P^n = \pi^n R = R\pi^n$.

Мы будем рассматривать R -модули в левом векторном пространстве конечной размерности над K; если V — такое пространство, то R -модуль в V есть подгруппа M в V, такая, что $R \cdot M = M$.

Предложение 5. *Пусть V — левое векторное пространство конечной размерности над K и M — некоторый R-модуль в V. Обозначим через W подпространство в V, порожденное над K множеством M. Множество M открыто и замкнуто в W; оно компактно в том и только в том случае, когда оно конечно порождено как R-модуль.*

Пусть $m_1, \ldots, m_r$ — максимальное множество линейно независимых над K элементов из M; они образуют базис пространства W над K. Согласно теореме 3 п.16.1.2, множество $Rm_1 + \ldots + Rm_r$ является открытой подгруппой в W; а поскольку оба множества, M и W — M, являются объединениями классов смежности по отношению к этой подгруппе, оба они открыты. Если M компактно, то оно является объединением конечного числа таких классов и, следовательно, конечно порождено; обратное очевидно.

Далее, в силу следствия 2 теор. 6 п.16.1.4 замкнутая подгруппа X в V удовлетворяет условию $R \cdot X = X$ в том и только в том случае, когда $\pi X \subset X$ и $aX \subset X$ для каждого a из некоторой полной системы A представителей поля R/P в R. В частности, если $q = p$, т. е. если R/P — простое поле, можно взять $A = \{0, 1, \ldots, p-1\}$, так что $aX \subset X$ для всех $a \in A$, и, значит, X является R –модулем тогда и только тогда, когда $\pi X \subset X$. В случае $K = \mathbf{Q}_p$ можно взять $\pi = p$, тогда каждая замкнутая подгруппа является R -модулем.

В самом K, рассматриваемом как левое векторное пространство над K, каждый R -модуль, не сводящийся к $\{0\}$, является объединением множеств P^n и, следовательно, совпадает или с K, или с одним из этих множеств.

Определение 2. *K-решеткой в левом векторном пространстве V конечной размерности над K, называется компактный открытый R-модуль в V.*

Мы будем говорить просто «решетка» вместо «K-решетка», если это не сможет вызвать недоразумений. Если L есть p-поле, содержащееся в K, то каждая K-решетка является L-решеткой; обратное неверно, если $L \neq K$. Если L—решетка в V и W—подпространство в V, то ясно, что $L \cap W$ — решетка в W. Аналогично если f — инъективное линейное отображение пространства V' в V, то $f^{-1}(L)$—решетка в V', и если f — сюръективное линейное отображение пространства V на V'', то $f'(L)$ — решетка в V''.

Если N — некоторая K-норма в V, то множества L_r, определяемые условием $N(v) \leqslant r$, являются K-решетками для любого $r>0$. Действительно, условие (iii) из определения 1 п.16.2.1 вместе с условием (ii), примененным к $x = -1$, показывает, что множество L есть

подгруппа в V; из (ii) следует тогда, что оно есть R-модуль, а из предложения 1 п.16.2.1, что оно есть компактная окрестность нуля в V и, следовательно, открыто, поскольку является подгруппой. Это утверждение допускает обращение. Более общим образом имеет место следующее

Предложение 6. *Пусть M — открытый R-модуль в V; для каждого $v \in V$ положим*

$$N_M(v) = \inf_{x \in K^\times,\, xv \in M} \mathrm{mod}_K(x)^{-1}.$$

Тогда N_M как функция на V удовлетворяет условиям (ii) *и* (iii) *определения* 1 р.16.2.1 *и M есть подмножество в V, определяемое уравнением $N_M(v) \leqslant 1$. Функция N_M является K-нормой в том и только в том случае, когда M есть K-решетка в V.*

Если $a \in K^\times$, то $x \cdot av \in M$ тогда и только тогда, когда $x = ya^{-1}$, где $yv \in M$; это дает равенство $N_M(av) = \mathrm{mod}_K(a)\, N_M(v)$, справедливое также и для $a = 0$, ибо $N_M(0) = 0$. Таким образом, N_M удовлетворяет условию (ii) определения 1. Для каждого $v \in V$ пусть M_v — множество элементов x из K, для которых $xv \in M$; поскольку оно — открытый R-молулъ в K, то оно совпадает или с K, или с P^n для некоторого $n \in \mathbf{Z}$. Если $M_v = K$, то $N_M(v) = 0$; а если $M_v = P^n$, то $xv \in M$ в том и только в том случае, когда $\mathrm{mod}_K(x) \leqslant q^{-n}$, так что $N_M(v) = q^n$. В частности, $N_M(v) \leqslant 1$ тогда и только тогда, когда $M_v \supset R$, т. е. когда $v \in M$. Пусть v, w принадлежат V и таковы, что $N_M(v) \geqslant N_M(w)$; тогда $M_v \subset M_w$ и $xv \in M$ влечет $xw \in M$, откуда $x(v + w) \in M$. Поэтому $M_{v+w} \supset \supset M_v$ и, следовательно, $N_M(v + w) \leqslant N_M(v)$; этим доказано условие (iii) из определения 1. Наконец, множество M является K-решеткой в том и только в том случае, когда оно компактно, а N_M является K-нормой в том и только в том случае, когда $N_M(v) > 0$ для всех $v \neq 0$, т. е. тогда и только тогда, когда $M_v \neq K$ для $v \neq 0$. По предложению 1 п.16.2.1, если N_M есть K-норма, то M компактно. Обратно, предположим, что M компактно, и выберем $v \neq 0$. Тогда M_v есть подмножество в K, соответствующее множеству $(Kv) \cap M$ при изоморфизме $x \to xv$ из K на Kv, поэтому M_v компактно и не может совпадать с K. Доказательство завершено.

Следствие 1. *Открытый R-модуль M в V является K-решеткой в том и только в том случае, когда он не содержит отличных от нуля подпространств в V.*

Как было показано выше, если M некомпактно, то N_M не может быть K-нормой, так что в V существует элемент $v \neq 0$, такой, что $N_M(v) = 0$ и, следовательно, $M_v = K$, т. е. $Kv \subset M$.

Обратно, поскольку каждое отличное от нуля подпространство в V замкнуто в V и некомпактно, такое подпространство не может содержаться в множестве M в силу компактности последнего.

Следствие 2. *Пусть M — открытый R-модуль в V, W — максимальное подпространство в V, содержащееся в M, W — какое-нибудь дополнительное к W подпространство в V. Тогда $M \cap W'$ является K-решеткой в W и $M = (M \cap W') + W$.*

Первое утверждение есть частный случай следствия 1, второе очевидно.

Предложение 6 показывает, что каждая K-решетка в V может быть определена неравенством $N(v) \leqslant 1$, где N — некоторая K-норма. Вот главная причина, почему мы посвятили п.16.2.1 рассмотрению норм. Для заданной K-решетки M норма N_M, определяемая предложением 6, может быть охарактеризована среди всех норм N, для которых M есть множество $N(v) \leq 1$, как норма, принимающая свои значения в множестве значений функции mod_K на K, т. е. в множестве $\{0\} \cup \{q^n\}_{n \in Z}$.

Предложение 7. *Если V имеет над K размерность 1 и если L есть K-решетка в V, то в V существует образующая v, такая, что $L = Rv$.*

Возьмем какую-нибудь образующую w пространства V; подмножество L_w в K, определяемое условием $xw \in L$, должно иметь вид P^n; беря $v = \pi^n w$, получаем $L = Rv$.

Теорема 1. *Пусть L — некоторая K-решетка в левом векторном пространстве V размерности n над K. Тогда в V существует базис $\{v_1, \ldots, v_n\}$, такой, что $L = \sum Rv_i$. Кроме того, если $W_1 = V, W_2, \ldots, W_n$ — последовательность подпространств в V, обладающая тем свойством, что W_i есть подпространство в W_{i-1} коразмерности $1, 2 \leqslant i \leqslant n$, то элементы v_i можно выбрать так, чтобы для каждого i множество $\{v_i, \ldots, v_n\}$ было базисом в W_i.*

Возьмем K-норму N, такую, что L определяется уравнением $N(v) \leqslant 1$. Выберем подпространства $V_1, \ldots, V_n$ из V так же, как в предложении 3 п.16.2.1. Тогда $L = \sum (L \cap V_i)$. Применяя предложение 7 для каждого i к V_i и $L \cap V_i$, получаем базис (v_i).

Теорема 1 применима, например, к случаю, когда K' есть p-поле, содержащее K, а R' — его максимальное компактное подкольцо. Ясно, что если рассматривать K' как левое векторное пространство над K, то R' является K-решеткой в K'. Следовательно, в K' существует базис $\{y_1, \ldots, y_n\}$ над K, такой, что $R' = \sum Ry_i$. Если записать теперь произвольное $y \in R'$ в виде $yy_i = \sum a_{ij} y_j$, где $a_{ij} \in K$, $1 \leqslant i, j \leqslant n$, то все a_{ij} должны лежать в R. В частности,

если K коммутативно, то из этих соотношений, выполняющихся в коммутативном поле $K(y)$, вытекает, что $\det(y \cdot 1_n - A) = 0$, где 1_n — единичная матрица, а $A = (a_{ij})$, так что мы получаем другое доказательство второй части предложения 6 п.16.1.4.

Теорема 2. *Пусть L, L' — две K-решетки в левом векторном пространстве V конечной размерности над K. Тогда в V существуют базис $\{v_1, \ldots, v_n\}$ и последовательность целых чисел $(\nu_1, \ldots, \nu_n)$, такие, что $L = \sum Rv_i$ и $L' = \sum P^{\nu_i} v_i$.*

Выберем K-нормы N и N' так, чтобы L определялась уравнением $N(v) \leqslant 1$, а L' — уравнением $N'(v) \leqslant 1$. Построим подпространства $V_1, \ldots, V_n$ в V так же, как в предложении 4 п.16.2.1. Тогда $L = \sum (L \cap V_i)$ и $L' = \sum (L' \cap V_i)$. Применим теперь предложение 7 для каждого i к V_i и $L \cap V_i$, а также к V_i и $L' \cap V_i$; это даст нам элементы ν_i, такие, что $L \cap V_i = Rv_i$, и элементы v_i', такие, что $L' \cap V_i = Rv_i'$. Записав v_i' в виде $v_i' = x_i v_i$, где $x_i \in K^\times$, и положив $\nu_i = \operatorname{ord}(x_i)$, получим целые числа ν_i, удовлетворяющие требуемым условиям.

Следствие 1. *Пусть V и L таковы, как в теоремах 1 и 2, и M — некоторый R-модуль в V. Тогда в V существуют базис $\{v_1, \ldots, v_n\}$ над K и целые числа r, s и $\nu_1, \ldots, \nu_r$, такие, что*

$$0 \leqslant r \leqslant s \leqslant n, \quad L = \sum Rv_i$$

и

$$M = \sum_{j=1}^{r} P^{\nu_j} v_j + \sum_{h=r+1}^{s} Kv_h.$$

Пусть W — подпространство в V, порожденное множеством M, и W' — максимальное подпространство, содержащееся в M. Обозначим через s размерность пространства W и через r — коразмерность W' в W. Выберем последовательность $W_1, \ldots, W_n$ из теоремы 1 так, чтобы она содержала пространства W и W'. По теореме 1 существует базис $\{w_1, \ldots, w_n\}$ пространства V, который порождает L как R-модуль и содержит базисы пространств W и W'. Нумеруя этот базис очевидным образом, можно добиться того, чтобы $\{w_1, \ldots, w_s\}$ было базисом в W, а $\{w_{r+1}, \ldots, w_s\}$ — базисом в W'. Обозначим через W'' подпространство с базисом $\{w_1, \ldots, w_r\}$. В силу предложения 5 M открыто в W; следовательно, по следствию 2 предл. 6 $M = M' + W'$, где $M' = M \cap W''$ есть K-решетка в W''. Применяя теперь к M' и $L' = L \cap W''$ теорему 2, находим базис $\{v_1, \ldots, v_r\}$ для W'' и целые числа $\nu_1, \ldots, \nu_r$, такие, что

$L' = \Sigma\, Rv_j$ и $M' = \Sigma\, P^{\nu_j} v_j$. Положив $v_i = w_i$ для $i > r$, получаем искомый базис.

Следствие 2. *Каждый конечно порожденный R-модуль* $\mathfrak{M}$ *является прямой суммой конечного числа слагаемых, каждое из которых изоморфно или R, или модулю* R/P^ν, *где* $\nu > 0$. *Кроме того, число слагаемых типа R и для каждого* $\nu > 0$ *число слагаемых типа* R/P^ν *определяются заданием модуля* $\mathfrak{M}$ *однозначно.*

Предположим, что $\mathfrak{M}$ порожден элементами $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Возьмем векторное пространство V размерности n над K с базисом $\{v_1, \ldots, v_n\}$ и положим $L = \Sigma\, Rv_i$. Формула

$$\sum x_i v_i \to \sum x_i \mathfrak{m}_i,$$

где x_i при всех $1 \leqslant i \leqslant n$ берутся из R, определяет тогда морфизм из L на $\mathfrak{M}$; следовательно, $\mathfrak{M}$ изоморфно L/M, где M — ядро этого морфизма. Применим теперь следствие 1 к L и M; поскольку $M \subset L$, имеем $\nu_j \geqslant 0$ для всех $1 \leqslant j \leqslant \nu$ и $r = s$. Отсюда следует первое утверждение. Что касается второго, то пусть $\mathfrak{M}_i = \pi^i \mathfrak{M}$ для $i \geqslant 0$. Так как все это R-модули, факторы $\mathfrak{N}_i = \mathfrak{M}_i/\mathfrak{M}_{i+1}$ также являются R-модулями; поскольку $\pi\, \mathfrak{n} = 0$ для всех $\mathfrak{n} \in \mathfrak{N}_i$, то $\mathfrak{N}_i$ можно рассматривать как модуль, т. е. как векторное пространство, над полем $k = R/P$; в качестве такового оно имеет размерность n_i, зависящую только от $\mathfrak{M}$ и i. Запишем теперь $\mathfrak{M}$ в виде прямой суммы модулей R и R/P^ν в количествах соответственно N_0 и N_ν; сразу видно, что $n_i = N_0 + \sum_{\nu > i} N_\nu$. Поэтому $N_0 = n_i$ для достаточно больших i и $N_\nu = n_{\nu-1} - n_\nu$.

Следствие 3. *Целые* $r, s, \nu_1, \ldots, \nu_r$ *из следствия* 1 *зависят только от L и M.*

Поскольку s — размерность подпространства W, порожденного M, а $s - r$ — размерность максимального подпространства, содержащегося в M, они зависят только от M. Положим $L_1 = L \cap W$ и выберем $i \geqslant 0$ так, чтобы $\pi^i L_1 \subset M$; наше утверждение следует теперь из следствия 2, примененного к R-модулю $M/\pi^i L_1$.

Число изоморфных R слагаемых модуля $\mathfrak{M}$ из следствия 2 называется *рангом* модуля $\mathfrak{M}$; используя это определение, получаем

Следствие 4. *Пусть* $\mathfrak{M}$ — *конечно порожденный R-модуль и* $\mathfrak{M}'$ — *его подмодуль. Тогда ранг модуля* $\mathfrak{M}$ *равен сумме рангов модулей* $\mathfrak{M}'$ *и* $\mathfrak{M}/\mathfrak{M}'$.

Как и в доказательстве следствия 2, запишем $\mathfrak{M}$ в виде L/M, где L — решетка $\sum Rv_i$ в векторном пространстве V с базисом

$\{v_1, \ldots, v_n\}$ и M — некоторый R-модуль. Прообраз $\mathfrak{M}'$ в L будет тогда R-модулем L', и три модуля из нашего следствия изоморфны соответственно L/M, L'/M и L/L'. Пусть W, V' — подпространства в V, порожденные соответственно множествами M и L'. Как вытекает из следствия 1, ранги модулей L/M, L'/M и L/L' равны соответственно коразмерностям W в V, W в V' и V' в V.

16.2.3. Мультипликативная структура локалных полей

Сохраним те же обозначения, что и раньше. Для каждого целого $n \geqslant 1$ множество $1+P^n$ элементов x из R, которые $\equiv 1\ (P^n)$, является, очевидно, открытой и компактной подгруппой в $R^\times$, и эти подгруппы образуют фундаментальную систему окрестностей единицы в $R^\times$. Далее, теорема 7 п.16.1.4 показывает, что если $M^\times$ — произвольная подгруппа порядка $q-1$ в $R^\times$, то $R^\times = M^\times \cdot (1+P)$, а из теоремы 6 п.16.1.4 следует, что $K^\times = \Pi \cdot R^\times$, если Π — дискретная подгруппа в $K^\times$, изоморфная $\mathbf{Z}$ и порожденная простым элементом поля K. Произведения в этих формулах являются «полупрямыми».

Начиная с этого места и до конца параграфа будет предполагаться, что K — коммутативное p-поле; упомянутые произведения являются в этом случае прямыми произведениями, так что можно написать $K^\times = \Pi \times R^\times$ и $R^\times = M^\times \times (1+P)$; кроме того, по теореме 7 п.16.1.4 $M^\times$ будет группой корней из единицы в поле K степени, взаимно простой с p. Исследование структуры группы $K^\times$ сводится, таким образом, к изучению структуры $1+P$.

Выберем какое-нибудь $x \in 1+P$; для каждого $a \in \mathbf{Z}$ элемент x^a будет лежать в $1+P$, и отображение $a \to x^a$ является гомоморфизмом аддитивной группы $\mathbf{Z}$ в мультипликативную группу $1+P$; так как из леммы 5, использовавшейся при доказательстве теоремы 7 п.16.1.4, вытекает, что $x^a \in 1+P^{n+1}$ при $a \equiv 0\ (p^n)$, т. е. при $|a|_p \leqslant p^{-n}$, то наш гомоморфизм непрерывен, если снабдить $\mathbf{Z}$ p-адической топологией, т. е. топологией, индуцируемой в $\mathbf{Z}$ полем $\mathbf{Q}_p$. Поскольку множество $1+P$ компактно, этот гомоморфизм однозначно продолжается до непрерывного гомоморфизма, обозначаемого снова через $a \to x^a$, аддитивной группы $\mathbf{Z}_p$ в мультипликативную группу $1+P$. Если $x \in 1+P^n$, то x^a лежит в $1+P^n$ для всех $a \in \mathbf{Z}$ и, следовательно, для всех $a \in \mathbf{Z}_p$. Используя формулу $y^b (x^a)^{-1} = (yx^{-1})^b x^{b-a}$ и обычные рассуждения, отсюда можно просто вывести, что отображение $(a, x) \to x^a$ группы $\mathbf{Z}_p \times (1+P)$ в $1+P$ непрерывно. Немедленно проверяется, что это отображение определяет на группе $1+P$ структуру $\mathbf{Z}_p$-модуля

(«сложение» векторов записывается мультипликативно, а «умножение» на элементы из $\mathbf{Z}_p$—экспоненциально).

Предложение 8. *Если n — целое число, взаимно простое с p, а ν — целое число, большее единицы, то отображение* $x \to x^n$ *индуцирует автоморфизм на группе* $1 + P^\nu$; $(K^\times)^n$ *является открытой подгруппой в* $K^\times$ *индекса* $n \cdot (n,\ q - 1)$, *и если n делит q* — 1, *то этот индекс равен* n^2.

Первое утверждение есть частный случай того факта, что если a — обратимый элемент в $\mathbf{Z}_p$, то отображение $x \to x^a$ является автоморфизмом группы $1 + P^\nu$; отсюда следует, что $(K^\times)^n$ открыто в $K^\times$. Кроме того, как мы видели выше, группа $K^\times$ есть прямое произведение группы П, изоморфной $\mathbf{Z}$, циклической группы $M^\times$ порядка q — 1 и группы $1 + P$. Поэтому индекс $(K^\times)^n$ в $K^\times$ является произведением соответствующих индексов для $\mathbf{П}$, $M^\times$ и $1 + P$. Ясно, что они равны соответственно n, наибольшему общему делителю $(n, q - 1)$ чисел n и q — 1 и 1. Доказательство закончено.

Определим теперь структуру $\mathbf{Z}_p$-модуля на группе $1+P$. Это зависит от характеристики поля K. Если K — поле характеристики нуль, то, как мы уже отмечали, оно является конечным алгебраическим расширением поля $\mathbf{Q}_p$ и его максимальное компактное подкольцо можно рассматривать как $\mathbf{Q}_p$-решетку в K. Теорема 1 из п.16.2.2 показывает тогда, что оно есть прямое произведение множителей, изоморфных $\mathbf{Z}_p$, в числе, равном степени K над $\mathbf{Q}_p$.

Предложение 9. *Пусть K — коммутативное p-поле характеристики нуль с максимальным компактным подкольцом R. Тогда существует целое число* $m \geq 0$, *такое, что* $1+P$ *как* $\mathbf{Z}_p$*-модуль (записываемый мультипликативно) изоморфен* $\mathbf{Z}_p$*-модулю* $R \times (\mathbf{Z}_p/p^m\mathbf{Z}_p)$ *(записываемому аддитивно). При этом m есть наибольшее целое, такое, что K содержит примитивный корень* p^m*-й степени из единицы.*

Для произвольных $x \in R$ и $a \in \mathbf{N}$ биномиальную формулу можно записать в виде

$$(1 + x)^a = 1 + ax + ax \sum_{i=2}^{a} \binom{a-1}{i-1} x^{i-1}/i.$$

Для $i \geqslant 2$ обозначим через p^h наибольшую степень p, делящую i; если $h = 0$, то $i - 1 \geqslant h$; а если $h > 0$, то, поскольку $i \geqslant p^h$, сразу видно, что i — 1>h, за исключением случая $i = p = 2$, так что всегда $2(i - 1) > h$. В написанной выше формуле сумма в последнем члене в правой части принадлежит, следовательно, pR, если $x \in p^2R$. Для $x \in p^2R$, $a \in \mathbf{N}$ это дает

$$(1 + x)^a \equiv 1 + ax \quad (pax R). \tag{3}$$

Это сравнение остается по непрерывности справедливым для всех $x \in p^2R$ и $a \in \mathbf{Z}_p$ ввиду плотности $\mathbf{N}$ в $\mathbf{Z}_p$. Если теперь обозначить через d степень K над $\mathbf{Q}_p$, то по теореме 1 п.16.2.2 можно найти базис $\{v_1, \ldots, v_d\}$ в K над $\mathbf{Q}_p$, такой, что $R = \sum \mathbf{Z}_p v_i$. В силу (3) имеем для всех $1 \leqslant i \leqslant d$, $\nu \geqslant 1$, $a_i \in \mathbf{Z}_p$

$$(1 + p^2 v_i)^{p^{\nu-1} a_i} \equiv 1 + p^{\nu+1} a_i v_i \quad (p^{\nu+2} R)$$

и, следовательно,

$$\prod_{i=1}^{d} (1 + p^2 v_i)^{p^{\nu-1} a_i} \equiv 1 + p^{\nu+1} \sum_{i=1}^{d} a_i v_i \quad (p^{\nu+2} R). \tag{4}$$

Отсюда вытекает, что если $x_1 \in p^2R$, то мы можем определить по индукции последовательность $(x_1, x_2, \ldots)$ с $x_\nu \in p^{\nu+1}R$, положив для каждого $\nu \geqslant 1$

$$x_\nu = p^{\nu+1} \sum_i a_{\nu i} v_i,$$

где $a_{\nu i} \in \mathbf{Z}_p$, $1 \leqslant i \leqslant d$. Тогда

$$1 + x_{\nu+1} = (1 + x_\nu) \prod_i (1 + p^2 v_i)^{-p^{\nu-1} a_{\nu i}}.$$

Ясно также, что

$$1 + x_1 = \prod_i (1 + p^2 v_i)^{b_i}, \tag{5}$$

где b_i задается формулой

$$b_i = \sum_{\nu=1}^{+\infty} p^{\nu-1} a_{\nu i},$$

$1 \leqslant i \leqslant d$. Это показывает, что как мультипликативный $\mathbf{Z}_p$-модуль группа $1 + p^2R$ порождается d элементами $1 + p^2 v_i$; а поскольку она — открытая подгруппа в компактной группе $1 + P$ и потому конечного индекса в ней и поскольку $1 + P$ как $\mathbf{Z}_p$-модуль порождается элементами $1 + p^2 v_i$ и полной системой представителей классов смежности в $1 + P$ по подгруппе $1 + p^2R$, то $1 + P$ — конечно порожденная группа. Предположим теперь, что (5) может иметь место при $x_1 = 0$ и b_i не всех равных нулю; взяв тогда в качестве $\nu - 1$ наименьший из порядков b_i в $\mathbf{Q}_p$, можно написать $b_i = p^{\nu-1} a_i$, где $\nu \geqslant 1$ и $a_i \in \mathbf{Z}_p$, $1 \leqslant i \leqslant d$, причем не все a_i принадлежат $p\mathbf{Z}_p$. Сравнение (4) дает тогда $\sum a_i v_i \equiv 0 \ (pR)$, т. е. $\sum (p^{-1} a_i) v_i \in R$, что противоречит определению v_i. Это показывает, что $1 + p^2R$ как $\mathbf{Z}_p$-модуль является свободным модулем, порожденным элементами $1 + p^2 v_i$, и, следовательно, изоморфен $(\mathbf{Z}_p)^d$. Мы можем теперь

применить к модулям $1 + P$ и $1 + p^2R$ следствие 4 теор. 2 п.16.2.2. Поскольку их фактормодуль конечен, его ранг равен нулю; а модуль $1 + p^2R$ как изоморфный $(\mathbf{Z}_p)^d$ есть модуль ранга d. Поэтому $1 + P$ имеет ранг d и изоморфен по следствию 2 теор. 2 п.16.2.2 прямому произведению d сомножителей, изоморфных $\mathbf{Z}_p$, и некоторого конечного числа сомножителей, каждый из которых изоморфен модулю вида $\mathbf{Z}_p/p^\nu\mathbf{Z}_p$. Поскольку последние суть конечные группы, их произведение совпадает с группой всех элементов конечного порядка в $1 + P$ и потому само есть конечная группа, порядок которой является некоторой степенью p. Отсюда следует, что она есть группа всех корней из единицы в $1 + P$, и притом циклическая группа порядка p^m, где p^m — наибольший из порядков ее элементов (лемма 1 п.16.1.1). Таким образом, как $\mathbf{Z}_p$-модуль эта группа изоморфна $\mathbf{Z}_p/p^m\mathbf{Z}_p$. Записав, наконец, $K^\times$ в виде прямого произведения П, $M^\times$ и $1 + P$, мы видим, что каждый корень из единицы, степень которого есть некоторая степень p, содержится в $1 + P$. Доказательство закончено.

Следствие. *Пусть K таково, как в предложении* 9. *Тогда для каждого целого $n \geqslant 1$ $(K^\times)^n$ является открытой подгруппой в $K^\times$ конечного индекса, равного $n \cdot (n, r) \cdot \mathrm{mod}_K (n)^{-1}$, где r — порядок группы всех корней из единицы в K.*

Ясно, что последняя группа разлагается в прямое произведение $M^\times$ и группы порядка p^m, состоящей из корней из единицы в $1 + P$. Следовательно, она циклична и имеет порядок $r = (q - 1)\, p^m$, а $K^\times$ есть прямое произведение П, этой группы и $\mathbf{Z}_p$-модуля, изоморфного R. Далее, nR есть открытая подгруппа в аддитивной группе кольца R, индекс которой в R по определению функции mod_K равен $\mathrm{mod}_K (n)^{-1}$. Используя те же соображения, что и в доказательстве предложения 8, получаем утверждение следствия.

Предложение 10. *Пусть K — коммутативное p-поле характеристики p. Тогда $1 + P$ как $\mathbf{Z}_p$-модуль является прямым произведением бесконечного счетного семейства модулей, изоморфных $\mathbf{Z}_p$.*

По теореме 8 п.16.2.4 K можно рассматривать как поле формальных степенных рядов от одной переменной π с коэффициентами в поле $\mathbf{F}_q$ из $q = p^f$ элементов. В данном случае легко явно указать семейство свободных образующих $\mathbf{Z}_p$-модуля $1 + P$. В самом деле, выберем какой-нибудь базис $\{\alpha_1, \ldots, \alpha_f\}$ поля $\mathbf{F}_q$ над простым полем $\mathbf{F}_p$. В качестве образующих модуля $1+P$ можно взять элементы $1 + \alpha_i\pi^n$, где $1 \leqslant i \leqslant f$, а n пробегает множество всех целых чисел 0, взаимно простых с p. Для каждого $N > 0$ положим $N = np^\nu$, где $\nu \geqslant 0$ и n взаимно просто с p. Для произвольных целых a_i, $1 \leqslant i \leqslant f$, имеем

$$\prod_{i=1}^{f}(1+\alpha_i\pi^n)^{a_i p^\nu} = \prod_i (1+\beta_i\pi^N)^{a_i} \equiv 1+\left(\sum_i a_i\beta_i\right)\pi^N \qquad (P^{N+1}),$$

где $\beta_i = \alpha_i^{p^\nu}$. Так как отображение $x \to x^{p^\nu}$ есть автоморфизм поля $\mathbf{F}_q$ над $\mathbf{F}_p$, то β_1 также образуют базис поля $\mathbf{F}_q$ над $\mathbf{F}_p$; следовательно, для произвольного заданного $\alpha \in \mathbf{F}_q$ можно одним и только одним способом выбрать целые числа a_i так, чтобы $0 \leqslant a_i < p$ и $\sum a_i\beta_i = \alpha$. Возьмем теперь какое-нибудь $x_1 \in P$ и определим по индукции последовательность $(x_1, x_2, \ldots)$, где $x_N \in P^N$ при всех $N \geqslant 1$. Для каждого N положим, как и выше, $N = np^\nu$, где n взаимно просто с p, и выберем целые числа a_i так, чтобы $0 \leqslant a_i < p$ для $1 \leqslant i \leqslant f$ и чтобы

$$y_N = \prod_i (1+\alpha_i\pi^n)^{a_i p^\nu} \equiv 1 + x_N \qquad (P^{N+1}).$$

В силу сказанного выше это можно сделать, и притом только одним способом. Положим теперь

$$1 + x_{N+1} = (1 + x_N)\, y_N^{-1}.$$

Сопоставляя эти формулы, сразу видим, что они дают для $1+x_1$ представление в виде сходящегося бесконечного произведения множителей типа $(1+\alpha_i\pi^n)b$, где $1 \leqslant i \leqslant f$, n взаимно просто с p и $b \in \mathbf{Z}_p$. Кроме того, из проведенных вычислений следует, что это представление единственно. Наши утверждения доказаны.

16.2.4. Решетки над R

Понятие решетки в том виде, как оно было развито для p-полей в п.16.2.1,2, неприменимо к **R**-полям. Подходящим здесь является следующее

Определение 3. R -*решеткой в векторном пространстве V конечной размерности над некоторым* **R**-*полем называется дискретная подгруппа L в V, такая, что* V/L *компактно.*

Напомним теперь некоторые элементарные факты о дискретных подгруппах. Пусть G — топологическая группа, Γ — ее дискретная подгруппа и φ — каноническое отображение группы G на G/Γ. Если U — окрестность единичного элемента e в G, такая, что $U^{-1} \cdot U$ не содержит элементов группы Γ, отличных от e, то φ индуцирует на каждом множестве gU с $g \in G$ гомеоморфизм этого множества на его образ в G/Γ. Это можно выразить, сказав, что φ является «локальным гомеоморфизмом»; если Γ — нормальная подгруппа в G, то можно сказать, что φ является «локальным изоморфизмом», поскольку в этом случае φ переводит групповой закон на G в групповой закон на

G/Γ. Предположим, что группа G локально компактна и что на ней задана правоинвариантная мера α. Тогда, как легко видеть, существует одна и только одна мера α' на G/Γ, такая, что для любого измеримого подмножества X в G, взаимно однозначно отображаемого на его образ $\varphi(X) = X'$ в G/Γ, $\alpha'(X')$ равно $\alpha(X)$. Это справедливо, в частности, для любого измеримого подмножества всякого множества вида gU, где U такое же, как и выше. Если теперь f — произвольная непрерывная функция на G с компактным носителем, то

$$\int_G f(g)\, d\alpha(g) = \int_{G/\Gamma} \left(\sum_{\gamma \in \Gamma} f(g\gamma) \right) d\alpha'(\dot{g}). \tag{6}$$

Здесь мы положили $\dot{g} = \varphi(g)$, и подинтегральное выражение в правой части, хотя и записано как функция от g, может рассматриваться как функция от $\dot{g}$, поскольку оно постоянно на классах смежности $g\Gamma$. В самом деле, это очевидно, если носитель функции f содержится в одном из множеств gU, а общий случай сразу следует отсюда. Кроме того, как хорошо известно из теории интегрирования, справедливость равенства (6) для всех непрерывных функций с компактным носителем влечет его справедливость для всех интегрируемых функций и для всех измеримых функций со значениями в R_+. Ясно, что мера α' инвариантна относительно действия группы G на G/Γ в том и только в том случае, когда мера α левоинвариантна; это, в частности, всегда так, когда множество G/Γ компактно, ибо тогда G/Γ является множеством конечной меры, инвариантной относительно действия группы G. Если при этом подгруппа Γ нормальна в G, то α' есть мера Хаара на G/Γ.

В описанной выше ситуации мера α' называется *образом* меры α в G/Γ, и мы будем обозначать ее просто через α, если это не сможет вызвать недоразумений. Следующая лемма (играющая роль утверждения, которое в классической теории чисел известно как теорема Минковского) теперь очевидна.

Лемма 1. *Пусть G — локально компактная группа с мерой Хаара α, Γ — ее дискретная подгруппа, такая, что множество G/Γ компактно, и X — измеримое подмножество в G, для которого $\alpha(X) > \alpha(G/\Gamma)$. Тогда существуют два различных элемента x, x' из X, такие, что $x^{-1}x' \in \Gamma$.*

Нужно только заметить, что поскольку G/Γ компактно, каждая правоинвариантная мера на G также левоинвариантна и, следовательно, мера Хаара α является двусторонне-инвариантной, а ее образ на G/Γ корректно определен.

Лемма 2. *Пусть G,* α *и* Γ *таковы, как в лемме 1, и пусть* Γ_1 — *дискретная подгруппа группы G, содержащая* Γ. *Тогда* Γ *имеет конечный индекс в* Γ_1 *и этот индекс определяется соотношением*

$$\alpha(G/\Gamma) = [\Gamma_1 : \Gamma]\,\alpha(G/\Gamma_1).$$

Поскольку множество G/Γ компактно, существует непрерывная функция $f_0 \geqslant 0$ на G с компактным носителем, такая, что для всех $g \in G$

$$f_1(g) = \sum_{\gamma \in \Gamma} f_0(g\gamma) > 0.$$

Функция $f = f_0/f_1$ непрерывна на G, имеет тот же носитель, что и f_0, и такова, что сумма $\sum f(g\gamma)$, где суммирование производится по всем $\gamma \in \Gamma$, равна 1 при всех g. Из этого факта вытекает, что аналогичная сумма, взятая по всем $\gamma \in \Gamma_1$, имеет постоянное значение $[\Gamma_1 : \Gamma]$. Применив теперь к G, f и Γ, а также к G, f и Γ_1 формулу (6), получим утверждение нашей леммы.

Выведем теперь из этих фактов следующий классический результат об **R**-решетках.

Предложение 11. *Пусть L — подгруппа векторного пространства V размерности n над* **R**. *Следующие три утверждения эквивалентны:* (i) *L является* **R** *-решеткой в V;* (ii) *L дискретна в V, конечно порождена и содержит базис* (v_i) *пространства V над* **R**; (iii) *в V существует базис над* **R**, *порождающий группу L.*

Пусть имеет место (iii). Рассмотрим изоморфизм

$$(x_1, \ldots, x_n) \to \sum x_i v_i \tag{7}$$

из $\mathbf{R}^n$ на V. Подгруппа L является образом подгруппы $\mathbf{Z}^n$ относительно этого изоморфизма и потому дискретна в V, а факторгруппа V/L изоморфна $(\mathbf{R}/\mathbf{Z})^n$ и потому компактна. Таким образом, (iii) влечет (i) и (ii). Предположим теперь, что выполняется (i). Пусть W — подпространство в V, порожденное решеткой L, а W' — дополнительное к W подпространство в V. Как локально компактная группа V есть прямое произведение W и W, а L есть дискретная подгруппа в W. Следовательно, факторпространство V/L изоморфно прямому произведению W/L и W' и, значит, не может быть компактным, если W' не является таковым. Поэтому W' должно равняться $\{0\}$, а $W = V$, так что L содержит базис пространства V над **R**. Пусть теперь α — мера Хаара на V, для которой $\alpha(V/L) = 1$. Для каждого базиса $B = \{v_1, \ldots, v_n\}$ в V, содержащегося в L, обозначим через φ_B изоморфизм $\mathbf{R}^n$ на V, определяемый формулой (7); он отображает $\mathbf{Z}^n$ на подрешетку L_B в L, порожденную B, а меру Лебега λ на $\mathbf{R}^n$ — в некоторое скалярное кратное $m_B^{-1}\alpha$ меры α. Так как $\lambda(\mathbf{R}^n/\mathbf{Z}^n) = 1$, то имеем $m_B^{-1}\alpha(V/L_B) = 1$.

По лемме 2 отсюда следует, что m_B является индексом L_B в L. Выберем теперь B так, чтобы этот индекс имел наименьшее возможное значение, и покажем, что тогда $L_B = L$. Действительно, допустим, что L содержит вектор w, не лежащий в L_B, и запишем его в виде $w = \sum_1^n a_i v_i$ с коэффициентами a_i из $\mathbf{R}$. Поскольку w не принадлежит L_B, по крайней мере один из коэффициентов, например a_1, не лежит в $\mathbf{Z}$. Заменяя w на $w - mv_1$, где $m \in \mathbf{Z}$, $m < a_1 < m + 1$, видим, что можно считать, что $0 < a_1 < 1$. Пусть теперь $v_i' = w$, $v_i' = v_i$ для $2 \leqslant i \leqslant n$, и $B' = \{v_1', \ldots, v_n'\}$. Ясно, что B' является базисом пространства V, содержащимся в L. Тривиальное вычисление показывает, что $\varphi_B^{-1} \circ \varphi_{B'}$ является автоморфизмом пространства $\mathbf{R}^n$, задаваемым формулой

$$(x_1, \ldots, x_n) \to (a_1 x_1, x_2 + a_2 x_1, \ldots, x_n + a_n x_1),$$

причем модуль этого автоморфизма равен a_1. Возьмем какое-нибудь измеримое подмножество X в $\mathbf{R}^n$ и положим $Y = \varphi_{B'}(X)$ и $Y' = \varphi_{B'}(X)$. По определению m_B, $m_{B'}$ имеем $\alpha(Y) = m_B \lambda(X)$, $\alpha(Y') = m_{B'} \lambda(X)$ и, следовательно, модуль автоморфизма $\varphi_{B'} \circ \varphi_B^{-1}$, отображающего Y на Y', равен $m_{B'}/m_B$. Поскольку автоморфизм $\varphi_{B'} \circ \varphi_B^{-1}$ можно записать в виде $\varphi_{B'} \circ (\varphi_B^{-1} \circ \varphi_{B'}) \circ \varphi_B^{-1}$, у него тот же самый модуль, что и у автоморфизма $\varphi_B^{-1} \circ \varphi_{B'}$. Это дает $m_{B'}/m_B = a_1 < 1$, что противоречит определению B. Таким образом, (i) влечет (ii) и (iii), и доказательство завершено.

16.2.5. Двойственность над локальными полями

К числу наиболее важных свойств коммутативных локально компактных групп принадлежат те свойства, которые образуют содержание так называемой теории двойственности. Напомним, что если G — такая группа, то ее *характером* (в смысле этой теории) называется непрерывный гомоморфизм из G в мультипликативную группу комплексных чисел, по модулю равных единице. Если g^* — характер, то его значение в точке g группы G обычно обозначается через $\langle g, g^* \rangle_G$, а иногда просто через $\langle g, g^* \rangle$, если это не может вызвать недоразумений. Будем записывать групповой закон в G аддитивно. Введем на множестве G^* характеров группы G коммутативную групповую структуру, также записываемую аддитивно, положив

$$\langle g, g_1^* + g_2^* \rangle_G = \langle g, g_1^* \rangle_G \cdot \langle g, g_2^* \rangle_G.$$

Отметим, что единичный элемент группы G^*, который обозначается в аддитивной записи нулем, соответствует *тривиальному* характеру группы G, принимающему во всех точках значение 1. Можно топологизировать группу G^*, снабдив ее топологией равномерной сходимости на компактных подмножествах в G. Группа G^* превращается таким образом в локально компактную группу, именуемую *топологической двойственной* к группе G, или просто двойственной к ней, если это не может привести к путанице. Обратно, характеры группы G* суть функции $g^* \to \langle g, g^* \rangle_G$, определяемые элементами $g \in G$, и это соответствие определяет изоморфизм между G и двойственной к G^*. Иначе говоря, положив

$$\langle g^*, g \rangle_{G^*} = \langle g, g^* \rangle_G,$$

мы можем отождествить G с двойственной к G^*, и в дальнейшем всегда будет предполагаться, что они отождествлены таким образом. Группа G компактна в том и только том случае, когда группа G^* дискретна, а посему G дискретна тогда и только тогда, когда G* компактна.

Пусть H — произвольная замкнутая подгруппа в G. Характеры группы G, индуцирующие тривиальный характер на H, образуют замкнутую подгруппу в G*, которая будет обозначаться через H_*. Будем говорить, что подгруппа H_* *ассоциирована с H по двойственности.* Она изоморфна группе, двойственной к G/H. В случае когда G рассматривается как двойственная к G^*, подгруппа в G, ассоциированная с H_*, есть сама подгруппа H, которая, следовательно, изоморфна двойственной к G^*/H_*. Так как H открыта в G в том и только в том случае, когда G/H дискретна, видим, что это имеет место тогда и только тогда, когда H_* компактна. Таким образом H_* открыта в G* в том и только в том случае, когда группа H компактна. Аналогично H дискретна в том и только в том случае, когда G^*/H_* компактна, и G/H компактна тогда и только тогда, когда группа H_* дискретна.

Все это применимо к аддитивной группе произвольного левого векторного пространства V конечной размерности над недискретным локально компактным полем K (коммутативным или нет). В этом случае, если V^* — топологическое двойственное к V и $v^* \in V^*$, то для каждого $a \in K$ функция $v \to \langle av, v^* \rangle_V$ является, очевидно, характером группы V, который будет обозначаться через v^*a. Обращаясь к определениям, находим, что V^* превращается тем самым в правое векторное пространство над K. В силу следствия 2 теор. 3 п.16.2.1-2 размерность V^* должна быть конечна. Иными словами,

структура V^* как правого векторного пространства над K задается формулой

$$\langle av, v^* \rangle_V = \langle v, v^* a \rangle_V. \quad (8)$$

Обратно, если V и V^* — двойственные группы и V^* имеет структуру правого векторного пространства над K, то можно использовать формулу (8) для того, чтобы определить V как левое векторное пространство над K. Итак, мы можем отождествлять V с двойственным к V^*, даже если рассматривать их как векторные пространства над K. Если L — произвольная замкнутая подгруппа в V, то подгруппа $L\%$, ассоциированная с L по двойственности, состоит из тех элементов u^* из V^*, для которых $\langle v, v^* \rangle_V = 1$ при всех $v \in L$. С учетом формулы (8) отсюда следует, что если L — левый модуль над некоторым подкольцом поля K, то L_* является правым модулем над тем же самым подкольцом, и обратно. В частности, если K — некоторое p-поле и R — его максимальное компактное подкольцо, то L есть левый R-модуль тогда и только тогда, когда L_* — правый R-модуль. Поскольку, как мы видели, L компактен и открыт в V тогда и только тогда, когда L_* таков же в V^*, получаем, что L является K-решеткой в том и только в том случае, когда L_* есть K-решетка. В случае когда это так, будем говорить, что K-решетки L и L_* *двойственны* друг другу; при этом aL и $L_* a^{-1}$ двойственны друг другу при каждом $a \in K^\times$. С другой стороны, ясно, что если K есть **R, C** или **H**, то L является **R**-решеткой тогда и только тогда, когда L_* есть **R**-решетка.

Далее, если V таково, как выше, можно рассматривать его *алгебраическое двойственное* V', которое является пространством K-линейных форм на V. Как хорошо известно, если обозначить через $[v, v']_V$ значение в точке v линейной формы v' на пространстве V, то можно наделить V «естественной» структурой правого векторного пространства над K с помощью формулы

$$[av, v'b]_V = a\,[v, v']_V\,b,$$

выполняющейся для всех $v \in V$, $v' \in V'$ и всех $a, b \in K$. Если χ — какой-нибудь характер аддитивной группы поля K, то для каждого $v' \in V'$ существует элемент v^* из топологического двойственного V^*, для которого $\langle v, v^* \rangle_V = \chi([v, v']_V)$ при всех $v \in V$. Используем это, чтобы установить связь между алгебраическим и топологическим двойственными.

Теорема 3. *Пусть K — недискретное локально компактное поле, V — левое векторное пространство конечной размерности n над K, и пусть χ — нетривиальный характер аддитивной группы поля K. Тогда*

топологическое двойственное V является правым векторным пространством размерности n над K и формула*

$$\langle v, v^* \rangle_V = \chi([v, v']_V) \text{ для всех } v \in V$$

определяет биективное отображение $v' \to v^*$ *алгебраического двойственного V′ к V в пространство V*. Если* $\chi(xy) = \chi(yx)$ *для всех x, y из K, то это отображение является изоморфизмом структур V′ и V* как правых векторных пространств над K.*

Пусть X_K — топологическое двойственное к K. Структура K как левого векторного пространства размерности 1 над самим собой определяет структуру правого векторного пространства на X_K; в качестве такового оно имеет конечную размерность d. Подобным образом структура K как правого векторного пространства над K определяет на X_K структуру левого векторного пространства над K некоторой размерности d'. Пусть V таково, как в теореме 3. Выбрав какой-нибудь его базис над K, представим пространство V в виде прямой суммы n подпространств размерности 1. Его двойственное V^* изоморфно, следовательно, как правое векторное пространство, прямой сумме n подпространств, изоморфных X_K, и имеет потому размерность nd. Аналогично двойственное к V^* есть левое векторное пространство размерности ndd', и так как оно изоморфно V, с которым мы договорились его отождествлять, получаем, что $ndd' = n$ и $d = d' = 1$. Пусть характер χ таков, как в теореме 3; он определяет элемент $c^* \neq 0$ в аддитивно записываемой группе X_K, так что $\chi(t) = \langle t, c^* \rangle_K$ для всех $t \in K$. Поскольку $d' = 1$, каждый элемент из X_K можно однозначно записать в виде xc^*, где $x \in K$, и поскольку $d = 1$, каждый элемент из X_K однозначно записывается как c^*y с $y \in K$. Отношение $xc^* = c^*y$ определяет тем самым биекцию α поля K на себя, и немедленно проверяется, что она является автоморфизмом поля. В силу (8) c^*y является характером $t \to \chi(yt)$ поля K и аналогично xc^* является характером $t \to \chi(tx)$. Таким образом, $\chi(tx) = \chi(\alpha(x)\, t)$ для всех x, t из K, чем автоморфизм α и определяется однозначно. В частности, он тождествен на центре поля K и тождествен везде, если $\chi(tx) = \chi(xt)$ для всех x, t из K. Рассмотрим теперь отображение $v' \to v^*$ из V' в V^*, определенное в теореме 3. Выберем $x \in K$, положим $w' = v'x$ и предположим, что исследуемое отображение переводит w' в w^*. Имеем

$$\chi([v, w']_V) = \chi([v, v']_V x) = \chi(\alpha(x)\,[v, v']_V) = \chi([\alpha(x)\, v, v']_V).$$

Ввиду определения v^* и w^* это дает

$$\langle v, w^* \rangle_V = \langle \alpha(x)\, v, v^* \rangle_V = \langle v, v^* \alpha(x) \rangle_V$$

для всех v и, значит, $w^* = v^*\alpha(x)$. Этот факт обычно выражают, говоря, что отображение $v' \to v^*$ α-*полулинейно.* В то же время ясно, что это отображение инъективно. Действительно, равенство $v^* = 0$ означает, что $\chi([v, v']_V)$ равно 1 для всех $v \in V$ и, следовательно, $\chi(x[v, v']_V)$ равно 1 для всех $x \in K$ и всех $v \in V$, а поскольку характер χ нетривиален, отсюда следует, что $[v, v']_V = 0$ при всех v, т. е. $v' = 0$. Так как V' и V^* имеют одинаковую, размерность n над K, α-полулинейное отображение из V' в V^* не может быть инъективным, не будучи биективным. Тем самым доказательство закончено.

Для удобства ссылок сформулируем отдельно результат о характерах поля K.

Следствие. *Пусть K и χ таковы, как в теореме* 3. *Тогда каждый характер поля K может быть записан, и притом единственным образом, в виде $t \to \chi(tx)$, где $x \in K$, или в виде $t \to \chi(yt)$, где $y \in K$.*

Можно было бы сформулировать теорему 3 более «внутренним» образом, сказав, что существует канонический изоморфизм между V^* и тензорным произведением $V^* \otimes_K X_K$, задаваемый формулой из теоремы 3 (и аналогично канонический изоформизм между V^* и $X_K \otimes_K V'$, если V несет структуру правого векторного пространства). Мы предоставляем читателю самому убедиться в этом. Следует также отметить, что всегда существует нетривиальный характер поля K, для которого $\chi(xy) = \chi(yx)$ при всех $x, y \in K$; можно взять, например, $\chi = \chi_0 \circ \tau$, где τ — «приведенный след» в K над центром K_0, а χ_0 — нетривиальный характер в K_0. Тот же результат можно было бы вывести и из того факта, что, согласно теореме Сколема — Нётер (которая появится ниже), отображение α из доказательства теоремы 3 должно быть внутренним автоморфизмом поля K. Конечно, различение правого и левого становится совершенно излишним, если рассматриваются только коммутативные поля.

Обычно подразумевается, что раз и навсегда выбран некий характер поля K со свойствами, описанными в теореме 3, чтобы отождествить, с помощью описанного в теореме изоморфизма, топологические и алгебраические двойственные всех векторных пространств над K. При этом χ обычно именуется *базисным характером.* В частности, как показано в следствии теоремы 3, можно при этом отождествлять поле K с его топологическим двойственным. В случае когда это делается для p-поля K, подгруппа в K, ассоциированная по двойственности с подгруппой вида P^n, должна быть подгруппой того же вида, поскольку

вообще двойственное к *K*-решетке является *K*-решеткой. Чтобы сформулировать более точное утверждение, введем следующее определение.

Определение 4. *Пусть K — некоторое p-поле, R — его максимальное компактное подкольцо и P — максимальный идеал в R. Порядком нетривиального характера χ поля K называется наибольшее целое число* $\nu \in \mathbf{Z}$, *такое, что* χ *равен* 1 *на* $P^{-\nu}$; *порядок характера* χ *будет обозначаться через* ord (χ).

Иными словами, $P^{-\nu}$ есть двойственная к *R K*-решетка, если *K* отождествляется со своим двойственным при помощи χ. Это показывает, что *v* конечно.

Предложение 12. *Пусть K — некоторое p-поле,* χ *— его нетривиальный характер порядка* ν. *Тогда для любого* $n \in \mathbf{Z}$ $\chi(xt) = 1$ *при всех* $t \in P^n$ *в том и только в том случае, когда* $x \in P^{-n-\nu}$.

Это утверждение очевидно. Его можно выразить, сказав, что двойственная к P^n *K*-решетка есть $P^{-n-\nu}$, если *K* отождествляется со своим двойственным при помощи χ.

Что касается явной конструкции характеров локальных полей, то для случая поля **R** она хорошо известна; в качестве базисного характера можно взять характер, задаваемый формулой $\chi_0(x) = \mathbf{e}(x) = e^{2\pi i x}$. В **C** или *H* можно взять в качестве базисного любой характер вида $\chi_0 \circ f$, где *f* — любая отличная от нуля линейная **R**-форма (например, след над **R**). Если *K* — локальное поле характеристики *p,* его можно представить как поле формальных степенных рядов $x = \Sigma a^i T^i$ с коэффициентами из F_q, и в качестве базисного можно взять характер порядка 0, определяемый равенством $\chi(x) = \psi(a_{-1})$, где ψ— какой-нибудь нетривиальный характер аддитивной группы поля $\mathbf{F}_q$.

16.3. Точка A-полей

16.3.1. A-поля и их пополнения

Под *полем алгебраических чисел* обычно понимают всякое конечное алгебраическое расширение поля **Q**. Основной задачей теории чисел является изучение полей алгебраических чисел с помощью их вложений в локальные поля. Было обнаружено, что методы, которые при этом используются, могут быть с очень небольшими изменениями применены к некоторым полям характеристики $p>1$, причем одновременное изучение этих двух типов полей проливает допол-

нительный свет на каждый из них. Учитывая это, приведем теперь определение полей, которые и будем, начиная с этого места, изучать.

Определение 1. *Поле называется* **A***-полем, если оно является или конечным алгебраическим расширением поля* **Q**, *или конечно порожденным расширением конечного простого поля* $\mathbf{F}_p$, *имеющего над* $\mathbf{F}_p$ *степень трансцендентности* 1**.**

Итак, если k есть **A**-поле характеристики $p>1$, оно должно содержать трансцендентный над $\mathbf{F}_p$ элемент t и, следовательно, является конечным алгебраическим расширением поля $\mathbf{F}_p(t)$. Таким образом, если обозначить раз и навсегда независимую переменную через T, так что $\mathbf{F}_p(T)$ есть поле рациональных функций от T с коэффициентами в $\mathbf{F}_p$, то **A**-полями характеристики p будут в точности те поля, которые суть конечные алгебраические расширения поля $\mathbf{F}_p(T)$. Заметим, что такое поле всегда содержит бесконечно много полей, изоморфных $\mathbf{F}_p(T)$.

Мы будем изучать **A**-поля, вкладывая их в локальные поля. В силу теорем 5 и 8 п.16.1 возможно говорить о множестве всех локальных полей, рассматриваемых с точностью до изоморфизма. В самом деле, для заданного $p > 1$ локальные поля характеристики p находятся, с точностью до изоморфизма, во взаимно однозначном соответствии с конечными полями $\boldsymbol{F}_q$ из $q = p^n$ элементов, в то время как локальные p-поля характеристики 0 изоморфны подполям алгебраического замыкания поля $\mathbf{Q}_p$, имеющим конечную степень над $\mathbf{Q}_p$. Позже мы установим, что полей последнего типа лишь счетное число, но здесь это нам не понадобится. Теперь имеет смысл следующее определение, позволяющее говорить о множестве точек **A**-полей.

Определение 2. *Пусть* X *— изоморфное вложение* **A***-поля* k *в локальное поле* K. *Пара* (λ, K) *называется пополнением поля* k, *если* $\lambda(k)$ *плотно в* K. *Два пополнения* (λ, K) *и* (λ', K') *поля* k *называются эквивалентными, если существует такой изоморфизм* ρ *поля* K *на* K', *что* $\lambda' = \rho \circ \lambda$. *Под точкой поля* K *будем понимать класс эквивалентности его пополнений.*

Определение 3. *Точка* **A***-поля* k, *определяемая пополнением* (λ, K), *называется вещественной, если поле* K *изоморфно* **R**; *мнимой, если* K *изоморфно* **C**; *бесконечной в обоих этих случаях и конечной в остальных случаях.*

Пусть v — точка поля k. Очевидно, что функция $\mathrm{mod}_K \circ \lambda$ на k одна и та же для всех пополнений (λ, K), принадлежащих v. Будем записывать ее в виде $x \to |x|_v$. Если v — мнимая точка, то $\mathrm{mod}_K (x - y)^{1/2}$ является метрикой на K, во всех остальных случаях это верно для $\mathrm{mod}_K (x - y)$. Следовательно, мы всегда можем получить пополнение поля k, принадлежащее к v, взяв пополнение относительно

метрики $|x-y|_v^{\alpha}$, где $\alpha = 1/2$, если v мнимо, и $a = 1$ в остальных случаях. Это пополнение будет обозначаться через k_v и называться *пополнением поля k в точке v*. Для всех $x \in k_v$ положим $|x|_v = \mathrm{mod}_{k_v}(x)$. Если v — конечная точка, то мы будем обозначать через r_v максимальное компактное подкольцо поля k_v, а через p_v — его максимальный идеал. Это — подмножества в k_v, задаваемые соответственно условиями $|x|_v \leqslant 1$ и $|x|_v < 1$.

Как видно из теоремы 5 п.16.1.2, поле **Q** имеет одну бесконечную точку, соответствующую вложению **Q** в поле $\mathbf{R} = \mathbf{Q}_\infty$; эта точка будет обозначаться через ∞. Та же теорема показывает, что конечные точки поля **Q** находятся во взаимно однозначном соответствии с рациональными простыми числами, с которыми их можно отождествить. Точке p соответствует вложение **Q** в $\mathbf{Q}_p$.

Знание точек поля **Q** является для нас исходным пунктом при определении точек полей алгебраических чисел, рассматриваемых как конечные алгебраические расширения поля **Q**. Для того чтобы тем же методом исследовать **A**-поля характеристики $p > 1$, нужно знать точки поля $\mathbf{F}_p(T)$. Прежде чем заниматься их нахождением, приведем ряд общих результатов о точках алгебраических расширений.

Предложение 1. *Пусть k — произвольное поле, k_0 — его бесконечное подполе и λ — изоморфное вложение k_0 в локальное поле K. Замыкание K_0 множества $\lambda(k_0)$ в K является локальным полем, и замыкание множества $\lambda(k)$ в K есть поле, порожденное $\lambda(k)$ над K_0.*

Первое утверждение сразу вытекает из следствия 3 предл. 2 п. 16.1.2. По следствию 2 теор. 3 п. 16.1.2 K должно поэтому иметь конечную степень над K_0, так что в силу теоремы 3 п. 16.1.2 каждое векторное пространство над K_0, содержащееся в поле K, замкнуто в нем. Поле K_1, порожденное $\lambda(k)$ над K_0, является таким подпространством. С другой стороны, очевидно, что замыкание множества $\lambda(k)$ в K есть поле, содержащее $\lambda(k_0)$, а значит, и K_0 и $\lambda(k)$. Таким образом, оно совпадает с K_1.

Следствие. *Пусть k — некоторое* **A***-поле, k'— его конечное алгебраическое расширение и w — точка поля k'. Пусть, далее, λ — естественное вложение поля k' в его пополнение k в w. Тогда k'_w есть конечное алгебраическое расширение замыкания $\lambda(k)$ в k'_w и вложение поля k в это замыкание, индуцируемое вложением λ_v определяет точку v поля k.*

В силу наших определений это частный случай предложения 1.

Мы имеем теперь возможность ввести следующее определение.

Определение 4. *Если k и k' таковы, как в следствии предложения* 1, *то говорят, что v — точка поля k, лежащая под w, а w — точка, лежащая над v, и пишут* $w \mid v$.

В описанной ситуации мы будем обычно отождествлять поле k_v с замыканием поля k в k'_w.

Теорема 1. *Пусть k — какое-нибудь* **A**-*поле, k' — его алгебраическое расширение и v — его точка. Тогда существует точка поля k', лежащая над v, и таких точек может быть лишь конечное число.*

Пусть K — алгебраическое замыкание поля k_v и k'' —алгебраическое замыкание поля k в K. Так как k'' — алгебраически замкнуто, существует по меньшей мере один изоморфизм λ над k из k' в k''. Обозначим через K_λ поле, порожденное над k_v множеством $\lambda(k')$; оно является конечным алгебраическим расширением поля k_v, и потому его можно наделить структурой топологического векторного пространства конечной размерности над k_v. Тем самым оно превращается в локальное поле. Но тогда по предложению 1 (λ, K_λ) есть пополнение поля k' и определяет точку в k', которая, очевидно, лежит над v. Обратно, пусть w — какая-нибудь точка поля k'', лежащая над v. Тогда по следствию предл. 1 существует по меньшей мере один изоморфизм φ над k_v поля k'_w в K. Пусть λ — изоморфизм из k' в K, индуцируемый на k' морфизмом φ. Ясно, что λ отображает k' в k''. В силу предложения 1 поле k'_w порождается над k_v множеством k', так что поле $\varphi(k'_w)$— это то же самое поле, которое обозначалось выше через K_λ. Далее, снова используя следствие 1 теор. 3 п. 16.1.2, получаем, что φ есть топологический изоморфизм поля k'_w на K_λ, так что w — та точка поля k', которая определяется пополнением (λ, K_λ). Итак, точек поля k', лежащих над v, существует столько же, сколько имеется различных изоморфизмов λ над k из поля k' в k''. Но хорошо известно (и легко доказывается), что поскольку k' — конечное алгебраическое расширение поля k, таких изоморфизмов существует лишь конечное число.

Следствие. *Всякое* **A**-*поле имеет не более чем конечное число бесконечных точек; оно имеет по меньшей мере одну такую точку, если его характеристика равна нулю, и ни одной в противном случае.*

Последнее утверждение очевидно. Остальные суть частные случаи теоремы 1, ибо точка **A**-поля характеристики 0 бесконечна в том и только в том случае, когда она лежит над точкой ∞ поля $\mathbf{Q}$.

Перейдем теперь к нахождению точек поля $\mathbf{F}_p(T)$. Более общим образом мы определим все точки полей $\mathbf{F}_q(T)$, где $\mathbf{F}_q$ — произвольное конечное поле. Удобно говорить, что многочлен π из $\mathbf{F}_q[T]$ *прост,* если он унитарен, неприводим в кольце $\mathbf{F}_q[T]$ и имеет степень >0.

Теорема 2. *Поле* $k = \mathbf{F}_q(T)$ *имеет одну и только одну точку* v, *для которой* $|T|_v > 1$; *в этой точке* T^{-1} *является простым элементом поля* k_v *и модуль поля* k_v *равен* q. *Для каждого простого многочлена* π *из* $\mathbf{F}_q[T]$ *поле* k *имеет одну и только одну точку* v, *такую, что* $|\pi|_v < 1$; *в этой точке* π *является простым элементом поля* k_v, *модуль которого равен* q^{δ}, *где* δ *— степень многочлена* π. *Все эти точки различны, и поле* k *не имеет других точек.*

Пусть v — точка поля k. Предположим сначала, что $|T|_v \leqslant 1$. Тогда $\mathbf{F}_q[T]$ содержится в r_v. Обозначим через ρ канонический гомоморфизм кольца r_v на конечное поле r_v/p_v; он индуцирует на $\mathbf{F}_q[T]$ гомоморфизм кольца $\mathbf{F}_q[T]$ на его образ, ядро которого $p_v \cap \mathbf{F}_q[T]$ является, очевидно, простым идеалом в $\mathbf{F}_q[T]$. Поскольку кольцо $\mathbf{F}_q[T]$ бесконечно, а поле r_v/p_v конечно, этот идеал не может равняться $\{0\}$ и, следовательно, является идеалом $\pi \cdot \mathbf{F}_q[T]$, порожденным в $\mathbf{F}_q[T]$ некоторым простым многочленом π. Поэтому $|\pi|_v < 1$ и $|\alpha|_v = 1$ для каждого многочлена α из $\mathbf{F}_q[T]$, взаимно простого с π. Каждое $\xi \in k^{\times}$ можно записать в виде $\xi = \pi^n \alpha/\alpha'$, где $n \in \mathbf{Z}$, а α, α' — многочлены из $\mathbf{F}_q[T]$, взаимно простые с π. При этом $|\xi|_v = |\pi|_v^n$. В частности, ξ принадлежит r_v тогда и только тогда, когда $n \geq 0$, т. е. когда его можно записать в виде $\xi = \beta/\alpha$, где α, β— многочлены из $\mathbf{F}_q[T]$, причем α взаимно прост с π. Так как $\mathbf{F}_q[T]$ плотно в k_v, области значений, принимаемых функцией $|x|_v$ на $\mathbf{F}_q[T]$ и на k_v, совпадают между собой. Отсюда следует, что π — простой элемент поля k_v. Пусть теперь δ — степень многочлена π. Образ кольца $\mathbf{F}_q[T]$ в r_v/p_v изоморфен полю $\mathbf{F}_q[T]/\pi \cdot \mathbf{F}_q[T]$, которое есть расширение поля $\mathbf{F}_q$ степени δ и состоит потому из q^{δ} элементов. Ясно, что образ каждого элемента кольца $r_v \cap \mathbf{F}_q(T)$ должен принадлежать этому же полю, которое, поскольку $\mathbf{F}_q[T]$ плотно в k_v, является не чем иным, как полем r_v/p_v. Это показывает, что модуль поля k_v равен q^{δ} и $|\pi|_v = q^{-\delta}$. Таким образом, функция $|\xi|_v$ на поле k однозначно определяется заданием π, так что при заданном π существует самое большее одна точка v поля k, свойства которой мы только что описали. Предположим теперь, что $|T|_v > 1$. Тогда $|T^{-1}|_v < 1$, и можно поступить точно так же, как и выше, заменив $\mathbf{F}_q[T]$ на $\mathbf{F}_q[T^{-1}]$ и π на T^{-1}. Легко видеть, что если $\xi = \beta/\alpha$, где многочлены β и α из $\mathrm{F_q}[T]$ отличны от нуля и имеют степени соответственно b и a, то $|\xi|_v = q^{b-a}$. Теперь ясно, что если π — простой многочлен, то $|\pi|_v$ не может быть <1, за исключением точки v, описанной выше (если таковая существует), и что то же самое верно для T^{-1}. Докажем существование таких точек. Разберем сначала

случай $\pi = T$. Кольцо $\mathbf{F}_q[T]$ можно в этом случае вложить очевидным образом в кольцо формальных степенных рядов $\sum_0^\infty a_i T^i$ с коэффициентами из $\mathbf{F}_q$. Ясно, что, расширяя это вложение на соответствующие поля, можно получить точку поля k, отвечающую многочлену $\pi = T$. Заменяя T на T^{-1} видим, что то же самое верно для T^{-1}. Возьмем теперь какой-нибудь простой многочлен π степени δ. Поле $\mathbf{F}_q(T)$ содержит $\mathbf{F}_q(\pi)$ и алгебраично над ним. Его степень d над $\mathbf{F}_q(\pi)$ не превосходит δ. Как мы только что доказали, в $\mathbf{F}_q(\pi)$ существует точка w, для которой $|\pi|_w = q^{-1}$. В силу теоремы 1 поле $\mathbf{F}_q(T)$ имеет точку v, лежащую над w. По следствию 2 теор. 3 п.16.1.2 имеем $|\pi|_v = |\pi|_w^d = q^{-d}$. Это завершает доказательство, показывая одновременно, что $d = \delta$.

Следствие. *В обозначениях теоремы 2 пусть v — точка поля k, соответствующая простому многочлену π степени δ. Тогда многочлены степени $< \delta$ из $\mathbf{F}_q[T]$ образуют полную систему представителей классов смежности кольца r_v по модулю идеала p_v.*

Это сразу следует из доказанного выше и из того факта, что эти многочлены образуют полную систему представителей классов кольца $\mathbf{F}_q[T]$ по модулю π.

Условимся, начиная с этого места, говорить, что свойство, относящееся к точке некоторого **A**-поля, выполняется *почти для всех* (или *для почти всех) точек из k* (или выполняется *почти всюду,* в случае когда последнее выражение не может привести к недоразумениям), если оно верно для всех точек, кроме, быть может, конечного числа. Это соглашение используется, например, в формулировке нашего следующего результата.

Теорема 3. *Пусть k — некоторое* **A**-*поле и ξ — какой-нибудь его элемент. Тогда $|\xi|_v \leqslant 1$ почти для всех точек поля k.*

Если $k = \mathbf{Q}$, то это очевидно, ибо в этом случае ξ можно записать в виде a/b, где a, b — элементы из $\mathbf{Z}$, причем, $b \neq 0$ и $|\xi|_p \leqslant 1$ для всех простых p, не делящих b. Пусть теперь k — какое-нибудь **A**-поле характеристики 0, т. е. поле алгебраических чисел. Тогда ξ удовлетворяет уравнению

$$\xi^n + a_1\xi^{n-1} + \ldots + a_n = 0,$$

коэффициенты которого a_i принадлежат $\mathbf{Q}$. Пусть P — конечное множество, состоящее из ∞ и всех простых чисел, встречающихся в знаменателях чисел a_i. По теореме 1 множество P' точек поля k, лежащих над точками из P, конечно. Выберем какую-нибудь точку v поля k, не принадлежащую P'. Тогда точка p поля $\mathbf{Q}$, лежащая под v, не принадлежит P и, следовательно, $|a_i|_p \leqslant 1$ для $1 \leqslant i \leqslant n$. Таким

образом, ξ — целый элемент над $\mathbf{Z}_p$. Ввиду предложения 6 п.16.1.4 отсюда следует, что ξ находится в r_v, т.е. $|\xi|_v \leqslant 1$. Что касается **A**-полей характеристики $p>1$, то к ним применимо аналогичное доказательство. Можно рассуждать и следующим образом. Если элемент ξ алгебраичен над простым полем, то $|\xi|_v = 1$ или 0 для всех v в соответствии с тем, отличен элемент ξ от нуля или нет. Действительно, если это не так, то k алгебраично над $\mathbf{F}_p(\xi)$. Пусть v — точка поля k и w — точка из $\mathbf{F}_p(\xi)$, лежащая под ней. В силу следствия 2 теор. 3 п.16.1.2 $|\xi|_v > 1$ тогда и только тогда, когда $|\xi|_w > 1$. По теореме 2 поле $\mathbf{F}_p(\xi)$ имеет только одну точку с таким свойством. Применение теоремы 1 завершает доказательство.

Следствие 1. *Пусть E — конечномерное векторное пространство над* **A**-*полем k и ε, ε' — два конечных подмножества в E, содержащих базисы этого пространства. Положим $E_v = E \otimes_k k_v$ для каждой конечной точки v поля k и через ε_v и ε'_v обозначим r_v-модули, порожденные в E_v соответственно ε и ε'. Тогда $\varepsilon_v = \varepsilon'_v$ почти для всех v.*

Здесь, как и всюду далее в подобных ситуациях, мы будем рассматривать E как вложенное в E_v с помощью вложения $e \to e \otimes 1_{k_v}$. Положим $\varepsilon = \{e_1, \ldots, e_r\}$ и $\varepsilon' = \{e'_1, \ldots, e'_s\}$. Поскольку ε содержит базис пространства E над k, e'_j можно записать (вообще говоря, неоднозначно) в виде $e'_j = \sum c_{ji} e_i$, $1 \leqslant j \leqslant s$, с коэффициентами c_{ij} из k. Поэтому $\varepsilon'_v \subset \varepsilon_v$ всякий раз, когда все $|c_{ji}|_v \leqslant 1$, следовательно, почти для всех v. Меняя местами ε и ε', получаем утверждение нашего следствия.

Следствие 2. *Пусть $\mathcal{A}$ — конечномерная алгебра над* **A**-*полем k, α — ее конечное подмножество, содержащее какой-нибудь базис алгебры $\mathcal{A}$ над k. Положим $\mathcal{A}_v = \mathcal{A} \otimes_k k_v$ для каждой конечной точки v поля k и через α_v обозначим r_v-модуль, порожденный множеством α в $\mathcal{A}_v$. Тогда почти для всех v α_v — компактное подкольцо алгебры $\mathcal{A}_v$.*

Положим $\alpha = \{a_1, \ldots, a_r\}$ и $\alpha' = \{1, a_1, \ldots, a_r\}$. Так как α содержит базис алгебры $\mathcal{A}$ над k, можно написать $a_i a_j = \sum c_{ijh} a_h$, $1 \leqslant i, j \leqslant r$, где коэффициенты $c_{ijh} \in k$. Следовательно, α_v является подкольцом в $\mathcal{A}_v$, если все $|c_{ijh}|_v \leqslant 1$, т. е. почти для всех v. Очевидно, оно компактно, и $\alpha_v = \alpha'_v$ почти для всех v.

16.3.2. Тензорные произведения коммутативных полей

Доказательство теоремы 1 дает для **A**-поля k и его конечного алгебраического расширения k' конструкцию точек поля k', лежащих над заданной точкой поля k. Наряду с этой конструкцией рассмотрим еще одну, основанную на использовании тензорного произведения $k' \otimes_k k_v$. Для простоты ограничимся случаем, когда поле k' сепарабельно над k. Этого достаточно для наших целей в силу следующей леммы.

Лемма 1. *Каждое* **A**-*поле характеристики* $p>1$ *изоморфно некоторому сепарабельному алгебраическому расширению конечной степени поля* $\mathbf{F}_p(T)$.

Пусть k — такое поле. Представим его в виде $\mathbf{F}_p(x_1, \ldots, x_N)$, где по меньшей мере одно из x_i, например x_1, трансцендентно над $\mathbf{F}_p$. Докажем индукцией по N, что существует x_i, такое, что k сепарабельно над $\mathbf{F}_p(x_i)$. Это очевидно, если $N = 1$, а также если $x_2, \ldots, x_N$ все алгебраичны над $\mathbf{F}_p$, ибо в этом случае они сепарабельны над $\mathbf{F}_p$ по теореме 2 п.16.1.1 и, значит, поле k сепарабельно над $\mathbf{F}_p(x_1)$. Если же это не так, то по предположению индукции при некотором $i \geq 2$ поле $\mathbf{F}_p(x_2, \ldots, x_N)$ сепарабельно над некоторым $\mathbf{F}_p(x_i)$, скажем над $\mathbf{F}_p(x_2)$, так что само k сепарабельно над $\mathbf{F}_p(x_1, x_2)$. Поскольку k имеет над $\mathbf{F}_p$ степень трансцендентности 1, в кольце $\mathbf{F}_p[X_1, X_2]$ существует неприводимый многочлен Φ, для которого $\Phi(x_1, x_2) = 0$. Многочлен Φ не является многочленом вида Φ'^p, где $\Phi' \in \mathbf{F}_p[X_1, X_2]$; так как каждый элемент α из $\mathbf{F}_p$ удовлетворяет уравнению $\alpha^p = \alpha$, то это можно выразить, сказав, что Φ содержит по меньшей мере один член вида $\alpha X_1^a \cdot X_2^b$, где $\alpha \neq 0$ и a или b взаимно просто с p. Пусть для определенности a взаимно просто с p. Тогда x_1 сепарабельно над $\mathbf{F}_p(x_2)$, так что k также сепарабельно над $\mathbf{F}_p(x_2)$.

В оставшейся части этого параграфа будут изучаться чисто алгебраические свойства тензорных произведений вида $k' \otimes_k K$, где k — произвольное поле, k' — его сепарабельное алгебраическое расширение конечной степени и K — некоторое поле, содержащее k. В п.16.2.4 эта теория будет применяться к случаю, когда k есть **A**-поле, а K — его пополнение. Но сначала получим ответ на один технический вопрос.

Лемма 2. *Если коммутативное кольцо* B *может быть представлено в виде прямой суммы полей, то это можно сделать только одним способом. При этом гомоморфизм кольца* B *в поле должен равняться нулю на всех слагаемых, кроме одного.*

Пусть B — прямая сумма полей $K_1, \ldots, K_r$. Положим $e_i = 1_{K_i}$. Тогда $K_i = e_i B$ и $1_B = \Sigma e_i$ является единичным элементом в B. Ясно, что решения в B уравнения $X^2 = X$ («идемпотенты» кольца B) будут частичными суммами для Σe_i; поэтому e_i однозначно характеризуются среди решений уравнения $X^2 = X$ тем, что их нельзя представить в виде $e + e'$, где e, e' — решения, отличные от нуля. Если f — гомоморфизм кольца B в поле K', то он должен переводить каждое e_i в решение уравнения $X^2 = X$ в поле K', т. е. в 1 или в 0. Если $f(e_i) = 1$, то $f(e_j) = 0$ для всех $j \neq i$, ибо $e_i e_j = 0$ при $i \neq j$. Отсюда следует, что f равно нулю на на K_j.

Предложение 2. *Пусть k — поле, $k' = k(\xi)$ — его сепарабельное расширение, порожденное корнем ξ, неприводимого унитарного многочлена F степени n из $k[X]$. Пусть K — поле, содержащее k, и $F_1, \ldots, F_r$ — неприводимые унитарные многочлены из $K[X]$, такие, что $F = F_1 \ldots F_r$. Для каждого i обозначим через ξ_i какой-нибудь корень многочлена F_i в некотором расширении поля K. Тогда алгебра $A = k' \otimes_k K$ над K изоморфна прямой сумме полей $K(\xi_i)$.*

Так как k' сепарабельно над k, то F не имеет кратных корней ни в одном расширении поля k, так что все F_i различны. Обозначим через ρ k-линейный гомоморфизм кольца $k[X]$ на поле k'', с ядром $F \cdot k[X]$, переводящий X в ξ. Его можно однозначно продолжить до K-линейного гомоморфизма ρ' кольца $k[X]$ на A, с ядром $F \cdot k[X]$, определяющего изоморфизм кольца $A' = K[X]/F \cdot K[X]$ на A. Покажем теперь, что алгебра A' изоморфна прямой сумме B алгебр $B_i = K[X]/F_i \cdot K[X]$ над K; а так как последние изоморфны полям из формулировки предложения, то доказательство тем самым будет завершено. Пусть f — произвольный элемент из $K[X]$; обозначим через $\overline{f}$ его образ в A, а через $\overline{f_i}$ — его образы в кольцах B_i. Очевидно, что каждый элемент $\overline{f_i}$ однозначно определяется элементом $\overline{f}$, так что отображение $\overline{f} \to (\overline{f_1}, \ldots, \overline{f_r})$ является гомоморфизмом φ из A' в B. Хорошо известно (и легко доказывается индукцией по r), что, поскольку F_i взаимно просты, существуют многочлены $p_1, \ldots, p_r$ из $K[X]$, такие, что $F^{-1} = \Sigma p_i F_i^{-1}$. Отсюда следует, что для всех i и всех $j \neq i$

$$p_i F_i^{-1} F \equiv 1 \ (F_i), \quad p_i F_i^{-1} F \equiv 0 \ (F_j). \tag{1}$$

Возьмем в кольце $K[X]$ r многочленов $f_1, \ldots, f_r$ и для каждого r обозначим через $\overline{f_i}$ образ многочлена f_i в B_i. Положим $f =$

$= \sum p_i F_i^{-1} F \bar{f}_i$ и обозначим через $\bar{f}$ образ f в A'. Элемент $\bar{f}$ однозначно определяется набором $\bar{f}_i$, так что $(\bar{f}_1, \ldots, \bar{f}_r) \to \bar{f}$ есть отображение ψ из B в A'. Ясно, что отображение $\psi \circ \varphi$ тождественно на A'; как показывает (1), $\varphi \circ \psi$ также тождественно на B. Следовательно, φ — изоморфизм кольца A' на B.

Пусть k, k' и K таковы, как в предложении 2. Ясно, что изоморфизм λ из k' в расширение K' поля K индуцирует тождественный морфизм на k в том и только том случае, когда он k-линеен. Такой изоморфизм называется *собственным над K,* если K' порождается над K множеством $\lambda(k)$, а пара (λ, K') называется *собственным вложением* k' *над* K. Два таких вложения (λ, K') и (λ', K'') называются *эквивалентными,* если найдется K-линейный изоморфизм ρ поля K' на K'', такой, что $\lambda' = \rho \circ \lambda$. Отметим, что эти понятия являются теми алгебраическими понятиями, которые лежат в основе определения 2 и предложения 1 из п.16.2.1.

Предложение 3. *Пусть k — поле, k' — его сепарабельное алгебраическое расширение конечной степени n, K — поле, содержащее k, и пусть $A = k' \otimes_k K$. Тогда с точностью до эквивалентности существует только конечное число собственных над K вложений (λ_i, K_i), $1 \leqslant i \leqslant r$, поля k'. Сумма степеней полей K_i над K равна n. Отображение $(\lambda_1, \ldots, \lambda_r)$ поля k' в прямую сумму B полей K_i является k-линейным изоморфизмом из k' в B, а его K-линейное расширение φ на алгебру A является изоморфизмом A на B.*

Пусть $k' = k(\xi)$ и F — неприводимый унитарный многочлен из кольца $k[X]$, имеющий корнем ξ. Применим к k, k', ξ, F и K предложение 2. Получим, что существует K-линейный изоморфизм φ алгебры A на некоторую прямую сумму B полей K_i. Обозначим для каждого i через β_i проекцию из B в K_i; тогда $\mu_i = \beta_i \circ \varphi$ будет K-линейным изоморфизмом алгебры A на K_i, индуцирующим на поле k' k-линейный изоморфизм λ_i в K_i. Очевидно, μ_i есть K-линейное продолжение морфизма λ_i на A, так что отображение φ, или, что то же самое, $(\mu_1, \ldots, \mu_r)$, является K-линейным расширением морфизма $(\lambda_1, \ldots, \lambda_r)$ на A. Если вложение λ_i не собственно над K, то должно существовать поле $K'' \neq K_i$, промежуточное между K и K_i и такое, что λ_i отображает k' в K''; μ_i отображает потому A в K'', но не на K_i. Пусть теперь λ — какой-нибудь k-линейный изоморфизм поля k' в поле K', содержащее K, и μ — его K-линейное продолжение на алгебру A. Очевидно, μ является гомоморфизмом из A в K', так что $\mu \circ \varphi^{-1}$ — гомоморфизм из B в K'. В силу леммы 2 он равен нулю на всех, кроме одного, слагаемых K_i кольца B и, следовательно, может быть записан как $\sigma \circ \beta_i$, где σ — некоторый K-линейный гомоморфизм поля K_i в K'.

Поскольку это поле, а гомоморфизм σ не равен нулю, он должен быть изоморфизмом поля K_i на его образ K'_i в K'. Это дает $\mu = \sigma \circ \mu_i$, значит $\lambda = \sigma \circ \lambda_i$. Если $K'_i \neq K'$, то морфизм λ, переводящий k' в K'_i несобствен; следовательно, если λ собствен, то σ— изоморфизм поля K_i на K', так что вложения (λ, K') и (λ_i, K_i) эквивалентны. Наконец, если мы имеем в тоже время $\lambda = \sigma' \circ \lambda_j$, где $j \neq i$ и σ' — изоморфизм из K_j в K', то $\mu = \sigma' \circ \mu_j$, следовательно, $\mu \circ \varphi^{-1} = \sigma' \circ \beta_j$, и $\mu \circ \varphi^{-1}$ ' должно быть на K_i отлично от нуля. В частности, если λ собствен, то (λ, K') эквивалентно не более чем одному из вложений (λ_i, K_i); это означает, что все эти вложения неэквивалентны, чем и заканчивается доказательство.

Следствие 1. *Пусть в тех же обозначениях, что и выше,* λ — *произвольный k-линейный изоморфизм из поля k' в поле K', содержащее K. Тогда существуют такое единственное i и такой единственный изоморфизм* σ *из* K_i *в K', что* $\lambda = \sigma \circ \lambda_i$.

Это уже доказано выше. Это является также непосредственным следствием предложения 3 и того факта, что для подполя K'' в K', порожденного над K множеством $\lambda(k')$, (λ, K'') есть собственное вложение поля k' над K и, значит, эквивалентно одному из вложений (λ_i, K_i).

