С. Б. КАТОК

p-адический анализ в сравнении с вещественным

Перевод с английского
П. А. Колгушкина

Москва
МЦНМО
2004

УДК 511.6 + 517.1
ББК 22.132 + 22.161
К29

Каток С. Б.

К29 p-адический анализ в сравнении с вещественным / Пер. с англ. П. А. Колгушкина. — М.: МЦНМО, 2004. — 112 с.: ил.

ISBN 5-94057-149-2

В брошюре излагаются основные сведения, связанные с p-адическим анализом: приводится определение p-адических чисел, изучается их топология, функции от p-адического аргумента. Подробно рассматриваются отличия от классического вещественного анализа.

Для студентов младших курсов физико-математических специальностей.

ББК 22.132 + 22.161

Перевод выполнен по изданию:
S. Katok, p-adic analysis in comparison with real // MASS selecta / Ed. by S. Katok, A. Sossinsky, and S. Tabachnikov. Providence: AMS, 2003. P. 11—87.

ISBN 5-94057-149-2

Оглавление

Предисловие

Эти заметки появились как результат курса «Действительный и p-адический анализ», который был прочитан автором по программе MASS в осеннем семестре 2000 г. Выбор темы был обусловлен как внутренней красотой предмета p-адического анализа, не вполне обычного для студентов младших курсов, так и возможностью сравнить этот предмет с более знакомым им вещественным аналогом.

У этого подхода есть несколько педагогических преимуществ. И действительные, и p-адические числа получаются из рациональных при помощи процедуры под названием пополнение (которая может быть применена к любому метрическому пространству), если использовать различные расстояния на множестве рациональных чисел: обычное евклидово расстояние для действительных чисел и новое p-адическое для p-адических, для произвольного простого числа p. Тот факт, что p-адическое расстояние удовлетворяет «сильному неравенству треугольника», является причиной многих удивительных свойств p-адических чисел, а также приводит к интересным отличиям от классического вещественного анализа, подобно тому как отрицание пятого постулата Евклида о параллельных прямых приводит к неевклидовой геометрии. С другой стороны, похожими оказываются утверждения, не зависящие от «сильного неравенства треугольника», и в этих случаях одно и то же доказательство работает и для вещественного, и для p-адического случая. Анализ отличий помогает студентам лучше понять доказательства в обоих случаях.

Хотя материал этих заметок описывается в нескольких как классических, так и недавних работах [1, 2, 4, 5, 6, 7, 8, 10], в них он или остается на сравнительно элементарном уровне с бóльшим акцентом на теоретико-числовых аспектах, или довольно быстро выходит на уровень, слишком сложный для студентов младших курсов. Мой собственный вклад состоял в отборе подходящего материала, в упрощении некоторых доказательств и изложении их в подходящем контексте.

Я также включила в этот курс несколько тем из вещественного анализа и элементарной топологии, которые обычно не изучаются студентами (вполне несвязные пространства и канторовы множества, точки разрыва отображений и теорему Бэра о категории, сюръективность изометрий компактных метрических пространств). Эти темы помогли студентам лучше понять вещественный анализ и связать вещественный и p-адический контекст. Стандартное описание этих тем можно найти в книге [9]. Основные понятия алгебры обсуждаются очень кратко, и читатель отсылается к любому стандартному учебнику по абстрактной алгебре, например к [3].

Курс сопровождался значительным количеством задач для самостоятельного решения (с акцентом на доказательства), которые присутствуют и в этих заметках. В частности, некоторые части доказательств из основного текста оставляются в качестве упражнений. Хотя эти упражнения могут затруднить непрерывное чтение, они помогают студентам глубже понять предмет и делают эти заметки вполне подходящими для самостоятельного изучения.

Помимо решения задач студентам было предложено сделать доклады на дополнительные темы. Доклады, некоторые из которых были на довольно высоком уровне, включали следующие: «Конечные расширения p-адических чисел и p-адические окружности»; «Изометрии на множестве целых p-адических чисел»; «p-адический соленоид»; «X-адическая норма на пространстве степенных рядов»; «Функция Сигнум»; «Разбиения на треугольники равной площади»; «Евклидовы модели множества целых p-адических чисел»; «Построение графической модели кривой Пеано с помощью канторова множества»; «Модифицированный гармонический ряд»; «О диагональных кубических уравнениях».

Глава 1

Арифметика p-адических чисел

Цель первой части этих лекций — ввести главный объект: *поле p-адических чисел* $\mathbb{Q}_p$, определенное для каждого простого числа p.

Так же как и поле действительных чисел $\mathbb{R}$, поле $\mathbb{Q}_p$ может быть построено из поля рациональных чисел $\mathbb{Q}$ как *пополнение* по некоторой норме. Эта норма зависит от простого числа p и кардинально отличается от стандартной евклидовой нормы, которая используется для определения множества $\mathbb{R}$. Однако в обоих случаях результатом пополнения является *нормированное поле* ($\mathbb{R}$ и $\mathbb{Q}_p$); это общее понятие детально изучается в § 2. Но сначала (§ 1) мы напоминаем, что представляет собой процедура пополнения в более знакомом случае действительных чисел (от $\mathbb{Q}$ к $\mathbb{R}$), и только потом переходим к обобщению на произвольные нормированные поля (§ 3).

После этих предварительных замечаний мы переходим к центральному разделу части 1 (§ 4), где строится поле $\mathbb{Q}_p$.

В §§ 5—8 рассматриваются алгебраические и структурные свойства p-адических чисел. Там, а также и в последующих частях, мы будем постоянно сравнивать $\mathbb{Q}_p$ и $\mathbb{R}$, подчеркивая как их сходства, так и различия. Наконец, в §§ 9, 10 обсуждаются дополнительные вопросы, напрямую не связанные с основным содержанием курса.