Следствие 2. *В тех же обозначениях, что и выше, предположим, что k' есть расширение Галуа поля k с группой Галуа G. Пусть* (λ, *K')* — *произвольное собственное вложение поля k' над K. Тогда K' будет расширением Галуа поля K и для каждого автоморфизма* ρ *поля K' над K найдется единственное* $\sigma \in G$, *такое, что* $\rho \circ \lambda = \lambda \circ \sigma$. *Соответствие* $\rho \to \sigma$ *является изоморфизмом группы Галуа поля K' над K на некоторую подгруппу H группы G. Все собственные вложения поля k' над K имеют, с точностью до эквивалентности, вид* $(\lambda \circ \sigma, K')$, *где* $\sigma \in G$; *если* $\sigma, \sigma' \in G$, *то вложения* $(\lambda \circ \sigma', K')$ *и* $(\lambda \circ \sigma, K)$ *эквивалентны тогда и только тогда, когда* $\sigma' \in H\sigma$.

Ясно, что $\lambda(k')$ есть расширение Галуа поля k, а так как K' порождено над K множеством $\lambda(k')$, то K' есть расширение Галуа поля K и ограничение на $\lambda(k')$ автоморфизмов поля K' над K определяет инъективное отображение группы Галуа H_1 поля K' над K в соответствующую группу поля $\lambda(k')$ над k. Но это равносильно первой части нашего следствия. Для любого $\sigma \in G$ вложение $(\lambda \circ \sigma, K')$ является, очевидно, собственным вложением поля k' над K. Если σ, σ' принадлежат G, то $(\lambda \circ \sigma', K)$ и $(\lambda \circ \sigma, K)$ эквивалентны в том и только в том случае, когда существует автоморфизм ρ поля K' над K, такой, что $\lambda \circ \sigma' = \rho \circ \lambda \circ \sigma$, т. е. $\rho \circ \lambda = \lambda \circ (\sigma' \circ \sigma^{-1})$. Последнее

выполняется в том и только в том случае, когда $\sigma' \circ \sigma^{-1}$ принадлежит H. Таким образом, число неэквивалентных собственных вложений такого вида равно индексу группы H в G, т. е. n/n', где n, n' — степени соответственно поля k' над k и поля K' над K. Ввиду предложения 3 для любого множества неэквивалентных собственных вложений (λ_i, K_i) поля k' над K сумма степеней полей K_i над K не должна превосходить n. Итак, с точностью до эквивалентности, каждое вложение указанного типа имеет вид $(\lambda \circ \sigma, K')$.

Полезен тот частный случай следствия 2, когда k' есть подполе в K', порождающее K' над K. Тогда в качестве λ можно взять тождественное отображение; собственные вложения поля k' над K будут иметь вид (σ, K'), где $\sigma \in G$, а отображение $\rho \to \sigma$ группы Галуа поля K' над K в группу поля k' над k будет ограничением на k' автоморфизмов поля K' над K.

Следствие 3. *Пусть k и k' таковы, как в предложении* 3, *и пусть K — алгебраически замкнутое или сепарабельно алгебраически замкнутое поле, содержащее k. Тогда существует n, но не более чем n, различных k-линейных изоморфизмов $\lambda_1, \ldots, \lambda_n$ из k' в K. Они линейно независимы над K, и если λ, λ' — любые два из них, а K — алгебраическое замыкание поля k, то найдется автоморфизм α поля K, для которого $\lambda' = \alpha \circ \lambda$.*

Поле K называется *сепарабельно алгебраически замкнутым,* если у него нет сепарабельных алгебраических расширений, отличных от него самого. Первое очевидное утверждение нашего следствия включено в него для удобства ссылок, а также как иллюстрация предложения 3, частным случаем которого оно является. В самом деле, если K таково, как в следствии, то все K_i из этого предложения должны совпадать с K. Второе утверждение (представляющее собой хорошо известную теорему Дедекинда, легко доказываемую и непосредственно) можно извлечь из предложения 3 следующим образом. Предположим, что $\sum c_i \lambda_i = 0$ для некоторых $c_i \in K$, $1 \leqslant i \leqslant n$, т. е. что $\sum c_i \lambda_i(\xi) = 0$ для всех $\xi \in k'$. Вводя μ_i и β_i так же, как и в доказательстве предложения 3, находим, что $\sum c_i \mu_i = 0$ и, значит, $\sum c_i \beta_i = 0$, что, очевидно, возможно, только если все c_i равны нулю. Из единственности, с точностью до изоморфизма, алгебраического замыкания поля k следует, что каждое λ_i продолжается до изоморфизма алгебраического замыкания $\overline{k}$ поля k' на K. Отсюда вытекает последнее утверждение следствия, включенное в его формулировку также для удобства ссылок.

Следствие 4. *В предположениях и обозначениях следствия* 3 *предположим еще, что k' есть расширение Галуа над k. Тогда все* λ_i *отображают k' на одно и то же подполе в K.*
Это вытекает из следствия 2.

16.3.3. Следы и нормы

Напомним сначала понятие полиномиального отображения. Пусть *E, E'* — векторные пространства конечной размерности над полем *k*, имеющим бесконечное число элементов, и пусть $\varepsilon = \{e_1, \ldots, e_n\}$ и $\varepsilon' = \{e'_1, \ldots, e'_m\}$ — их базисы над полем *k*. Отображение *f* из *E* в *E'* называется *полиномиальным,* если в кольце $k[X_1, \ldots, X_n]$ найдутся такие многочлены P_j, что для всех значений x_i из *k*

$$f\left(\sum_i x_i e_i\right) = \sum_j P_j(x_1, \ldots, x_n)\, e'_j.$$

Ясно, что это определение не зависит от выбора базисов $\varepsilon, \varepsilon'$. Далее, поскольку в *k* бесконечно много элементов, многочлены P_j однозначно определяются по f, ε и ε'. Если $E' = k$, то *f* называется *полиномиальной функцией;* степень соответствующего многочлена *P* не зависит от выбора ε и называется *степенью f.* Если *K* — произвольное поле, содержащее *k*, и $E_K = E \otimes_k K, E'_K = E' \otimes_k K$, то существует одно и только одно полиномиальное отображение из E_K в E'_K, совпадающее с *f* на *E.* Оно называется *продолжением* отображения *f* на E_K и E'_K (или, короче, на *K)* и обозначается по-прежнему через *f.* Это продолжение задается, по отношению к базисам $\varepsilon, \varepsilon'$ пространств E_K, E'_K над *K,* теми же многочленами, что и раньше.

Пусть *E* такое же, как и выше. Обозначим через End *(E)* кольцо его эндоморфизмов, рассматриваемое как алгебра над *k.* Для $a \in \mathrm{End}\, E$ через tr *(a)* и det *(a)* обозначаются соответственно след и определитель *a.* Первый является линейной формой, а последний —полиномиальной функцией (степень которой равна размерности пространства *F)* на пространстве End (*E*), рассматриваемом как векторное пространство над *k.*

Пусть теперь $\mathcal{A}$ — алгебра конечной размерности над *k;* как всегда, мы предполагаем, что у нее есть единичный элемент 1. Для каждого $a \in \mathcal{A}$ обозначим через $\rho(a)$ эндоморфизм $x \to ax$ алгебры $\mathcal{A}$, рассматриваемой как векторное пространство над полем *k.* Обозначая через $\mathrm{End}(\mathcal{A})$ алгебру всех эндоморфизмов этого векторного пространства, мы можем рассматривать ρ как гомоморфизм из $\mathcal{A}$ в $\mathrm{End}(\mathcal{A})$. Этот гомоморифзм известен под названием

регулярного представления алгебры $\mathcal{A}$; поскольку $\mathcal{A}$ имеет единицу, он является изоморфизмом $\mathcal{A}$ на некоторую подалгебру в $\mathrm{End}(\mathcal{A})$. След и определитель отображения ρ называются *регулярным следом* и *регулярной нормой* в алгебре $\mathcal{A}$ над k и обозначаются соответственно через $\mathrm{Tr}_{\mathcal{A}/k}$ и $\mathrm{N}_{\mathcal{A}/k}$ или (если не может возникнуть недоразумений) просто Tr и N. Регулярный след есть линейная форма на $\mathcal{A}$, рассматриваемом как векторное пространство над k, а регулярная норма есть полиномиальная функция степени, равной размерности $\mathcal{A}$ над k. Если K — поле, содержащее k, и A расширено над K до алгебры $\mathcal{A}_K = \mathcal{A} \otimes_k K$, то регулярный след и регулярная норма в алгебре $\mathcal{A}_K$ над K являются соответственно продолжениями $\mathrm{Tr}_{\mathcal{A}/k}$ и $\mathrm{N}_{\mathcal{A}/k}$ на $\mathcal{A}_K$ и обозначаются по-прежнему через $\mathrm{Tr}_{\mathcal{A}/k}$ и $\mathrm{N}_{\mathcal{A}/k}$. В случае когда A есть поле k' конечной степени над k, слово «регулярный», как правило, опускается и $\mathrm{Tr}_{k'/k}$ и $\mathrm{N}_{k'/k}$ называются соответственно *следом* и *нормой* в поле k' над k. Посмотрим теперь, как эти понятия применяются в ситуации, описанной в п.16.3.2.

Предложение 4. *Пусть k — поле, k' — его сепарабельное алгебраическое расширение конечной степени n и K — поле, содержащее k. Положим $A = k' \otimes_k K$, и пусть $(\lambda_i, K_i)_{1 \leqslant i \leqslant r}$ — максимальное множество неэквивалентных собственных вложений поля k' над K и для каждого i μ_i суть K-линейные продолжения λ_i на A. Тогда для всех $a \in A$*

$$\mathrm{Tr}_{k'/k}(a) = \sum_{i=1}^{r} \mathrm{Tr}_{K_i/K}(\mu_i(a)), \quad \mathrm{N}_{k'/k}(a) = \prod_{i=1}^{r} \mathrm{N}_{K_i/K}(\mu_i(a)).$$

Действительно, пусть обозначения будут те же, что использовавшиеся в предложении 3 п.16.3.2 и в его доказательстве. Положим $b = \varphi(a)$. Для каждого i проекция элемента b на K_i равна $\beta_i(b) = \mu_i(a)$. Поэтому $\mathrm{Tr}_{k'/k}(a)$ и $\mathrm{N}_{k'/k}(a)$ являются следом и определителем отображения $y \to by$, рассматриваемого как эндоморфизм алгебры B. Выбирая в B базис, являющийся объединением базисов пространств K_i над K, получаем формулы предложения 4.

Следствие 1. *Если k и k' таковы, как в предложении* 4, *то k-линейная форма $\mathrm{Tr}_{k'/k}$ на k' отлична от нуля.*

Выберем в предложении 4 в качестве K алгебраически замкнутое поле, содержащее k; тогда $K_i = K$ для всех i, а из предложения 4 вытекает, что $\mathrm{Tr}_{k'/k}(a) = \Sigma\, \mu_i(a)$. В тех же обозначениях, что и прежде, положим $b = \varphi(a)$, так что $\beta_i(b) = \mu_i(a)$. Поскольку проекции $\beta_i(b)$ элемента b на слагаемые кольца B можно выбирать

произвольно, выберем их так, чтобы $\mathrm{Tr}_{k'/k}(a)$ не равнялся нулю. Так как форма $\mathrm{Tr}_{k'/k}$ на A является продолжением на A k–линейной формы $\mathrm{Tr}_{k'/k}$ на k', а последняя не равна нулю, то и первая не равна нулю.

Следствие 1. *В обозначениях и предположениях предложения* 4 *имеем для всех* $x \in k'$

$$\mathrm{Tr}_{k'/k}(x) = \sum_i \mathrm{Tr}_{K_i/K}(\lambda_i(x)); \quad \mathrm{N}_{k'/k}(x) = \prod_i \mathrm{N}_{K_i/K}(\lambda_i(x)).$$

Следствие 3. *Пусть* k, k' *такие же, как в предложении* 4, K — *алгебраически замкнутое поле, содержащее* k, *и* $\lambda_1, \ldots, \lambda_n$— *различные* k*-линейные изоморфизмы из* k' *в поле* K.. *Тогда для всех* $x \in k'$

$$\mathrm{Tr}_{k'/k}(x) = \sum_i \lambda_i(x), \quad \mathrm{N}_{k'/k}(x) = \prod_i \lambda_i(x).$$

Это следует из предложения 4 и следствия 3 предл. 3 п.16.3.2.

Следствие 4. *Пусть* k, k' *таковы, как в предложении* 4, *и* k'' — *сепарабельное алгебраическое расширение поля* k', *имеющее конечную степень. Тогда*

$$\mathrm{Tr}_{k''/k} = \mathrm{Tr}_{k''/k'} \circ \mathrm{Tr}_{k'/k}, \quad \mathrm{N}_{k''/k} = \mathrm{N}_{k''/k'} \circ \mathrm{N}_{k'/k}.$$

Возьмем в качестве K алгебраическое замыкание поля k'' и определим λ_i, как в следствии 3. Обозначим через n' степень поля k'' над k' и через λ'_j, $1 \leqslant j \leqslant n'$, различные k'-линейные изоморфизмы поля k'' в K. Каждое λ_i продолжается до автоморифзма φ_i поля K. Положим $\lambda''_{ij} = \varphi_i \circ \lambda'_j$ при $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n'$; мы получим k'-линейные изоморфизмы из k'' в K. Ясно, что если $\lambda''_{ij} = \lambda''_{hl}$, то $i=h$, ибо λ''_{ij} индуцирует на k' отображение λ_i, и j=l, ибо $\varphi_i^{-1} \circ \lambda''_{ij} = \lambda'_j$. Далее, если λ'' — произвольный k-линейный изоморфизм из k'' в K, то он должен индуцировать на k' один из изоморфизмов λ_i, следовательно, отображение $\varphi_i^{-1} \circ \lambda''$ k'-линейно и, значит, должно совпадать с одним из λ'_j. Таким образом, $\lambda'' = \lambda'_{ij}$. Следствие 3 дает теперь для $x \in k''$

$$\mathrm{Tr}_{k''/k}(x) = \sum_{i,j} \lambda''_{ij}(x) = \sum_i \varphi_i\left(\sum_j \lambda'_j(x)\right) =$$

$$= \sum_i \varphi_i(\mathrm{Tr}_{k''/k'}(x)) = \sum_i \lambda_i(\mathrm{Tr}_{k''/k'}(x)) = \mathrm{Tr}_{k'/k}(\mathrm{Tr}_{k''/k'}(x)),$$

чем доказано наше первое утверждение. Формулу для нормы можно вывести в точности тем же способом.

Для полноты рассмотрим вкратце след и норму в несепарабельных расширениях. Пусть k'— произвольное алгебраическое расширение поля k конечной степени. Как хорошо известно, оно содержит единственное максимальное сепарабельное подрасширение k'_0, над которым оно чисто несепарабельно. Пусть $q = p^m$ — степень поля k' над k'_0, где p — характеристика. Легко видеть, что $x^q \in k'_0$ при всех $x \in k'$. Выберем какой-нибудь базис $\{\xi_1, \ldots, \xi_q\}$ поля k' над k'_0 и

элемент $a \in k'$. Как векторное пространство над k поле k' есть прямая сумма подпространств $\xi_i k'_0$, $1 \leqslant i \leqslant q$, которые инвариантны относительно отображения $x \to a^q x$, поскольку $a^q \in k'_0$. Следовательно,

$$N_{k'/k}(a^q) = N_{k'_0/k}(a^q)^q,$$

откуда вытекает, что

$$N_{k'/k}(a) = N_{k'_0/k}(a^q).$$

Обозначим через n_0 степень поля k'_0 над k, так что степень k' над k равна $n = n_0 q$. Если K — алгебраически замкнутое поле, содержащее k, то каждый k-линейный изоморфизм из k'_0 в K может быть однозначно продолжен до отображения из k' в K. В силу следствия 3 предл. 3 п.16.3.2 существует n_0 таких изоморфизмов λ_i, $1 \leqslant i \leqslant n_0$, и, комбинируя приведенную выше формулу для $N_{k'/k}$ со следствием 3 предл. 4 (примененным к k'_0 и k), получаем

$$N_{k'/k}(x) = \prod_i \lambda_i(x)^{n/n_0}$$

при всех $x \in k'$. Пусть теперь k'' — произвольное конечное расширение поля k'. Поступая так же, как и при доказательстве следствия 4 предл. 4, находим, что снова

$$N_{k''/k} = N_{k''/k} \circ N_{k'/k}.$$

Таким образом, это соотношение выполняется независимо от того, сепарабельны поля k' и k'' над k или нет.

Что касается следа, то из элементарных свойств определителя и определения следа и нормы следует, что для произвольной алгебры $\mathcal{A}$ над k $\mathrm{Tr}_{\mathcal{A}/k}(x)$ как линейная форма на $\mathcal{A}$ является суммой членов степени 1 в представлении полиномиальной функции $N_{\mathcal{A}/k}(1 + x)$ как многочлена от координат точки $x \in \mathcal{A}$ в некотором базисе алгебры $\mathcal{A}$. Применяя это к нашей ситуации, находим, что $\mathrm{Tr}_{k'/k}(x)$ есть сумма членов степени 1 в многочлене $N_{k'/k}(1 + x)$. А поскольку последний равен $N_{k'_0/k}(1 + x^q)$, то $\mathrm{Tr}_{k'/k}(x)$ содержит только члены, степень которых кратна q. Это показывает, что $\mathrm{Tr}_{k'/k} = 0$ при $q > 1$. Таким образом, в силу следствия 1 предл. 4 $\mathrm{Tr}_{k'/k} \neq 0$ тогда и только тогда, когда k' сепарабельно над k.

Предложение 5. *Пусть k' — сепарабельное алгебраическое расширение степени n поля k и $\{a_1, \ldots, a_n\}$ — его базис над k. Тогда определитель матрицы*

$$(\mathrm{Tr}_{k'/k}(a_i a_j))_{1 \leqslant i,\, j \leqslant n}$$

не равен 0.

В силу следствия 1 предл. 4 это частный случай следующей леммы, которая нам понадобится.

Лемма 3. *Пусть k' — произвольное расширение степени n поля k, E— векторное пространство над k, «несущее» k', и λ — какая-нибудь отличная от нуля линейная форма на E. Тогда отображение* $(x, y) \to \lambda(xy)$ *является невырожденной билинейной формой на* $E \times E$; *пространство E можно отождествить с его алгебраическим двойственным E', положив* $[x, y] = \lambda(xy)$; *определитель матрицы* $(\lambda(a_i a_j))$ *отличен от нуля для любого базиса* $a_1, \ldots, a_n$ *поля k' над k.*

Так как λ не равно нулю, существует такое $a \in k'$, что $\lambda(a) \neq 0$. Для каждого $y \in k'$ построим k-линейную форму λ_y на k'', положив $\lambda_y(x) = \lambda(xy)$, $x \in k'$. Отображение $y \to \lambda_y$ является морфизмом из E в его двойственное E'. Ядро этого морфизма равно нулю, ибо $y \neq 0$ влечет $\lambda_y(ay^{-1}) \neq 0$, т. е. $\lambda_y \neq 0$. А так как E и E' имеют над k одинаковую размерность, видим, что $y \to \lambda_y$— это изоморфизм E на E'. Отождествляя E и E' с помощью этого изоморфизма, получаем $[x, y] = \lambda(xy)$. Но по определению это означает невырожденность формы $(x, y) \to \lambda(xy)$. Наконец, если бы определитель матрицы $(\lambda(a_i a_j))$ был равен нулю, то в поле k можно было бы найти такие элементы $y_1, \ldots, y_n$, не все равные нулю, что $\sum_j \lambda(a_i a_j) y_j = 0$, так что, полагая

$$y = \sum_j a_j y_j,$$

мы находим, что $\lambda_y(a_i) = 0$ для всех i, и, значит, $\lambda_y = 0$, что противоречит доказанному выше.

16.3.4. Тензорные произведения A-полей и локальных полей

Пусть k — некоторое **A**-поле, k' — его сепарабельное расширение, v — точка и k_v — пополнение в этой точке. В силу предложения 1 п.16.3.1 и его следствия пополнения (λ, K') поля k', индуцирующие на k его естественное вложение в k_v, совпадают с собственными вложениями поля k' над k_v, введенными в п.16.3.2. Мы можем, следовательно, использовать предложения 2 и 3 из п.16.3.2 для определения точек поля k', лежащих над v. Этим мы и займемся.

Теорема 4. *Пусть k — некоторое* **A**-*поле, k' — его сепарабельное алгебраическое расширение конечной степени n и α — базис над k. Для каждой точки v поля k обозначим через* k_v *пополнение поля k в v и положим* $A_v = k' \otimes_k k_v$. *Далее, для всякой конечной точки v*

обозначим через r_v максимальное компактное подкольцо в k_v и через α_v обозначим r_v-модуль, порожденный множеством α в A_v. Пусть $w_1, \ldots, w_r$ —точки поля k', лежащие над v; k'_i — пополнения поля k' в точках w_i, λ_i —естественные проекции из k' в k'_i и μ_i — их k_v-линейные продолжения на A_v. Тогда отображение $\Phi_v = (\mu_1, \ldots, \mu_r)$ является изоморфизмом алгебры A_v на прямую сумму B_v полей k'_i и почти для всех v отображает α_0 на сумму максимальных компактных подколец n полей k'_i.

Если в предложении 3 п.16.3.2 положить $K = k_v$, то первое утверждение превращается в частный случай этого предложения. Коротко, но несколько вольно это можно выразить, сказав, что пополнения k'_i поля k' в точках, лежащих над v, суть слагаемые алгебры $k' \otimes_k k_v$, представленной в виде прямой суммы полей. Возьмем теперь в качестве v произвольную конечную точку поля k. Как легко видеть, сумма колец r'_i есть максимальное компактное подкольцо в B_v, а его образ ρ_v относительно Φ_v^{-1} есть, следовательно, максимальное компактное подкольцо в A_v. Нам нужно показать, что почти для всех v оно совпадает с α_v. Но ρ_v является k_v-решеткой в A_v, ибо каждое r'_i содержит r_v. По теореме 1 п.16.2.2 найдется такой базис $\{u_{v,1}, \ldots, u_{v,n}\}$ алгебры A_v над k_v, что ρ_v будет r_v -модулем, порожденным этим базисом. По следствию 2 теор. 3 п.16.3.1 α_v — компактное подкольцо в A_v, содержащееся поэтому в ρ_v почти для всех v. Обозначим через P конечное множество точек поля k, для которых это не так. Если $\alpha = \{a_1, \ldots, a_n\}$, то для точек v, не содержащихся в P, α_v принадлежит ρ_v и можно написать $a_i = \sum c_{v,ij} u_{v,j}$, где $c_{v,ij} \in r_v$. Матрица $C_v = (c_{v,ij})$ принадлежит, следовательно, кольцу $M_n(r_v)$, и $\alpha_v = \rho_v$ в том и только в том случае, когда эта матрица обратима в $M_n(r_v)$, т. е. когда ее определитель обратим в r_v.

Сокращая теперь запись $\mathrm{Tr}_{k'/k}$ до Tr, обозначим через Δ определитель матрицы

$$M = (\mathrm{Tr}(a_i a_j))_{1 \leqslant i, j \leqslant n}.$$

Этот определитель лежит в k и в силу предложения 5 п.16.3.3 не равен нулю. Применяя к Δ и Δ^{-1} теорему 3 п.16.3.1, видим, что $|\Delta|_v = 1$ почти для всех v. С другой стороны, если u — произвольный элемент из A_v, то $\mathrm{Tr}(u)$ является следом отображения $x \to ux$ алгебры A_v. Записав $u \cdot u_{v,i} = \sum d_{ij} u_{v,j}$, где $d_{ij} \in k_v$ и $1 \leqslant i, j \leqslant n$, получим $\mathrm{Tr}(u) = \sum d_{ii}$. Так как ρ_v — кольцо, то при $u \in \rho_v$ все d_{ij} находятся в r_v. Это показывает, что Tr переводит ρ_v в r_v. Следовательно, если мы обозначим через N_v матрицу $(\mathrm{Tr}(u_{v,i} u_{v,j}))$, то N_v принадлежит $M_n(r_v)$. Подставляя в матрицу M вместо a_i выражение

$\sum c_{v,ij}u_{v,j}$, получаем $M = C_v N_v {}^t C_v$, откуда $\Delta = \det(N_v)\ \overline{\det}(C_v)^{\alpha}$. Здесь N_v лежит в $M_n(r_n)$, равно как и C_v при $v \notin P$, и почти для всех v $|\Delta|_v = 1$. Отсюда, очевидно, следует, что $|\det(C_v)|_v = 1$ почти для всех v, что и требовалось доказать.

Далее будет показано, что теорема 4 остается справедливой, даже если поле k' не предполагается сепарабельным над k.

Следствие 1. *В предположениях и обозначениях теоремы* 4 *сумма степеней над* k_v *пополнений* k'_i *поля* k' *в точках, лежащих над* v, *равна степени* n *поля* k' *над* k.

В самом деле, эта сумма равна размерности B_v над k_v, а размерность A_v над k_v есть n.

Следствие 2. *Пусть* k *— алгебраическое расширение степени* n *поля* $\mathbf{Q}$. *Обозначим через* r_1 *число его вещественных точек и через* r_2 *— число мнимых. Тогда* $r_1 + 2r_2 = n$.

Для доказательства достаточно в следствии 1 заменить k, k', v на $\mathbf{Q}$, k, ∞.

Следствие 3. *В обозначениях и предположениях теоремы* 4 *продолжения* $\mathrm{Tr}_{k'/k}$ *и* $\mathrm{N}_{k'/k}$ *на* A_v *задаются формулами*

$$\mathrm{Tr}_{k'/k}(x) = \sum_i \mathrm{Tr}_{k'_i/k_v}(\mu_i(x)), \quad \mathrm{N}_{k'/k}(x) = \prod_i \mathrm{N}_{k'_i/k_v}(\mu_i(x)).$$

Это следует из предложения 4 п.16.3.3, примененного к ситуации, описываемой теоремой 4.

Следствие 4. В *предположениях и обозначениях теоремы* 4 *допустим еще, что* k' *есть расширение Галуа поля* k *с группой Галуа* G. *Пусть* w *— одна из точек* w_i *поля* k'. *Тогда пополнение* k'_w *поля* k' *в точке* w *будет расширением Галуа над* k_v; *ограничение на* k' *группы Галуа* H *поля* k'_w *над* k_v *определяет изоморфизм этой группы на подгруппу в* G, *состоящую из автоморфизмов, оставляющих точку* w *на месте. Точки* w_i *суть образы точки* w *относительно* G, *и все поля* k'_i *изоморфны полю* k'_w.

Пусть λ — такое изоморфное вложение поля k' в локальное поле K, что $\lambda(k')$ плотно в K. Это вложение задает по определению точку поля k', и ее образ относительно автоморфизма σ поля k' можно рассматривать как точку, определенную вложением $\lambda \circ \sigma$. Применяя следствие 2 предл. 3 п.16.3.2 к естественному вложению поля k' в k'_w и учитывая теорему 4, получаем наше утверждение.

16.4. Адели

16.4.1. Адели А-полей

Повсюду в этой главе через k будет обозначаться некоторое **A**-поле. Если v — точка поля k, то через k_v будет обозначаться пополнение поля k относительно v. Если v — конечная точка поля k, то мы обозначаем через r_v максимальное компактное подкольцо в k_v и через p_v максимальный идеал в r_v; эти подмножества в k_v определяются соответственно условиям $|x|_v \leqslant 1$ и $|x|_v < 1$. Мы обозначаем далее через P_∞ множество всех бесконечных точек поля k и через P — любое конечное множество точек поля k, содержащее P_∞. Для любого такого множества P положим

$$k_{\mathbf{A}}(P) = \prod_{v \in P} k_v \times \prod_{v \notin P} r_v, \tag{1}$$

где второе произведение берется по всем точкам поля k, не лежащим в P. Наделенное обычной топологией произведения множество $k_{\mathbf{A}}(P)$ локально компактно, потому что k_0 таковы, а r_v компактны. Наделим $k_A(P)$ структурой кольца, определив сложение и умножение покомпонентно. Ясно, что тем самым мы превратим $k_A(P)$ в топологическое кольцо. Рассматриваемое лишь как множество, $k_A(P)$ можно было бы определить как подмножество в произведении $\prod k_v$, состоящее из тех элементов $x = (x_v)$ этого произведения, для которых $|x_v|_v \leq 1$ при всех v, не лежащих в P. Если P' — другое конечное множество точек поля k и $P' \supset P$, то кольцо $k_A(P)$ содержится в $k_{\mathbf{A}}(P')$, причем его топология и кольцевая структура индуцируются топологией и кольцевой структурой на $k_A(P')$ и $k_A(P)$ является открытым подмножеством в $k_A(P')$.

Теперь мы определим локально компактное топологическое кольцо k_A — так называемое кольцо аделей поля k. Как множество оно есть объединение всех множеств $k_A(P)$; другими словами, оно состоит из элементов $x = (x_v)$ произведения $\prod k_v$, которые при почти всех v удовлетворяют условию $|x_v|_v \leqslant 1$. Определим структуру топологического кольца на k_A условием, что всякое кольцо $k_A(P)$ является открытым подкольцом в k_A. Это означает, во-первых, что если $x = (x_v)$ и $y = (y_v)$ лежат в k_A, то $x + y = (x_v + y_v)$ и $xy = (x_v y_v)$; ясно, что при этом и сумма, и произведение действительно лежат в k_A. Во-вторых, мы получим фундаментальную систему окрестностей нуля в аддитивной группе кольца k_A, взяв такую систему в любом из колец $k_A(P)$, например в $k_{\mathbf{A}}(P_\infty)$, которое является наименьшим среди колец

k_A *(P).* Эквивалентным образом мы получим такую систему, взяв все множества вида $\prod U_v$, где U_v — окрестность нуля в k_0 для всех v и $U_v = r_v$ почти для всех v.

Определение 1. *Под кольцом k_A аделей A-поля k мы понимаем объединение множеств k_A (P), определенных формулой* (1), *где в качестве P берутся все конечные множества точек поля k, содержащие множество всех бесконечных точек. Структура топологического кольца на k_A определяется условием, что всякое k_A (P) является открытым подкольцом в k_A.*

Элементы кольца k_A будут называться ***аделями*** поля k. Возьмем точку v поля k. В случае когда P содержит v, кольцо k_A *(P)* можно записать как произведение поля k_v и некоторого бесконечного произведения. Обозначая последнее через $k'_A(P, v)$, мы можем проделать с произведениями $k'_A(P, v)$ то же самое, что мы делали с произведениями k_A *(P),* беря теперь в качестве P все конечные множества точек поля k, содержащие P_∞ и v. Объединение всех k'_A *(P, v)* будет тогда локально компактным кольцом k'_A *(v),* и k_A, очевидно, изоморфно произведению $k_v \times k'_A(v)$. При этом изоморфизме первый сомножитель k_v последнего произведения, очевидно, отображается на множество тех аделей $x = (x_v)$, для которых $x_w = 0$ для всех точек $w \neq v$. Это множество будет называться *квазисомножителем* в k_A, соответствующим v, и будет всегда отождествляться с k_v. Отображение $(x_v) \to x_v$ из k_A на k_v, соответствующее проекции из произведения $k_v \times k'_A(v)$ на первый сомножитель, будет называться *проекцией* из k_A на квазисомножитель k_v; очевидно, эта проекция непрерывна. Ясно также, что вместо одной точки v поля k можно было начать с любого конечного множества P_0 таких точек и прийти к записи k_A в виде произведения полей k_v по $v \in P_0$ и еще одного сомножителя.

Возьмем любой характер χ аддитивной группы кольца k_A. Для каждого P он индуцирует на k_A *(P)* некоторый характер χ_P и для каждого v некоторый характер χ_v на квазисомножителе k_v. Хорошо известно, что характер на бесконечном произведении компактных групп должен индуцировать тривиальный характер 1 на почти всех сомножителях. Применяя это к характеру, индуцированному характером χ_P на произведении $\prod r_v$ в (1), мы видим, что χ_v тривиален на r_v почти для всех v. Тогда для всех $x = (x_v)$ из k_A имеем

$$\chi(x) = \prod_v \chi_v(x_v). \tag{2}$$

Произведение здесь берется по всем точкам v поля k; для всякого $x = (x_v)$ из k_A почти все сомножители равны 1.

Пусть ξ — элемент из k. Положив $x_v = \xi$ при всех v, мы определим в силу теоремы 3 п. 16.3.1 некоторый адель $x = (x_v)$. Обозначим его через $\varphi(\xi)$ и назовем φ *каноническим вложением* поля k в k_A. Часто мы будем, если это не может привести к путанице, отождествлять k с его образом в k_A при вложении φ.

Пусть E — конечномерное векторное пространство размерности n над k. Для всякой точки v поля k будем писать $E_v = E \otimes_k k_v$. Как обычно, мы считаем E «естественно» вложенным в E_v посредством инъективного отображения $e \to e \otimes 1_{k_v}$. С другой стороны, поскольку k вложено в k_A определенным выше каноническим вложением φ, то мы можем рассмотреть тензорное произведение $E_A = E \otimes_k k_A$ и считать E «естественно» вложенным в него посредством отображения $e \to e \otimes \varphi(1)$. Определим топологию на E_A как самую грубую, в которой k_A -линейные продолжения на E_A линейных форм на E непрерывны. Эквивалентное определение: возьмем какой-нибудь базис ε в E над k; он определяет изоморфизм k^n на E, а следовательно, изоморфизм $(k_A)^n$ на E_A; топология на E_A получается перенесением на E_A посредством этого изоморфизма топологии с $(k_A)^n$; легко проверяется непосредственно, что она не зависит от выбора ε.

Пусть E и E' — конечномерные векторные пространства над k и f — полиномиальное отображение из E в E'. Тогда f можно очевидным образом продолжить до отображения из E_A в E'_A, а именно, это отображение определяется теми же самыми многочленами, если E, E' отождествлены с пространствами k^n, k^m, а следовательно, E_A, E'_A с $(k_A)^n$, $(k_A)^m$ при каком-либо выборе базисов в E, E' над k. Это продолжение отображения f будет обозначаться опять через f. Ясно, что оно непрерывно, поскольку сложение и умножение на k_A непрерывны.

Предложение 1. *Пусть E — векторное пространство конечной размерности n над k, и пусть ε — конечное подмножества в E, содержащее базис векторного пространства E над k. Для всякой конечной точки v поля k обозначим через ε_v r_v-модуль, порожденный подмножеством ε в E_v. Для всякого конечного множества P точек поля k, содержащего P_∞, запишем*

$$E_A(P, \varepsilon) = \prod_{v \in P} E_v \times \prod_{v \notin P} \varepsilon_v.$$

Тогда все $E_A(P, \varepsilon)$ являются открытыми подгруппами в E_A и E_A есть объединение этих подгрупп.

Это следует понимать в том смысле, что всякое произведение $E_A(P, \varepsilon)$ наделено своей топологией произведения и что последняя совпадает с топологией, индуцированной топологией пространства E_A. Ясно, что ε_v является k_v-решеткой в E_v и, следовательно, открытым и

компактным подножеством в E_v для всякой конечной точки v. Поэтому $E_{\mathbf{A}}(P, \varepsilon)$— открытая подгруппа в $E_{\mathbf{A}}(P', \varepsilon)$, если $P \subset P'$. Возьмем какой-нибудь базис ε' в E над k и с его помощью определим изоморфизм k^n на E и, следовательно, $(k_{\mathbf{A}})^n$ на E_A. Из наших определений видно, что E_A является объединением множеств $E_{\mathbf{A}}(P, \varepsilon')$ и что эти множества открыты в E_A. По следствию 1 из теор. 3 п.16.3.1 существует такое конечное множество P_0 точек поля k, содержащее P_∞, что $\varepsilon_v = \varepsilon'_v$ для v, не лежащих в P_0. Отсюда видно что E_A является объединением множеств $E_{\mathbf{A}}(P, \varepsilon)$, а также что при $P' \supset P \cup P_0$, множество $E_{\mathbf{A}}(P, \varepsilon)$ открыто в E_A (P', ε'), а следовательно, в E_A. Можно было бы использовать предложение 1 для непосредственного определения топологии на E_A, в точности так же, как выше была определена топология на k_A; тогда из следствия 1 теор. 3 п. 16.3.1 вытекала бы независимость этой топологии от выбора ε.

Следствие 1. *В предположениях и обозначениях предложения* 1 *пусть C — компактное подмножество в E_A. Тогда существует такое конечное множество P точек поля k, что* $C \subset E_{\mathbf{A}}(P, \varepsilon)$.

Так как C содержится в объединении открытых множеств $E_{\mathbf{A}}(P, \varepsilon)$, то оно должно содержаться в объединении конечного числа таких множеств $E_{\mathbf{A}}(P_i, \varepsilon)$, а следовательно, в $E_{\mathbf{A}}(P, \varepsilon)$ при $P = \bigcup P_i$.

Пусть $\mathcal{A}$ — любая алгебра конечной размерности над k. Мы будем обозначать через $\mathcal{A}_{\mathbf{A}}$ топологическое кольцо, полученное продолжением на пространство $\mathcal{A}_{\mathbf{A}}$ указанным выше способом закона умножения на $\mathcal{A}$. Ясно, что можно рассматривать $\mathcal{A}_{\mathbf{A}}$ как алгебру над k_A, и $k_{\mathbf{A}} \cdot 1_{\mathbf{A}}$ является замкнутым подпространством и подкольцом в $\mathcal{A}_{\mathbf{A}}$, изоморфным $k_{\mathbf{A}}$.

Следствие 2. *Пусть $\mathcal{A}$ — алгебра конечной размерности над k и α — конечное подмножество в $\mathcal{A}$, содержащее базис векторного пространства $\mathcal{A}$ над k. Для всякой конечной точки v поля k обозначим через α_v r_v-модуль, порожденный подмножеством a в $\mathcal{A}_v$. Для всякого конечного множества P точек поля k, содержащего P_∞, запишем*

$$\mathcal{A}_{\mathbf{A}}(P, \alpha) = \prod_{v \in P} \mathcal{A}_v \times \prod_{v \notin P} \alpha_v.$$

Тогда существует множество P_0, обладающее тем свойством, что $\mathcal{A}_{\mathbf{A}}(P, \alpha)$ является открытым подкольцом в A_A для любого $P \supset P_0$, и $\mathcal{A}_{\mathbf{A}}$ есть объединение этих подколец.

Это вытекает из следствия 2 теор. 3 п.16.3.1 и из предложения 1.

Возьмем теперь алгебраическое расширение k' поля k конечной степени. Так как k' является **A**-полем, то мы можем применить к нему общую конструкцию и получить таким образом кольцо k'_A его аделей.

С другой стороны, мы можем считать k' алгеброй над k и применить к этой алгебре описанную выше конструкцию, что дает кольцо, которое мы обозначим через $(k'/k)_{\mathbf{A}}$. Как мы видели, это — алгебра над k_A; она содержит замкнутое подкольцо $k_{\mathbf{A}} \cdot 1_{k'}$, которое мы очевидным образом отождествим с k_A. Центральным в теории аделей является тот факт, что определенные таким образом кольца k'_A и $(k'/k)_{\mathbf{A}}$ канонически изоморфны. Это будет доказано сейчас, но лишь для случая, когда k' сепарабельно над k. Несепарабельный случай будет разобран дальше.

Теорема 1. *Пусть k — некоторое* **A***-поле и k' — его сепарабельное алгебраическое расширение конечной степени над k. Тогда существует единственный изоморфизм* Ф *из* $(k'/k)_{\mathbf{A}}$ *на* k'_A *со следующими свойствами:* (i) Ф *индуцирует тождественное отображение на k', если k' естественно вложено как в* $(k'/k)_{\mathbf{A}}$, *так и в* k'_A; (ii) *на всяком квазисомножителе* $(k'/k)_v$ *в* $(k'/k)_{\mathbf{A}}$ *изоморфизм* Ф *индуцирует k_v-линейный изоморфизм Φ_v алгебры* $(k'/k)_v$ *на произведение квазисомножителей* k'_w *в* $k'_{\mathbf{A}}$, *соответствующих точкам w поля k', лежащим над v.*

Обозначим через $\mathcal{A}$ алгебру k'/k, т. е. поле k', рассматриваемое как алгебра над k. Тогда в объясненных выше обозначениях $\mathcal{A}_{\mathbf{A}}$ совпадает с $(k'/k)_{\mathbf{A}}$, а $\mathcal{A}_v$ совпадает с $(k'/k)_v$, т. е. с алгеброй $k' \otimes_k k_v$ над k_v, которой мы занимались в п. 16.4. Для конечного числа слагаемых прямая сумма означает то же самое, что произведение. Поэтому мы можем интерпретировать теорему 4 п. 16.4 как определяющую изоморфизм Φ_v из $(k'/k)_v$ на произведение $\prod k'_w$ полей k'_w по всем точкам w, лежащим над v. Этот изоморфизм k_v-линеен и отображает каждый элемент $\xi \in k'$ на элемент $(\xi, \ldots, \xi)$ в $\prod k'_w$; он однозначно характеризуется этими свойствами. Аналогичным образом если мы выберем какой-нибудь базис α в k' над k, то та же самая теорема показывает, что почти для всех v изоморфизм Φ_v отображает α_v на произведение $\prod r'_w$ максимальных компактных подколец в полях k'_w. Пусть P_0 — такое содержащее P_∞ конечное множество точек поля k, что Φ_v обладает этим свойством для всех v, не лежащих в P_0. Для всякой точки w поля k' обозначим через $f(w)$ точку поля k, лежащую под v. Тогда при $P \supset P_0$ отображения Φ_v очевидным образом определяют изоморфизм Φ_P из $\mathcal{A}_{\mathbf{A}}(P, \alpha)$ на $k'_{\mathbf{A}}(f^{-1}(P))$, где $\mathcal{A}_{\mathbf{A}}(P, \alpha)$ — открытое подкольцо в $\mathcal{A}_{\mathbf{A}} = (k'/k)_{\mathbf{A}}$, определенное в следствии 2 предл. 1. Так как каждое множество $f^{-1}(P)$ конечно и каждое конечное множество P' точек поля k' содержится в $f^{-1}(P)$ при $P = f(P')$, то k'_A является объединением множеств $k'_{\mathbf{A}}(f^{-1}(P))$ при $P \supset P_0$. Поскольку Φ_{P_1} совпадает с Φ_P на

области определения Φ_P при $P_1 \supset P$, то существует изоморфизм Ф из $\mathcal{A}_{\mathbf{A}}$ на k'_A, который совпадает с Φ_P на его области определения для любого $P \supset P_0$. Теперь ясно, что Ф обладает свойствами, сформулированными в нашей теореме, и что он однозначно характеризуется этими свойствами.

Следствие 1. *В предположениях и обозначениях теоремы* 1 *для каждой точки w поля k' обозначим, через f (w) точку поля k, лежащую под w. Тогда если* $x = (x_v) \in k_{\mathbf{A}}$, *то* Ф *(x) есть такой элемент* $y = (y_w)$ *в* k'_A, *что* $y_w = x_{f(w)}$ *для каждой точки w поля k'.*

Это следует из того факта, что Ф (1) = 1, и из k_v-линейности Φ_v для каждой точки *v*.

Начиная с этого места, k_A будет обычно отождествляться со своим образом в k'_A при изоморфизме, индуцированном на k_A описанным в следствии 1 изоморфизмом Ф. Ясно, что k_A будет при этом замкнутым подкольцом в k'_A.

Следствие 2. *Пусть k и k' таковы, как в теореме* 1, *и пусть* E/k' — *векторное пространство конечной размерности над k'. Обозначим через* E/k *то же пространство, рассматриваемое как векторное пространство над k. Тогда тождественное отображение из* E/k *на* E/k' *может быть однозначно продолжено до* k_A *-линейного отображения из* $(E/k)_{\mathbf{A}}$ *в* $(E/k')_{\mathbf{A}}$, *и это продолжение является изоморфизмом из* $(E/k)_{\mathbf{A}}$ *на* $(E/k')_{\mathbf{A}}$.

Для $E = k'$ — это, ввиду следствия 1, простая переформулировка теоремы 1. Отсюда следует справедливость утверждения для случая $E = k'^n$, а следовательно, и для общего случая, потому что *E* можно всегда отождествить с пространством k'^n, выбрав некоторый базис.

В соответствии с данными выше определениями *k* -линейная форма $\mathrm{Tr}_{k'/k}$ и полиномиальная функция $\mathrm{N}_{k'/k}$ на пространстве *k'*, рассматриваемом как векторное пространство над *k*, могут быть продолжены до отображений $\mathrm{Tr}_{k'/k}$, $\mathrm{N}_{k'/k}$ из $(k'/k)_{\mathbf{A}}$ в k_A. При этом $\mathrm{Tr}_{k'/k} \circ \Phi^{-1}$ и $\mathrm{N}_{k'/k} \circ \Phi^{-1}$ суть отображения из k'_A в k_A. Упростим формулировку нашего очередного следствия, отождествив $(k'/k)_{\mathbf{A}}$ с $k'x$ посредством изоморфизма Ф, так что последние наши два отображения можно записать просто как $\mathrm{Tr}_{k'/k}$ и $\mathrm{N}_{k'/k}$.

Следствие 3. *Пусть* $x'=(x'_w)$ — *любой элемент из* k'_A. *Положим* $y = \mathrm{Tr}_{k'/k}(x')$ *и* $z = \mathrm{N}_{k'/k}(x')$. *Тогда y, z являются элементами* (y_0), (z_0) *из* k_A, *задаваемыми соответственно равенствами*

$$y_v = \sum_{w \mid v} \mathrm{Tr}_{k'_w/k_v}(x'_w), \quad z_v = \prod_{w \mid v} \mathrm{N}_{k'_w/k_v}(x'_w)$$

для каждой точки v поля k, где сумма и произведение берутся по всем точкам w поля k', лежащим над v.

16.4.2. Основные теоремы

Ввиду леммы 1 п. 16.3.2 каждое **A**-поле является сепарабельным алгебраическим расширением одного из полей **Q** или $\mathbf{F}_p$ *(T).* Теорема 1 п. 16.4.1 дает нам возможность доказывать свойства адельных пространств, отправляясь от частных случаев $k = \mathbf{Q}$ и $k = \mathbf{F}_p$ (*T*). Этот метод принесет ряд важных результатов, для формулировки которых мы упростим обозначения, отождествив **A**-поля и векторные пространства над такими полями при помощи объясненного в п. 16.4.1 способа с их естественными образами в соответствующих адельных пространствах. В доказательствах мы снова используем φ для обозначения канонического вложения **A**-поля k в k_A.

Теорема 2. *Пусть k — некоторое* **A***-поле и E — конечномерное векторное пространство над k. Тогда E дискретно в* E_A *и факторпространство* E_A/E *компактно.*

Ввиду следствия 2 теор. 1 п. 16.4.1 и леммы 1 п. 16.3.2 достаточно доказать это для $k = \mathbf{Q}$ и $k = \mathbf{F}_p$ *(T).* Если n — размерность пространства E, то E изоморфно k^n, так что если теорема доказана в случае $E = k$, то она справедлива и в общем случае. Таким образом, нам нужно разобрать только случаи $E = k = \mathbf{Q}$ и $E = k = \mathbf{F}_P(T)$. Начнем с **Q**.

Для всякого простого числа p обозначим через $\mathbf{Q}^{(p)}$ множество таких ξ из **Q**, что $|\xi|_{p'} \leqslant 1$ для всех простых p', отличных от p. Ясно, что это — подкольцо в **Q**, состоящее из чисел вида $p^{-n}a$, где $n \in \mathbf{N}$ и $a \in \mathbf{Z}$.

Лемма 1. *Для каждого простого числа p имеем* $\mathbf{Q}_p = \mathbf{Q}^{(p)} + \mathbf{Z}_p$ *и* $\mathbf{Q}^{(p)} \cap \mathbf{Z}_p = \mathbf{Z}$.

Первое утверждение вытекает из следствия 2 теор. 6 п. 16.1.4, примененного к $\mathbf{Q}_p$, простому элементу p и множеству представителей $\{0, 1, \ldots, p-1\}$. Второе очевидно.

Лемма 2. *Положим* $A_\infty = \mathbf{R} \times \prod \mathbf{Z}_p$ *и обозначим через* φ *каноническое вложение поля* **Q** *в* $\mathbf{Q}_A$. *Тогда* $\mathbf{Q}_\mathbf{A} = \varphi(\mathbf{Q}) + A_\infty$ *и* $\varphi(\mathbf{Q}) \cap A_\infty = \varphi(\mathbf{Z})$.

Имеем $A_\infty = \mathbf{Q}_\mathbf{A}(\{\infty\})$, где использовано обозначение (1) п. 16.4.1. Поэтому A_∞ является открытым подкольцом в $\mathbf{Q}_\mathbf{A}$. Второе утверждение леммы очевидно. Возьмем теперь любой элемент $x=(x_v)$ из $\mathbf{Q}_\mathbf{A}$. Обозначим через P множество таких простых p, что x_p не лежит в $\mathbf{Z}_p$; это множество конечно. Первая часть леммы 1 показывает, что для всякого $p \in P$ мы можем записать $x_p = \xi_p + x'_p$, где $\xi_p \in \mathbf{Q}^{(p)}$ и $x'_p \in \mathbf{Z}_p$. Для $p \notin P$ положим $\xi_p = 0$ и $x'_p = x_p$. Положим, далее, $\xi = \sum \xi_p$, где сумма берется по всем p, и $y = x - \varphi(\xi)$. Если

$y = (y_v)$, то для каждого простого числа p имеем

$$y_p = x_p - \xi_p - \sum_{p' \neq p} \xi_{p'} = x'_p - \sum_{p' \neq p} \xi_{p'}.$$

По определению $\mathbf{Q}^{(p)}$ все члены в правой части лежат в $\mathbf{Z}_p$. Отсюда видно, что y лежит в A_∞, следовательно, x лежит в $\varphi(\mathbf{Q}) + A_\infty$.

Теперь мы можем доказать нашу теорему для случая $E - k = \mathbf{Q}$. Так как A_∞ открыто в $\mathbf{Q}_A$, то первое утверждение будет доказано, если показать, что множество $\varphi(\mathbf{Q}) \cap A_\infty$, т. е. $\varphi(\mathbf{Z})$ дискретно в A_∞. Но это очевидно, поскольку проекция множества $\varphi(\mathbf{Z})$ на сомножитель $\mathbf{R}$ произведения A_∞ равна $\mathbf{Z}$, а $\mathbf{Z}$ дискретно в $\mathbf{R}$. Обозначим теперь через I замкнутый интервал $[-1/2, 1/2]$ в $\mathbf{R}$ и положим $C = I \times \prod \mathbf{Z}_p$. Ясно, что $A_\infty = \varphi(\mathbf{Z}) + C$, откуда $\mathbf{Q}_A = \varphi(\mathbf{Q}) + C$. Поскольку C компактно, этим доказательство и заканчивается.

При $E = k = \mathbf{F}_p(T)$ доказательство аналогично и даже проще. Для всякой точки v поля k обозначим через $k^{(v)}$ множество таких элементов ξ из k, что $|\xi|_w \leqslant 1$ для всех точек w поля k, отличных от v.

Лемма 3. *Для каждой точки v поля k имеем* $k_v = k^{(v)} + r_v$ *и* $k^{(v)} \cap r_v = \mathbf{F}_p$.

Последнее утверждение очевидно ввиду определения функции $|\xi|_v$ на k, которое было дано в доказательстве теоремы 2 п. 16.3.1. Что касается первого утверждения, то достаточно рассмотреть точку, связанную с неприводимым многочленом π из $\mathbf{F}_p[T]$, поскольку в противном случае мы просто заменим T на T^{-1}. В этом случае наше утверждение вытекает из следствия 2 теор. 6 п. 16.1.4, примененного к k_v, к простому элементу π и к множеству представителей, которое дается следствием теор. 2 п. 16.3.1.

Лемма 4. *Положим* $A_0 = \prod r_v$. *Тогда* $k_A = \varphi(k) + A_0$ *и* $\varphi(k) \cap A_0 = \varphi(\mathbf{F}_p)$.

Имеем $A_0 = k_A(\varnothing)$, где опять используется обозначение (1) п. 16.4.1. Это — компактное открытое подкольцо в k_A. Последнее утверждение снова очевидно. Возьмем какое-нибудь $x = (x_v)$ из k_A. Лемма 3 показывает, что для каждой v, для которой $|x_v|_v > 1$, мы можем записать $x_v = \xi_v + x'_v$, где $\xi_v \in k^{(v)}$ и $x'_v \in r_v$. Для всех других точек v положим $\xi_v = 0$ и $x'_v = x_v$. Положим далее $\xi = \Sigma\, \xi_v$ и $y = x - \varphi(\xi)$. Точно так же, как в доказательстве леммы 2, получаем, что $y \in A_0$.

Наша теорема теперь очевидна для $E = k = \mathbf{F}_p(T)$, поскольку A_0 компактно и открыто в k_A и поле $\mathbf{F}_p$ конечно. Доказательство теоремы закончено.

Теперь мы рассмотрим векторное пространство E над **A**-полем k, алгебраически двойственное к нему пространство E' и соответствующие адельные пространства E_A, E'_A. Мы обозначаем через $[e, e']$ значение в точке $e \in E$ линейной формы, определяемой точкой $e' \in E'$, и используем то же самое обозначение для продолжения этой билинейной формы на $E_{\mathbf{A}} \times E'_{\mathbf{A}}$. Так как аддитивная группа пространства E_A является локально компактной коммутативной группой, то можно рассмотреть топологическую двойственную к ней группу, которую обозначим через E^*_A. Обозначим, далее, через $\langle e, e^* \rangle$ значение в точке $e \in E_{\mathbf{A}}$ характера, определяемого точкой $e^*_{\mathbf{A}} \in E^*$. В этих обозначениях справедлива

Теорема 3. *Пусть k — некоторое A-поле и χ — нетривиальный характер на k_A, тривиальный на k. Пусть E — конечномерное векторное пространство над k, E' — алгебраическое двойственное к нему, а E^*_A — топологическое двойственное к E_A. Тогда формула*

$$\langle e, e^* \rangle = \chi([e, e']) \text{ для всех } e \in E_{\mathbf{A}} \quad (e' \in E'_{\mathbf{A}},\ e^* \in E^*_{\mathbf{A}})$$

определяет изоморфизм $e' \to e^*$ из $E'_{\mathbf{A}}$ на $E^*_{\mathbf{A}}$. Кроме того, если e' таков, что $\chi([e, e']) = 1$ при всех $e \in E$, то $e' \in E'$.

Последнее утверждение означает, что определенный в нашей теореме изоморфизм $e' \to e^*$ из E_A на E^*_A отображает E' на подгруппу в E^*_A, ассоциированную по двойственности с дискретной подгруппой E в E_A.

Мы начнем с рассмотрения случая $E = k = \mathbf{Q}$. Используем снова те же обозначения, что и в первой части доказательства теоремы 2. Ввиду леммы 2 каждый характер на A_∞, тривиальный на $\varphi(\mathbf{Z})$, можно однозначно продолжить до характера на $\mathbf{Q}_A$, тривиального на $\varphi(\mathbf{Q})$. Мы получим такой характер χ, положив $\chi(x) = \mathbf{e}(-x_\infty)$ при $x = (x_v) \in A_\infty$ (напомним, что мы пишем $\mathbf{e}(t) = e^{2\pi i t}$ при $t \in \mathbf{R}$). Если мы продолжим этот характер до характера χ на $\mathbf{Q}_A$, тривиального на $\varphi(\mathbf{Q})$, и для каждой точки v поля $\mathbf{Q}$ обозначим через χ_v характер на квазисомножителе $\mathbf{Q}_v$ в $\mathbf{Q}_A$, индуцированный характером χ, то χ, очевидно, характеризуется следующими свойствами: этот характер тривиален на $\varphi(\mathbf{Q})$; характер χ_p тривиален на $\mathbf{Z}_p$ для каждого простого числа p и $\chi_\infty(x) = \mathbf{e}(-x)$ при $x \in \mathbf{R}$. Для вычисления χ_p рассмотрим снова группу $\mathbf{Q}^{(p)}$, определенную при доказательстве теоремы 2, и возьмем любое число $\xi \in \mathbf{Q}^{(p)}$. Тогда $\xi \in \mathbf{Z}_{p'}$ для всех простых $p' \neq p$, так что по формуле 2 п.16.4.1 имеем

$$1 = \chi(\varphi(\xi)) = \chi_\infty(\xi)\, \chi_p(\xi) = \mathbf{e}(-\xi)\, \chi_p(\xi)$$

и потому $\chi_p(\xi) = \mathbf{e}(\xi)$. По лемме 1 характер χ_p вполне определяется этим свойством и тем фактом, что он тривиален на $\mathbf{Z}_p$. Его ядро совпадает с $\mathbf{Z}_p$. Поэтому этот характер имеет порядок 0 в смысле определения 4 п.16.2.5.

Пусть теперь χ' — любой характер на $\mathbf{Q}_A$. Для каждой точки v поля $\mathbf{Q}$ обозначим через χ'_v характер, индуцированный на квазисомножителе $\mathbf{Q}_v$ в $\mathbf{Q}_A$ характером χ'. По следствию теор. 3 п.16.2.5 можно однозначно записать χ'_v в виде $\chi'_v(x) = \chi_v(a_v x)$, где $a_v \in \mathbf{Q}_v$. Как мы отмечали, когда писали формулу (2) п.16.4.1, характер χ'_p должен быть тривиальным на $\mathbf{Z}_p$ почти для всех p, поскольку характер χ' непрерывен на $\mathbf{Q}_A$. Отсюда следует, что $\chi_p(a_p) = 1$ и, следовательно, $a_p \in \mathbf{Z}_p$ почти для всех p. Поэтому $a = (a_v)$ лежит в $\mathbf{Q}_A$, так что по формуле (2) п.16.4.1 χ' совпадает с характером χ_a на $\mathbf{Q}_A$, задаваемым равенством $\chi_a(x) = \chi(ax)$ при всех $x \in \mathbf{Q}_A$. Таким образом, мы показали, что отображение $a \to \chi_a$ из $\mathbf{Q}_A$ в пространство $G = \mathbf{Q}_A^*$ (топологическое двойственное к $\mathbf{Q}_A$) сюръективно. Сразу видно, что оно непрерывно и инъективно, так что оно является биективным морфизмом из $\mathbf{Q}_A$ на его двойственное пространство G. Обозначим через Г подгруппу в G, ассоциированную по двойственности с $\varphi(\mathbf{Q})$, т. е. состоящую из характеров на $\mathbf{Q}_A$, тривиальных на $\varphi(\mathbf{Q})$. Поскольку характер χ обладает последним свойством, то это же верно для χ_a при всех $a \in \varphi(\mathbf{Q})$, так что $a \to \chi_a$ отображает $\varphi(\mathbf{Q})$ в Г. Обратно, пусть b таков, что $\chi_b \in \Gamma$. Как и в доказательстве теоремы 2 для $\mathbf{Q}$, положим $C = I \times \prod \mathbf{Z}_p$, где $I = [-1/2, 1/2]$. Мы показали там, что $\mathbf{Q}_A = \varphi(\mathbf{Q}) + C$. Поэтому можно записать b в виде $b = \varphi(\xi) + c$, где $c \in C$, $\xi \in \mathbf{Q}$, и, значит, $\chi_c \in \Gamma$. Записав $c = (c_v)$ и используя тот факт, что $c_p \in \mathbf{Z}_p$ при всех p, имеем

$$1 = \chi_c(\varphi(1)) = \chi(c) = \chi_\infty(c_\infty) = \mathbf{e}(-c_\infty),$$

откуда $c_\infty = 0$, ибо $c_\infty \in I$. Поэтому характер χ_c тривиален на $A_\infty = \mathbf{R} \times \prod \mathbf{Z}_p$. Так как он тривиален и на $\varphi(\mathbf{Q})$, то лемма 2 показывает, что он тривиален на $\mathbf{Q}_A$, так что $c=0$, откуда $b \in \varphi(\mathbf{Q})$. Поэтому $a \to \chi_a$ отображает $\varphi(\mathbf{Q})$ на Г. Наконец, поскольку подгруппа $\varphi(\mathbf{Q})$ дискретна в $\mathbf{Q}_A$ и $\mathbf{Q}_A/\varphi(\mathbf{Q})$ компактна, из теории двойственности следует, что Г дискретна в G и что G/Γ компактна. Следовательно, $a \to \chi_a$ определяет биективный морфизм компактной группы $\mathbf{Q}_A/\varphi(\mathbf{Q})$ на компактную группу G/Γ. Хорошо известно, что такой морфизм обязан быть изоморфизмом. Так как G «локально изоморфна» с G/Γ, а $\mathbf{Q}_A$ с $\mathbf{Q}_A/\varphi(\mathbf{Q})$, отсюда следует, что отображение $a \to \chi_a$ непрерывно в обе стороны, так что оно является

изоморфизмом. Этим заканчивается наше доказательство для $E = k = \mathbf{Q}$.

Возьмем теперь $E = k = \mathbf{F}_p(T)$. По аналогии со случаем $k = \mathbf{Q}$ обозначим через ∞ точку поля k, для которой T^{-1} является простым элементом (хотя это, разумеется, не бесконечная точка). Имеем $|T^{-1}|_\infty = p^{-1}$. Мы можем теперь применить к k_∞, к простому элементу T^{-1} и к множеству представителей $\mathbf{F}_p$ следствие 2 теор. 6 п. 16.1.4 и, согласно этому следствию, отождествить k_∞, с полем формальных степенных рядов

$$x = \sum_{i=n}^{+\infty} a_i T^{-i}, \tag{3}$$

где $n \in \mathbf{Z}$ и $a_i \in \mathbf{F}_p$ при всех $i \geq n$. Обозначим через ψ характер аддитивной группы поля $\mathbf{F}_q$, для которого $\psi(1) = e(1/p)$. Определим характер χ_∞ на k_∞, положив $\chi_\infty(x) = \psi(-a_1)$, где x задается формулой (3); при $x \in \mathbf{F}_p(T)$ имеем $a_1 = 0$, откуда $\chi_\infty(x) = 1$. Положим теперь $A_\infty = k_\infty \times \prod r_v$, где произведение берется по всем точкам v поля k, отличным от ∞. Используя обозначение (1) п.16.4.1, получаем $A_\infty = k_A(\{\infty\})$. Это — открытое подкольцо в k_A, содержащее множество A_0, определенное в лемме 4, так что по этой лемме $k_A = \varphi(k) + A_\infty$. Если $\xi \in k$, то $\varphi(\xi)$ лежит в A_∞, в том и только в том случае, когда $|\xi|_v \leqslant 1$ для всех точек v поля k, связанных с неприводимыми многочленами из $\mathbf{F}_p(T)$, т. е. в том и только в том случае, когда ξ лежит в $\mathbf{F}_p(T)$. Это означает, что $\varphi(k) \cap A_\infty = \varphi(\mathbf{F}_p[T])$. В соответствии с этим каждый характер на A_∞, тривиальный на $\varphi(\mathbf{F}_p[T])$, можно однозначно продолжить до характера на k_A, тривиального на $\varphi(k)$. Применяя это к характеру χ на A_∞, для которого $\chi(x) = \chi_\infty(x_\infty)$ при $x = (x_v) \in A_\infty$, получаем характер χ на k_A, который можно охарактеризовать следующими свойствами: χ тривиален на $\varphi(k)$; для каждой точки $v \neq \infty$ характер χ_v, индуцированный на k_v характером χ, тривиален на r_v; χ индуцирует на k_∞, характер χ_∞, определенный выше. Для вычисления характера χ_v, где точка v связана с неприводимым многочленом π; степени δ из $\mathbf{F}_p(T)$, обозначим через $k_0^{(v)}$ множество таких элементов ξ из k, что $|\xi|_w \leqslant 1$ для всех точек w поля k, отличных от v, и $|\xi|_\infty < 1$. Те же самые рассуждения, что и использовавшиеся в доказательстве леммы 3, показывают сейчас, что k_v разлагается в прямую сумму $k_0^{(v)}$ и r_v. Так как характер χ_v тривиален на r_v, он вполне определен своими значениями на $k_0^{(v)}$. Возьмем $\xi \in k_0^{(v)}$; этот элемент можно записать как $\xi = \pi^{-n}\alpha$, где $n \in \mathbf{N}$ и α — многочлен степени $< n\delta$ из $\mathbf{F}_p[T]$. Обозначим через a_1 коэффициент при $T^{n\delta-1}$ в α. Так как многочлен π

унитарен, то его можно записать в виде $T^{\delta}\omega$, где ω лежит в $\mathbf{F}_p\,[T^{-1}]$ и имеет свободный член, равный 1. Отсюда вытекает, что

$$\xi = \pi^{-n}\alpha = \omega^{-n}T^{-n\delta}\alpha \equiv a_1T^{-1} \quad (T^{-2})$$

в кольце r_∞, откуда $\chi_\infty(\xi) = \psi(-a_1)$ по определению χ_∞. По формуле (2) п.16.4.1 имеем

$$1 = \chi(\varphi(\xi)) = \chi_\infty(\xi)\,\chi_v(\xi) = \psi(-a_1)\,\chi_v(\xi),$$

поэтому $\chi_v(\xi) = \psi(a_1)$, чем завершается определение характера χ_v. Далее, если ξ таков, как выше, и отличен от нуля, то обозначим через d степень многочлена α и через a коэффициент при T^d в α. Тогда $\chi_v(\xi T^{n\delta-1-d})$ принимает значение $\psi(a)$, которое не равно 1, поскольку $a \neq 0$. Это показывает, что если ξ — ненулевой элемент в $k_0^{(v)}$, то $\chi_v(\xi t)$ не может равняться 1 при всех $t \in r_v$. Так как характер χ_v тривиален на r_v и так как $k_v = k_0^{(v)} + r_v$, то с учетом предложения 12 п.16.2.5 заключаем, что характер χ_v имеет порядок 0 в смысле определения 4 п.16.2.5. Другими словами, если элемент x из k_v таков, что $\chi_v(xt) = 1$ при всех $t \in r_v$, то x должен лежать в r_v.

Теперь мы можем продолжить доказательство точно так же, как в случае $k = \mathbf{Q}$. Пусть χ' — любой характер на k_A. Для всякой точки v поля k характер χ_v, индуцированный на k_v характером χ, можно записать в виде $\chi'_v(x) = \chi_v(a_v x)$, где $a_v \in k_v$. Из того факта, что характер χ'_v должен быть тривиален на r_v почти для всех v, вытекает, что элемент $a = (a_v)$ лежит в k_A, так что χ' совпадает с характером χ_a, определенным формулой $\chi_a(x) = \chi(ax)$. Как и прежде, мы видим, что отображение $a \to \chi_a$ является биективным морфизмом из k_A на группу $G = k_A^*$ (топологическую двойственную к k_A) и что этот морфизм отображает $\varphi(k)$ в подгруппу $\Gamma \subset G$, ассоциированную по двойственности с $\varphi(k)$. Предположим, что $\chi_b \in \Gamma$ при некотором $b \in k_A$. Согласно лемме 4 мы можем записать b в виде $b = \varphi(\xi) + c$, где $\xi \in k$, $c \in A_0$. Очевидно, χ_c тривиален на $\varphi(k)$. Положим $c = (c_v)$, так что $c_v \in r_v$ при всех v. Существует такой элемент $\gamma \in \mathbf{F}_p$, что $c_\infty \equiv \gamma\ (T^{-1})$. Заменяя ξ на $\xi + \gamma$ и c на $c - \varphi(\gamma)$, получаем, что $c_\infty \equiv 0\ (T^{-1})$. Далее имеем

$$1 = \chi_A(\varphi(1)) = \chi(c) = \chi_\infty(c_\infty),$$

откуда ввиду определения χ_∞ следует, что c_∞ лежит в $T^{-2}r_\infty$ и, значит, $\chi_\infty(c_\infty t) = 1$ при всех $t \in r_\infty$. Следовательно, характер χ_c тривиален на A_0, а потому и на k_A (лемма 4). Таким образом, $c = 0$ и, значит, $b \in \varphi(k)$. Заканчивается доказательство точно так же, как в случае $k = \mathbf{Q}$.

Теперь мы можем завершить доказательство нашей теоремы чисто формальным рассуждением. Обозначим через $T(E/k, \chi)$ утверждение теоремы 3. То, что мы уже доказали, можно выразить, сказав, что для каждого из полей $k = \mathbf{Q}$ и $k = \mathbf{F}_p(T)$ существует характер χ на k_A, для которого выполняется $T(k/k, \chi)$. Отсюда, очевидно, следует справедливость $T(k^n/k, \chi)$ для каждого n, так что $T(E/k, \chi)$ выполняется для каждого векторного пространства E над k. Возьмем, в частности, конечное алгебраическое расширение k' поля k. Как и в лемме 3 п. 16.3.3, обозначим через E пространство k', рассматриваемое как векторное пространство над k ; выберем k -линейную форму λ на E, отличную от 0, и отождествим E с алгебраическим двойственным к нему пространством E', полагая $[x, y] = \lambda(xy)$. Мы можем тогда продолжить λ до отображения из E_A в k_A и тем самым продолжить отождествление пространств E и E' до отождествления пространств E_A и E'_A. Поэтому мы имеем опять $[x, y] = \lambda(xy)$ при $x, y \in E_{\mathbf{A}} = (k'/k)_{\mathbf{A}}$. Положим $\chi' = \chi \circ \lambda$. Это, очевидно, нетривиальный характер на E_A, тривиальный на E. Предположим теперь, что k' сепарабельно над k. Тогда мы можем отождествить E_A с k'_A посредством изоморфизма Ф, описанного в теореме 1 п.16.4.1. При этом χ' перейдет в нетривиальный характер на k'_A, тривиальный на k', и утверждение $T(E/k, \chi)$ превращается в точности в утверждение $T(k'/k', \chi')$. Так как в качестве k' можно взять любое **A**-поле, взяв в качестве k или **Q**, или $\mathbf{F}_p$ (T), то мы убеждаемся, что для каждого **A**-поля k теорема 3 верна по меньшей мере при одном выборе характера χ. Предположим теперь, что $T(k/k, \chi)$ справедливо для всякого такого поля, и пусть χ_1 — еще один характер с указанными в теореме 3 свойствами. Из $T(k/k, \chi)$ следует, что χ_1 имеет вид $\chi_1(x)=\chi(ax)$, где $a \in k$ и $a \neq 0$. Тогда отображение $e' \to e^*$, определенное, как в теореме 3, но с помощью χ_1, является композицией аналогичного отображения, определенного с помощью χ, и отображения $e' \to ae'$ из E'_A в себя. Так как последнее отображение является, очевидно, автоморфизмом пространства E'_A, отображающим E' на себя, то мы видим, что $T(E/k, \chi)$ эквивалентно $T(E/k, \chi_1)$. Этим наше доказательство завершено.

Следствие 1. *Пусть характер χ такой, как в теореме* 3. *Обозначим для каждой точки v поля k через χ_v характер, индуцированный характером χ на квазисомножителе k_v в k. Тогда для каждой точки v характер χ_v нетривиален и почти для всех конечных точек v поля k характер χ_v имеет порядок* 0 *в смысле определения* 4 п. 16.2.5.

Для всякого $a \in k_{\mathbf{A}}$ обозначим через χ_a характер на k_A, определенный формулой $\chi_a(x) = \chi(ax)$. Если бы χ был тривиален на

квазисомножителе k_v, то этот квазисомножитель лежал бы в ядре морфизма $a \to \chi_a$ из k_A в топологическое двойственное к нему пространство. Поскольку по теореме 3 этот морфизм является изоморфизмом, это привело бы к противоречию. В частности, для каждой конечной точки v поля k мы можем положить $\mathbf{v}(v) = \mathrm{ord}(\chi_v)$ в смысле определения 4 п. 16.2.5. Для всякого отображения $v \to n(v)$ множества конечных точек поля k в $\mathbf{Z}$ обозначим через $G(n)$ группу тех элементов $x = (x_v)$ из k_A, для которых $\mathrm{ord}(x_v) \to n(v)$ для всех конечных точек v, и через $H(n)$ — подгруппу в $G(n)$, состоящую из таких элементов $x = (x_v)$ из $G(n)$, что $x_w = 0$ для всех бесконечных точек w поля k. В силу определения топологии на k_A очевидно, что группа $G(n)$ открыта в k_A тогда и только тогда, когда $n(v) \leqslant 0$ почти для всех v. Ясно также, что подгруппа $H(n)$ компактна, если $n(v) \geqslant 0$ почти для всех v. Обратно, по следствию 1 предл. 1 п. 16.4.1 каждое компактное подмножество в k_A содержится в одном из множеств $k_A(P)$ (мы применяем обозначение (1) п. 16.4.1), так что подгруппа $H(n)$ не может быть компактной, за исключением случая, когда $n(v) \geqslant 0$ почти для всех v. Поэтому это условие необходимо и достаточно для компактности $H(n)$. Теперь предложение 12 гл. п. 16.2.5 в сочетании с тем фактом, что характер χ_w нетривиален для любой бесконечной точки поля k, показывает, что множество тех элементов x из k_A, для которых $\chi(xy) = 1$ при всех $y \in G(0)$, совпадает с $H(-v)$ и что множество тех элементов x, для которых $\chi(xy) = 1$ при всех $y \in H(0)$, совпадает с $G(-v)$. Отождествляя k_A с топологическим двойственным к нему пространством посредством изоморфизма, описанного в теореме 3, мы видим, что $H(-v)$ и $G(-v)$ являются подгруппами в k_A, ассоциированными по двойственности с $G(0)$ и $H(0)$ соответственно. Так как группа $G(0)$ открыта, а $H(0)$ компактна, то из теории двойственности вытекает, что подгруппа $H(-v)$ должна быть компактной, а $G(-v)$ — открытой. Как мы уже видели, отсюда следует, что $-v(v) \geqslant 0$ почти для всех v и что почти $-v(v) \leqslant 0$ для всех v.

Следствие 2. *Пусть E — конечномерное векторное пространство над k, и пусть v — любая точка поля k. Тогда подгруппа $E + E_v$ всюду плотна в E_A.*

Если это справедливо для $E = k$, то, очевидно, верно и для $E = k^n$, а потому и для любого E. Если бы подгруппа $k + k_v$ не была плотна в k_A, то существовал бы нетривиальный характер на k_A, который был бы тривиален как на k, так и на k_v; но это противоречит следствию 1.

Как и в случае локальных полей, часто бывает удобно, выбрав раз и навсегда *базисный характер* χ со свойствами, описанными в теореме 3,

отождествлять для всех конечномерных векторных пространств E над k топологическое двойственное к E_A с пространством E'_A посредством изоморфизма из этой теоремы. Для каждого квазисомножителя k_v и k_A в качестве базисного характера будет при этом браться характер χ_v, индуцированный на k_v характером χ, и этот характер χ_v будет использоваться для отождествления топологических и алгебраических двойственных к векторным пространствам над k_v, как объяснялось в п.16. 2.5. Имея все это в виду, получаем

Следствие 3. *Пусть предположения и обозначения таковы, как в предложении* 1 п.16.4.1, *и пусть E — векторное пространство над k и E' — алгебраическое двойственное к нему. Пусть, далее, ε, ε' — конечные подмножества в E и в E' соответственно, содержащие базисы этих пространств над k. Для каждой точки v поля k отождествим E'_v с топологическим двойственным к E_v, как описано выше. Тогда почти для всех конечных точек v поля k k_v-решетка ε'_v двойственна к ε_v.*

Для $E = E' = k$ и $\varepsilon = \varepsilon' = \{1\}$ это просто переформулировка следствия 1; в случае когда $\varepsilon = \{e_1, \ldots, e_n\}$ является базисом в E и $\varepsilon' = \{e'_1, \ldots, e'_n\}$— двойственный базис в E' (для которого $[e_i, e'_j] = 1$ при $i = j$ и 0 при $i \neq j$), это вытекает из того же следствия. Отсюда с помощью следствия 1 теор. 3 п. 16.3.1 получаем наше утверждение в общем случае.

16.4.3. Идели

Как и прежде (см. п.16.3.3), если E — векторное пространство конечной размерности над полем k, то мы обозначаем через End (E) кольцо эндоморфизмов пространства E, рассматриваемое как алгебра над k. Мы будем обозначать через Aut (E) группу автоморфизмов пространства E, т. е. группу $\mathrm{End}(E)^\times$ обратимых элементов в End (E). Эта группа совпадает с подмножеством в End (E), определяемым условием $\det(a) \neq 0$. Поэтому если k — топологическое поле, то Aut (E) является открытым подмножеством в End (E). Ясно, что в топологии, индуцированной топологией из End (E), Aut (E) является топологической группой. Если K — поле, содержащее поле k, то End (E_K) совпадает с $\mathrm{End}(E)_K = \mathrm{End}(E) \otimes_k K$ и определитель на End (E_K) совпадает с продолжением на это пространство определителя на End (E).

Пусть $\mathcal{A}$ —алгебра конечной размерности над k. Обозначим через ρ ее регулярное представление в $\mathrm{End}(\mathcal{A})$, определенное в п. 16.3.3, и как обычно обозначим через $\mathcal{A}^\times$ группу обратимых элементов из $\mathcal{A}$.

Возьмем произвольный элемент a из $\mathcal{A}$. Очевидно, $\rho(a)$ есть эндоморфизм $x \to ax$ векторного пространства $\mathcal{A}$. Если $\rho(a)$ — автоморфизм, то он сюръективен, так что существует $b \in \mathcal{A}$, для которого $ab = 1_{\mathcal{A}}$. Тогда $b = a^{-1}$ и $a \in \mathcal{A}^{\times}$. Поскольку обратное утверждение тривиально, отсюда видно, что $\mathcal{A}^{\times}$ совпадает с подмножеством в $\mathcal{A}$, определенным условием $N_{\mathcal{A}/k}(a) \neq 0$. Поэтому если k — топологическое поле, то $\mathcal{A}^{\times}$— открытое подмножество в $\mathcal{A}$. Кроме того, тогда ρ является топологическим изоморфизмом из $\mathcal{A}$ на подалгебру в $\mathrm{End}(\mathcal{A})$, отображающим $\mathcal{A}^{\times}$ на $\rho(\mathcal{A}) \cap \mathrm{Aut}(\mathcal{A})$. Отсюда следует, что $\mathcal{A}^{\times}$ является тогда топологической группой в топологии, индуцированной топологией из $\mathcal{A}$.

Пусть теперь $\mathcal{A}$ — алгебра конечной размерности над **A**-полем k. Рассмотрим группу $\mathcal{A}_{\mathbf{A}}^{\times}$ обратимых элементов кольца $\mathcal{A}_{\mathbf{A}}$. Простейшие примеры в случае $\mathcal{A} = k$ показывают, что отображение $x \to x^{-1}$ не является непрерывным на этой группе в топологии, индуцированной топологией из $\mathcal{A}_{\mathbf{A}}$. Снабдим эту группу самой грубой топологией, для которой ее вложение в $\mathcal{A}_{\mathbf{A}}$ и отображение $x \to x^{-1}$ непрерывны. Более удобным образом это сделано в следующем определении.

Определение 2. *Пусть $\mathcal{A}$ — алгебра конечной размерности над* **A***-полем k. Тогда мы обозначаем через $\mathcal{A}_{\mathbf{A}}^{\times}$ группу обратимых элементов кольца $\mathcal{A}_{\mathbf{A}}$, наделенную топологией, для которой отображение $x \to (x, x^{-1})$ является гомеоморфизмом $\mathcal{A}_{\mathbf{A}}^{\times}$ на ее образ в $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$.*

Обычно (особенно в случае $\mathcal{A} = k$) **группу $\mathcal{A}_{\mathbf{A}}^{\times}$ с такой топологией называют *идельной группой* алгебры $\mathcal{A}$, а ее элементы называют *иделями* алгебры $\mathcal{A}$.** Очевидно, что отображения $(x, y) \to xy$ и $x \to x^{-1}$ непрерывны на $\mathcal{A}_{\mathbf{A}}^{\times}$, так что наше определение превращает ее в топологическую группу. В то же время, если мы обозначим через f отображение $(x, y) \to xy$ из $\mathcal{A} \times \mathcal{A}$ в $\mathcal{A}$ и его естественное продолжение на $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$, то наше определение говорит, что множество $\mathcal{A}_{\mathbf{A}}^{\times}$ гомеоморфно подмножеству $f^{-1}(\{1\})$ последнего пространства. Так как отображение f непрерывно, то это подмножество замкнуто, так что группа $\mathcal{A}_{\mathbf{A}}^{\times}$ локально компактна. Ясно также, что группа $\mathcal{A}^{\times}$ канонически вложена в группу $\mathcal{A}_{\mathbf{A}}^{\times}$. Поскольку при отображении $x \to (x, x^{-1})$ группа $\mathcal{A}^{\times}$ переходит в пересечение множества $f^{-1}(\{1\})$ с дискретным подмножеством $\mathcal{A} \times \mathcal{A}$ в $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$, то это — дискретная подгруппа в $\mathcal{A}_{\mathbf{A}}^{\times}$.

Используя следствие 2 теор. 3 п.16.2.1 и следствие 2 предл. 1 п.16.4.1, можно дать другое определение идельной группы алгебры

$\mathcal{A}$, эквивалентное определению 2. Как и в упомянутых утверждениях, возьмем конечное подмножество α *в* $\mathcal{A}$, содержащее базис $\mathcal{A}$ над k, и для всякой конечной точки v поля k обозначим через α_v r_v-модуль, порожденный подмножеством α в $\mathcal{A}_v$. По следствию 2 теор. 3 п.16.3.1 существует такое содержащее P_∞ конечное множество P_0 точек поля k, что для всех v, не лежащих в P_0, α_v является компактным подкольцом в $\mathcal{A}_v$ (содержащим единичный элемент). Для всякой точки v, как мы видели, $\mathcal{A}_v^\times$ есть открытое подмножество в $\mathcal{A}_v$ и отображение $x \to x^{-1}$ непрерывно на этом подмножестве. Поэтому отображением $x \to (x, x^{-1})$ оно гомеоморфно переводится в свой образ в $\mathcal{A}_v \times \mathcal{A}_v$. Для v, не лежащих в P_0, $\alpha_0^\times$ есть множество тех элементов из $\mathcal{A}_v^\times$, которые отображением $x \to (x, x^{-1})$ переводятся в $\alpha_v \times \alpha_v$, поэтому $\alpha_v^\times$ является открытой компактной подгруппой в $\mathcal{A}_v$ и открытым компактным подмножеством в α_v. Мы докажем сейчас следующий результат, аналогичный следствию 2 предл.1 п.16.4.1.

Предложение 2. *Пусть* $\mathcal{A}$, α, α_v *и* P_0 *таковы, как указано выше, и пусть* P *— любое конечное множество точек поля* k, *содержащее* P_0. *Тогда группа*

$$\mathcal{A}_\mathbf{A}(P, \alpha)^\times = \prod_{v \in P} \mathcal{A}_v^\times \times \prod_{v \notin P} \alpha_v^\times \tag{4}$$

является открытой подгруппой в $\mathcal{A}_\mathbf{A}^\times$; *топологии, индуцированные на ней топологиями из* $\mathcal{A}_\mathbf{A}^\times$ *и из* $\mathcal{A}_\mathbf{A}$, *совпадают обе с топологией произведения в правой части формулы* (4); $\mathcal{A}_\mathbf{A}^\times$ *является объединением этих групп.*

Пусть множество $\mathcal{A}_\mathbf{A}(P, \alpha)$ определено, как в следствии 2 предл. 1 п.16.4.1. Топология, индуцированная на $\mathcal{A}_\mathbf{A}(P, \alpha)^\times$ топологией из $\mathcal{A}_\mathbf{A}$, индуцирована также топологией из $\mathcal{A}_\mathbf{A}(P, \alpha)$ и потому совпадает с топологией произведения в правой части формулы (4). Для всякой точки и подмножество $\mathcal{A}_v{}^\times$ открыто в $\mathcal{A}_v$ и отображение $x \to x^{-1}$ непрерывно на нем. Поэтому отображение $x \to x^{-1}$ непрерывно на группе $\mathcal{A}_\mathbf{A}(P, \alpha)^\times$, наделенной топологией произведения. Отсюда следует, что отображение $x \to (x, x^{-1})$ есть гомеоморфизм из $\mathcal{A}_\mathbf{A}(P, \alpha)^\times$ на образ этой группы в $\mathcal{A}_\mathbf{A} \times \mathcal{A}_\mathbf{A}$. Поэтому топология произведения на этой группе индуцирована также топологией из $\mathcal{A}_\mathbf{A}^\times$. Далее, $\mathcal{A}_\mathbf{A}(P, \alpha)^\times$ совпадает с тем подмножеством в $\mathcal{A}_\mathbf{A}^\times$, которое отображением $x \to (x, x^{-1})$ переводится в $\mathcal{A}_\mathbf{A}(P, \alpha) \times \mathcal{A}_\mathbf{A}(P, \alpha)$. Так как последнее множество открыто в $\mathcal{A}_\mathbf{A} \times \mathcal{A}_\mathbf{A}$ и так как $\mathcal{A}_\mathbf{A} \times \mathcal{A}_\mathbf{A}$ является объединением множеств такого вида, это завершает доказательство.

Следствие. *Элемент* $a = (a_v)$ *из* k_A *лежит вв* $k_{\mathbf{A}}^{\times}$ *том и только том случае, когда* $a_v \neq 0$ *для всех* v *и почти* $|a_v|_v = 1$ *для всех* v. *Для каждого конечного множества* P *точек поля* k, *содержащего* P_∞, *группа*

$$k_{\mathbf{A}}(P)^{\times} = \prod_{v \in P} k_v^{\times} \times \prod_{v \notin P} r^{\times}$$

является открытой подгруппой в $k_{\mathbf{A}}^{\times}$ *и* $k_{\mathbf{A}}^{\times}$ *есть объединение таких групп.*

Первое утверждение очевидно; остальные утверждения — частный случай предложения 2.

Для каждого элемента $a = (a_v)$ из $k_{\mathbf{A}}^{\times}$ положим

$$|a|_{k_{\mathbf{A}}} = \prod_v |a_v|_v,$$

где произведение берется по всем точкам v поля k; ввиду следствия предл. 2 почти все сомножители в этом произведении равны 1 для любого a из $k_{\mathbf{A}}^{\times}$. Обычно, когда ясно, о каком поле идет речь, мы будем писать $|a|_{\mathbf{A}}$ вместо $|a|_{k_{\mathbf{A}}}$; иногда $|a|_{\mathbf{A}}$ будем называть *модулем* иделя a.

Предложение 3. *Пусть* E — *векторное пространство конечной размерности* n *над* k, $\mathcal{A} = \mathrm{End}(E)$ *и* $a = (a_v)$ — *некоторый элемент из* $\mathcal{A}_A$. *Тогда следующие утверждения эквивалентны:* (i) a *лежит в* $\mathcal{A}_{\mathbf{A}}^{\times}$; (ii) $\det(a)$ *лежит в* $k_{\mathbf{A}}^{\times}$; (iii) $e \to ae$ *есть изоморфизм пространства* E_A. *В случае когда эти утверждения выполняются, модуль последнего автоморфизма равен* $|\det(a)|_{\mathbf{A}}$. *Кроме того, отображения* $a \to \det(a)$ *и* $a \to |\det(a)|_{\mathbf{A}}$ *являются морфизмами из* $\mathcal{A}_{\mathbf{A}}^{\times}$ *в* $k_{\mathbf{A}}^{\times}$ *и в* $\mathbf{R}_+^{\times}$ *соответственно.*

Выберем какой-нибудь базис ε *в* E над k и используем его для отождествления E с k^n и $\mathcal{A}$ с $M_n(k)$. Тогда базис α в $\mathcal{A}$ над k задается «матричными единицами» $a_{\lambda\mu}$ с $1 \leqslant \lambda, \mu \leqslant n$, где $a_{\lambda\mu}$ — матрица (x_{ij}), $x_{\lambda\mu} = 1$ и $x_{ij} = 0$ при $(i, j) \neq (\lambda, \mu)$. Для каждой точки v поля k элемент a_v из $M_n(k_v)$ обратим в $M_n(k_v)$ тогда и только тогда, когда $\det(a_v) \neq 0$. Для каждой конечной точки v поля k элемент a_v из $M_n(r_v)$ обратим в $M_n(r_v)$ тогда и только тогда, когда $\det(a_v)$ обратим в r_v, т. е. тогда и только тогда, когда $|\det(a_v)|_v = 1$. В обозначениях предложения 2 и его следствия это означает, что a лежит в $\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times}$ в том и только том случае, когда $\det(a)$ лежит в $k_A(P)^{\times}$. Ясно, что отсюда следует эквивалентность утверждений (i) и (ii) нашего предложения; это показывает также, что отображение $a \to \det(a)$ из $\mathcal{A}_{\mathbf{A}}^{\times}$ в $k_{\mathbf{A}}^{\times}$ непрерывно на $\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times}$ для каждого P, а значит, непрерывно на $\mathcal{A}_{\mathbf{A}}^{\times}$. Поскольку, очевидно, отображение

$z \to |z|_{\mathbf{A}}$ из $k_{\mathbf{A}}^{\times}$ в $\mathbf{R}_{+}^{\times}$ непрерывно на $k_{\mathbf{A}}(P)^{\times}$ для каждого P, а следовательно и на $k_{\mathbf{A}}^{\times}$, то отображение $a \to |\det(a)|_{\mathbf{A}}$ есть непрерывный морфизм из $\mathcal{A}_{\mathbf{A}}^{\times}$ в $\mathbf{R}_{+}^{\times}$. Если элемент a лежит в $\mathcal{A}_{\mathbf{A}}^{\times}$, то обратный элемент a^{-1} лежит в $\mathcal{A}_A$ и эндоморфизм $e \to ae$ пространства E_A имеет обратный $e \to a^{-1}e$, т. е. является автоморфизмом. Обратно, возьмем любой элемент $a = (a_v)$ из $\mathcal{A}_A$. Предложение 1 п.16.4.1, примененное к $\mathcal{A}$ и α, показывает, что a_v содержится в $M_n(k_v)$ для всех v и в $M_n(r_v)$ почти для всех v. Это же предложение, примененное к E и ε, показывает, что в E_A фундаментальную систему окрестностей нуля образуют множества $U = \prod U_v$, где U_v — окрестность нуля в $E_v = (k_v)^n$ для всех v и $U_v = (r_v)^n$ почти для всех v. Если отображение $e \to ae$ есть автоморфизм пространства E_A, то оно должно отображать каждую окрестность нуля на окрестность нуля. Отсюда следует, что элемент a_v обратим в $M_n(k_0)$ при всех v и что почти для всех v образ множества $(r_v)^n$ относительно a_v содержит $(r_v)^n$, т. е. что a_v^{-1} лежит в $M_n(r_v)$ почти для всех v. Как мы заметили выше, это равносильно тому, что a лежит в $\mathcal{A}_{\mathbf{A}}^{\times}$. Пусть теперь P — конечное множество точек поля k, содержащее P_∞ и такое, что a_0 лежит в $M_n(r_v)^{\times}$ для всех v, не лежащих в P. Так как множество $E_{\mathbf{A}}(P, \varepsilon)$ открыто в E_A и инвариантно относительно отображения $e \to ae$, то модуль автоморфизма $e \to ae$ на E_A совпадает с его модулем на множестве $E_{\mathbf{A}}(P, \varepsilon)$. В силу определения этого множества (предложение 1 п.16.4.1) последний модуль равен произведению модулей автоморфизмов $e_v \to a_v e_v$ на сомножителях произведения $E_{\mathbf{A}}(P, \varepsilon)$. По следствию 3 теор. 3 п.16.1.2 эти модули равны $|\det(a_v)|_v$, чем и заканчивается наше доказательство.

Следствие. *Пусть $\mathcal{A}$ — алгебра конечной размерности над k и a — элемент из $\mathcal{A}_{\mathbf{A}}$. Тогда следующие утверждения эквивалентны:* (i) *a лежит в $\mathcal{A}_{\mathbf{A}}$;* (ii) $\mathrm{N}_{\mathcal{A}/k}(a)$ *лежит в* $k_{\mathbf{A}}^{\times}$; (iii) $x \to ax$ *есть автоморфизм аддитивной группы алгебры $\mathcal{A}_{\mathbf{A}}$. В случае когда эти утверждения выполняются, модуль последнего автоморфизма равен* $|\mathrm{N}_{\mathcal{A}/k}(a)|_{\mathbf{A}}$. *Кроме того,* $a \to \mathrm{N}_{\mathcal{A}/k}(a)$ *и* $a \to |\mathrm{N}_{\mathcal{A}/k}(a)|_{\mathbf{A}}$ *суть морфизмы группы $\mathcal{A}_{\mathbf{A}}^{\times}$ в $k_{\mathbf{A}}^{\times}$ и в $\mathbf{R}_{+}^{\times}$ соответственно.*

Поскольку (как мы всегда предполагаем) $\mathcal{A}$ содержит единицу, то из (iii) следует (i). Все остальные наши утверждения вытекают из предложения 3, примененного к алгебре $\mathcal{A}$, рассматриваемой как векторное пространство E над k, и к вложению алгебры $\mathcal{A}$ в End (E), задаваемому регулярным представлением ρ.

Все, что мы сказали про эндоморфизм $x \to ax$ алгебры $\mathcal{A}$, столь же применимо к эндоморфизму $x \to xa$. Определитель $\mathrm{N}'(a)$ последнего эндоморфизма называется иногда *корегулярной нормой* на $\mathcal{A}$. Как и регулярная норма, это — полиномиальная функция, степень которой равна размерности $\mathcal{A}$ над *k;* модуль автоморфизма $x \to xa$ аддитивной группы алгебры $\mathcal{A}_{\mathbf{A}}$, для $a \in \mathcal{A}_{\mathbf{A}}^{\times}$, равен $|\mathrm{N}'(a)|_{\mathbf{A}}$. Очевидно, что $\mathrm{N}' = \mathrm{N}_{\mathcal{A}/k}$, если алгебра $\mathcal{A}$ коммутативна; известно, что то же самое верно для всех полупростых алгебр; для простых алгебр, в частности для алгебр с делением, это будет доказано далее; здесь нам это не понадобится.

Теорема 4. *Пусть D — алгебра с делением конечной размерности над k. Для каждого вещественного числа* $\mu \geq 1$ *обозначим через* D_μ, *множество таких элементов d из* $D_{\mathbf{A}}^{\times}$, *что модули автоморфизмов* $x \to dx$ *и* $x \to xd$ *группы* D_A *соответственно* $\leq \mu$ *и* $\geqslant \mu^{-1}$. *Тогда* D_μ *является замкнутым подмножеством в* $D_{\mathbf{A}}^{\times}$ *и его образ в* $D_{\mathbf{A}}^{\times}/D^{\times}$ *компактен.*

Обозначим через N регулярную норму $N_{D/k}$ и через N' корегулярную норму, определенную выше. По следствию предл. 3 отображение $d \to |\mathrm{N}(d)|_{\mathbf{A}}$ непрерывно на $D_{\mathbf{A}}^{\times}$; по аналогичным причинам это верно и для отображения $d \to |\mathrm{N}'(d)|_{\mathbf{A}}$. Ввиду того же следствия отсюда вытекает замкнутость D_μ. По теореме 2 п.16.4.2 D есть дискретное подмножество в D_A и факторгруппа $D_{\mathbf{A}}/D$ компактна. Поэтому существует мера Хаара α на D_A, для которой $\alpha(D_{\mathbf{A}}/D) = 1$; эта мера определяется указанным в п.16.2.4 способом. Так как группа D_A некомпактна, то мы можем выбрать компактное подмножество C в D_A, для которого $\alpha(C) > \mu$. Обозначим через C' образ множества $C \times C$ при отображении $(x, y) \to x - y$ из $D_{\mathbf{A}} \times D_{\mathbf{A}}$ в D_A и через C'' образ множества $C' \times C'$ при отображении $(x, y) \to xy$ из $D_{\mathbf{A}} \times D_{\mathbf{A}}$ в D_A. Поскольку эти отображения непрерывны, то C' и C'' компактны. Возьмем любой элемент $d \in D_\mu$. Так как модуль автоморфизма $x \to xd$ не меньше μ^{-1}, то он отображает C на множество Cd, мера которого больше 1. Поэтому в силу леммы 1 п. 16.2.4 существуют такие два элемента x, y в C, что элемент $xd - yd$ лежит в D и отличен от нуля, т. е. этот элемент лежит в $D^{\times}$. Запишем $c_1 = x - y$ и $\delta_1 = c_1 d$. Тогда $c_1 \in C'$ и $\delta_1 \in D^{\times}$. Аналогично автоморфизм $x \to d^{-1}x$, являясь обратным к автоморфизму $x \to dx$, имеет модуль не меньше μ^{-1} и, значит, отображает C на множество $d^{-1}C$ меры >1; как и выше, заключаем, что существует $c_2 \in C'$, для которого элемент $\delta_2 = d^{-1}c_2$ лежит в $D^{\times}$. Тогда $\delta_1\delta_2 = c_1c_2$, так что $\delta_1\delta_2$ лежит в $D^{\times} \cap C''$. Но это пересечение — конечное множество, поскольку подмножество D

дискретно, а C'' компактно в D_A. Обозначим через $\gamma_1, \ldots, \gamma_N$ все различные элементы множества $D^\times \cap C''$. Элемент c_1c_2 равен одному из них, скажем γ_i, так что $\gamma_i^{-1}c_1c_2 = 1$. Отсюда видно, что элемент c_2 обратим в D_A и обратный элемент c_2^{-1} равен $\gamma_i^{-1}c_1$. Поскольку $d\delta_2 = c_2$, мы заключаем, что $d\ddot{o}_2$ принадлежит множеству X тех элементов x из $D_{\mathbf{A}}^{\times}$, образы которых при отображении $x \to (x, x^{-1})$ лежат в объединении множеств $C' \times (\gamma_i^{-1}C')$, $1 \leqslant i \leqslant N$. В силу определения 2 X является компактным подмножеством в $D^{\times}{}_A$ Так как $D_{\mu} \subset X \cdot D^{\times}$, то образ множества D^{μ} в $D_{\mathbf{A}}^{\times}/D^{\times}$ содержится в образе множества X, чем наша теорема и доказана.

16.4.4. Идели А-полей

Здесь мы рассмотрим более подробно случай $\mathcal{A} = k$.

Теорема 5. *Пусть k — произвольное* **A***-поле. Тогда морфизм $z \to |z|_{\mathbf{A}}$ группы $k_{\mathbf{A}}^{\times}$ в $\mathbf{R}_+^{\times}$ индуцирует на $k^{\times}$ отображение, тождественно равное* 1.

Если $\xi \in k^{\times}$, то $x \to \xi x$ есть автоморфизм группы k_A, отображающий k в себя. По теореме 2 п.16.4.2 поле k дискретно в k_A и факторгруппа $k_{\mathbf{A}}/k$ компактна. Поэтому модуль автоморфизма $x \to \xi x$, который по предложению 3 п.16.4.3 совпадает с $|\xi|_{\mathbf{A}}$ (если взять в этом предложении $E = k$), равен 1.

Теорема 5 известна как *формула произведения Артина*. Начиная с этого места, мы будем обозначать через $k_{\mathbf{A}}^1$ ядро морфизма $z \to |z|_{\mathbf{A}}$, т. е. подгруппу в $k_{\mathbf{A}}^{\times}$, задаваемую условием $|z|_{\mathbf{A}} = 1$; по теореме 5

$$k_{\mathbf{A}}^1 \supset k^{\times}.$$

Следствие 1. *Если k — поле характеристики $p > 1$, то $k^{\times}{}_A$ разлагается в прямое произведение подгруппы $k^1{}_A$ и некоторой дискретной подгруппы, изоморфной* **Z**.

Для каждой точки v поля k поле k_v имеет характеристику p, так что $|x|_v$ для каждого $x \in k_v^{\times}$ лежит в подгруппе в $\mathbf{R}_+^{\times}$, порожденной элементом p. Поэтому то же самое верно для $|z|_{\mathbf{A}}$ при каждом $z \in k_{\mathbf{A}}^{\times}$. Другими словами, образ группы $k^{\times}{}_A$ при морфизме $z \to |z|_{\mathbf{A}}$ является подгруппой в группе, порожденной элементом p в $\mathbf{R}_+^{\times}$. Так как этот образ, очевидно, не сводится к $\{1\}$, то он порождается некоторым целым числом $Q = p^N$, где $N \geqslant 1$ — целое число. Возьмем $z_1 \in k_{\mathbf{A}}^{\times}$, для которого $|z_1|_{\mathbf{A}} = Q$. Тогда $k_{\mathbf{A}}^{\times}$ разлагается в прямое произведение

подгруппы k^1_A и подгруппы, порожденной элементом z_1, которая, очевидно, дискретна и изоморфна группе Z.

Следствие 2. *Предположим, что характеристика поля k равна нулю. Для каждого* $\lambda \in \mathbf{R}^{\times}_{+}$ *обозначим через* $z(\lambda)$ *идель* (z_v), *такой, что* $z_v = 1$ *для всех конечных точек* v *и* $z_w = \lambda$ *для всех бесконечных точек* w *поля* k. *Тогда отображение* $\lambda \to z(\lambda)$ *есть изоморфизм группы* $\mathbf{R}^{\times}_{+}$ *на замкнутую подгруппу* M *в* $k^{\times}_{\mathbf{A}}$ *и* $k^{\times}_{\mathbf{A}}$ *разлагается в прямое произведение подгрупп* k^1_A *и* M.

В обозначениях следствия предл. 2 п.16.4.3 очевидно, что $\lambda \to z(\lambda)$ есть изоморфизм из $\mathbf{R}^{\times}_{+}$ на подгруппу M в $k_{\mathbf{A}}(P_\infty)^{\times}$. Определение модуля $|z|_{\mathbf{A}}$ вместе со следствием 2 теор. 4 п. 16.3.4 показывают, что $|z(\lambda)|_{\mathbf{A}} = \lambda^n$, где n — *степень поля* k над **Q**. Наше последнее утверждение теперь очевидно.

Теорема 6. *Пусть* k^1_A — *подгруппа в* $k^{\times}_{\mathbf{A}}$, *определенная условием* $|z|_{\mathbf{A}} = 1$. *Тогда* $k^{\times}$ *является дискретной подгруппой в* k^1_A, *факторгруппа* $k^1_{\mathbf{A}}/k^{\times}$ *компактна и* $k^{\times}_{\mathbf{A}}/k^{\times}$ *разлагается в прямое произведение этой компактной группы и группы, изоморфной* $\mathbf{R}^{\times}_{+}$ *в случае характеристики нуль и изоморфной* **Z** *в случае ненулевой характеристики.*

Первое утверждение содержится в теореме 5; второе является частным случаем теоремы 4 п.16.4.3 при $D = k$, $\mu = 1$; остальные утверждения вытекают из следствий теор. 5.

Теперь мы исследуем более подробно структуру различных подгрупп в $k^{\times}_{\mathbf{A}}$ и в $k^{\times}$ и некоторых их факторгрупп. Условимся обозначать через $\Omega(P)$ группу, которая в следствии предл. 2 п.16.4.3 обозначалась через $k_{\mathbf{A}}(P)^{\times}$. Другими словами, начиная с этого места, мы будем писать

$$\Omega(P) = \prod_{v \in P} k_v^{\times} \times \prod_{v \notin P} r_v^{\times} \,. \tag{5}$$

Как всегда, P предполагается конечным множеством точек поля k, содержащим множество P_∞ всех бесконечных точек; P может быть пустым, но только не в случае характеристики нуль. Напомним, что $\Omega(P)$ всегда является открытой подгруппой в $k^{\times}_{\mathbf{A}}$; ясно, что она компактна тогда и только тогда, когда P пусто. Мы будем также писать

$$\Omega_1(P) = \Omega(P) \cap k^1_{\mathbf{A}}.$$

В случае когда характеристика поля k равна $p > 1$, мы можем, взять здесь $P = \varnothing$, тогда $\Omega_1(\varnothing) = \Omega(\varnothing)$.

Теорема 7. *Если* P *не пусто, то группа* $k^{\times}_{\mathbf{A}}/k^{\times}\Omega(P)$ *конечна. Если характеристика поля* k *равна* $p > 1$, *то группа* $k^1_{\mathbf{A}}/k^{\times}\,\Omega(\varnothing)$

конечна и $k_{\mathbf{A}}^{\times}/k^{\times}\,\Omega\,(\varnothing)$ *разлагается в прямое произведение этой группы на группу, изоморфную* **Z.**

Во всех случаях группа $k_{\mathbf{A}}^{1}/k^{\times}\,\Omega_1\,(P)$ изоморфна факторгруппе группы $k_{\mathbf{A}}^{1}/k^{\times}$ по образу в $k_{\mathbf{A}}^{1}/k^{\times}$ группы $\Omega_1\,(P)$. Так как группа $\Omega_1\,(P)$ открыта в $k^1{}_A$, то и этот образ открыт; так как факторгруппа $k_{\mathbf{A}}^{1}/k^{\times}$ компактна по теореме 6, то указанная выше факторгруппа по этому образу конечна. Если k имеет характеристику нуль, то $\Omega(P)$ содержит группу M, определенную в следствии 2 теор. 5, и это следствие показывает, что $\Omega\,(P)$ разлагается в прямое произведение подгрупп $\Omega_1\,(P)$ и M, так что можно отождествить $k_{\mathbf{A}}^{\times}/k^{\times}\Omega\,(P)$ с $k_{\mathbf{A}}^{1}/k^{\times}\Omega_1\,(P)$. Предположим теперь, что k имеет характеристику $p > 1$. Поскольку $\Omega\,(\varnothing) = \Omega_1\,(\varnothing)$, следствие 1 теор. 5 показывает, что $k_{\mathbf{A}}^{\times}/k^{\times}\,\Omega\,(\varnothing)$ разлагается в прямое произведение конечной группы $g = k_{\mathbf{A}}^{1}/k^{\times}\,\Omega\,(\varnothing)$ и группы γ, изоморфной **Z.** Если $P \neq \varnothing$, то $\Omega\,(P)$ содержит $\Omega\,(\varnothing)$ и не содержится в $k^1{}_A$. Поэтому $k_{\mathbf{A}}^{\times}/k^{\times}\,\Omega\,(P)$ совпадает с факторгруппой группы $k_{\mathbf{A}}^{\times}/k^{\times}\Omega\,(\varnothing)$, т. е. группы $g \times \gamma$, по образу в ней группы $k^{\times}\,\Omega\,(P)$, и этот образ не содержится в образе g группы $k^1{}_A$. Отсюда видно, что эта факторгруппа конечна.

Следствие. *В обозначениях теоремы 7 можно выбрать P так, чтобы* $k_{\mathbf{A}}^{\times} = k^{\times}\,\Omega\,(P)$.

Возьмем любое непустое P' и выберем полное множество представителей $z_1, \ldots, z_N$ для классов в $k_{\mathbf{A}}^{\times}$ по модулю $k^{\times}\Omega\,(P')$. Так как $k_{\mathbf{A}}^{\times}$ есть объединение всех групп $\Omega\,(P)$, то можно выбрать $P \supset P'$ так, чтобы все z_i лежали в $\Omega\,(P)$. Тогда P будет обладать требуемым свойством.

В случае когда k — после алгебраических чисел и $P = P_\infty$, теорема 1, как будет показано в следующей главе, по существу совпадает с классической теоремой о конечности числа классов идеалов в k.

Теорема 8. *Пусть F — множество тех элементов* ξ *из k, для которых* $|\xi|_v \leqslant 1$ *для всех точек v поля k. Положим* $E = F - \{0\}$. *Тогда E совпадает с конечной циклической группой, состоящей из всех корней из* 1 *в k.*

Множество F является пересечением поля k с множеством тех элементов (x_v) из k_A, для которых $|x_v|_v \leqslant 1$ для всех v. Ясно, что последнее множество компактно, а по теореме 2 в.16.4.2 k дискретно в k_A. Поэтому F конечно. Если $\xi \in E$, то теорема 5 показывает, что для всех v должно выполняться равенство $|\xi|_v = 1$. Поэтому E является подгруппой конечного порядка в k^x, откуда, согласно лемме 1 п.16.1.1,

следует цикличность *E*. Обратно, очевидно, что каждый корень из 1 в *k* должен содержаться в *E*.

Следствие. *Если k — поле характеристики p* > 1, *то множество F, определенное в теореме* 8, *является конечным полем, которое совпадает с алгебраическим замыканием в k простого поля в k.*

Множество *F* можно в этом случае записать в виде $F = k \cap (\prod r_v)$, где произведение берется по всем точкам *v* поля *k*. Отсюда видно, что *F* является кольцом; поскольку $E = F - \{0\}$ есть группа, то *F* — поле. По теореме 2 п.16.1.1 если отличный от нуля элемент поля *k* алгебраичен над простым полем, то он является корнем из 1 и, значит, лежит в *E* по теореме 8.

В случае когда *k* имеет характеристику $p > 1$, конечное поле *F*, определенное в следствии теор. 8, называется *полем констант* в *k*. Пусть множество *P* то же, что и выше. Определим подгруппу *E (P)* в k^x, положив

$$E(P) = k^\times \cap \Omega(P) = k^\times \cap \left(\prod_{v \in P} k_v^\times \times \prod_{v \notin P} r_v^\times\right).$$

Эта подгруппа состоит из тех элементов ξ группы k^x, для которых $|\xi|_v = 1$ для всех *v*, не лежащих в *P*. Очевидно, что *E (P)* содержит группу *E*, определенную в теореме 8. Так как k^x дискретна в $k_{\mathbf{A}}^\times$, *то E (P)* является дискретной подгруппой в $\Omega(P)$, а также ввиду теоремы 5 в $\Omega_1(P)$. Можно еще описать *E (P)* как группу $k(P)^\times$ обратимых элементов (или, в традиционной терминологии, «единиц») подкольца *k (P)* в *k*, задаваемого равенством

$$k(P) = k \cap \left(\prod_{v \in P} k_v \times \prod_{v \notin P} r_v\right)$$

и состоящего из элементов ξ в *k*, таких, что $|\xi|_v \leqslant 1$ для всех *v*, не лежащих в *P*. Для определения структуры группы *E(P)* нам понадобится одна элементарная лемма.

Лемма 5. *Пусть G — группа, изоморфная группе* $\mathbf{R}^r \times \mathbf{Z}^{s+1-r}$, *где* $s \geqslant r \geqslant 0$. *Пусть* λ в *случае* $r > 0$ *есть какой-нибудь морфизм группы G в* **R**, *нетривиальный на* $\mathbf{R}^r$, *а в противном случае — любой нетривиальный морфизм группы G в* **Z**. *Пусть, далее,* G_1 *— ядро морфизма* λ *и* Γ *— такая дискретная подгруппа в G, что факторгруппа* G_1/Γ *компактна. Тогда подгруппа* Γ *изоморфна* $\mathbf{Z}^s$.

Можно считать, что $G = \mathbf{R}^r \times \mathbf{Z}^{s+1-r}$. Тогда каждый элемент *x* из *G* можно записать в виде $(x_0, \ldots, x_s)$, где $x_i \in \mathbf{R}$ при $0 \leqslant i < r$ и $x_i \in \mathbf{Z}$ при $i \geqslant r$, а λ можно записать в виде

$$x = (x_0, \ldots, x_s) \longrightarrow \lambda(x) = \sum_{i=0}^{s} a_i x_i,$$

где $a_i \in \mathbf{R}$ при всех i, если $r > 0$, и $a_i \in \mathbf{Z}$ при всех i, если $r = 0$; в обоих случаях в силу наших предположений относительно λ можно считать, что $a_0 \neq 0$, а в первом случае можно считать, что $a_0 = 1$. Рассмотрим группу G как очевидным образом вложенную в векторное пространство $V = \mathbf{R}^{s+1}$ над $\mathbf{R}$. Тогда приведенная выше формула определяет λ как линейную форму на V. Пусть V_1 — подпространство в V, определенное уравнением $\lambda(x) = 0$, так что $G_1 = G \cap V_1$. Для $1 \leqslant j \leqslant s$ обозначим через e_j точку (x_i) в V, для которой $x_0 = -a_j$, $x_j = a_0$ и $x_i = 0$ при $i \neq 0$ и $i \neq j$. Так как множество $\{e_1, \ldots, e_s\}$ является базисом в V_1, то оно порождает $\mathbf{R}$-решетку H в V_1, так что факторгруппа V_1/H компактна. Поскольку $H \subset G_1$ и G_1 замкнуто в V_1, отсюда следует компактность фактор-группы V_1/G_1. Поэтому если подгруппа Γ такая, как в нашей лемме, то факторгруппа V_1/Γ компактна, так что Γ является $\mathbf{R}$-решеткой в V_1 и, следовательно, изоморфна $\mathbf{Z}^s$ согласно предложению 11 п.16.2.4.

Теорема 9. *Пусть P — любое конечное множество точек поля k, содержащее P_∞, и пусть $E(P)$ — подгруппа в $k^\times$, состоящая из тех элементов ξ в $k^\times$, для которых $|\xi|_v = 1$ для всех v, не лежащих в P. Тогда $E(P)$ разлагается в прямое произведение группы E всех корней из 1 в k и группы, изоморфной $\mathbf{Z}^s$, где $s=0$, если P пусто, и $s = \operatorname{card}(P) - 1$ в противном случае* (здесь card *(P)*—это число точек в *P*.)

Если P пусто, то наша теорема содержится в теореме 8, поэтому можно считать, что $P \neq \varnothing$. Обозначим через ν морфизм из $\Omega(P)$ в $\mathbf{R}_+^\times$, индуцированный отображением $z \to |z|_{\mathbf{A}}$. Его ядро совпадает с $\Omega_1(P)$ и открыто в k^1_A. Канонический морфизм из $k^1_{\mathbf{A}}$ на $k^1_{\mathbf{A}}/k^\times$ индуцирует на $\Omega_1(P)$ морфизм этой подгруппы на ее образ в $k^1_{\mathbf{A}}/k^\times$; ядро этого морфизма равно $E(P)$, ибо $k^\times \cap \Omega_1(P)$ совпадает с $k^\times \cap \Omega(P)$. Поэтому факторгруппа $\Omega_1(P)/E(P)$ изоморфна открытой подгруппе в $k^1_{\mathbf{A}}/k^\times$ и, следовательно, компактна по теореме 6. С другой стороны, обозначим для всякой точки v поля k через U_v компактную подгруппу в $k_v^\times$, определенную условием $|x|_v = 1$; эта подгруппа совпадает с $r_v^\times$, в случае когда v — конечная точка. Положим $U = \prod U_v$, где произведение берется по всем точкам поля k. Это — компактная подгруппа в $\Omega(P)$ и в $\Omega_1(P)$. Положим, далее, $G = \Omega(P)/U$. Ясно, что эта группа изоморфна произведению групп $k_v^\times/U_v$ по $v \in P$. Поскольку группа $k_v^\times/U_v$ изоморфна группе $\mathbf{R}_+^\times$ или, что то же самое, группе $\mathbf{R}$, в случае когда v — бесконечная точка, и изоморфна $\mathbf{Z}$ в противном случае, то G изоморфна $\mathbf{R}^r \times \mathbf{Z}^{s+1-r}$, где r — число бесконечных точек поля k, а s — число из

формулировки теоремы. Так как U содержится в ядре $\Omega_1(P)$ морфизма v группы $\Omega(P)$, то v определяет на группе G морфизм этой группы в $\mathbf{R}_+^\times$; этот морфизм, очевидно, нетривиален на каждом из сомножителей $k_v^\times/U_v$ в G, и в частности на тех из них, которые изоморфны **R**, если таковые сомножители имеются, т. е. если $r > 0$. С другой стороны, если $r = 0$, то по следствию 1 теор. 5 $|z|_A$ принимает значения в группе, изоморфной **Z**, так что с точностью до изоморфизма λ отображает G в **Z**. Поэтому G и λ удовлетворяют предположениям леммы 5; ядро d морфизма G_1 равно в рассматриваемом случае образу группы $\Omega_1(P)$ в G, т. е. $\Omega_1(P)/U$. Обозначим теперь через Γ образ группы $E(P)$ в G. Если W — любая компактная окрестность единицы в $\Omega(P)$, то множество WU компактно и потому имеет конечное пересечение с $E(P)$. Так как образ этого пересечения в G совпадает с пересечением подгруппы Γ с образом множества WU в G и так как последний образ является окрестностью единицы в G, отсюда видно, что подгруппа Γ дискретна в G. Факторгруппа G_1/Γ изоморфна $\Omega_1(P)/E(P)\,U$, т. е. факторгруппе компактной группы $\Omega_1(P)/E(P)$, и потому компактна. Мы можем теперь применить к G, λ и Γ лемму 5; получаем, что группа Γ изоморфна $\mathbf{Z}^s$. Так как $E(P) \cap U = E$, то у морфизма группы $E(P)$ на Γ, индуцированного каноническим морфизмом группы $\Omega(P)$ на G, ядро равно E. Пусть теперь $e_1, \ldots, e_s$ — представители в $E(P)$ множества свободных образующих группы Γ. Очевидно, они порождают в $E(P)$ подгруппу, изоморфную $\mathbf{Z}^s$, и $E(P)$ разлагается в прямое произведение группы E и этой подгруппы. Доказательство нашей теоремы закончено.

Попутно мы доказали также следующее

Следствие. *Предположим, что P не пусто и группа E (P) такова, как в теореме* 9. *Положим* $\Omega_1(P) = \Omega(P) \cap k_{\mathbf{A}}^1$ *и* $G_1 = \Omega_1(P)/U$, *где U — группа тех элементов* (z_v) *из* $k_{\mathbf{A}}^\times$, *для которых* $|z_v|_v = 1$ *при всех v. Тогда образ* Γ *группы E (P) в* G_1 *дискретен в* G_1 *и факторгруппа* G_1/Γ *компактна.*

В случае когда k — поле алгебраических чисел и $P = P_\infty$, теорема 9, как будет показано в следующей главе, совпадает со знаменитой «теоремой об единицах» Дирихле.

16.5. Поля алгебраических чисел

16.5. 1. Порядки в алгебрах над Q

Нам понадобятся некоторые элементарные результаты о векторных пространствах над **Q**, связанные со следующим понятием.

Определение 1. *Пусть E — векторное пространство конечной размерности над* **Q**. *Под* **Q**-*решеткой в E мы понимаем конечно порожденную подгруппу в E, содержащую базис векторного пространства E над* **Q**.

Предложение 1. *Пусть E — векторное пространство конечной размерности над* **Q**, *и пусть L, L' — две* **Q**-*решетки в E. Тогда существует такое целое число $m > 0$, что $mL \subset L'$.*

Пусть $\{e_1, \ldots, e_r\}$ и $\{e'_1, \ldots, e'_s\}$ — конечные множества образующих для L и L' соответственно. Так как второе множество должно содержать базис для E над **Q**, то e_i можно записать (вообще говоря, не единственным способом) в виде $e_i = \sum a_{ij}e'_j, 1 \leqslant i \leqslant r$, где коэффициенты $a_{ij} \in \mathbf{Q}$. Возьмем в качестве m такое целое положительное число, что $ma_{ij} \in \mathbf{Z}$ при всех i, j. Тогда $mL \subset L'$.

Следствие 1. *Пусть E таково, как в предложении* 1. *Тогда каждая* **Q**-*решетка L в E порождается некоторым базисом векторного пространства E над* **Q**.

Пусть β — какой-нибудь базис в E над **Q**, содержащийся в L, и пусть L' — **Q**-решетка, порожденная множеством β. Согласно предложению 1, существует такое целое число $m > 0$, что $mL \subset L'$. Рассмотрим E как подмножество в $E_{\mathbf{R}} = E \otimes_{\mathbf{Q}} \mathbf{R}$. Согласно предложению 11 п. 16.2.4 L' является **R**-решеткой в $E_{\mathbf{R}}$. Так как L содержится в $m^{-1}L'$, то то же самое предложение показывает, во-первых, что L также является **R**-решеткой в $E_{\mathbf{R}}$, а во-вторых, что L порождается некоторым базисом в $E_{\mathbf{R}}$ над **R**. Поскольку этот базис содержится в E, то он, очевидно, является базисом векторного пространства E над **Q**.

Следствие 2. *Пусть E и L таковы, как в следствии* 1. *Тогда каждая подгруппа L' в L, содержащая базис пространства E над* **Q**, *является* **Q**-*решеткой в E.*

Пусть β' — базис пространства E над **Q**, содержащийся в L', и пусть L'' — **Q**-решетка, порожденная множеством β'. Согласно предложению 1, существует такое целое $m > 0$, что $mL \subset L''$. Тогда $m^{-1}L'' \supset L \supset L' \supset L''$. Ясно, что L'' имеет индекс m^n в $m^{-1}L''$, где n — размерность E над **Q**. Следовательно, L'' имеет конечный индекс в L'. Поскольку L' порождается множеством β' и любым полным множеством представителей классов L'/L'', наше следствие доказано.

Определение 2. *Пусть $\mathcal{A}$ — алгебра конечной размерности над* **Q**. *Подкольцо в $\mathcal{A}$ будем называть порядком в $\mathcal{A}$, если оно является* **Q**-*решеткой в алгебре $\mathcal{A}$, рассматриваемой как векторное пространство над* **Q**.

Здесь, как всегда, подразумевается, что подкольцо в $\mathcal{A}$ содержит единицу алгебры $\mathcal{A}$.

Предложение 2. *Каждая алгебра $\mathcal{A}$ конечной размерности над* **Q** *содержит по крайней мере один порядок.*

Пусть $\{a_1, \ldots, a_N\}$— какое-нибудь конечное подмножество в $\mathcal{A}$, содержащее базис векторного пространства $\mathcal{A}$ над **Q**. Тогда для всех i, j мы можем записать $a_i a_j = \sum c_{ijh} a_h$, где коэффициенты $c_{ijh} \in \mathbf{Q}$. Пусть m — такое целое положительное число, что $mc_{ijh} \in \mathbf{Z}$ для всех i, j, h. Тогда **Q**-решетка, порожденная элементами $1, ma_1, \ldots, ma_N$, является порядком.

Возьмем для примера $\mathcal{A} = \mathbf{Q}$. По следствию 1 предл. 1 каждая **Q**-решетка в **Q** имеет вид $a\mathbf{Z}$, где $a \in \mathbf{Q}^\times$. Если эта решетка является порядком, то $a^{-1} \in a\mathbf{Z}$, так что $a \in \mathbf{Z}$, и $1 \in a\mathbf{Z}$, так что $a^{-1} \in \mathbf{Z}$, откуда $a = \pm 1$. Это показывает, что **Z** является единственным порядком в **Q**.

Предложение 3. *Пусть a — произвольный элемент некоторого порядка в алгебре $\mathcal{A}$, конечномерной над* **Q**. *Тогда a цел над* **Z** *и* $\mathrm{Tr}_{\mathcal{A}/\mathbf{Q}}(a), \mathrm{N}_{\mathcal{A}/\mathbf{Q}}(a) \in \mathbf{Z}$.

Пусть R — порядок, содержащий элемент a, и пусть $\{a_1, \ldots, a_N\}$ — конечное множество образующих для R. Тогда при $1 \leqslant i \leqslant N$ можно записать $a \cdot a_i = \sum c_{ij} a_j$, где коэффициенты $c_{ij} \in \mathbf{Z}$. Это равенство можно переписать в виде $\sum (\delta_{ij} a - c_{ij})\, a_j = 0$, где (δ_{ij}) — единичная матрица I_N. Обозначим через $D(T)$ определитель матрицы $(\delta_{ij} T - c_{ij})$, где T — независимая переменная, и через $D_{ij}(T)$ ... — миноры этой матрицы, $1 \leqslant i, \leqslant N$; $D(T)$ и $D_{ij}(T)$ являются многочленами из $\mathbf{Z}[T]$, и

$$\sum_i D_{ih}(T) \cdot (\delta_{ij} T - c_{ij}) = \delta_{hj} D(T)$$

при $1 \leqslant h, j \leqslant N$. Подставляя a вместо T, умножая справа на a_j и суммируя по всем j от 1 до N, получаем $D(a)\, a_h = 0$ при всех h; следовательно, $D(a)\, x = 0$ при всех x. При $x = 1$ это дает $D(a) = 0$, чем доказано наше первое утверждение, поскольку многочлен $D(T)$ имеет целые коэффициенты и старший коэффициент равен 1. В силу следствия 1 предл. 1 можно считать, что в качестве множества $\{a_1, \ldots, a_N\}$ взят базис для $\mathcal{A}$ над **Q**. Тогда $\mathrm{Tr}_{\mathcal{A}/\mathbf{Q}}(a)$ и $\mathrm{N}_{\mathcal{A}/\mathbf{Q}}(a)$ равны следу и определителю матрицы (c_{ij}) и, значит, являются целыми числами.

16.5.2. Решетки над полями алгебраических чисел

Начиная с этого места и до конца главы k обозначает некоторое поле алгебраических чисел. Мы будем использовать обозначения, введенные в п.16.4. В частности, для любой точки v поля k через k_v обозначается соответствующее пополнение поля k; если v — конечная точка, то r_v — максимальное компактное подкольцо в k_v и p_v — максимальный идеал в r_v. Через k_A обозначается кольцо аделей поля k, а через φ — каноническое вложение $k \to k_{\mathbf{A}}$. Каноническое вложение любого конечномерного векторного пространства E над k в соответствующее адельное пространство E_A будет обозначаться через φ_E; как было показано в п.16.4.1, при этом вложении $e \to e \otimes \varphi$ (1).

Рассмотрим теперь алгебру $k \otimes_{\mathbf{Q}} \mathbf{R}$ над $\mathbf{R}$; в теореме 1 п.16.4.1 эта же алгебра обозначалась через $(k/\mathbf{Q})_\infty$. Имеется изоморфизм Φ_∞ этой алгебры на прямое произведение $\prod k_w$ пополнений поля k по всем его бесконечным точкам w; этот изоморфизм вполне характеризуется свойствами, сформулированными в теореме 4 п.16.3.4. Для упрощения обозначений отождествим посредством Φ_∞ алгебру $(k/\mathbf{Q})_\infty$ с $\prod k_w$ и будем обозначать обе алгебры через k_∞. Аналогично если E — любое конечномерное векторное пространство над k, то будем писать E_∞ вместо $E \otimes_{\mathbf{Q}} \mathbf{R}$; в следствии 2 теор. I п.16.4.1 это же пространство обозначалось через $(E/\mathbf{Q})_\infty$; поскольку это пространство совпадает также с $E \otimes_k k_\infty$, мы отождествляем его с произведением $\prod E_w$, взятым по всем бесконечным точкам w поля k.

Открытую подгруппу $k_{\mathbf{A}}(P_\infty) \subset k_{\mathbf{A}}$, задаваемую формулой (1) п.16.4.1, можно теперь записать как $k_\infty \times (\prod r_v)$, где последнее произведение берется по всем конечным точкам v поля k и является компактным. В этой и в аналогичных ситуациях оказывается полезной следующая теоретико-групповая лемма.

Лемма 1. *Пусть G — локально компактная группа с открытой подгруппой G_1 вида $G_1 = G' \times G''$, где G' локально компактна, а G'' компактна, и пусть Γ — такая дискретная подгруппа в G, что пространство G/Γ компактно. Обозначим через Γ' проекцию группы $\Gamma \cap G_1$ на G'. Тогда множество Γ' дискретно в G', а множество G'/Γ' компактно.*

Пусть W — компактная окрестность нейтрального элемента в G' (нет необходимости предполагать, что группы G, G', G'' коммутативны, хотя в дальнейшем будет использоваться только этот случай). Поскольку множество $W \times G''$ компактно, его пересечение с Γ конечно. Так как проекция этого пересечения на G' совпадает с

$W \cap \Gamma'$, то множество Γ' дискретно. Множества $G_1\Gamma$ и $G - G_1\Gamma$ открыты, поскольку они являются объединениями левых смежных классов по открытой подгруппе G_1. Поэтому образ группы G_1 в G/Γ открыт и замкнут там и, следовательно, компактен. Так как он изоморфен G_1/Γ_1, где $\Gamma_1 = \Gamma \cap G_1$, то существует такое компактное подмножество C в G_1 что $G_1 = C \cdot \Gamma_1$. Но тогда $G' = C' \cdot \Gamma'$, где C' — проекция C на G', чем и доказана компактность G'/Γ'.

Теорема 1. *Пусть k — некоторое поле алгебраических чисел. Положим* $\mathfrak{r} = \bigcap_v (k \cap r_v)$, *где v пробегает все конечные точки поля k. Тогда* $\mathfrak{r}$ *есть порядок в k; это единственный максимальный порядок в k, и он совпадает с целым замыканием кольца* **Z** *в k.*

Как объяснялось выше, запишем $k_{\mathbf{A}}(P_\infty)$ в виде произведения $k_\infty \times (\prod r_v)$. Ясно, что элемент $\xi \in k$ лежит в $\mathfrak{r}$ в том и только в том случае, когда $\varphi(\xi)$ лежит в этом произведении; обозначим в этом случае через $\varphi_\infty(\xi)$ и $\psi(\xi)$ проекции $\varphi(\xi)$ на k_∞ и на $\prod r_v$ соответственно. Очевидно, $\mathfrak{r}$ является подкольцом в k. Теперь применим лемму 1 к

$$G = k_{\mathbf{A}},\ G_1 = k_{\mathbf{A}}(P_\infty),\ G' = k_\infty,\ G'' = \prod r_v,\ \Gamma = \varphi(k).$$

Согласно этой лемме $\Gamma = \varphi_\infty(\mathfrak{r})$ является **R**-решеткой в k_∞. Так как φ_∞ совпадает с вложением, индуцированным на $\mathfrak{r}$ естественным вложением поля k в $k_\infty = k \otimes_{\mathbf{Q}} \mathbf{R}$, отсюда следует, что $\mathfrak{r}$ является **Q**-решеткой в k. Следовательно, $\mathfrak{r}$ есть порядок. Пусть $\mathfrak{r}'$ — любое подкольцо в k, аддитивная группа которого конечно порождена. Ясно, что r_v-модуль, порожденный множеством $\mathfrak{r}'$ в k_v, является компактным подкольцом в k_v. Этот модуль содержит r_v, поскольку $\mathfrak{r}'$ содержит 1; поэтому он совпадает с r_v, так что $\mathfrak{r}' \subset r_v$. Так как это справедливо для всех v, то $\mathfrak{r}' \subset \mathfrak{r}$.

Согласно предложению 3 п.16.5.1 $\mathfrak{r}$ содержится в целом алгебраическом замыкании кольца **Z** в k. Обратно, если некоторый элемент поля k цел над **Z**, то предложение 6 п. 16.1.4 показывает, что этот элемент лежит в r_v при всех v, а следовательно, лежит в $\mathfrak{r}$.

Отображение $\psi\colon \mathfrak{r} \to \prod r_v$, определенное в доказательстве теоремы 1, будем называть *каноническим вложением* кольца $\mathfrak{r}$ в произведение $\prod r_v$. При этом вложении каждому $\xi \in \mathfrak{r}$ сопоставляется элемент (x_v) этого произведения с $x_v = \xi$ при всех v. Отображение ψ осуществляет изоморфизм кольца $\mathfrak{r}$ на кольцо $\psi(\mathfrak{r})$; сложение и умножение в $\prod r_v$ определяются покоординатно. В этих обозначениях справедливо

Следствие 1. *Пусть* k, $\mathfrak{r}$ *и* ψ *таковы, как выше. Тогда кольцо* $\psi(\mathfrak{r})$ *плотно в* $\prod r_v$ *и его проекция на каждое частичное*

произведение плотна там. В частности, r_v совпадает с замыканием $\mathfrak{r}$ в k_v.

Пусть G, G_1, G', G'', Γ таковы, как в доказательстве теормы 1. По следствию 2 теор. 3 п.14.4.2 кольцо $k_\infty + \varphi(k)$, которое мы теперь обозначаем через $G\Gamma$, плотно в $\bar{G} = k_{\mathbf{A}}$, так что его пересечение с G_i должно быть плотно в G_1. Так как это пересечение равно $k_\infty + \varphi(\mathfrak{r})$, отсюда следует, что его проекция на $G'' = \prod r_v$, совпадающая с проекцией $\psi(\mathfrak{r})$ кольца $\varphi(\mathfrak{r})$ на G'', плотна там. Второе утверждение нашего следствия тривиальным образом следует из первого.

Следствие 2. *Если k' — конечное алгебраическое расширение поля k, то максимальный порядок в k' совпадает с целым замыканием кольца $\mathfrak{r}$ в k'.*

Это снова вытекает из предложения 6 п. 16.1.4; рассуждения в точности те же, что и в доказательстве теоремы 1.

Определение 3. *Пусть k — некоторое поле алгебраических чисел, $\mathfrak{r}$ — максимальный порядок в k и E — векторное пространство конечной размерности над k. Всякий конечно порожденный $\mathfrak{r}$-модуль, содержащий базис векторного пространства E над k, будем называть k-решеткой в E.*

Если k' — конечное алгебраическое расширение поля k, $\mathfrak{r}'$ — максимальный порядок в k' и E — векторное пространство конечной размерности над k', то, очевидно, $\mathfrak{r}'$-модуль в E является k'-решеткой тогда и только тогда, когда он является k-решеткой в E, рассматриваемом как векторное пространство над k.

Пусть E — векторное пространство конечной размерности над k, L — некоторая k-решетка в E и ε — конечное подмножество в E, порождающее L как $\mathfrak{r}$-модуль. Тогда для каждой конечной точки v поля k r_v-модуль ε_v, порожденный множеством ε, совпадает с r_v-модулем L_v, порожденным решеткой L. Согласно предложению 1 п. 16.4.1 $E_{\mathbf{A}}(P_\infty, \varepsilon)$ совпадает с $E_\infty \times \prod L_v$ и является открытой подгруппой в E_A. Для каждого $e \in L$ можно определить элемент (e_v) в $\prod L_v$, положив $e_v = e$ при всех v. Обозначим этот элемент через $\psi_L(e)$; отображение ψ_L будем называть *каноническим вложением* решетки L в $\prod L_v$. Имеет место

Предложение 4. *Пусть E — векторное пространство конечной размерности над k и L — некоторая k-решетка в E. Для каждой конечной точки v поля k через L_v обозначим r_v-модуль, порожденный решеткой L в E_v. Пусть $\psi_L\colon L \to \prod L_v$ — соответствующее каноническое вложение. Тогда образ $\psi_L(L)$ плотен в $\prod L_v$ и его*

проекции на каждое частичное произведение плотны там; в частности, L_v для каждой точки v совпадает с замыканием L в E_v.

Пусть $\varepsilon = \{e_1, \ldots, e_N\}$ — какое-нибудь конечное подмножество в L, порождающее L как $\mathfrak{r}$-модуль. Возьмем любой элемент $(e_v) \in \in \prod L_v$. Для каждой точки v можно записать e_v в виде $e_v = \sum x_v^{(i)} e_i$, где коэффициенты $x_v^{(i)} \in r_v$. Положим $x_i = (x_v^{(i)})$ при $1 \leqslant i \leqslant N$. Тогда $x_i \in \prod r_v$. По следствию 1 теор. 1 можно найти такие $\xi_i \in \mathfrak{r}$, что для каждого i элементы $\psi(\xi_i)$ сколь угодно близки к x_i. Тогда, очевидно, элемент $\psi_L(\sum \xi_i e_i)$ может быть сделан сколь угодно близким к e_v.

Теорема 2. *Пусть k — некоторое поле алгебраических чисел, E — векторное пространство конечной размерности над k и L — некоторая k-решетка в E. Для каждой конечной точки v поля k пусть L_v — замыкание решетки L в E_v и M_v —произвольная k_v- решетка в E_v. Тогда k-решетка M в E, замыкание которой в E_v совпадает с M_v при всех v, существует в том и только том случае, когда $M_v = L_v$ почти для всех v; при этом существует только одна такая k-решетка; она задается равенством*

$$M = \bigcap_v (E \cap M_v).$$

Предположим, что такая k-решетка M существует. Тогда ввиду предложения 4 равенство $M_v = L_v$ почти для всех v есть простая переформулировка следствия 1 теор. 3 п. 16.3.1. Предположим теперь, что $M_v = L_v$ почти для всех v. В силу предложения 1 п. 16.4.1 отсюда следует открытость множества $E_\infty \times \prod M_v$ в E_A. Поэтому к $G = E_{\mathbf{A}}$, $G' = E_\infty$, $G'' = \prod M_v$, $\Gamma = \varphi_E(E)$, где $\varphi_E\colon E \to E_{\mathbf{A}}$ — каноническое вложение, можно применить лемму 1. Ясно, что если положить $M = \bigcap (E \cap M_v)$, то $\varphi_E(M)$ совпадает с $\varphi_E(E) \cap G_1$, где $G_1 = G' \times G''$. По лемме 1 M является **R**-решеткой в E_∞ и, следовательно, **Q**-решеткой в E. Так как, очевидно, M есть $\mathfrak{r}$-модуль, то M является k-решеткой. По следствию 2 теор. 3 п. 16.4.2 группа $E_\infty + \varphi_E(E)$ плотна в E_A, поэтому ее пересечение $E_\infty + \varphi_E(M)$ с G_1 плотно в G_1. Другими словами, проекция $\varphi_E(M)$ на $G'' = \prod M_v$ плотна там; следовательно, решетка M плотна в M_v для каждой точки v. Как и выше, обозначим через ψ_M каноническое вложение $M \to \prod M_v$. Предположим, далее, что существует другая k-решетка M' в E с замыканиями M_v в E_v для всех v. Ясно, что $M' \subset M$. Кроме того, согласно предложению 4, образ $\psi_M(M')$ плотен в $\prod M_v$, а следовательно, и в $\psi_M(M)$. По предложению 1 существует такое целое число $m > 0$, что $M' \supset mM$. Обозначим

через G_m образ G_1 при автоморфизме $e \to \varphi(m)\, e$ пространства E_A. Можно записать G_m в виде $G_m = G' \times G''_m$, где $G''_m = \prod (mM_v)$. Ясно, что $mM_v = M_v$ почти для всех v (а именно для всех конечных точек поля k, которые не лежат над простыми делителями числа m в $\mathbf{Z}$) и G''_m является открытой подгруппой в G''. Далее, $\varphi_E(mM)$ совпадает с $\varphi_E(E) \cap G_m$, а следовательно, и с $\varphi_E(M) \cap G_m$ и содержится в $\psi_M(M')$. Другими словами, $\psi_M(M) \cap G''_m \subset \psi_M(M')$. Возьмем теперь произвольный элемент $\mu \in M$. Так как группа $\psi_M(M')$ плотна в $\psi_M(M)$, то существует такой элемент $\mu' \in M'$, что $\psi_M(\mu - \mu') \in G''_m$. Тогда $\psi_M(\mu - \mu') \in \psi_M(M')$, так что $\mu - \mu' \in M'$ и $\mu \in M'$. Это рассуждение показывает, что $M = M'$. Доказательство теоремы закончено.

Следствие. *Пусть L, L' — две k-решетки в E. Тогда $L + L'$ и $L \cap L'$ являются k-решетками в E и для каждой конечной точки v поля k замыкания этих решеток в E_v выражаются через замыкания L_v, L'_v решеток L, L' формулами*

$$(L + L')_v = L_v + L'_v, \quad (L \cap L')_v = L_v \cap L'_v.$$

Утверждения о $L + L'$ следуют из предложения 4. Рассмотрим пересечение $L \cap L'$. Положим $M_v = L_v \cap L'_v$. Для каждой точки v это—k_v-решетка в E_v, и M_v совпадает с L_v почти для всех v. Поэтому существует k-решетка M в E с замыканием M_v в E_v для каждой v, и M задается как $\cap (E \cap M_v)$. Но по теореме 2 последнее множество совпадает с $L \cap L'$.

16.5.3. Идеалы

В этом параграфе через k будет обозначаться некоторое поле алгебраических чисел и через $\mathfrak{r}$ — максимальный порядок в k. Результаты п.16.5.2 будут применяться к случаю $E = k$. Ясно, что отличный от $\{0\}$ $\mathfrak{r}$-модуль в k является k-решеткой в том и только том случае, когда он конечно порожден. Согласно предложению 1 п.16.5.1, для любой k-решетки $\mathfrak{a}$ в k существует такое целое число $m > 0$, что $m\mathfrak{a} \subset \mathfrak{r}$. Тогда, очевидно, $m\mathfrak{a}$ является идеалом в кольце $\mathfrak{r}$. Поэтому в силу следствия 2 предл. 1 п.16.5.1 каждый идеал в $\mathfrak{r}$, отличный от $\{0\}$, является k-решеткой. Отсюда видно, что подмножество в k является k-решеткой тогда и только тогда, когда оно имеет вид $\xi\mathfrak{a}$, где $\mathfrak{a}$ — идеал в $\mathfrak{r}$, отличный от $\{0\}$, а $\xi \in k^\times$.

Определение 4. *Всякую k-решетку в k будем называть дробным идеалом в k; дробный идеал в k будем называть целым, если он содержится в $\mathfrak{r}$.*

В соответствии с этим определением $\{0\}$ не является дробным идеалом.

Пусть $\mathfrak{a}$ —дробный идеал в k и L — некоторая k-решетка в конечномерном векторном пространстве E над k. Под $\mathfrak{a}L$ будем понимать подгруппу в E, порожденную всеми элементами вида αe, где $\alpha \in \mathfrak{a}$, $e \in L$. Ясно, что $\mathfrak{a}L$ является k-решеткой в E. Пусть v — произвольная конечная точка поля k. Обозначим, как выше, через $\mathfrak{a}_v$ замыкание $\mathfrak{a}$ в k_v и через L_v, $(\mathfrak{a}L)_v$—замыкания L, $\mathfrak{a}L$ в E_v. Согласно предложению 4 п.16.5.2, эти замыкания порождаются как r_v-модули соответственно множествами $\mathfrak{a}$ и L, $\mathfrak{a}L$. Отсюда ясно, что $(\mathfrak{a}L)_v$ совпадает с подгруппой $\mathfrak{a}_v L_v \subset E_v$, порожденной элементами αe с $\alpha \in \mathfrak{a}_v$, $e \in L_v$.

В частности, если $\mathfrak{a}$, $\mathfrak{b}$—два дробных идеала в k, то $\mathfrak{a}\mathfrak{b}$ есть подгруппа аддитивной группы поля k, порожденная элементами вида $\alpha\beta$, где $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$; $\mathfrak{a}\mathfrak{b}$ является дробным идеалом в k, и $(\mathfrak{a}\mathfrak{b})_v = \mathfrak{a}_v\mathfrak{b}_v$ для каждой конечной точки v поля k. Если p_v — максимальный идеал в r_v, то каждая k_v -решетка в k_v имеет вид p_v^n, где $n \in \mathbf{Z}$. В частности, можно записать $\mathfrak{a}_v = p_v^a$, $\mathfrak{b}_v = p_v^b$, где a, $b \in \mathbf{Z}$, и очевидно, что $\mathfrak{a}_v\mathfrak{b}_v = p_v^{a+b}$.

Теорема 3. *Пусть k — поле алгебраических чисел и $\mathfrak{r}$—его максимальный порядок. Для каждой конечной точки v поля k положим $\mathfrak{p}_v = \mathfrak{r} \cap p_v$. Тогда отображение $v \to \mathfrak{p}_v$ является биекцией множества конечных точек поля k на множество простых идеалов в $\mathfrak{r}$, отличных от $\{0\}$. Относительно операции $(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{a}\mathfrak{b}$ множество дробных идеалов в k является группой с нейтральным элементом $\mathfrak{r}$; это – свободная абелева группа, порожденная простыми идеалами в $\mathfrak{r}$; отличные от $\{0\}$ идеалы в $\mathfrak{r}$ образуют моноид, порожденный этими простыми идеалами.*

Для каждого дробного идеала $\mathfrak{a}$ в k запись $\mathfrak{a}_v = p_v^{a(v)}$ определяет отображение $v \to a(v)$ множества конечных точек поля k в $\mathbf{Z}$. Для $\mathfrak{a} = \mathfrak{r}$ все $a(v)$ равны нулю. Теорема 2 п.16.5.2 показывает, что заданному отображению $v \to a(v)$ тогда и только тогда соответствует некоторый дробный идеал $\mathfrak{a}$, когда $a(v) = 0$ почти для всех v, и что в случае когда это так, $\mathfrak{a}$ определен однозначно, а именно $\mathfrak{a} = \bigcap (k \cap p_v^{a(v)})$. Если $\mathfrak{b}$ соответствует аналогично отображению $v \to b(v)$, то, как показано выше, $\mathfrak{a}\mathfrak{b}$ соответствует отображению $v \to a(v) + b(v)$. Ясно также, что $\mathfrak{a} \subset \mathfrak{b}$ в том и только том случае, когда $a(v) \geqslant b(v)$ при всех v; в частности, дробный идеал $\mathfrak{a}$ цел тогда и только тогда, когда $a(v) \geqslant 0$ при всех v. Для любого заданного v положим $a(v) = 1$ и $a(v') = 0$ при всех $v' \neq v$ и обозначим через $\mathfrak{p}_v$ соответствующий идеал $\mathfrak{p}_v = \mathfrak{r} \cap p_v$. Ясно, что

дробные идеалы образуют свободную абелеву группу, порожденную идеалами $\mathfrak{p}_v$. Так как p_v — простой идеал в r_v, то $\mathfrak{p}_v$—простой идеал в $\mathfrak{r}$. Покажем теперь, что этими идеалами исчерпываются все ненулевые простые идеалы кольца $\mathfrak{r}$. Пусть $\mathfrak{a}$—произвольный идеал в $\mathfrak{r}$, так что $a(v) \geqslant 0$ при всех v. Если идеал $\mathfrak{a}$ отличен от $\mathfrak{r}$ и всех $\mathfrak{p}_v$, то мы можем записать его в виде $\mathfrak{a}'\mathfrak{a}''$, где $\mathfrak{a}'$, $\mathfrak{a}'$ — идеалы в $\mathfrak{r}$, отличные от $\mathfrak{r}$. Тогда $\mathfrak{a}'$ содержит $\mathfrak{a}$ и не совпадает с $\mathfrak{a}$, так что множество $\mathfrak{a}' - \mathfrak{a}$ непусто; то же самое справедливо для $\mathfrak{a}'' - \mathfrak{a}$. Возьмем элементы $\alpha' \in \mathfrak{a}' - \mathfrak{a}$ и $\alpha'' \in \mathfrak{a}'' - \mathfrak{a}$. Тогда $\alpha'\alpha'' \in \mathfrak{a}$, хотя ни α', ни α'' не лежат в $\mathfrak{a}$; следовательно, идеал $\mathfrak{a}$ не прост. Доказательство теоремы закончено.

Следствие 1. *Пусть* $\mathfrak{a}$, $\mathfrak{b}$ *—два дробных идеала в k. Для каждой точки v обозначим через a(v) и b(v) показатели степеней при* $\mathfrak{p}_v$ *в разложениях* $\mathfrak{a}$ *и* $\mathfrak{b}$ *в произведения степеней простых идеалов в* $\mathfrak{r}$. *Тогда* $\mathfrak{a} + \mathfrak{b}$ *и* $\mathfrak{a} \cap \mathfrak{b}$ *являются дробными идеалами в k, и показатели степеней при* $\mathfrak{p}_v$ *в аналогичных разложениях этих идеалов равны соответственно* $\min(a(v), b(v))$ *и* $\max(a(v), b(v))$.

Это вытекает из теоремы 3 и следствия теор. 2 п.16.5.2.

Как обычно, два идеала $\mathfrak{a}$, $\mathfrak{b}$ в $\mathfrak{r}$ называются взаимно простыми, если $\mathfrak{a} + \mathfrak{b} = \mathfrak{r}$.

Следствие 2. *Каждый дробный идеал* $\mathfrak{a}$ *в k может быть одним и только одним способом записан в виде* $\mathfrak{b}\mathfrak{c}^{-1}$, *где* $\mathfrak{b}$ *и* $\mathfrak{c}$ *—взаимно простые идеалы в* $\mathfrak{r}$.

Это следует из теоремы 3 и следствия 1.

По аналогии со случаем $k = \mathbf{Q}$ идеалы $\mathfrak{b}$, $\mathfrak{c}$ из следствия 2 называются соответственно *числителем* и *знаменателем* дробного идеала $\mathfrak{a}$.

Группу дробных идеалов поля k будем обозначать через $I(k)$. Если $a = (a_v)$ — произвольный элемент из $k_{\mathbf{A}}^{\times}$, то по следствию предл. 2 п.16.4.3 $|a_v|_v = 1$ и, значит, $a_v r_v = r_v$ почти для всех конечных точек v поля k. Поэтому по теореме 3 существует один и только один дробный идеал $\mathfrak{a}$ в k, такой, что $\mathfrak{a}_v = a_v r_v$ для всех конечных точек v; обозначим этот идеал через $\mathrm{id}(a)$. Отображение $a \to \mathrm{id}(a)$ группы $k_{\mathbf{A}}^{\times}$ в $I(k)$, очевидно, сюръективно. Обозначим через Ω_∞ ядро этого отображения, которое, очевидно, равно $k_\infty^{\times} \times (\prod r_v^{\times})$, т. е. $k_{\mathbf{A}}(P_\infty)^{\times}$ в обозначениях следствия предложения 2 п. 16.4.3 и $\Omega(P_\infty)$ в обозначениях формулы (5) п. 16.4.4. Так как подгруппа Ω_∞ открыта в $k_{\mathbf{A}}^{\times}$, то отображение $a \to \mathrm{id}(a)$ есть морфизм группы $k_{\mathbf{A}}^{\times}$ на группу $I(k)$, наделенную дискретной топологией. Таким образом, можно отождествить $I(k)$ с $k_{\mathbf{A}}^{\times}/\Omega_\infty$.

В частности, для каждого $\xi \in k^{\times}$ имеем $\mathrm{id}(\xi) = \xi\mathfrak{r}$. Этот $\mathfrak{r}$-

модуль, порожденный элементом ξ в k, часто обозначается через (ξ), а его числитель и знаменатель, определенные выше, называются *числителем* и *знаменателем* элемента ξ. Дробный идеал называется *главным,* если он имеет вид $\xi\mathfrak{r}$, где $\xi \in k^{\times}$. Главные идеалы образуют подгруппу $P(k)$ в $I(k)$, которая является образом группы $k^{\times}$ относительно морфизма, индуцированного отображением $a \to \mathrm{id}\,(a)$. Отождествляя $I(k)$ с факторгруппой $k_{\mathbf{A}}^{\times}/\Omega_{\infty}$, мы видим, что $P(k)$ совпадает с образом группы $k^{\times}$ в этой факторгруппе. Поэтому можно отождествить $I(k)/P(k)$ с группой $k_{\mathbf{A}}^{\times}/k^{\times}\Omega_{\infty}$, которая конечна по теореме 7 п. 16.4.4. Элементы группы $I(k)/P(k)$, другими словами, смежные классы в $I(k)$ по модулю $P(k)$, известны как *классы идеалов* поля k. Число этих классов, т. е. индекс подгруппы $P(k)$ в $I(k)$, будет обозначаться через h.

Теорема 4. *Пусть k — поле алгебраических чисел, E — конечномерное векторное пространство над k и L, M — две k-решетки в E, такие, что $L \supset M$. Для каждой конечной точки v поля k обозначим через L_v, M_v замыкания решеток L, M в E_v и через λ_v — естественный гомоморфизм $L/M \to L_v/M_v$. Тогда отображение $x \to (\lambda_v(x))$, где v пробегает все конечные точки поля k, является изоморфизмом $\mathfrak{r}$-модулей*

$$L/M \to \prod_v (L_v/M_v).$$

Здесь $\mathfrak{r}$ — максимальный порядок в k.

Обозначим рассматриваемое отображение через λ. Очевидно, оно является гомоморфизмом $\mathfrak{r}$-модулей. Пусть x — любой элемент из L/M и e — его представитель в L. Если $\lambda(x) = 0$, то e должен лежать в M_v при всех v. По теореме 2 п.16.5.2 отсюда следует, что $e \in M$ и $x = 0$. Поэтому гомоморфизм λ инъективен. Возьмем теперь любой элемент $y = (y_v) \in \prod (L_v/M_v)$ и для каждого v представитель $e_v \in L_v$ элемента y_v. Положим $e = (e_v)$. Так как $M_v = L_v$ почти для всех v, то подгруппа $\prod M_v$ открыта в $\prod L_v$. Поэтому, согласно предложению 4 п.16.5.2, существует такой элемент $e_0 \in L$, что $\psi_L(e_0) - e \in \prod M_v$, где ψ_L обозначает каноническое вложение $L \to \prod L_v$. Другими словами, если x_0 — образ элемента e_0 в L/M, то $\lambda(x_0) = y$, чем доказана сюръективность гомоморфизма λ.

Следствие 1. *В обозначениях и предположениях теоремы* 4
$[L : M] = \prod [L_v : M_v]$.

Это очевидно. Следует заметить, что $L_v = M_v$ почти для всех v и M_v является открытой подгруппой компактной группы L_v, так что число $[L_v : M_v]$ всегда конечно и почти всегда равно 1. Конечность

индекса $[L : M]$ неявно содержится в предложении 1 п.16.5.1, а также в лемме 2 п.16.2.4.

Следствие 2. *Пусть v — конечная точка поля k, и пусть $\mathfrak{p}_v = \mathfrak{r} \cap p_v$ — соответствующий точке v простой идеал в максимальном порядке $\mathfrak{r}$ поля k. Тогда естественный гомоморфизм $\mathfrak{r}/\mathfrak{p}_v \to r_v/p_v$ является изоморфизмом кольца $\mathfrak{r}/\mathfrak{p}_v$ на поле вычетов r_v/p_v кольца r_v.*

Следствие 3. *Пусть $\mathfrak{a}$, $\mathfrak{b}$—два дробных идеала в k, $\mathfrak{a} \supset \mathfrak{b}$, и пусть $\mathfrak{a}^{-1}\mathfrak{b} = \prod \mathfrak{p}_v^{n(v)}$ —разложение дробного идеала $\mathfrak{a}^{-1}\mathfrak{b}$ в произведение степеней простых идеалов кольца $\mathfrak{r}$. Тогда $[\mathfrak{a} : \mathfrak{b}] = \prod [\mathfrak{r} : \mathfrak{p}_v]^{n(v)}$.*

По следствию 1 индекс $[\mathfrak{a} : \mathfrak{b}]$ равен произведению индексов $[\mathfrak{a}_v : \mathfrak{b}_v]$ по всем v. Для данного v можно записать $\mathfrak{a}_v = p_v^a$, $\mathfrak{b}_v = p_v^b$. Поэтому

$$b - a = n(v).$$

Следствие 2 теор. 6 п.16.1.4 показывает, что $[p_v^a : p_v^b] = q^{b-a}$, где $q = [r_v : p_v]$. Отсюда и из следствия 2 вытекает наше утверждение.

Определение 5. *Пусть k—некоторое поле алгебраических чисел, $\mathfrak{r}$—его максимальный порядок и $\mathfrak{a} \to \mathfrak{N}(\mathfrak{a})$—такой гомоморфизм группы дробных идеалов поля k в $\mathbf{Q}^\times$, что $\mathfrak{N}(\mathfrak{p}) = [\mathfrak{r} : \mathfrak{p}]$ для всех простых идеалов $\mathfrak{p}$ в $\mathfrak{r}$. Тогда число $\mathfrak{N}(\mathfrak{a})$ называется нормой дробного идеала $\mathfrak{a}$ в k.*

Следствие 3 теор. 5 можно теперь переформулировать следующим образом: если $\mathfrak{a}$, $\mathfrak{b}$—дробные идеалы в k и $\mathfrak{a} \supset \mathfrak{b}$, то $[\mathfrak{a} : \mathfrak{b}] = \mathfrak{N}(\mathfrak{b})/\mathfrak{N}(\mathfrak{a})$. В частности, если $\mathfrak{a}$ цел, то $[\mathfrak{r} : \mathfrak{a}] = \mathfrak{N}(\mathfrak{a})$.

Предложение 5. *Пусть $a = (a_v)$— произвольный элемент из $k_{\mathbf{A}}^\times$. Тогда $\mathfrak{N}(\mathrm{id}(a)) = \prod |a_v|_v^{-1}$, где произведение берется по всем конечным точкам поля k.*

В силу определения 5 достаточно проверить это равенство в случае, когда $\mathrm{id}(a)$ — простой идеал в $\mathfrak{r}$, т. е. когда a_v — простой элемент в k_v для некоторой конечной точки v и $|a_{v'}|_{v'} = 1$ для всех конечных точек $v' \neq v$ поля k. Но в этом случае равенство очевидно.

Следствие 1. *Для всякого элемента $\xi \in k^\times$ имеет место равенство $\mathrm{N}_{k/\mathbf{Q}}(\xi) = (-1)^\rho \mathfrak{N}(\mathrm{id}(\xi))$, где ρ — число вещественных точек w поля k, для которых образ элемента ξ в k_w строго отрицателен.*

Комбинируя предложение 5 с теоремой 5 п. 16.4.4, получаем, что норма $\mathfrak{N}(\mathrm{id}(\xi))$ равна произведению $\prod |\xi_w|_w$, взятому по бесконечным точкам w поля k.

Для всякой вещественной точки w поля k и всякого $x \in k_w^*$ имеем $x = (\text{sign } x) \cdot |x|_w$; для всякой мнимой точки w поля k и всякого $x \in k_w^\times$ имеем $N_{k_w/\mathbf{R}}(x) = x\bar{x} = |x|_w$. Наше утверждение вытекает теперь из следствия 3 теор. 4 п. 16.3.4, примененного к k, **Q** и точке ∞ поля **Q**.

Следствие 2. *Элемент* ξ *максимального порядка* $\mathfrak{r}$ *поля* k *обратим в* $\mathfrak{r}$ *тогда и только тогда, когда* $N_{k/\mathbf{Q}}(\xi) = \pm 1$.

Ясно, что ξ обратим в $\mathfrak{r}$, тогда и только тогда, когда $\xi\mathfrak{r} = \mathfrak{r}$. Так как $\xi\mathfrak{r}$— это то же самое, что $\mathrm{id}(\xi)$, то наше утверждение вытекает из следствия 1 и того факта, что $|\mathfrak{r} : \mathfrak{a}| = \mathfrak{N}(\mathfrak{a})$ для каждого идеала $\mathfrak{a}$ в кольце $\mathfrak{r}$.

Элементы группы $\mathfrak{r}^\times$, т. е. обратимые элементы кольца $\mathfrak{r}$, называются по традиции «единицами» в k. В обозначениях п. 16.4.4 $\mathfrak{r}^\times = E(P_\infty)$; структура этой группы описывается теоремой 9 п. 16.4.4: если число бесконечных точек поля k равно $r + 1$, то группа $\mathfrak{r}^\times$ изоморфна прямому произведению циклической группы E всех корней из 1 в k и группы, изоморфной $\mathbf{Z}^r$. Это — «теорема об единицах» Дирихле.

16.5.4. Фундаментальные множества

Пусть Γ — дискретная подгруппа в локально компактной группе G. Под *фундаментальным множеством в* G относительно Γ по традиции понимается полное множество X представителей классов смежности группы G по модулю Γ, причем требуется, чтобы X было измеримо, и обычно предполагается, что X обладает некоторыми дополнительными свойствами, например является борелевским множеством и т. п. Тогда формула 6 п.16.2.4, примененная к G, к Γ, к мере Хаара α на G и к характеристической функции множества X, показывает, что $\alpha(X) = \alpha(G/\Gamma)$. Таким образом, меру $\alpha(G/\Gamma)$ иногда можно эффективно вычислить с помощью построения подходящего фундаментального множества. Более общим образом, назовем измеримое подмножество X в G *фундаментальным порядка* ν относительно Γ, если оно содержит в точности ν точек из каждого смежного класса по модулю Γ; тогда та же самая формула дает $\alpha(X) = \nu\alpha(G/\Gamma)$. Применим теперь все это к случаям $G = k_\mathbf{A}$ и $G = k_\mathbf{A}^\times$.

Пусть k и $\mathfrak{r}$ такие, как выше, и n — степень поля k над **Q**. Так как $\mathfrak{r}$ является **Q**-решеткой в k, рассматриваемом как векторное пространство над **Q**, то, согласно предложению 11 п. 16.2.4, $\mathfrak{r}$

порождается некоторым базисом $\{\xi_1, \ldots, \xi_n\}$ в k над $\mathbf{Q}$. Поэтому этот базис является также базисом в $k_\infty = k \otimes_{\mathbf{Q}} \mathbf{R}$ над $\mathbf{R}$. Следовательно, положив $\theta(u) = \sum u_i \xi_i$ для $u = (u_1, \ldots, u_n) \in \mathbf{R}^n$, мы определим изоморфизм $\theta\colon \mathbf{R}^n \to k_\infty$.

Предложение 6. *Пусть k, $\mathfrak{r}$ и θ такие, как выше; обозначим через I интервал $0 \leqslant t < 1$ в $\mathbf{R}$. Тогда множество $\theta(I^n) \times \prod_v r_v$, где произведение взято по всем конечным точкам v поля k, является фундаментальным множеством в k_A относительно k.*

Обозначим рассматриваемое множество через X. Оно, очевидно, измеримо. Нам надо показать, что каждый элемент $x \in k_\mathbf{A}$ может быть записан одним и только одним способом в виде $x_0 + \xi$, где $x_0 \in X$ и $\xi \in k$. По следствию 2 теор. 3 п.16.4.2 группа $k_\infty + k$ плотна в k_A. Следовательно, поскольку подгруппа $k_\infty \times \prod r_v$ открыта, для любого $x \in k_\mathbf{A}$ существует такой $\eta \in k$, что $x - \eta \in k_\infty \times \prod r_v$. Из определения $\mathfrak{r}$ видно, что элемент $\eta' \in k$ обладает таким же свойством тогда и только тогда, когда $\eta' - \eta \in \mathfrak{r}$. Полагая $y = x - \eta$ и обозначая через y_∞ проекцию этого элемента из произведения $k_\infty \times \prod r_v$ на k_∞, можно записать $y_\infty = \theta(u)$, где $u = (u_1, \ldots, u_n) \in \mathbf{R}^n$. Для каждого i найдем такое $a_i \in \mathbf{Z}$, что $a_i \leqslant u_i < a_i + 1$, т. е. $u_i - a_i \in I$. Положим $\xi = \eta - \sum_i a_i \xi_i$ и $x_0 = x - \xi$. Так как $\xi - \eta \in \mathfrak{r}$, то $x_0 \in k_\infty \times \prod r_v$. Далее, проекция элемента x_0 на k_∞ равная

$$y_\infty - \sum_i a_i \xi_i = \sum_i (u_i - a_i) \xi_i,$$

лежит в $\theta(I^n)$. Ясно также, что последнее условие не будет выполняться ни при каком другом выборе целых чисел a_i. Тем самым наше утверждение доказано.

Предложение 6 будет сейчас использовано для вычисления меры $\alpha(k_\mathbf{A}/k)$ для явно заданной меры Хаара α на k_A. Такую меру можно построить следующим образом. Для каждой точки v поля k выберем меру Хаара α_v на k_v. Если $\alpha_v(r_v) = 1$ почти для всех v, то произведение мер $\prod \alpha_v$ корректно определено и является мерой Хаара на каждой из открытых подгрупп $k_\mathbf{A}(P) \subset k_\mathbf{A}$, определенных формулой (1) п.16.4.1. Ясно, что существует одна и только одна мера Хаара на k_A, которая совпадает с этими мерами на их областях определения и которую мы будем обозначать через $\prod \alpha_v$. В частности, обозначим через β меру Хаара $\prod \beta_v$, которая получается, если взять $\beta_v(r_v) = 1$ для всех конечных точек v поля k, а для

бесконечных точек определить меру следующим образом. Если w — вещественная точка, то пусть β_w — мера Лебега на $k_w = \mathbf{R}$, т. е. $d\beta_w(x) = dx$. Если же w — мнимая точка, то меру β_w на $k_w = \mathbf{C}$ выберем так, чтобы $d\beta_w(x) = |dx \wedge d\bar{x}|$; это означает, что если мы положим $x = u + iv$, где $u, v \in \mathbf{R}$, так что $dx \wedge d\bar{x} = -2i(du \wedge dv)$, то β_w, есть мера, соответствующая дифференциальной форме $2du \wedge dv$; другими словами, $\beta_w/2$ есть мера Лебега на плоскости u, v.

Для вычисления $\beta(k_A/k)$ нам понадобится еще одно определение. В уже много раз применявшихся выше обозначениях рассмотрим матрицу

$$M = (\mathrm{Tr}_{k/\mathbf{Q}}(\xi_i \xi_j))_{1 \leqslant i,j \leqslant n} \qquad (1)$$

и обозначим через D ее определитель. По предложению 5 п.16.3.3 $D \neq 0$; по предложению 3 п.16.5.1 $M \in M_n(\mathbf{Z})$, так что $D \in \mathbf{Z}$. Если $k = \mathbf{Q}$, то $\mathfrak{r} = \mathbf{Z}$, так что $\xi_1 = \pm 1$ и, следовательно, $D = 1$. Если $\{\eta_1, \ldots, \eta_n\}$ — другое множество образующих для $\mathfrak{r}$ и N — матрица, полученная заменой в (1) ξ_i на η_i, то можно записать $\eta_i = \sum a_{ij}\xi_j$, где $a_{ij} \in \mathbf{Z}$ при всех i, j. Тогда $N = AM^tA$, где A — матрица (a_{ij}). Аналогично можно записать $\xi_i = \sum b_{ij}\eta_j$, где $b_{ij} \in \mathbf{Z}$ при всех i, j. Обозначая через B матрицу (b_{ij}), получаем $AB = 1$; следовательно, $\det(A) \det(B) = 1$. Так как $\det(A)$ и $\det(B)$ лежат в $\mathbf{Z}$, отсюда вытекает, что $\det(A) = \pm 1$, значит $\det(N) = \det(M)$. Другими словами, определитель D матрицы M не зависит от выбора базиса. Этим оправдано следующее

Определение 6. *Пусть k и $\{\xi_1, \ldots, \xi_n\}$ таковы, как выше. Тогда определитель D матрицы M, задаваемой формулой* (1), *называется дискриминантом поля k.*

Предложение 7. *Пусть $\beta = \prod \beta_v$ — мера Хаара на k_A, причем $\beta_v(r_v) = 1$ для всех конечных точек v, $d\beta_w(x) = dx$ для всех вещественных точек w и $d\beta_w(x) = |dx \wedge d\bar{x}|$ для всех мнимых точек w поля k. Тогда $\beta(k_A/k) = |D|^{1/2}$, где D — дискриминант поля k.*

Обозначим через β_∞ меру $\prod \beta_w$ на $k_\infty = \prod k_w$, где произведения берутся по всем бесконечным точкам w поля k. По предложению 6 $\beta(k_A/k)$ совпадает с $\beta_\infty(\theta(I^n))$, поэтому наше предложение будет доказано, если мы покажем, что

$$d\beta_\infty(\theta(u)) = |D|^{1/2} du_1 \ldots du_n.$$

Обозначим через r_1 и r_2 соответственно число вещественных и мнимых точек поля k и положим $r = r_1 + r_2 - 1$. Пусть $w_0, \ldots, w_r$ — бесконечные точки поля k, упорядоченные так, что точка w_i вещественна при $i < r_i$ и мнима при $i \geqslant r_1$. Для каждого i обозначим через k_i пополнение поля k относительно w_i, через λ_i — естественное вложение $k \to k_i$ и через μ_i — $\mathbf{R}$-линейное продолжение вложения λ_i на k_∞. Если, как это было сделано выше, отождествить k_∞ с $\prod k_i$, то теорема 4 п. 16.3.4 показывает, что μ_i является проекцией из k_∞ на k_i. По следствию 1 предл. 3 п.16.3.2 каждое изоморфное вложение $\lambda' : k \to \mathbf{C}$ имеет вид $\sigma \circ \lambda_i$, где σ — некоторый R-линейный изоморфизм поля k_i в $\mathbf{C}$; очевидно, что если $k_i = \mathbf{R}$, т. е. если $i < r_1$, то σ есть естественное вложение поля k_i в $\mathbf{C}$, а если $k_i = \mathbf{C}$, т. е. $i \geqslant r_1$, то σ — это одно из двух отображений $x \to x$ или $x \to \bar{x}$ поля $\mathbf{C}$ на $\mathbf{C}$. Поэтому, если положить $\lambda'_i = \lambda_i$ при $0 \leqslant i \leqslant r$ и $\lambda'_{r_2+i} = \bar{\lambda}_i$ при $r_1 \leqslant i \leqslant r$, то вложениями λ'_h, $0 \leqslant h \leqslant n-1$, будут исчерпываться все различные изоморфизмы поля k в $\mathbf{C}$. Обозначая теперь $\mathbf{R}$-линейное продолжение вложения λ'_h на k_∞ через μ'_h, имеем

$$\mu'_h(\theta(u)) = \sum_{i=1}^{n} \lambda'_h(\xi_i)\, u_i,$$

где $u = (u_1, \ldots, u_n) \in \mathbf{R}^n$ и $0 \leqslant h \leqslant n-1$. Обозначим через N матрицу коэффициентов $(\lambda'_h(\xi_i))$ в правой части равенства. Согласно следствию 3 предложения 4 п. 16.3.3, $\mathrm{Tr}_{k/\mathbf{Q}}(\xi) = \sum \lambda'_h(\xi)$ при всех $\xi \in k$; поскольку λ'_h суть изоморфизмы, отсюда вытекает, что

$$M = \left(\sum_h \lambda'_h(\xi_i)\, \lambda'_h(\xi_j)\right) = {}^tN \cdot N,$$

следовательно, $D = \det(N)^2$. В то же время во внешней алгебре дифференциальных форм на $\mathbf{R}^n$ выполняются соотношения

(2)

$$\prod_h d\mu'_h(\theta(u)) = \pm \prod_{0 \leqslant i < r_1} d\mu_i(\theta(u)) \wedge$$
$$\wedge \prod_{r_1 \leqslant j \leqslant r} (d\mu_j(\theta(u)) \wedge d\bar{\mu}_j(\theta(u))) = \pm \det(N)\, du_1 \wedge \ldots \wedge du_n.$$

Ввиду определения мер β_w доказательство предложения 7 закончено. Можно заметить, что если умножить (2) на i^{r_2}, то получится вещественная дифференциальная форма на $\mathbf{R}^n$. Поэтому $i^{r_2} \det(N)$ — вещественное число; другими словами, $(-1)^{r_2} D > 0$.

Следствие 1. *Если* $k \neq \mathbf{Q}$, *то* $|D| > 1$.

Придерживаясь введенных выше обозначений, для $0 \leqslant i \leqslant r$ выберем $c_i \in \mathbf{R}_+^\times$ и обозначим через $Y(c)$ множество таких элементов

$y = (y_v) \in k_{\mathbf{A}}$, что $| y_v |_v \leqslant 1$ для всех конечных точек v поля k и $| y_{w_i} |_{w_i} \leqslant c_i/2$ при $0 \leqslant i \leqslant r$. Для каждой бесконечной точки w и каждого $c \in \mathbf{R}_+^\times$ подмножество в k_w, задаваемое неравенством $| x |_w \leqslant c/2$, является интервалом длины c, если w — вещественная точка, и кругом β_w-меры πc, если w — мнимая точка. С учетом определения β это дает $\beta(Y(c)) = \pi^{r_2} \prod c_i$. Если это число больше, чем $| D |^{1/2}$, то лемма 1 п.16. 2.4 в сочетании с предложением 7 показывает, что существуют такие $y,\ y' \in Y(c)$, что $\eta = y - y' \in k^\times$. Тогда $| \eta |_v \leqslant 1$ для всех конечных точек v поля k, $(\eta)_{w_i} \leqslant c_i$, если w_i — вещественная точка, и, очевидно, $| \eta |_{w_i} \leqslant 2c_i$, если w_i — мнимая точка. Отсюда ввиду теоремы 5 п. 16.4.4 вытекает, что $2^{r_2} \prod c_i \geqslant 1$. Предположим, что $r_2 > 0$. Тогда если бы $| D | = 1$, то, выбрав c_i так, чтобы $\prod c_i$ было $> \pi^{-r_2}$ и $< 2^{-r_2}$, мы получили бы противоречие. Теперь предположим, что $r_2 = 0$, так что $r_1 = n$, и $| D | = 1$. Тогда при любом выборе c_i, удовлетворяющем условию $\prod c_i > 1$, существует $\eta \in k^\times$ с указанными выше свойствами. Ясно, что множество элементов $x = (x_v) \in k_{\mathbf{A}}$, таких, что $| x_v |_v \leqslant 1$ для всех конечных точек v и $| x_w |_w \leqslant 2$ для всех бесконечных точек w, компактно и потому содержит лишь конечное число элементов $\eta_1, \ldots, \eta_N$ поля k. Следовательно, можно выбрать $c' > 1$ так, чтобы ни одно из η_ν не удовлетворяло неравенствам $1 \leqslant | \eta_\nu |_{w_0} \leqslant c'$. Выберем теперь c_i так, чтобы выполнялись неравенства $\prod c_i > 1$, $1 < c_0 < c'$, $c_0 < 2$ и $c_i < 1$ при $1 \leqslant i \leqslant n-1$. Тогда существует $\eta \in k^\times$, для которого $| \eta |_{w_i} \leqslant c_i$ при $0 \leqslant i \leqslant n-1$ и $| \eta |_v \leqslant 1$ для всех конечных точек v. Ввиду нашего выбора c' и c_i отсюда следует, что $| \eta |_{w_i} < 1$ при $i > 0$ и $| \eta |_{w_0} \leqslant 1$. Но если $n \neq 1$, это противоречит теореме 5 п. 16.4.4.

Следствие 2. *Существует лишь конечное число полей алгебраических чисел заданной степени n над* $\mathbf{Q}$ *и с заданным дискриминантом D.*

Поскольку это утверждение нигде в дальнейшем не используется, мы дадим лишь набросок доказательства. Рассуждая точно так же, как выше, мы видим, что существует такое число $\eta \in k^\times$, что $| \eta |_v \leqslant 1$ для всех конечных точек v поля k и $| \eta |_w < 1$ для всех бесконечных точек w, кроме одной такой точки w_0, причем образ $\lambda_0(\eta)$ числа η в k_{w_0} лежит в интервале $| x | \leqslant 2 | D |^{1/2}$, если точка w_0 вещественна, и в прямоугольнике, задаваемом неравенствами $| u | \leqslant 1$, $| v | \leqslant | D |^{1/2}$, $x = u + iv$, если точка w мнима. Поскольку должно выполняться неравенство $| \eta |_{w_0} > 1$, из

последнего условия следует, что число $\lambda_0(\eta)$ невещественно, если точка w_0 мнима. Отсюда вытекает, что $k = \mathbf{Q}(\eta)$. Действительно, в противном случае обозначим через u точку поля $\mathbf{Q}(\eta)$, лежащую под w_0; тогда $|\eta|_w \geqslant 1$ для всех точек w поля k, лежащих над u, если таких точек больше одной, и число $\lambda_0(\eta)$ должно быть вещественным, если точка u вещественна, а w_0 мнима; поскольку это не так, следствие 1 теор. 4 п.16.3.4 показывает, что степень k над $\mathbf{Q}(\eta)$ не может быть больше 1. Отсюда следует, что все $\lambda'_h(\eta)$, $0 \leqslant h \leqslant n-1$, различны, так что $\prod(x - \lambda'_h(\eta))$ — неприводимый многочлен в $\mathbf{Q}[x]$ со старшим коэффициентом 1 и с корнем η. Коэффициенты этого многочлена, очевидно, ограничены по модулю некоторым числом, зависящим от $|D|$; все они лежат в $\mathbf{Z}$, ибо $|\eta|_v \leqslant 1$ для всех конечных точек v поля k, другими словами, $\eta \in \mathfrak{r}$, т. е. элемент η цел над $\mathbf{Z}$. Поэтому таких многочленов, а следовательно, и чисел η, может быть при заданном D лишь конечное число.

Теперь мы рассмотрим соответствующие вопросы для $k_{\mathbf{A}}^{\times}/k^{\times}$. Как и выше, обозначим через Ω_∞ ядро отображения $a \to \mathrm{id}(a)$. Это не что иное, как группа $k_\infty^{\times} \times \prod r_v^{\times} \subset k_{\mathbf{A}}$, или $\Omega(P_\infty)$ в обозначениях п.16. 4.4. Будем писать Ω_1 вместо $\Omega_1(P_\infty)$ для обозначения $\Omega_\infty \cap k_{\mathbf{A}}^1$. Как и в п. 16.4.4, обозначим через U группу таких элементов $(z_v) \in k_{\mathbf{A}}^{\times}$, что $|z|_v = 1$ для всех точек v, конечных и бесконечных; это компактная подгруппа в Ω_1. Как было отмечено в п. 16.5.3, $\mathfrak{r}^{\times}$ совпадает с группой, обозначавшейся в п. 16.4.4 через $E(P_\infty)$. По-прежнему будем обозначать через E циклическую группу корней из 1 в k. Запишем опять бесконечные точки $w_0, \ldots, w_r$ поля k в каком-нибудь порядке. Для каждого аделя $z = (z_v) \in \Omega_\infty$ положим

$$l(z) = (\log(|z_{w_0}|_{w_0}, \ldots, \log(|z_{w_r}|_{w_r})). \tag{3}$$

Отображение $l\colon \Omega_\infty \to \mathbf{R}^{r+1}$, определенное формулой (3), является, очевидно, морфизмом (мультипликативно записываемой) группы Ω_∞ на (аддитивно записываемую) группу $\mathbf{R}^{r+1}$; ядро этого морфизма совпадает с U. Пусть λ — линейная форма на $\mathbf{R}^{r+1}$, задаваемая равенством $\lambda(x) = \sum x_i$, где $x = (x_0, \ldots, x_r)$. Тогда $\log(|z|_{\mathbf{A}}) = \lambda(l(z))$ при $z \in \Omega_\infty$. Поэтому если H — гиперплоскость в $\mathbf{R}^{r+1}$, определяемая уравнением $\lambda(x) = 0$, то множество $l^{-1}(H)$, являющееся ядром отображения $\lambda \circ l$, совпадает с Ω_1 и l индуцирует морфизм из Ω_1 на H с ядром U. Этот морфизм мы можем использовать для отождествления группы $G_1 = \Omega_1/U$ с векторным пространством H. Положим $\Gamma = l(\mathfrak{r}^{\times})$. По следствию теор. 9 п.16.4.4 Γ есть дискретная подгруппа в H, и факторгруппа H/Γ компактна; другими словами, Γ есть $\mathbf{R}$-решетка в H. Отсюда следует

(так же, как и при доказательстве теоремы 9 п. 16.4.4), что r элементов $\varepsilon_1, \ldots, \varepsilon_r$ из $\mathfrak{r}^\times$ будут свободными образующими для некоторой подгруппы в $\mathfrak{r}^\times$ тогда и только тогда, когда их образы $l(\varepsilon_i)$ в $\mathbf{R}^{r+1}$ образуют базис в H, и что $\mathfrak{r}^\times$ разлагается в прямое произведение подгруппы E и этой подгруппы в том и только в том случае, когда эти образы порождают группу Г; в этом случае будем говорить, что ε_i образуют *систему свободных образующих для* $\mathfrak{r}^\times$ *по модулю* E. Предположим теперь, что такая система образующих уже выбрана. Для $0 \leqslant i \leqslant r$ обозначим через δ_i степень поля k_{w_i} над $\mathbf{R}$; $\delta_i = 1$ или 2 в соответствии с тем, вещественна или мнима точка w_i. По следствию 2 теор. 4 п. 16.3.4 $\sum_i \delta_i = n$, т. е. $\lambda(\delta) = n$, если обозначить через δ вектор $(\delta_0, \ldots, \delta_r)$ в $\mathbf{R}^{r+1}$. Отсюда следует, что δ вместе с векторами $l(\varepsilon_i)$, $1 \leqslant i \leqslant r$, образует базис в $\mathbf{R}^{n+1}$, так что можно следующим образом определить автоморфизм F пространства $\mathbf{R}^{n+1}$:

$$t = (t_1, \ldots, t_r) \to F(t) = n^{-1} t_0 \delta + \sum_{i=1}^{n} t_i l(\varepsilon_i) \tag{4}$$

Имеем $\lambda(F(t)) = t_0$ и

$$l\left(\eta \prod_i \varepsilon_i^{n_i}\right) = F(0, n_1, \ldots, n_r), \tag{5}$$

где $\eta \in E$ и $(n_1, \ldots, n_r) \in \mathbf{Z}^r$.

Предложение 8. *Положим* $\Omega_\infty = k_\infty^\times \times \prod r_v^\times$, *и пусть* I *— морфизм из* Ω_∞ *на* $\mathbf{R}^{n+1}$, *задаваемый формулой* (3); $\{a_1, \ldots, a_h\}$ *— полное множество представителей смежных классов: по модулю* $k^\times \Omega_\infty$ *в* $k_\mathbf{A}^\times$; E *— группа всех корней из* 1 *в* k; e *— порядок этой группы;* $\{\varepsilon_1, \ldots, \varepsilon_r\}$ *— система свободных образующих: для* $\mathfrak{r}^\times$ *по модулю* E; F *— автоморфизм пространства* $\mathbf{R}^{r+1}$, *задаваемый формулой* (4), *и* I *— интервал* $0 \leqslant t < 1$ *в* $\mathbf{R}$. *Тогда объединение множеств* $a_i l^{-1}(F(\mathbf{R} \times I^r))$, $1 \leqslant i \leqslant h$, *является фундаментальным множеством порядка* e *в* $k_\mathbf{A}^\times$ *по модулю* $k^\times$.

Возьмем произвольный элемент $z = (z_v)$ в $k_\mathbf{A}^\times$. Существует один и только один индекс i, для которого $a_i^{-1} z \in k^\times \Omega_\infty$. Можно записать $z = a_i \xi z'$, где $\xi \in k^\times$, $z' \in \Omega_\infty$, причем элемент z' однозначно определен по модулю $k^\times \cap \Omega_\infty$, т. е. по модулю $\mathfrak{r}^\times$. Положим $F^{-1}(l(z')) = (t_0, \ldots, t_r)$. Для $1 \leqslant i \leqslant r$ возьмем такие $n_i \in \mathbf{Z}$, что $n_i \leqslant t_i < n_i + 1$. Положим $\varepsilon = \prod \varepsilon_i^{n_i}$, $z'' = \varepsilon^{-1} z'$ и $\varepsilon' = \xi\varepsilon$. Тогда $z = \xi' a_i z''$ и ввиду (4) и (5) $l(z'') \in F(\mathbf{R} \times I^r)$. Далее ясно, что этими условиями элемент z'' определен однозначно по модулю E. Доказательство предложения закончено.

Как мы видели в п.16.5.3, морфизм $z \to \mathrm{id}\,(z)$ из $k_{\mathbf{A}}^{\times}$ на $I\,(k)$ определяет изоморфизм группы $k_{\mathbf{A}}^{\times}/k^{\times}\Omega_{\infty}$ на группу $I\,(k)/P\,(k)$ классов идеалов поля k. Поэтому число h, фигурирующее в формулировке предложения 8, совпадает с порядком этой группы, и идеалы a_i из этого предложения могут быть охарактеризованы тем свойством, что дробные идеалы $\mathrm{id}\,(a_i)$ являются представителями классов идеалов поля k.

Теперь определим меру Хаара γ на $k_{\mathbf{A}}^{\times}$. Как и в случае $k_{\mathbf{A}}$, это можно сделать, выбрав для каждой точки v меру Хаара γ_v на $k_{\mathbf{A}}^{\times}$ так, чтобы $\gamma_v\,(r_v^{\times}) = 1$ почти для всех v, и потребовав, чтобы γ совпадала с $\prod \gamma_v$ на каждой группе $k_{\mathbf{A}}\,(P_{\infty})^{\times}$. Полученную меру γ будем обозначать через $\prod \gamma_v$. Как и в случае k_A, нам понадобится одно определение.

Определение 7. *Во введенных выше обозначениях пусть L — матрица, составленная из строчек $n^{-1}\delta$, $l\,(\varepsilon_1)$, . . ., $l\,(\varepsilon_r)$. Тогда $R = |\det(L)|$ называется регулятором поля k.*

Так как L является матрицей автоморфизма $F\colon \mathbf{R}^{n+1} \to \mathbf{R}^{n+1}$, задаваемого формулой (4), то F имеет определитель $\pm R$. Наше определение будет оправдано, если мы докажем независимость R от выбора ε_i. Это легко можно было бы сделать таким же способом, как и для дискриминанта. Но мы получим этот факт как следствие приводимого ниже предложения.

Предложение 9. *Пусть $\gamma = \prod \gamma_v$ — мера Хаара на $k_{\mathbf{A}}^{\times}$, где $\gamma_v\,(r_v^{\times}) = 1$ для всех конечных точек v поля k, $d\gamma_w\,(x) = |x|^{-1}\,dx$ для каждой вещественной точки w и $d\gamma_w\,(x) = (x\bar{x})^{-1}\,|dx \wedge d\bar{x}|$ для каждой мнимой точки w. Для каждого числа $m > 1$ в $\mathbf{R}$ обозначим через $C\,(m)$ образ в $k_{\mathbf{A}}^{\times}/k^{\times}$ подмножества в $k_{\mathbf{A}}^{\times}$, определенного неравенствами $1 \leqslant |z|_{\mathbf{A}} \leqslant m$. Тогда $\gamma\,(C\,(m)) = c_k \log(m)$, где $c_k = 2^{r_1}\,(2\pi)^{r_2}\,hR/e$.*

Здесь, как и выше, r_1 и r_2 — это соответственно число вещественных и число мнимых точек поля k, h — число классов идеалов, R — регулятор и e — порядок группы E всех корней из 1 в k, который всегда четен, так как $\pm 1 \in k$. Очевидно, $e = 2$ при $r_1 > 0$, поскольку $\mathbf{R}$ не содержит никаких корней из 1, кроме ± 1.

Доказательство предложения начнем с того, что заменим представителей a_i смежных классов в $k_{\mathbf{A}}^{\times}$ по модулю $k^{\times}\,\Omega_{\infty}$, введенных в предложении 8. А именно для каждого i заменим a_i на $a_i b_i^{-1}$, где $b_i \in \Omega_{\infty}$ и $|b_i|_{\mathbf{A}} = |a_i|_{\mathbf{A}}$. Теперь $|a_i|_{\mathbf{A}} = 1$ при $1 \leqslant i \leqslant h$ и, согласно предложению 8, $e\gamma\,(C\,(m)) = h\gamma\,(X)$, где X — пересечение

множества $l^{-1}(F(\mathbf{R} \times I^r))$ с множеством $1 \leqslant |z|_A \leqslant m$ в $k_A^\times$. Как мы видели выше, если $z \in \Omega_\infty$ и $F^{-1}(l(z)) = (t_0, \ldots, t_r)$, то

$$\log(|z|_A) = \lambda(l(z)) = \lambda(F(t)) = t_0.$$

Поэтому множество X может быть записано в виде $l^{-1}(F(J \times I^r))$, где J — интервал $0 \leqslant t \leqslant \log(m)$ в $\mathbf{R}$. Поскольку l— морфизм из Ω_∞ на $\mathbf{R}^{r+1}$ с компактным ядром U, то для любого компактного подмножества $Y \subset \mathbf{R}^{r+1}$ прообраз $l^{-1}(Y)$ является компактным подмножеством в Ω_∞ и отображение $Y \to \gamma(l^{-1}(Y))$ определяет меру Хаара на $\mathbf{R}^{r+1}$, которая, как известно, есть некоторое кратное $c\alpha$ меры Лебега α на $\mathbf{R}^{r+1}$, где постоянная $c > 0$. Отсюда вытекает, что $\gamma(x) = c\alpha(F(J \times I^r))$. По определению регулятор R равен модулю определителя автоморфизма F пространства $\mathbf{R}^{r+1}$, откуда

$$\gamma(X) = c\alpha(F(J \times I^r)) = cR\alpha(J \times I^r) = cR\log(m).$$

Осталось только найти c. Возьмем $Y = J^{n+1}$, так что $\alpha(Y) = (\log m)^{r+1}$. Тогда $l^{-1}(Y)$ есть множество элементов $(z_v) \in \Omega_\infty$, таких, что $1 \leqslant |z|_w \leqslant m$ для всех бесконечных точек w поля k. Ввиду нашего определения меры γ имеем $\gamma(l^{-1}(Y)) = a^{r_1}b^{r_2}$, где

$$a = 2\int_1^m x^{-1}\,dx = 2\log m,$$

$$b = \iint_{1 \leqslant x\bar{x} \leqslant m} (x\bar{x})^{-1} |dx \wedge d\hat{x}| = 2\pi \log m.$$

Это дает $c = 2^{r_1}(2\pi)^{r_2}$, чем и заканчивается доказательство.

Предложение 9 показывает, что R не зависит от выбора ε_i, как и утверждалось.

16.6. Теорема Римана – Роха

Классическая теория полей алгебраических чисел, изложенная в п. 16.5, опирается на тот факт, что в таких полях имеется непустое множество точек, а именно бесконечных точек, выделяющихся своими внутренними свойствами. Можно было бы развить аналогичную теорию для **A**-полей характеристики $p > 1$ с произвольно выделенным конечным множеством точек; эта точка зрения была принята Дедекиндом и Вебером на ранних стадиях развития теории. Какому бы методу ни следовать, изучение таких полей очень скоро приводит к результатам, которые нельзя как следует понять без использования понятий, относящихся к **алгебраической геометрии**, которая лежит в стороне от основного содержания этой книги. Излагаемые здесь

результаты надо рассматривать главным образом как иллюстрацию развитых выше методов и как введение в более общую теорию.

Начиная с этого места во всей главе k обозначает некоторое **A**-поле характеристики $p > 1$. В следствии теор. 8 п.16.4.4 было определено конечное поле F, названное *полем констант* в k. Это — алгебраическое замыкание простого поля в k и, следовательно, оно может быть описано как максимальное конечное поле, содержащееся в k. Начиная с этого места число элементов в поле F обозначается через q и F отождествляется с $\mathbf{F}_q$. Тогда для каждой точки v поля k пополнение k_v содержит $\mathbf{F}_q$. В силу следствия 1 теор. 7 п. 16.1.4 и следствия 2 теор. 2 п. 16.1.1 отсюда вытекает, что модуль q_v поля k_v имеет вид q^d, где d — целое число ≥ 1, называемое *степенью точки* v и обозначаемое через $\deg v$.

Под ***дивизором*** поля k понимается элемент свободной абелевой группы $D(k)$, порожденной точками поля k. Будучи записываема аддитивно, эта группа состоит из формальных сумм $\sum_v a(v) \cdot v$, где $a(v) \in \mathbf{Z}$ для каждой точки v поля k и $a(v) = 0$ почти для всех v. Для дивизора $\mathfrak{a} = \sum a(v) \cdot v$ будем писать $\mathfrak{a} \succ 0$, если $a(v) \geqslant 0$ при всех v. Пусть $\mathfrak{a}$, $\mathfrak{b}$ — два дивизора. Мы пишем $\mathfrak{a} \succ \mathfrak{b}$, если $\mathfrak{a} - \mathfrak{b} \succ 0$. Для каждого дивизора $\mathfrak{a} = \sum a(v) \cdot v$ положим $\deg(\mathfrak{a}) = \sum a(v) \deg(v)$ и назовем это число *степенью* дивизора $\mathfrak{a}$. Ясно, что отображение $\mathfrak{a} \to \deg(\mathfrak{a})$ есть нетривиальный морфизм $D(k) \to \mathbf{Z}$; далее будет доказано, что этот морфизм сюръективен. Ядро этого морфизма, т. е. группа дивизоров степени 0, будет обозначаться через $D_0(k)$. Очевидно, что если $\mathfrak{a} \succ 0$, то $\deg(\mathfrak{a}) \geqslant 0$, причем $\deg(\mathfrak{a}) > 0$ при $\mathfrak{a} \neq 0$, и что если $\mathfrak{a} \succ \mathfrak{b}$, то $\deg \mathfrak{a} \geqslant \deg \mathfrak{b}$.

Пусть $a = (a_v)$ — произвольный элемент из $k_{\mathbf{A}}^{\times}$. Для каждой точки v можно написать $a_v r_v = p_v^{a(v)}$, где $a(v) = \operatorname{ord}_v(a_v)$. Почти для всех v имеем $|a_v|_v = 1$, следовательно, $a(v) = 0$, так что $\sum a(v) \cdot v$ — дивизор поля k. Этот дивизор будем обозначать через $\operatorname{div}(a)$. Ясно, что отображение $\operatorname{div}: k_{\mathbf{A}}^{\times} \to D(k)$ есть сюръективный морфизм, ядром которого является $\prod_v r_v^{\times}$ — та самая группа, которую мы обозначали в п. 16.4.4 через $\Omega(\varnothing)$. Поэтому этот морфизм можно использовать для отождествления $D(k)$ с $k_{\mathbf{A}}^{\times}/\Omega(\varnothing)$. Из определения $|a|_{\mathbf{A}}$ сразу видно, что если $a \in k_{\mathbf{A}}^{\times}$ и $\operatorname{div}(a) = \mathfrak{a}$, то $|a|_{\mathbf{A}} = q^{-\deg(\mathfrak{a})}$. Следовательно, $D_0(k)$ совпадает с образом в $D(k)$ группы $k_{\mathbf{A}}^1$ при морфизме $a \to \operatorname{div}(a)$; в частности, образ $P(k)$ группы $k^{\times}$ в $D(k)$ при этом морфизме содержится в $D_0(k)$. Группу

$P(k)$ принято называть группой *главных дивизоров.* Морфизм $a \to \mathrm{div}\,(a)$ определяет, очевидно, изоморфизмы групп $k_{\mathbf{A}}^1/\Omega\,(\varnothing)$, $k_{\mathbf{A}}^1/k^{\times}\Omega\,(\varnothing)$ и $k_{\mathbf{A}}^{\times}/k^{\times}\Omega\,(\varnothing)$ на $D_0\,(k)$, $D_0\,(k)/P\,(k)$ и $D\,(k)/P\,(k)$ соответственно. Группу $D\,(k)/P\,(k)$ принято называть группой *классов дивизоров* поля k, а $D_0\,(k)/P\,(k)$ — группой классов дивизоров степени 0. Теорема 7 п.16.4.4 показывает, что последняя группа конечна, а предыдущая является прямым произведением этой последней и группы, изоморфной группе $\mathbf{Z}$.

Рассмотрим теперь векторные пространства над k. Имеет место следующий результат, частный случай которого уже встречался в п. 16.4.

Предложение 1. *Пусть E — векторное пространство конечной размерности над k и ε — некоторый базис в E над k. Для каждой точки v поля k пусть $\mathfrak{e}_v$ — r_v-модуль, порожденный множеством ε в E_v, и L_v — некоторая k_v-решетка в E_v. Подгруппа $\prod L_v$ открыта и компактна в E_A в том и только в том случае, когда $L_v = \varepsilon_v$ почти для всех v.*

Если P — такое конечное множество точек, что $L_v \subset \mathfrak{e}_v$ для всех точек v, не лежащих в P, то $\prod L_v$ — компактная подгруппа в $E_{\mathbf{A}}\,(P,\ \mathfrak{e})$, а следовательно, и в E_A; обратное утверждение вытекает из следствия 1 предл. п. 16.4.1. Предположим теперь, что $\prod L_v$ — компактная подгруппа в E_A, т. е. $L_v \subset \mathfrak{e}_v$ почти для всех v. Эта подгруппа открыта тогда и только тогда, когда она содержит некоторую окрестность нуля. Предложение 1 п. 16.4.1 показывает, что это имеет место в том и только в том случае, когда $L_v \supset \mathfrak{e}_v$ почти для всех v. Доказательство закончено.

В обозначениях предложения 1 систему $L = (L_v)$ будем называть *когерентной системой* k_v-решеток или, короче, когерентной системой, соответствующей векторному пространству E, если $L_v = \mathfrak{e}_v$ почти для всех точек v. В этом случае будем писать $U\,(L) = \prod L_v$ и $\Lambda\,(L) = E \cap U\,(L)$. Согласно предложению 1, подгруппа $U(L)$ открыта и компактна. Кроме того, она является модулем над открытым и компактным подкольцом $\prod r_v$ в k_{A}. Что касается группы $\Lambda\,(L)$, то это — конечная подгруппа в E, поскольку подгруппа E дискретна, а подгруппа $U\,(L)$ компактна в E_A. Далее, $\Lambda\,(L)$ является модулем над кольцом $k \cap (\prod r_v)$. Поскольку это кольцо по теореме 8 п. 16.4.4 и ее следствию совпадает с полем констант $\mathbf{F}_q$ поля k, отсюда вытекает, что $\Lambda\,(L)$ является векторным пространством над $\mathbf{F}_q$.

Размерность этого пространства обозначим через $\lambda(L)$. Тогда $\Lambda(L)$ состоит из $q^{\lambda(L)}$ элементов.

Предложение 2. *Положим* $\mathcal{A} = \mathrm{End}(E)$, *и пусть* $L=(L_v)$, $M=(M_v)$ — *две когерентные системы, соответствующие пространству E. Тогда существует такой элемент* $a = (a_v) \in \mathcal{A}_{\mathbf{A}}$, *что* $M_v = a_v L_v$ *для всех точек v. Кроме того, дивизор* $\mathrm{div}(\det(a))$ *однозначно определяется по L и M.*

По теореме 1 п. 16.2.2 для каждой точки v существуют такие базисы α_v, β_v в E_v над k_v, что L_v, M_v являются r_v-модулями, порожденными соответственно множествами α_v и β_v. Обозначим через a_v-атоморфизм пространства E_v, который отображает базис α_v на β_v. Тогда $M_v = a_v L_v$. Положим $d_v = \det(a_v)$. Если μ_v — произвольная мера Хаара на E_v, то по следствию 3 теор. 3 п.16.1.2 $|d_v|_v = \mu_v(M_v)/\mu_v(L_v)$, так что $|d_v|_v$ не зависит от выбора базисов α_v и β_v. Далее, по условию $L_v = M_v$, откуда $|d_v|_v = 1$, почти для всех v. В силу предложения 3 п.16.4.3 отсюда следует, что $a = (a_v) \in \mathcal{A}_{\mathbf{A}}^{\times}$ и $d = (d_v) = \det(a) \in k_{\mathbf{A}}^{\times}$. Поскольку $|d_v|_v$ зависит только от L_v и M_v, то и $\mathrm{div}(d)$ зависит только от L и M.

Будем писать $M = aL$ в ситуации, описанной в предложении.

Следствие 1. *Пусть* ε — *базис пространства E над k. Положим* $L_0=(\varepsilon_v)$, *и пусть L — произвольная когерентная система, соответствующая пространству E. Тогда существует такой элемент* $a \in \mathcal{A}_{\mathbf{A}}^{\times}$, *что* $L = aL_0$. *Дивизор* $\mathfrak{d} = \mathrm{div}(\det(a))$ *зависит только от L и* ε, *а его класс и степень зависят только от L.*

Лишь последнее утверждение нуждается в доказательстве. Заменим ε каким-нибудь другим базисом ε', положим $L_0' = (\varepsilon_v')$ и обозначим через α автоморфизм пространства E над k, который отображает ε' на ε. Тогда $L_0 = \alpha L_0'$ и, следовательно, $L = a\alpha L_0'$, так что $\mathfrak{d}$ надо заменить на $\mathfrak{d} + \mathrm{div}(\det(a))$. Но второе слагаемое в последней сумме является главным дивизором, и, значит, его степень равна 0.

Следствие 2. *Существует такая мера Хаара* μ *на* $E_{\mathbf{A}}$, *что* $\mu(\prod \varepsilon_v) = 1$ *для каждого базиса* ε *в E над k. Если L и* $\mathfrak{d}$ *таковы, как в следствии* 1, *то для этой меры* $\mu(U(L)) = q^{-\delta(L)}$, *где*

$$U(L) = \prod L_v \text{ и } \delta(L) = \deg(\mathfrak{d}).$$

Возьмем какой-нибудь базис ε и выберем μ так, чтобы $\mu(\prod \varepsilon_v) = 1$. Если a таково, как в следствии 1, то $U(L)$ совпадает с образом группы $U(L_0) = \prod \varepsilon_v$ при отображении $e \to ae$. Поэтому мера $\mu(U(L))$ равна модулю этого автоморфизма, который совпадает с $|\det(a)|_{\mathbf{A}}$ по предложению 3 п.16.4.3. В силу наших определений это число равно

$q^{-\delta(L)}$, что и утверждается в нашем следствии. Согласно следствию 1, это число не зависит от ε, поэтому при замене ε на какой-нибудь другой базис ε' мы получим такую меру μ', что $\mu'(U(L))$ совпадает с $\mu(U(L))$, откуда $\mu' = \mu$, так что μ

$$\mu\left(\prod \varepsilon_v'\right) = 1.$$

Как и в п.16.4.2, выберем теперь какой-нибудь нетривиальный характер χ на k_A, тривиальный на k, и обозначим через χ_v характер, индуцированный характером χ на k_v. Для каждой точки v характер χ_v нетривиален по следствию 1 теор. 3 п. 16.4.2. Пусть E такое, как выше, и E' — алгебраическое двойственное к нему. Как объяснялось в п.16.4.2, отождествим с помощью χ пространство $E'_{\mathbf{A}}$ с топологическим двойственным к E_A посредством изоморфизма, описанного в теореме 3 п. 16.4.2, а также для каждой точки v отождествим с помощью χ_v пространство E'_v с топологическим двойственным к E_v посредством изоморфизма, описанного в теореме 3 п. 16.4.2. Пусть $L = (L_v)$ — когерентная система, соответствующая пространству E. Для каждой точки v обозначим через L'_v решетку, двойственную с L_v. С учетом только что сделанных отождествлений L'_v является k_v-решеткой в E'_v и $\prod L'_v$ является подгруппой в E_A, ассоциированной по двойственности с подгруппой $U(L) = \prod L_v$ в $E_{\mathbf{A}}$. Так как подгруппа $U(L)$ компактна, то подгруппа $\prod L'_v$ открыта, а так как $U(L)$ открыта, то $\coprod L'_v$ компактна. В силу предложения 1 отсюда вытекает, что $L' = (L'_v)$ есть когерентная система, соответствующая пространству E' (этот факт вытекает также из следствия 3 теор. 3 п. 16.4.2). Система L' называется *двойственной* к L.

Теорема 1. *Для каждого К-поля k характеристики p>1 существует целое число $g \geqslant 0$ со следующим свойством. Если E — векторное пространство конечной размерности n над k, L — произвольная когерентная система, соответствующая пространству E, и L' — система, двойственная к L, то*

$$\lambda(L) = \lambda(L') - \delta(L) - n(g-1).$$

Положим $U = U(L)$, $U' = U(L')$. Как мы только что видели, U' есть подгруппа в E'_A, ассоциированная по двойственности с подгруппой U в E_A. По определению $\lambda(L)$ и $\lambda(L')$ равны соответственно размерностям векторных пространств $\Lambda = E \cap U$ и $\Lambda' = E' \cap U'$ над полем констант $\mathbf{F}_q$ поля k. По теореме 3 п.16.4.2 подгруппой в E'_A, ассоциированной по двойственности с подгруппой $E \subset E_{\mathbf{A}}$, является E'. Поэтому подгруппой в $E'_{\mathbf{A}}$, ассоциированной по двойственности с $E + U$, является Λ', так что группа $E_{\mathbf{A}}/(E + U)$

двойственна к Λ' и имеет то же самое число элементов $q^{\lambda(L')}$, что и Λ'. Ясно, что группа $E_\Lambda/(E + U)$ изоморфна $(E_\Lambda/E)/(E + U/E)$. Возьмем меру Хаара μ на E_A, определенную следствием 2 предл. 2, и обозначим снова через μ ее образ в E_Λ/E (п.16.2.4). Так как индекс подгруппы $(E + U)/E$ в E_Λ/E равен $q^{\lambda(L')}$, то

$$\mu\,(E_\Lambda/E) = q^{\lambda(L')}\,\mu\,(E + U/E).$$

Канонический морфизм $E_\Lambda \to E_\Lambda/E$ отображает U на $(E + U)/E$ и имеет конечное ядро $\Lambda = E \cap U$. Поскольку Λ состоит из $q^{\lambda(L)}$ элементов, отсюда вытекает, например по лемме 2 п.16.2.4, что

$$\mu\,(U) = q^{\lambda(L)}\,\mu\,(E + U/E).$$

Комбинируя эти формулы со следствием 2 предл. 2, согласно которому $\mu\,(U) = q^{-\delta(L)}$, получаем, что

$$\mu\,(E_\Lambda/E) = q^{\lambda(L')-\lambda(L)-\delta(L)}.$$

Отсюда видно, что число $\mu\,(E_\Lambda/E)$ имеет вид q^r, где $r \in \mathbf{Z}$. В частности, применяя следствие 2 предл. 2 к $E = k$ и к базису $\varepsilon = \{1\}$, получаем такую меру Хаара μ_1 на k_A, что $\mu_1\,(\prod r_v) = 1$, и мы видим, что $\mu_1\,(k_A/k) = q^\gamma$, где $\gamma \in \mathbf{Z}$. Отождествим теперь наше пространство E с k^n, выбрав некоторый базис ε в E над k. Ясно, что мера μ на E_A, определенная следствием 2 предл. 2, является произведением $(\mu_1)^n$ мер μ_1 на n сомножителях произведения $E_\Lambda = (k_\Lambda)^n$, откуда $q^r = (q^\gamma)^n$, т. е. $r = \gamma n$. Это дает нам искомую формулу с $g = \gamma + 1$. Остается только показать, что $g \geqslant 0$. Для этого применим нашу формулу к случаю $E = k$, $L_v = r_v$ при всех v. Тогда $\Lambda = \mathbf{F}_a$, $\lambda\,(L) = 1$ и, очевидно, $\delta\,(L) = 0$, откуда $g = \lambda\,(L')$. Но последняя величина неотрицательна по определению.

Следствие 1. *Пусть* μ *— мера Хаара на* E_A, *определенная следствием* 2 *предл.* 2. *Тогда* $\mu\,(E_\Lambda/E) = q^{n(q-1)}$. *В частности, если* μ_1 *— мера Хаара на* k_A, *для которой* $\mu_1\,(\prod r_v) = 1$, *то*

$$\mu_1\,(k_\Lambda/k) = q^{g-1}.$$

Это было доказано выше.

Следствие 2. *В обозначениях теоремы* 2 $E_\Lambda = E + U$ *тогда и только тогда, когда* $\lambda\,(L') = 0$.

Это частный случай того, что было доказано выше.

Определение 1. *Целое число* g, *определенное в теореме* 1, *называется родом поля* k.

Приведем теперь полученные выше результаты к более явному виду для случая $E = k$. В этом случае когерентная система $L = (L_v)$ задается набором $L_v = p_v^{-a(v)}$, где $a\,(v) = 0$ почти для всех v.

Следовательно, такие системы находятся во взаимно однозначном соответствии с дивизорами поля k. Поэтому для дивизора $\mathfrak{a} = \sum a(v) \cdot v$ когерентную систему $(p_v^{-a(v)})$ будем обозначать через $L(\mathfrak{a})$, так что $L(0)$ —это когерентная система (r_v), и мы видим, что $L(\mathfrak{a})$— это когерентная система $a^{-1}L(0)$, где $a \in k_{\mathbf{A}}^{\times}$ и $\mathfrak{a} = \operatorname{div}(a)$. Для $L = L(\mathfrak{a})$ будем писать $U(\mathfrak{a})$, $\Lambda(\mathfrak{a})$, $\lambda(\mathfrak{a})$, $\delta(\mathfrak{a})$ вместо $U(L)$, $\Lambda(L)$, $\lambda(L)$, $\delta(L)$. Очевидно, $\delta(\mathfrak{a}) = -\deg(\mathfrak{a})$. По определению группа $\Lambda(\mathfrak{a})$ может быть записана как $\bigcap_v (k \cap p_v^{-a(v)})$; другими словами, она состоит из нуля и тех элементов $\xi \in k^{\times}$, для которых $\operatorname{ord}_v(\xi) \geqslant -a(v)$ при всех v, или, что то же самое, для которых $\operatorname{div}(\xi) \succ -\mathfrak{a}$. Так как степень дивизора $\operatorname{div}(\xi)$ равна нулю для всех $\xi \in k^{\times}$, отсюда видно, что $\Lambda(\mathfrak{a}) = \{0\}$ и, следовательно, $\lambda(\mathfrak{a}) = 0$, если $\deg(\mathfrak{a}) < 0$.

Выберем теперь, как выше, базисный характер χ на k_A. Для каждой точки v поля k обозначим через $v(v)$ порядок характера χ_v (см. определение 4 п.16.2.5), индуцированного на k_v характером χ. По следствию 1 теор. 3 п.16.4.2 $v(v)$==0 почти для всех v, так что $\mathfrak{c} = \sum v(v) \cdot v$— дивизор поля k. Назовем его *дивизором характера* χ и обозначим через $\operatorname{div}(\chi)$. Если χ_1 — другой такой характер, то по теореме 3 п.16.4.2 он может быть записан как $x \to \chi(\xi x)$ с $\xi \in k^{\times}$, и сразу видно, что $\operatorname{div}(\chi_1) = \operatorname{div}(\chi) + \operatorname{div}(\xi)$. Таким образом, когда χ пробегает все нетривиальные характеры на k_A, тривиальные на k, дивизоры $\operatorname{div}(\chi)$ образуют смежный класс дивизоров по модулю группы $P(k)$ главных дивизоров поля k. Этот класс принято называть *каноническим классом,* а его элементы — *каноническими дивизорами.*

Как и раньше, отождествим при помощи χ группу k_A с топологической двойственной к ней и положим $\mathfrak{c} = \operatorname{div}(\chi)$. Используя предложение 12 п.16.2.5, сразу видим, что система, двойственная к $L(\mathfrak{a})$, совпадает с $L(\mathfrak{c} - \mathfrak{a})$. Теорема 1 дает теперь следующий результат.

Теорема 2. *Пусть* $\mathfrak{c}$ *— канонический дивизор поля* k. *Тогда*

$$\lambda(\mathfrak{a}) = \lambda(\mathfrak{c} - \mathfrak{a}) + \deg(\mathfrak{a}) - g + 1$$

для каждого дивизора $\mathfrak{a}$ *поля* k.

Следствие 1. *Если* $\mathfrak{c}$ *— канонический дивизор, то* $\deg(\mathfrak{c}) = 2g - 2$ *и* $\lambda(\mathfrak{c}) = g$.

Первое равенство получается, если заменить в теореме $2\mathfrak{a}$ на $\mathfrak{c} - \mathfrak{a}$, а второе, если взять $\mathfrak{a} = 0$.

Следствие 2. *Если* $\mathfrak{a}$*— дивизор степени* $\geqslant 2g - 2$, *то*

$$\lambda(\mathfrak{a}) = \deg(\mathfrak{a}) - g + 1.$$

Действительно, в этом случае $\deg(\mathfrak{c} - \mathfrak{a}) < 0$, откуда, как мы отмечали выше, вытекает равенство $\lambda(\mathfrak{c} - \mathfrak{a}) = 0$, а значит, по теореме 2, и доказываемое равенство.

Следствие 3. *Пусть* $\mathfrak{a} = \sum a(v) \cdot v$ *—дивизор степени* $> 2g - 2$. *Тогда* $k_{\mathbf{A}} = k \dotplus (\prod_v p_v^{-a(v)})$.

Это утверждение является частным случаем следствия 2 теор. 1 при $E = k$, $L = L(\mathfrak{a})$, ибо в этом случае, как показано выше, $L' = L(\mathfrak{c} - \mathfrak{a})$ и $\lambda(L') = 0$.

Теорема 2 — это *теорема Римана — Роха* для «функционального поля» k с *конечным* полем констант. Доказательство в общем случае может быть получено совершенно аналогичным путем; понятие плотности следует заменить понятием «линейной плотности» для векторных пространств над произвольным полем K, наделяемым дискретной топологией; вместо меры Хаара следует использовать «относительную размерность» компактных и открытых подпространств локально компактных векторных пространств над K. Мы не будем здесь рассматривать это обобщение.

Отметим еще один момент, имеющий некоторое значение. Вместо того чтобы с помощью базисного характера отождествлять пространство G, топологическое двойственное к k_A, с самим пространством k_A, рассмотрим G как k_A-модуль, полагая $\langle x, ax^* \rangle = \langle ax, x^* \rangle$, где $x \in k_{\mathbf{A}}$, $x^* \in G$, $a \in k_{\mathbf{A}}$. Обозначим через Γ подгруппу в G, ассоциированную по двойственности с k. Тогда теорема 3 п.16.4.2 может быть выражена следующим образом: для любого отличного от нуля элемента γ в Γ отображение $x \to x\gamma$ является изоморфизмом из k_A на G, отображающим k на Γ. В частности, подгруппа Γ обладает «внутренне» присущей ей структурой векторного пространства размерности 1 над k. Теперь можно «канонически» определить дифференцирование из k в Γ, т. е. отображение $x \to dx$ из k в Γ, для которого $d(xy) = x \cdot dy \dotplus y \cdot dx$ при всех x, $y \in k$, и пространство Γ можно отождествить с k-модулем всех формальных сумм $\sum y_i\, dx_i$, где x_i, $y_i \in k$. Это остается справедливым для каждого сепарабельного алгебраического расширения конечной степени над любым полем $K(T)$, где T — неизвестная над основным полем K. Даже для изучаемого здесь случая конечного поля констант эту тему трудно разрабатывать должным образом, не расширяя основного поля до его алгебраического замыкания, и мы нигде в дальнейшем не будем возвращаться к этой теме.

16.7. Дзета-функция А-полей

16.7.1. Сходимость Эйлерова произведения

Начиная с этого места k будет обозначать произвольное **A**-поле характеристики нуль или $p > 1$. Обозначения будут прежними: если v — точка поля k, то k_v — это соответствующее пополнение поля k; если v — конечная точка, то r_v — это максимальное компактное подкольцо в k_v, а p_v — максимальный идеал в r_v. Кроме того, в последнем случае условимся раз и навсегда обозначать через q_v модуль поля k_v и через π_v — простой элемент в k_v, так что по теореме 6 п. 16.1.4 r_v/p_v — это поле из q_v элементов и $|\pi_v|_v = q_v^{-1}$. Если k — поле характеристики $p > 1$, то будем обозначать через q число элементов в его поле констант и отождествлять это поле с $\mathbf{F}_q$. Тогда в соответствии с определениями п.16.6 $q_v = q^{\deg(v)}$ для каждой точки v.

Под *эйлеровым произведением,* соответствующим полю k, будем понимать любое произведение вида

$$\prod_v (1 - \theta_v q_v^{-s})^{-1},$$

где $s \in \mathbf{C}$, $\theta_v \in \mathbf{C}$ и $|\theta_v| \leqslant 1$ при всех v; произведение берется по всем или почти всем конечным точкам поля k. Это же название употребляют для произведений более общего типа, но последние нам здесь не встретятся. Основной результат о сходимости эйлеровых произведений формулируется так:

Предложение 1. *Пусть k — произвольное* **A**-*поле. Тогда произведение*

$$\zeta_k(\sigma) = \prod_v (1 - q_v^{-\sigma})^{-1},$$

где $\sigma \in \mathbf{R}$, а v пробегает все конечные точки поля k, сходится при $\sigma > 1$ и стремится к 1 при $\sigma \to +\infty$.

Предположим сперва, что характеристика поля k равна нулю, и обозначим через n степень поля k над $\mathbf{Q}$. По следствию 1 теор. 4 п.16.3.4 имеется не более n точек поля k, лежащих над фиксированной точкой p поля $\mathbf{Q}$. Для каждой такой точки v поле k_v является p-полем, так что q_v имеет вид p^v, где $v \geqslant 1$, и поэтому $q_v \geqslant p$. При $\sigma > 0$ это дает

$$1 < \zeta_k(\sigma) \leqslant \prod (1 - p^{-\sigma})^{-n},$$

где произведение берется по всем простым числам p. Теперь запишем

$$\zeta(\sigma) = \prod (1 - p^{-\sigma})^{-1} = \prod (1 + p^{-\sigma} + p^{-2\sigma} + \ldots).$$

Раскрывая скобки в последнем произведении, получаем

$$\zeta(\sigma) = \sum_{\nu=1}^{+\infty} \nu^{-\sigma},$$

ибо каждое целое число $\nu \geqslant 1$ может быть однозначно представлено в виде произведения степеней простых чисел. Далее, при $\sigma > 1$ имеем

$$1 < \zeta(\sigma) < 1 + \sum_{\nu=2}^{+\infty} \int_{\nu-1}^{\nu} t^{-\sigma}\, dt = 1 + \int_{1}^{+\infty} t^{-\sigma}\, dt = 1 + (\sigma - 1)^{-1},$$

откуда видно, что $\zeta(\sigma)$ сходится при $\sigma > 1$ и стремится к 1 при $\sigma \to +\infty$. Таким образом, наше предложение доказано в случае числового поля *k*.

Теперь предположим, что *k* — поле характеристики $p>1$. Тогда, согласно лемме 1 п. 16.3.2, *k* можно представить как сепарабельное алгебраическое расширение конечной степени *n* поля $\mathbf{F}_p$ *(T)*. По теореме 2 п.16.3.1 поле $\mathbf{F}_p$ *(T)* имеет точку ∞, соответствующую простому элементу T^{-1}, а все остальные точки находятся во взаимно однозначном соответствии с неприводимыми многочленами π из $\mathbf{F}_p[T]$. Очевидно, достаточно доказать утверждение нашего предложения не для самого произведения $\zeta_k(\sigma)$, а для аналогичного произведения $\eta(\sigma)$, взятого по всем точкам *v* поля *k*, не лежащим над точкой ∞ поля $\mathbf{F}_p$ *(T)*. Точно так же, как в случае характеристики нуль, мы видим, что $1 < \eta(\sigma) \leqslant \zeta_p(\sigma)^n$, где через $\zeta_p(\sigma)$ обозначено произведение

$$\zeta_p(\sigma) = \prod (1 - p^{-\deg(\pi)\sigma})^{-1} = \prod (1 + p^{-\deg(\pi)\sigma} + p^{-2\deg(\pi)\sigma} + \ldots),$$

взятое по всем унитарным неприводимым многочленам π из $\mathbf{F}_p[T]$. Так как каждый унитарный многочлен из $\mathbf{F}_p[T]$ может быть однозначно представлен в виде произведения степеней унитарных неприводимых многочленов, то

$$\zeta_p(\sigma) = \sum p^{-\deg(\mu)\sigma},$$

где сумма берется по всем унитарным многочленам μ из $\mathbf{F}_p[T]$. Поскольку для каждого $\delta \geqslant 0$ имеется ровно p^{δ} унитарных многочленов степени δ, мы получаем, что

$$\zeta_p(\sigma) = \sum_{\delta=0}^{+\infty} p^{\delta(1-\sigma)} = (1 - p^{1-\sigma})^{-1},$$

чем завершено доказательство в случае ненулевой характеристики.

Следствие 1. *Пусть P — конечное множество точек поля k, содержащее P_∞, и для каждой точки v, не лежащей в P, выбрано число* $\theta_v \in \mathbf{C}$, *такое, что* $|\theta_v| \leqslant 1$. *Для всякого* $s \in \mathbf{C}$ *положим*

$$E(s) = \prod_{v \notin P} (1 - \theta_v q_v^{-s})^{-1}.$$

Тогда при $\mathrm{Re}(s) > 1$ *произведение* $E(s)$ *абсолютно сходится, голоморфно по* s *и не равно нулю и* $E(s) \to 1$ *равномерно относительно* $\mathrm{Im}(s)$ *при* $\mathrm{Re}(s) \to +\infty$.

В самом деле, для $\sigma = \mathrm{Re}(s)$ ряд $\log E(s)$ мажорируется рядом $\log \zeta_k(\sigma)$. Утверждение следствия вытекает поэтому из предложения 1 и хорошо известных элементарных теорем о равномерно сходящихся рядах голоморфных функций.

Следствие 2. *Пусть* k_0 *— некоторое* **A***-поле, содержащееся в* k, *и пусть* M *— такое множество конечных точек поля* k, *что почти для всех* $v \in M$ *модулярная степень* $f(v)$ *поля* k_v *над замыканием поля* k_0 *в* k_v *больше* 1. *Тогда произведение*

$$p(M, \sigma) = \prod_{v \in M} (1 - q_v^{-\sigma})^{-1}$$

абсолютно сходится при $\sigma > 1/2$.

Если характеристика поля k равна нулю, то поля k и k_0 имеют конечную степень над $\mathbf{Q}$; если же k — поле характеристики $p > 1$ и T — любой элемент из k_0, не алгебраичный над простым полем $\mathbf{F}_p$, то k и k_0 имеют конечную степень над $\mathbf{F}_p(T)$. В обоих случаях k имеет конечную степень n над k_0. Пусть v — конечная точка поля k и u —точка поля k_0, лежащая под v. Тогда замыкание поля k_0 в k_v равно $(k_0)_u$ и k порождает поле k_v над $(k_0)_u$. Поэтому степень поля k_v над $(k_0)_u$ не превосходит n, так что $1 \leqslant f(v) \leqslant n$. Таким образом, M является объединением множеств $M_1, \ldots, M_n$, состоящих соответственно из тех точек $v \in M$, для которых $f(v) = f$, где $1 \leqslant f \leqslant n$. Наше предположение относительно M означает, что множество M_1 конечно, так что достаточно доказать наше утверждение для каждого из множеств M_f, $f \geqslant 2$. По следствию 1 теор. 4 п. 16.3.4 над всякой конечной точкой u поля k_0 имеется не более n/f точек $v \in M_f$. Поэтому произведение $p(M_f, \sigma)$ мажорируется произведением $\zeta_{k_0}(f\sigma)^{n/f}$, которое при $\sigma > 1/f$ абсолютно сходится по предложению 1.

Следствие 3. *Пусть* M *таково, как в следствии* 2, *и пусть для каждой точки* $v \in M$ *выбрано число* $\theta_v \in \mathbf{C}$, *для которого* $|\theta_v| \leqslant 1$. *Тогда при* $\mathrm{Re}(s) > 1/2$ *произведение*

$$\prod_{v \in M} (1 - \theta_v q_v^{-s})^{-1}$$

абсолютно сходится, голоморфно по s *и отлично от нуля.*

Доказательство аналогично доказательству следствия 1, надо только учесть следствие 2.

16.7. 2. Преобразования Фурье и стандартные функции

Теория дзета-функций существенно связана с преобразованиями Фурье на группах k_v, k_A, соответствующих **A**-полю k. Начнем с того, что напомним результаты, которые нам понадобятся.

Пусть G, G^* и $\langle g, g^* \rangle$ таковы, как в п. 16.2.5, и пусть Ф — непрерывная функция на G, интегрируемая по мере Хаара α, заданной на G. Тогда функция Ф* на G^*, определенная формулой

$$\Phi^*(g^*) = \int_G \Phi(g) \langle g, g^* \rangle \, d\alpha(g),$$

называется *преобразованием Фурье функции* Ф относительно меры α. Легко проверяется, что эта функция непрерывна на G*. Если заменить α на $c\alpha, c \in \mathbf{R}_+^\times$, то, очевидно, Ф* заменится на $c\Phi^*$.

Лемма 1. *Пусть* $g \to \lambda g$ *— автоморфизм группы* G, $\mathrm{mod}_G(\lambda)$ *— модуль автоморфизма* λ *и* $g^* \to g^*\lambda^*$ *— автоморфизм группы,* G^*, *для которого* $\langle \lambda g, g^* \rangle = \langle g, g^*\lambda^* \rangle$ *при всех* $g \in G$, $g^* \in G^*$. *Тогда если* Ф* *— преобразование Фурье функции* Ф, *то преобразованием Фурье функции* $g \to \Phi(\lambda^{-1}g)$ *является функция* $g^* \to$ $\to \mathrm{mod}_G(\lambda)\, \Phi^*(g^*\lambda^*)$.

Это получается, если заменить g на λg в интеграле, определяющем преобразование Фурье от $\Phi(\lambda^{-1}g)$.

Согласно теории преобразований Фурье, существует такая мера Хаара α* на G^*, что для любой интегрируемой функции Ф* на G*, определяемой написанным выше интегралом, Ф задается следующей «формулой обращения Фурье»:

$$\Phi(g) = \int_{G^*} \Phi^*(g^*) \langle -g, g^* \rangle \, d\alpha^*(g^*).$$

Мы говорим тогда, что Ф есть *обратное преобразование Фурье* функции Ф*. Мера α* называется *двойственной к мере* α. Ясно, что двойственной мерой к $c\alpha$, $c \in \mathbf{R}_+^\times$, является мера $c^{-1}\alpha^*$. В частности, если предположить, что группа G* отождествлена с G при помощи некоторого изоморфизма $G \to G^*$, то $\alpha^* = m\alpha$, где $m \in \mathbf{R}_+^\times$, и поскольку двойственной к $c\alpha$ будет мера $c^{-1}m\alpha$, существует одна и только одна мера Хаара на G, а именно $m^{1/2}\alpha$, которая совпадает со своей двойственной при заданном отождествлении G и G*. Эта мера называется *самодвойственной мерой Хаара* на G. Если группа G компактна, то группа G* дискретна. В этом случае, взяв Ф = 1, мы сразу видим, что если α — мера Хаара на G, для которой $\alpha(G) = 1$, то $\alpha^*(\{0\}) = 1$ для двойственной меры α* на G^*.

Функцию Ф на G будем называть *допустимой* для G, если она непрерывна и интегрируема и ее преобразование Фурье Ф* является интегрируемой функцией на G*. Пусть теперь Г — такая дискретная подгруппа в G, что факторгруппа G/Γ компактна, и пусть Г* — подгруппа в G^*, ассоциированная по двойственности с Г. Так как G/Γ компактна, то Г* дискретна; так как Г дискретна, то G^*/Γ_* компактна. Возьмем меру Хаара α на G, для которой $\alpha\,(G/\Gamma) = 1$. Функцию Ф на G будем называть *допустимой для* (G, Г), если она допустима для G и оба ряда

$$\sum_{\gamma\in\Gamma} \Phi\,(g+\gamma),\quad \sum_{\gamma^*\in\Gamma_*} \Phi^*\,(g^*+\gamma^*)$$

абсолютно сходятся, равномерно на каждом компактном подмножестве относительно g *и* g^*. Первый из этих рядов определяет тогда непрерывную функцию F на G, постоянную на каждом классе смежности по модулю Г. Эту функцию можно очевидным образом рассматривать как функцию на G/Γ. Так как группа Γ_* двойственна к G/Γ, то функция F имеет преобразованием Фурье

$$\gamma^* \longrightarrow \int\limits_{G/\Gamma} \left(\sum_{\gamma\in\Gamma} \Phi\,(g+\gamma)\right) \langle g,\ \gamma^*\rangle\, d\alpha\,(\dot{g}),$$

где, как обычно, $\dot{g}$ — образ элемента g в G/Γ при каноническом гомоморфизме $G \to G/\Gamma$; подинтегральная функция, хоть она и записана как функция от g, но, будучи постоянна на каждом классе смежности по модулю Г, рассматривается как функция от $\dot{g}$. Согласно формуле 6 п.16.2.4, этот интеграл равен $\Phi^*\,(\gamma^*)$, так что преобразование Фурье функции F, рассматриваемой как функция на G/Г, совпадает с функцией, которую Ф* индуцирует на Г*. Так как функция Ф по предположению допустима для $(G,\ \Gamma)$, то Ф* интегрируема на Г*, так что по формуле обращения Фурье для G/Γ и Γ_* находим

$$F\,(g) = \sum_{\gamma\in\Gamma} \Phi\,(g+\gamma) = \sum_{\gamma^*\in\Gamma_*} \Phi^*\,(\gamma^*)\cdot\langle -g,\ \gamma^*\rangle.$$

При $g = 0$ получаем

$$\sum_{\gamma\in\Gamma} \Phi\,(\gamma) = \sum_{\gamma^*\in\Gamma_*} \Phi^*\,(\gamma^*). \tag{1}$$

Эту формулу принято называть *формулой суммирования Пуассона.* Ее справедливость доказана нами для любой допустимой для (G, Г) функции Ф и для такой меры α, что $\alpha\,(G/\Gamma) = 1$.

Предположим, что существуют допустимые для (G, Г) функции Ф, для которых обе части равенства (1) отличны от нуля. Это предположение (которое легко следует из общей теории преобра-

зований Фурье) мы проверим с помощью явного построения в том единственном интересующем нас случае, когда $G = E_A$, $\Gamma = E$, где E — векторное пространство конечной размерности над **A**-полем. Обозначим через α^* меру, двойственную к α, положим $\alpha^*(G^*/\Gamma_*) = c$ и поменяем в проведенных выше вычислениях G и G* ролями, отправляясь от функции Ф* и беря ее обратное преобразование Фурье относительно меры Хаара $c^{-1}\alpha^*$ на G*. Так как это преобразование совпадает с $c^{-1}\Phi$, то мы получим как конечный результат формулу (1), в которой вместо Ф будет стоять $c^{-1}\Phi$, откуда $c = 1$.

Таким образом, доказано, что меры Хаара α, α^* на G, G*, задаваемые условиями $\alpha(G/\Gamma) = 1$, $\alpha^*(G^*/\Gamma_*) = 1$, двойственны друг другу. В частности, пусть существует изоморфизм из G на G*, который отображает Г на Г*; если использовать его для отождествления G с G*, то самодвойственная мера на G — это та мера Хаара, для которой $\alpha(G/\Gamma) = 1$.

Теперь мы построим некоторые специальные типы допустимых функций для интересующих нас групп. Эти функции будут называться «стандартными» функциями. Функция, заданная на топологическом пространстве, называется *локально постоянной,* если для любой точки существует такая ее окрестность, на которой функция постоянна. Если f — локально постоянная функция, то множество $f^{-1}(\{a\})$ открыто для каждого значения a и в то же время замкнуто, так как его дополнение является объединением открытых множеств $f^{-1}(\{b\})$, $b \neq a$. На связном пространстве, например на любом векторном пространстве над **R**, локально постоянными функциями являются только константы.

Определение 1. *Пусть E — векторное пространство конечной размерности над р-полем K. Под стандартной функцией на E мы понимаем комплекснозначную локально постоянную функцию на E с компактным носителем.*

Нам будет достаточно рассмотреть случай коммутативного поля K. Пусть E^* — топологическая двойственная к E группа, т. е. группа, двойственная к пространству E, рассматриваемому как локально компактная группа. Способом, описанным в п.16.2.5, определим на E^* структуру векторного пространства над K; как мы там доказали, векторное пространство E^* над K имеет ту же самую размерность, что и E. В этих обозначениях имеем

Предложение 2. *Функция* Ф *на E стандартна тогда и только тогда, когда существуют такие K-решетки L, M в E, что $L \supset M$, Φ равна нулю вне L и постоянна на смежных классах в L по модулю M. Если это имеет место и если L_*, M_* — двойственные к L, M*

К-решетки, то $M_* \supset L_*$ *и преобразование Фурье* Φ* *функции Φ равно нулю вне M* и постоянно на классах смежности в M* по модулю* L_*.

Если Φ, *L, M* обладает свойствами, указанными в предложении, то Φ, очевидно, стандартна. Обратно, предположим, что Φ стандартна. Возьмем какую-нибудь *K*-норму *N* на *E* и обозначим через μ верхнюю грань нормы *N* на носителе функции Φ. Тогда, как мы видели в главе п.16.2.2, множество *L,* определенное неравенством $N(e) \leqslant \mu$, является *K*-решеткой, и эта решетка содержит носитель Φ. Так как множества $\Phi^{-1}(\{a\})$, $a \in \mathbf{C}$, открыты, а множество *L* компактно, то *L* содержится в объединении конечного числа таких множеств. Другими словами, функция Φ на *L* принимает лишь конечное число значений $a_1, \ldots, a_n$. Выберем такое $\varepsilon > 0$, что $|a_i - a_j| > \varepsilon$ при $i \neq j$. Поскольку Φ равномерно непрерывна на *L,* существует такое $\delta > 0$, что $|\Phi(e) - \Phi(e')| \leqslant \varepsilon$ при $N(e - e') \leqslant \delta$, где $e, e' \in L$. Тогда множество *M,* определяемое неравенством $N(e) \leqslant \delta$, является *K*-решеткой, содержащейся в *L* при $\delta \leqslant \mu$, причем Φ постоянна на классах смежности в *L* по модулю *M.* Рассмотрим теперь преобразование Фурье

$$\Phi^*(e^*) = \int_E \Phi(e) \langle e, e^* \rangle \, d\alpha(e),$$

где α— произвольная мера Хаара на *E.* Так как Φ равна нулю вне *L,* то интеграл не изменится, если мы возьмем его по *L.* Заменим e^* на $e_1^* + e_1^*$, где $e_1^* \in L_*$. Поскольку по определению $\langle e, e_1^* \rangle = 1$ при всех $e \in L$, интеграл при этом не изменится. Следовательно, Φ* постоянна на классах смежности в *E** по модулю L_*. С другой стороны, поскольку *M* — открытая подгруппа в компактной группе *L,* то *L* есть объединение конечного числа классов смежности $e_i + M$. Так как Φ постоянна на каждом из этих классов, то

$$\Phi^*(e^*) = \sum_i \Phi(e_i) \int_M \langle e_i + e, e^* \rangle \, d\alpha(e) =$$

$$= \sum_i \Phi(e_i) \langle e_i e^* \rangle \int_M \langle e, e^* \rangle \, d\alpha(e). \tag{2}$$

Поскольку последний интеграл, очевидно, равен нулю, если характер $e \to \langle e, e^* \rangle$ нетривиален на *M,* т. е. если $e^* \notin M_*$, то функция Φ* равна нулю вне *M**.

Следствие 1. *Если* Φ *— характеристическая функция К-решетки L в E, то* $\alpha(L)^{-1}\Phi^*$ *— характеристическая функция К-решетки* L_* *в E*, двойственной к L, и* $\alpha^*(L_*) = \alpha(L)^{-1}$, *где* α* *— мера, двойственная к* α.

Первое утверждение вытекает из (2) при $L = M$, $\Phi(0) = 1$, поэтому обратное преобразование Фурье функции Φ^* равно $\alpha^*(L_*)\,\alpha(L)\,\Phi$. Поскольку последняя функция должна совпасть с Φ, получаем второе утверждение.

Следствие 2. *Каждая стандартная функция на E допустима для E.*

Это — очевидное .следствие предложения 2 и определений.

В очередном следствии отождествим K с топологическим двойственным к нему при помощи характера χ на K способом, объясненным в п.16.2.5, т. е. принимая, что $\langle x, y\rangle = \chi(xy)$ при $x, y \in K$. После такого отождествления можно говорить о самодвойственной мере на K.

Следствие 3. *Пусть R — максимальное компактное подкольцо в K, φ— его характеристическая функция, χ — нетривиальный характер на K порядка ν и α — самодвойственная мера на K при отождествлении K с его двойственным при помощи χ. Пусть элемент $a \in K^\times$ таков, что $\operatorname{ord}_K(a) = \nu$. Тогда $\alpha(R) = \operatorname{mod}_K(a)^{1/2}$ и преобразованием Фурье функции φ является функция $y \to \operatorname{mod}_K(a)^{1/2}\,\varphi(ay)$.*

Применим к $E = K$, $L = R$ следствие 1. Тогда по предложению 12 п.16.2.5 $L_* = P^{-\nu}$, т. е. $L_* = a^{-1}R$, если элемент a таков, как сказано выше. Характеристическая функция K-решетки L_* равна $\varphi(ay)$, и $\alpha(L_*) = \operatorname{mod}_K(a)^{-1}\alpha(R)$. Теперь наше утверждение вытекает из следствия 1.

Определение 2. *Пусть E — векторное пространство конечной размерности над* **R**. *Под стандартной функцией на E мы будем понимать любую функцию вида $e \to p(e)\exp(-q(e))$, где p — комплексная полиномиальная функция на E, а q — вещественная положительно определенная квадратичная форма на E.*

Предложение 3. *Пусть E таково, как в определении* 2. *Тогда каждая стандартная функция на E обладает преобразованием Фурье, причем последнее также является стандартной функцией, и каждая стандартная функция допустима для (E, L), где L — любая* R-*решетка в E.*

Выберем такой базис в E над **R**, чтобы при отождествлении E с $\mathbf{R}^n$ при помощи этого базиса квадратичная форма q имела вид $q(x) = \pi\sum x_\nu^2$. Очевидно, что первое утверждение достаточно доказать для функции $M(x)\exp(-q(x))$, где $M(x)$ — одночлен от x_ν. По теореме 3 п.16.2.5 мы можем отождествить пространство $\mathbf{R}^n$ с двойственным к нему, полагая $\langle x, y\rangle = \mathbf{e}(\sum x_\nu y_\nu)$. Мы видим, что достаточно рассмотреть случай n=1, т. е. показать, что преобразование

Фурье функции $x^m \exp(-\pi x^2)$ является стандартной функцией на $\mathbf{R}$ для каждого целого числа $m \geqslant 0$. Но, как следует из хорошо известной формулы

$$\exp(-\pi y^2) = \int \exp(-\pi x^2 + 2\pi i x y)\, dx,$$

преобразованием Фурье функции $\exp(-\pi x^2)$ является функция $\exp(-\pi y^2)$. Дифференцируя обе части формулы m раз по y и используя индукцию по m, убеждаемся, что левая часть будет иметь вид $p_m(y) \exp(-\pi y^2)$, где p_m — многочлен степени m, а в правой части дифференцирование может быть внесено под знак интеграла. Это дает

$$p_m(y) \exp(-\pi y^2) = \int (2\pi i x)^m \exp(-\pi x^2 + 2\pi i x y)\, dx,$$

чем доказано первое утверждение предложения. Пусть теперь L — некоторая $\mathbf{R}$-решетка в E. По предложению 11 п.16.2.4 существует базис векторного пространства E над $\mathbf{R}$, порождающий группу L. Другими словами, отождествляя E с $\mathbf{R}^n$ посредством этого базиса, можно считать, что $E = \mathbf{R}^n$ и $L = \mathbf{Z}^n$. Для того чтобы доказать, что стандартные функции на $\mathbf{R}^n$ допустимы для $(\mathbf{R}^n, \mathbf{Z}^n)$, достаточно показать, что для любой такой функции Φ ряд $\sum |\Phi(x + v)|$, взятый по всем $v \in \mathbf{Z}^n$, равномерно сходится на каждом компактном подмножестве C в R^n. Положим $\Phi(x) = p(x) \exp(-q(x))$ и $r(x) = \sum x_v^2$. Выберем такое $\delta > 0$, чтобы квадратичная форма $q - \delta r$ была положительно определена; для этого достаточно взять $\delta < \mu$, где μ — нижняя грань функции q на сфере $r = 1$. Тогда $\Phi(y) \exp(\delta r(y - x)) \to 0$ при $r(y) \to \infty$ равномерно по $x \in C$.

Отсюда следует, что эта функция ограничена при $x \in C$ и при всех $y \in \mathbf{R}^n$. Поэтому, заменяя y на $x + u$, получаем, что для некоторого $A > 0$

$$|\Phi(x + u)| \leqslant A \exp(-\delta r(u))$$

при всех $x \in C$, откуда

$$\sum_v |\Phi(x+v)| \leqslant A \sum_v \exp\Big(-\delta \sum_i v_i^2\Big) = A\Big(\sum_{v=-\infty}^{+\infty} \exp(-\delta v^2)\Big)^n,$$

чем и заканчивается доказательство.

Для некоторых специальных случаев предложения 3, в которых $E = \mathbf{R}$ или $\mathbf{C}$, нам понадобятся более точные утверждения. Выберем *базисный* характер χ на $\mathbf{R}$ (соотв. на $\mathbf{C}$) и отождествим с помощью этого характера пространство $\mathbf{R}$ (соотв. $\mathbf{C}$) с топологическим двойственным к нему подобно тому, как мы делали это выше для p-полей (см. п.16.2.5).

Самодвойственные меры будем брать относительно этого отождествления.

Предложение 4. *Самодвойственной мерой на* $\mathbf{R}$, *соответствующей базисному характеру* $\chi(x) = \mathbf{e}(-ax)$, *где* $a \in \mathbf{R}^{\times}$, *является мера* $d\alpha(x) = |a|^{1/2} dx$. *Если* $\varphi_A(x) = x^A \exp(-\pi x^2)$, *где* $A = 0$ *или* 1, *то преобразованием Фурье функции* φ_A *является функция* $\varphi'_A(y) = i^{-A} |a|^{1/2} \varphi_A(ay)$.

Положим $d\alpha(x) = c \cdot dx$, где $c \in \mathbf{R}^{\times}_{+}$. Тогда φ'_0 задается формулой

$$\varphi'_0(y) = c \int_{\mathbf{R}} \exp(-\pi x^2 - 2\pi i a x y)\, dx;$$

как уже отмечалось, последнее выражение равно $c\varphi_0(ay)$. Применяя теперь формулу обращения Фурье и лемму 1, получаем $c = |a|^{1/2}$. Дифференцируя обе части формулы для $\varphi'_0(y)$ по y, получаем преобразование Фурье функции φ_1.

Предложение 5. *Самодвойственной мерой на* $\mathbf{C}$, *соответствующей базисному характеру* $\chi(x) = \mathbf{e}(-ax - \bar{a}\bar{x})$, *где* $a \in \mathbf{C}^{\times}$, *является мера* $d\alpha(x) = (a\bar{a})^{1/2} |dx \wedge d\bar{x}|$. *Если* $\varphi_A(x) = x^A \exp(-2\pi x\bar{x})$, *где* A — *целое неотрицательное число, то преобразованием Фурье функции* φ_A *является функция* $i^{-A}(a\bar{a})^{1/2} \overline{\varphi_A(ay)}$, *а преобразованием Фурье функции* $\overline{\varphi_A}$ — *функция* $i^A (a\bar{a})^{1/2} \varphi_A(ay)$.

Доказательства утверждений относительно α и относительно преобразования Фурье функции φ_0 совершенно аналогичны доказательствам аналогичных утверждений в предложении 4. Дифференцируя A раз по y формулу для преобразования Фурье функции φ_0, получаем преобразование Фурье от φ_A из которого получается преобразование Фурье функции $\overline{\varphi_A}$.

Определение 3. *Пусть* E — *векторное пространство конечной размерности над* $\mathbf{A}$-*полем* k, ε — *базис в* E *над* k, *и пусть для каждой конечной точки* v *поля* k ε_v *есть* r_v-*модуль, порожденный в* E_v *базисом* ε. *Под стандартной функцией на* E_A *будем понимать функцию вида*

$$e = (e_v) \to \Phi(e) = \prod_v \Phi_v(e_v),$$

где Φ_v — *стандартная функция на* E_v *для каждой точки* v *поля* k *и* Φ_v — *характеристическая функция модуля* ε_v *почти для всех* v.

Следствие 1 теор. 3 п.16.3.1 показывает, что последнее условие не зависит от выбора базиса ε. Формула, которая определяет функцию Φ и которую мы будем записывать короче так: $\Phi = \prod \Phi_v$, имеет смысл

в силу предложения 1 п.16.4.1, согласно которому почти все сомножители в правой части равны 1 для любого e из E_A. Это предложение показывает также, что функция Ф равна нулю вне $E_{\mathbf{A}}(P, \varepsilon)$ для подходящего P, т. е. что Ф непрерывна.

Аналогично случаю k_A в п.16.5.4 меру Хаара на E_A можно определить, выбрав для каждой точки v меру Хаара α_v на E_v так, чтобы $\alpha_v(\varepsilon_v) = 1$ почти для всех v. В случае когда меры α_v удовлетворяют последнему условию, будем говорить, что они *когерентны*. В этом случае существует единственная мера α на E_A, которая совпадает с произведением мер $\prod \alpha_v$ на каждой открытой подгруппе $E_{\mathbf{A}}(P, \varepsilon)$ в $E_{\mathbf{A}}$. Для этой меры будем писать $\alpha = \prod \alpha_v$. Ясно, что для любой меры Хаара α на E_A можно найти когерентную систему мер α_v, для которой $\alpha = \prod \alpha_v$, выбирая какое-нибудь множество когерентных мер на пространствах E_v и соответствующим образом изменяя каждую из них.

Начиная с этого места, мы выберем *базисный* характер χ на k_A, т. е. нетривиальный характер на k_A, тривиальный на k. Обозначим через χ_v характер на k_v, индуцированный характером χ. Этот характер нетривиален по следствию 1 теор. 3 п.16.4.2. Для любого векторного пространства E конечной размерности над k обозначим через E' алгебраическое двойственное к нему и с помощью χ и χ_v отождествим топологические двойственные к E_A и E_v с $E'_{\mathbf{A}}$ и E'_v соответственно, способом, описанным в п.16.4.2, т. е. используя теорему 3 п.16.4.2 в случае первого пространства и теорему 3 п.16.2.5 в случае второго для каждой точки v.

Теорема 1. *Пусть E — векторное пространство конечной размерности над* **A***-полем k, α_v — когерентные меры Хаара на пространствах E_v и $\Phi = \prod \Phi_v$ — стандартная функция на E_A. Тогда преобразованием Фурье функции Ф относительно меры $\alpha = \prod \alpha_v$ на E_A является стандартная функция на $E'_{\mathbf{A}}$, задаваемая равенством $\Phi' = \prod \Phi'_v$, где для каждой v функция Φ'_v есть преобразование Фурье функции Φ_v относительно меры α_v. При этом* Ф *допустима для (E_A, E).*

Пусть ε, ε' — базисы в E, E' над k. Для каждой конечной точки v определим ε_v, как выше, и ε'_v аналогичным образом. По следствию 3 теор. 3 п.16.4.2 существует такое содержащее P_∞ конечное множество P точек поля k, что k_v-решетка ε'_v двойственна к ε_v для v, не лежащих в P. Ввиду нашего предположения о α_v можно считать, что множество P выбрано так, что $\alpha_v(\varepsilon_v) = 1$ при $v \notin P$. Тогда по следствию 1 предл. 2 преобразование Фурье характеристической функции модуля ε_v будет

характеристической функцией модуля ε'_v и $\alpha'_v(\varepsilon'_v) = 1$ для двойственной к α_v меры α'_v при всех $v \notin P$. Пусть теперь $\Phi = \prod \Phi_v$ — стандартная функция на E_A. Для каждой точки v ооозначим через Φ'_v преобразование Фурье функции Φ_v относительно меры α_v. Из только что сказанного и из предложений 2 и 3 следует, что $\Phi' = \prod \Phi'_v$ — стандартная функция на E'_A. Покажем, что эта функция является преобразованием Фурье от Ф. Заменяя, если это необходимо, P большим множеством, можно считать, что Φ_v является характеристической функцией модуля ε_v при $v \notin P$. Тогда носитель функции Ф содержится в $E_{\mathbf{A}}(P, \varepsilon)$, так что преобразование Фурье Φ'' функции Ф задается интегралом

$$\Phi''(e') = \int \Phi(e)\,\chi([e, e'])\,d\alpha(e),$$

взятым по $E_{\mathbf{A}}(P, \varepsilon)$. В силу наших определений подинтегральная функция здесь задается следующим образом:

$$\Phi(e)\,\chi([e; e']) = \prod_v (\Phi_v(e_v)\,\chi_v([e_v, e'_v])),$$

где $e = (e_v)$, $e' = (e'_v)$. Далее, при фиксированном e' сомножители в правой части равенства, соответствующие точкам v, имеют почти для всех v постоянное значение 1 на ε_v. Согласно определению группы $E_{\mathbf{A}}(P, \varepsilon)$ в предложении 1 п.16.4.1, отсюда следует, что $\Phi''(e')$ совпадает с $\Phi'(e')$.

Для того чтобы доказать допустимость Ф для (E_A, E), достаточно показать, что ряд

$$\sum_{\eta \in E} |\Phi(e+\eta)| = \sum_{\eta \in E} \left|\prod_v \Phi_v(e_v+\eta)\right| \tag{3}$$

равномерно сходится на каждом компактном подмножестве $C \subset E_{\mathbf{A}}$. По следствию 1 предложения 1 п.16.4.1 С содержится в некотором множестве $E_{\mathbf{A}}(P, \varepsilon)$. Выберем P так, чтобы множество $E_{\mathbf{A}}(P, \varepsilon)$ содержало помимо множества C еще и носитель функции Ф. Для каждой точки v из P обозначим через C_v проекцию множества C на E_v. Для каждой конечной точки из P обозначим через C'_v носитель функции Φ_v. Для v, не лежащих в P, положим $C_v = C'_v = \varepsilon_v$. Так как $\prod C_v$ компактно и содержит С, достаточно будет доказать наше утверждение для $C = \prod C_v$. Предположим сначала, что k — поле характеристики $p > 1$. Тогда функция Ф равна нулю вне компактного множества $C' = \prod C'_v$, так что все слагаемые в (3) равны нулю, кроме членов, соответствующих элементам $\eta \in E \cap C''$, где C'' — образ множества $C \times C'$ при отображении $(e, e') \to e' - e$. Так как C''

компактно, то $E \cap C^{n}$ конечно, и наше утверждение очевидно. Пусть теперь характеристика поля k равна нулю. Для каждой конечной точки $v \in P$ возьмем некоторую k_v-норму N_v на E_v и обозначим через L_v k_v-решетку тех e_v, для которых $N_v(e_v) \leqslant \mu$, где μ — верхняя грань значений нормы N_v на компактном множестве $C_v \cup C'_v$. Для точек v, не лежащих в P, положим $L_v = \varepsilon_v$. Положим, далее, $L = \bigcap (E \cap L_v)$, где v пробегает все конечные точки поля k. По теореме 2 п.16.4.2 L является k-решеткой в E с замыканиями L_v в E_v для всех конечных v. Для $e = (e_v) \in C$, очевидно, $\Phi_v(e_v + \eta) = 0$ при $\eta \notin E \cap L_v$, так что $\Phi(e + \eta) = 0$ при η, не лежащих в L. Кроме того, если A_v — верхняя грань $|\Phi_v|$ для каждой конечной точки v поля k, то $A_v = 1$ почти для всех v. Полагая

$$A = \prod A_v,$$

мы видим, что при $e \in C$ ряд (3) мажорируется рядом

$$A \sum_{\eta \in L} \left| \prod_w \Phi_w (e_w + \eta) \right|,$$

где произведение берется по бесконечным точкам w поля k. Как объяснялось в п.16.5.2, положим $E_\infty = E \otimes_{\mathbf{Q}} \mathbf{R}$ и отождествим это пространство с произведением $\prod E_w$, взятым по бесконечным точкам поля k. Очевидно, что функция Φ_∞ на E_∞, определенная при $e_\infty = (e_w)$ формулой

$$\Phi_\infty (e_\infty) = \prod_w \Phi_w (e_w),$$

стандартна. Поскольку L есть k-решетка в E, то L является $\mathbf{Q}$-решеткой в E, рассматриваемом как векторное пространство над $\mathbf{Q}$, а следовательно, и $\mathbf{R}$-решеткой в E_∞. Теперь остается воспользоваться предложением 3.

Следствие 1. *Если α_v — когерентные меры на E_v, то двойственные к ним меры α'_v также когерентны; мерой, двойственной к $\alpha = \prod \alpha_v$, является мера $\alpha' = \prod \alpha'_v$. Если $\alpha(E_{\mathbf{A}}/E) = 1$, то $\alpha'(E'_{\mathbf{A}}/E') = 1$.*

Первое утверждение было доказано выше; второе следует из теоремы 1 и определений. Что касается последнего утверждения, то, согласно теореме 3 п.16.4.2, E' является подгруппой в E'_A, ассоциированной по двойственности с подгруппой E в E_A. Поэтому, как мы уже видели, наше утверждение следует из формулы Пуассона, при условии что мы можем предъявить допустимую для (E_A, E) функцию Φ, для которой левая часть равенства (1) отлична от нуля. Но по теореме 1 любая стандартная функция $\Phi \geqslant 0$, для которой $\Phi(0) > 0$, обладает этим свойством.

Важен частный случай $E = E' = k$, $[x, y] = xy$. Отождествляя, как и раньше, пространства k_A и k_v с двойственными к ним при помощи характеров χ, χ_v, мы получаем в этом случае

Следствие 2. *Пусть* α, α_v — *самодвойственные меры на* $k_\mathbf{A}$, k_v. *Тогда меры* α_v *когерентны,* $\alpha = \prod \alpha_v$ *и* $\alpha(k_\mathbf{A}/k) = 1$.

Возьмем любые когерентные меры β_v на группах k_v. По следствию 1 двойственные к ним меры β_v' когерентны, откуда вытекает, что $\beta_v = \beta_v'$ почти для всех v. Другими словами, мера β_v совпадает с самодвойственной мерой α_v почти для всех v и, значит, меры α_v когерентны. Остальные наши утверждения вытекают теперь из следствия 1.

В обозначениях следствия 1 мера α на E_A, для которой $\alpha(E_\mathbf{A}/E) = 1$, известна как *мера Тамагавы* на E_A; следствие 1 показывает, что двойственная к ней мера является мерой Тамагавы на E'_A. В частности, на k_A мера Тамагавы — это то же самое, что самодвойственная мера. Для каждой конечной точки v поля k обозначим через $\nu(v)$ порядок характера χ_v; по следствию 1 теор. 3 п.16.4.2 $\nu(v) = 0$ почти для всех v. Выберем такие $a_v \in k_v^\times$, что $\mathrm{ord}_v(a_v) = \nu(v)$. Далее, для каждой вещественной точки v поля k применим к характеру $x \to \mathbf{e}(-x)$ следствие теор. 3 п.16.2.5, которое показывает, что существует один и только один элемент $a_v \in k_v^\times$, такой, что $\chi_v(x) = \mathbf{e}(-a_v x)$ при всех $x \in k_v$. Аналогично для каждой мнимой точки v существует один и только один элемент $a_v \in k_v^\times$, для которого $\chi_v(x) = \mathbf{e}(-a_v x - \overline{a_v}\,\overline{x})$ при всех $x \in k_v$. Так как $\nu(v) = 0$ почти для всех v, то $(a_v) \in k_\mathbf{A}^\times$.

Определение 4. *Пусть* χ — *нетривиальный характер на* k_A, *тривиальный на* k *и индуцирующий для каждой точки* v *характер* χ_v *на* k_v. *Идель* $a = (a_v)$ *поля* k *будем называть дифферентным иделем, связанным с* χ, *если* $\mathrm{ord}_v(a_v)$ *равен порядку* $\nu(v)$ *характера* χ_v *для каждой конечной точки* v *поля* k, $\chi_v(x) = \mathbf{e}(-a_v x)$ *для каждой вещественной точки* v *и* $\chi_v(x) = \mathbf{e}(-a_v x - \overline{a_v}\,\overline{x})$ *для каждой мнимой точки* v *поля* k.

Ясно, что для заданного χ дифферентный идель a однозначно определен по модулю $\prod r_v^\times$, где произведение берется по всем конечным точкам v поля k. Если χ_1 —другой такой характер, то по теореме 3 п.16.4.2 его можно записать в виде $\chi_1(x) = \chi(\xi x)$, где $\xi \in k^\times$. Тогда ξa, где идель a такой, как выше, будет дифферентным иделем, связанным с χ_1. Следовательно, множество всех дифферентных иделей является классом смежности в $k_\mathbf{A}^\times$ по модулю

$k^{\times} \prod r_v^{\times}$. Если k — поле характеристики $p > 1$, то a тогда и только тогда является дифферентным иделем, связанным с χ, когда $\mathbf{div}\ (a) = \mathbf{div}\ (\chi)$ в смысле, объясненном в п.16.6; откуда следует, что div (a) лежит в каноническом классе.

Предложение 6. *Пусть a — дифферентный идель. Тогда, если характеристика поля k равна нулю, то $|a|_{\mathbf{A}} = |D|^{-1}$, где D — дискриминант поля k, а если k — поле характеристики $p > 1$, $\mathbf{F}_q$ — его поле констант и g — его род, то $|a|_{\mathbf{A}} = q^{2-2g}$.*

Последнее утверждение эквивалентно равенству $\deg(\mathrm{div}\ (a)) = 2g - 2$; так как div *(a)* является каноническим дивизором, то это утверждение совпадает со следствием 1 теор. 2 п.16.6. В случае характеристики нуль пусть α, α_v — самодвойственные меры на $k_{\mathbf{A}}$, k_v, так что $\alpha = \prod \alpha_v$ (следствие 2 теор. 1). Пусть мера $\beta = \prod \beta_v$ такова, как в предложении 7 п.16.5.4. Применяя следствие 3 предложения 2 и предложения 4 и 5, получаем, что $\alpha = |a|_{\mathbf{A}}^{1/2} \beta$. Так как по следствию 2 теор. 1 $\alpha(k_{\mathbf{A}}/k) = 1$ и по предложению 7 п.16.5.4 $\beta(k_{\mathbf{A}}/k) = |D|^{1/2}$, то $|a|_{\mathbf{A}} = |D|^{-1}$.

16.7.3. Квазихарактеры

Сначала мы изложим некоторые вспомогательные результаты. Как обычно, для всякого $z \in \mathbf{C}$ обозначаем через Re (z) и Im (z) его вещественную и мнимую части и полагаем $|z| = (z\bar{z})^{1/2}$, $|z|_{\infty} = \mathrm{mod}_{\mathbf{C}}(z) = z\bar{z}$.

Лемма 2. *Характер ω группы G тривиален, если $\mathrm{Re}\ (\omega(g)) > 0$ при всех $g \in G$.*

Если $z \in \mathbf{C}$, $|z| = 1$, $z \neq 1$ и $\mathrm{Re}\ (z) > 0$, то $z = \mathbf{e}(t)$, где $t \in \mathbf{R}$, $0 < |t| < 1/4$. Обозначим через n наименьшее целое число, для которого $n|t| > 1/4$. Тогда $(n-1)|t| \leqslant 1/4$, следовательно, $1/4 < n|t| < 1/2$ и $\mathrm{Re}\ (z^n) < 0$. Поэтому подмножество в **C**, определенное условиями $|z| = 1$, $\mathrm{Re}\ (z) > 0$, не содержит иных подгрупп в $\mathbf{C}^{\times}$, кроме $\{1\}$.

Лемма 3. *Каждый гомоморфизм ω компактной группы G в $\mathbf{C}^{\times}$ является характером на G.*

В самом деле, отображение $g \to |\omega(g)|$ должно переводить G в компактную подгруппу в $\mathbf{R}_+^{\times}$, а таких подгрупп там нет, за исключением {1}.

Группа *G* называется *вполне несвязной,* если существует фундаментальная система окрестностей нейтрального элемента в *G*,

состоящая из подгрупп G. Например, если K—некоторое p-поле с максимальным компактным подкольцом R и максимальным идеалом P в R, то группы K и $K^{\times}$ вполне несвязны: подгруппы P^n в K и подгруппы $1 + P^n$ в $K^{\times}$, $n \geqslant 1$, образуют такие фундаментальные системы.

Лемма 4. *Пусть группа G локально компактна и вполне несвязна. Тогда каждое представление* $G \to \mathbf{C}^{\times}$ *локально постоянно.*

Если G компактна, то каждое такое представление является характером конечного порядка на G. Обратно, если G — компактная коммутативная группа и каждое ее представление имеет конечный порядок, то G вполне несвязна.

Если G локально компактна и вполне несвязна, то леммы 2 и 3 показывают, что каждое представление $G \to \mathbf{C}^{\times}$ тривиально на некоторой открытой подгруппе в G и, следовательно, локально постоянно. Если G компактна, то любая открытая подгруппа в G имеет конечный индекс, откуда вытекает второе утверждение леммы. Если G коммутативна и компактна, то двойственная к ней группа G* дискретна. Так как G может быть отождествлена с группой, двойственной к G^*, то в этом случае существует фундаментальная система окрестностей нуля в G, состоящая из множеств, определенных условиями вида $|\omega_i(g) - 1| \leqslant \varepsilon$ $(1 \leqslant i \leqslant N)$, где ω_i— характеры на G. Если все ω_i имеют конечный порядок, то можно найти такое $\varepsilon > 0$, что из этих неравенств следуют равенства $\omega_i(g) = 1$ при $1 \leqslant i \leqslant N$, тогда таким образом определенная окрестность является подгруппой в G.

Начиная с этого места, нас будут интересовать главным образом представления в $\mathbf{C}^{\times}$ групп вида $K^{\times}$, где K — локальное поле, и вида $k_{\mathbf{A}}^{\times}/k^{\times}$, где k — некоторое **A**-поле. Все эти группы обладают свойством, описанным в следующем определении.

Определение 5. *Группу G будем называть квазикомпактной, если она разлагается в прямое произведение компактной коммутативной группы* G_1 *и группы, изоморфной* **R** *или* **Z**. *Представление такой группы G в* $\mathbf{C}^{\times}$ *будем называть квазихарактером на G.*

Нетрудно было бы показать, что группа G квазикомпактна в том и только в том случае, когда она коммутативна и локально компактна, а двойственная к ней группа G^* локально изоморфна **R**, т. е. имеет открытую подгруппу, изоморфную **R** или $\mathbf{R}/\mathbf{Z}$; последнее условие можно даже заменить следующим более слабым: G^* имеет окрестность нуля, гомеоморфную **R**. Отсюда легко вывести, что G квазикомпактна в том и только в том случае, когда в ней имеется такая компактная подгруппа G_1, что группа G/G_1 изоморфна **R** или **Z**. Эти факты нам не понадобятся в последующем. Ясно, что если G обладает свойством,

описанным в определении 5, то G_1 является ее единственной максимальной компактной подгруппой.

Определение 6. *Для квазикомпактной группы G квазихарактер на G будем называть главным, если он тривиален на максимальной компактной подгруппе G_1 в G.*

Квазихарактеры квазикомпактной группы G очевидным образом образуют группу, которую мы будем обозначать через $\Omega(G)$ и записывать мультипликативно. Иными словами, если $\omega, \omega' \in \Omega(G)$, то мы обозначаем через $\omega\omega'$ квазихарактер $g \to \omega(g)\omega'(g)$ на G. Ясно, что главные квазихарактеры образуют подгруппу Ω_1 в $\Omega(G)$.

Предложение 7. *Пусть G — квазикомпактная группа и G_1 — ее максимальная компактная подгруппа. Тогда G имеет нетривиальные представления в $\mathbf{R}_+^\times$; если ω_1 — такое представление, то его ядро совпадает с G_1 и каждое представление $G \to \mathbf{R}_+^\times$ может быть записано одним и только одним способом в виде $g \to \omega_1(g)^\sigma$, где $\sigma \in \mathbf{R}$.*

Пусть $G = G_1 \times N$, где группа N изоморфна $\mathbf{R}$ или $\mathbf{Z}$. По лемме 3 каждое представление $\omega: G \to \mathbf{R}_+^\times$ тривиально на G_1; записывая элементы из G в виде пар (g_1, n) с $g_1 \in G_1$, $n \in N$, мы видим, что ω должно иметь вид $(g_1, n) \to \varphi(n)$, где φ — представление $N \to \mathbf{R}_+^\times$. Отождествим N с группой $\mathbf{R}$ или $\mathbf{Z}$, той, которой она изоморфна. В первом случае условие на φ означает, что отображение $n \to \log \varphi(n)$ определяет эндоморфизм группы $\mathbf{R}$ и, значит, имеет вид $n \to an$, где $a \in \mathbf{R}$, так что $\varphi(n) = \exp(an)$. В случае $N = \mathbf{Z}$ представление φ, очевидно, имеет вид $\varphi(n) = b^n$, где $b \in \mathbf{R}_+^\times$, и может быть записано в виде $\varphi(n) = \exp(an)$, где $a = \log b$. В обоих случаях φ нетривиально, если $a \neq 0$. Поэтому если ω_1 таково, как в предложении 7, то оно может быть записано в виде $\omega_1(g_1, n) = \exp(a_1 n)$, где $a_1 \neq 0$. Ядро этого представления, очевидно, равно G_1. Далее, если ω, φ, a таковы, как выше, то $\omega = (\omega_1)^\sigma$, где $\sigma = a/a_1$, причем элемент σ определен однозначно.

Следствие 1. *Пусть G, G_1 и ω_1 таковы, как в предложении 7. Тогда группа Ω_1 главных квазихарактеров на G изоморфна $\mathbf{C}$ или $\mathbf{C}^\times$, смотря по тому, чему изоморфна группа G/G_1, группе $\mathbf{R}$ или группе $\mathbf{Z}$. Каждый такой квазихарактер имеет вид*

$$g \to \omega_s(g) = \omega_1(g)^s,$$

где $s \in \mathbf{C}$. Отображение $s \to \omega_s$ является морфизмом из $\mathbf{C}$ на Ω_1. Ядро этого морфизма равно $\{0\}$ или имеет вид $a\mathbf{Z}$, где $a \in \mathbf{R}_+^\times$, смотря по тому, изоморфна G/G_1 группе $\mathbf{R}$ или $\mathbf{Z}$.

Пусть ω — произвольный квазихарактер на G. Во введенных выше обозначениях предложение 7, примененное к отображению $g \to |\omega(g)|$, показывает, что $|\omega| = \omega_\sigma$, где $\sigma \in \mathbf{R}$. Поэтому $\omega' = \omega_\sigma^{-1}\omega$ является характером на G. Если ω тривиален на G_1, то это же верно для ω', и применяя те же обозначения, что и в доказательстве предложения 7, можно записать $\omega'(g_1, n) = \psi(n)$, где ψ— характер на N. Как и в том доказательстве, отождествим группу N с изоморфной ей группой $\mathbf{R}$ или $\mathbf{Z}$; в обоих случаях $\omega_1(g, n) = \exp(a_1 n)$. Каждый характер на N может быть записан в виде $\psi(n) = \mathbf{e}(\tau n)$, где $\tau \in \mathbf{R}$; этот факт очевиден для $N = \mathbf{Z}$ и хорошо известен (и является частным случаем теоремы 3 п.16.2.5) для $N = \mathbf{R}$. Отсюда вытекает, что $\omega = \omega_s$, где $s = \sigma + 2\pi i\tau/a_1$. При этом σ и ψ однозначно определяются по ω; τ однозначно определяется по ψ в случае $N = \mathbf{R}$ и однозначно определяется по модулю $\mathbf{Z}$ в случае $N = \mathbf{Z}$. Отсюда видно, что $s \to \omega_s$ является изоморфизмом из $\mathbf{C}$ на Ω_1, если $N = \mathbf{R}$, а если $N = \mathbf{Z}$, *то* мы имеем $\omega(g_1, n) = u^n$, где $u = \exp(a_1 s)$ и $u \to \omega$ есть изоморфизм из $\mathbf{C}^\times$ на Ω_1. Доказательство закончено.

Следствие 2. *Пусть G — квазикомпактная группа, а именно прямое произведение компактной группы G_1 и группы N, изоморфной* $\mathbf{R}$ *или* $\mathbf{Z}$. *Тогда группа $\Omega(G)$ квазихарактеров на G разлагается в прямое произведение группы Ω_1, фигурирующей в следствии* 1, *и группы характеров на G, тривиальных на N; последняя группа изоморфна группе, двойственной к G_1.*

Как уже было отмечено выше, каждый квазихарактер ω на G может быть однозначно представлен в виде $\omega_\sigma\psi$, где ψ — характер на G и $\sigma \in \mathbf{R}$. Ясно, что ψ можно однозначно записать как $\psi_1\psi_2$, где ψ_1 тривиален на G_1, а ψ_2 тривиален на N. Поэтому $\omega = (\omega_\sigma\psi_1)\psi_2$ и $\omega_\sigma\psi_1 \in \Omega_1$. Последнее утверждение нашего следствия очевидно.

До сих пор мы ни слова не говорили о топологии на $\Omega(G)$. Введем на Ω_1 не только топологию, но даже комплексную структуру с помощью морфизма $s \to \omega_s$ из $\mathbf{C}$ на Ω_1, определенного в следствии 1 предл. 7. Введем на $\Omega(G)$ топологию, в которой Ω_1 является открытой подгруппой в $\Omega(G)$, и определим на $\Omega(G)$ комплексную структуру, перенеся при помощи трансляций комплексную структуру с Ω_1 на каждый класс смежности по модулю Ω_1. Тогда группа $\Omega(G)/\Omega_1$ дискретна и, следовательно, топологически изоморфна группе, двойственной к G_1, потому что та группа тоже дискретна. Компоненты связности в $\Omega(G)$ являются классами смежности по модулю Ω_1, и все они изоморфны $\mathbf{C}$ или $\mathbf{C}^\times$, в зависимости от того, какая реализуется из двух возможностей для G/G_1.

Изложенные выше понятия и результаты можно применить к случаю $G = K^{\times}$, где K — любое локальное поле с представлением $\omega_1(x) = \mathrm{mod}_K(x)$. В качестве N можно взять подгруппу $\mathbf{R}_+^{\times}$ в $K^{\times}$, если $K = \mathbf{R}$ или $\mathbf{C}$, и группу, порожденную любым простым элементом π в K, если K есть p-поле. В последнем случае это дает

Предложение 8. *Пусть K — некоторое p-поле и π— простой элемент в K. Тогда главные квазихарактеры на $K^{\times}$— это отображения вида $x \to \mathrm{mod}_K(x)^s$, где $s \in \mathbf{C}$. Группа $\Omega(K^{\times})$ квазихарактеров на $K^{\times}$ разлагается в прямое произведение группы главных квазихарактеров и группы характеров ψ на $K^{\times}$, для которых $\psi(\pi) = 1$.*

По лемме 4 каждый квазихарактер на $K^{\times}$ локально постоянен. Если буквы R и P имеют свои обычные значения, то группы $R^{\times}$ и $1+P^n$ при $n \geqslant 1$ открыты в $K^{\times}$ и образуют фундаментальную систему окрестностей единицы. Этим оправдано следующее определение.

Определение 7. *Пусть K — некоторое p-поле, R — его максимальное компактное подкольцо и P — максимальный идеал в R. Пусть, далее, ω — квазихарактер на $K^{\times}$ и f — наименьшее из тех неотрицательных целых чисел, для которых $\omega(x) = 1$ при $x \in R^{\times}$, $x - 1 \in P^f$. Тогда P^f называется ведущим идеалом для* ω.

Очевидно, что квазихарактер ω является главным в том и только в том случае, когда $f = 0$, т. е. когда его ведущий идеал совпадает с R; в этом случае мы будем говорить, что со *неразветвлен.*

Для $K = \mathbf{R}$ или $\mathbf{C}$ имеет место следующий результат.

Предложение 9. *Каждый квазихарактер* на $\mathbf{R}^{\times}$ *можно одним и только одним способом записать в виде $x \to x^{-A}|x|^s$, где $A = 0$ или 1 и $s \in \mathbf{C}$. Каждый квазихарактер на $\mathbf{C}^{\times}$ можно одним и только одним способом записать в виде $x \to x^{-A}\bar{x}^{-B}(x\bar{x})^s$, где A и B — целые числа,* $\inf(A, B) = 0$ *и $s \in \mathbf{C}$.*

Для $\mathbf{R}^{\times}$ это вытекает из предложения 7 и его следствий, поскольку здесь $G_1 = \{\pm 1\}$. Для $G = \mathbf{C}^{\times}$ группа G_1 определяется уравнением $x\bar{x} = 1$. Так как эта группа двойственна группе $\mathbf{Z}$, то ее характеры — это функции $x \to x^n$, где $n \in \mathbf{Z}$. Каждую такую функцию можно записать при $n \leq 0$ в виде $x \to (x/|x|)^{-A}$, где $A = -n \geq 0$, а при $n \geq 0$ в виде $x \to (\bar{x}/|x|)^{-B}$, где $B = n \geq 0$. Отсюда и из предложения 7 следует наше утверждение.

16.7.4. Квазихарактеры А-полей

По теореме 6 п.16.4.4 группа $k_{\mathbf{A}}^{\times}/k^{\times}$ квазикомпактна для любого **A**-поля k. Начиная с этого места, будем писать $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$. Эта группа известна как *группа классов иделей* поля k. Обозначим через $\Omega(G_k)$ группу квазихарактеров на G_k, наделенную топологией и комплексной структурой, определенными в п.16.7.3. Квазихарактеры на G_k будем очевидным образом отождествлять с представлениями $k_{\mathbf{A}}^{\times} \to \mathbf{C}^{\times}$, тривиальными на $k^{\times}$.

Поскольку $z \to |z|_{\mathbf{A}}$ есть нетривиальное представление $k_{\mathbf{A}}^{\times} \to \mathbf{R}_{+}^{\times}$, тривиальное на $k^{\times}$, то оно определяет нетривиальное представление $G_k \to \mathbf{R}_{+}^{\times}$, которое будем обозначать через ω_1 и к которому можно применить предложение 7 п.16.7.3 и его следствия, снова записывая $\omega_s = (\omega_1)^s$ при $s \in \mathbf{C}$. В частности, ядро $G_k^1 = k_{\mathbf{A}}^1/k^{\times}$ представления ω_1 является максимальной компактной подгруппой в G_k; $s \to \omega_s$ есть морфизм группы $\mathbf{C}$ на группу Ω_1 главных квазихарактеров на G_k; если ω — произвольный квазихарактер на G_k, то существует одно и только одно число $\sigma \in \mathbf{R}$, для которого $|\omega| = \omega_\sigma$. Если характеристика поля k равна нулю, то по следствию 2 теор. 5 п.16.4.4 группа G_k разлагается в прямое произведение подгруппы G_k^1 и образа N в G_k группы M, определенной в этом следствии. С другой стороны, если k — поле характеристики $p > 1$, то выберем какой-нибудь элемент $z_1 \in k_{\mathbf{A}}^{\times}$ среди тех, для которых $|z|_{\mathbf{A}}$ принимает свое наименьшее значение $Q > 1$. Поскольку, как мы видели в п.16.6, все значения $|z|_{\mathbf{A}}$ имеют вид q^n с $n \in \mathbf{Z}$, если полем констант поля k является $\mathbf{F}_q$, то $Q = q^{\nu}$, где $\nu \geqslant 1$; позже мы убедимся, что $\nu = 1$ и $Q = q$ (см. следствие 6 теорема 2 п.16.7.5). Обозначим через M подгруппу в $k_{\mathbf{A}}^{\times}$, порожденную элементом z_1 и через N — ее образ в G_k. Во всех случаях (нулевой и ненулевой характеристики) мы будем отождествлять группу N с ее образом в $\mathbf{R}_{+}^{\times}$ при отображении ω_1 так что ω_1 можно рассматривать как проекцию произведения $G_k = G_k^1 \times N$ на сомножитель N. Таким образом, $N = \mathbf{R}_{+}^{\times}$, если характеристика поля k равна нулю, а в противном случае N есть подгруппа в $\mathbf{R}_{+}^{\times}$, порожденная элементом Q. Отсюда вытекает, что в последнем случае морфизм $s \to \omega_s$ из $\mathbf{C}$ на Ω_1 имеет то же самое ядро, что и морфизм $s \to Q^s$ из $\mathbf{C}$ на $\mathbf{C}^{\times}$, т. е. $2\pi i (\log Q)^{-1} \mathbf{Z}$.

Пусть ω — произвольный квазихарактер на G_k. Рассматривая его как представление $k_{\mathbf{A}}^{\times} \to \mathbf{C}^{\times}$, тривиальное на $k^{\times}$, обозначим для каждой точки v поля k через ω_v индуцированный им квазихарактер на $k_v^{\times}$.

Поскольку группы $k_{\mathbf{A}}(P)^{\times}$, определенные в следствии предложения 2 п.16.4.3, открыты в $k_{\mathbf{A}}^{\times}$, каждая окрестность единицы в $k_{\mathbf{A}}^{\times}$ содержит подгруппу вида $\prod_{v \in P} r_v^{\times}$. Поэтому в силу леммы 2 п.16.7.3 ω тривиален на некоторой подгруппе такого вида, другими словами, квазихарактер ω_v не разветвлен почти для всех *v*. Следовательно, для всех $z = (z_v) \in k_{\mathbf{A}}^{\times}$ мы имеем $\omega(z) = \prod \omega_v(z_v)$, где произведение берется по всем точкам *v* поля *k;* для каждого *z* почти все сомножители в произведении равны 1. Мы будем писать для краткости $\omega = \prod \omega_v$.

Теперь мы можем сформулировать главную цель настоящей главы. Это — исследование интегралов вида

$$Z(\omega, \Phi) = \int\limits_{k_{\mathbf{A}}^{\times}} \Phi(j(z))\, \omega(z)\, d\mu(z), \tag{4}$$

где обозначения имеют следующий смысл. В качестве μ берется мера Хаара на $k_{\mathbf{A}}^{\times}$; в качестве ω — квазихарактер на $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$, рассматриваемый как функция на $k_{\mathbf{A}}^{\times}$; в качестве Φ — стандартная функция на k_A. Через *j* обозначается естественная биекция группы $k_{\mathbf{A}}^{\times}$ на множество обратимых элементов кольца k_A; согласно предложению 2 п.16.4.3, это — непрерывное отображение $k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}$. Допуская вольность в обозначениях, мы будем обычно писать $\Phi(z)$ вместо $\Phi(j(z))$.

Что касается меры μ, как уже было замечено в п.16.5.4 в случае характеристики нуль, такую меру можно определить, выбрав для каждой точки *v* меру Хаара μ_v на $k_v^{\times}$ таким образом, чтобы $\mu_v(r_v^{\times}) = 1$ почти для всех *v*. Мы пишем $\mu = \prod \mu_v$ для обозначения меры, которая совпадает с произведением мер $\prod \mu_v$ на каждой Подгруппе $k_{\mathbf{A}}(P)^{\times}$. Меры μ_v устроены так.

Лемма 5. *Пусть К — локальное поле и* α *— мера Хаара на К. Тогда формула* $d\mu(x) = \mathrm{mod}_K(x)^{-1}\, d\alpha(x)$ *определяет меру Хаара* μ *на* $K^{\times}$. *При этом, если К — некоторое р-поле, q — его модуль и R — максимальное компактное подкольцо, то* $\mu(R^{\times}) = (1 - q^{-1})\, \alpha(R)$.

По определению функции mod_K, при отображение $\alpha \in K^{\times}$ $x \to ax$ оставляет меру μ инвариантной, чем доказано первое утверждение. Второе следует из теоремы 6 п.16.1.4.

Предложение 10. *Пусть* $\Phi = \prod \Phi_v$ *— стандартная функция на* $k_{\mathbf{A}}$, $\omega = \prod \omega_v$ *— квазихарактер на* $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$ *и*

$\mu = \prod \mu_v$ — *мера Хаара на* $k_{\mathbf{A}}^{\times}$. *Предположим, что* $|\omega| = \omega_\sigma$, *где* $\sigma > 1$. *Тогда интеграл* $Z(\omega, \Phi)$ *в* (4) *абсолютно сходится и его значение задается также абсолютно сходящимся произведением*

$$Z(\omega, \Phi) = \prod_v \left(\int_{k_v^{\times}} \Phi_v(x)\, \omega_v(x)\, d\mu_v(x) \right). \tag{5}$$

Для каждой конечной точки v поля k положим $\Psi_v = |\Phi_v|$; для каждой бесконечной точки w поля k выберем такую стандартную функцию Ψ_w на k_w, что $\Psi_w \geqslant |\Phi_w|$. Тогда, очевидно, $\Psi = \prod \Psi_v$ будет стандартной функцией на k_A, мажорирующей $|\Phi|$, и $Z(\omega_\sigma, \Psi)$ мажорирует $Z(\omega, \Phi)$. Обозначим через $I(P)$, $J(P)$ интегралы по $k_{\mathbf{A}}(P)^{\times}$ от $\Phi\omega\, d\mu$ и $\Psi\omega_\sigma\, d\mu$ соответственно и через I_v, J_v интегралы по $k_v^{\times}$ от $\Phi_v\omega_v\, d\mu_v$ и $\Psi_v\, |\omega_v|\, d\mu_v$ соответственно; для каждой конечной точки v обозначим через I'_v, J'_v те же интегралы, но взятые по $r_v^{\times}$, а не по $k_v^{\times}$; I_v является отвечающим точке v сомножителем в правой части равенства (5). Почти для всех конечных точек v поля k функция Φ_v является характеристической функцией кольца r_v, квазихарактер ω_v неразветвлен и $\mu_v(r_v^{\times}) = 1$; пусть P_0 — такое конечное множество точек, содержащее P_∞, что эти свойства имеют место при всех v, не лежащих в P_0. Тогда $I'_v = J'_v = 1$ при $v \notin P_0$. Отсюда вытекает, что при всех $P \supset P_0$

$$I(P) = \prod_{v \in P} I_v, \quad J(P) = \prod_{v \in P} J_v.$$

Поэтому $Z(\omega_\sigma, \Psi) < +\infty$ при условии, что все интегралы J_v и бесконечное произведение сходятся. Если мы покажем, что это условие выполняется, отсюда будет следовать также, что $Z(\omega, \Phi)$, интегралы I_v и произведение $\prod I_v$ все абсолютно сходятся и что интеграл $Z(\omega, \Phi)$ равен последнему произведению, а именно это мы и хотим доказать. Для любой точки v возьмем какую-нибудь меру Хаара α_v на k_v. Тогда по лемме 5 $d\mu_v(x) = m_v\, |x|_v^{-1}\, d\alpha_v(x)$ при некотором $m_v \in \mathbf{R}_+^{\times}$. Это дает

$$J_v = m_v \int_{k_v^{\times}} \Psi_v(x)\, |x|_v^{\sigma-1}\, d\alpha_v(x).$$

Из нашего определения стандартной функции сразу видно, что последний интеграл сходится при $\sigma \geqslant 1$; на самом деле для сходимости достаточно, чтобы выполнялось неравенство $\sigma > 0$, но нам это здесь не нужно. С другой стороны, для точки v, не лежащей в P, имеем

$$J_v = \sum_{\nu=0}^{+\infty} \int\limits_{u_\nu} |x|_v^\sigma \, d\mu_v(x) = \sum_{\nu=0}^{+\infty} q_v^{-\nu\sigma} = (1 - q_v^{-\sigma})^{-1},$$

поскольку $k_v^\times \cap r_v$ является объединением попарно непересекающихся множеств $u_\nu = \pi_v^\nu r_v^\times$, $\nu \geqslant 0$. Предложение 1 п.16.7.1 показывает теперь, что произведение $\prod J_v$ сходится. Доказательство закончено.

Метод вычисления, который мы только что применили для J_v, можно применить и для интеграла I_v. Получающийся при этом результат сформулируем как следующее

Предложение 11. *Пусть K — некоторое p-поле, q — его модуль, R — его максимальное компактное подкольца и* μ *— мера Хаара на* $K^\times$, *для которой* $\mu(R^\times) = 1$. *Обозначим через* φ *характеристическую функцию кольца R. Тогда при* $\mathrm{Re}\,(s) > 0$

$$\int\limits_{K^\times} \varphi(x) \, \mathrm{mod}_K(x)^s \, d\mu(x) = (1 - q^{-s})^{-1}.$$

В самом деле, мы можем представить $K^\times \cap R$ как объединение попарно непересекающихся множеств $U_\nu = \pi^\nu R^\times = P^\nu - P^{\nu+1}$, $\nu \geqslant 0$. Тогда интеграл можно записать в виде ряда

$$\sum_{\nu=0}^{+\infty} \int\limits_{U_\nu} \mathrm{mod}_K(x)^s \, d\mu(x) = \sum_{\nu=0}^{+\infty} q^{-\nu s},$$

который абсолютно сходится при $\mathrm{Re}\,(s) > 0$ и имеет указанное выше значение.

16.7.5. Функциональное уравнение

Прежде всего мы выберем некоторую меру Хаара на $k_\mathbf{A}^\times$. А именно на компактной группе G_k^1 возьмем меру Хаара μ_1, для которой $\mu_1(G_k^1) = 1$. На группе N возьмем меру ν, для которой $d\nu(n) = n^{-1}\,dn$, если $N = \mathbf{R}_+^\times$, и $\nu(\{1\}) = 1$ в противном случае. На $G_k = G_k^1 \times N$ возьмем меру $\mu = \mu_1 \times \nu$. Наконец, на $k_\mathbf{A}^\times$ возьмем такую меру μ, образ которой в $G_k = k_\mathbf{A}^\times / k^\times$ совпадает (в объясненном в п.16.2.4 смысле) с только что определенной мерой.

Лемма 6. *Пусть* F_1 *— измеримая функция на N, причем* $0 \leqslant F_1 \leqslant 1$ *и существует компактный интервал* $[t_0, t_1]$ *в* $\mathbf{R}_+^\times$, *для которого* $F_1(n) = 1$ *при* $n \in N$, $n < t_0$, *и* $F_1(n) = 0$ *при* $n \in N$, $n > t_1$. *Тогда интеграл*

$$\lambda(s) = \int_N n^s F_1(n)\, dv(n)$$

абсолютно сходится при $\mathrm{Re}(s) > 0$. *Функцию* $\lambda(s)$ *можно аналитически продолжить до функции, мероморфной на всей s-плоскости. Если положить* $\lambda_0(s) = s^{-1}$ *в случае*

$$N = \mathbf{R}_+^\times \text{ и } \lambda_0(s) = \frac{1}{2}(1 + Q^{-s}) \times (1 - Q^{-s})^{-1}$$

вслучае $N = \{Q^\nu\}_{\nu \in \mathbf{Z}}$, *то* $\lambda - \lambda_0$ *будет целой функцией от s. Наконец, если* $F_1(n) + F_1(n^{-1}) = 1$ *при всех* $n \in N$, *то* $\lambda(s) + \lambda(-s) = 0$.

Возьмем сначала в качестве F_1 функцию f_1 для которой $f_1(n) = 1$ при $n < 1$, $f_1(1) = 1/2$, $f_1(n) = 0$ при $n > 1$. Тогда функция K равна интегралу $\int_0^1 n^{s-1}\, dn$ в случае $N = \mathbf{R}_+^\times$ и ряду $\frac{1}{2} + \sum_1^{+\infty} Q^{-\nu s}$ в случае $N = \{Q^\nu\}$. В обоих случаях при $\mathrm{Re}(s) > 0$ имеют место абсолютная сходимость и равенство $\lambda = \lambda_0$. Для произвольной функции F_1 это дает

$$\lambda(s) - \lambda_0(s) = \int_N n^s (F_1(n) - f_1(n))\, dv(n).$$

Так как $F_1 - f_1$ есть ограниченная измеримая функция с компактным носителем на N, то последний интеграл абсолютно сходится при всех s, причем сходимость равномерна на каждом компактном подмножестве s-плоскости. Следовательно, этот интеграл определяет целую функцию от s. Предположим теперь, что $F_1(n) + F_1(n^{-1}) = 1$. Так как функция f_1 обладает тем же свойством, то для функции $F_2 = F_1 - f_1$ имеем $F_2(n^{-1}) = -F_2(n)$. Заменяя в последнем интеграле n на n^{-1} и учитывая равенство $\lambda_0(-s) = -\lambda_0(s)$, получаем, что $\lambda(-s) = -\lambda(s)$.

Из леммы 6 следует, что в точке $s = 0$ функция λ имеет вычет 1, если $N = \mathbf{R}_+^\times$, и вычет $(\log Q)^{-1}$, если $N = \{Q^\nu\}$. Здесь и ниже подразумевается, что вычеты берутся относительно переменной s. Напомним, что если функция $f(s)$ от s имеет простой полюс в точке $s = s_0$, то ее вычет равен $\lim (s - s_0) f(s)$ при $s \to s_0$.

Теорема 2. *Пусть* Φ — *стандартная функция на* k_A. *Тогда функция* $\omega \to Z(\omega, \Phi)$, *определенная формулой* (4) п.16.7.4 б *случае, когда интеграл в* (4) *абсолютно сходится, может быть аналитически продолжена до функции, мероморфной на всем комплексном многообразии* $\Omega(G_k)$. *Эта функция удовлетворяет уравнению*

$$Z(\omega, \Phi) = Z(\omega_1 \omega^{-1}, \Phi'),$$

где Φ' *— преобразование Фурье функции* Φ *относительно меры Тамагавы на* k_A. *Кроме того,* $Z(\omega, \Phi)$ *голоморфна всюду на* $\Omega(G_k)$, *за исключением простых полюсов* ω_0 *и* ω_1 *с вычетами соответственно* $-\rho\Phi(0)$ *и* $\rho\Phi'(0)$, *где* $\rho = 1$, *если* $N = \mathbf{R}_+^\times$, *и* $\rho = (\log Q)^{-1}$, *если* $N = \{Q^v\}$.

Выберем на $\mathbf{R}_+^\times$ две непрерывные функции F_0, F_1 со следующими свойствами: (i) $F_0 \geqslant 0$, $F_1 \geqslant 0$, $F_0 + F_1 = 1$; (ii) существует такой компактный интервал $[t_0, t_1]$ в $\mathbf{R}_+^\times$, что $F_0(t) = 0$ при $0 < t < t_0$ и $F_1(t) = 0$ при $t > t_1$. Возьмем любое $B > 1$. Тогда при $\sigma \in \mathbf{R}$, $\sigma \leqslant B$, $t \in \mathbf{R}_+^\times$ имеем $t^\sigma F_0(t) \leqslant t_0^{\sigma - B} t^B$. Для $i = 0, 1$ запишем

$$Z_i = Z_i(\omega, \Phi) = \int\limits_{k_A^\times} \Phi(z)\, \omega(z)\, F_i(|z|_A)\, d\mu(z).$$

Положим, как и прежде, $|\omega| = \omega_\sigma$, где $\sigma \in \mathbf{R}$. По предложению 10 п.16.7.4 Z_0 и Z_1 абсолютно сходятся при $\sigma > 1$. С другой стороны, при $\sigma \leqslant B$ интеграл Z_0 мажорируется интегралом

$$\int\limits_{k_A^\times} |\Phi(z)| \cdot |z|_A^\sigma F_0(|z|_A)\, d\mu(z) \leqslant t_0^{\sigma - B} \int\limits_{k_A^\times} |\Phi(z)| \cdot |z|_A^B\, d\mu(z),$$

который сходится по предложению 10 п.16.7.4. В частности, $Z_0(\omega_s \omega, \Phi)$ абсолютно сходится при всех $s \in \mathbf{C}$, и легко проверяется, что эта сходимость равномерна по s, принадлежащим любому компактному подмножеству в $\mathbf{C}$. Так как квазихарактеры $\omega_s \omega$ при $s \in \mathbf{C}$ образуют компоненту связности элемента $\omega \in \Omega(G_k)$ и комплексная структура на этой компоненте определяется переменной s, отсюда видно, что функция $\omega \to Z_0(\omega, \Phi)$ голоморфна на всем пространстве $\Omega(G_k)$.

Теперь применим к группе $k_A^\times$, дискретной подгруппе $k^\times$ и интегралам Z_0, Z_1 формулу (6) п.16.2.4. Мы получим

$$Z_i = \int\limits_{G_k} \left(\sum_{\xi \in k^\times} \Phi(z\xi) \right) \omega(z)\, F_i(|z|_A)\, d\mu(\dot{z}),$$

где $\dot{z}$ — образ элемента $z \in k_A^\times$ в $G_k = k_A^\times / k^\times$ и подинтегральное выражение рассматривается как функция от $\dot{z}$. Здесь интегралы для Z_0, Z_1 абсолютно сходятся, если этим свойством обладают исходные интегралы для Z_0, Z_1, т. е. абсолютно сходятся при $\sigma > 1$ в случае Z_1 и при всех σ в случае Z_0.

Для каждого $z \in k_{\mathbf{A}}^{\times}$ к автоморфизму $x \to z^{-1}x$ группы k_A применима лемма 1 п.16.7.2; применяя формулу Пуассона, т. е. формулу (1) из п.16.7.2, к функции $x \to \Phi(zx)$, получаем

$$\Phi(0) + \sum_{\xi \in k^{\times}} \Phi(z\xi) = |z|_{\mathbf{A}}^{-1} \left(\Phi'(0) + \sum_{\xi \in k^{\times}} \Phi'(\xi z^{-1})\right),$$

следовательно,

$$Z_1 = \int_{G_k} \left(\sum_{\xi \in k^{\times}} \Phi'(\xi z^{-1}) + \Phi'(0) - |z|_{\mathbf{A}} \Phi(0) \right) |z|_{\mathbf{A}}^{-1} \omega(z) F_1(|z|_{\mathbf{A}})\, d\mu(\dot{z}).$$

Но то, что мы доказали для Z_0, остается верным при замене ω на $\omega_1\omega^{-1}$, Φ на Φ' и F_0 на функцию $t \to F_1(t^{-1})$. Обозначая через Z_0' результат этой замены, получаем

$$Z_0' = \int_{\mathbf{A}}^{\times} \Phi'(z) |z|_{\mathbf{A}} \omega(z)^{-1} F_1(|z_1|_{\mathbf{A}}^{-1})\, d\mu(z),$$

где интеграл абсолютно сходится и голоморфен на всем пространстве $\Omega(G_k)$. Заменим в этом интеграле z на z^{-1}. Тогда мера Хаара μ аменится на меру Хаара $c\mu$, где $c^2 = 1$, поскольку мы имеем дело с автоморфизмом второго порядка группы $k_{\mathbf{A}}^{\times}$. Следовательно, $c = 1$. После указанной замены переменной снова применим формулу 6 п.16.2.4 к $k_{\mathbf{A}}^{\times}$ и $k^{\times}$. Это даст

$$Z_0' = \int_{G_k} \left(\sum_{\xi \in k^{\times}} \Phi'(\xi^{-1} z^{-1}) \right) |z|_{\mathbf{A}}^{-1} \omega(z) F_1(|z|_{\mathbf{A}})\, d\mu(\dot{z}),$$

где интеграл опять абсолютно сходится при всех ω. Поскольку $\xi \to \xi^{-1}$ есть биекция группы $k^{\times}$ на себя, мы видим, что

$$Z_1 - Z_0' = \int_{G_k} (\Phi'(0) - |z|_{\mathbf{A}} \Phi(0)) |z|_{\mathbf{A}}^{-1} \omega(z) F_1(|z|_{\mathbf{A}})\, d\mu(\dot{z}),$$

где интеграл абсолютно сходится при $\sigma > 1$, потому что этим свойством обладают интегралы Z_1 и Z_0'. По следствию 2 предложения 7 п.16.2.3 $\omega = \omega_s \psi$, где ψ— характер на G_k, тривиальный на N. В силу нашего определения μ как меры $\mu_1 \times \nu$ на $G_k = G_k' \times N$ последняя формула может быть переписана следующим образом:

$$Z_1 - Z_0' = \left(\int_{G_k^1} \psi\, d\mu_1 \right) \cdot \left(\int_N (\Phi'(0) - n\Phi(0))\, n^{s-1} F_1(n)\, d\nu(n) \right).$$

Первый сомножитель в правой части есть 1 или 0 в зависимости от того, тривиален или нет характер ψ, т. е. является или не является главным квазихарактер ω. Обозначим этот сомножитель через δ_{ω}.

Второй сомножитель можно сразу вычислить с помощью леммы 6. В результате получаем

$$Z_1 - Z_0' = \delta_\omega (\Phi' (0) \lambda (s - 1) - \Phi (0) \lambda (s)),$$

где λ — функция, определенная в упомянутой лемме. Поскольку $Z (\omega, \Phi) = Z_0 + Z_1$, нами доказано, что функцию $Z (\omega, \Phi)$ можно продолжить до функции, голоморфной всюду на $\Omega (G_k)$, кроме компоненты связности Ω_1 точки $\omega_0 = 1$, а на этой компоненте — до мероморфной функции, имеющей самое большее те же полюсы, что и функции $\lambda (s - 1)$ и $\lambda (s)$. Что касается последних полюсов и их вычетов, то они даются леммой 6 и являются именно такими, как утверждается в теореме.

Наконец, предположим, что мы выбрали F_0, F_1 так, что $F_0 (t) = F_1 (t^{-1})$ при всех t. Это можно сделать, взяв в качестве F_1 такую непрерывную при $t \geqslant 1$ функцию, что $0 \leqslant F_1 (t) \leqslant 1$ при всех $t \geqslant 1$, $F_1 (1) = 1/2$ и $F_1 (t) = 0$ при $t \geqslant t_1$, и положив, $F_1 (t) = 1 - F_1 (t^{-1})$ при $0 < t < 1$ и $F_0 = 1 - F_1$. При таком выборе Имеем $Z_0' = Z_0 (\omega_1 \omega^{-1}, \Phi')$ и потому

$$Z (\omega, \Phi) = Z_0 (\omega, \Phi) + Z_0 (\omega_1 \omega^{-1}, \Phi') + \delta_\omega (\Phi' (0) \lambda (s - 1) - \Phi (0) \lambda (s)).$$

Заменим в этой формуле ω на $\omega_1 \omega^{-1}$ и Φ на Φ'. В силу формулы обращения Фурье функция Φ' перейдет при этом в функцию Φ'', для которой $\Phi'' (x) = \Phi (-x)$. Так как квазихарактер ω тривиален на $k^\times$, то $\omega (-1) = 1$ и, значит, $\omega (-z) = \omega (z)$ при всех z, так что $Z_0 (\omega, \Phi'')$ совпадает с $Z_0 (\omega, \Phi)$. Поэтому наша замена приводит просто к перестановке первых двух членов в правой части формулы. Поскольку при этом s заменяется на $1 - s$, то согласно лемме 6 последний член не меняется. Этим завершается вывод «функционального уравнения» в теореме 2.

Следствие 1. *Пусть P — конечное множество точек поля k, содержащее P_∞. Тогда произведение*

$$p (k, P, s) = \prod_{v \notin P} (1 - q_v^{-s})^{-1}$$

абсолютно сходится при $\mathrm{Re}\,(s) > 1$ и функция $(s - 1)\, p (k, P, s)$ стремится при $s \to 1$ к конечному строго положительному пределу.

Первое утверждение содержится в следствии 1 предл. 1 п.16.7.1. Далее, возьмем такие же меры Хаара α_v на k_v и μ_v на $k_v^\times$, как и выше. По лемме 5 п.16.7.4 для каждой точки v имеем $d\mu_v (x) =$

$= m_v \mid x \mid_v^{-1} d\alpha_v(x)$, где $m_v > 0$. Возьмем такую стандартную функцию Ф, что Φ_v есть характеристическая функция кольца r_v при всех $v \notin P$, $\Phi_v \geqslant 0$ и $\Phi_v(0) > 0$ при всех v. Применим к $Z(\omega_s, \Phi)$ при $\mathrm{Re}(s) > 1$ предложение 10 п.16.7.4. Сомножитель I_v, соответствующий точке v, в правой части этого предложения может быть теперь записан в виде

$$I_v = m_v \int_{k_v^\times} \Phi_v(x) \mid x \mid_v^{s-1} d\alpha_v(x).$$

При $v \notin P$ согласно предложению 11 п.16.7.4 I_v отличается от $(1 - q_v^{-s})^{-1}$ лишь скалярным множителем $\mu_v(r_v^\times)$, который всегда >0 и который равен 1 почти для всех v. Для $v \in P$, как легко проверить, функция I_v непрерывна при $\mathrm{Re}(s) \geqslant 1$ (легко показать, что на самом деле эта функция голоморфна при $\mathrm{Re}(s) > 0$, и в следующем параграфе будет получен намного более точный результат при одном специальном выборе Ф). При $s \to 1$ имеем $I_v \to m_v \int \Phi_v \, d\alpha_v > 0$. Отсюда видно, что функция $Z(\omega_s, \Phi)$ отличается от произведения $p(k, P, s)$ из нашего следствия лишь на множитель, который стремится к конечному положительному пределу при $s \to 1$. С другой стороны, теорема 2 показывает, что $Z(\omega_s, \Phi)$ имеет простой полюс в точке $s=1$ с вычетом $\rho\Phi'(0)$, где $\rho > 0$. Поскольку $\Phi'(0) = \int \Phi \, d\alpha$ и последний интеграл, очевидно, положителен, наше доказательство закончено.

Следствие 2. *Пусть P — таково, как выше, и пусть ω — такой нетривиальный характер на $k_A^\times$, тривиальный на $k^\times$, что ω_v неразветвлен для всех $v \notin P$; для таких v положим $\lambda(v) = \omega_v(\pi_v)$, где π_v — простой элемент в k_v. Тогда произведение*

$$p(k, P, \omega, s) = \prod_{v \notin P} (1 - \lambda(v) q_v^{-s})^{-1}$$

абсолютно сходится при $\mathrm{Re}(s) > 1$ *и стремится к конечному пределу при $s \to 1$; если характер ω^2 нетривиален, то этот предел отличен от нуля.*

Так как ω — характер, то $\mid \lambda(v) \mid = 1$ для всех $v \notin P$, так что первое утверждение содержится опять в следствии 1 предл. 1 п.16.7.1. Возьмем такие же α_v, μ_v, как и выше, и выберем Ф так, чтобы Φ_v была характеристической функцией кольца r_v при $v \notin P$. Применим к $Z(\omega_s, \omega, \Phi)$ при $\mathrm{Re}(s) > 1$ предложение 10 п.16.7.4. Сейчас сомножитель I_v имеет вид

$$I_v = m_v \int_{k_v^\times} \Phi_v(x)\,\omega_v(x)\,|x|_v^{s-1}\,d\alpha_v(x).$$

При $v \notin P$ характер ω_v неразветвлен и может быть записан в виде $\omega_v(x) = |x|_v^{s_v}$, где s_v определяется равенством $\lambda(v) = q_v^{-s_v}$. Предложение 11 п.16.7.4 показывает, что I_v отличается от $(1-\lambda(v)\,q_v^{-1})^{-1}$ лишь скалярным множителем $\mu_v(r_v^\times)$, который равен 1 почти для всех v. Как и выше, замечаем, что для $v \in P$ функция I_v непрерывна при $\mathrm{Re}(s) \geqslant 1$. Учитывая для бесконечных точек предложение 9, легко получаем, что для каждой точки $v \in P$ функцию Φ_v можно выбрать так, чтобы $I_v \neq 0$ при $s=1$; мы будем предполагать, что она так и выбрана (при некоторых специальных выборах Φ_v интеграл I_v будет точно подсчитан в п.16.7.7). Мы видим, что функция $Z(\omega_s\omega, \Phi)$ отличается от произведения $p(k, P, \omega, s)$ из нашего следствия лишь множителем, который при $s \to 1$ стремится к конечному, отличному от нуля пределу. Ввиду теоремы 2 этим доказано второе утверждение нашего следствия. Для доказательства последнего утверждения следствия нам понадобится следующая лемма.

Лемма 7. *Для* $t \in \mathbf{C}$, $\lambda \in \mathbf{C}$ *положим* $\varphi(\lambda, t) = (1-t)^3 \times (1-\lambda t)^4 (1-\bar{\lambda}^2 t)$. *Тогда* $|\varphi(\lambda, t)| < 1$ *при* $t \in \mathbf{R}$, $0 < t < 1$, $\lambda\bar{\lambda} = 1$.

В самом деле, мы имеем

$$\log|\varphi(\lambda, t)|^2 = \log(\varphi(\lambda, t)\,\varphi(\bar{\lambda}t)) =$$

$$= -\sum_{n=1}^{\infty} \frac{t^n}{n}(6 + 4\lambda^n - 4\bar{\lambda}^n + \lambda^{2n} + \bar{\lambda}^{2n}) =$$

$$= -\sum_{n=1}^{\infty} \frac{t^n}{n}(2 + \lambda^n + \bar{\lambda}^n)^2 < 0.$$

Если теперь функция $\varphi(\lambda, t)$ определена, как в лемме, то

$$p(k, P, s)^3\, p(k, P, \omega, s)^4\, p(k, P, \omega^2, s) = \prod_{v \notin P} \varphi(\lambda(v)\,q_v^{-s})^{-1}.$$

Согласно лемме, это произведение по абсолютной величине > 1 при $s \in \mathbf{R}$, $s > 1$, так что оно не может стремиться к 0 при $s \to 1$. При s, стремящемся к 1, как было показано выше, $p(k, P, \omega^2, s)$ стремится к конечному пределу, если характер ω^2 нетривиален, и $p(k, P, \omega, s)$ есть произведение сомножителя, стремящегося к отличному от нуля конечному пределу, и функции $Z(\omega_s\omega, \Phi)$, которая голоморфна в некоторой окрестности точки $s = 1$. Поэтому

если $p(k, \omega, P, s)$ стремится к нулю, то эта функция должна иметь вид $F(s)(s-1)$, где функция F ограничена. Ввиду следствия 1 отсюда следует, что левая часть последней формулы стремится к нулю при $s \to 1$, чем и заканчивается наше доказательство.

Отметим тот важный факт, что заключение нашего следствия остается справедливым даже для $\omega^2 = 1$.

Следствие 3. *Пусть k_0 — некоторое* **A***-поле, содержащееся в k, и пусть V — такое множество конечных точек поля k, что почти для всех конечных точек $v \notin V$ поля k модулярная степень поля k_v над замыканием поля k_0 в k_v больше единицы. Тогда произведение*

$$q(k, V, s) = \prod_{v \notin V} (1 - q_v^{-s})^{-1}$$

абсолютно сходится при $\mathrm{Re}(s) > 1$ *и функция* $(s-1)\,q(k, V, s)$ *стремится при* $s \to 1$ *к конечному строго положительному пределу.*

В самом деле, в обозначениях следствия 1 $p(k, P_\infty, s)$ есть произведение нашего произведения $q(k, V, s)$ на аналогичное произведение, взятое по множеству M всех конечных точек v поля k, не лежащих в V. Применяя к последнему произведению следствие 3 предл. 1 п.16.7.1, а к $p(k, P_\infty, s)$ —следствие 1, получаем наше утверждение. Из нашего следствия вытекает, что множество V не может быть конечным, другими словами, что существует бесконечно много точек v поля k, для которых соответствующая модулярная степень равна единице.

Следствие 4. *Пусть k_0 и V таковы, как в следствии* 3, *и пусть k' — сепарабельное алгебраическое расширение поля k конечной степени n. Предположим, что над каждой точкой $v \in V$ существует n различных точек поля k'. Тогда $k' = k$.*

Обозначим через V множество точек поля k', лежащих над точками из V. По следствию 1 теор. 4 п.16.3.4, если $v \in V$ и w лежит над v, то $k'_w = k_v$, следовательно $q'_w = q_v$. Для любой точки v поля k и любой лежащей над v точки w поля k' модулярная степень k'_w над замыканием поля k_0 в k_v не меньше модулярной степени поля k_v над этим замыканием. Поэтому почти для всех $v \notin V$, или, что то же самое, почти для всех $w \notin V'$, модулярная степень > 1.

Теперь мы можем применить следствие 3 к произведениям $q(k, V, s)$ и $q(k', V', s)$. Так как последнее произведение равно $q(k, V, s)^n$, мы получаем $n = 1$.

Следствие 5. *Пусть k — некоторое* **A***-поле характеристики $p > 1$ и P — конечное множество точек поля k. Тогда существует такой дивизор $\mathfrak{m} = \sum m(v) \cdot v$ степени* 1 *поля k, что $m(v)=0$ при всех $v \in P$.*

Обозначим через v наибольший общий делитель степеней всех точек v, не лежащих в P. Нам надо показать, что $v = 1$. Пусть $F = \mathbf{F}_q$ — поле констант поля k. По теореме 2 п.16.1.1 в алгебраическом замыкании поля k существует поле F' из q^v элементов и это поле сепарабельно над F. Обозначим через k' композит полей k и F' и через n его степень над k; поле k' сепарабельно над k. Пусть v — произвольная точка поля k, не лежащая в P, и w — некоторая точка поля k', лежащая над v. По предложению 1 п.16.3.1 k'_w порождается над k_v полем k', а следовательно, и полем F'. По определению числа v модуль поля k_v имеет вид q^{vr}, где r — целое число. Поэтому из следствия 1 теор. 7 п.16.1.4 в сочетании со следствием 2 теор. 2 п.16.1.1 вытекает, что k_v содержит подполе из q^v элементов. По теореме 2 п.16.1.1 k'_w не может содержать более одного поля из q^v элементов. Поэтому $F' \subset k_v$ и, значит, $k'_w = k_v$.

Следствие 1 теор. 4 п.16.3.4 показывает теперь, что над каждой не лежащей в P точкой v поля k имеется n различных точек поля k'. Полагая в следствии 4 $k_0 = k$ и беря в качестве V дополнение множества P, получаем $k' = k$ и, следовательно, $F' \subset F$, т. е. $v = 1$.

Следствие 6. *Пусть поле k таково, как в следствии* 5, *и* $\mathbf{F}_q$ *— его поле констант. Тогда группа N значений нормы $|z|_{\mathbf{A}}$ на $k_{\mathbf{A}}^{\times}$ порождается элементом q.*

Как мы видели в п.16.7.4, N порождается группами значений норм $|x|_v$ на $k_v^{\times}$, а следовательно, модулями $q_v = q^{\deg(v)}$ при всех v. Поэтому она имеет образующую $Q = q^v$, где v — наибольший общий делитель всех степеней $\deg(v)$. По следствию 5 $v = 1$.

Учитывая следствие 6, можно следующим образом переформулировать последнее утверждение теоремы 2 в случае характеристики $p > 1$.

Следствие 7. *Пусть k и $\mathbf{F}_q$ таковы, как в следствии* 6, *и обозначения таковы, как в теореме* 2. *Тогда функция $Z(\omega_s, \Phi) + \Phi(0)(1 - q^{-s})^{-1}$ голоморфна в точке $s = 0$.*

Это следует из только что упомянутых результатов и того факта, что функция $(1 - q^{-s})^{-1}$ имеет в точке $s = 0$ вычет $(\log q)^{-1}$.

16.7.6. Дедекиндова дзета-функция

Специальный выбор функции Φ в $Z(\omega, \Phi)$ приводит к определению важных функций на компонентах связности пространства $\Omega(G_k)$; эти функции будут подробно исследованы. Мы начнем с рассмотрения компоненты связности Ω_1 точки $\omega_0 = 1 \text{в} \Omega(G_k)$, т. е.

группы главных квазихарактеров на G_k. Функцию Φ выберем следующим образом. Для любой конечной точки v поля k возьмем в качестве Φ_v характеристическую функцию кольца r_v. В случае когда точка v вещественна, т. е. $k_v = \mathbf{R}$, возьмем $\Phi_v(x) = \exp(-\pi x^2)$. В случае когда точка v мнима, т. е. $k_v = \mathbf{C}$, возьмем $\Phi_v(x) = \exp(-2\pi x\bar{x})$. Теперь нам следует вычислить сомножители в произведении (5) для $Z(\omega, \Phi)$ при сделанном выборе Φ и при $\omega = \omega_s$. Для конечных точек v значения этих сомножителей даются предложением 11 п.16.7.4 с точностью до скалярного множителя, зависящего от μ. Для бесконечных точек эти сомножители таковы.

Лемма 8. *Пусть* G_1, G_2 *определены для всех* $s \in \mathbf{C}$ *формулами*

$$G_1(s) = \pi^{-s/2}\,\Gamma(s/2), \quad G_2(s) = (2\pi)^{1-s}\,\Gamma(s).$$

Тогда при $\mathrm{Re}(s) > 0$ *имеем*

$$\int_{\mathbf{R}^\times} \exp(-\pi x^2)\,|x|^{s-1}\,dx = G_1(s),$$

$$\int_{\mathbf{C}^\times} \exp(-2\pi x\bar{x})\,(x\bar{x})^{s-1}\,|dx \wedge d\bar{x}| = G_2(s).$$

Это сразу становится видно, если сделать замену переменных, а именно $|x| = t^{1/2}$ в первом интеграле и $x = t^{1/2}e(u)$ во втором, где $t \in \mathbf{R}_+^\times$, $u \in \mathbf{R}$, $0 \leqslant u < 1$; в последнем случае

$$|dx \wedge d\bar{x}| = 2\pi\,dt\,du.$$

Рассмотрим теперь меру $\gamma = \prod \gamma_v$ на $k_{\mathbf{A}}^\times$, где γ_v таковы, что $\gamma_v(r_v^\times) = 1$ для каждой конечной точки v, $d\gamma_v(x) = |x|^{-1}\,dx$, если точка v вещественна, и $d\gamma_v(x) = (x\bar{x})^{-1}\,|dx \wedge d\bar{x}|$, если точка v мнима. Для поля k характеристики нуль эта мера уже рассматривалась в предложении 9 п.16.5.4. Соотношение между мерой γ и мерой μ, введенной в начале п.16.7.5, таково.

Предложение 12. *Пусть мера* μ *такая, как в* п.16.7.5, *а мера* γ *такая, как выше. Если характеристика поля* k *равна нулю, то* $\gamma = c_k\mu$, *где* c_k *— число, определенное в предложении* 9 п.16.5.4. *Если* k *— поле характеристики* $p > 1$ *с полем констант* $\mathbf{F}_q$ *и* h *— числоклассов дивизоров степени* 0 *поля* k, *то* $\gamma = c_k\mu$, *где*

$$c_k = h/(q-1).$$

Ввиду нашего определения меры μ первое утверждение есть просто переформулировка предложения 9 п.16.5.4. Пусть теперь характеристика поля k равна $p > 1$. Положим $U = \prod r_v^\times$. Эта группа

обозначалась в п.16.4.4 через $\Omega(\varnothing)$; это открытая подгруппа в $k_{\mathbf{A}}^{\times}$. По определению $\gamma(U) = 1$. Как и в п.16.2.4, будем обозначать по-прежнему через γ образ меры γ в $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$. Если, как и выше, G_k^1 — образ в G_k группы $k_{\mathbf{A}}^1$, то мера μ определяется условием $\mu(G_k^1) = 1$, так что $\gamma = c_k\mu$, где $c_k = \gamma(G_k^1)$. Обозначим через U' образ в G_k группы U. По теореме 8 п.16.4.4 и ее следствию ядро морфизма группы U на U', индуцированного каноническим морфизмом группы $k_{\mathbf{A}}^{\times}$ на G_k, совпадает с $\mathbf{F}_q^{\times}$, так что мы можем подсчитать $\gamma(U')$, положив в лемме 2 п.16.2.4 $G = U$, $\Gamma_1 = \mathbf{F}_q^{\times}$, $\Gamma = \{1\}$. Это дает $\gamma(U') = (q-1)^{-1}$. Ясно, что индекс подгруппы V в G_k^1 равен индексу подгруппы $k^{\times}U$ в $k_{\mathbf{A}}^1$. Но, как мы видели в п.16.6, группу $k_{\mathbf{A}}^1/k^{\times}U$ можно отождествить с группой $D_0(k)/P(k)$ классов дивизоров степени 0 поля k, поэтому наш индекс равен n. Следовательно, $\gamma(G_k^1) = h/(q-1)$.

Для каждой бесконечной точки w поля k положим $G_w = G_1$, если эта точка вещественна, и $G_w = G_2$, если она мнима. Комбинируя предложение 10 п.16.7.4, предложение 11 п.16.7.4, лемму 8 и предложение 12, мы получаем, что при $\mathrm{Re}\,(s)>1$ для функции Φ, выбранной, как указано выше, имеет место равенство

$$Z(\omega_s, \Phi) = c_k^{-1} \prod_{w \in \bar{P}_\infty} G_w(s) \prod_{v \notin \bar{P}_\infty} (1 - q_v^{-s})^{-1}, \tag{6}$$

где c_k те же, что в предложении 12. По теореме 2 п.16.7.5 левую часть можно продолжить до функции, мероморфной на всей s-плоскости. Поскольку то же самое можно сделать для сомножителей G_w, последнее произведение в правой части также можно продолжить до функции, мероморфной на всей s-плоскости. Этим оправдано следующее определение.

Определение 8. *Мероморфная функция ζ_k на s-плоскости, задаваемая при* $\mathrm{Re}\,(s) > 1$ *произведением*

$$\zeta_k(s) = \prod_v (1 - q_v^{-s})^{-1},$$

взятым по всем конечным точкам v поля k, называется дедекиндовой дзета-функцией поля k.

Если функция Φ такова, как выше, то ее преобразование Фурье Φ' дается теоремой 1 п.16.7.2 и ее следствием 2 в сочетании со следствием 3 предложения 2 п.16.7.2 и предложениями 4 и 5 п.16.7.2. А именно

$$\Phi'(y) = |a|_{\mathbf{A}}^{1/2} \Phi(ay),$$

где a — дифферентный идель, связанный с базисным характером χ. Ввиду определения функции $Z(\omega, \Phi)$ (формула (4) п.16.7.4) имеем

$$Z(\omega, \Phi') = |a|_{\mathbf{A}}^{1/2} \omega(a)^{-1} Z(\omega, \Phi);$$

в частности, при $\omega = \omega_s$, т. е. в случае $\omega(x) = |x|_{\mathbf{A}}^{s}$, получаем

$$Z(\omega_s, \Phi') = |a|_{\mathbf{A}}^{1-2s} Z(\omega_s, \Phi), \tag{7}$$

причем значение $|a|_{\mathbf{A}}$ дается предложением 6 п.16.7.2.

Теперь мы подготовлены к формулировке наших основных результатов о дзета-функции.

Теорема 3. *Пусть k — некоторое поле алгебраических чисел с r_1 вещественными точками и r_2 мнимыми точками. Обозначим через ζ_k дзета-функцию этого поля и положим*

$$Z_k(s) = G_1(s)^{r_1} G_2(s)^{r_2} \zeta_k(s).$$

Тогда Z_k является мероморфной функцией на s-плоскости, голоморфной всюду, кроме точек s = 0 и s=1, в которых у нее простые полюсы, и имеет место функциональное уравнение

$$Z_k(s) = |D|^{\frac{1}{2}-s} Z_k(1-s),$$

где D — дискриминант поля k. Вычеты функции Z_k в точках s = 0 и s = 1 равны соответственно — c_k и $|D|^{-1/2} c_k$, где

$$c_k = 2^{r_1} (2\pi)^{r_2} hR/e;$$

здесь h — число классов идеалов поля k, R — его регулятор и e — число корней из 1 в k.

Эта теорема следует из формул (6) и (7), предложения 6 п.16.7.2 и теоремы 2 п.16.7.5.

Следствие. *Дедекиндова дзета-функция $\zeta_k(s)$ имеет в точке s = 1 вычет $|D|^{-1/2} c_k$.*

Это следует из теоремы 3 и хорошо известного равенства $G_1(1) = G_2(1) = 1$.

Теорема 4. *Пусть k — некоторое* **A***-поле характеристики p>1,* $\mathbf{F}_q$*— его поле констант и g — его род. Тогда его дзета-функция может быть записана в виде*

$$\zeta_k(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

где P — многочлен степени 2g *с коэффициентами в* **Z***, для которого*

$$P(u) = q^g u^{2g} P(1/qu). \tag{8}$$

Кроме того, P (0) = 1, *а P* (1) *равно числу h классов дивизоров степени* 0 *поля k.*

В самом деле, следствие 6 теоремы 2 п.16.7.5 показывает, что морфизм $s \rightsquigarrow \omega_s$ имеет то же самое ядро, что и морфизм $s \to q^{-s}$, так что функция $\zeta_k(s)$ может быть записана в виде $R(q^{-s})$, где R — мероморфная на $\mathbf{C}^{\times}$ функция с простыми полюсами в 1 и в q^{-1}. Далее, следствие 1 предложения 1 п.16.7.1 показывает, что $R(u) \to 1$ при

$u \to 0$, так что функция R голоморфна в этой точке и R (0) = 1. Поэтому можно записать $R(u) = P(u)/(1-u)(1-qu)$, где P — целая функция на u-плоскости и P (0) = 1. Теперь формула (7) в сочетании с формулой (6) и предложением 6 п.16.7.2 дает формулу (8) нашей теоремы, из которой очевидно следует, что P является многочленом степени 2g. Наконец, следствие 7 теоремы 2 п.16.7.5 вместе с предложением 12 дает $P(1) = n$.

16.7.7. *L*-функции

Сейчас мы обобщим полученные выше результаты на случай произвольного квазихарактера на G_k. Для этого примем следующие обозначения. Пусть ω — любой квазихарактер на G_k. Как мы видели в п.16.7. 3—4, $|\omega| = \omega_\sigma$, где $\sigma \in \mathbf{R}$. Для каждой точки v обозначим через ω_v квазихарактер на $k_v^\times$, индуцированный квазихарактером ω. Для каждой конечной точки v обозначим через $p_v^{f(v)}$ ведущий идеал квазихарактера ω_v ; при этом $f(v) = 0$ в том и только в том случае, когда ω_v неразветвлен, что, как мы видели в п.16.7.4, имеет место почти для всех конечных точек поля k. Для неразветвленного ω_v запишем $\omega_v(x) = |x|_v^{s_v}$, где $s_v \in \mathbf{C}$. Очевидно, $\mathrm{Re}(s_v) = \sigma$. К бесконечным точкам поля k применимо предложение 9 п.16.7.3, которое показывает, что ω_v можно записать в виде $\omega_v(x) = x^{-A}|x|^{s_v}$ в случае вещественной точки v, где $A = 0$ или 1 и $s_v \in \in \mathbf{C}$, и в виде $\omega_v(x) = x^{-A}\bar{x}^{-B}(x\bar{x})^{s_v}$ в случае мнимой точки v, где $\inf(A, B) = 0$ и $s_v \in \mathbf{C}$. В первом случае положим $N_v = A$, так что $\mathrm{Re}(s_v) = N_v + \sigma$, а во втором случае положим $N_v = \sup(A, B)$, так что $\mathrm{Re}(s_v) = (N_v/2) + \sigma$. Поскольку компонента связности квазихарактера ω в группе $\Omega(G_k)$ всех квазихарактеров на G_k состоит из квазихарактеров $\omega_s\omega$, $s \in \mathbf{C}$, то целые числа $f(v)$ и N_v постоянны на этой компоненте. Они все равны нулю, если ω — главный квазихарактер или, более общим образом, когда ω тривиален на группе U тех иделей (z_v), для которых $|z_v|_v = 1$ для всех точек v поля k. Структура группы квазихарактеров, обладающих таким свойством, легко определяется с помощью методов, использованных при доказательстве теоремы 9 п.16.4.4.

Далее, применяя те же самые обозначения, что и выше, сопоставим каждому ω некую стандартную функцию $\Phi_\omega = \prod \Phi_v$ на k_A, определенную следующим образом. Для каждой конечной точки v, для которой $f(v)=0$, т. е. квазихарактер ω_v неразветвлен, возьмем в качестве Φ_v, как и прежде, характеристическую функцию кольца r_v.

Для каждой конечной точки v, для которой $f(v) \geqslant 1$, положим функцию Φ_v равной ω_v^{-1} на $r_v^{\times}$ и нулю вне $r_v^{\times}$. Для каждой бесконечной точки v возьмем $\Phi_v(x) = x^A \exp(-\pi x^2)$, если эта точка вещественна, и $\Phi_v(x) = x^A \bar{x}^{-B} \exp(2\pi x\bar{x})$, если она мнима, где целые числа A, B такие, как сказано выше. Определенную таким образом функцию Φ_ω будем называть *стандартной функцией, связанной с* ω. Ясно, что она не меняется при замене ω на $\omega_s\omega$ с любым $s \in \mathbf{C}$ и что функцией, связанной с $\bar{\omega}$, с $\omega^{-1} = \omega_{-2\sigma}\bar{\omega}$ и с $\omega' = \omega_1\omega^{-1}$, будет одна и та же функция $\bar{\Phi}_\omega$.

Нам нужно знать преобразование Фурье от Φ_ω, или, что ввиду теоремы 1 п.16.7.2 то же самое, преобразования Фурье функций Φ_v, определенных выше. Для вычисления этих преобразований достаточно полученных ранее результатов, за исключением случая конечной точки v с разветвленным ω_v. Для этого случая докажем следующее

Предложение 13. *Пусть K — некоторое p-поле, R — его максимальное компактное подкольцо, P — максимальный идеал в R и ω — квазихарактер на $K^{\times}$ с ведущим идеалом P^f, где $f \geqslant 1$. Пусть, далее, χ — характер порядка v на K, α — самодвойственная мера на K, соответствующая характеру χ, $b \in K^{\times}$, $\operatorname{ord}_K(b) = v + f$, и пусть φ — функция на K, равная ω^{-1} на $R^{\times}$ и нулю вне $R^{\times}$. Тогда преобразованием Фурье функции φ является функция*

$$\varphi'(y) = \varkappa \operatorname{mod}_K(b)^{1/2}\,\overline{\varphi(by)},$$

где $\varkappa$ — комплексное число, удовлетворяющее условию $\varkappa\bar{\varkappa} = 1$ и задаваемое формулой

$$\varkappa = \operatorname{mod}_K(b)^{-1/2} \int_{R^{\times}} \omega(x)^{-1}\chi(b^{-1}x)\,d\alpha(x).$$

По предложению 12 п.16.2.5 K-решетка P^f двойственна к P^{-f-v}. Так как функция φ постоянна на классах смежности в K по модулю P^f, то предложение 2 п.16.7.2 показывает, что φ' равна нулю вне $P^{-f-v} = b^{-1}R$. По определению φ имеем

$$\varphi'(y) = \int_{R^{\times}} \omega(x)^{-1}\chi(xy)\,d\alpha(x). \tag{9}$$

Очевидно, что мера, индуцированная на $R^{\times}$ мерой α, является мерой Хаара на $R^{\times}$ (это следует также из леммы 5 п.16.7.4). Возьмем элемент y, для которого $\operatorname{ord}_K(y) \geqslant -f - v + 1$. Тогда по предложению 12 п.16.2.5 функция $x \to \chi(xy)$ постоянна на классах смежности по модулю P^{f-1}. Предположим сначала, что $f = 1$. Тогда $\chi(xy) = 1$ на R, так что (9) есть интеграл по $R^{\times}$ от $\omega^{-1}\,d\alpha$; этот интеграл равен нулю,

потому что ω является нетривиальным характером на компактной группе R^x. Предположим теперь, что $f > 1$. Тогда интеграл (9) является суммой аналогичных интегралов, взятых по классам смежности по модулю P^{f-1}, содержащимся в R^x, т. е. по классам смежности в R^x по подгруппе $1 + P^{f-1}$. Поскольку из определения ведущего идеала следует, что квазихарактер ω нетривиален на подгруппе $1 + P^{f-1}$, то по той же причине, что и раньше, получаем снова, что $\varphi'(y) = 0$ в рассматриваемом случае. Теперь возьмем в (9) $y = b^{-1}u$, где $u \in R^\times$. Заменяя $u^{-1}x$ на x, получаем $\varphi'(b^{-1}u) = \omega(u)\varphi'(b^{-1})$. Этим доказано, что φ' имеет вид $c\varphi(by)$, где $c \in \mathbf{C}^\times$. Применяя формулу обращения Фурье и лемму 1 п.16.7.2, получаем $c\bar{c} = \mathrm{mod}_K(b)$. Поскольку $c = \varphi'(b^{-1})$, для $\varkappa$ имеет место формула из формулировки предложения. Равенство $\varkappa\bar{\varkappa} = 1$ для $\varkappa$, определенного этой формулой, легко проверяется непосредственно. Заметим еще, что поскольку подинтегральная функция постоянна на классах смежности в R по модулю P^f, то наш интеграл можно переписать как некоторую сумму по R/P^f. Такого типа суммы известны как *гауссовы суммы*.

Предложение 14. *Пусть* ω — *квазихарактер на* G_k *и* Φ_ω — *стандартная функция, связанная с* ω. *Тогда преобразование Фурье функции* Φ_ω, *соответствующее базисному характеру* χ *на* k_A, *определяется формулой*

$$\Phi'(y) = \varkappa\,|b|_A^{1/2}\overline{\Phi_\omega(by)} = \varkappa\,|b|_A^{1/2}\Phi_{\bar{\omega}}(by),$$

где $\varkappa = \prod \varkappa_v$, $\varkappa_v \in \mathbf{C}$, $\varkappa_v\bar{\varkappa}_v = 1$ *при всех* v, $b = (b_v) \in k_A^\times$ *и* $\varkappa_v$, b_v *задаются следующим образом. Пусть* $a=(a_v)$ — *дифферентный идель, связанный с* χ; *тогда* $b_v = a_v$ *для всякой бесконечной точки* v *и* $\mathrm{ord}_v(b_v a_v^{-1}) = f(v)$ *для всякой конечной точки* v *поля* k. *Для каждой бесконечной точки* v *поля* k *имеем* $\varkappa_v = i^{-N_v}$, *для каждой конечной точки* v, *в которой* $f(v)=0$, $\varkappa_v = 1$, *для остальных точек*

$$\varkappa_v = |b_v|_v^{-1/2}\int_{r_v^\times}\omega_v(x)^{-1}\chi_v(b_v^{-1}x)\,d\alpha_v(x),$$

где α_v — *самодвойственная мера Хаара на* k_v, *связанная с характером* χ_v. Это следует из предложения 13, предложений 4 и 5 п.16.7.2 и следствия 3 предложения 2 п.16.7.2.

Следствие. *Пусть квазихарактер* ω *таков, как в предложении* 14. *Положим* $\omega' = \omega_1\omega^{-1}$. *Тогда* $Z(\omega, \Phi_\omega) = \varkappa\,|b|_A^{-1/2} \times$ $\times\,\omega(b)\,Z(\omega', \Phi_{\omega'})$.

Согласно теореме 2 п.16.7.5, $Z(\omega, \Phi_\omega) = Z(\omega', \Phi')$ при всех ω,

где функция Φ' такова, как в предложении 14. Выразим $Z(\omega', \Phi')$ как интеграл (4) п.16.7.4, в предположении, что этот интеграл сходится; сразу видно, что это предположение выполняется при $\sigma < 0$. Представляя Φ', как в предложении 14, и производя в интеграле замену переменной $z \to b^{-1}z$, получаем правую часть формулы нашего следствия. По теореме 2 п.16.7.5 обе части можно продолжить аналитически на всю компоненту связности квазихарактера ω в $\Omega(G_k)$, так что результат справедлив всюду.

Применим теперь к $Z(\omega, \Phi_\omega)$ предложение 10 п.16.7.4. При $\sigma > 1$ это даст нам бесконечное произведение, все сомножители которого известны, за исключением сомножителей, соответствующих тем точкам *v* поля *k*, для которых $f(v) > 0$. Что касается таких сомножителей, то при нашем выборе Φ_v они, очевидно, равны $\mu_v(r_v^\times)$. Положим, как в п.16.7.6, $G_w = G_1$ в случае вещественной точки и $G_w = G_2$ в случае мнимой точки *w*. Учитывая предложение 11 п.16.7.4, лемму 8 п.16.7.6 и предложение 12 п.16.7. 6, получаем, что при $\sigma > 1$

$$Z(\omega, \Phi_\omega) = c_k^{-1} \prod_{w \in P_\infty} G_w(s_w) \prod_{v \notin P} (1 - q_v^{-s_v})^{-1}, \tag{10}$$

где *P* — множество, состоящее из всех бесконечных точек и тех конечных точек *v*, для которых $f(v) > 0$.

Для каждой точки *v* поля *k*, не принадлежащей к только что определенному множеству *P*, положим $\lambda(v) = q_v^{-s_v}$. Таким образом, мы определили $\lambda(v)$ для тех конечных точек, в которых квазихарактер ω_v неразветвлен. По определению чисел s_v для таких точек можно записать $\lambda(v) = \omega_v(\pi_v)$, где π_v — простой элемент поля k_v, или $\lambda(v) = \omega(\pi_v)$, если считать группу $k_v^\times$ вложенной как квазисомножитель в $k_\mathbf{A}^\times$. Ясно, что $|\lambda(v)| = q_v^{-\sigma}$.

Заменим теперь в (10) α на $\omega_s\omega$, где $s \in \mathbf{C}$. При этом, как отмечалось выше, Φ_ω не изменится, а правая часть равенства (10) перейдет в произведение, которое абсолютно сходится при $\mathrm{Re}(s) > 1$ — *а.* Теорема 2 п.16.7.5 показывает, что функцию $Z(\omega_s\omega, \Phi_\omega)$ можно аналитически продолжить на всю *s*-плоскость (как голоморфную функцию, если квазихарактер ω не главный). То же самое верно для сомножителей G_w, $w \in P_\infty$. Поэтому мы можем ввести мероморфную функцию $L(s, \omega)$, задаваемую при $\mathrm{Re}(s) > 1$ — σ произведением

$$L(s, \omega) = \prod_v (1 - \lambda(v) q_v^{-s})^{-1}, \tag{11}$$

взятым по всем конечным точкам v, в которых ω_v неразветвлен. Для формулировки нашего конечного результата в случае характеристики нуль введем в рассмотрение идеал $\mathfrak{f} = \prod \mathfrak{p}_v^{f(v)}$ в $\mathfrak{r}$. Он называется *ведущим идеалом квазихарактера* ω.

Теорема 5. *Пусть k — некоторое поле алгебраических чисел и ω — неглавный квазихарактер на $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$ с ведущим идеалом* $\mathfrak{f}$. *Тогда функция*

$$\Lambda(s, \omega) = \prod_{w \in P_\infty} G_w(s + s_w) \cdot L(s, \omega)$$

является целой функцией от s *и удовлетворяет функциональному уравнению*

$$\Lambda(s, \omega) = \varkappa\omega(b)(|D|\mathfrak{N}(\mathfrak{f}))^{\frac{1}{2}-s}\Lambda(1-s, \omega^{-1}),$$

где $\varkappa$ *и* b *такие, как в предложении* 14.

Это непосредственно вытекает из следствия предложения 14, если заменить ω на $\omega_s\omega$ и учесть определения a, b, $\mathfrak{f}$ и тот факт, что $|a|_{\mathbf{A}} = |D|^{-1}$. Как хорошо известно, $\Gamma(s)^{-1}$ есть целая функция, поэтому то же верно для функций $G_w(s + s_w)^{-1}$, и из теоремы 5 следует, что $L(s, \omega)$ является целой функцией от s.

Как вытекает из их определения, введенные выше функции не зависят по существу от выбора ω в заданной компоненте связности пространства $\Omega(G_k)$. Более точно, они не зависят от такого выбора с точностью до трансляции в s-плоскости, поскольку для любого $t \in \mathbf{C}$ функция $L(s, \omega_t\omega)$ совпадает с $L(s + t, \omega)$ и аналогичное утверждение справедливо для $\Lambda(s, \omega)$. Поэтому ввиду следствия 2 предложения 7 п.16.7.3 всегда можно считать, заменяя, если необходимо, ω на $\omega_{-t}\omega$ с $t \in \mathbf{C}$, что ω является характером на $k_{\mathbf{A}}^{\times}$, тривиальным на $k^{\times}$, а также на группе M, определенной в следствии 2 теор. 5 п.16.4.4. Последнее предположение можно записать так: $\sum(\delta_v s_v - N_v) = 0$, где сумма берется по бесконечным точкам поля k, s_v и N_v таковы, как выше, а $\delta_v = 1$ или 2 соответственно тому, $k_v = \mathbf{R}$ или $\mathbf{C}$. Отсюда следует, что ω является характером и, значит, $\sigma = 0$.

С другой стороны, если k — поле характеристики $p > 1$, то введем дивизор $\mathfrak{f} = \sum f(v) \cdot v$ и назовем его *ведущим дивизором для* ω.

Теорема 6. *Пусть k — некоторое* **A***-поле характеристики p>1, $\mathbf{F}_q$— его поле констант, g — его род и ω —неглавный квазихарактер на $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$ с ведущим дивизором* $\mathfrak{f}$. *Тогда $L(s, \omega) = P(q^{-s}, \omega)$, где $P(u, \omega)$— многочлен степени $2g - 2 + \deg(\mathfrak{f})$ от u и*

$$P(u, \omega) = \varkappa\omega(b) \cdot (q^{1/2}u)^{2g-2+\deg(f)} \cdot P(1/qu, \omega^{-1}),$$

где $\varkappa$ *и* b *такие, как в предложении* 14.

Тот факт, что $L(s, \omega) = P(q^{-s}, \omega)$, где функция $P(u, \omega)$ голоморфна на всей u-плоскости, доказывается точно так же, как соответствующий факт в теореме 4. Последняя формула нашей теоремы непосредственно вытекает теперь из следствия предложения 14, если заменить там ω на $\omega_s\omega$ и учесть определения a, b, f и тот факт, что $|a|_A = q^{2-2g}$. Эта формула показывает, что $P(u, \omega)$ является многочленом нужной степени.

Отметим здесь снова, что для $t \in \mathbf{C}$ функция $P(u, \omega_t\omega)$ совпадает с $P(q^{-t}u, \omega)$. Учитывая следствие 6 теор. 2 п.16.7. 5, имеем $k_A^\times = k_A^1 \times M$, где M — подгруппа в $k_A^\times$, порожденная элементом z_1 с $|z_1|_A = q$, т. е. таким элементом z_1, что $\operatorname{div}(z_1)$ имеет степень —1. Следствие 2 предл. 7 п.16.7.3 показывает, что, заменив, если необходимо, ω на $\omega_{-t}\omega$ с подходящим $t \in \mathbf{C}$, можно считать, что $\omega(z_1) = 1$. Это же следствие показывает поэтому, что ω есть характер на $k_A^\times$, т. е. $\sigma = 0$. Кроме того, сопоставляя этот факт с леммой 4 п.16.7.3 и тем очевидным обстоятельством, что в рассматриваемом сейчас случае группа $k_A^\times$, а значит, и группы k_A^1, G_k, G_k^1 вполне несвязны, убеждаемся, что ω является характером конечного порядка на $k_A^\times$.

16.8. Коэффициенты L-рядов

Пусть задано эйлерово произведение типа стоящего в правой части равенства (11). Возникает вопрос, можно ли его получить, исходя из некоторого квазихарактера ω на $k_A^\times/k^\times$. Ответ на этот вопрос, а также на несколько более общий вопрос, который будет вскоре поставлен, вытекает из следующего результата.

Предложение 15. *Пусть* P *— конечное множество точек поля* k, *содержащее* P_∞, *и пусть* G_P *— подгруппа в* $k_A^\times$, *состоящая из тех иделей* (z_v), *для которых* $z_v = 1$ *при всех* $v \in P$. *Тогда подгруппа* $k^\times G_P$ *плотна в* $k_A^\times$.

Положим $k_P = \prod_{v \in P} k_v$, где произведение берется по $v \in P$. Обозначим через A_P подгруппу в k_A, состоящую из аделей (x_v), для которых $x_v = 0$ при всех $v \in P$. Тогда $k_A = k_P \times A_P$, $k_A^\times = k_P^\times \times G_P$, и наше утверждение состоит в том, что проекция из $k_A^\times$ на $k_P^\times$ отображает $k^\times$ на всюду плотную подгруппу в $k_P^\times$. Но действительно $k_P^\times$ является открытым подмножеством в k_P и его топология индуцирована

топологией из k_P. Наше утверждение вытекает поэтому из следствия 2 теор. 3 п.16.4.2, которое показывает, что проекция из k_A на k_P отображает k на всюду плотное подмножество в k_P.

Из предложения 15 следует, что непрерывное представление ω группы $k_{\mathbf{A}}^{\times}$ в любую группу Г, тривиальное на $k^{\times}$, однозначно определено, если почти для всех v известны его значения на группах $k_v^{\times}$. В частности, в случае когда $\Gamma = \mathbf{C}^{\times}$ или в том более общем случае, когда группа Г такова, что каждый морфизм $k_{\mathbf{A}}^{\times} \to \Gamma$ тривиален на $r_v^{\times}$ почти для всех v, представление ω однозначно определено, если почти для всех v заданы значения $\omega(\pi_v)$. Ясно, что всякая конечная группа обладает таким свойством, потому что ядро каждого морфизма из $k_{\mathbf{A}}^{\times}$ в конечную группу открыто в $k_{\mathbf{A}}^{\times}$ и, следовательно, содержит

$$\prod_{v \notin P} r_v^{\times}$$

при некотором P. По тем же самым причинам, что и для $\mathbf{C}^{\times}$, тем же свойством обладает всякая группа Г, не содержащая произвольно малых подгрупп. Другой случай представлен следующим предложением.

Предложение 16. *Пусть K — некоторое p-поле, и пусть характеристика поля k не равна p. Тогда каждый морфизм $\omega: k_{\mathbf{A}}^{\times} \to K^{\times}$ тривиален на $r_v^{\times}$ почти для всех v и локально постоянен на $k_v^{\times}$, если k_v не является p-полем.*

Так как характеристика поля k не равна p, то $|p|_v = 1$ почти для всех v, а для точек v, удовлетворяющих этому условию, поле k_v не является p-полем. Поскольку каждый морфизм связной группы во вполне несвязную, очевидно, тривиален, то ω тривиален на $k_v^{\times}$, если $k_v = \mathbf{C}$, и на $\mathbf{R}_+^{\times}$, если $k_v = \mathbf{R}$. Обозначим через R максимальное компактное подкольцо в K и через P — его максимальный идеал. Пусть v — любая конечная точка поля k, для которой k_v не является p-полем, и пусть $m \geqslant 1$ таково, что ω отображает $1 + p_v^m$ в $1 + P$. Согласно предложению 8 п.16.2.3, для любого $n \geq 0$ каждый элемент $z \in 1 + p_v^m$ можно записать в виде z'^{p^n}, где $z' \in 1 + p_v^m$, поэтому $\omega(z) \in (1 + P)^{p^n}$, а следовательно, $\omega(z) \in 1 + P^{n+1}$, по лемме 5 п.16.1.4. Поскольку число n произвольно, отсюда видно, что ω тривиален на $1 + p_v^m$, а следовательно, локально постоянен на $k_v^{\times}$. В поле K имеется лишь конечное число корней из 1, что вытекает из теоремы 7 п.16.1.4 в случае характеристики p и из этой же теоремы и предложения 9 п.16.2.3 в случае характеристики нуль. Поэтому можно выбрать такое $v > 0$, что в $1 + P^v$ не содержится корней из 1,

отличных от 1. Возьмем окрестность единицы в $k_{\mathbf{A}}^{\times}$, которая морфизмом ω отображается в $1 + P^{v}$. Поскольку почти для всех v эта окрестность содержит $r_v^{\times}$, мы видим, что почти для всех v морфизм ω тривиален на $1 + p_v$ и на группе всех корней из 1 в k_v, а следовательно, и на $r_v^{\times}$.

Для каждого конечного множества P точек поля k, содержащего P_∞, положим $G'_P = \coprod_{v \notin P} r_v^{\times}$. Это — открытая подгруппа в G_P, определенная в предложении 15. Она состоит из тех иделей (z_v), для которых $z_v = 1$ при $v \in P$ и $z_v \in r_v^{\times}$, т. е. $|z_v|_v = 1$ при $v \notin P$. Пусть Γ — любая группа, обладающая описанным выше свойством, и ω — любой морфизм группы $k_{\mathbf{A}}^{\times}$ в Γ. Тогда существует такое множество P, что ω тривиален на G'_P и потому определяет морфизм $\varphi: G_P/G'_P \to \Gamma$. Если, кроме того, ω тривиален на k^x, то предложение 15 показывает, что ω однозначно определяется по φ. Обсудим теперь условия на φ, при которых такой морфизм ω существует.

Пусть k — некоторое поле алгебраических чисел и P таково, как выше. Будем говорить, что дробный идеал в k *взаимно прост* с P, если не существует простого идеала $\mathfrak{p}_v$, соответствующего точке $v \in P$ и входящего в идеал с отличным от нуля показателем. Аналогично для поля k характеристики $p > 1$ мы будем говорить, что данный дивизор *взаимно прост* с P, если не существует точки $v \in P$, входящей в этот дивизор с отличным от нуля коэффициентом. Будем обозначать через $I(P)$ (соотв. через $D(P)$) группу дробных идеалов поля k (соотв. группу дивизоров поля k), взаимно простых с P. Ясно, что морфизм $z \to \mathrm{id}(z)$ из $k_{\mathbf{A}}^{\times}$ на $I(k)$ (соотв. морфизм $z \to \mathrm{div}(z)$ из $k_{\mathbf{A}}^{\times}$ на $D(k)$) определяет изоморфизм из G_P/G'_P на $I(P)$ (соотв. на $D(P)$), с помощью которого можно отождествить эти группы друг с другом или, что то же самое, со свободной абелевой группой, порожденной точками поля k, не лежащими в P. В частности, каждый морфизм $v \to \lambda(v)$ множества этих точек в коммутативную группу Γ можно единственным образом продолжить до морфизма φ из $I(P)$ (соответственно из $D(P)$) в Γ; при этом $\varphi \circ (\mathrm{id})$ (соответственно $\varphi \circ (\mathrm{div})$) есть морфизм $G_P \to \Gamma$, тривиальный на G'_P.

Предложение 17. *Пусть* φ*— морфизм из* $I(P)$ *(соотв. из* $D(P)$*) в коммутативную группу* Γ. *Для каждой точки* $v \in P$ *пусть* g_v *— открытая подгруппа в* $k_v^{\times}$, *содержащаяся в* $r_v^{\times}$, *если точка* v *конечна. Тогда морфизм* $\varphi \circ (\mathrm{id})$ *(соотв.* $\varphi \circ (\mathrm{div})$*) группы* G_P *в* Γ *в*

том и только в том случае может быть продолжен до морфиз-ма $\omega\colon k_{\mathbf{A}}^{\times} \to \Gamma$, *тривиального на* $k^{\times}$, *когда для каждой точки* $v \in P$ *можно найти такой морфизм* $\psi_v\colon g_v \to \Gamma$, *что* $\varphi(\mathrm{id}(\xi))$ *(соотв.* $\varphi(\mathrm{div}(\xi))$*) совпадает с* $\prod \psi_v(\xi)$ *при всех* $\xi \in \bigcap (k^{\times} \cap g_v)$. *В этом случае морфизм* ω *единствен и индуцирует* ψ_v^{-1} *на* g_v *для всех* $v \in P$.

Положим $g = \prod_{v \in P} g_v$. Эту группу можно очевидным образом рассматривать как подгруппу в $k_{\mathbf{A}}^{\times}$. Тогда группа $g \cdot G_P$ является открытой подгруппой в $k_{\mathbf{A}}^{\times}$ и разлагается в прямое произведение подгрупп g и G_P. Следовательно, $k^{\times} g \cdot G_P$ является открытой подгруппой в $k_{\mathbf{A}}^{\times}$ и, значит, в силу предложения 15 совпадает с $k_{\mathbf{A}}^{\times}$. Теперь очевидно, что морфизм $g \cdot G_P \to \Gamma$ в том и только в том случае можно продолжить до морфизма группы $k_{\mathbf{A}}^{\times} = k^{\times} g \cdot G_P$, тривиального на $k^{\times}$, когда он тривиален на группе $\gamma = k^{\times} \cap \bigcap (g \cdot G_P)$, и что в этом случае продолжение единственно. Ясно, что γ совпадает с группой $\bigcap (k^{\times} \cap g_v)$ из формулировки предложения. Так как морфизм $z \to \mathrm{id}(z)$ (соотв. $z \to \mathrm{div}(z)$) тривиален на g, то он отображает $g \cdot G_P = g \times G_P$ на $I(P)$ (соотв. на $D(P)$). Поэтому если обозначить через φ_1 морфизм $\varphi \circ (\mathrm{id})$ (соотв. $\varphi \circ (\mathrm{div})$) из G_P в Γ, то мы видим, что его продолжения на $g \cdot G_P$ имеют вид $\psi^{-1}\varphi_1$, где ψ — произвольный морфизм из g в Γ. Обозначая через ψ_v морфизм, индуцированный на g_v морфизмом ψ, получаем наше утверждение.

Очевидно, что если условия предложения 17 выполняются при данном выборе групп g_v и морфизмов ψ_v, то они будут выполняться также, если заменить каждую группу g_v любой ее открытой подгруппой g_v', а ψ_v — индуцированным на ней морфизмом. Например, в случае $k_v = \mathbf{R}$ всегда можно взять $g_v = \mathbf{R}_+^{\times}$; в случае когда v — конечная точка, можно взять в качестве g_v любую из групп $1 + p_v^m$ с $m \geqslant 1$. На той же идее основано следующее

Следствие. *В условиях предложения* 17 *предположим, что группа* Γ *либо* (a) *дискретна, либо* (b) *совпадает с* $\mathbf{C}^{\times}$, *либо* (c) *совпадает с группой* $K^{\times}$, *где* $K^{\times}$ *— некоторое локальное p-поле. Тогда продолжение* ω *существует в том и только в том случае, когда можно найти группы* g_v *и морфизмы* ψ_v, *обладающие свойствами, указанными в предложении* 17, *и следующим дополнительным свойством: в случае* (a) $\psi_v = 1$ *для всех* $v \in P$; *в случае* (b) $\psi_v = 1$ *для всех конечных точек* $v \in P$; *в случае* (c) $\psi_v = 1$ *для всех точек* $v \in P$, *для которых* k_v *не является p-полем.*

В самом деле, предположим, что условия предложения ψ_v. Тогда в случае (a) мы можем для каждой точки $v \in P$ заменить g_v ядром g'_v морфизма ψ_v, поскольку это ядро является открытой подгруппой в g_v; при этомов ψ_v заменится на 1. В случае (b) можно сделать аналогичную замену для каждой конечной точки $v \in P$ (лемма 4 п.16.7.3); по тем же причинам можно точно так же поступить и в случае любой группы Г, не обладающей произвольно малыми подгруппами. Случай (c) рассматривается аналогично с использованием предложения 16.

Очевидно, достаточно проверять выполнение условий предложения 17 не для всех ξ из группы $\gamma = \bigcap (k^\times \cap g_v)$, а лишь на множестве образующих этой группы. В этой связи оказывается иногда полезным следующий результат.

Предложение 18. *В обозначениях предложения* 17 *предположим, что k — поле алгебраических чисел и* $\mathfrak{r}$ *— максимальный порядок в k. Тогда группа* $\gamma = \bigcap (k^\times \cap g_v)$ *порождается множеством* $\gamma \cap \mathfrak{r}$.

Возьмем любой элемент $\xi \in \gamma$ и запишем $\xi\mathfrak{r} = \mathfrak{b}\mathfrak{a}^{-1}$, где $\mathfrak{a}$, $\mathfrak{b}$— взаимно простые идеалы в $\mathfrak{r}$. Для каждой конечной точки $v \in P$ имеем $\xi \in \mathfrak{r}_v^\times$, так что $\mathfrak{p}_v$ не делит $\mathfrak{a}$ или $\mathfrak{b}$. Применяя следствие 1 теор. 1 п.16.4.2 к проекции $\mathfrak{r} \to \prod \mathfrak{r}_v$, где произведение берется по тем конечным точкам v поля k, которые либо лежат в P, либо соответствуют простым идеалам, делящим $\mathfrak{a}$, мы видим, что существует такой элемент $\alpha \in \mathfrak{r}$, что $\alpha \in g_v$ для каждой конечной точки $v \in P$, $\alpha \in \mathfrak{a}$ и $\alpha \neq 0$. Тогда элемент α^2 удовлетворяет тем же самым условиям и содержится в g_v для каждой бесконечной точки v, так что он содержится в γ, а следовательно, и в $\gamma \cap \mathfrak{r}$. Следовательно, и $\xi\alpha^2 \in \gamma \cap \mathfrak{r}$, чем и доказано наше предложение.

Пусть, в частности, $g_v = 1 + \mathfrak{p}_v^{m(v)}$, где $m(v) \geqslant 1$ для каждой конечной точки $v \in P$. Положим $\mathfrak{m} = \prod \mathfrak{p}_v^{m(v)}$ и обозначим через $v_1, \ldots, v_\rho$ все вещественные точки поля k, для которых $g_v = \mathbf{R}_+^\times$. Тогда сразу видно, что множество $\gamma \cap \mathfrak{r}$ из предложения 17 состоит из тех элементов кольца $\mathfrak{r}$, которые $\equiv 1\ (\mathfrak{m})$ и образы которых в k_{v_i} строго положительны для $1 \leqslant i \leqslant \rho$.

16.9. Следы и нормы

16.9.1. Следы и нормы в локальных полях

В п.16.8.1—3 мы будем рассматривать исключительно локальные поля (предполагаемые коммутативными). Обозначим через K рас-

сматриваемое локальное поле и через K' — алгебраическое расширение поля K конечной степени n над K. Если K является $\mathbf{R}$-полем, то $K' \neq K$ только в случае $K = \mathbf{R}$, $K' = \mathbf{C}$, $n = 2$; в этом случае по следствию 3 предл. 4 п.16.3.3 $\mathrm{Tr}_{\mathbf{C}/\mathbf{R}}(x) = x + \bar{x}$ и $\mathrm{N}_{\mathbf{C}/\mathbf{R}}(x) = x\bar{x}$, причем $\mathrm{Tr}_{\mathbf{C}/\mathbf{R}}$ отображает $\mathbf{C}$ на $\mathbf{R}$, а $\mathrm{N}_{\mathbf{C}/\mathbf{R}}$ отображает $\mathbf{C}^\times$ на группу $\mathbf{R}_+^\times$, которая является подгруппой индекса 2 в $\mathbf{R}^\times$.

Начиная с этого места вплоть до конца п.16.8.3 мы предполагаем, что K есть p-поле, и используем наши обычные обозначения для таких полей, так что q — это модуль поля K, R — его максимальное компактное подкольцо, P — максимальный идеал в R и π — простой элемент в K. Для поля K', введенного выше, мы применяем аналогичные обозначения, а именно q', R', P', π'. Обозначим, далее, через f модулярную степень поля K' над K и через e индекс ветвления поля K' над K (см. определение 4 в п.16.1.4). Тогда $q' = q^f$ и $n = ef$ по следствию 6 теор. 6 п.16.1.4. Так как $e = \mathrm{ord}_{K'}(\pi)$, то R'-модуль в K', порожденный множеством $P^\nu = \pi^\nu R$, при любом $\nu \in \mathbf{Z}$ совпадает с $P'^{e\nu}$; мы будем обозначать его через $\iota(P^\nu)$.

Согласно следствию 1 предл. 4 п.16.3.3 и замечаниям, сделанным после этого предложения, $\mathrm{Tr}_{K'/K} \neq 0$ в том и только в том случае, когда расширение K' над K сепарабельно; в этом случае, будучи K-линейным, след отображает K' на K. По определению нормы и по следствию 3 теор. 3 п.16.1.2 при всех $x' \in \dot{K}'$ имеем

$$\mathrm{mod}_{K'}(x') = \mathrm{mod}_K(\mathrm{N}_{K'/K}(x')). \tag{1}$$

Ввиду теоремы 6 п.16.1.4 отсюда следует, что $x' \in R'$ в том и только в том случае, когда $\mathrm{N}_{K'/K}(x') \in R$, и $x' \in R'^\times$ в том и только в том случае, когда $\mathrm{N}_{K'/K}(x') \in R^\times$. Так как $\mathrm{mod}_K(\pi) = q^{-1}$ и $\mathrm{mod}_{K'}(\pi') = q^{-1}$, то при $x' \neq 0$ равенство (1) можно записать также следующим образом:

$$\mathrm{ord}_K(\mathrm{N}_{K'/K}(x')) = f \cdot \mathrm{ord}_{K'}(x'). \tag{2}$$

Начиная с этого места, мы будем писать Tr, N вместо $\mathrm{Tr}_{K'/K}$, $\mathrm{N}_{K'/K}$, кроме тех случаев, когда одновременно рассматриваются более чем два поля K, K'. Для каждого $\nu \in \mathbf{Z}$ будем писать $\mathfrak{N}(P'^\nu) = P^\nu$; согласно (2), это есть R-модуль в K, порожденный образом P'^ν при отображении N.

Предложение 1. *Пусть поле K' сепарабельно над K. Тогда если $x' \in R'$, то $\mathrm{Tr}(x') \in R$, а если $x' \in P'$, то $\mathrm{Tr}(x') \in P$ и $\mathrm{N}(1 + x') = 1 + \mathrm{Tr}(x') + y$, где $y \in R \cap x'^2 R'$.*

Пусть K — алгебраическое замыкание поля K'. Обозначим через $\lambda_1, \ldots, \lambda_n$ различные K-линейные изоморфизмы $K' \to \bar{K}$.

Тогда по следствию 3 предл. 4 п.16.3.3 имеем

$$\mathrm{Tr}\,(x') = \sum_i \lambda_i\,(x'), \qquad \mathrm{N}\,(1 + x') = \prod_i (1 + \lambda_i\,(x')). \tag{3}$$

Обозначим через K'' композит полей $\lambda_i\,(K')$, который является наименьшим расширением Галуа поля K в $\bar{K}$, содержащим поле K'. Определим R'', P'' для K'' так же, как R, P определены для K. По следствию 5 теор. 6 п.16.1.4 имеем $\lambda_i\,(R') \subset R''$ и $\lambda_i\,(P') \subset P''$ при всех i, так что $\mathrm{Tr}\,(x')$ лежит в R'' при $x' \in R'$ и в P'' при $x' \in P'$. Поскольку то же самое следствие показывает, что $R = K \cap R''$ и $P = K \cap P''$, справедливость утверждений относительно Tr доказана. Предположим теперь, что $x' \in R'$, $x' \neq 0$, и положим

$$y = \mathrm{N}\,(1 + x') - 1 - \mathrm{Tr}\,(x').$$

Ввиду (3) это есть сумма одночленов степени $\geqslant 2$ от $\lambda_i\,(x')$. Так как один из изоморфизмов λ_i тождествен и изоморфизмы λ_i по следствию 2 предл. 3 п.16.3.2 отличаются друг от друга лишь на автоморфизмы поля K'' над K, то все $\lambda_i\,(x')$ имеют тот же порядок в K'', что и x', так что $yx'^{-2} \in R''$, если $x' \in R'$. Поскольку $R' = K' \cap R''$, этим доказано наше последнее утверждение. В силу того факта, что Tr = 0, если поле K' не сепарабельно над K, и в силу относящихся к этому случаю замечаний в п.16.3.3 наше предложение верно и в несепарабельном случае.

Следствие. *Если* $x' \in P'^{-e+1}$, *то* $\mathrm{Tr}\,(x') \in R$.

По определению $e = \mathrm{ord}_{K'}\,(\pi)$. Поэтому наше условие означает, что $\pi x' \in P'$, откуда $\mathrm{Tr}\,(\pi x') \in P$ по предложению 1, следовательно $\mathrm{Tr}\,(x') \in R$ ввиду K-линейности Tr.

Определение 1. *Пусть поле K' сепарабельно над K и d — наибольшее из целых чисел v, таких, что $\mathrm{Tr}\,(x') \in R$ при всех $x' \in P'^{-v}$. Тогда P'^{d} называется дифферентой поля K' над K, а d — показателем дифференты.*

Дифференту мы будем обозначать через $D\,(K'/K)$ или просто через D. Если поле K' несепарабельно над K, то Tr = 0, так что след отображает P'^{-v} в R при всех v; в этом случае положим $d = +\infty$, $D\,(K'/K) = 0$.

Согласно следствию предл. 1, $d \geqslant e - 1$. В частности, если d=0, то e = 1, так что поле K' неразветвлено над K. Обратное утверждение тоже верно; оно будет вытекать из следующих результатов.

Предложение 2. *Пусть поле K' неразветвлено над K. Обозначим через ρ, ρ' канонические гомоморфизмы $R \to k = R/P$ и $R' \to k' = R'/P'$ соответственно. Тогда при $x' \in R'$ имеем*

$$\rho\,(\mathrm{Tr}\,(x')) = \mathrm{Tr}_{k'/k}\,(\rho'\,(x')), \quad \rho\,(\mathrm{N}\,(x')) = \mathrm{N}_{k'/k}\,(\rho'\,(x')).$$

Как и в теореме 7 п.16.1.4 и ее следствиях, обозначим через $M'^{\times}$ группу корней из 1 в K', порядок которых взаимно прост с p. По следствию 2 из этой теоремы K' является циклическим расширением степени f над K и его группа Галуа порождается автоморфизмом Фробениуса, который индуцирует на $M'^{\times}$ перестановку $\mu \to \mu^q$. Ввиду следствия 2 теор. 2 п.16.1.1 это означает в точности то, что автоморфизмы поля K' над K определяют на $k' = R'/P'$ автоморфизмы, составляющие всю группу Галуа поля k' над k. Наше утверждение следует теперь из этого факта, из формул $\mathrm{Tr}\,(x') = \sum \lambda_i (x')$, $\mathrm{N}\,(x') = \prod \lambda_i (x')$ и из аналогичных формул для k и k', т. е. из следствия 3 предл. 4 п.16.3.3, примененного сначала к K и K', а затем к k и k'.

Предложение 3. *Пусть поле K' неразветвлено над K.Тогда* Tr *сюръективно отображает P'^{ν} на P^{ν} для каждого $\nu \in \mathbf{Z}$, а* N *сюръективно отображает $R'^{\times}$ на $R^{\times}$.*

Пусть k, k' такие, как в предложении 2. Так как k' сепарабельно над k, то $\mathrm{Tr}_{k'/k} \neq 0$. Первая формула из предложения 2 показывает, что образ Tr(R') кольца R' при отображении Tr не содержится в P. Поскольку этот образ содержится в R согласно предложению 1 и поскольку он является R-модулем, ибо R' является R-модулем, а Tr K-линеен, то он совпадает с R. Так как поле K' неразветвлено, то простой элемент π в K является также простым элементом в K'. Поэтому $P'^{\nu} = \pi^{\nu} P'$ при $\nu \in \mathbf{Z}$. Ввиду K-линейности отображения Tr получаем

$$\mathrm{Tr}\,(P'^{\nu}) = \pi^{\nu}\mathrm{Tr}\,(R') = \pi^{\nu} R = P^{\nu}.$$

Что касается нормы, то положим $G_0 = R^{\times}, G'_0 = R'^{\times}$, $G_{\nu} = 1 + P^{\nu}$ и $G'_{\nu} = 1 + P'^{\nu}$ при всех $\nu \geqslant 1$. Последнее утверждение предложения 1 показывает, что для каждого $\nu \geqslant 1$ норма N отображает G'_{ν} в G_{ν}, а также с учетом только что доказанного для следа, что она определяет на $G'_{\nu}/G'_{\nu+1}$ сюръективный морфизм этой группы на $G_{\nu}/G_{\nu+1}$. С другой стороны, обозначим через φ автоморфизм Фробениуса поля K' над K и через μ образующую группы $M'^{\times}$ корней из 1 в $K'^{\times}$, порядок которых взаимно прост с p. Тогда элемент μ имеет порядок $q^f - 1$, т. е. $q^i \neq 1$, а его норма равна

$$\mathrm{N}\,(\mu) = \prod_{i=0}^{f-1} \mu^{\varphi^i} = \prod_{i=0}^{f-1} \mu^{q^i} = \mu^{1+q+\ldots+q^{f-1}} = \mu^{(q^f-1)/(q-1)}.$$

Ясно, что это — корень степени $q - 1$ из 1, а следовательно, образующая группы $M^{\times}$ корней из 1 в K, порядок которых взаимно прост с p. Так как $M^{\times}$ образует полное множество представителей смежных классов в $G_0 = R^{\times}$ по модулю $G_1 = 1 + P$, отсюда видно, что N

определяет на G'_0/G'_1 сюръективный морфизм этой группы на G_0/G_1. Теперь для каждого элемента $x_0 \in R^{\times}$ мы можем индуктивно определить такие две последовательности (x_ν), (x'_ν), что

$$x_\nu \in G_\nu, \quad x'_\nu \in G'_\nu, \quad \mathrm{N}(x'_\nu) \in x_\nu G_{\nu+1}$$

и

$$x_{\nu+1} = \mathrm{N}(x'_\nu)^{-1} x_\nu$$

при всех $\nu \geq 0$. Поэтому для $y'_\nu = x'_0 x'_1 \ldots x'_{\nu-1}$ имеем $\mathrm{N}(y'_\nu) = x_0 x_\nu^{-1}$. Ясно, что последовательность (y'_ν) стремится к некоторому пределу $y' \in R'^{\times}$ и что $\mathrm{N}(y') = x_0$.

Следствие. *Пусть K' — произвольное расширение конечной степени поля K. Тогда дифферента поля K' над K равна R' (т. е. $d = 0$) в том и только в том случае, когда поле K' неразветвлено над K.*

Предложение 3 показывает, что $d = 0$, если поле K' неразветвлено над K. Обратно, если $d = 0$, то K' сепарабельно над K и, как мы уже отмечали выше, из следствия 1 предл. 1 вытекает, что $e = 1$.

Предложение 4. *Пусть поле K' сепарабельно над K и P'^d — его дифферента над K. Тогда для каждого $\nu \in \mathbf{Z}$ образ P'^ν в K при отображении* Tr *равен P^μ, где целое число μ определяется условием* $e\mu \leqslant \nu + d < e(\mu + 1)$.

Так как след Tr K-линеен и отличен от нуля, он отображает каждую K-решетку в K' и, в частности, каждое множество P'^ν на K-решетку в K, т. е. на множество вида P^μ. Пусть μ удовлетворяет условию нашего предложения. Тогда поскольку $\mathrm{ord}_{K'}(\pi) = e$, то P'^ν содержится в $\pi^\mu P'^{-d}$ и содержит $\pi^{\mu+1} P'^{-d-1}$. Ввиду определения числа d и K-линейности следа Tr, отсюда следует, что $\mathrm{Tr}(P'^\nu)$ содержится в $\pi^\mu R = P^\mu$ и не содержится в $\pi^{\mu+1} R = P^{\mu+1}$.

Доказательство закончено.

Следствие 1. *Для каждого $x' \in K'^{\times}$ имеем*

$$\mathrm{ord}_{K'}(\mathrm{Tr}(x')) = e \cdot \mathrm{ord}_K(\mathrm{Tr}(x')) \geqslant \mathrm{ord}_{K'}(x') + d - e + 1.$$

В самом деле, если положить $\nu = \mathrm{ord}_K(x')$ и определить μ как в предложении 4, то левая часть неравенства в нашем следствии будет не меньше $e\mu$, согласно упомянутому предложению, а $e\mu > \nu + d - e$ по определению μ.

Следствие 2. *Тогда и только тогда* $\mathrm{Tr}(R') = R$, *когда $d = e - 1$.*

В самом деле, по предложению 4 из равенств $\mu = \nu = 0$ вытекает неравенство $d < e$. Так как по следствию предл. 1 $d \geqslant e - 1$, то получаем $d = e - 1$.

Если $d = e - 1$, то говорят, что поле K' *хорошо разветвлено* над K.

Следствие 3. *Пусть* χ *— характер порядка* μ *на К. Тогда* $\chi \circ \mathrm{Tr}$ — *характер порядка* $d + e\mu$ *на К'*.

Наше предположение означает, что характер χ тривиален на $P^{-\mu}$, но не на $P^{-\mu-1}$. Положим $\nu = d + e\mu$. Предложение 4 показывает, что $\mathrm{Tr}\,(P'^{-\nu}) = P^{-\mu}$, а $\mathrm{Tr}\,(P'^{-\nu-1}) = P^{-\mu-1}$. Поэтому отображение $\chi \circ \mathrm{Tr}$ тривиально на $P'^{-\nu}$, но не на $P'^{-\nu-1}$, что и требовалось доказать.

В нашем очередном следствии мы рассмотрим алгебраическое расширение конечной степени K'' над K'; R'', P'' будут иметь тот же самый смысл для K'', что R, P для K. Для всякого $\nu \in \mathbf{Z}$ будем обозначать через $\iota'(P'^{\nu})$ R''-модуль в K'', порожденный множеством P'^{ν}; если $e' = \mathrm{ord}_{K'}(\pi')$ — степень ветвления поля K'' над K', то $\iota'(P'^{\nu}) = P''^{e'\nu}$. В этих обозначениях имеет место

Следствие 4. *Пусть* K, K', K'' *таковы, как выше, и пусть* $D = P'^{d}$, $D' = P''^{d'}$, $D'' = P''^{d''}$ — *дифференты соответственно поля* K' *над* K, *поля* K'' *над* K' *и поля* K'' *над* K. *Тогда* $D'' = \iota'(D) \cdot D'$ *и* $d'' = e'd + d'$, *где* e' — *индекс ветвления поля* K'' *над* K'.

Это утверждение тривиально, если поле K'' несепарабельно над K, ибо тогда $D'' = 0$ и либо D, либо D' равна нулю. Поэтому можно считать, что поле K'' сепарабельно над K. Нам нужно доказать, что $d'' = \delta$, где $\delta = e'd + d'$. В самом деле, по предложению 4 $\mathrm{Tr}_{K''/K'}$ отображает $P''^{-\delta}$ на P'^{-d} и $P''^{-\delta-1}$ на P'^{-d-1}, а $\mathrm{Tr}_{K'/K}$ отображает P'^{-d} на R и P'^{-d-1} на P^{1}. Наше утверждение следует теперь из «транзитивности следов», т. е. из следствия 4 предл. 4 п.16.3.3.

Следствие 5. *Пусть* K *и* K' *такие, как выше, и пусть* K_1 — *максимальное неразветвленное расширение поля* K, *содержащееся в* K'. *Тогда* K' *имеет ту же самую дифференту над* K, *что и над* K_1.

Определение K_1 см. в следствии 4 теор. 7 п.16.1.4. Наше утверждение вытекает из следствия 4 в сочетании со следствием предл. 3.

Предложение 5. *Пусть* K, K' *таковы, как в предложении* 4. *Тогда норма* N *определяет открытый морфизм группы* $K'^{\times}$ *на некоторую открытую подгруппу в* $K^{\times}$.

Как и выше, обозначим через P'^{d} дифференту поля K' над K и положим $G_\nu = 1 + P^{\nu}$, $G'_\nu = 1 + P'^{\nu}$ при $\nu \geqslant 1$. Возьмем любое $\mu > 2d$ и положим $\nu = e\mu - d$. По предложению 4 $\mathrm{Tr}\,(P'^{\nu}) = P^{\mu}$. Кроме того, имеем $e(\mu - 1) \geqslant 2d$, откуда $2\nu \geqslant e(\mu + 1)$, следовательно, $P'^{2\nu} \subset \pi^{\mu+1}R'$, а потому $K \cap P'^{2\nu} \subset P^{\mu+1}$. Теперь последняя часть предложения 1 показывает, что N, во-первых, отображает G'_ν в G_μ, а во-вторых, определяет сюръективный морфизм из G'_ν на

$G_\mu/G_{\mu+1}$. Взяв любой элемент $x_0 \in G_\mu$, мы можем теперь построить по индукции две такие последовательности (x_i), (x'_i), что

$$x_i \in G_{\mu+i},\ x'_i \in G'_{\nu+ei},\quad \mathrm{N}(x'_i) \in x_i G_{\mu+i+1}$$

и

$$x_{i+1} = \mathrm{N}(x'_i)^{-1} x_i$$

при всех $i \geq 0$.

Полагая $y'_i = x'_n x'_1 \ldots x'_i$, имеем $\mathrm{N}(y'_i) = x_0 x_{i+1}^{-1}$. Ясно, что последовательность (y'_i) сходится к некоторому пределу $y' \in G'_\nu$, причем $\mathrm{N}(y') = x_0$. Это показывает, что N отображает G'_ν на G_μ, чем и доказано наше предложение, поскольку группы G_μ, G'_ν $(\mu > 2d, \nu = e\mu - d)$ образуют фундаментальные системы окрестностей единицы в $K^\times$ и в $K'^\times$ соответственно.

Используя следствие 2 предл. 4 п.16.1.4 и результаты п.16.3.3, можно было бы легко показать, что заключение нашего предложения остается верным для любого расширения конечной степени K' поля K, не обязательно сепарабельного. Очевидно, что оно выполняется также для **R**-полей.

16.9.2. Вычисление дифференты

Обозначения и предположения в этом параграфе те же, что и в п.16.9.1. Если рассматривать K' как векторное пространство размерности n над K, то R' является K-решеткой, к которой можно применить теорему 1 п.16.2.2. В результате мы получаем, что в K' над K существует базис $\{\alpha_1, \ldots, \alpha_n\}$, для которого $R' = \sum R\alpha_i$. Предположим теперь, что K' сепарабельно над K, так что $\mathrm{Tr} \neq 0$. Тогда по лемме 3 п.16.3.3 можно отождествить векторное пространство K' над K с алгебраическим двойственным к нему, положив $[x', y'] = \mathrm{Tr}(x', y')$. Базис $\{\beta_1, \ldots, \beta_n\}$, двойственный к $\{\alpha_1, \ldots, \alpha_n\}$, определяется равенствами при $\mathrm{Tr}(\alpha_i \beta_j) = \delta_{ij}$ $1 \leqslant i, j \leqslant n$.

Предложение 6. *Пусть поле K' сепарабельно над K и $D = P'^d$ — его дифферента. Пусть $\{\alpha_1, \ldots, \alpha_n\}$ — такой базис в K' над K, что $R' = \sum R\alpha_i$, и пусть $\{\beta_1, \ldots, \beta_n\}$ — базис в K' над K, определяемый условием $\mathrm{Tr}(\alpha_i, \beta_j) = \delta_{ij}$ при $1 \leqslant i, j \leqslant n$. Тогда $D^{-1} = P'^{-d} = \sum R\beta_i$.*

В самом деле, возьмем любые элементы $x' \in R'$, $y' \in K'$ и запишем их в виде $x' = \sum x_i \alpha_i$ и $y' = \sum y_i \beta_i$, где $x_i \in R$ и $y_i \in K$ при $1 \leqslant i \leqslant n$. Тогда $\mathrm{Tr}(x', y') = \sum x_i y_i$, откуда видно, что в том и

только в том случае $\mathrm{Tr}\,(x'y') \in R$ при всех $x' \in R'$, т. е. Tr отображает $R'y'$ в R, когда $y_i \in R$ при всех i. По определению дифферента это означает, что $y' \in P'^{-d}$ тогда и только тогда, когда $y' \in \sum R\beta_i$, что и требовалось доказать.

Следствие 1. *В предположениях предложения* 6 *обозначим через* Δ *определитель матрицы*

$$M = (\mathrm{Tr}\,(\alpha_i\alpha_j))_{1 \leqslant i,\ j \leqslant n}.$$

Тогда $\mathrm{ord}_K(\Delta) = fd$ *и* $\Delta R = \mathfrak{N}(D)$.

Запишем $\alpha_i = \sum a_{ij}\beta_j$, где $a_{ij} \in K$ при $1 \leqslant i,\ j \leqslant n$. Умножив обе части на α_j и взяв след, получим, что $\mathrm{Tr}\,(\alpha_i\alpha_j) = a_{ij}$ и, следовательно, $M = (a_{ij})$. Поэтому автоморфизм векторного пространства K' над K, переводящий базис $\{\beta_1, \ldots, \beta_n\}$ в базис $\{\alpha_1, \ldots, \alpha_n\}$ и, следовательно, отображающий K-решетку D^{-1} на R', представляется в первом из этих базисов матрицей (a_{ij}), причем его модуль равен $\mathrm{mod}_K(\Delta)$ по следствию 3 теор. 3 п.16.1.2. Так как автоморфизм $x' \to \pi'^d x'$ также отображает $D^{-1} = P'^{-d}$ на R', то его модуль $\mathrm{mod}_{K'}(\pi'^d)$ должен совпадать с $\mathrm{mod}_K(\Delta)$. Это дает равенство $fd = \mathrm{ord}_K(\Delta)$, откуда $\mathfrak{N}(D) = \Delta R$.

Заметим, что наше следствие остается справедливым и в несепарабельном случае, потому что тогда Tr = 0 и $D = 0$. Из нашего результата, очевидно, вытекает, что $\mathrm{ord}_K(\Delta)$ не зависит от выбора $\alpha_1, \ldots, \alpha_n$. Этим фактом, который можно было бы легко проверить и непосредственно, оправдано следующее определение.

Определение 2. *Пусть* Δ *таково, как в следствии предложения* 6. *Тогда идеал* ΔR *в* R *называется дискриминантом поля* K' *над* K.

Предположим дополнительно, что K' — сепарабельное расширение степени n над K, и обозначим через $\bar{K}$ алгебраическое замыкание поля K'. Как и в п.16.9.1, пусть $\lambda_1, \ldots, \lambda_n$ суть n различных K-линейных изоморфизмов $K' \to \bar{K}$. Среди них есть тождественный изоморфизм, пусть это будет λ_1. Возьмем любой элемент $\xi \in K'$ и положим $\xi_i = \lambda_i(\xi)$ при $1 \leqslant i \leqslant n$, так что, в частности, $\xi_1 = \xi$. Если v — степень поля K' над $K(\xi)$, то имеется v различных $K(\xi)$-линейных изоморфизмов $K' \to \bar{K}$. Следовательно, среди изоморфизмов λ_i имеется ровно v таких, которые оставляют элемент ξ неподвижным. Это показывает, что $K(\xi) = K'$ в том и только в том случае, когда $\xi_i \neq \xi$ при всех $i \neq 1$.

Пусть теперь X — неизвестная над K. С помощью способа, описанного в п.16.3.3, мы можем продолжить K-линейное отображение $\mathrm{Tr}\colon K' \to K$ и полиномиальное отображение $\mathrm{N}\colon K' \to K$ до

отображения из $K'[X] = K' \otimes_K K[X]$ в $K[X]$, которые мы обозначим опять через Tr и N. Положим, далее,

$$F(X) = \mathrm{N}(X - \xi) = \prod_{i=1}^{n} (X - \xi_i) = X^n + \sum_{i=1}^{n} a_i X^{n-i}. \tag{4}$$

Это — унитарный многочлен из $K[X]$. Обозначая через F' его формальную производную, имеем

$$F'(\xi) = \prod_{i=2}^{n} (\xi - \xi_i).$$

Согласно доказанному выше, $K(\xi) = K'$ в том и только в том случае, когда $F'(\xi) \neq 0$. Хорошо известно и легко проверяется, что $F(X)^{-1}$ допускает в $\bar{K}(X)$ «разложение на простейшие дроби», задаваемое формулой

$$\frac{1}{F(X)} = \sum_{i=1}^{n} \frac{1}{F'(\xi_i)(X - \xi_i)}.$$

Рассматривая поле $\bar{K}(X)$ как очевидным образом вложенное в поле формальных степенных рядов от X^{-1} с коэффициентами в $\bar{K}$, получаем отсюда

$$X^{-n}\left(1 + \sum_{i=1}^{n} a_i X^{-i}\right)^{-1} = \sum_{i=1}^{n} F'(\xi_i)^{-1} \sum_{\nu=0}^{+\infty} \xi_i^{\nu} X^{-\nu-1},$$

что можно переписать еще так:

$$X^{-n} \sum_{\nu=0}^{+\infty} \left(\sum_{i=1}^{n} a_i X^{-i}\right)^{\nu} = \sum_{\nu=0}^{\nu+\infty} \mathrm{Tr}\left(F'(\xi)^{-1} \xi^{\nu}\right) X^{-\nu-1}.$$

Сравнивая коэффициенты в левой и правой частях, находим

$$P_\nu(a) = \mathrm{Tr}\left(F'(\xi)^{-1} \xi^{\nu}\right) \tag{5}$$

при $\nu \geqslant 0$, где $P_\nu(a)$ при всех ν является многочленом из $\mathbf{Z}[a_1, \ldots, a_n]$, $P_\nu = 0$ при $0 \leqslant \nu < n - 1$ и $P_{n-1} = 1$.

Предложение 7. *Пусть K' — сепарабельное расширение степени n над K, D — его дифферента, и для любого $\xi \in K'$ пусть F — многочлен, определенный формулой* (4). *Тогда все коэффициенты a_i многочлена F лежат в R, если $\xi \in R'$, и в P, если $\xi \in P'$. Кроме того, если $\xi \in R'$, то $F'(\xi) D^{-1}$ содержится в $R[\xi]$, и это — наибольший R'-модуль, содержащийся в $R[\xi]$.*

Утверждения относительно a_i доказываются точно так же, как утверждения о следе в предложении 1. В самом деле, если $\xi_i = \lambda_i(\xi)$ определены, как выше, то из предположения $\xi \in R'$ (соотв. $\xi \in P'$) следует, что $\xi_i \in \lambda_i(R')$ (соотв. $\xi_i \in \lambda_i(P')$) для всякого i, а потому ξ_i лежит в максимальном компактном подкольце R'' композита K'' полей $\lambda_i(K')$ (соотв. в максимальном идеале P'' кольца R''). Формула

(4) показывает тогда, что все a_i лежат в R'', а следовательно в $R = K \cap R''$ (соотв. в P'', а следовательно в $P = K \cap P''$). Что касается утверждения относительно $F'(\xi)$, то предположим сначала, что $F'(\xi) = 0$. Как мы видели, это имеет место в том и только в том случае, когда $K(\xi) \neq K'$. В этом случае поле $K(\xi)$, а следовательно и $R[\xi]$, не может содержать никакого R-модуля, отличного от $\{0\}$, чем и доказано наше утверждение.

Предположим теперь, что $F'(\xi) \neq 0$. Тогда $K' = K(\xi)$, так что $\{1, \xi, \ldots, \xi^{n-1}\}$ есть базис в K' над K. Поскольку многочлен F унитарен и содержится в $R[X]$, а $F(\xi) = 0$, то из хорошо известного элементарного рассуждения вытекает, что $R[\xi]$ совпадает с R-модулем $\sum_{i=0}^{n-1} R\xi^i$. Возьмем теперь любой элемент $x' \in K'$. Запишем $F'(\xi)\, x' = \sum_{i=0}^{n-1} x_i \xi^i$, где $x_i \in K$ при $0 \leqslant i \leqslant n-1$. Умножая обе части на $F'(\xi)^{-1}\, \xi^{\nu}$ и беря следы, получаем в силу формулы (5)

$$\mathrm{Tr}\,(x'\xi^{\nu}) = \sum_{i=0}^{n-1} x_i P_{\nu+i}(a) \tag{6}$$

при всех $\nu \geqslant 0$. В частности, при $0 \leqslant \nu \leqslant n-1$ имеем

$$x_{n-\nu-1} = \mathrm{Tr}\,(x'\xi^{\nu}) = \sum_{i=n-\nu}^{n-1} x_i P_{\nu+i}(a). \tag{7}$$

Предположим сначала, что $x' \in D^{-1}$. Используя формулу (7) и индукцию по ν для $0 \leqslant \nu \leqslant n-1$, находим, что все $x_i \in R$, т.е. $F'(\xi)\, x' \in R[\xi]$, так что $F'(\xi)\, D^{-1} \subset R[\xi]$. Предположим теперь, что $x_i \in R$ при $0 \leqslant i \leqslant n-1$, т. е. что $F'(\xi)\, x' \in R[\xi]$. Тогда формула (6) при $\nu = 0$ показывает, что $\mathrm{Tr}\,(x') \in R$. Заменяя x' на $x'y'$ с $y' \in R'$, мы видим, что если x' таков, что $F'(\xi)\, x'R' \subset R[\xi]$, то $x' \in D^{-1}$. Этим доказано наше последнее утверждение.

Следствие 1. В *обозначениях и предположениях предложения 7* $D = F'(\xi)\, R'$ *тогда и только тогда, когда* $R' = R[\xi]$.

Это сразу вытекает из второй части предложения 7.

Следствие 2. *В обозначениях и предположениях предложения 7 допустим дополнительно, что K' вполне разветвлено над K, и положим*

$$F(X) = \mathrm{N}(X - \pi') = X^n + \sum_{i=1}^{n} a_i X^{n-i},$$

где π' *— любой простой элемент в K'. Тогда* $\mathrm{ord}_K(a_i) \geqslant 1$ *при*

$1 \leq i \leq n$, $\mathrm{ord}_K(a_n) = 1$ и $D = F'(\pi')\,R'$.

Взяв в предложении 7 $\xi = \pi'$, мы получим первое утверждение. Второе очевидно ввиду формулы 2 п.16.9.1, поскольку $a_n = N(-\pi')$. Последнее утверждение вытекает из следствия 1, с учетом предложения 4 п.16.1.4.

Следствие 3. *В обозначениях и предположениях следствия* 2 *поле K' хорошо разветвлено тогда и только тогда, когда n взаимно просто с P.*

Поскольку K' вполне разветвлено, то в наших обычных обозначениях $f = 1$ и $n = e$. По следствию 2 $d = \mathrm{ord}_{K'}(F'(\pi'))$, и все члены в $F'(\pi')$, кроме первого члена $n\pi'^{n-1}$, имеют порядок $\geqslant e = \mathrm{ord}_{K'}(\pi)$ в K'. Поэтому тогда и только тогда $d = e - 1$, т. е. K' хорошо разветвлено, когда $\mathrm{ord}_{K'}(n) = 0$, т. е. когда n взаимно просто с p.

Многочлен F, удовлетворяющий условиям следствия 2, т. е. унитарный многочлен $X^n + \sum_{i=1}^{n} a_i X^{n-i}$ в $K[X]$, для которого $\mathrm{ord}_K(a_i) \geqslant 1$ при всех i и $\mathrm{ord}_K(a_n) = 1$, называется *многочленом Эйзенштейна* над K.

Предложение 8. *Пусть F — многочлен Эйзенштейна над K. Тогда F неприводим в $K[X]$, и если π' — корень многочлена F в произвольном расширении поля K, то поле $K(\pi')$ является хорошо разветвленным расширением поля K, π' — простым элементом в $K(\pi')$.*

Предположим, что $F = GH$, где $G,\ H \in K[X]$. Пусть a, b — наименьшие целые числа, для которых многочлены $G_1 = \pi^a G$ и $H_1 = \pi^b H$ лежат в $R[X]$. Положим $F_1 = \pi^{a+b} F$, так что $F_1 = G_1 H_1$. Положим, далее, $k = R/P$ и обозначим через F_0, G_0, H_0 многочлены из $k[X]$, получаемые заменой каждого коэффициента в многочленах F_1, G_1, H_1 соответственно образом этого коэффициента в R/P при каноническом гомоморфизме $R \to R/P$. Ввиду определения чисел a, b многочлены G_0 и H_0 отличны от нуля, так что $F_0 \neq 0$. Отсюда следует, что $a + b = 0$, $F_1 = F$ и $F_0 = X^n$, а значит, существует такое ν, что $G_0 = X^\nu$, $H_0 = X^{n-\nu}$. Поэтому степени многочленов G_1 и H_1 не меньше соответственно ν и $n - \nu$. Поскольку $F_1 = G_1 H_1$, они равны соответственно ν и $n - \nu$. Если $\nu > 0$, $n - \nu > 0$, то обозначим через g и h свободные члены в G_1 и H_1 соответственно. Так как $G_0 = X^\nu$ и $H_0 = X^{n-\nu}$, то $g,\ h \in P$. Поскольку свободный член в F равен теперь gh, то он лежит в P^2, что противоречит определению многочлена Эйзенштейна. Пусть теперь π' — корень многочлена F в некотором расширении поля K, которое можно считать алгебраически замкнутым. Так как F неприводим, то

различные K-линейные изоморфизмы поля $K' = K(\pi')$ в это расширение отображают π' на все различные корни многочлена F, так что $F(X) = N(X - \pi')$, откуда по определению многочлена Эйзенштейна $\mathrm{ord}_K(N(\pi')) = 1$. В силу формулы 2 п.16.9.1 отсюда следует, что $f = 1$ и что π' — простой элемент в K'.

16.9.3. Теория ветвления

В этом параграфе нам будет удобно записывать изоморфизмы и автоморфизмы полей экспоненциально, т. е. как $x \to x^{\lambda}$ и т. п.

Далее, удобно будет следующим образом продолжить ord_K, где поле K такое же, как выше, на все алгебраические расширения поля K. Пусть x' — любой элемент такого расширения; K' — любое расширение конечной степени поля K, содержащее x'; π, как и прежде,— простой элемент в K. Положим

$$\mathrm{ord}_K(x') = \mathrm{ord}_{K'}(x')/\mathrm{ord}_{K'}(\pi).$$

Если заменить здесь K' любым аналогичным полем K'', содержащим K', то $\mathrm{ord}_K(x')$ и $\mathrm{ord}_{K'}(\pi)$ умножатся оба на индекс ветвления поля K'' над K', так что наше определение $\mathrm{ord}_K(x')$ не зависит от выбора K'', разумеется, можно взять в определении $K' = K(x')$. Пользуясь этой возможностью выбора подходящего K', мы видим, что ord_K совпадает на $K^{\times}$ с ранее определенным отображением $\mathrm{ord}_K\colon K^{\times} \to \mathbf{Z}$ и определяет отображение каждого алгебраического расширения поля K в $\mathbf{Q} \cup \{+\infty\}$, причем $\mathrm{ord}_K(x') = +\infty$ в том и только в том случае, когда $x' = 0$.

Пусть, как и прежде, K' — расширение степени n поля K', предположим, что это расширение сепарабельно. Сохраним в силе обозначения п.16.9.1—2. В частности, $D = P'^{d}$ — дифферента поля K' над K. Обозначим через K_1 максимальное неразветвленное расширение поля K, содержащееся в K' (согласно следствию 4 теор. 7 п.16.1.4 K_1 определено однозначно). Тогда поле K' имеет степень e над K_1 и по следствию 5 предл. 4 п.16.9.1 его дифферента над K_1 равна D. Положим

$$F(X) = N_{K'/K_1}(X - \pi').$$

По следствию 2 предл. 7 п.16.9.2 это — многочлен Эйзенштейна над K_1 и $D = F'(\pi')R'$.

Пусть L — любое содержащее K' расширение Галуа конечной степени над K. Например, в качестве L можно взять композит образов поля K' при всех различных K-линейных изоморфизмах поля K' в некоторое его алгебраическое замыкание $\bar{K}$. Для каждого K-линейного изоморфизма $x' \to x'^{\lambda}$ из K' в L положим

$$\nu(\lambda) = \min_{x' \in R'} \operatorname{ord}_{K'}(x' - x'^{\lambda}) = \min_{x' \in R'} \operatorname{ord}_{L}(x' - x'^{\lambda}) / \operatorname{ord}_{L}(\pi').$$

Так как $\operatorname{ord}_L (x' - x'^{\lambda})$ — целое неотрицательное число или $+\infty$, то функция ν определена корректно; она принимает значение $+\infty$ в том и только в том случае, когда λ есть тождественное отображение, т. е. естественное вложение поля K' в L, которое мы будем обозначать через ε. Согласно теореме 7 п.16.1.4 и ее следствиям 3 и 4 поле K_1 порождено над K корнями из 1 в K', порядок которых взаимно прост с p, и эти корни вместе с нулем образуют полное множество представителей для R'/P' в R'. Поэтому если автоморфизм K индуцирует на K_1 не тождественное отображение, то существует такой корень ξ, для которого $\xi^{\lambda} \neq \xi$. Тогда $\xi - \xi^{\lambda}$ лежит в K', но не в P', так что, беря $x' = \xi$, получаем $\nu(\lambda) = 0$.

Предположим теперь, что λ индуцирует на K_1 тождественное отображение. Так как K' хорошо разветвлено над K_1, то предложение 4 п.16.1.4 показывает, что $R' = R_1[\pi']$, где R_1 — максимальное компактное подкольцо в K_1, так что каждый элемент $x' \in R'$ может быть записан в виде $G(\pi')$, где $G \in R_1[X]$. Это дает

$$x' - x'^{\lambda} = G(\pi') - G(\pi'^{\lambda}) = (\pi' - \pi'^{\lambda}) H(\pi', \pi'^{\lambda}),$$

где $H \in R_1[X, Y]$. Как уже отмечалось в доказательстве предложения 1, π'^{λ} имеет тот же самый порядок в L, что и π'. Отсюда следует, что $\operatorname{ord}_{K'}(\pi'^{\lambda}) = \operatorname{ord}_{K'}(\pi') = 1$, так что

$$\operatorname{ord}_{K'}(x' - x'^{\lambda}) \geqslant \operatorname{ord}_{K'}(\pi' - \pi'^{\lambda}) \geqslant 1,$$

поэтому для любого изоморфизма λ, тождественного на K_1, имеем

$$\nu(\lambda) = \operatorname{ord}_{K'}(\pi' - \pi'^{\lambda}) \geqslant 1, \tag{8}$$

откуда следует, что $\operatorname{ord}_{K'}(\pi' - \pi'^{\lambda})$ не зависит от выбора n'. Далее, для F, определенного, как выше, имеем по формуле (4) п.16.9.2

$$F(X) = \prod_{\lambda} (X - \pi'^{\lambda}),$$

где произведение берется по всем различным K_1-линейным изоморфизмам λ: $K' \to L$, откуда

$$F'(\pi') = \prod_{\lambda \neq \varepsilon} (\pi' - \pi'^{\lambda}),$$

где произведение берется по тем же самым изоморфизмам, кроме тождественного. Это дает

$$d = \operatorname{ord}_{K'}(F'(\pi')) = \sum_{\lambda \neq \varepsilon} \nu(\lambda),$$

где сумма берется по тем же самым изоморфизмам, а также

$$d - e + 1 = \sum_{\lambda \neq \varepsilon} (v(\lambda) - 1),$$

ибо число таких изоморфизмов равно e— 1. Поскольку $v(\lambda) = 0$, если изоморфизм λ нетождествен на K_1, полученные формулы можно переписать так:

$$d = \sum_{\lambda \neq \varepsilon} v(\lambda), \quad d - e + 1 = \sum_{\lambda \neq \varepsilon} (v(\lambda) - 1)^{+}. \tag{9}$$

Здесь суммы берутся теперь по всем различным K-линейным изоморфизмам $K' \to L$, отличным от тождественного; кроме того, в последней сумме число членов, больших нуля, не превосходит $e - 1$.

Если само K' является расширением Галуа поля K, то мы можем взять $L = K'$. Тогда изоморфизмы λ — это автоморфизмы поля K' над K. Они образуют группу Галуа $\mathfrak{g}$ поля K' над K. Из определения $v(\lambda)$ видно, что теперь это — целое число или $+\infty$. Если $\lambda \neq \varepsilon$, то $v(\lambda)$— наибольшее из целых чисел v, таких, что λ определяет тождественное отображение на кольце R/P^v. Для всякого $v \geqslant 0$ автоморфизмы λ поля K' над K, для которых $v(\lambda) \geqslant v$, образуют подгруппу $\mathfrak{g}_v$, в $\mathfrak{g}$; группа $\mathfrak{g}_0$ совпадает с $\mathfrak{g}$, а группы $\mathfrak{g}_v$ при $v \geqslant 1$ известны как *высшие группы ветвления* поля K' над K. Группа $\mathfrak{g}_1$, которую принято по традиции называть *группой инерции* поля K', состоит, как мы видели выше, из автоморфизмов поля K', индуцирующих тождественное отображение на K_1 иными словами, это есть подгруппа в $\mathfrak{g}_0 = \mathfrak{g}$, связанная с K_1 в смысле теории Галуа. Порядок группы $\mathfrak{g}_1$ равен e, и группу $\mathfrak{g}_0/\mathfrak{g}_1$ можно отождествить с группой Галуа поля K_1 над K, которая, как мы знаем, является циклической группой порядка f и порождается автоморфизмом Фробениуса поля K_1 над K.

По-прежнему считая K' расширением Галуа поля K, обозначим через g_v порядок группы $\mathfrak{g}_v$ для каждого $v \geqslant 0$. Тогда $g_v - 1$ есть число отличных от ε элементов λ из $\mathfrak{g}$, для которых $v(\lambda) \geqslant v$. Поэтому мы можем переписать (9) следующим образом:

$$d = \sum_{v=1}^{+\infty} (g_v - 1), \quad d - e + 1 = \sum_{v=2}^{+\infty} (g_v - 1). \tag{10}$$

Предложение 9. *Пусть K' — расширение Галуа поля K с группой Галуа $\mathfrak{g} = \mathfrak{g}_0$, и пусть $\mathfrak{g}_v$, $v \geqslant 1$,— высшие группы ветвления. Положим $G'_0 = R'^{\times}$ и $G'_v = 1 + P'^v$ при $v \geqslant 1$. Тогда для всякого $v \geqslant 1$ группа $\mathfrak{g}_v$ состоит из тех элементов $\lambda \in \mathfrak{g}_1$, для которых $\pi'^{\lambda}\pi'^{-1} \in G'_{v-1}$. Для таких λ образ $\gamma(\lambda)$ элемента $\pi'^{\lambda}\pi'^{-1}$ в группе $\Gamma_v = G'_{v-1}/G'_v$ не зависит от выбора простого элемента π' в K', и отображение $\lambda \to \gamma(\lambda)$ есть морфизм $\mathfrak{g}_v \to \Gamma_v$ с ядром $\mathfrak{g}_{v+1}$.*

Первое утверждение следует из соотношения (8) и определений. Заменим π' каким-нибудь другим простым элементом в K', который можно записать в виде $\pi' u$, где $u \in R'^{\times}$. Для $\lambda \in \mathfrak{g}_\nu$ это вызовет лишь появление в $\pi'^{\lambda}\pi'^{-1}$ добавочного множителя $u^{\lambda}u^{-1}$, который по определению $\mathfrak{g}_\nu$ лежит в $1 + P'^{\nu}$, т. е. в G'_ν. Это показывает, что $\gamma(\lambda)$ не зависит от выбора π'. Пусть $\lambda, \mu \in \mathfrak{g}_\nu$. Положим $u = \pi'^{\lambda}\pi'^{-1}$, $v = \pi'^{\mu}\pi'^{-1}$. Тогда $\pi'^{\lambda\mu}\pi'^{-1} = (u^{\mu}u^{-1})uv$. Так как $u \in R'^{\times}$, то $u^{\mu}u^{-1} \in G'_\nu$. Это показывает, что отображение $\lambda \to \gamma(\lambda)$ есть морфизм и, очевидно, что его ядро совпадает с $\mathfrak{g}_{\nu+1}$.

Следствие 1. *Для каждого* $\nu \geqslant 0$ *группа* $\mathfrak{g}_\nu/\mathfrak{g}_{\nu+1}$ *коммутативна. При* $\nu = 0$ *эта группа является циклической группой порядка* f; *при* $\nu = 1$ *— циклической группой порядка* e_0, *делящего* $q' - 1$, *где* q' *— модуль поля* K'', *при* $\nu \geqslant 2$ *она изоморфна некоторой подгруппе аддитивной группы кольца* R'/P' *и ее порядок делит* q'.

Для $\nu = 0$ это было доказано выше. Положим теперь $k' = R'/P'$. Это — поле из q' элементов. Канонический морфизм из R' на k' индуцирует на G'_0 морфизм из G'_0 на $k'^{\times}$ с ядром G'_1, так что Γ_1 является циклической группой порядка $q' - 1$. Аналогично при $\nu \geq 2$ отображение $x' \to 1 + \pi'^{\nu-1}x'$ из R' на $G'_{\nu-1}$ определяет изоморфизм из R'/P' на Γ_ν. Наши утверждения для $\nu \geq 1$ вытекают из этих фактов и предложения 9.

Следствие 2. *В предположениях и обозначениях следствия* 1 $e = e_0 p^N$, *где* $N \geqslant 0$ *и* e_0 *взаимно просто с* p.

Это очевидно ввиду следствия 1, поскольку $\mathfrak{g}_1$ имеет порядок e.

Следствие 3. *Если* $\nu(\lambda)$ *имеет одно и то же значение* ν *при всех* $\lambda \neq 0$ *в* $\mathfrak{g}$, *то* $\mathfrak{g}$ *есть коммутативная группа, порядок которой делит* $q - 1$, *если* $\nu = 1$, *и делит* q, *если* $\nu \geq 2$.

В самом деле, мы имеем $\mathfrak{g}_\nu = \mathfrak{g}$, $\mathfrak{g}_{\nu+1} = \{\varepsilon\}$. Кроме того, если $\nu \geq 1$, то $e = n$, а значит, $f = 1$ и $q = q'$.

Наконец, числа $\nu(\lambda)$ обладают важными «свойствами транзитивности». Пусть, как и выше, K' — сепарабельное расширение конечной степени n поля K, но не обязательно расширение Галуа, K'' — сепарабельное расширение конечной степени поля K'. Возьмем в качестве L расширение Галуа конечной степени над K, содержащее K''. Пусть K_2 — максимальное неразветвленное расширение поля K, содержащееся в K''. Обозначим через K'_2 композит полей K' и K_2, через e' индекс ветвления поля K'' над K' и через f' — его модулярную степень над K'. Так как K' имеет тот же самый модуль q', что и K_1, и K'' и K'_2 имеют тот же самый модуль, что и K_2, то K_2 является неразветвленным расширением степени f' над K_1 и K_2 является

максимальным неразветвленным расширением поля K', содержащимся в K'', причем его степень над K' равна f'. Поскольку степень поля K' над K_1 равна e, отсюда следует, что степень поля K'_2 над K_1 равна ef'. Поэтому степень поля K'_2 над K_2 равна e. Всякий K_2-линейный изоморфизм $\sigma\colon K'_2 \to L$ индуцирует K_1-линейный изоморфизм $\lambda\colon K' \to L$. Поскольку K_2 является композитом полей K', K_2, то два таких изоморфизма σ, σ' не могут совпадать на K' при $\sigma \neq \sigma'$. Так как имеется ровно e таких изоморфизмов и столько же K_1 линейных изоморфизмов из K' в L, то $\sigma \to \lambda$ есть биекция первого множества на второе. В частности, каждый изоморфизм $\lambda\colon K' \to L$, тождественный на K_1, можно однозначно продолжить до изоморфизма $\sigma\colon K'_2 \to L$, тождественного на K_2.

Пусть теперь π'' — какой-нибудь простой элемент в K''. Положим

$$G(X) = \mathrm{N}_{K''/K'_2}(X - \pi'') = X^{e'} + \sum_{i=1}^{e'} \alpha_i X^{e'-i}.$$

По следствию 2 предл. 7 п.16.9.2 это — многочлен Эйзенштейна над K'_2. В частности, $\alpha_{e'}$ — простой элемент в K'_2, равно как и π', ибо K'_2 неразветвлено над K'. Пусть λ — любой нетождественный автоморфизм из K' в L, тождественный на K_1. Как мы видели выше, его можно единственным образом продолжить до изоморфизма $\sigma\colon K'_2 \to L$, тождественного на K_2. Обозначим через G^σ многочлен, полученный применением σ к каждому коэффициенту многочлена G. Тогда

$$G(X) - G^\sigma(X) = \alpha_{e'} - \alpha_{e'}^\sigma + \sum_{i=1}^{e'-1} (\alpha_i - \alpha_i^\sigma) X^{e'-i}.$$

Так как $\alpha_{e'}$ и π' — простые элементы в K'_2 и так как K'_2 неразветвлено над K, то с учетом уже доказанного имеем

$$\mathrm{ord}_{K'_2}(\alpha_{e'} - \alpha_{e'}^\sigma) = \mathrm{ord}_{K'_2}(\pi' - \pi'^\sigma) = \mathrm{ord}_K(\pi' - \pi'^\lambda) = \nu(\lambda),$$

$$\mathrm{ord}_{K'_2}(\alpha_i - \alpha_i^\sigma) \geqslant \mathrm{ord}_{K'_2}(\pi' - \pi'^\sigma) = \nu(\lambda) \quad (1 \leqslant i \leqslant e'),$$

откуда

$$\mathrm{ord}_K\ (G(\pi'') - G^\sigma(\pi'')) = \nu(\lambda).$$

Но $G(\pi'') = 0$. С другой стороны, G^σ — это унитарный многочлен, корни которого суть образы π''^τ элемента π'' при различных автоморфизмах $\tau\colon K'' \to L$, совпадающих на K'_2 с σ. Другими словами,

$$G^\sigma(\pi'') = \prod_\tau (\pi'' - \pi''^\tau),$$

где произведение берется по различным автоморфизмам $\tau\colon K'' \to L$,

индуцирующим λ на K' и тождественным на K_2. Пусть теперь функция $\nu'(\tau)$ определена для K, K'', τ так же, как $\nu(\lambda)$ была определена для K, K', λ. Другими словами, положим $\nu'(\tau) = 0$, если автоморфизм τ нетождествен на K_2, а в противном случае положим

$$\nu'(\tau) = \operatorname{ord}_{K''}(\pi'' - \pi''\tau).$$

Поскольку $\operatorname{ord}_{K''} = e' \cdot \operatorname{ord}_{K'}$, то из предыдущих формул вытекает равенство

$$e'\nu(\lambda) = \sum_{\tau} \nu'(\tau), \tag{11}$$

где сумму можно брать по всем изоморфизмам $\tau\colon K'' \to L$, совпадающим с λ на K', ибо автоморфизмы, нетождественные на K_1, не вносят никакого вклада в сумму в правой части. По аналогичной причине равенство (11) остается справедливым, в случае когда $\lambda\colon K' \to L$ — изоморфизм, нетождественный на K_1. Сопоставляя формулы (9) и (11), получаем еще одно доказательство следствия 4 предл. 4 п.16.9.1.

Пусть теперь L — расширение Галуа поля K не обязательно конечной степени. Обозначим через $\mathfrak{G}$ его группу Галуа, топологизированную обычным образом (в качестве фундаментальной системы окрестностей единицы берутся все подгруппы в $\mathfrak{G}$, соответствующие содержащимся в L расширениям конечной степени поля K). Тогда группа $\mathfrak{G}$ компактна и формулы (11) и (9) в совокупности со следствием 4 предл. 4 п.16.9.1 можно интерпретировать, сказав, что на семействе всех открытых и замкнутых подмножеств в $\mathfrak{G}$ существует конечно аддитивная функция $\mathbf{H}$ со следующим свойством. Пусть K' — любое расширение конечной степени поля K, содержащееся в L, e — его индекс ветвления над K и d — показатель его дифференты. Обозначим через $\mathfrak{H}$ открытую и замкнутую подгруппу в $\mathfrak{G}$, состоящую из автоморфизмов, тождественных на K'. Тогда $\mathbf{H}(\mathfrak{H}) = d/e$ и $\mathbf{H}(\mathfrak{H}\lambda) = -\nu(\lambda)/e$ для каждого класса смежности $\mathfrak{H}\lambda$ в $\mathfrak{G}$, отличного от $\mathfrak{H}$ (определение $\nu(\lambda)$ см. выше). Поэтому мы получим линейную форму $f \to \mathbf{H}(f)$, т. е. «распределение» на пространстве всех локально постоянных функций f на $\mathfrak{G}$, положив $\mathbf{H}(f) = \mathbf{H}(\mathfrak{H}\lambda)$ для характеристической функции f любого класса смежности $\mathfrak{H}\lambda$, где $\lambda \in \mathfrak{G}$ и подгруппа $\mathfrak{H}$ такая, как выше. Линейная форма $\mathbf{H}$ определяется этим соглашением однозначно, потому что всякая локально постоянная функция на $\mathfrak{G}$ может быть записана как конечная линейная комбинация указанных характеристических функций. Мы будем называть $\mathbf{H}$ *распределением Хербранда* на $\mathfrak{G}$. Из наших предыдущих результатов следует, что

знание **Н** дает нам знание свойств ветвления любых полей K'' над K', где K'', K' имеют конечную степень над K и $K \subset K' \subset K'' \subset L$.

16.9.4. Следы и нормы в А-полях

В этом параграфе мы рассматриваем некоторое **А**-поле k и некоторое сепарабельное алгебраическое расширение k' поля k конечной степени n над k. Объяснения обозначений см. в п.16.4.

Теорема 1. *Пусть k — некоторое* **А***-поле и k' — сепарабельное расширение конечной степени поля k. Тогда k'_w неразветвлено над замыканием k_v поля k в k'_w почти для всех конечных точек w поля k'.*

Пусть χ— базисный характер для k, т. е. нетривиальный характер на k_A, тривиальный на k. Положим $\chi' = \chi \circ \mathrm{Tr}_{k'/k}$. Это — характер на $k'_{\mathbf{A}}$, тривиальный на k'. Так как след $\mathrm{Tr}_{k'/k}$ не равен нулю и так как он k-линеен на k', то существует элемент $\xi \in k'$, для которого $\mathrm{Tr}_{k'/k}(\xi) = 1$. Поскольку продолжение следа $\mathrm{Tr}_{k'/k}$ на $k'_{\mathbf{A}}$ является k_A-линейным, отсюда следует, что оно отображает $k'_{\mathbf{A}}$ на k_A сюръективно, так что характер χ' нетривиален на $k'_{\mathbf{A}}$. Пусть w — конечная точка поля k' и v — та точка поля k, над которой лежит w. Обозначим через χ_v и χ'_w соответственно характеры, индуцированные характерами χ на k_v и χ' на k'_w. По следствию 3 теор. 1 п.16.4.1 имеем $\chi'_w = \chi_v \circ \mathrm{Tr}_{k'_w/k_v}$. По следствию 1 теор. 3 п.16.4.2 χ_v имеет порядок 0 почти для всех v и χ'_w имеет порядок 0 почти для всех w. Отсюда и из следствия 3 предл. 4 п.16.8.1 вытекает наше утверждение.

Следствие. *В предположениях теоремы* 1 $\mathrm{N}_{k'/k}$ *является открытым морфизмом из $k'^{\times}_{\mathbf{A}}$ на открытую подгруппу в $k^{\times}_{\mathbf{A}}$.*

Согласно следствию 3 теор. 1 п.16.4.1 $\mathrm{N}_{k'/k}$ индуцирует $\mathrm{N}_{k'_w/k_v}$ на $k'^{\times}_w$ почти для всех точек w поля k'. По предложению 5 п.16.9.1 индуцированная норма для всех w, включая бесконечные точки, является открытым морфизмом из $k'^{\times}_w$ на открытую подгруппу в $k^{\times}_v$. По теореме 1 (в совокупности с предложением 3 п.16.9.1) она отображает $r'^{\times}_w$ на $r^{\times}_v$ почти для всех v. В силу следствия предложения 2 п.16.4.3 наше утверждение вытекает из этих фактов.

Если k'_w и k_v такие, как выше, то поле k'_w, которое порождается над k_v полем k', сепарабельно над k_v, так что в случае, когда v и, следовательно, w — конечные точки, дифферента поля k'_w над k_v отлична от нуля и может быть записана как $p_w^{d(w)}$, где $d(w) \geqslant 0$. Этим оправдано следующее определение.

Определение 3. *Пусть k', k такие, как в теореме* 1. *Для каждой конечной точки w поля k' пусть* $\mathfrak{p}_w^{d(w)}$ *— дифферента поля* k'_w *над замыканием* k_v *поля k в* k'_w. *Тогда под дифферентой поля k' над k мы понимаем идеал* $\prod \mathfrak{p}_w^{d(w)}$ *в k", в случае если k, k' — поля характеристики нуль, и дивизор* $\sum d(w) \cdot w$ *поля k', в случаеесли k, k'— поля характеристики p>*1. *Мы будем обозначать дифференту через* $\mathfrak{d}_{k'/k}$ *или просто через* $\mathfrak{d}$, *если это не может привести к путанице.*

Теперь мы рассмотрим раздельно случаи характеристики нуль и характеристики $p>1$.

Предложение 10. *Пусть k — некоторое поле алгебраических чисел, k' — конечное алгебраическое расширение поля k,* $\mathfrak{r}$, $\mathfrak{r}'$ *— их максимальные порядки и* $\mathfrak{d}$ *— дифферента поля k' над k. Тогда* $\mathfrak{d}^{-1}$ *совпадает с множеством тех элементов* $\eta \in k'$, *для которых* $\mathrm{Tr}(\xi\eta) \in \mathfrak{r}$ *при всех* $\xi \in \mathfrak{r}'$.

Возьмем любое $\xi \in \mathfrak{r}'$ и любое $\eta \in \mathfrak{d}^{-1}$. Тогда $\xi\eta \in \mathfrak{d}^{-1}$. По определению это означает, что $\xi\eta \in k'$ и $\xi\eta \in p_w^{-d(w)}$ для всех конечных точек w поля k'. Отсюда следует, что для всех таких точек $\mathrm{Tr}_{k'_w/k_v}(\xi\eta) \in r_v$, поэтому согласно следствию 3 теор. 1 п.16.4.1, $\mathrm{Tr}_{k'_w/k_v}(\xi\eta)$ лежит в $k \cap r_v$ при всех v, и следовательно, лежит в $\mathfrak{r}$. Обратно, предположим, что $\mathrm{Tr}(\xi\eta) \in \mathfrak{r}$ при всех $\xi \in \mathfrak{r}'$ для некоторого $\eta \in k'$. Возьмем $x' = (x'_w) \in k'_{\mathbf{A}}$ и положим $z = \mathrm{Tr}_{k'/k}(x'\eta)$. Тогда по следствию 3 теор. 1 п.16.4.1 $z = (z_v)$ задается формулой.

$$z_v = \sum_{w|v} \mathrm{Tr}_{k'_w/k_v}(x'_w\eta).$$

Пусть v — конечная точка поля k. Согласно следствию 1 теор. 1 п.16.5.2 проекция кольца $\mathfrak{r}'$ на произведение $\prod r'_w$, взятое по всем точкам w, лежащим над v, всюду плотна в этом произведении. Так как по нашему предположению $z_v \in r_v$ для любого $x' \in \mathfrak{r}'$ и так как z_v непрерывно зависит от x', то $z_v \in r_v$ при любом выборе $x'_w \in r'_w$ для всех точек w, лежащих над v. Отсюда вытекает, что $\mathrm{Tr}_{k'_w/k_v}$ отображает $\eta r'_w$ в r_v, а значит, по определению дифференты, $\eta \in p_w^{-d(w)}$. Поскольку это имеет место для всех w, элемент η должен лежать в $\mathfrak{d}^{-1}$.

Следствие. *Если* $\mathfrak{a}'$ *— любой дробный идеал в k', то множество тех элементов* $\eta \in k'$, *для которых* $\mathrm{Tr}_{k'/k}(\xi\eta) \in \mathfrak{r}$ *при всех* $\xi \in \mathfrak{a}'$, *совпадает с дробным идеалом* $\mathfrak{a}'^{-1}\mathfrak{d}^{-1}$.

В самом деле, ввиду предложения 10 это множество состоит из всех η, для которых $\eta\mathfrak{a}' \subset \mathfrak{d}^{-1}$.

Теперь введем два морфизма ι, $\mathfrak{N}$ групп $I(k)$, $I(k')$ дробных идеалов полей k, k' друг в друга. Для этого рассмотрим снова морфизм $a \to \mathrm{id}(a)$ из $k_{\mathbf{A}}^{\times}$ на $I(k)$ с ядром $\Omega_\infty = k_{\mathbf{A}}(P_\infty)^{\times}$, который был определен в п.16.5.3. Как там отмечалось, с помощью этого морфизма можно отождествить $I(k)$ с $k_{\mathbf{A}}^{\times}/\Omega_\infty$. Напомним, что $\Omega_\infty = k_\infty^{\times} \times \prod r_v^{\times}$ — это группа, состоящая из иделей (z_v), для которых $|z_v|_v = 1$ для всякой конечной точки v поля k. Если Ω'_∞ — аналогичная группа для поля k', то мы можем также отождествить $I(k') \subset k_{\mathbf{A}}^{'\times}/\Omega'_\infty$. Обозначим теперь через ι естественное вложение $k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}^{'\times}$. По следствию 1 теор. 1 п.16.4.1 оно отображает каждый элемент $z = (z_v) \in k_{\mathbf{A}}^{\times}$ в такой элемент $\iota(z) = (z'_w) \in k_{\mathbf{A}}^{'\times}$, что $z'_w = z_v$ для любой точки w, лежащей над v. Тогда $|z_v|_v = 1$ влечет $|z'_w|_w = 1$, так что $\iota(z) \in \Omega'_\infty$ тогда и только тогда, когда $z \in \Omega_\infty$. Отсюда видно, что ι определяет инъективный морфизм $I(k) \to I(k')$, который мы будем называть *естественным вложением* группы $I(k)$ *в* $I(k')$ и который будет обозначаться также через ι. В этих обозначениях имеем $(\mathrm{id}) \circ \iota = \iota \circ (\mathrm{id})$; это равенство можно рассматривать также как определение инъекции $\iota\colon I(k) \to I(k')$. Ясно, что если k'' — расширение конечной степени поля k' и если морфизмы $\iota'\colon k_{\mathbf{A}}^{'\times} \to k_{\mathbf{A}}^{''\times}$ и $\iota''\colon k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}^{''\times}$ определены так же, как был определен морфизм $\iota\colon k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}^{'\times}$, то $\iota'' = \iota' \circ \iota$; поэтому соответствующее соотношение выполняется и для естественных вложений $I(k) \to I(k'')$, $I(k') \to I(k'')$ и $I(k) \to I(k')$. С другой стороны, следствие 3 теор. 1 п.16.4.1 в сочетании с формулой (1) п.16.9.1 показывает, что норма $\mathrm{N}_{k'/k}$ отображает Ω'_∞ в Ω_∞ и потому определяет морфизм который тоже принято называть *нормой;* обозначим его через $\mathfrak{N}_{k'/k}$. Имеем $(\mathrm{id}) \circ \mathrm{N}_{k'/k} = \mathfrak{N}_{k'/k} \circ (\mathrm{id})$; это равенство можно рассматривать как определение $\mathfrak{N}_{k'/k}$. Если k'' таково, как выше, то $\mathfrak{N}_{k''/k} = \mathfrak{N}_{k'/k} \circ \mathfrak{N}_{k''/k'}$; это вытекает из соответствующего соотношения для обычных норм. Далее, если n — степень поля k' над k, то $\mathrm{N}_{k'/k}(x) = x^n$ для всех $x \in k$; это непосредственно следует из определения $\mathrm{N}_{k'/k}$. Отсюда вытекает соответствующее соотношение для продолжения нормы $\mathrm{N}_{k'/k}$ на $k_{\mathbf{A}}$. Для $z \in k_{\mathbf{A}}^{\times}$ мы можем записать это соотношение в виде $\mathrm{N}_{k'/k}(\iota(z)) = z^n$, откуда следует, что $\mathfrak{N}_{k'/k}(\iota(\mathfrak{a})) = \mathfrak{a}^n$ при всех $\mathfrak{a} \in I(k)$.

По теореме 3 п.16.5.3 $I(k)$ и $I(k')$ являются свободными группами, порожденными соответственно простыми идеалами $\mathfrak{p}_v$, $\mathfrak{p}'_w$ в

$\mathfrak{r}$, $\mathfrak{r}'$. Сейчас мы дадим описание морфизмов ι, $\mathfrak{N}_{k'/k}$ в терминах этих $\mathfrak{r}$ образующих.

Предложение 11. *Для всякой конечной точки v поля k и всякой точки w поля k', лежащей над v, обозначим через e(w) индекс ветвления и через $f(w)$ модулярную степень поля k'_w над k_v. Тогда*

$$\iota(\mathfrak{p}_v) = \prod_{w|v} \mathfrak{p}_w^{e(w)}, \quad \mathfrak{N}_{k'/k}(\mathfrak{p}'_w) = \mathfrak{p}_v^{f(w)}, \quad \sum_{w|v} e(w) f(w) = n,$$

где произведение в первой формуле и сумма в последней берутся по всем точкам w поля k', лежащим над v.

Первая формула следует из определений, а вторая — из определений, следствия 3 теор. 1 п.16.4.1 и формулы (1) п.16.9.1. Что касается последней формулы, то она вытекает из следствия 1 теор. 4 п.16.3.4, поскольку $e(w) f(w)$ совпадает со степенью поля k'_w над k_v; она непосредственно следует также из первых двух формул и равенства $\mathfrak{N}_{k'/k}(\iota(\mathfrak{p}_v)) = \mathfrak{p}_v^n$.

Следствие. *Пусть k — некоторое поле алгебраических чисел и $\mathfrak{a}$ — дробный идеал в k. Тогда $\mathfrak{N}_{k/\mathbf{Q}}(\mathfrak{a})$ совпадает с дробным идеалом $\mathfrak{N}(\mathfrak{a})\mathbf{Z}$ в* **Q**, *где $\mathfrak{N}$ — норма, введенная в определении* 5 *п.*16.5.3.

Это вытекает из последнего определения и второй формулы предложения 11, примененной к полям *k* и **Q**.

Так как каждый идеал в кольце **Z** имеет вид $m\mathbf{Z}$, где $m \in \mathbf{N}$, то каждый дробный идеал в **Q** может быть одним и только одним способом записан в виде $r\mathbf{Z}$, где $r \in \mathbf{Q}$, $r > 0$. Поэтому можно отождествить группу $I(\mathbf{Q})$ дробных идеалов поля **Q** с группой $\mathbf{Q}_+^\times = \mathbf{Q}^\times \cap \mathbf{R}_+^\times$ при помощи изоморфизма $r \to r\mathbf{Z}$ первой группы на вторую. Тогда норма $\mathfrak{N}$ из определения 5 п.16.5.3 совпадает с нормой

$$\mathfrak{N}_{k/\mathbf{Q}},$$

определенной выше.

Предложение 12. *Пусть χ — характер на $\mathbf{Q}_A$, тривиальный на* **Q**, *для которого $\chi_\infty(x) = \mathbf{e}(-x)$; k — некоторое поле алгебраических чисел, $\chi' = \chi \circ \mathrm{Tr}_{k/\mathbf{Q}}$; $a = (a_v)$ — дифферентный идель, связанный с χ'. Тогда $a_v = 1$ для каждой бесконечной точки v поля k и* $\mathrm{id}(a)$ *совпадает с дифферентой $\mathfrak{d}_{k/\mathbf{Q}}$ поля k над* **Q**.

Характер χ таков же, как введенный в первой части доказательства теоремы 3 п.16.4.2. Там показано, что он однозначно определен сформулированным выше условием и что χ_p имеет порядок 0 для каждой точки *p* поля **Q**. Наше первое утверждение непосредственно следует теперь из определения дифферентного иделя в п.16.7.2, если учесть следствие 3 теор. 1 п.16.4.1. Последнее утверждение вытекает из того же результата, если учесть следствие 3 предл. 4 п.16.9.1.

Следствие. *Пусть поле k таково, как в предложении* 12, *и D — его дискриминант. Тогда* $|D| = \mathfrak{N}(\mathfrak{d}_{k/\mathbf{Q}})$.

Если идель a таков, как в предложении 12, то $|a|_{\mathbf{A}} = |D|^{-1}$ по предложению 6 п.16.7.2. С другой стороны, поскольку $a_v = 1$ для всех бесконечных точек v поля k, то из определения нормы $\mathfrak{N}$ следует, что $|a|_{\mathbf{A}} = \mathfrak{N}(\mathrm{id}(a))^{-1}$. В силу предложения 12 утверждение доказано.

Теперь следующим образом обобщим определение дискриминанта, т. е. определение 6 п.16.5.4.

Определение 4. *Пусть k — некоторое поле алгебраических чисел, k' — конечное расширение поля k и* $\mathfrak{d}$*— дифферента поля k' над k. Тогда идеал* $\mathfrak{D} = \mathfrak{N}_{k'/k}(\mathfrak{d})$ *в максимальном порядке* $\mathfrak{r}$ *поля k называется дискриминантом поля k' над k.*

Следует обратить внимание на то, что в соответствии с этим определением дискриминантом поля k над $\mathbf{Q}$ является не D, а идеал $D\mathbf{Z} = |D|\mathbf{Z}$ в $\mathbf{Z}$. По заданному идеалу D определяется согласно замечанию в конце доказательства предложения 7 п.16.5.4 с помощью формулы $D = (-1)^{r_2}|D|$.

Предложение 13. *Пусть k, k', k'' — поля алгебраических чисел и* $k \subset k' \subset k''$, *и пусть* $\mathfrak{d}$ *и* $\mathfrak{D}$, $\mathfrak{d}'$ *и* $\mathfrak{D}'$, $\mathfrak{d}''$ *и* $\mathfrak{D}''$ *- дифференты и дискриминанты соответственно поля k' над k, поля k'' над k', поля k'' над k. Тогда*

$$\mathfrak{d}'' = \iota'(\mathfrak{d})\,\mathfrak{d}', \quad \mathfrak{D}'' = \mathfrak{D}'^{n'}\mathfrak{N}_{k'/k}(\mathfrak{D}'),$$

где ι' *— естественное вложение* $I(k') \to I(k'')$ *и n' — степень поля k'' над k'.*

Первая формула следует из соответствующего локального результата, т. е. из следствия 4 предл. 4 п.16.9.1. Отсюда и из определения 4, с учетом свойства транзитивности норм, вытекает вторая формула.

Пусть теперь k — некоторое $\mathbf{A}$-поле характеристики $p > 1$ и k' — сепарабельное расширение поля k конечной степени n. Так как отображение $a \to \mathrm{div}(a)$ есть морфизм из $k_{\mathbf{A}}^{\times}$ на группу $D(k)$ дивизоров поля k с ядром $\prod_v r_v^{\times}$, то точно так же, как в случае числовых полей, мы видим, что естественное вложение $k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}'^{\times}$ определяет инъективный морфизм $\iota: D(k) \to D(k')$, который мы будем называть естественным вложением группы $D(k)$ в $D(k')$. Аналогично норменное отображение $N_{k'/k}: k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}^{\times}$ определяет морфизм $D(k') \to D(k)$, который мы будем обозначать через $\mathfrak{S}_{k'/k}$ (обозначение $\mathfrak{N}$ было бы здесь неудобно, поскольку группа дивизоров записывается аддитивно). Свойства морфизмов ι и $\mathfrak{S}$ аналогичны свойствам

морфизмов ι и $\mathfrak{N}$ в случае числовых полей. В частности, $\mathfrak{S}_{k'/k}(\iota(\mathfrak{a})) = n\mathfrak{a}$ для каждого дивизора а поля k и, в обозначениях предложения 11,

$$\iota(v) = \sum_{w|v} e(w) \cdot w, \quad \mathfrak{S}_{k'/k}(w) = f(w) \cdot v, \quad \sum_{w|v} e(w) f(w) = n,$$

причем доказательство остается прежним. Пусть $\mathbf{F}_q$, $\mathbf{F}_{q'}$— поля констант в k и k', и пусть f_0 — степень второго поля над первым. Тогда, по определению $f(w)$ и степени точки, $f_0 \deg(w) = f(w) \deg(v)$ и, следовательно, сначала для точек, а затем и для произвольных дивизоров мы получаем

$$\deg(\mathfrak{S}_{k'/k}(\mathfrak{a}')) = f_0 \deg(\mathfrak{a}'), \quad \deg(\iota(\mathfrak{a})) = (n/f_0) \deg(\mathfrak{a}), \quad (12)$$

где $\mathfrak{a}'$ — произвольный дивизор поля k', а $\mathfrak{a}$ — произвольный дивизор поля k.

Пусть $\mathfrak{d}$— дифферента поля k' над k. Определим *дискриминант* поля k' над k как дивизор $\mathfrak{S}_{k'/k}(\mathfrak{d})$ поля k. В обозначениях, аналогичных обозначениям предложения 13, имеем

$$\mathfrak{d}'' = \iota'(\mathfrak{d}) + \mathfrak{d}', \quad \mathfrak{D}'' = n'\mathfrak{D} + \mathfrak{S}_{k'/k}(\mathfrak{D}').$$

Предложение 14. *Пусть k и k' такие, как выше, $\mathfrak{d}$— дифферента поля k' над k и $\mathfrak{c}$— канонический дивизор поля k. Тогда дивизор $\iota(\mathfrak{c}) + \mathfrak{d}$ является каноническим дивизором поля k'.*

По определению канонического дивизора существует базисный характер χ, для которого $\mathfrak{c} = \operatorname{div}(\chi)$. Тогда следствие 3 предл. 4 п.16.9.1 в сочетании со следствием 3 теор. 1 п.16.4.1 и с определениями показывает, что $\operatorname{div}(\chi \circ \mathrm{Tr}_{k'/k}) = \iota(\mathfrak{c}) + \mathfrak{d}$.

Следствие. *Пусть k, k' и $\mathfrak{d}$ таковы, как в предложении* 14, *g — род поля k, n — степень поля k' над k и f_0 — степень поля констант в k' над полем констант в k. Тогда род g' поля k' задается формулой*

$$2g' - 2 = (n/f_0)(2g - 2) + \deg(\mathfrak{d}).$$

Это вытекает из предложения 14, следствия 1 теор. 2 п.16.6 и второй из формул (12). Отсюда следует, что степень дифференты всегда четна.

16.9.5. Расщепимые точки в сепарабельных расширениях

Теорему 1 п.16.9.4 можно переформулировать следующим образом: в предположениях и обозначениях этой теоремы почти для всех точек w поля k' степень поля k'_w над k_v равна модулярной степени поля k'_w над k_v. Поэтому следствия 2 и 3 предл. 1 п.16.7.1 и следствия 3 и 4 теор. 2

п.16.7.5 остаются справедливыми при замене «степени» на «модулярную степень», если дополнительно предположить сепарабельность поля k над k_0. Мы рассмотрим некоторые следствия из этих результатов.

Как и прежде, пусть k — некоторое **A**-поле, k' — сепарабельное расширение поля k конечной степени n и v — некоторая точка поля k. Мы можем записать $k' = k(\xi)$, где ξ — корень некоторого неприводимого унитарного многочлена $F \in k[X]$ степени n. Сопоставление теоремы 4 п.16.3.4 с предложением 2 п.16.3.2 показывает, что точки w поля k', лежащие над v, находятся во взаимно однозначном соответствии с неприводимыми унитарными многочленами из $k_v[X]$, делящими F. Если для каждой такой точки w обозначить через F_w соответствующий ей многочлен, то степень поля k'_w над k_v равна степени многочлена F_w. По теореме 1 п.16.9.4 почти для всех v эта степень равна модулярной степени поля k'_w над k_v. Мы видели также, что лежащие над v точки w, для которых $k'_w = k_v$, находятся во взаимно однозначном соответствии с корнями многочлена F в k_v. По следствию 1 теор. 4 п.16.3.4 тогда и только тогда имеется n различных точек поля k', лежащих над v, когда $k'_w = k_v$ для каждой такой точки. В случае когда это так, говорят, что точка v *вполне расщепима* в k'; это имеет место в том и только в том случае, когда F имеет n различных корней в k_v. Если L — расширение Галуа поля k, то по следствию 4 теор. 4 п.16.3.4 пополнения поля L по его точкам, лежащим над v, все между собой изоморфны. Поэтому если $L_u = k_v$ для одной такой точки u, то точка v вполне расщепима в L. Пусть $k' = k(\xi)$ — поле, промежуточное между k и L. Тогда определенный выше многочлен F разлагается в $L[X]$ на линейные множители и наименьшее расширение Галуа L' поля k, содержащееся в L и содержащее k', является подполем в L, порожденным над k корнями F в L. Если теперь t — точка поля L', лежащая над v, то L'_t порождается над k_v корнями многочлена F, так что $L'_t = k_v$ в том и только в том случае, когда точка v вполне расщепима в k'. В этом случае, как мы уже видели, она расщепима также и в L'.

Предложение 15. *Пусть k', k'' — два расширения поля k, содержащиеся оба в некотором сепарабельном расширении L конечной степени над k, и пусть X — множество таких точек v поля k, что $k'_w = k_v$ по крайней мере для одной точки w поля k', лежащей над v. Тогда если почти все точки $v \in X$ вполне расщепимы в k'', то k'' содержится в k'.*

Можно считать, что L есть композит полей k' и k''. Обозначим через W множество тех точек w поля k', для которых точки v, лежащие под w, вполне расщепимы в k'' и $k'_w = k_v$. Пусть u — точка поля L, лежащая

над w, и t — точка поля k'', лежащая под u. Поле L_u порождается над k_v полем L, а следовательно, полями k'_w и k''_t. Поэтому если $w \in W$, то $L_u = k_v$. Это показывает, что все точки из W вполне расщепимы в L. Рассмотрим теперь точку w поля k', не лежащую в W. Обозначим через v точку поля k, лежащую под w. Если $k_v = k'_w$,' то точка $v \in X$, так что она должна содержаться в конечном подмножестве в X, состоящем из тех точек в X, которые не вполне расщепимы в k''. Если $k_v \neq k'_w$, то степень поля k'_w над k_v больше 1. По теореме 1 п.16.9.4 эта степень совпадает с модулярной степенью, если исключить некоторое конечное множество точек. Таким образом, показано, что модулярная степень поля k'_w над k_v больше 1 почти для всех точек w поля k'', не лежащих в W. Применяя теперь к k, k' и L следствие 4 теор. 2 п.16.7.5 (в этом следствии надо заменить k_0, k, k' на k, k', L), получаем, что $k' = L$, т. е. $k'' \subset k'$.

Следствие. *Пусть k', k'' — два расширения Галуа поля k, содержащиеся в некотором расширении конечной степени поля k. Пусть S' и S'' — множества точек поля k, вполне расщепимых в k' и k'' соответственно. Тогда k' содержит k'' в том и только в том случае, когда S'' содержит почти все точки $v \in S'$.*

Если $k' \supset k''$, то, очевидно, точки поля k, вполне расщепимые в k', вполне расщепимы и в k''. Обратно, поскольку k' — расширение Галуа, то S' совпадает с множеством X из предложения 15 и наше утверждение следует из этого предложения. В частности, мы видим, что k' должно совпадать с k'', если S' и S'' различаются лишь конечным числом элементов.

16.9. 6. Применение к несепарабельным расширениям

Мы докажем, что один из основных наших результатов, а именно теорема 1 п.16.4.1 об изоморфизме между k'_A и $(k'/k)_A$, сформулированная и доказанная для сепарабельных расширений, остается справедливым и без предположения сепарабельности. Для этого нам понадобится одна лемма.

Лемма 1. *Пусть k — некоторое* **A***-поле характеристики $p > 1$. Тогда поле k чисто несепарабельно и имеет степень p над своим образом k^v при эндоморфизме $x \to x^p$.*

По лемме 1 п.16.3.2 можно записать поле k в виде $k = \mathbf{F}_p(x_0, \ldots, x_N)$, где элемент x_0 трансцендентен над $\mathbf{F}_p$, а элементы x_i сепарабельно алгебраичны над $\mathbf{F}_p(x_0)$ для $1 \leqslant i \leqslant N$. Тогда $k^p = \mathbf{F}_p(x_0^p, \ldots, x_N^p)$. Положим $k' = k^p(x_0) = \mathbf{F}_p(x_0, x_1^p, \ldots, x_N^p)$. Так как каждый элемент x_i чисто несепарабелен над $\mathbf{F}_p(x_i^p)$ и сепарабелен

над $\mathbf{F}_p(x_0)$, то поле k одновременно чисто несепарабельно и сепарабельно над k', так что $k = k'$. Отсюда следует, что k есть чисто несепарабельное расширение степени 1 или p над k^v. Если бы поле k совпадало с k^p, то оно содержало бы элемент y, такой, что $y^p = x_0$. Ясно, что элемент y не может содержаться в $\mathbf{F}_p(x_0)$, так что он чисто несепарабелен над $\mathbf{F}_p(x_0)$, вопреки предположению о сепарабельности поля k над $\mathbf{F}_p(x_0)$.

Теперь для распространения теоремы 1 п.16.4.1 на случай несепарабельного расширения k' поля k достаточно, очевидно, доказать справедливость в этом случае теоремы 4 п.16.3.4, поскольку лишь эта теорема используется при доказательстве теоремы 1 п.16.4.1. Сначала мы сделаем это для чисто несепарабельного расширения степени p поля k. Пусть k' — такое расширение. Тогда для любого $x' \in k'$ должно существовать такое целое $n \geq 0$, что $x'^{p^n} \in k$, и если n — наименьшее среди таких чисел, то степень элемента x' над k равна p^n. Так как эта степень должна быть $\leq p$, то $n = 0$ или 1. Это показывает, что $k'^p \subset k \subset k'$; следовательно, в силу леммы 1 $k = k'^p$. Для этого случая докажем следующее

Предложение 16. *Пусть k' — некоторое* **A**-*поле характеристики $p > 1$, и пусть $k = k'^p$. Тогда над каждой точкой v поля k лежит одна и только одна точка w поля k'. Эта точка является образом точки v при изоморфизме $x \to x^{1/p}$ поля k в k', $k_v = (k'_w)^p$ и k_v-линейное продолжение Φ_v естественного вложения поля k' в k'_w на $A_v = k' \otimes_k k_v$ является изоморфизмом из A_v на k'_w. Кроме того, если α — какой-либо базис в k' над k и α_v для каждой точки v есть r_v-модуль, порожденный в A_v множеством α, то Φ_v отображает α_v на максимальное компактное подкольцо r'_w в k'_w почти для всех v.*

Пусть v — точка поля k и w — точка поля k', лежащая над v. По следствию предложения 1 п.16.3.1 поле k' порождается над k_v полем k'', следовательно, оно чисто несепарабельно над k_v и его степень равна 1 или p. В первом случае каждый элемент из k должен быть p-й степенью в k_v, что невозможно, поскольку k плотно в k_v и, значит, содержит хотя бы один простой элемент поля k_v. Поэтому согласно следствию 2 предл. 4 п.16.1.4 поле k'_w определено однозначно с точностью до изоморфизма и отображение $y \to y^p$ есть изоморфизм из k'_w на k_v. Пусть λ — естественное вложение $k' \to k'_w$. Это вложение должно индуцировать на k естественное вложение $\lambda_0 : k \to k_v$. Поэтому для каждого $\xi \in k'$ имеем $\lambda_0(\xi^p) = \lambda(\xi)^p$. Так как это равенство однозначно определяет $\lambda(\xi)$, то мы видим, что точка w однозначно определяется по точке v, а также что точка w является образом точки v при изоморфизме $x \to x^{1/p}$. Если теперь отображение Φ_v таково, как в

нашем предложении, то, очевидно, оно является сюръективным гомоморфизмом из A_v на k'_w. Так как оба пространства имеют размерность p над k_v, то Φ_v является изоморфизмом. Наконец, пусть α — какой-либо базис в k' над k. Ввиду следствия 1 теор. 3 п.16.3.1 и леммы 1 п.16.3.2 можно считать, что α содержит такой элемент a, что k' является сепарабельным алгебраическим расширением поля $\mathbf{F}_p(a)$. Пусть точки v и w такие, как выше, и пусть u — точка поля $k_0 = \mathbf{F}_p(a)$, лежащая под w. По теореме 1 п.16.9.4 почти для всех w поле k'_w неразветвлено над $(k_0)_u$. Возьмем точку w, для которой это имеет место. Поскольку, как показывает теорема 2 п.16.3.3, поле k_0 имеет в точности одну точку u, для которой $|a|_u > 1$, то можно считать также, что w не лежит над этой точкой. Тогда по той же теореме существует такой многочлен $\pi \in \mathbf{F}_p[T]$, что $\pi(a)$ есть простой элемент в $(k_0)_u$ и, следовательно, в k'_w, ибо k'_w неразветвлено над $(k_0)_u$. Далее, по следствию 2 теор. 3 п.16.3.1 α_v есть компактное подкольцо в A_v почти для всех v. Отсюда следует, что оно содержит 1 и поэтому $r_v \cdot 1$. Поскольку это кольцо содержит a, оно содержит также $\pi(a)$, а следовательно, содержит кольцо $r_v[\pi(a)]$ и, значит, согласно предложению 4 п.16.1.4 и его следствиям, совпадает с r'_w.

Ясно, что из предложения 16 вытекает справедливость теоремы 4 п.16.3.4 для случая, когда $k = k'^p$. Рассмотрим теперь произвольное расширение k' конечной степени над k. Обозначим через k'_0 максимальное сепарабельное алгебраическое расширение поля k, содержащееся в k'. Пусть p^m — степень поля k над k'_0 и $x' \in k'$. Тогда существует такое $n \geq 0$, что $x'^{p^n} \in k'_0$, и если n — наименьшее среди таких чисел, то x' имеет степень p^n над k'_a, так что $n \leqslant m$. Это показывает, что $k' \supset k'_0 \supset k'^{p^m}$. Применяя к последовательности полей $k', k'^p, \ldots, k'^{p^m}$ лемму 1, мы видим, что каждое из этих полей имеет степень p над последующим, так что k' имеет степень p^m над полем k'^{p^m}, которое поэтому совпадает с k'_0. Теперь проведем индукцию по m. Допустим, что теорема 4 п.16.3.4 справедлива для расширения k'^p поля k; нам следует доказать ее справедливость для расширения k' поля k. Положим $k'' = k'^p$. Пусть v — некоторая точка поля k. Обозначим через $w'_1, \ldots, w'_r$ точки поля k'', лежащие над v, и для каждого i обозначим через k''_i пополнение поля k'' относительно w'_i. По предложению 16 для каждого i существует одна и только одна точка w поля k', лежащая над w'_i, и пополнение k'_i поля k' относительно w_i может быть отождествлено с $k' \otimes_{k''} k''_i$. По предположению индукции имеет место изоморфизм Φ'_v из $A'_v = k'' \otimes_k k_v$ на прямую сумму полей k'', удовлетворяющий условиям, указанным в формулировке теоремы. По свойствам тензорных произведений

произведение $A_v = k' \otimes_k k_v$ очевидным образом канонически изоморфно произведению $k' \otimes_{k''} A''_v$, а значит, прямой сумме произведений $k' \otimes_{k''} k''_i$ и, следовательно, прямой сумме полей k'_i. Очевидно, что так определенный изоморфизм Φ_v из A_v в последнюю сумму обладает всеми нужными свойствами. Что касается последнего утверждения теоремы, то его можно аналогичным способом вывести из нашего предположения индукции с помощью предложения 16, если взять какой-нибудь базис α' в k'' над k, какой-нибудь базис β в k' над k'' и в качестве базиса в k' над k взять базис α, состоящий из всех произведений $a'b$ элементов $a' \in \alpha'$ и $b \in \beta$.

17. Нечеткие числа

17.1. Основные определения

В теории нечетких систем выделяются нечеткие множества, которые определяются на оси действительных чисел. Например, нечеткие множества чисел, «близких числу 7» (рис. 1) определены на множестве $\mathbf{R}$ и, кроме того, являются нормальными и выпуклыми, а также имеют непрерывные функции принадлежности. Дадим определение понятия «нечеткое число».

Определение 1

Нечетким числом называется нечеткое множество A, определенное на множестве действительных чисел $A \subseteq \mathbf{R}$, функция принадлежности которого

$$\mu_A : \mathbf{R}[0,1]$$

отвечает условиям:

1) $\sup_{x \in \mathbf{R}} \mu_A(x) = 1$, т.е. нечеткое множество A нормализовано;

2) $\mu_A\left[\lambda x_1 + (1-\lambda)\, x \min\left\{\mu_A(x_1), \mu_A(x_2)\right\}\right]$, т.е. множество A выпуклое;

3) $\mu_A(x)$.

На рис. 1 представлены примеры нечетких чисел.

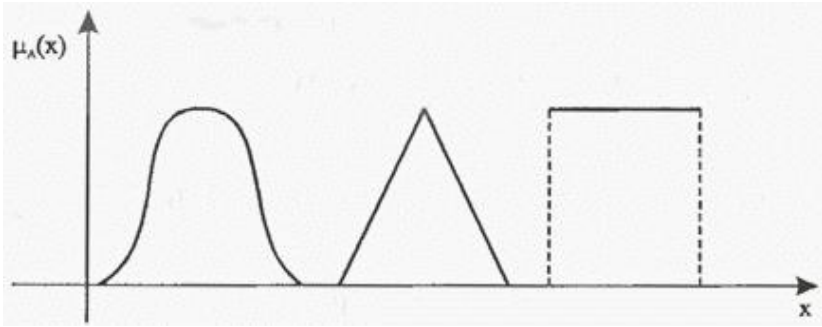


Рис. 1. Примеры нечетких чисел.

В теории нечетких систем различаются положительные и отрицательные нечеткие числа.

Определение 2.

Нечеткое число $A \subseteq \mathbf{R}$ положительно, если $\mu_A(x) = 0$ для всех $x < 0$.

Нечеткое число $A \subseteq \mathbf{R}$ отрицательно, если $\mu_A(x) = 0$ для всех $x > 0$.

На рис. 2 представлен пример положительного и отрицательного нечетких чисел, а также такого нечеткого числа, которое не является ни положительным, ни отрицательным.

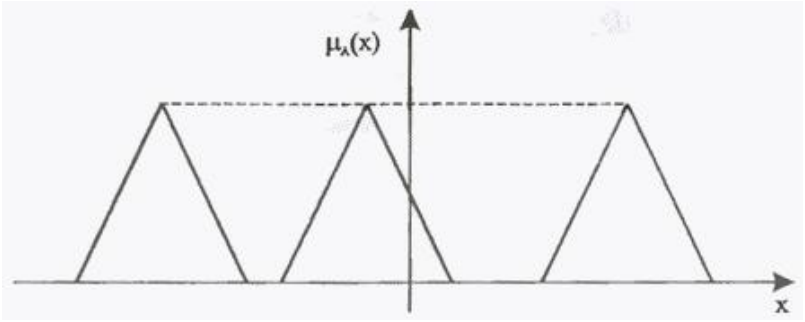


Рис. 2. Примеры нечетких чисел: положительного, отрицательного, а также такого, которое не является ни положительным, ни отрицательным.

Основные арифметические операции на нечетких числах будут заданы с помощью принципа расширения, который позволяет сформулировать определения суммирования, вычитания, умножения и деления двух нечетких чисел $A_1, A_2 \subseteq \mathbf{R}$. В определении 3 отображение принимает вид

$$y = f(x_1, x_2) = \begin{cases} x_1 + x_2 & \text{при сложении нечетких чисел } A_1 \text{ и } A_2, \\ x_1 - x_2 & \text{при вычитании нечетких чисел } A_1 \text{ и } A_2, \\ x_1 \cdot x_2 & \text{при умножении нечетких чисел } A_1 \text{ и } A_2, \\ x_1 / x_2 & \text{при делении нечетких чисел } A_1 \text{ и } A_2. \end{cases}$$

Определение 3

Основные арифметические операции на нечетких числах $A_1, A_2 \subseteq \mathbf{R}$ определяются следующим образом:

а) суммирование двух нечетких чисел A_1 и A_2 обозначается

$$A_1 \oplus A_2 \overset{def}{=} B, \qquad (1)$$

причем функция принадлежности суммы (1) задается выражением в виде

$$\mu_B(y) = \sup_{\substack{x_1, x_2 \\ y = x_1 + x_2}} \min\left\{\mu_{A_1}(x_1), \mu_{A_2}(x_2)\right\}, \qquad (2)$$

б) вычитание двух нечетких чисел A_1 и A_2 обозначается

$$A_1 \ominus A_2 \overset{def}{=} B, \qquad (3)$$

причем функция принадлежности разности (3) задается выражением (в виде

$$\mu_B(y) = \sup_{\substack{x_1, x_2 \\ y = x_1 - x_2}} \min\left\{\mu_{A_1}(x_1), \mu_{A_2}(x_2)\right\}, \qquad (4)$$

в) умножение двух нечетких чисел A_1 и A_2 обозначается

$$A_1 \odot A_2 \overset{def}{=} B, \qquad (5)$$

причем функция принадлежности произведения (5) задается выражением в виде

$$\mu_B(y) = \sup_{\substack{x_1, x_2 \\ y = x_1 \cdot x_2}} \min\left\{\mu_{A_1}(x_1), \mu_{A_2}(x_2)\right\}, \qquad (6)$$

г) деление двух нечетких чисел A_1 и A_2 обозначается

$$A_1(:)A_2 \overset{def}{=} B, \tag{7}$$

причем функция принадлежности частного (7) задается выражением в виде

$$\mu_B(y) = \sup_{\substack{x_1,x_2 \\ y=x_1:x_2}} \min\left\{\mu_{A_1}(x_1), \mu_{A_2}(x_2)\right\}. \tag{3.109}$$

Поскольку с точки зрения приложений нас в первую очередь интересуют нечеткие числа, имеющие непрерывные функции принадлежности, то для иллюстрации приведенных определений рассмотрим дискретный случай.

Пример 1.

Сложим и перемножим два нечетких числа, имеющих вид

$$A_1 = \frac{0,7}{2} + \frac{1}{3} + \frac{0,6}{4}, \tag{9}$$

$$A_2 = \frac{0,8}{3} + \frac{1}{4} + \frac{0,5}{6}. \tag{10}$$

В соответствии с формулой (2) получаем

$$A_1 \oplus A_2 = \frac{\min(0,7;0,8)}{5} + \frac{\max\{\min(0,7;1), \min(1;0,8)\}}{6} + \frac{\max\{\min(1;1), \min(0,6;0,8)\}}{7} + \\ + \frac{\max\{\min(0,7;0,5), \min(0,6;1)\}}{8} + \frac{\min(1;0,5)}{9} + \frac{\min(0,6;0,5)}{10} = \\ = \frac{0,7}{5} + \frac{0,8}{6} + \frac{1}{7} + \frac{0,6}{8} + \frac{0,5}{9} + \frac{0,5}{10}. \tag{11}$$

На основании выражения (6) получаем

$$A_1 \odot A_2 = \frac{\min(0,7;0,8)}{6} + \frac{\min(0,7;1)}{8} + \frac{\min(1;0,8)}{9} +$$
$$+ \frac{\max\{\min(0,7;0,5), \min(1;1), \min(0,6;0,8)\}}{12} +$$
$$+ \frac{\min(0,6;1)}{16} + \frac{\min(1;0,5)}{18} + \frac{\min(0,6;0,5)}{24} =$$
$$= \frac{0,7}{6} + \frac{0,7}{8} + \frac{0,8}{9} + \frac{1}{2} + \frac{0,6}{16} + \frac{0,5}{18} + \frac{0,5}{24}. \quad (12)$$

В приведенном примере мы сложили и перемножили два нечетких числа (9) и (10), получив в качестве суммы нечеткое множество (11), а в качестве произведения - нечеткое множество (12). Легко проверить, что нечеткие множества (11) и (12) являются нормальными и выпуклыми, и что они представляют собой нечеткие числа. Однако результатом арифметических операций над нечеткими числами не всегда оказывается нечеткое число. Эта проблема устраняется тогда, когда операции выполняются над нечеткими числами, имеющими непрерывные функции принадлежности, что утверждается следующей теоремой:

Теорема 1 (Дюбуа и Прейда).

Если нечеткие числа A_1 и A_2 имеют непрерывные функции принадлежности, то результатом арифметических операций суммирования, вычитания, умножения и деления будут нечеткие числа.

Мы обсудили основные двухаргументные (бинарные) операции на нечетких множествах. Одноаргументные (унарные) операции определяются также с помощью принципа расширения. Если f - отображение

$$f : \mathbf{R} \to \mathbf{R} \quad (13)$$

и $A \subseteq \mathbf{R}$, $y = f(x)$, то получаем

$$\mu_B(y) = \sup_{\substack{x \\ y=f(x)}} \mu_A(x), \qquad (14)$$

где $B = f(A)$.

Приведем теперь несколько примеров унарных операций на нечетких числах.

1. Операция изменения знака. В результате операции $f(x) = -x$ получаем нечеткое число, противоположное нечеткому числу $A \subseteq \mathbf{R}$. Это число обозначается - $A \subseteq \mathbf{R}$, а его функция принадлежности равна

$$\mu_{-A}(x) = \mu_A(-x). \qquad (15)$$

Нечеткие числа A и $-A$ симметричны относительно оси x.

2. Операция обращения. В результате операции $f(x) = x^{-1}$, $x \neq 0$, получаем нечеткое число, обратное нечеткому числу $A \subseteq \mathbf{R}$. Это число обозначается $A^{-1} \subseteq \mathbf{R}$, а его функция принадлежности равна

$$\mu_{A^{-1}}(x) = \mu_A\left(x^{-1}\right). \qquad (16)$$

Предполагается, что нечеткое число A положительно или отрицательно. Если A таковым не является, то нечеткое множество

$B = f(A) = A^{-1}$ не выпукло и, следовательно, B не может считаться нечетким числом.

3. Операция масштабирования. В результате операции $f(x) = \lambda^x$, $\lambda \neq 0$, получаем нечеткое число, масштабированное относительно нечеткого числа $A \subseteq \mathbf{R}$. Это число обозначается $\lambda A \subseteq \mathbf{R}$, а его функция принадлежности равна

$$\mu_{\lambda A}(x) = \mu_A\left(x\lambda^{-1}\right). \tag{17}$$

4. Операция экспонирования. В результате операции $f(x) = e^x$, $x > 0$, получаем степень нечеткого числа $A \subseteq \mathbf{R}$. Это число обозначается $e^A \subseteq \mathbf{R}$, а его функция принадлежности равна

$$\mu_{e^A}(x) = \begin{cases} \mu_A(\log x) & \text{для } x > 0, \\ 0 & \text{для } x < 0, \end{cases} \tag{18}$$

поэтому e^A - положительное нечеткое число.

5. Операция расчета абсолютного значения. Абсолютное значение нечеткого числа $A \subseteq R$ обозначается $|A| \subseteq \mathbf{R}$ и определяется как

$$\mu_{|A|}(x) = \begin{cases} \max\left(\mu_A(x), \mu_A(-x)\right) & \text{для } x \geq 0, \\ 0 & \text{для } x < 0. \end{cases} \tag{19}$$

Очевидно, что $|A|$ - положительное нечеткое число.

Пример 2.

Если

$$A = \frac{0,7}{1} + \frac{1}{2} + \frac{0,6}{5}, \tag{20}$$

то нечеткое число $-A$ имеет вид

$$-A = \frac{0,6}{-5} + \frac{1}{-2} + \frac{0,7}{-1}, \tag{21}$$

тогда как нечеткое число A^{-1} записывается в виде

$$A^{-1} = \frac{0,6}{2} + \frac{1}{0,5} + \frac{0,7}{1}. \tag{22}$$

С использованием определения 3 легко проверить, что в приведенном примере

$$A + (-A) \neq \frac{1}{0}, \tag{23}$$

а также

$$A \cdot A^{-1} \neq \frac{1}{1}. \tag{24}$$

По этой причине для нечетких систем характерно отсутствие нечетких чисел, противоположных или обратных относительно суммирования и умножения. Этот факт, в частности, делает невозможным применение метода исключения для решения уравнений, в которых присутствуют нечеткие числа.

Арифметические операции над нечеткими числами требуют проведения достаточно сложных вычислений. Поэтому Дюбуа и Прейд предложили некоторую частную форму представления нечетких чисел при помощи трех параметров, что значительно упрощает нечеткую арифметику. Пусть L и P - функции, выполняющие отображение

$$(-\infty,\infty)\to[0,1] \tag{25}$$

и удовлетворяющие условиям:

1) $L(-x)=L(x)$, $P(-x)=P(x)$,

2) $L(0)=1$, $P(0)=1$,

3) L и P - функции, невозрастающие на интервале $[0,+\infty)$.

В качестве примеров функций L и P можно привести

$$L(x)=P(x)=e^{-|x|^p},\ p>0, \tag{26}$$

$$L(x)=P(x)=\frac{1}{1+|x|^p},\ p>0, \tag{27}$$

$$L(x)=P(x)=\max\left(0,1-|x|^p\right),\ p>0, \tag{28}$$

$$L(x)=P(x)=\begin{cases}1 & \text{для } x\in[-1;1],\\ 0 & \text{для } x\notin[-1;1].\end{cases} \tag{29}$$

Приведем теперь определение нечеткого числа типа $L-P$.

Определение 4.

Нечеткое число $A \subseteq \mathbf{R}$ будет нечетким числом типа $L-P$ тогда и только тогда, когда его функция принадлежности имеет вид

$$A(x)=\begin{cases} L\left(\dfrac{m-x}{\alpha}\right), & \text{если } x \le m, \\ P\left(\dfrac{x-m}{\beta}\right), & \text{если } x \ge m, \end{cases} \tag{30}$$

где m - действительное число, называемое средним значением нечеткого числа $A(\mu_A(m)=1)$, α - положительное действительное число, называемое левосторонним разбросом, β - положительное действительное число, называемое правосторонним разбросом.

Заметим, что при увеличении разбросов α и β число A становится «более» нечетким. Нечеткое число типа $L-P$ можно сокращенно записать в виде

$$A=(m_A, \alpha_A, \beta_A)_{LP}. \tag{31}$$

Пример 3.

Нечеткое число «примерно 9» можно определить как

$$A=(9,3,3)_{LP}. \tag{32}$$

Функция принадлежности этого числа представлена на рис. 3, причем

$$L(x) = P(x) = \frac{1}{1+x^2}. \tag{33}$$

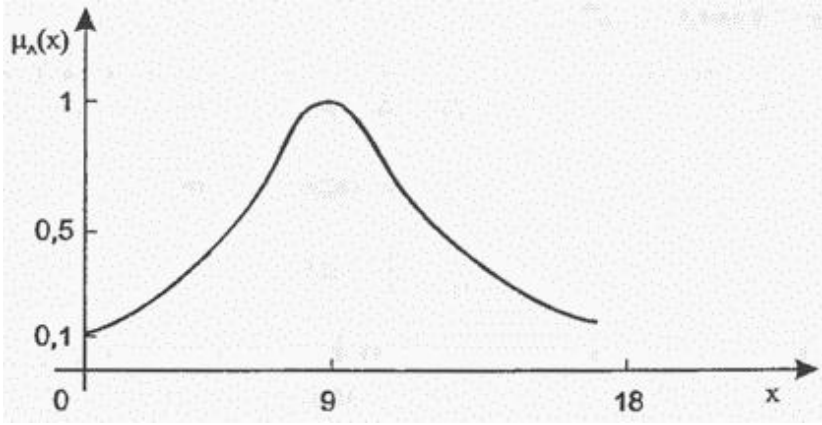


Рис. 3. Иллюстрация к примеру 3.

Арифметические операции над нечеткими числами типа $L-P$ сводятся к операции над тремя параметрами. Нечеткое число, противоположное нечеткому числу (31), равно

$$-A = (-m_A, \alpha, \beta)_{LP}. \tag{34}$$

Сумма нечетких чисел

$$A = (m_A, \alpha_A, \beta_A) \text{ и } B = (m_B, \alpha_B, \beta_B)$$

имеет вид

$$A \oplus B = (m_A + m_B, \alpha_A + \alpha_B, \beta_A + \beta_B)_{LP}. \tag{35}$$

Другие арифметические операции (например, умножение и деление) над нечеткими числами типа $L-P$ более сложны, а их результат имеет приближенный характер.

Функция принадлежности $\mu_A(x)$ нечеткого числа типа $L-P$ принимает значение 1 только в точке $x=m$. Модифицируем теперь определение 4 так, чтобы $\mu_A(x)=1$ не только в единственной точке $x=m$, но и во всех точках на интервале $[m_1, m_2]$, где $m_1 < m_2$ и $m_1, m_2 \in \mathbf{R}$.

В этом случае мы получаем определение так называемого плоского нечеткого числа. Это определение можно использовать для моделирования нечетких интервалов.

Определение 5.

Плоским нечетким числом типа $L-P$ называется нечеткое число с функцией принадлежности

$$A(x)=\begin{cases} L\left(\dfrac{m_1-x}{\alpha}\right), & \text{если } x \le m_1, \\ 1, & \text{если } m_1 \le x \le m_2, \\ P\left(\dfrac{x-m_2}{\beta}\right), & \text{если } x \ge m_2. \end{cases} \tag{36}$$

Плоское нечеткое число A можно отождествить с нечетким интервалом A вида

$$A=(m_1, m_2, \alpha, \beta)_{LP}. \tag{37}$$

Пример 4.

Рассмотрим неточное утверждение «стоимость велосипеда в этом магазине составляет от 3 до 6 тысяч рублей». Адекватной формализацией этого утверждения может считаться нечеткий интервал A вида

$$A = (3, 6, \alpha, \beta)_{LP}. \tag{38}$$

На рис. 4 представлен примерный график функции принадлежности нечеткого интервала (38).

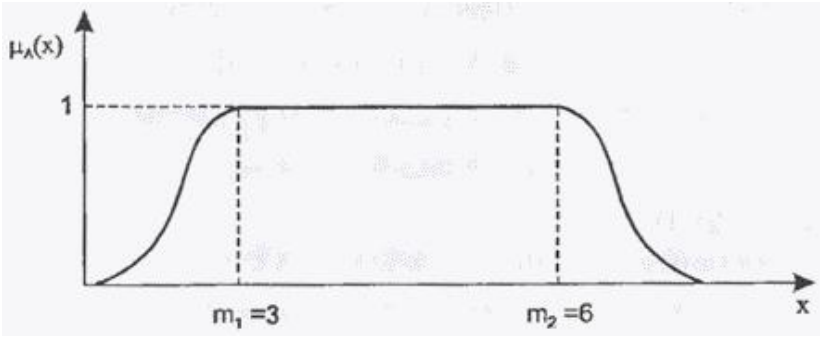


Рис. 4. Иллюстрация к примеру 4: нечеткий интервал «от 3 до 6 тысяч рублей».

Напомним, что нечеткое число — это нечеткое подмножество универсального множества действительных чисел, имеющее нормальную и выпуклую функцию принадлежности, то есть такую, что: a) существует значение носителя, в котором функция принадлежности равна единице, а также b) при отступлении от своего максимума влево или вправо функция принадлежности не возрастает.

Нечеткое число A **унимодально**, если условие $\mu_A(x) = 1$ справедливо только для одной точки действительной оси.

Выпуклое нечеткое число A называется **нечетким нулем**, если

$$\mu_A(0) = \sup_X (\mu_A(x)).$$

Подмножество $S_A \subseteq R$ называется **носителем** нечеткого числа A, если

$$S = \{x | \mu_A(x) > 0\}.$$

Нечеткое число A **положительно**, если $\forall x \in S_A \; x > 0$, и **отрицательно**, если $\forall x \in S_A \; x < 0$.

Согласно принципу обобщения Заде было введено понятие арифметических операций на множестве нечетких чисел. Для произвольных нечетких чисел A, B, C и для любых чисел $x, y, z \in R$ справедливо

$$C = A \tilde{*} B \quad \Leftrightarrow \quad \sup_{z=x*y} (\mu_A(x) \wedge \mu_B(y)).$$

Расширенные бинарные арифметические операции (сложение, умножение и пр.) для нечетких чисел определяются через соответствующие операции для четких чисел с использованием принципа обобщения следующим образом:

$$C = A \tilde{+} B \quad \Leftrightarrow \quad \sup_{z=x+y} (\mu_A(x) \wedge \mu_B(y)).$$

$$C = A \tilde{-} B \quad \Leftrightarrow \quad \sup_{z=x-y} (\mu_A(x) \wedge \mu_B(y)).$$

$$C = A \tilde{\cdot} B \quad \Leftrightarrow \quad \sup_{z=xy} (\mu_A(x) \wedge \mu_B(y)).$$

$$C = A \tilde{\div} B \quad \Leftrightarrow \quad \sup_{z=x/y} (\mu_A(x) \wedge \mu_B(y)).$$

Анализ свойств арифметических операций над нечеткими числами показал, что нечеткое число не имеет противоположного и обратного

чисел, сложение и умножение коммутативны, ассоциативны и в общем случае недистрибутивны.

При решении задач математического моделирования нечетких систем можно использовать нечеткие числа (L-R)-типа, которые предполагают более простую интерпретацию расширенных бинарных отношений.

Нечеткие числа (L-R)-типа — это разновидность нечетких чисел специального вида, т.е. задаваемых по определенным правилам с целью снижения объема вычислений при операциях над ними.

Функции принадлежности нечетких чисел (L-R)-типа задаются с помощью невозрастающих на множестве неотрицательных действительных чисел функций действительного переменного $L(x)$ и $R(x)$, удовлетворяющих свойствам:

а) $L(-x) = L(x)$, $R(-x) = R(x)$;

б) $L(0) = R(0)$.

Очевидно, что к классу $(L-R)$-функций относятся функции, графики которых имеют следующий вид (см. рис. 5).

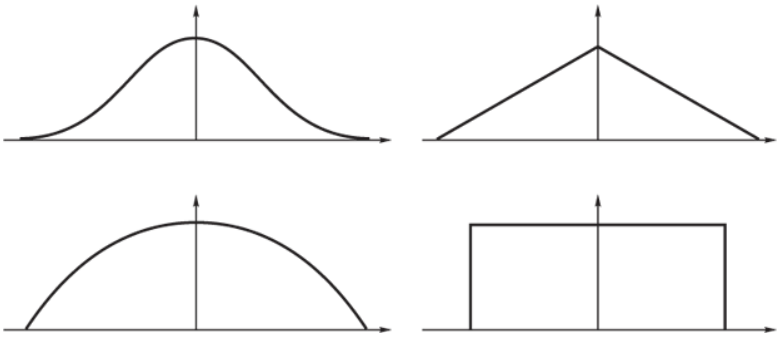


Рис. 5.

Пусть $L(y)$ и $R(y)$ — функции $(L-R)$-типа. Унимодальное нечеткое число A с **модой** a (т.е. $m_A(a)=1$) задается с помощью $L(y)$ и $R(y)$ следующим образом:

$$\mu_A(x)=\begin{cases} L\left(\frac{a-x}{\alpha}\right), & \text{если } x \leqslant a, \\ R\left(\frac{x-a}{\beta}\right), & \text{если } x \geqslant a. \end{cases}$$

где a — мода; $\alpha>0$, $\beta>0$ — левый и правый коэффициенты нечеткости.

Таким образом, при заданных $L(y)$ и $R(y)$ нечеткое число (унимодальное) задается тройкой $A=(a;\alpha,\beta)$.

Толерантное нечеткое число задается, соответственно, четверкой параметров $A=(a_1,a_2;\alpha,\beta)$, где a_1 и a_2 — границы толерантности, т.е. в промежутке $[a_1,a_2]$ значение функции принадлежности равно 1.

Примеры графиков функций принадлежности нечетких чисел $(L-R)$-типа приведены на рис. 6.

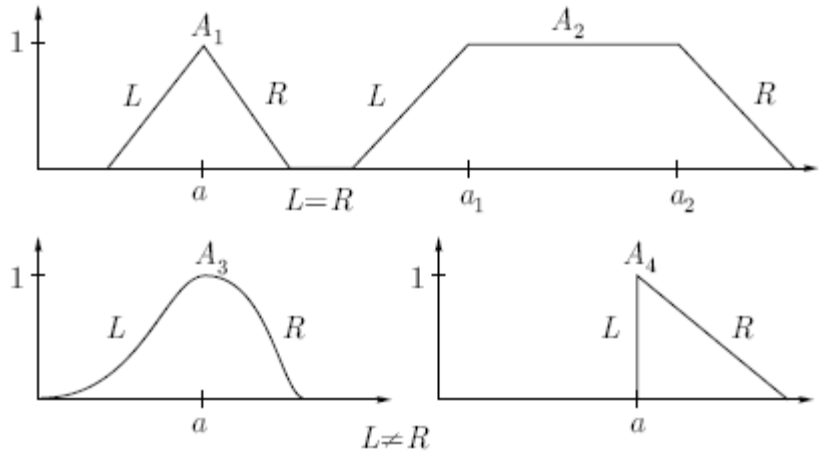


Рис. 6.

Толерантные нечеткие числа (L-R)-типа **называют** трапецоидными числами. Если мы оцениваем параметр качественно, например, говоря: "Это значение параметра является **средним** ", необходимо ввести уточняющее высказывание типа " **Среднее** значение — это **примерно** от a до b ", которое есть предмет экспертной оценки (нечеткой классификации), и тогда можно использовать для моделирования нечетких классификаций трапецоидные числа. На самом деле, это самый естественный способ неуверенной классификации.

Унимодальные нечеткие числа (L-R)-типа **называют** треугольными числами. Треугольные числа формализуют высказывания типа **"приблизительно равно** a **"**. Ясно, что $a \pm \delta \approx a$, причем по мере убывания δ до нуля степень уверенности в оценке растет до единицы.

Нечеткие треугольные числа — это наиболее часто используемый тип нечетких чисел, причем чаще всего — в качестве прогнозных значений параметра.

17.2. Нечеткие треугольные числа

На практике часто используется альтернативное определение нечеткого треугольного числа.

Определение. Треугольным нечетким числом A называется тройка $\langle a, b, c\rangle$ $(a \leqslant b \leqslant c)$ действительных чисел, через которые его функция принадлежности μ_S определяется следующим образом:

$$\mu_A(x) = \begin{cases} \frac{x-a}{b-a}, & \text{если } x \in [a, b], \\ \frac{x-c}{b-c}, & \text{если } x \in [b, c], \\ 0, & \text{в противном случае.} \end{cases}$$

Второе число b тройки $\langle a, b, c\rangle$ обычно называют **модой** или **четким значением** нечеткого треугольного числа. Числа a и c характеризуют степень размытости четкого числа.

Например, на рис. 7 изображено нечеткое треугольное число $A = \langle 1, 5, 7\rangle$, которое лингвистически можно проинтерпретировать как "около 5" или "приблизительно 5".

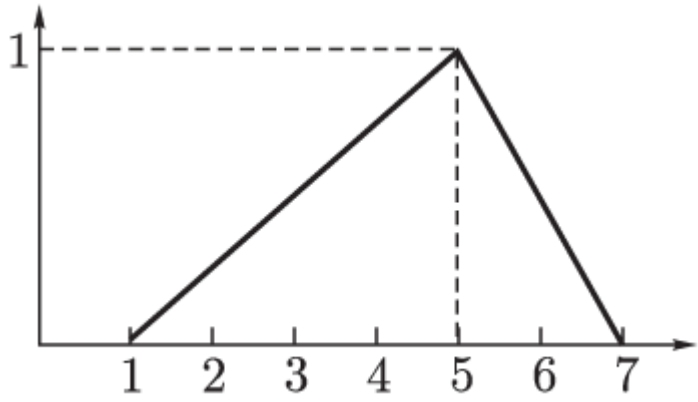


Рис. 7.

В общем случае при определении нечеткого треугольного числа не обязательно использовать линейные функции. Часто в различных приложениях используются две функции, из которых одна монотонно возрастает на интервале $[a,b]$, а другая монотонно убывает на интервале $[b,c]$. Однако Купер предложил так называемый landmark-based метод для систем управления, в соответствие с которым монотонности и дифференцируемости данных функций на соответствующих отрезках достаточно для того, чтобы система сходилась и имела единственное решение. Таким образом, без потери общности, каждое нечеткое треугольное число может быть представлено упорядоченной тройкой действительных чисел.

Если $A = \langle a_A, b_A, c_a \rangle$ и $B = \langle a_B, b_B, c_b \rangle$ — треугольные нечеткие числа, то, согласно принципу обобщения Заде, нечеткое треугольное число $C = A * B$ также является треугольным и характеризуется тройкой $\langle a_C, b_C, c_c \rangle$, где

$$a_C = \min\{a_A * a_B,\ a_A * c_B,\ c_A * a_B,\ c_A * c_B\},$$
$$c_C = \max\{a_A * a_B,\ a_A * c_B,\ c_A * a_B,\ c_A * c_B\},$$
$$b_C = b_A * b_B.$$

К сожалению, даже при ограничении нашего виденья нечетких чисел до понятия треугольных чисел, проблемы противоположного, обратного элементов и дистрибутивности остаются нерешенными.

Было предложено ввести некоторые ограничения на вычисление частных случаев вида $A * A$. Ограничения эти позволяют получить противоположный и обратный элементы. Однако проблема дистрибутивности таким способом не решается. Более того, ограничения кажутся довольно искусственными: чем, к примеру, можно объяснить различие в алгоритмах вычисления $A - A$ и $A - B$?

Есть еще один существенный недостаток такого подхода. Размытость произведения зависит не только от размытости сомножителей, но и от

того, какое место данные нечеткие числа занимают на числовой оси. Например, пусть

$A_1 = \langle 1, 2, 3\rangle,\ B_1 = \langle 2, 3, 4\rangle$ и $A_2 = \langle 99, 100, 101\rangle,\ B_2 = \langle 100, 101, 102\rangle.$

Тогда

$$A_1 \cdot B_1 = \langle 2, 6, 12\rangle$$

и

$$A_2 \cdot B_2 = \langle 9\,900, 10\,100, 10\,302\rangle .$$

Число $A_2 \cdot B_2$ получается гораздо более размытое, чем $A_1 \cdot B_1$.

Позднее было предложено другое определение нечеткого числа.

Определение. Нечетким числом u называется пара $(\underline{u}, \overline{u})$ функций $\underline{u}, \overline{u} : [0,1] \to R$, удовлетворяющих следующим условиям:

- $\underline{u}(r)$ — монотонно возрастающая непрерывная функция;
- $\overline{u}(r)$ — монотонно убывающая непрерывная функция;
- $\forall r\ \underline{u}(r) \leqslant \overline{u}(r).$

Это позволило ввести понятие меры и превратить множество нечетких чисел в топологическое пространство.

Далее предложена следующая модификация определения нечеткого числа.

Определение. Для любого нечеткого числа $u = (\underline{u}, \overline{u})$ число $u_0 = \frac{1}{2}(\underline{u}(1) + \overline{u}(1))$ называется локальным $u_* = u_0 - \underline{u}$ индексом числа u, две неубывающие непрерывные функции $u_* = u_0 - \underline{u}$ и $u^* = \overline{u} - u_0$ называются левым и правым индексами нечеткости, соответственно.

Согласно данному определению, каждое нечеткое число может быть представлено следующим образом: $(u_0,\ u_*, u^*)$.

Далее вводится понятие арифметических операций над нечеткими числами такого вида. Для любых нечетких чисел $u = (u_0,\ u_*, u^*)$ и $v = (v_0,\ v_*,\ v^*)$ они определяются следующим образом:

$$u * v = (u_0 * v_0,\ \ u_* \vee v_*,\ \ u^* \vee v^*).$$

Этот подход позволяет решить проблему дистрибутивности, так как размытость числа $u * v$ для всех четырех операций вычисляется при помощи единственного оператора, который дистрибутивен относительно самого себя (т.е. коммутативен, ассоциативен и идемпотентен).

Несмотря на это преимущество, проблемы противоположного и обратного элементов и при таком подходе остаются нерешенными.

17.3. Четкие арифметики нечетких треугольных чисел

Вернемся к рассмотрению нечетких треугольных чисел как частного случая нечетких чисел $(L-R)$-типа, т.е. имеющих вид $(a;\alpha,\beta)$.

Мы будем строить арифметику $\langle \Re, \tilde{+}, \tilde{\cdot} \rangle$, где $\tilde{+}, \tilde{\cdot}$ — операции сложения и умножения, определенные на нечетких треугольных числах. В построенной арифметике для каждого элемента будут существовать противоположные и обратные элементы. Поэтому нет никакой необходимости в определении операций вычитания и деления.

Определяя операции сложения и умножения, мы можем вычислять размытость суммы и произведения нечетких треугольных чисел либо по одному алгоритму, либо по разным. Сперва рассмотрим случай, когда размытость суммы и произведения нечетких треугольных чисел вычисляется по одному алгоритму. Определим операции сложения и умножения нечетких треугольных чисел следующим образом:

$$(a_1;\ \alpha_1, \beta_1)\tilde{*}(a_2;\ \alpha_2, \beta_2) = (a_1 * a_2;\ \alpha_1 O \alpha_2, \beta_1 O \beta_2).$$

где $*$ — либо сложение, либо умножение, O — некоторая бинарная операция, определенная на множестве неотрицательных действительных чисел.

Опишем, какими свойствами должна обладать операция O для того, чтобы сложение и умножение были коммутативны, ассоциативны, дистрибутивны, а также существовали противоположные и обратные элементы.

Очевидно, что для того, чтобы операция $\tilde{*}$ была коммутативной и ассоциативной, O также должна быть коммутативной и ассоциативной, т.е. удовлетворять следующим условиям:

$$\begin{aligned} &\alpha\, O\beta = \beta\, O\alpha, \\ &(\alpha\, O\beta)\, O\gamma = \alpha\, O\,(\beta\, O\gamma). \end{aligned} \qquad (39)$$

Пусть $0 = \langle a_0; \alpha_0, \beta_0 \rangle$ — нечеткий ноль. Очевидно, что его мода a_0 равна нулю, а коэффициенты размытости α_0, и β_0 фиксированные значения. Тогда для любого $\alpha \in R^+$ имеем

$$\alpha\, O\alpha_0 = \alpha_0\, O\alpha = \alpha\, O\beta_0 = \beta_0\, O\alpha.$$

Для того, чтобы каждое нечеткое число обладало противоположным, необходимо, чтобы для любого $\alpha \in R^+$ существовали $\alpha',\ \beta' \in R^+$, такие, что

$$\alpha\, O\alpha' = \alpha'\, O\alpha = \alpha_0 \qquad \text{и} \qquad \alpha\, O\beta' = \beta'\, O\alpha = \beta_0.$$

Аналогично, если $1 = \langle a_1; \alpha_1, \beta_1 \rangle$ — нечеткая единица, то для любого $\alpha \in R^+$ имеем

$$\alpha\, O\alpha_1 = \alpha_1\, O\alpha = \alpha\, O\beta_1 = \beta_1\, O\alpha.$$

И для любого $\alpha \in R^+$ существуют $\alpha'',\ \beta'' \in \mathrm{R}^+$, такие, что

$$\alpha\ \mathrm{O}\alpha'' = \alpha''\ \mathrm{O}\alpha = \alpha_1 \qquad \text{и} \qquad \alpha\ \mathrm{O}\beta'' = \beta''\ \mathrm{O}\alpha = \beta_1.$$

Легко заметить, что алгебраическая система $\langle R^+, O\rangle$ образует абелеву группу. Следовательно, $\alpha_0 = \beta_0 = \alpha_1 = \beta_1 = e$ и для любого $\alpha \in R^+$ имеем $\alpha' = \beta' = \alpha'' = \beta'' = \alpha^{-1}$.

Для того, чтобы операции $\tilde{+},\ \tilde{\cdot}$ удовлетворяли условию дистрибутивности, необходимо и достаточно, чтобы для любых $\alpha, \beta, \gamma \in R^+$ операция O удовлетворяла следующему условию:

$$(\alpha\ \mathrm{O}\beta)\ \mathrm{O}\ (\alpha\ \mathrm{O}\gamma) = \alpha\ \mathrm{O}\ (\beta\ \mathrm{O}\gamma). \qquad (40)$$

Если O коммутативна и ассоциативна, то получим

$$(\alpha\ \mathrm{O}\beta)\ \mathrm{O}\ (\alpha\ \mathrm{O}\gamma) = (\alpha\ \mathrm{O}\alpha)\ \mathrm{O}\ (\beta\ \mathrm{O}\gamma).$$

Следовательно, для того, чтобы условие (40) выполнялось, достаточно, чтобы O была коммутативна, ассоциативна и идемпотентна, т.е. удовлетворяла условиям (39) и для любого $\alpha \in R^+$

$$\alpha\ \mathrm{O}\alpha = \alpha.$$

Нетрудно показать, что никакая группа не обладает свойством идемпотентности.

Вывод

Невозможно построить арифметику нечетких треугольных чисел, изоморфную арифметике действительных (четких) чисел, если размытость суммы и произведения нечетких треугольных чисел вычисляется по одному алгоритму.

Теперь рассмотрим случай, когда размытость суммы и произведения определяются по разным алгоритмам. Пусть

$$(a_1;\ \alpha_1, \beta_1)\tilde{+}(a_2;\ \alpha_2, \beta_2) = (a_1 + a_2;\ \alpha_1 \oplus \alpha_2, \beta_1 \oplus \beta_2),$$
$$(a_1;\ \alpha_1, \beta_1)\tilde{\cdot}(a_2;\ \alpha_2, \beta_2) = (a_1 \cdot a_2;\ \alpha_1 \otimes \alpha_2, \beta_1 \otimes \beta_2).$$

Очевидно, что если алгебраическая система $\langle R^+, \oplus, \otimes \rangle$ удовлетворяет свойствам коммутативности, ассоциативности, дистрибутивности, существования нейтрального и единичного элементов, существования противоположного и обратного элементов, то она образует ассоциативное, коммутативное кольцо с единицей и с делением (т.е. почти поле).

Пример. Рассмотрим поле $\langle R, +, \cdot \rangle$ действительных чисел. Функция $f(x) = e^x$ является взаимно однозначным отображением R на R^+. Определим операции $\oplus$ и $\otimes$ таким образом, чтобы f являлось изоморфизмом соответствующих систем. Очевидно, что должны выполняться следующие равенства:

$$\alpha \oplus \beta = \mathrm{f}(\mathrm{f}^{-1}(\alpha) + \mathrm{f}^{-1}(\beta)),$$
$$\alpha \otimes \beta = \mathrm{f}(\mathrm{f}^{-1}(\alpha) \cdot \mathrm{f}^{-1}(\beta)).$$

Таким образом, мы получим

$$\alpha \oplus \beta = e^{\ln \alpha + \ln \beta} = \alpha\beta,$$
$$\alpha \otimes \beta = e^{\ln \alpha \ln \beta}.$$

Нетрудно убедиться, что при таком задании операций размытости арифметика $\Re$ будет коммутативной, ассоциативной и дистрибутивной. Роль нулевого элемента будет выполнять нечеткое треугольное число $0 = \langle 0; 1, 1 \rangle$; роль единичного элемента — нечеткое треугольное число $1 = \langle 1; e, e \rangle$. Для произвольного

нечеткого треугольного числа $A = \langle a; \alpha, \beta \rangle$ противоположным числом будет $-\mathrm{A} = \langle -\mathrm{a};\ \frac{1}{\alpha}, \frac{1}{\beta} \rangle$ и обратным элементом будет $A^{-1} =< \frac{1}{a};\ e^{\frac{1}{\ln \alpha}}, e^{\frac{1}{\ln \beta}} >$.

Недостатком этой арифметики является то, что в нее не входят четкие и "получеткие" числа, т.е. числа, у которых хотя бы один из коэффициентов размытости равен нулю. Но этого легко избежать, если доопределить ее, например, следующим образом:

$$\alpha = 0 \& \beta = 0 \quad \Rightarrow \quad \alpha \oplus \beta = \alpha \otimes \beta = 0.$$

Заметим, что, варьируя мощность изоморфного поля, мы тем самым варьируем и мощность множества коэффициентов размытости, используемых в данной арифметике.

17.4. Размытые арифметики нечетких треугольных чисел

В предыдущем параграфе мы доказали, что возможно построить арифметику нечетких треугольных чисел, аналогичную арифметике четких чисел. Однако, на наш взгляд, каждая такая арифметика будет обладать одним существенным недостатком.

Рассмотрим арифметику $\Re$, описанную в примере. Пусть $N_i = \langle 0; \alpha_i, \beta_i \rangle$, где $\alpha_i \vee \beta_i \neq 1$. Для произвольного числа $A = \langle a; \alpha, \beta \rangle$ выполняется

$$A \tilde{+} N_i = \langle a;\ \alpha\alpha_i, \beta\beta_i \rangle.$$

Если A имеет некоторое лингвистическое значение (например, "приблизительно a"), то нечеткое число $A \tilde{+} N_i$ является некоторым модификатором числа A (например, "более или менее приблизительно a"). Таким образом, нечеткое число N_i является

"приблизительно нулевым элементом". Более того, при $\alpha \to 1$ и $\beta \to 1$ эта "приблизительность" возрастает. Однако при формальном описании арифметики $\Re$ это свойство нигде не отражается.

Рассмотрим подход к арифметике нечетких чисел, который успешно формализует описанное выше свойство без потери свойств, аналогичных свойствам четкой арифметики. При этом подходе нечеткость рассуждений увеличивается, но это не всегда является минусом.

Основная идея данного подхода заключается в том, что понятие нечеткости накладывается на арифметические операции. То есть результатом произведения (или сложения) двух нечетких треугольных чисел является не одно конкретное нечеткое треугольное число, а нечеткое множество, определенное на множестве нечетких треугольных чисел. Такие операции названы **размытыми операциями**. Следовательно, и арифметику нечетких чисел с размытыми операциями мы будем называть **размытой** (сокращенно **РА-НТЧ**). Рассмотренные выше арифметики мы будем называть **четкими** (сокращенно **ЧА-НТЧ**).

Пусть нам задана некоторая **ЧА-НТЧ** $\tilde{\Re} = \langle \Re, \tilde{+}, \tilde{\cdot} \rangle$. На базе этой арифметики будем строить **РА-НТЧ** $\tilde{\Re} = \langle \Re, \tilde{+}, \tilde{\cdot} \rangle$.

Пусть нам даны нечеткие числа $A = \langle a; \alpha_A, \beta_A \rangle$ и $B = \langle b; \alpha_B, \beta_B \rangle$. Множество $\tilde{A} * B$ является нечетким подмножеством множества $\Re$ с функцией приоритета $\mu_{\tilde{A}*B}$, которая для любого нечеткого треугольного числа $C = \langle c; \alpha_C, \beta_C \rangle$ удовлетворяет условию

$$\mu_{\tilde{A}*B}(\mathrm{C}) = \begin{cases} 0, & \text{если } \mathrm{c} \neq \mathrm{a} * \mathrm{b}, \\ \frac{1}{\max\{\alpha^*, \beta^*\}+1}, & \text{в противном случае.} \end{cases} \quad (41)$$

где $\alpha^* = |\alpha_C - \alpha_A * \alpha_B|, \quad \beta^* = |\beta_C - \beta_A * \beta_B|$.

Введем новое обозначение. Пусть $\mu_{\tilde{A*B}}(C) = \gamma$. Тогда, если $\gamma > 0$, то будем записывать $\tilde{A} * B =_{\gamma} C$. Если же $\gamma = 0$, то будем записывать $\tilde{A} * B \neq C$. Число

$$C^k = A\tilde{*}B =< a * b;\ \alpha_A * \alpha_B, \beta_A * \beta_b >$$

назовем **каноническим представителем** произведения $\tilde{A} * B$. Очевидно, что

$$\tilde{A} * B =_1 C \quad \Leftrightarrow \quad C = C^k.$$

Для всех остальных нечетких чисел, чья мода равна $a * b$, значение функции принадлежности уменьшается с увеличением "удаленности" данного числа от канонического представителя.

Независимо от задания арифметики $\tilde{\Re}$, размытая арифметика $\tilde{\Re}$ будет обладать слабым свойством коммутативности, т.е. для любых $A, B \in \Re$ будет выполнено следующее равенство множеств

$$\tilde{A} * B = \tilde{B} * A.$$

На самом деле, если найдется такое число $\gamma_1 > 0$, что $\tilde{A} * B =_{\gamma_1} C$, то, согласно (41), имеем $c = a * b$. Так как на множестве действительных чисел и сложение, и умножение коммутативны, то $c = b * a$, и, следовательно, найдется такое число $\gamma_2 > 0$, что $\tilde{B} * A =_{\gamma_2} C$. Заметим, что в общем случае $\gamma_1 \neq \gamma_2$. Именно поэтому свойство названо "слабым".

Если **ЧА-НТЧ** $\tilde{\Re}$ обладает свойством коммутативности, то **РА-НТЧ** $\tilde{\Re}$ будет обладать сильным свойством коммутативности, т.е. для любых $A,\ B,\ C \in \Re$ выполняется

$$\tilde{A} * B =_{\gamma} C \quad \Leftrightarrow \quad \tilde{B} * A =_{\gamma} C.$$

Прежде чем говорить об ассоциативности и дистрибутивности, необходимо рассмотреть алгоритм вычисления арифметических выражений, содержащих более двух нечетких треугольных чисел.

Пусть $F(A_1, A_3, \ldots, A_n)$ — некоторое арифметическое выражение, содержащие нечеткие числа $A_1, A_2, \ldots, A_n$. Сперва найдем канонический представитель $C^k =< c; \alpha^k, \beta^k >$ этого выражения, т.е. значение выражения в **ЧА-НТЧ** $\tilde{\Re}$. Тогда для любого $C \in \Re$ имеем

$$\mu_F(C) = \begin{cases} 0, & \text{если } c \neq F(a_1, ..., a_n), \\ \frac{1}{\max\{\alpha^*, \beta^*\}+1}, & \text{в противном случае.} \end{cases}$$

где $\alpha^* = |\alpha_C - \alpha^k|, \quad \beta^* = |\beta_C - \beta^k|.$

Нетрудно убедиться, что полученная арифметика будет обладать свойствами слабой ассоциативности и слабой дистрибутивности, т.е. для любых $A, B, C \in \Re$ выполнены следующие равенства множеств:

$$\tilde{A} * (\tilde{B} * C) = (\tilde{A} * B)\tilde{} * C,$$
$$\tilde{A} \cdot (\tilde{B} + C) = (\tilde{A} + B)\tilde{} \cdot (\tilde{A} + C).$$

Необходимым и достаточным условием для выполнения сильных свойств ассоциативности и дистрибутивности является условие выполнения этих свойств в арифметике $\tilde{\Re}$.

В построенной арифметике $\tilde{\Re}$ следующим образом определим понятия нулевого и единичного элементов. Элемент $N \in \Re$ называется **нулевым**, если для любого $A \in \Re$ найдутся такие числа $\gamma_1, \gamma_2 \in (0, 1]$, что

$$\tilde{A} + N = {}_{\gamma_1}A \quad \text{и} \quad \tilde{N} + A = {}_{\gamma_2}A.$$

И, аналогично, элемент $E \in \Re$ называется **единичным**, если для любого $A \in \Re$ найдутся такие числа $\gamma_1, \gamma_2 \in (0,1]$, что

$$\tilde{A} \cdot E = {}_{\gamma_1}A \quad \text{и} \quad \tilde{E} \cdot A = {}_{\gamma_2}A.$$

Нетрудно убедиться, что все нечеткие треугольные числа, мода которых равна нулю, являются нулевыми, и нечеткие треугольные числа, мода которых равна единице, являются единичными.

Вернемся теперь к рассмотрению проблемы, описанной в начале данного параграфа. Пусть число $N_0 =< 0; \alpha_0, \beta_0 >$ — нулевой элемент в арифметике $\tilde{\Re}$. Тогда для любого $A \in \Re$ имеем $\tilde{A} + N_0 = {}_1A$ и $N_0 \tilde{+} A = {}_1A$.

Если $N_i =< 0; \alpha_i, \beta_i > (\alpha_i \neq \alpha_0$, или $\beta_i \neq \beta_0)$. Тогда найдутся такие числа $\gamma_1, \gamma_2 \in (0,1]$, что $\tilde{A} + N_i = {}_{\gamma_1}A$ и $N_i \tilde{+} A = {}_{\gamma_2}A$. Более того,

$$\alpha_i \to \alpha_0 \quad \Rightarrow \quad \gamma_1 \to 1,$$
$$\beta_i \to \beta_0 \quad \Rightarrow \quad \gamma_2 \to 1.$$

Проблема противоположного и обратного элементов решается по аналогии с проблемой коммутативности; в слабом варианте проблема решается автоматически, а усиленный вариант зависит от того, существуют ли противоположный и обратный элементы в арифметике $\tilde{\Re}$.

18. Развитие понятия о «числе»

В разделе собраны научно-методические работы, опубликованные С. Л. Блюминым и направленные на популяризацию некоторых представлений о многообразии алгебраических структур, элементы которых часто именуются «числами», возникающих и применяемых при формализации реальных явлений, объектов и процессов.

Представленный материал позволяет проследить «развитие понятия о числе» от исходных для всей фундаментальной и прикладной математики натуральных чисел до использующихся в современной математике и ее приложениях нечетких и сверхнатуральных чисел.

Данная тема вполне обоснованно может рассматриваться как дальнейшее «развитие понятия о «числе»» в свете некоторых современных представлений. Действительно, возвращаясь, с одной стороны, к классическому, с исторической и методической точек зрения, процессу расширения множеств (не числовых полей, в связи с чем здесь и далее часто используются кавычки) натуральных и целых «чисел» до множеств (истинных числовых полей) рациональных, действительных и комплексных чисел, эта тема, с другой стороны, трактует указанный процесс расширения алгебраических структур таким образом, что в нее укладываются как давно известные (но отличные от вышеуказанных) множества двойных, дуальных, гиперкомплексных и других «чисел», так и возникшие сравнительно недавно в современной фундаментальной и особенно прикладной математике, -в первую очередь в связи с проблемами математического моделирования, принятия решений и вообще искусственного интеллекта, теории и практики социально-экономических и вообще управляемых систем, - идемпотентные, нечеткие, сверхнатуральные, решеточные и другие «числа»; все они образуют алгебраические структуры, отличные от числовых полей.

Достоинства представленного материала заключаются в том, что, будучи, в соответствии с самим духом темы, вполне элементарным, он доступен восприятию при первом знакомстве; будучи, с точки зрения «традиционной» математики, вполне нетрадиционным, он позволяет, в сравнительном аспекте, глубже понять, казалось бы, хорошо известные факты, обратить внимание на их, подчас неожиданные, аспекты; будучи, с научной точки зрения, новым, он ориентирует в современных путях развития аппарата прикладной математики и стимулирует его использование в актуальных научных исследованиях.

Разнообразные «числовые» системы столь интенсивно «плодятся» в современных исследованиях, что специалисты периодически обращаются к истокам происхождения самого понятия о числе,

стремясь критически осмыслить как вновь появляющиеся, так и освященные веками «числа», их адекватность математическому моделированию реальных явлений, объектов и процессов.

Материал, представленный в разделе, позволяет проследить «развитие понятия о числе» от исходных для всей фундаментальной и прикладной математики натуральных чисел до использующихся в современной математике и ее приложениях нечетких и сверхнатуральных чисел.

18.1. Некоторые научно-методические аспекты

Развитие понятия о числе (как элементе *числового поля,* удовлетворяющего известному набору аксиом) является важным методическим аспектом преподавания математики (фактически отражающим и соответствующий исторический процесс): **последовательно изучают, погружая, вкладывая предыдущую алгебраическую структуру в последующую (расширяя предыдущую до последующей), одномерные *полукольцо* N натуральных «чисел», *кольцо* Z целых «чисел», *поле* Q рациональных чисел (чисто алгебраическая часть цепочки), *поле* R действительных чисел (уже с привлечением анализа; эта часть цепочки стандартно изучается в средней школе), двумерное *поле* C комплексных чисел (переход от R к C также носит чисто алгебраический характер; изучается в математических классах средней школы и стандартно в высшей школе).** Аксиомы числового поля начинают полностью выполняться в **Q, R, C** (с этим связано использование кавычек) и нарушаются в ряде известных продолжений и ответвлений цепочки. Так, продолжая ее с сохранением аксиомы *обратимости* элементов (кроме нулевого), переходят к гиперкомплексным «числам» (их изучение возможно в математической высшей школе), а именно, **четырехмерному *телу* H кватернионов**, где нарушается аксиома *коммутативности,* и **восьмимерной *алгебре Кэли* Ca «чисел» Кэли или октав**, где нарушается и аксиома *ассоциативности.* В соответствии с известной теоремой Фробениуса продолжение цепочки с сохранением последних аксиом невозможно без нарушения аксиомы обратимости. С другой стороны, уже в низших размерностях известны ответвления цепочки с нарушением аксиомы обратимости: например, двумерные *алгебры* $\mathbf{K}_{pq}$ квазикомплексных «чисел», характерными представителями которых (в отличие от поля **C**) являются **алгебра U двойных «чисел» и алгебра V дуальных «чисел»**; некоторые **трехмерные алгебры**, в частности, алгебра Tr триплексных «чисел»; некоторые **четырехмерные алгебры**, в

частности (в отличие от тела **H**), алгебра Qu **квадриплексных «чисел» (бикомплексных «чисел», тесаринов**; существуют и другие примеры).

Нарушение свойства обратимости элементов мотивирует изучение более общего свойства их *обобщенной обратимости* или *регулярности* (по Дж. фон Нейману). **Алгебра U регулярна**: каждый необратимый ее элемент обобщенно обратим. В сравнении с классической ситуацией регулярная алгебра по отношению к свойству обобщенной обратимости аналогична полю по отношению к свойству (обычной) обратимости. **Алгебра же V нерегулярна**: каждый необратимый ее элемент, кроме нулевого, не является и обобщенно обратимым. Сравнение с классической ситуацией в этом случае могло бы привести к вопросу о возможности погружения алгебры **V** в такую алгебру, в которой каждый необратимый элемент из V был бы обратим; однако более корректна постановка вопроса о возможности погружения алгебры **V** в такую алгебру **W**, в которой каждый необратимый элемент из **V** обобщенно обратим. Этот вопрос решен в ряде работ, где построенная алгебра **W** названа ***алгеброй внедуальных «чисел».*** Из общеалгебраических соображений классическое «развитие понятия о числе» соответствует процедуре *симметризации* коммутативных ассоциативных внутренних законов композиции; в свете этого построение алгебры **W** может быть охарактеризовано как *обобщенная симметризация.* Алгебра **W** независимо построена из несколько иных соображений и использована в связи с проблематикой современной «супер»-физики. Приведем некоторые детали.

Алгебра V определяется аналогично полю **C** комплексных чисел: она состоит из элементов $v=a+be$, где a,b - действительные числа, e - «дуальная» единица, удовлетворяющая соотношению $e^2=0$. Операции сложения элементов, их умножения на действительные числа и между собой, сопряжения и взятия модуля выполняются по правилам:

Обратный

$$v_1+v_2=(a_1+b_1e)+(a_2+b_2e)=(a_1+a_2)+(b_1+b_2)e, \qquad cv=c(a+be)=ca+cbe,$$
$$v_1v_2=(a_1+b_1e)(a_2+b_2e)=a_1a_2+(a_1b_2+a_2b_1)e, \; v^{\cdot}=a-be, \; /v/^2=vv^{\cdot}=a^2 .$$

элемент v^{-1} ищется из условия $vv^{-1}=1$, приводящего к системе линейных алгебраических уравнений с определителем $D=a^2$, существует при условии $a=/=0$ и вычисляется по той же формуле, что и в случае комплексных чисел: $v^{-1}=\overline{v}\,/\,/v/^2$. В случае же $a=0$ элемент необратим; его обобщенный обратный $\tilde{v}$ ищется из условия $v\tilde{v}v=v$ и существует только для $v=0$; это и означает, что алгебра **V** нерегулярна.

Алгебра **W**, в которой существуют обобщенные обратные ко всем элементам алгебры **V**, строится следующим образом. Она состоит из элементов

$$w=a+be+cf+dg+kh,$$

где *a,b,c,d,k* - действительные числа, *e, f* - дуальные единицы, удовлетворяющие соотношениям $e^2=f=0$ и связанные между собой условиями регулярности *efe=e, fef=f,* а *g, h* — идемпотентные единицы, удовлетворяющие соотношениям $g^2=g$, $h^2=h$ и связанные с *e, f* соотношениями *g=ef, h=fe,* вследствие чего непосредственно выполняются соотношения ортогональности *eg= gf=he=fh=gh=hg=0,* а благодаря условиям регулярности - соотношения *eh=ge=e, fg=hf=f.* Перечисленные соотношения полностью определяют таблицу умножения базисных единиц алгебры **W**, в соответствии с которой выполняются операции над произвольными элементами. Обратный элемент w^{-1} существует при условии $D=aN^2 =/=0$ и вычисляется по формуле

$$w^{-1} =N[N-abe-acf+(M-ad)g+(M-ak)h]/D,$$

где *N=(a+d)(a+k)-bc, M=bc-dk.*

В случае же *D=0* элемент *w* необратим, но обобщенно обратим; это возможно либо если *a=0,* либо если *N=0,* либо если одновременно *a=N=0,* то есть если *M=0;* в последнем случае, при условии *b=/=0,* множество обобщенных обратных вычисляется по формуле

$$w^- =x+ye+b^{-1}[1-(d+k)x-cy-ds-kt]f+sg+th,$$

где *x,y,s,t* - любые действительные числа. В частности, для ненулевых необратимых элементов *v=be* из **V**

$$v^- =(be)^- =x+ye+b^{-1}f+sg+th,$$

где *x,y,s,t* - любые действительные числа, чем и достигнута цель обобщенной симметризации. Отметим, что в ряде работ, преследуя иные цели, приводят выражение для w^{-1} (в сопоставлении с обращением в антикоммутативных, но не регулярных *алгебрах Грассмана* **G**, частным случаем которых является **V**), но не указывают в явном виде выражения для $\overline{w}, \overline{v}$.

В ряде работ указано представление алгебры **W** как *свободного произведения* двух алгебр **V** по модулю условия регулярности: $\mathbf{W} = \mathbf{V_1} \times \mathbf{V_2} /^{\sim reg}$. Вопрос об использовании свободного произведения алгебр как основы для обобщенной симметризации не обсуждается.

18.2. Классические аналогии и приложения

С точки зрения современных представлений общей и прикладной алгебры известное каждому школьнику развитие понятия о числе представляет собой последовательное расширение *(симметризацию* по принятой терминологии):

1.1) полукольца **N** натуральных «чисел» до кольца **Z** целых «чисел» или

1.2) полукольца **N** натуральных «чисел» до полуполя Q_+ положительных рациональных «чисел»;

2.1) кольца **Z** целых «чисел» до поля **Q** рациональных чисел или

2.2) полуполя $\mathbf{Q}_+$ положительных рациональных «чисел» до поля **Q** рациональных чисел.

Кавычки использованы для того, чтобы подчеркнуть, что, вопреки «обычным» названиям, в алгебраических структурах **N, Z,** $\mathbf{Q}_+$ выполняются не все аксиомы числового поля: так, в **N** не существуют противоположные и обратные ко всем элементам, в **Z** не существуют обратные, а в $\mathbf{Q}_+$ -противоположные ко всем элементам.

Завершает развитие понятия о числе расширение поля **Q** рациональных чисел до поля **R** действительных чисел, а его - до поля $\mathbf{C} = \{c = a + bi, a, b \in \mathbf{R}, i^2 = -1\}$ комплексных чисел.

С другой стороны, в алгебре известны альтернативные последнему расширения:

3.1) поля **R** действительных чисел до кольца $\mathbf{U} = \{u = a + b\,e,\ \ a, b \in \mathbf{R}, e^2 = 1\}$ двойных «чисел» и

3.2) поля **R** действительных чисел до кольца $\mathbf{V} = \{v = a + b\,f,\ \ a, b \in \mathbf{R}, f^2 = 0\}$ дуальных «чисел»;

в них не для каждого ненулевого элемента существует обратный.

Ниже проведен полезный с методической точки зрения сравнительный анализ указанных расширений, указаны сходные и отличительные черты в их построении. Затем приведен, также в сравнительном аспекте, менее традиционный пример, связанный с некоторыми приложениями.

Для удобства изложения напомним определения некоторых основных алгебраических структур.

Полугруппа есть множество с ассоциативной операцией.

Коммутативное полукольцо с нулем и единицей есть

- коммутативная аддитивная полугруппа с 0 относительно сложения +,
- коммутативная мультипликативная полугруппа с 1 относительно умножения *

- умножение дистрибутивно относительно сложения.

Коммутативное кольцо с единицей есть коммутативное полукольцо с нулем и единицей, в котором коммутативная аддитивная полугруппа с 0 есть коммутативная аддитивная группа с 0.

Полуполе есть коммутативное полукольцо с нулем и единицей, в котором коммутативная мультипликативная полугруппа с 1 есть коммутативная мультипликативная группа с 1 (исключая 0).

Поле есть коммутативное кольцо с единицей, в котором коммутативная мультипликативная полугруппа с 1 есть коммутативная мультипликативная группа с 1 (исключая 0) или

Поле есть полуполе, в котором коммутативная аддитивная полугруппа с 0 есть коммутативная аддитивная группа с 0.

Описанное расширение алгебраических структур удобно представить в виде схемы:

коммутативное полукольцо с нулем и единицей

/ \

коммутативное кольцо с единицей полуполе

\ /

поле

Стандартным подходом к расширению алгебраических структур служат методы пар.

Метод пар I типа служит для расширения полукольца **N** натуральных «чисел» до кольца **Z** целых «чисел»: рассматривается множество пар *(k,l),(m,n)* натуральных «чисел» с операциями

$$(k,l) + (m,n) = (k + m,\ l + n), \quad (k,l)\,(m,n) = (k\,m + l\,n,\ k\,n + l\,m); \qquad (1)$$

с парой *(k,l)* отождествляются все пары *(m,n),* удовлетворяющие соотношению $k + n = l + m,$ то есть все пары вида $(k + s,l + s)$, где натуральное «число» *s* произвольно, и трактуются как целое «число» $k - l;$ все пары *(s,s)* трактуются как целое «число» 0; пары $(l + s,k + s)$ трактуются как противоположное $l-k$ к целому «числу», представляемому парами $(k + s,l + s);$ тем самым построено кольцо **Z**; аксиомы кольца проверяются непосредственно.

Обращает на себя внимание аналогия с методом пар *I* типа того способа, который служит для расширения поля *R* действительных чисел до кольца $U = \{u = a + b\,e,\ \ a, b \in R, e^2 = 1\}$, двойных «чисел»: трактуя пару *(a,b)* как двойное «число» $a + be,$ можно непосредственно убедиться в том, что операции выполняются по формулам (1). Это допускает естественное объяснение: целое «число» $k - l$ можно представить как $k + l(-1),$ где $(-1)^2=1,$ подобно тому, как $e^2=1.$

Метод пар II типа служит для расширения полукольца **N** натуральных «чисел» до полуполя $\mathbf{Q}_+$ положительных рациональных «чисел»: рассматривается множество пар *(k,l),(m,n)* натуральных «чисел» с операциями

$$(k,l)\,(m,n) = (k\ \ m,\ l\ \ n),\quad (k,l) + (m,n) = (k\,n + l\,m,\ \ l\,n); \tag{2}$$

с парой *(k,l)* отождествляются все пары *(k s, l s)* , где натуральное «число» *s* произвольно, и трактуются как положительное рациональное «число» (положительная дробь) *k / l ;* все пары *(s,s)* трактуются как положительное рациональное «число» 1; пары *(l s, k s)* трактуются как обратное *l/k* к положительному рациональному «числу», представляемому парами *(k s, l s);* тем самым построено полуполе $\mathbf{Q}_+$; аксиомы полуполя проверяются непосредственно.

Обращает на себя внимание некоторая аналогия с методом пар *II* типа того способа, который служит для расширения поля **R** действительных чисел до кольца $V = \{v = a + b\,f,\quad a,\ b \in R,\ f^2 = 0\}$ дуальных «чисел», однако эта аналогия является гораздо менее прямой, чем указанная ранее: для сопоставления с формулами (2) удобнее пару *(a,b)* трактовать как дуальное «число» $a\ f + b$; тогда сложение дуальных «чисел» выполняется подобно умножению дробей, то есть поэлементно, в то время как умножение дуальных «чисел» выполняется в точности так же, как сложение дробей.

Наряду с известными «гауссовыми числами» - рациональными комплексными числами или целыми комплексными «числами» - рассмотренные методы расширения алгебраических структур могут быть применены для построения рациональных, целых и даже натуральных двойных и дуальных «чисел».

Результаты проведенного сравнительного анализа могут найти применения при изучении алгебры и теории чисел, геометрии и физики, а также в некоторых приложениях математики, рассмотренных ниже.

Полуполе $\mathbf{R}_{max}$, известное также как алгебра (max, +), является одной из модельных алгебраических структур нового раздела математики - **идемпотентной математики**, в основе которой лежат полные или частичные замена и/или переименование обычных арифметических операций на новые основные операции, **включая идемпотентные операции, такие как максимум и минимум**. Такой подход приводит к интересным нетривиальным, нетрадиционным и часто неожиданным, результатам в самой математике и ее приложениях как в физике, так и в проблемах искусственного интеллекта, математического моделирования систем, их оптимизации и управления ими.

Полуполе $\mathbf{R}_{max}$ образовано из поля **R** действительных чисел присоединением к нему символа $\Theta = -\infty$, с обычными отношениями равенства и порядка и операциями «сложения» $a \oplus b = a \vee b = max(a,b)$ (выбор большего из двух элементов в смысле обычного отношения порядка) и «умножения» $a \otimes b = a + b$ (обычное сложение элементов). Непосредственно проверяется, что обе операции ассоциативны, коммутативны и имеют нейтральные элементы : «нулем» для «сложения» служит символ Θ, так как $a \oplus \Theta = max(a,-\infty) = a$, «единицей» для «умножения» служит обычный *0*, так как $a \otimes 0 = a + 0 = a$; символ Θ обладает свойством поглощения относительно «умножения», $a \otimes \Theta = a + (-\infty) = \Theta$. Операции связаны обычной дистрибутивностью, $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

Принципиальными отличиями полуполя $\mathbf{R}_{max}$ от поля **R** действительных чисел является идемпотентность операции сложения, а также то, что каждый элемент a из $\mathbf{R}_{max}$ имеет «обратный» $a^{(-1)}$ относительно «умножения» (им служит обычный противоположный $-a$, $a \otimes a^{(-1)} = a + (-a) = 0$), но ни один из элементов, кроме символа Θ, не имеет «противоположного» относительно «сложения» (ни для каких двух элементов $a,b \neq \Theta$ не может выполняться соотношение $a \oplus b = max(a,b) = \Theta = -\infty$, и только для Θ верно $\Theta \oplus \Theta = \Theta$). В этом проявляется некоторая аналогия с полукольцом **N** натуральных «чисел», где ни один из элементов не имеет противоположного в обычном смысле. Эта аналогия подсказывает попытку расширить $\mathbf{R}_{max}$ (подобно расширению полукольца **N** до кольца **Z** целых «чисел») так, чтобы в построенном расширении появились «противоположные» к элементам из $\mathbf{R}_{max}$. Оказывается, что если даже в этом расширении сохраняются «обратные», уже имеющиеся в $\mathbf{R}_{max}$, оно, тем не менее, не будет полным аналогом числового поля. Полученная алгебраическая структура названа *симметризацией* $\mathbf{S}_{max}$ полуполя $\mathbf{R}_{max}$. Рассмотрим подробнее ее построение.

Метод пар I типа в построении симметризации $\mathbf{S}_{max}$ полуполя $\mathbf{R}_{max}$ применяется следующим образом: рассматривается множество $\mathbf{R}_{max} \times \mathbf{R}_{max}$ пар $x=(x', x'')$, $y=(y', y'')$ элементов из $\mathbf{R}_{max}$ с операциями

$$(x', x'') \oplus (y', y'') = (x' \oplus y', x'' \oplus y''),$$

$$(x', x'') \otimes (y', y'') = (x' \otimes y' \oplus x'' \otimes y'', x' \otimes y'' \oplus x'' \otimes y'),$$

причем роль *нуля* играет пара (Θ, Θ), роль *единицы* - пара *(0, Θ), противоположная* пара определяется как $\theta\, x = (x'', x')$, *абсолютная величина* пары – как $/x/ = x' \oplus x''$, *оператор баланса* – как $x^{\bullet} = x\, \theta\, x = (/x/, /x/)$.

В отличие от рассмотренного ранее расширения (когда отождествлялись пары (x', x''), (y', y''),удовлетворявшие соотношению $x' + y'' = x'' + y'$), теперь пары (x', x''), (y', y''), удовлетворяющие соотношению $x' \oplus y'' = x'' \oplus y'$, отождествляются лишь при дополнительном условии $x' \neq x''$, $y' \neq y''$; этим определено *отношение эквивалентности* $\approx$; если дополнительное условие не выполнено, то пары, удовлетворяющие указанному соотношению, называются подчиненными *отношению баланса,* $(x', x'') \Delta (y', y'')$, а отождествляются, лишь если они просто равны. Множество пар с указанным отождествлением и называется *симметризацией* $\mathbf{S}_{max}$ полуполя $\mathbf{R}_{max}$.

Такая модификация отождествления связана с тем, что, в отличие от обычного арифметического сложения, когда из $a + b = a + c$ следует $b = c$ (условие *регулярности* или *«сокращения» по сложению),* теперь из $a \oplus b = a \oplus c$ или $max\ (a, b) = max\ (a, c)$ в общем случае, очевидно, *не* следует $b = c$; как следствие, отношение баланса само по себе не пригодно для отождествление пар, так как не является *отношением эквивалентности,* которое должно обладать стандартными свойствами *рефлексивности, симметричности* и *транзитивности* (нарушение транзитивности иллюстрируется простейшим примером: $(0,1) \Delta (1,1)$, $(1,1) \Delta (1,0)$, но *неверно,* что $(0,1) \Delta (1,0)$!). Предложенная же модификация отождествления осуществляется отношением эквивалентности $\approx$, очевидно, более сильным, чем отношение баланса.

Хотя это отношение эквивалентности уже описано выше, удобно представить его в следующей форме: пусть $Sol\ (a) = \{x \in \mathbf{R}_{max} \times \mathbf{R}_{max} : x \Delta a\}$; тогда $a \approx b \Leftrightarrow Sol\ (a) = Sol\ (b)$. Оно согласовано с операциями в $\mathbf{R}_{max} \times \mathbf{R}_{max}$, с отношением Δ и операторами θ, / /, *. Например, из цепочки соотношений

$$x \in Sol\ (a \oplus c) \Leftrightarrow x \Delta a \oplus c \Leftrightarrow x\, \theta\, c \Delta a \Leftrightarrow x\, \theta\, c \in Sol(a)$$

следует $Sol\ (a) = Sol\ (b) \Rightarrow Sol\ (a \oplus c) = Sol\ (b \oplus c)$ или $a \approx b \Rightarrow a \oplus c \approx b \oplus c$.

Различаются три типа классов эквивалентности:

$\underline{(t, -\infty)} = \{(t, x''): x'' < t\}$ - *«положительные»,*

$\underline{(-\infty, t)} = \{(x', t) : x' < t\}$ - *«отрицательные»,*

$\underline{(t, t)} = \{(t, t)\}$ - *«сбалансированные».*

Сопоставляя классы $\underline{(t, -\infty)}$ с элементами $t \in R_{max}$,можем отождествить $\mathbf{R}_{max}$ с подмножеством положительных или нулевого классов, обозначаемым $(R_{max})^{\oplus}$ Подмножество отрицательных или нулевого классов (вида θx для $x \in (R_{max})^{\Theta}$) обозначается $(\mathbf{R}_{max})^{\theta}$. Подмножество сбалансированных классов (вида $x^{\bullet}$) обозначается $(R_{max})^{\bullet}$. Это приводит к разложению

$$S_{max} = (R_{max})^{\theta} \cup (R_{max})^{\bullet} \cup (R_{max})^{\oplus},$$

причем Θ является единственным элементом, общим для любых двух из этих трех классов; это стоит сравнить с разложением $Z = N^{-} \cup \{0\} \cup N^{+}$.

Простейшие вычисления в $\mathbf{S}_{max}$ можно резюмировать так:

$a \theta b = a$ при $a>b$; $b \theta a = \theta b$ при $a > b$; $a \theta a = a^{\bullet}$.

Это показывает, что, несмотря на отмечавшиеся аналогии, предложенное расширение полуполя $\mathbf{R}_{max}$ не приводит к полю, в отличие, например, от расширения полуполя $\mathbf{Q}_{+}$ до поля $\mathbf{Q}$.

18.3. Развитие понятия о «числе» до деления на нуль и проблемы дистрибутивности

Как уже отмечалось, развитие понятия о числе представляет собой постепенное расширение полукольца **N** натуральных чисел с целью обеспечения выполнимости операций, обратных к основным и естественным операциям сложения, умножения и возведения в степень, то есть операций вычитания, деления, извлечения корня, логарифмирования и некоторых других. Эта цель достигается в кольце **Z** целых, полях **Q, R, C** рациональных, действительных и комплексных чисел, с единственным исключением: даже в числовых полях, как и в более общих или альтернативных им алгебраических структурах, невыполнима операция деления на нуль.

Тот факт, что мультипликативное обращение действительных чисел является частичной функцией, раздражает некоторых начинающих изучать математику: «Кто запретил деление на нуль?» Эта проблема не представляется серьезной с профессиональной точки зрения, но ситуация остается неэстетичной. Мы знаем, как расширить полукольцо

натуральных чисел, чтобы стали разрешимы уравнения типа $5 + x = 2$, $2x = 3$, $x^2 = 2$, $x^2 = -1$ и т. д., но мы не знаем, как делить на нуль. Имеются и конкретные, прагматические аспекты этой проблемы, особенно в связи с точными вычислениями над действительными числами: так как в общем случае неразрешима проблема, является ли действительное число ненулевым, то невозможно в общем случае сказать, является ли оно обратимым. Обсуждение в чисто алгебраическом контексте идеи присоединения к множеству действительных чисел двух дополнительных «чисел» $\infty = 1/0$, $\perp = 0/0$ для того, чтобы сделать деление всегда выполнимым, привело к предложению внести это присоединение уже в конструкцию рациональных чисел из целых, допуская не только ненулевые, но и произвольные знаменатели дробей. В результате была получена алгебраическая структура, отличная от структуры числового поля. Такие структуры названы «роликами» (wheel - колесо, колесико, ролик) и показано, как модифицировать конструкцию поля дробей из области целостности с тем, чтобы получить ролик дробей вместо поля дробей. Эта конструкция обобщена так, что оказывается применимой не только к областям целостности, но и к произвольным коммутативным полукольцам, и дано аксиоматическое определение роликов. Приведем это определение.

Пусть W - некоторое множество, 0 и 1 - константы - нульарные операции, / - унарная операция, + и * - бинарные операции, операции более низкой арности имеют более высокий приоритет, операция * имеет приоритет перед операцией +, x / y понимается как $x * (/ y)$, знак операции * обычно опускается.

Ролик определяется как алгебраическая структура $<W, 0, 1, +, *, />$, в которой выполняются следующие аксиомы:

(1) / - инволюция, то есть $/(/x) = x$, $/(x\,y) = (/y)(/x)$;
(2) $<W, 0, +>$ - коммутативный моноид;
(3) $<W, 1, *, />$ - коммутативный моноид с инволюцией;
(4) $00 = 0$;
(5) $/(x + 0y) = /x + 0y$;
(6) $(x + 0y)z = xz + 0y$;
(7) $(x + y)z + 0z = xz + y\,z$;
(8) $x/y + z + 0y = (x + yz)/y$;
(9) $x + 0/0 = 0/0$.

Следствиями аксиом являются соотношения:

(10) $/1 = 1$;
(11) $0x + 0\,y = 0x\,y$;
(12) $(0/0)\,x = 0/0$;

(13) $x/x = 1 + 0x/x;$
(14) $xz = yz \Rightarrow x + 0z/z = y + 0z/z.$

Последнее соотношение демонстрирует одно из преимуществ роликов по сравнению с кольцами, в которых некоторые правила выполняются при дополнительных условиях, тогда как их двойники в роликах верны всегда; так, в кольце $xz=yz$ влечет $x=y$ лишь с той оговоркой, что z не является делителем нуля, тогда как его двойник (14) в ролике верен при любом z.

Элемент / x в ролике называется /-обратным к элементу x; между тем, поскольку $<W, 1, *>$ - моноид, элемент x может иметь обычный обратный x^{-1} ; связь между ними устанавливается соотношениями:
(15) $x^{-1} + 0/x = /x + 0x^{-1};$
(16) $x^{-1} = /x + 0(x^{-1}/x^{-1});$
(17) $/x = x^{-1} + 0(x/x);$
(18) если xy имеет /-обратный, то x и y имеют обычные обратные $x^{-1} = y / (xy) = / x + 0\ y\ /y$, $y^{-1} = x/ (xy) = /y + 0\ x\ / x.$

Следует отметить, что «обычное» правило $0\ x = 0,$ означающее, что «нуль-члены» могут быть «уничтожены», заменяется правилами (5) - (6), означающими, что такие члены могут быть «передвинуты» тем или иным способом в содержащем их выражении.

В то же время элементы, удовлетворяющие условию $0\ x = 0$, играют особую роль во многих вычислениях; так, отличная от стандартной форма (7) аксиомы дистрибутивности принимает стандартный вид, существенный в определении полуколец, для тех z, для которых выполнено условие $0\ z = 0.$ Объяснением этому служит следующее утверждение:
(19) Подмножество $SW = \{ x \in W: 0\ x = 0 \}$ является полукольцом относительно операций 0,1,+,* данного ролика W.
Кроме того, справедливо утверждение:
(20) Подмножество $GW=\{x \in W:0x=0/x=0\}$ является мультипликативной группой полукольца SW.

К общему определению ролика приводит некоторая модификация метода пар II типа конструкции поля дробей (рациональных чисел) из кольца целых «чисел», выполненная для произвольного коммутативного кольца **R** с единицей и приводящая к ролику WR/P дробей этого кольца. Рассматривается множество RXR пар $(m,n), (r,s)$ - прямое произведение множества R на себя - только с мультипликативной структурой поэлементного умножения. Задается некоторый мультипликативный подмоноид P кольца R и рассматривается следующее отождествление (отношение конгруэнтности) пар: $(m',n') \sim (m'',n'') \Leftrightarrow \exists\ p',p''e\ P: (p'm',\ p'n') =$

=(p"m", p"n"); класс, содержащий пару *(m,n),* обозначается *[m,n];* операции над классами вводятся так: *0 = [0,1], 1 = [1,1],*
[m,n] [r,s] = [mr,ns], [m,n] + [r,s] = [ms + nr, ns], /[m,n] = [n,m] .
Полученная структура и является роликом *WR/P* дробей кольца *R* относительно подмоноида *P;* она удовлетворяет приведенным выше аксиомам ролика. Эта структура не является кольцом, если она нетривиальна, так как в общем случае не выполняется соотношение *0 x = 0:* при *x =[0,0]* имеем *0 x = [0,0],* что не равно *0 = [0,1]* (за исключением случая *0∈P,* когда отношение конгруэнтности несобственно и структура тривиальна). Аддитивная и мультипликативная структуры являются коммутативными моноидами; но групповая аддитивная структура нарушена, так как уравнение *[0,0] + x = 0 = [0,1]* не имеет решений в нетривиальных случаях; вместо этого справедлива формула $x - x = 0\, x^2$, если *x -y* определено как *x+ (-1)y,* где *-1 = [-1,1];* таким образом, *x - x = 0* верно только для тех *x,* которые удовлетворяют условию *0 x= 0* и роль которых в роликах уже отмечалась; следует отметить, что во многих роликах существует много таких *x*. Унарная операция / является инволюцией мультипликативного моноида; для /-обратного к *x* элемента */x* в общем случае не верно, что *x/x = 1* (см. выше соотношение (13)).

Отметим, что *WR/R = {0}* дает пример тривиального ролика дробей. Полный ролик дробей определяется как *WR/P0* , где *P0 = {p* e *P:pm=pn* $\Rightarrow$ *m=n};* он содержит хорошо известное кольцо дробей как подмножество *{x:0x=0};* более того, для его элементов справедливо соотношение *x y = 1* $\Rightarrow$ *y = / x* , так что базовая для роликов операция / может быть использована для вычисления обычных обратных к тем элементам, для которых они существуют. Конкретными примерами роликов дробей при *R* = Z являются:
WZ /(Z\{0}) = Q $\cup$ {/0, 0/0} ; *W(Z/2Z)* /{1} = {0, 1, /0, 0/0 };
WZ / {1} - множество дробей целых чисел, в котором не производится никаких отождествлений, так что две дроби считаются равными тогда и только тогда, когда у них равны числители и знаменатели.

Хорошо известно, что, добиваясь выполнения каких-либо свойств алгебраической структуры, часто приходится жертвовать другими ее свойствами; классический пример - потеря коммутативности при переходе от поля комплексных чисел к телу кватернионов, тогда как сохранение коммутативности ведет к потере обратимости всех ненулевых элементов. К примерам подобного рода можно отнести и искажение аксиомы дистрибутивности (7) в роликах. Рассмотрим некоторые проблемы, связанные с выполнимостью и модификациями аксиомы дистрибутивности в алгебраических структурах с двумя бинарными операциями.

Вернемся к методам пар и рассмотрим, для произвольного полукольца $S=<S, +, *>$, в котором сложение и умножение ассоциативны и умножение распределяет сложение, множество SXS пар $(m,n), (p,q), (r,s)$ со следующими операциями:

- поэлементное сложение: $(m, n)A(p, q)=(m+p, n+q);$
- поэлементное умножение: $(m,n)M(p,q)=(mp,nq);$
- U-операция, выполняемая как умножение двойных «чисел» и как умножение в методе пар I типа: $(m,n)U(p,q)=(mq+np,mp+nq);$
- V-операция, выполняемая как умножение дуальных «чисел» и как сложение в методе пар II типа, то есть как сложение дробей: $(m,n)V(p,q)=(mq+np,nq).$

Рассмотрим некоторые сочетания этих операций, не производя, в отличие от методов пар, каких-либо отождествлений пар элементов множества S.

Рассмотрим структуру $<SXS,A,M>$. Так как обе операции A и M выполняются поэлементно, то для них выполняются те же свойства, что и для исходных операций + и * полукольца S, так что данная структура - полукольцо, а именно - прямое произведение полукольца S на себя.

Рассмотрим структуру $<SXS,A, U>$. Как и выше, операция A ассоциативна как поэлементная; те факты, что операция U ассоциативна и распределяет операцию A, проверяются непосредственно, так что данная структура - полукольцо, прототипом которого является алгебра U двойных «чисел».

Рассмотрим структуру $<SXS,A,V>$. Как и выше, операция A ассоциативна как поэлементная; те факты, что операция V ассоциативна и распределяет операцию A, проверяются непосредственно, так что данная структура - полукольцо, прототипом которого является алгебра V дуальных «чисел».

Рассмотрим теперь структуру $<SXS,M,V>$. Как и выше, операция M ассоциативна как поэлементная; отмечалось и то, что операция V ассоциативна; проверка того, что операция M распределяет операцию V (ожидание этого мотивируется тем, что прототипом данной структуры является поле рациональных чисел), приводит к выражениям

$$((m,n)V(p,q))M(r,s)=(mq+np,nq)M(r,s)=(mqr+npr,nqs),$$
$$((m,n)M(r,s))V((p,q)M(r,s))=(mr,ns)V(pr,qs)=(mrqs+nspr,nsqs),$$

которые в общем случае не равны: равенство этих выражений в поле рациональных чисел достигается благодаря возможности сокращения дробей; в рассматриваемом здесь общем случае такая возможность не предполагается; при наличии в полукольце S аддитивного поглощающего элемента 0 и коммутативности исходных операций + и

* (это соответствует распространенному определению понятия коммутативного полукольца) первое выражение приводится ко второму с использованием дополнительного члена

$$(((m,n)V(p,q))M(r,s))V(0,s)=(mqr+npr,nqs)V(0,s)=(mqrs+nprs,nqss),$$

что сответствует формулировке (7) дистрибутивности в роликах. С другой стороны, без этого дополнительного члена имеет место частичная дистрибутивность - например, для множителей-пар *(r,s)*, удовлетворяющих условию *(0,1)M(r,s)=(0,1)*, или для таких, компоненты которых обладают свойствами *ss=s, rs=r*, то есть элемент *s* является идемпотентом, служащим единицей для элемента *r*. Таким образом, рассмотренная структура не является полукольцом, а является роликом, содержащим некоторые подполукольца.

Рассмотрим теперь структуру $<SXS,M,U>$. Как и выше, операция *M* ассоциативна как поэлементная; отмечалось и то, что операция *U* ассоциативна; проверка того, что операция *M* распределяет операцию *U* (ожидание этого, впрочем, ничем не мотивируется, так как известных прототипов данной структуры пока не встречено), приводит к выражениям

$$((m,n)U(p,q))M(r,s)=(mq+np,mp+nq)M(r,s)=(mqr+npr,mps+nqs),$$
$$((m,n)M(r,s))U((p,q)M(r,s))=(mr,ns)U(pr,qs)=(mrqs+nspr,mrpr+nsqs),$$

которые в общем случае не равны; в отличие от предыдущей, данная структура не является роликом; но, как и в предыдущей, в ней имеет место частичная дистрибутивность, например, для таких множителей-пар *(r,s)*, компоненты которых (при тех же предположениях об исходном полукольце) обладают свойствами *ss=rr=s, rs=r*, допускающими аналогичную интерпретацию. Таким образом, данная структура не является полукольцом или роликом, но содержит некоторые подполукольца.

Разновидностью операций типа *U* и *V* является ассоциативная *E*-операция $(m,n)E(p,q)=(mp+mq+np,nq)$. Структура $<SXS,A,E>$ является полукольцом, прототипом которого служит кольцо с единицей, в которое вкладывается некоторое кольцо.

С вышеизложенным связаны и некоторые другие операции и их сочетания, не обязательно над парами, известные из общей алгебры. Так, операция присоединенного умножения в кольце $xJy=x+y+xy$ связана со сложением соотношением $(x+y)Jz+z=xJz+yJz$, имеющим некоторое сходство с аксиомой дистрибутивности (7) в роликах. Аксиома (6) роликов имеет сходство с

модулярным законом в решетках. Возможны и сочетания некоторой операции с самой собой; так, известны структуры - дистрибутивные квазигруппы, в число аксиом которых входят соотношения $x(yz)=(xy)(xz)$, $(xy)z=(xz)(yz)$, трактующие обычную дистрибутивность $x(y+z)=xy+xz$, $(x+y)z=xz+yz$ в необычной ситуации совпадения операций сложения и умножения; известна и трактовка таких структур как «испорченных» групп, в которых ассоциативный закон заменен на тождества дистрибутивности, что подсказано одним из свойств операции среднего арифметического.

18.4. От натуральных до нечетких и сверхнатуральных чисел

В ряде работ изложены некоторые методические аспекты современных представлений о классической схеме «развития понятия о числе» и возможностях ее дальнейших обобщений, модификаций и применений. Развитие понятия о числе начинается с натуральных «чисел» (по поводу кавычек см. выше; в дальнейшем они опускаются) - «чисел, возникающих при счете», формальное обоснование которых лежит в теории множеств. Это обоснование и связанные с ним некоторые базовые вопросы теории множеств представляют определенный методический интерес.

Уже общепризнанно, что понятие множества принадлежит к числу первоначальных математических понятий, а теория множеств является основой современной фундаментальной и прикладной математики. При изучении теории множеств на всех уровнях естественнонаучного, технического, гуманитарного образования основное внимание уделяется оперированию с множествами - алгебре множеств. При решении той или иной задачи предполагается заданным универсальное для нее множество U, а операции выполняются над его частями или *подмножествами* A, включая несобственные - само множество U и *пустое* множество $\varnothing$, то есть над элементами его *булеана* B(U) - множества всех его подмножеств. С методической точки зрения представляется целесообразным уже на первых этапах изучения теории множеств подробно рассмотреть эти понятия, имеющие как указанное выше теоретическое, так и прикладное значение, в частности, являющиеся отправными для развития теории и практики нечетких множеств, широко применяющихся при решении многих проблем

математического моделирования, искусственного интеллекта, в задачах принятия решений в условиях неопределенности и др..

Придерживаясь, наряду с формальным подходом, более распространенной «наивной» точки зрения, пустое множество можно описать как «множество, не содержащее ни одного элемента». Принято считать, что пустое множество в известном смысле является простейшим из множеств; что существует только одно пустое множество, то есть что все пустые множества равны между собой; что пустое множество является подмножеством любого множества, а потому и входит в любой булеан; что любое подмножество пустого множества является пустым множеством. Последнее соглашение позволяет определить булеан пустого множества как $B(\varnothing)=\{\varnothing\}\neq\varnothing$, то есть как одноэлементное множество, единственным элементом которого является само пустое множество. При этом, в силу приведенных соглашений, выполняется как соотношение $\varnothing\in\{\varnothing\}=B(\varnothing)$, так и соотношение $\varnothing\subseteq\{\varnothing\}=B(\varnothing)$; следует отметить, что для других множеств подобные соотношения отличаются: так, для $A\subseteq U$ справедливо $A\subseteq A\in\{A\}$, но $A\not\subset\{A\}\neq A$; в частности, для $a\in A$ справедливо $a\in\{a\}$, но $a\not\subset\{a\}\neq a$. В силу соотношений, указанных для булеана пустого множества, его булеан, или второй булеан пустого множества, определяется как $B(B(\varnothing))=\{\varnothing,\{\varnothing\}\}$, а его булеан, или третий булеан пустого множества – как $B(B(B(\varnothing)))=\{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}$ (по поводу продолжения этого процесса см. ниже).

Пустое множество, при всей его простоте, играет базовую роль во многих вопросах математики и ее приложений. Это подтверждается, в частности, последующим изложением. Здесь приведем лишь простейшие примеры.

Одним из основных понятий универсальной алгебры является A_Ω-алгебра, где A - некоторое множество, Ω - область операторов, то есть множество операторов $\omega\in\Omega$ вместе с отображением $a: \Omega\to N$, где $a(\omega)$ называется арностью оператора ω; если $a(\omega)=n$, то ω называется n-арным, так что $\Omega(n)=\{\omega\in\Omega: a(\omega)=n\}$; структурой A_Ω-алгебры называется семейство отображений $\Omega(n)\to A^{A^n}$, $n\in N$ (обозначение степени символом ^ принято здесь для удобства изложения). В смысле этого понятия само множество можно считать $\varnothing$-алгеброй.

Другое основное понятие универсальной алгебры - оператор замыкания на множестве A как отображение C булеана B(A) в себя, обладающее свойствами: для всех

$X,Y \in \mathbf{B}(A)\ \{X \subseteq Y \Rightarrow C(X) \subseteq C(Y)\},\ \{X \subseteq C(X)\},\ \{C(C(X)) = C(X)\}.$

Одна из самых неожиданных конкретизаций оператора замыкания, носящая чисто логический характер, была дана в виде операции присоединения следствий и применятся в формальных теориях. А именно, теория определяется как произвольное множество X предложений некоторого языка L. Если X замкнуто относительно операции присоединения следствий, то есть X = C(X), то X называется теорией C. C(X) есть наименьшая теория C, содержащая X. В смысле этих понятий $\mathbf{C}(\square)$ есть система всех логически доказуемых или общезначимых предложений теории C.

Именно пустое множество лежит и в основе формального определения натуральных чисел, множество которых $\mathbf{N} = \{0,1,2, \ldots\}$, в отличие отукоренившегося представления, включает число 0; с этого числа, собственно, и начинается определение натуральных чисел. Действительно, говорят, что множества A и B равномощны или эквивалентны, если между ними можно установить взаимно-однозначное соответствие; это записывают в виде $|A| = B$, где |A| - кардинальное число или мощность множества A. Кардинальное число 0 определяют как $0 = |\varnothing|$; кардинальное число 1 – как $1 = |\{\varnothing\}|$, то есть как $1 = |\mathbf{B}(\varnothing)|$; кардинальное число 2 – как $2 = |\{\varnothing,\ \{\varnothing\}\}|$, то есть как $2 = |\mathbf{B}(\mathbf{B}(\varnothing))|$; следующим на этом пути было бы определено кардинальное число $4 = |\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}|$ то есть $4 = |\mathbf{B}(\mathbf{B}(\mathbf{B}(\varnothing)))|$. Другой путь состоит в том, что, введя операции - в частности, сложение - над кардинальными числами, говорят, что кардинальное число |A| конечно или является натуральным целым числом, если $|A| \neq |A| + 1$; в этом случае говорят, что множество A конечно, а |A| является числом его элементов. Так как $0 \neq 0+1=1,\ 1 \neq 1+1=2,\ 2 \neq 2+1,$ то введенные ранее кардинальные числа 0,1,2 являются натуральными числами. Далее определяют натуральные числа 3=2+1, 4=3+1 и, на этом пути, все множество **N** натуральных чисел или весь натуральный ряд. Равносильный путь, предложенный Дж. фон Нейманом, состоит в последовательном, рекуррентном индексировании множеств, начинающемся снова с пустого множества: $0 = \varnothing,\ 1 = \{0\},\ 2 = \{0,1\},\ 3 = \{0,1,2\},\ \ldots$. Этот подход можно описать и следующим образом. Интуитивная модель теории множеств Цермело строится с использованием, в качестве исходных, понятий пустого множества $\varnothing$ и операции порождения булеана B. Как уже отмечалось,

$\mathbf{B}(\varnothing)=\{\varnothing\},\ \mathbf{B}(\{\varnothing\})=\{\varnothing,\ \{\varnothing\}\},\ \mathbf{B}(\{\varnothing,\ \{\varnothing\})= \{\varnothing,\ \{\varnothing\},\ \{\{\varnothing\}\},\ \{\varnothing,\ \{\varnothing\}\}\}$

и т.д. Продолжая этот процесс, для каждого конечного числа можно получить множество с большим числом элементов, но никогда нельзя получить бесконечное множество. Поскольку для построения теории множеств необходимо наличие бесконечных множеств, то для завершения построения модели теории множеств Цермело вводится специальное предположение, на котором здесь останавливаться не будем. Однако существует более слабая теория множеств T_1, известная под названием общей теории множеств, отличающаяся от теории множеств Цермело отсутствием аксиомы бесконечности. Интуитивной моделью для T_1 является пространство, содержащее все множества, входящие во все последовательные булеаны пустого множества, то есть содержащее лишь конечные множества. Именно в теории T_1 можно построить теорию натуральных чисел по Дж. фон Нейману указанным выше способом: 0 отождествляется с $\varnothing$, 1 – с $\{\varnothing\}$, 2 – с $\{\varnothing, \{\varnothing\}\}$, 3 – с $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$ и вообще, если n отождествляется с множеством x, то n+1 отождествляется с классом $x \cup \{x\}$, состоящим из всех элементов множества x и самого множества x. Другими словами, число n просто отождествляется с множеством всех чисел, меньших, чем n. Теперь в T_1 можно определить предикат N(x), означающий, что x есть натуральное число; при помощи этого предиката можно ввести новые переменные, представляющие только натуральные числа.

Как уже отмечалось, простейшим из подмножеств любого множества является пустое множество, которое теперь, после определения числа 0, можно охарактеризовать как 0-элементное. Следующими по простоте являются одноэлементные подмножества. По каждому элементу $u \in U$ может быть построена последовательность кратных одноэлементных множеств

$u=<u;0> \in \{u\}=\{<u;0>\}=<u;1> \in \{\{u\}\}=\{\{<u;0>\}\}=\{<u;1>\}=<u;2> \in \{\{\{u\}\}\}=$
$\{\{\{<u;0>\}\}\}=\{\{<u;1>\}\}=\{<u;2>\}=<u;3> \in \ldots \in \{<u;k-1>\}=<u;k> \in \ldots,$

причем $|<u;k>|=1$ для любого тогда $k \in N\backslash\{0\}$, как равенство $|<u;0>|=|u|$, в данном контексте, не имеет смысла. По каждому множеству $A \subseteq U$ также может быть построена последовательность кратных одноэлементных множеств

$\{A\}=<A;1> \in \{\{A\}\}=\{<A;1>\}=<A;2> \in \{\{\{A\}\}\}=\{\{<A;1>\}\}=\{<A;2>\}=<A;3> \in \ldots$
$\in \{<A;k-1>\}=<A;k> \in \ldots,$ **и для единства обозначений,** $A=<A;0> \in <A;1>,$

причем $|A|=|<A;0>| \neq |<A;k>|=1$ для любого $k \in N\backslash\{0\}$. В частности, для пустого множества $|\varnothing|=|<\varnothing;0>|=0 \neq 1=|<\varnothing;k>|$ при любом $k \in N\backslash\{0\}$. Кратные одноэлементные множества являются

простейшими, после пустого множества, элементами кратных булеанов любого множества, определяемых следующим образом.

Как уже отмечалось, булеан B(A) некоторого множества A образован всеми его подмножествами, включая A и 0, причем $|B(A)| = 2^{|A|}$; по этой причине булеан множества A часто обозначают через $B(A)=2^A$. Подобно вышеизложенному могут быть определены кратные булеаны множества A, а именно, с использованием их же обозначений, а также введенных ранее обозначений для кратных одноэлементных множеств, $B(A;0)=A=$

$<A;0>\in B(A;1)=B(A)=\{A,...,\varnothing\}\in B(A;2)=B(B(A;1))=B(B(A))=\{B(A;1), ... , <A;1>, ... , <\varnothing;1>, <\varnothing;0>\}\in B(A;3)=B(B(A;2))=\{B(A;2), ... , <A;2>, ... , <\varnothing;2>, <\varnothing;1>, <\varnothing;0>\}\in ... \in B(A;k)=B(B(A;k-1))\in ...$,

или $B(A;0)=A$, $B(A;k)=2^{B(A;k-1)}$ для $k\in N\setminus\{0\}$, причем $|B(A;0)|=|A|$, $|B(A;k)|=2^{|B(A;k-1)|}$ для $k\in N\setminus\{0\}$. В частности, для пустого множества

$B(\varnothing;0)=\varnothing=<\varnothing;0> \in B(\varnothing;1) = \{\varnothing\}= <\varnothing;1>\in$

$B(\varnothing;2)=\{<\varnothing;1>,<\varnothing;0>\}\in B(\varnothing;3)=\{ B(\varnothing;2), <\varnothing;2>, <\varnothing;1>, <\varnothing;0> \}\in B(\varnothing;4) \in ...$

$\in B(\varnothing;k)=2^{B(\varnothing;k-1)} \in ...$,

причем $|B(\varnothing;0)|=0$, $|B(\varnothing;1)|=2^0=2^{(1-1)}=1$,

$|B(\varnothing;2)|=2^1=2^{(2-1)}=2$ - три первых, определенных выше, натуральных числа, но $|B(\varnothing;3)|=2^2=2^{(3-1)}=4$ и далее $|B(\varnothing;4)|=2^4=16$, $|B(\varnothing;5)|=2^16$,... . Обращает на себя внимание «сверхсильный» рост этой последовательности натуральных чисел; следует отметить.

Для того, чтобы, подобно всем этим числам, записать и число 0 как степень числа 2, можно использовать символ $-\infty$, если положить $2^{(-\infty)}=0$, то есть $-\infty=\log_2 0$; его присоединение к множеству действительных чисел, в контексте идемпотентной математики, приводит к идемпотентному полуполю $\mathbf{R}_{max}$; в рассматриваемом здесь контексте может оказаться полезным идемпотентное подполукольцо $\mathbf{N}max$ этого полуполя. Можно ввести в рассмотрение множество $B(\varnothing;-1)$, определив его так, чтобы $\varnothing=2^{B(\varnothing;-1)}$ и $|B(\varnothing;-1)|=\log_2 0 = -\infty$; это позволит записать $B(\varnothing;k)=2^{B(\varnothing;k-1)}$ и $|B(\varnothing;k)|=2^{|B(\varnothing;k-1)|}$ для любого $k\in N$. Для произвольного множества A можно ввести в рассмотрение множество $B(A;-1)$, определив его так, чтобы $A=2^{B(A;-1)}$ и

$|B(A;-1)| = \log_2 n$; это позволит записать $B(A;k)=2^B(A;k-1)$ и $|B(A;k)| = 2^{|B(A;k-1)|}$ для любого $k \in N$.

Таким образом, как отмечено выше и подтверждено примерами, кратные одноэлементные множества имеют минимальную, после пустого множества, мощность в каждом кратном булеане, тогда как каждый кратный булеан имеет максимальную мощность в следующем кратном булеане.

Прикладное значение кратных булеанов в задачах математического моделирования и искусственного интеллекта связано с тем, что если обычное - четкое - множество, то есть подмножество множества U, является, по определению, элементом его первого булеана B(U), то, как известно, нечеткое подмножество при определенных условиях может быть охарактеризовано набором четких множеств - его сечений или множеств уровня, то есть элементом второго булеана B(B(U)); наиболее существенное условие состоит в том, чтобы объединение подмножеств, входящих в набор, давало все множество U; этому условию удовлетворяют, например, сам первый булеан B(U) и вообще любой набор, включающий множество U, а также набор всех одноэлементных подмножеств множества U. Еще одним является условие частной замкнутости множеств набора относительно их пересечений.

Связь второго булеана с нечеткими множествами подсказывает его аксиоматическое описание. Хорошо известно, что первый булеан с операциями дополнения, объединения и пересечения четких множеств удовлетворяет аксиомам булевой алгебры - алгебраической структуры, относящейся к упоминавшимся выше идемпотентным полукольцам, а также к дистрибутивным решеткам с дополнениями. С другой стороны, известна аксиоматика нечеткой алгебры как MV-алгебры, отличающейся от булевой алгебры (и включающей последнюю как частный случай), предложенная за 7 лет до возникновения теории нечетких множеств. MV-алгебра, наряду с указанными выше булевыми операциями, использует специальные операции «сложения» и «умножения» - именно в случае идемпотентности последних MV-алгебра превращается в булеву алгебру. Представляет как теоретический, так и практический интерес интерпретация этих операций во втором булеане.

Представляется перспективным развитие подхода в направлении использования последующих кратных булеанов, что позволит повысить гибкость понятия нечеткого множества подобно тому, как принятое в настоящее время понятие нечеткого множества отличается большей гибкостью по сравнению с понятием четкого множества.

Как мы уже говорили, нечеткое число А определяется как нечеткое подмножество множества **R** действительных чисел, функция принадлежности которого удовлетворяет следующим специальным условиям:

- нормальность $\max_{x\in A} \mu_A(x)=1$ (часто дополнительно требуется
- унимодальность $\mu_A(x)=1$ только для одного $x\in A$) ;
- выпуклость $\mu_A(y)\geq\min\{\mu_A(x),\mu_A(z)\}$ для $z\geq y\geq x$.

Целый раздел теории нечетких множеств - нечеткая арифметика или мягкие вычисления - основан на введении аналогов арифметических операций над нечеткими числами. Эти операции вводятся через операции либо над функциями принадлежности на основе принципа расширения, либо над наборами сечений на основе интервального принципа. При втором подходе определяется уровень принадлежности как ордината функции принадлежности нечеткого числа; пересечение функции принадлежности с этим уровнем дает пару значений - границ интервала достоверности; иначе говоря, для нечеткого числа, как и для произвольного нечеткого множества, определяется набор сечений, срезов или множеств уровня, то есть представляющий это нечеткое число элемент второго булеана B(B(R)); при этом, с точки зрения данного рассмотрения, существенно то, что операции над нечеткими числами определяются через операции над наборами их сечений, выполняемыми по правилам интервальной арифметики. Следует отметить, что условия, предъявляемые к функциям принадлежности нечетких чисел, обеспечивают выполнение сформулированных ранее условий, при которых нечеткое число полностью характеризуется набором своих сечений. Таким образом, для нечеткой арифметики вполне естественным является оперирование с наборами четких множеств как с элементами второго булеана. Это подтверждает целесообразность подхода с позиций именно мягких вычислений.

Мультимножество или комплект, в отличие от обычного множества, может содержать кратные, повторяющиеся, совпадающие элементы, несколько экземпляров одного и того же элемента. Если обычное множество полностью описывается своей характеристической функцией, заданной на этом множестве и принимающей значения в множестве {0,1}, а нечеткое множество - функцией принадлежности, заданной на этом нечетком множестве и принимающей значения в множестве [0,1], то мультимножество описывается функцией экземплярности, заданной на этом мультимножестве и принимающей значения в множестве **N**\{0}. Простейшие и общеизвестные примеры мультимножеств таковы: основная теорема арифметики о том, что каждое положительное натуральное число однозначно представимо

произведением простых чисел (среди которых могут быть повторяющиеся), устанавливает взаимно однозначное соответствие между множеством **N**\{0} и множеством **F**(P) конечных мультимножеств простых чисел, называемых также конечными сверхнатуральными числами (здесь P - множество простых чисел); основная теорема алгебры о том, что каждый нормированный многочлен P(z) степени n над полем **C** комплексных чисел имеет ровно n корней (вообще говоря, комплексных и кратных), устанавливает взаимно однозначное соответствие между такими многочленами и мультимножествами их корней; в математической статистике мультимножествами являются случайные выборки, что особенно проявляется после их систематизации, при переходе к абсолютным частотам (переход к относительным частотам ближе уже к нечетким множествам). Мультимножества и сверхнатуральные числа находят приложения в теории сетей Петри, теории формальных языков и грамматик и многих других; так, терминальные строки нециклической контекстно-свободной грамматики образуют мультимножество, которое становится обычным множеством в том и только том случае, когда грамматика недвусмысленна. Аксиоматика алгебры мультимножеств с подходящими операциями соответствует уже упоминавшейся MV-алгебре.

Многие задачи математического моделирования и искусственного интеллекта приводятся к решению реляционных уравнений - мультимножественных или нечетких. Возможен и чисто алгебраический подход, приводящий к задаче исследования и решения матричных уравнений над полукольцами. Получаемые при этом результаты могут быть использованы, в частности, при моделировании информационных систем, содержащих базы данных и знаний с неполной информацией.

Полукольца, примеры которых уже упоминались выше, определяются как алгебраические структуры с двумя ассоциативными дистрибутивно связанными операциями (трактуемыми, например, как «аддитивная» или «сложение» и «мультипликативная» или «умножение»), иначе говоря, как две дистрибутивно связанные полугруппы. Это естественная область для задания матричных уравнений, однако из-за отсутствия, в общем случае, обратных операций в полугруппах возникают определенные проблемы при исследовании и решении таких уравнений. Следует отметить, что совокупность матриц над полукольцом является частичным (с точностью до согласования размеров при выполнении операций) полукольцом; использование понятия регулярного элемента его мультипликативной полугруппы (в предложенной трактовке -

обобщенно обратимой матрицы) позволяет до конца провести исследование уравнения на совместность и найти *некоторое* решение совместного уравнения; получение *общего* решения хорошо известно в случае, когда аддитивная полугруппа является *группой* (каждый элемент имеет *противоположный),* то есть полукольцо оказывается *кольцом;* в общем же случае с использованием понятия регулярного элемента аддитивной полугруппы (в предложенной трактовке - *обобщенно противоположимой* матрицы) пока не удается получить общее решение. В некоторых случаях оказывается возможным перейти из полукольца в некоторое ассоциированное с ним кольцо, решить в нем уравнение, используя при этом алгоритм обобщенного обращения матриц над ассоциативными кольцами, и, возвратившись в исходное полукольцо, получить в нем таким образом общее решение уравнения. Примером такого преобразования может служить обобщенная стоуновская двойственность между обобщенными булевыми алгебрами (дистрибутивными решетками с нулем и относительными дополнениями) и обобщенными булевыми кольцами (ассоциативными кольцами, все элементы которых идемпотентны. Обобщенные булевы алгебры образуют подкласс дистрибутивных решеток, которые в свою очередь образуют подкласс полуколец. В этой связи представляет интерес вопрос как о распространении обобщенной стоуновской двойственности на более общие полукольца, чем обобщенные булевы алгебры, так и о сопоставлении известных результатов с результатами, получаемыми на основе перехода в возникающие при этом кольца или иные алгебраические структуры, ассоциированные с исходными полукольцами.

Материал, представленный в данной работе, позволяет проследить «развитие понятия о числе» от исходных для всей фундаментальной и прикладной математики натуральных чисел до использующихся в современных задачах искусственного интеллекта нечетких и сверхнатуральных чисел.

Приложение 1

УРАВНЕНИЯ В ПОЛУКОЛЬЦАХ

Определим *полукольцо* $SR = < A, *, + >$ как две *двусторонне дистрибутивно связанные полугруппы* $<A, *>, <A, +>$, так что каждая из операций * , + *ассоциативна.* При таком определении полукольцо может быть охарактеризовано, например, как *«ассоциативное кольцо без 1, 0 и вычитания»,* которые при

исследовании и решении уравнений часто приходится вводить или заменять другими элементами и операциями, делая при этом дополнительные предположения и об основных операциях.

Непосредственно из определения полукольца следует, что в нем может быть записано *двустороннее неоднородное уравнение Сильвестра*

$$S(x) + e = T(x) + f,$$

где

$S(x) = a_1 * x * b_1 + ... + a_p * x * b_p$, $T(x) = c_1 * x * d_1 + ... + c_q * x * d_q$ - *отображения Сильвестра* (в случае одного слагаемого - *элементарные).* Его разновидностями являются, например, *одностороннее* (без b_i, d_i или a_i, c_i), *однородное* (без *e, f), элементарное* (с одним слагаемым в левой и/или правой части) уравнения, а также еще более специальные, например, $a * x * b = c$ (подробно рассмотренное ниже), $a * x = b$ («обычное линейное»), $a * x = b * x$ («простейшее однородное»), $x = b + a * x$ («дискретное стационарное уравнение Беллмана») и другие. Очевидно, что если * *коммутативна,* а *a , b идемпотентны (a* a = a , b* b = b),* то $a*x = b*x$ имеет решение $x=a * b;$ если в *SR* есть *1,* $a^0 = 1$, то $x = b + a* x$ имеет решение $x = a^{\$} * b$, где *транзитивное замыкание* $a^{\$} = a^0 + a^1 + ... + a^n + ...$ (формальная сумма).

Остановимся подробнее на *исследовании* и отыскании *общего решения* уравнения $a * x * b = c$, вводя только непосредственно используемые понятия и предположения и иллюстрируя предлагаемый подход такими «диаметрально противоположными» примерами, как *ассоциативные кольца с единицей* и *булевы алгебры.*

Предварительно напомним, что в *полугруппе* $S=<A, * >$, если коэффициенты *a, b* уравнения $a * x * b = c$ *регулярны (обобщенно обратимы),* то есть существует элемент *a (обобщенный обратный к a)* такой, что $a * a^- * a = a$, то же для *b,* то

$$\{a * x * b = c \ \textit{разрешимо}\} <=>$$
$$=> \{a * a^- c * b^- * b = c,\ x = a^- * c * b^- - \textit{некоторое его решение}\}.$$

Отметим два частных случая:

1) если *a - идемпотент (a * a = a,* а значит и $a * a * a = a$, так что можно положить $a^- = a$ *),* то же для *b,* то

$$\{a * x * b = c \ \textit{разрешимо}\} <=>$$
$$=> \{a * c * b = c,\ x = c - \textit{некоторое его решение}\}.$$

2) если $S=<A, *, 1>$ - *моноид* и *a обратим (* существует a^{-1}, *обратный* к *a,* такой, что $a * a^{-1} = a^{-1} * a = 1$*),* то же для *b,* то

*{a * x * b = c разрешимо, x=a $^{-1}$ * c * b $^{-1}$ - его единственное решение}.*

В общем случае возникает вопрос об описании общего решения уравнения. Ответ на него предполагает наличие дополнительных структур в А и дополнительных свойств элементов.

Напомним, например, что если $R=<A,*,+,0>$ - *ассоциативное кольцо,* то *общее решение* разрешимого уравнения записывается в виде $x = a^- * c * b^- + y - a^- * a * y * b * b^-$, где *y* из *A* произвольно.

Рассмотрим уравнение $a * x * b = c$ в полукольце $SR=<A, *, 1, +, 0>$, так что $<A,*,1>$, $<A,+,0>$ - *моноиды,* $0=/=1$ и $0*c=c*0=0$ для всех *c* из *A*.

Определение. Регулярные элементы *a, b регулярно дополняемы,* если существуют элементы $a\sim$, $b\wedge$ *(регулярные дополнения* для *a, b),* такие, что

$$a * a\sim = 0,\ a^- * a + a\sim = 1,\ b\wedge * b = 0,\ b * b^- + b\wedge = 1.$$

Предложение. Общее решение разрешимого уравнения записывается в виде

$$x = a^- * c * b^- + a^- * a * y * b\wedge + a\sim * y,$$

где *y* из *A* произвольно.

Доказательство.

(i) *x* - решение:

$$a * x * b = a * a^- * c * b^- * b + a * a^- * a * y * b\wedge * b + a * a\sim * y * b =$$
$$= c + a * y * (b\wedge * b) + (a * a\sim) * y * b = c + a * y * 0 + 0 * y * b = c;$$

(ii) любое решение x_0, $a * x_0 * b = c$, может быть выделено из *x* выбором, например, $y = x_0$:

$$x = a^- * c * b^- + a^- * a * x_0 * b\wedge + a\sim * x_0 = (a^- * a * x_0 * b * b^- + a^- * a * x_0 * b\wedge) +$$
$$+ a\sim * x_0 = a^- * a * x_0 * (b * b^- + b\wedge) + a\sim * x_0 = a^- * a * x_0 * 1 + a\sim * x_0 =$$
$$= (a^- * a + a\sim) * x_0 = 1 * x_0 = x_0.$$

Таким образом, исследование и решение данного уравнения в данном полукольце выполнено полностью. Отметим, что для уравнения $a * x = c$, когда $b = 1 = b$ - ив качестве $b\wedge$ может быть взят *0,* общее решение записывается в виде $x = a^- * c + a\sim * y$.

Пример 1. Если $R=<A,*,1,+,0>$ - *ассоциативное кольцо с единицей,* то регулярными дополнениями являются $a\sim = 1 - a^- * a$, $b\wedge = 1 - b * b^-$; условия на них выполнены по их определению; общее решение записывается в виде

$$x = a^- * c * b^- + a^- * a * y * (1 - b * b^-) + (1 - a^- * a) * y =$$
$$= a^- * c * b^- + y - a^- * a * y * b * b^-,$$

что совпадает с указанным выше.

Пример 2. Если $BA=<A,*,1,+,0,'>$ - булева алгебра, то есть операции коммутативны, элементы идемпотентны и потому

регулярны, так что можно положить $a^{\sim} = a, b^{\sim} = b$, то можно положить, в свою очередь, $a\sim = a'$, $b\wedge = b'$; нужные условия на такие элементы выполняются по определению булевой алгебры: $a * a' = 0$, $a + a' = 1$, то же для *b;* общее решение записывается в виде

$$x = c + a * y * b' + a' * y = c + (a' + a * b') * y = c + (a * b)' * y$$

и интерпретируется как *относительное дополнение* к $a * b$ в интервале $[c, y]$.

Приложение 2

УРАВНЕНИЯ В БИГРУППОИДАХ

Свойства операций в алгебраических структурах можно подразделить на глобальные (например: в полугруппе ассоциативность выполняется для любых наборов элементов), локальные (например: регулярность (обобщенная обратимость) - существование для *a* такого *g,* что *aga=a* - может иметь место для отдельных - но не всех - элементов полугруппы) и локально-глобальные (например: если *a* регулярен, то *agax=ax* для любого *x).* Если в алгебраической структуре с одной операцией не выполняются никакие глобальные свойства, то она известна как группоид; структуру с двумя операциями в подобной ситуации назовем бигруппоидом (например: биполугруппа не является полукольцом, если две ассоциативных операции не связаны дистрибутивно). Локальные же и локально-глобальные свойства выполняться в бигруппоидах могут, как и могут служить для решения некоторых задач.

В качестве примера рассмотрим исследование и решение в некотором бигруппоиде ВГ уравнения типа, рассмотренного в Приложении 1. Ввиду отсутствия (глобальной) ассоциативности ограничимся, например, уравнением $a* (x * b) = c$ (уравнение $(a * x) * b = c$ может быть рассмотрено аналогично).

Пусть уравнение разрешимо, то есть существует $x_0 \in$ ВГ такой, что $a* (x_0* b) = c$; это значит, что $\xi_0 = x_0 * b$ является решением уравнения $a * \xi = c$, то есть $a * \xi_0 = c$.

Потребуем для *a* выполнения следующего локально-глобального свойства: существует *g* такой, что для любого *k* выполняется соотношение

$$a * (g * (a * k)) = a * k .$$

Тогда

$$c = a * \xi_0 = a * (g * (a * \xi_0)) = a * (g * c);$$

тем самым получено условие на параметры a и c уравнения $a * \xi = c$, необходимое для разрешимости этого уравнения. Условие является и достаточным: если оно выполняется, то $\xi_1 = g * c$, очевидно, является некоторым решением этого уравнения.

Рассмотрим теперь уравнение $x * b = g * c$. Пусть оно разрешимо, то есть существует $x_1 \in B\Gamma$ такой, что $x_1 * b = g * c$.

Потребуем для b выполнения следующего локально-глобального свойства: существует h такой, что для любого k выполняется соотношение

$$((k * b) h * b = k * b.$$

Тогда

$$g * c = x_1 * b = ((x_1 * b) h * b = ((g * c) * h) * b;$$

в сочетании с полученным выше условием $c = a * (g * c)$ получаем условие

$$c = a * (((g * c) * h) * b)$$

на параметры a, b, c уравнения $a * (x * b) = c$, как необходимое, так и достаточное для его разрешимости: при выполнении этого условия $x_2 = (g * c) * h$, очевидно, является некоторым решением этого уравнения.

Для записи общего решения потребуем дополнительно выполнения следующих локально-глобальных свойств:

- для a — существует ζ, такой, что для любого k выполняется соотношение

$$g * (a * k) + \zeta * k = k;$$

- для b — существует η такой, что для любых k, l, m выполняется соотношение

$$(m * (l * (k * b))) * h + m * (l * (k * \eta)) = m * (l * k);$$

- для a и b - для любого k и любого l такого, что $a * (((g * l) * h) * b) = l$, выполняется соотношение

$$a * (((g * l) * h + g * (a * (k * \eta)) + \zeta * k) * b) = l.$$

Тогда общее решение уравнения $a * (x * b) = c$ может быть записано в виде

$$x = (g * c) * h + g * (a * (y * \eta)) + \zeta * y,$$

где $y \in B\Gamma$ произвольно. Это поверяется непосредственно с использованием сформулированных требований.

В ситуации Приложения 1, где бигруппоид является полукольцом, то есть операции ассоциативны и дистрибутивно связаны (глобальные

свойства), а элементы *a* и *b* регулярны и регулярно дополняемы (локальные свойства), представленные здесь критерий разрешимости и общее решение уравнения *a* (x * b) = c* сводятся к указанным там критерию разрешимости и общему решению уравнения *a * x * b = c* при $g = a^{-}$, $h = b^{-}$, $\zeta = a\sim$, $\eta = b\wedge$.

Сформулированные выше требования могут выполняться и в более общих алгебраических структурах, чем полукольца, например, в неассоциативных полукольцах (дистрибутивных бигруппоидах). Они тесно связаны с такими глобальными свойствами неассоциативных структур, как альтернативность, эластичность, моноассоциативность, выполнимость тождеств Якоби, Йордана, Мальцева, Муфанг, Бола и др.

18.5. Представление чисел в памяти компьютера

Для представления натурального числа в памяти компьютера, оно обычно переводится в двоичную систему счисления. Для представления отрицательных чисел используется т. н. дополнительный код числа, который получается путём прибавления единицы к инвертированному представлению модуля данного отрицательного числа в двоичной системе счисления.

Представление действительных чисел в памяти компьютера имеет некоторые ограничения связанные с используемой системой счисления, а также ограниченностью объёма памяти, выделяемого под числа. Действительные числа обычно представляются в виде чисел с плавающей запятой. При этом лишь некоторые из действительных чисел могут быть представлены в памяти компьютера точным значением, в то время как остальные числа представляются приближёнными значениями. В наиболее распространённом формате число с плавающей запятой представляется в виде последовательности битов, часть из которых кодирует собой мантиссу числа, другая часть — показатель степени, и ещё один бит используется для указания знака числа.

19. Системы счисления

— символический метод записи чисел, представление чисел с помощью письменных знаков.

Система счисления:

- даёт представления множества чисел (целых и/или вещественных);
- даёт каждому числу уникальное представление (или, по крайней мере, стандартное представление);
- отражает алгебраическую и арифметическую структуру чисел.

Системы счисления подразделяются на *позиционные*, *непозиционные* и *смешанные*.

19.1. Позиционные системы счисления

В позиционных системах счисления один и тот же числовой знак (цифра) в записи числа имеет различные значения в зависимости от того места (разряда), где он расположен. Изобретение позиционной нумерации, основанной на поместном значении цифр, приписывается шумерам и вавилонянам; развита была такая нумерация индусами и имела неоценимые последствия в истории человеческой цивилизации. К числу таких систем относится современная десятичная система счисления, возникновение которой связано со счётом на пальцах. В средневековой Европе она появилась через итальянских купцов, в свою очередь заимствовавших её у мусульман.

Под позиционной системой счисления обычно понимается *b*-ричная система счисления, которая определяется целым числом $b > 1$, называемым **основанием** системы счисления. Целое число *x* в *b*-ричной системе счисления представляется в виде конечной линейной комбинации степеней числа *b*:

$$x = \sum_{k=0}^{n-1} a_k b^k ,$$

где a_k — это целые числа, называемые **цифрами**, удовлетворяющие неравенству $0 \leq a_k \leq (b-1)$.

Каждая степень b^k в такой записи называется весовым коэффициентом разряда. Старшинство разрядов и соответствующих им цифр определяется значением показателя *k* (номером разряда). Обычно для ненулевого числа *x* требуют, чтобы старшая цифра a_{n-1} в его *b*-ричном представлении была также ненулевой.

Если не возникает разночтений (например, когда все цифры представляются в виде уникальных письменных знаков), число *x* записывают в виде последовательности его *b*-ричных цифр, перечисляемых по убыванию старшинства разрядов слева направо:

$$x = a_{n-1}a_{n-2}\ldots a_0.$$

Например, число *сто три* представляется в десятичной системе счисления в виде:

$$103 = 1 \cdot 10^2 + 0 \cdot 10^1 + 3 \cdot 10^0.$$

Наиболее употребляемыми в настоящее время позиционными системами являются:

- 1 — единичная (счёт на пальцах, зарубки, узелки «на память» и др.);
- 2 — двоичная (в дискретной математике, информатике, программировании);
- 3 — троичная;
- 8 — восьмеричная;
- 10 — десятичная (используется повсеместно);
- 12 — двенадцатеричная (счёт дюжинами);
- 16 — шестнадцатеричная (используется в программировании, информатике);
- 60 — шестидесятеричная (единицы измерения времени, измерение углов и, в частности, координат, долготы и широты).

В позиционных системах чем больше основание системы, тем меньшее количество разрядов (то есть записываемых цифр) требуется при записи числа.

19.2. Смешанные системы счисления

Смешанная система счисления является обобщением *b*-ричной системы счисления и также зачастую относится к позиционным системам счисления. Основанием смешанной системы счисления является возрастающая последовательность чисел $\{b_k\}_{k=0}^{\infty}$, и каждое число *x* в ней представляется как линейная комбинация:

$$x = \sum_{k=0}^{n-1} a_k b_k ,$$

где на коэффициенты a_k, называемые как и прежде *цифрами*, накладываются некоторые ограничения.

Записью числа *x* в смешанной системе счисления называется перечисление его цифр в порядке уменьшения индекса *k*, начиная с первого ненулевого.

В зависимости от вида b_k как функции от *k* смешанные системы счисления могут быть степенными, показательными и т. п. Когда $b_k = b^k$ для некоторого *b*, смешанная система счисления совпадает с *b*-ричной системой счисления.

Наиболее известным примером смешанной системы счисления являются представление времени в виде количества суток, часов, минут и секунд. При этом величина «*d* дней, *h* часов, *m* минут, *s* секунд» соответствует значению

$$d \cdot 24 \cdot 60 \cdot 60 + h \cdot 60 \cdot 60 + m \cdot 60 + s \text{ секунд.}$$

Факториальная система счисления

В **факториальной системе счисления** основаниями являются последовательность факториалов $b_k = k!$, и каждое натуральное число *x* представляется в виде:

$$x = \sum_{k=1}^{n} d_k k!$$

где $0 \le d_k \le k$.

Фибоначчиева система счисления

Фибоначчиева система счисления основывается на числах Фибоначчи. Каждое натуральное число *x* в ней представляется в виде:

$$x = \sum_{k=0}^{n} f_k F_k$$

где F_k — числа Фибоначчи, $f_k \in \{0,1\}$, при этом в записи $f_n f_{n-1} \cdots f_0$ не встречается две единицы подряд.

19.3. Непозиционные системы счисления

В непозиционных системах счисления величина, которую обозначает цифра, не зависит от положения в числе. При этом система может накладывать ограничения на положение цифр, например, чтобы они были расположены в порядке убывания.

Биномиальная система счисления

Представление, использующее биномиальные коэффициенты

$$x = \sum_{k=1}^{n} \binom{c_k}{k},$$

где $0 \le c_1 < c_2 < \ldots < c_n$.

Система остаточных классов (СОК)

Представление числа в системе остаточных классов основано на понятии вычета и китайской теореме об остатках. СОК определяется набором взаимно простых *модулей* $(m_1, m_2, \ldots, m_n)$ с произведением $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ так, что каждому целому числу x из отрезка $[0, M-1]$ ставится в соответствие набор вычетов $(x_1, x_2, \ldots, x_n)$, где

$$\begin{aligned} x &\equiv x_1 \pmod{m_1}; \\ x &\equiv x_2 \pmod{m_2}; \\ &\ldots \\ x &\equiv x_n \pmod{m_n}. \end{aligned}$$

При этом китайская теорема об остатках гарантирует однозначность представления для чисел из отрезка $[0, M-1]$.

В СОК арифметические операции (сложение, вычитание, умножение, деление) выполняются покомпонентно, если про результат известно, что он является целочисленным и также лежит в $[0, M-1]$.

Недостатками СОК является возможность представления только ограниченного количества чисел, а также отсутствие эффективных алгоритмов для сравнения чисел, представленых в СОК. Сравнение обычно осуществляется через перевод аргументов из СОК в смешанную систему счисления по основаниям $(m_1, m_1 \cdot m_2, \ldots, m_1 \cdot m_2 \cdot \ldots \cdot m_{n-1})$.

Система счисления Штерна-Броко

Система счисления Штерна-Броко — способ записи положительных рациональных чисел, основанный на дереве Штерна-Броко.

19.4. Системы счисления разных народов

Системы счисления в культуре

Индо-арабская система счисления

Арабская	Кхмерская
Индийские	Лаоская
Тамильская	Монгольская
Бирманская	Тайская

Восточноазиатские системы счисления

Китайская	
Японская	Вьетнамская
Сучжоу	Счётные палочки
Корейская	

Алфавитные системы счисления

Абджадия	Греческая
Армянская	Эфиопская
Ариабхата	Еврейская
Кириллическая	Катапаяди

Другие системы

Вавилонская	Аттическая
Египетская	Кипу
Этруская	Майская
Римская	

Позиционные системы счисления

Десятичная система счисления (10)

2, 3, 4, 5, 6, 7, 8, 9, 12, 16, 60

Нега-позиционная система счисления

Непозиционные системы счисления

Единичная (унарная) система счисления

Список систем счисления

Древнеегипетская система счисления

Древнеегипетская десятичная непозиционная система счисления возникла во второй половине третьего тысячелетия до н. э. Для

обозначения чисел 0, 1, 10, 10^2, 10^3, 10^4, 10^5, 10^6, 10^7 использовались специальные цифры. Числа в египетской системе счисления записывались как комбинации этих цифр, в которых каждая из цифр повторялась не более девяти раз. Значение числа равно простой сумме значений цифр, участвующих в его записи.

Вавилонская система счисления

Шестидесятеричная система счисления

Алфавитные системы счисления

Алфавитная запись чисел

Алфавитными системами счисления пользовались древние армяне, грузины, греки (ионическая система счисления), арабы (абджадия), евреи и другие народы Ближнего Востока. В славянских богослужебных книгах греческая алфавитная система была переведена на буквы кириллицы.

Еврейская система счисления

Еврейская система счисления в качестве цифр использует 22 буквы еврейского алфавита. Каждая буква имеет своё числовое значение от 1 до 400. Ноль отсутствует. Цифры, записанные таким образом, наиболее часто можно встретить в нумерации лет по иудейскому календарю.

Греческая система счисления

Римская система счисления

Римские цифры

Каноническим примером почти непозиционной системы счисления является римская, в которой в качестве цифр используются латинские буквы:

I	обозначает	1,
V —		5,
X —		10,
L —		50,
C —		100,
D —		500,
M — 1000		

Например,

$$II=1+1=2$$

здесь символ I обозначает 1 независимо от места в числе.

На самом деле, римская система не является полностью непозиционной, так как меньшая цифра, идущая перед большей, вычитается из неё, например:

$$IV = 4,$$

в то время как:

$$VI = 6$$

Система счисления майя

Майя использовали 20-ричную систему счисления за одним исключением: во втором разряде было не 20, а 18 ступеней, то есть за числом (17)(19) сразу следовало число (1)(0)(0). Это было сделано для облегчения расчётов календарного цикла, поскольку (1)(0)(0) = 360 примерно равно числу дней в солнечном году.

Для записи основными знаками были точки (единицы) и отрезки (пятёрки).

Кипу инков

Прообразом баз данных, широко использовавшихся в Центральных Андах (Перу, Боливия) в государственных и общественных целях в I—II тысячелетии н. э., была узелковая письменность Инков — кипу, состоявшая как из числовых записей десятичной системы, так и не числовых записей в двоичной системе кодирования. В кипу применялись первичные и дополнительные ключи, позиционные числа, кодирование цветом и *образование серий* повторяющихся данных. Кипу впервые в истории человечества использовалось для применения такого способа ведения бухгалтерского учёта как двойная запись.

Литература

1. Кантор И.Л., Солодовников А.С. Гиперкомплексные числа. - М.: Наука, 1973. -144 с.
2. Блюмин С.Л. Двумерные алгебры / Метод, указания.- Липецк: Изд-во ЛГТУ,1995.-18с.
3. Яглом И.М. Принцип относительности Галилея и неевклидова геометрия -М.: Наука, 1969.-303 с.
4. Немец С.Ю. Триплексные числа: обратимость и необратимость элементов, обобщенное обращение, решение уравнений // Регион, молодежи, науч. и инж. выставка «Шаг в будущее - Центр России». Сб. тез. докл. - Липецк: Изд-во ЛГТУ, 1999. - С. 7-8.
5. Немец С.Ю. Обобщенная обратимость в трехмерной алгебре // Студ. науч.-практ. конф. «Наука и молодежь на рубеже столетий».Сб. науч. тр. - Липецк: Изд-во ЛГТУ,2000.-С. 10-12.
б. Блюмин С.Л., Кривовяз Е.В., Немец С.Ю. К обратимости элементов *n*-кратных супералгебр // Воронеж. Вес. Матем. шк. «Современные методы в теории краевых задач (Понтрягинские чтения-1Х)».Тез.докл. - Воронеж: Изд-во ВГУ, 1998.-С. 221.
7. Розенфельд Б.А. Неевклидовы геометрии. - М.: Гостехтеориздат, 1955. - 678 с.
8. Блюмин С.Л., Миловидов СП. Исследование и решение матричных уравнений над ассоциативными кольцами // Журнал вычислительной математики и математической физики. - 1994. - Т. 34, № 2. - С. 163 - 174.
9. Бурбаки Н. Алгебра. Алгебраические структуры. Линейная и полилинейная алгебра. - М.: Физматгиз, 1962. - 516 с.
10. Duplij S., Marcinek W. Regular graded algebras and obstructed categories with duality. *Preprint.* // http://xxx.lanl.gov arXiv.org e-Print archive math.QA/0107022. 3 Jul2001. 13 p.
11. *К. Айерлэнд, М. Роузен.* Классическое введение в современную теорию чисел = A Classical Introduction to Modern Number Theory. — М.: Мир, 1987.
12. *З. И. Боревич, И. Р. Шафаревич.* Теория чисел. — М.: Наука, 1972. — 510 с.
13. *И. М. Виноградов.* Основы теории чисел. — М.-Л.: Гостехиздат, 1952. — 180 с.
14. *Ю. И. Манин, А. А. Панчишкин.* Введение в теорию чисел. — М.: ВИНИТИ, 1990. — Т. 49. — 341 с. — (Итоги науки и техники. Серия «Современные проблемы математики. Фундаментальные направления».).

15. *Арнольд В. И.* Геометрия комплексных чисел, кватернионов и спинов, МЦНМО, 2002
16. *Елисеев В. И.* «Введение в методы теории функций пространственного комплексного переменного», Центр научно-технического творчества молодежи Алгоритм. — М.:, НИАТ. — 1990. Шифр Д7-90/83308
17. *Понтрягин Л.* Комплексные числа, Квант, № 3, 1982.
18. Ван дер Варден Б.Л. Алгебра. - М.: Наука, 1979. - 579 с.

19. Литвинов Г.Л., Маслов В.П. Идемпотентная математика // Современный анализ и его приложения: Воронеж, зимн. матем. школа (ВЗМШ-2000). Тез. докл. - Воронеж: ВГУ, 2000. - С. 20-21.
20. Golan J.S. Semirings and their Applications. - Dordrecht: Kluwer, 1999. - 468 p.
21. Gaubert S., Plus M. Methods and Applications of (max, +) Linear Algebra // INRRIA Res. Rep. № 3088. 1997. - 231 p.
22. Блюмин С.Л. «Развитие понятия о числе»: некоторые научно-методические аспекты // Новые технологии в образовании: Междунар. электрон, науч. конф. Сб. науч. тр. - Воронеж: ВГПУ, 2001. - С.52-54.
23. Carlstrom J. Wheels - On Division by Zero // http://www.matematik.su.se/~jesper 2001.-47 p.
24. Setzer A. Wheels (draft) // http://www-compsci.swan.ac.uk/~csetzer/ 1997. - 9 p.
25. Англо-русский словарь математических терминов. - М.: Мир, 1994. - 416 с.
26. Общая алгебра / Под ред. Л.А. Скорнякова. Т.1.- М.: Наука, 1990.- 592 с.
27. Общая алгебра / Под ред. Л.А. Скорнякова. Т.2.- М.: Наука, 1991.- 480 с.
28. Белоусов В.Д. Основы теории квазигрупп и луп. - М.: Наука, 1967. - 111 с.
29. Бурбаки Н. Теория множеств. - М.: Мир, 1965. - 455 с.
30. Кон П. Универсальная алгебра. - М.: Мир, 1968. - 351 с.
31. Общая алгебра / Под общ. ред. Л.А. Скорнякова. Т. 1,2. - М.: Наука, 1990, 1991.-592, 480 с.
32. Литцман В. Великаны и карлики в мире чисел. - М.: ГИФМЛ, 1959. - 68 с.
33. Литвинов Г.Л., Маслов В.П., Соболевский А.Н. Идемпотентная математика и интервальный анализ. - Препринт. - М.: Междунар. Центр «Софус Ли», 1999. -28 с.

34. Seselja B., Tepavcevic A. Completion of ordered structures by cuts of fuzzy sets: an overview // Fuzzy Sets and Systems. - 2003. - No. 136. - P. 1-19.
35. Cignoli R., Dubuc E., Mundici D. Extending Stone duality to multisets and locally finite MV-algebras // Journal of Pure and Applied Algebra. - 2004. - Vol. 189. - No. 1-3.-P. 37-59.
36. Кнут Д. Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. - М.: Мир, 1977. -724 с.
37. Blyumin S., Golan J. One-sided complements and solutions of the equation aXb=c in semirings // International Journal of Mathematics and Mathematical Sciences. -2002. - Vol. 29. - No. 8. - P. 453-458
38.Golan J. Semirings and their Applications/J.Golan.-Dordrecht:Kluwer,1999.-285p.
39.Konstantinov M. On Properties of Sylvester and Lyapunov Operators/M. Konstantinov, V.Mehrmann, P.Petkov//Lin.Alg.Appl.-2000.-No.312.-P.35-71.
40.Nutt W. Unification in Monoidal Theories is Solving Linear Equations over
Semirings: RR-92-01 /W.Nutt.-Hamburg:DFKI, 1992.-57p.
41.Литвинов Г.Л. Идемпотентная математика/Г.Л.Литвинов, В.П.Маслов//
Воронеж. зимн. матем. школа «Современный анализ и егоприложения».Тез.докл.-Воронеж:ВГУ,2000.-С.20-22.
42. Блюмин С.Л. Регулярная (по Дж. фон Нейману) математика/С.Л.Блюмин//Воронеж, зимн. матем. школа «Современный анализ и его приложения».Тез.докл.-Воронеж:ВГУ,2000.-С.48-49.
43. Блюмин С.Л. «Линейные» соотношения над «бедными» алгебраическимиструктурами/С.Л.Блюмин//Междунар. науч. конф. «Нелинейный анализ ифункционально-дифференциальные уравнения».Тез.докл.-Воронеж:ВГУ,2000.-С.59-61.
44. Блюмин С.Л. Исследование и решение матричных уравнений над полукольцами/С.Л.Блюмин//Воронеж. зимн. матем. школа «Современные методы теории функций и смежные проблемы».Тез.докл.-Воронеж:ВГУ,2001.- С.44-46.
45. Блюмин С.Л. Формулы Клайна обобщенного обращения и регулярного дополнения блочных матриц над полукольцами/С.Л.Блюмин//Воронеж. весен. матем. школа «Современные методы в теории краевых задач. Понтрягинские чтения-ХП».Тез.докл.-Воронеж:ВГУ,2001.-С.27-28.
46. Blyumin S. On Some Operator Equations over Semirings/S.Blyumin//Int. Conf. on Functional Analysis in Ukr. Math. Congress-2001.Abstracts.-Kyiv:IMNANU,2001.- P.14.

47. Blyumin S. One-sided Complements and Solutions of the Equation aXb=c in Semirings/S.Blyumin, J.Golan//International Journal of Mathematics and Mathematical Sciences. - 2002. - Vol. 29. - No. 8. - P. 453-458.
48. Березин Ф. А. Метод вторичного квантования.— М.: Наука, 1965.—2-е изд.—М.: Наука, 1986.
49. Браттоли О., Робинсон Д. В. Операторные алгебры и квантовая статистическая механика.— М.: Мир, 1985.
50. В ей ль А. Основы теорпп чисел.—М.: Мир, 1972.
51. Владимиров В. С, В о л о в и ч И. В. Введение и суперанализ // Теорет. и мат. физика.— 1984.— Т. 59, № 1.— С. 3—27; Т. СО, № 2.— С. 169—198.
52. Гольфанд С. II., М а н и н 10. И. Методы гомологической алгебры. 1: Введение в теорию когомологий и производные категории.— М.: Наука, 1988.
53. Кириллов А. А. Элементы теории представлений.— М.: Наука, 1972.—2-е изд.—М.: Наука, 1978.
54. Коблиц Н. р-адическпе числа, р-адический анализ и дзета-функция.— М.: Мир, 1981.
55. Картье П. Сингулярные возмущения обыкновенных дифференциальных уравнений и нестандартный анализ // УМН.— 1984.— Т. 39, № 6.— С. 57—76; Нестандартный анализ и сингулярные возмущения обыкновенных дифференциальных уравнений // УМН.— 1984.— Т. 39, № 6.— С. 57—127.
56. Кириллов А. А., Клумова И. Н., Сосинский А. Г. Сюрреальные числа // Квант.— 1979.— № 11.— С. 2—9.
57. Л е й т е с Д. А. Введение в теорию супермногообразий // УМН.— 1980.- Т. 35.— № 1.— С. 3-57.
58 Манин Т.О. Калибровочные поля и комплексная геометрия.— М.: Наука, 1984.
58. Р е ш е т и х и и Н. 10., Т а х т а д ж я н Л. А., Ф а дд е е в Л. Д. Квантование групп Ли и алгебр Лп // Алгебра и анализ.—1989.—Т. 1,— № 1.— С. 178—206.
59. С л а в и о в А. А., Фаддеев Л. Д. Введшие в теорию калибровочных полей.— М.: Паука, 1978.
60. Успенский В. А. Что такое нестандартный анализ?— М.: Наука, 1987.
61. Итоги науки и техн. ВИНИТИ АН СССР Современные проблемы математики. Фундаментальные направления.
62. Х ь ю я м о л л е р Д. Расслоенные пространства.— М.: Мир, 1977.
63. Математическая энциклопедия. Т. 1—5.— М.: Советская

энциклопедия, 1982—1985.
64. *Боревич З. И., Шафаревич И. Р.* Теория чисел, — М.: Наука, 1985.
65. *Серр Ж.-П.* Курс арифметики, — М.: Мир, 1972.
66. Арифметические группы и автоморфные функции пер. с англ. и франц., М., 1969, с. 44-55.
67. Алгебраическая теория чисел, пер. с англ., М., 1969.
68. Итоги науки. Алгебра. Геометрия. Топология, т. 11, М., 1973, с. 5-37.

Научно-практическое издание

Кононюк Анатолий Ефимович

Обобщенная теория моделирования

Книга 2

Числа
как количественные оценки параметров моделей

Авторская редакция

Подписано в печать 25.07.2012 г.
Формат 60x84/16.
Усл. печ. л. 26,5. Тираж 300 экз.

Издатель и изготовитель:
Издательство «Освита Украины»
04214, г. Киев, ул. Героев Днепра, 63, к. 40
Свидетельство о внесении в Государственный реестр
издателей ДК №1957 от 23.04.2009 г.
Тел./факс (044) 411-4397; 237-5992
E-mail: osvita2005@ukr.net, www.rambook.ru