§ 1. От $\mathbb{Q}$ к $\mathbb{R}$; понятие пополнения

Действительные числа (их множество обозначается $\mathbb{R}$), получаются из рациональных с помощью процедуры, которая называется *пополнением*. Эту процедуру можно применить к любому *метрическому пространству*, т. е. пространству M с функцией расстояния d. Напомним, что функция

$$d: M \times M \to \mathbb{R},$$

определенная на множестве всех упорядоченных пар (x, y) элементов непустого множества M, называется *расстоянием*, если она обладает следующими тремя свойствами:

1) $d(x, y) \geqslant 0$; $d(x, y) = 0$ тогда и только тогда, когда $x = y$;
2) $d(x, y) = d(y, x)$ для любых $x, y \in M$;
3) $d(x, y) \leqslant d(x, z) + d(z, y)$ для любых $x, y, z \in M$.

Последовательность $\{r_n\}$ точек метрического пространства M называется *последовательностью Коши*, если для любого $\varepsilon > 0$ существует такое натуральное число N, что если $n, m > N$, то $d(r_n, r_m) < \varepsilon$. Если любая последовательность Коши из M имеет предел в M, то M называется *полным метрическим пространством*. Если пространство M не полное, то существует такое метрическое пространство $\overline{M}$, что

1) $\overline{M}$ полное;

2) $\overline{M}$ содержит подмножество $\overline{M}_0$, изометричное пространству M;

3) $\overline{M}_0$ всюду плотно в $\overline{M}$ (т. е. каждая точка из $\overline{M}$ является предельной точкой множества $\overline{M}_0$).

Доказательство представляет собой явную конструкцию пополнения $\overline{M}$. Его элементы — это классы эквивалентности последовательностей Коши из M (две последовательности Коши x_n и y_n называются *эквивалентными*, если $d(x_n, y_n) \to 0$). Подробности приведены ниже в теореме 3.4, где рассматривается частный случай метрических пространств, называемых *нормированными полями*, включающий $\mathbb{Q}$.

Для $M = \mathbb{Q}$ мы имеем обычное евклидово расстояние между рациональными числами:

$$d(r_1, r_2) = |r_1 - r_2|. \tag{1.1}$$

Заметим, что это расстояние «получается» из евклидовой нормы на $\mathbb{Q}$, которая представляет собой *абсолютную величину* и является обычным расстоянием на «числовой оси».

Другое описание пополнения множества $\mathbb{Q}$, приводящее к $\mathbb{R}$, более известное и не такое абстрактное, основывается на бесконечных десятичных дробях. Рациональные числа характеризуются тем, что их представления в виде бесконечной десятичной дроби являются периодическими (упражнение 1). С другой стороны, любая бесконечная десятичная дробь представляет некоторую точку на «числовой оси». Таким образом, удобно отождествить *действительные числа* с бесконечными десятичными дробями. Каждое положительное действительное число a может быть записано как десятичная дробь

$$a = \sum_{k=m}^{\infty} a_k 10^{-k}, \tag{1.2}$$

где m — некоторое целое число и коэффициенты или *цифры* a_k принимают значения

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

Это представление единственно всегда, кроме случая, когда $a_k = 0$ для всех $k > n$, в этом случае у числа a есть другое представление: $a'_n = a_n - 1$, $a'_k = 9$ для $k > n$ и $a'_k = a_k$ для $k < n$.

Несложно построить последовательность Коши, состоящую из рациональных чисел и не имеющую предела в $\mathbb{Q}$:

$$0{,}1,\ \ 0{,}1011,\ \ 0{,}10110111,\ \ 0{,}1011011101111,\ \ldots$$

С другой стороны, каждый класс эквивалентности последовательностей Коши, состоящих из рациональных чисел, содержит в качестве представителя представителя, последовательность частичных сумм ряда вида (1.2), пределом которой является бесконечная десятичная дробь (упражнение 2), причем это же верно для любой последовательности Коши бесконечных десятичных дробей. Иными словами, множество действительных чисел полно относительно евклидова расстояния (упражнение 3), и построение действительных чисел с помощью бесконечных десятичных дробей эквивалентно процедуре пополнения относительно евклидова расстояния. Представление (1.2) можно обобщить на *представления бесконечными дробями по основанию* g, где g — произвольное натуральное число, большее или равное 2; таким образом,

$$a = \sum_{k=m}^{\infty} a_k g^{-k},$$

где коэффициенты a_k принимают значения из множества $\{0, 1, \ldots, g-1\}$. Заметим, что показатели $-k$ уменьшаются и стремятся к $-\infty$.

Практически пополнение часто строится с помощью следующей конструкции.

Теорема 1.1. *Пусть M — полное метрическое пространство и X — подмножество в M. Тогда X полно в том и только в том случае, когда оно замкнуто в M. В частности, замыкание подмножества X в M можно рассматривать как пополнение подмножества X.*

Пример 1.2. Пополнение интервала (a, b) относительно обычного евклидова расстояния есть отрезок $[a, b]$, замыкание интервала (a, b) в $\mathbb{R}$.

Другие примеры представлены в упражнении 4.

Упражнения

1. Докажите, что число рационально тогда и только тогда, когда представляющая его бесконечная десятичная дробь является периодической.

2. Докажите, что для любой последовательности Коши рациональных чисел относительно евклидова расстояния существует эквивалентная ей последовательность частичных сумм ряда вида (1.2).

3. Используя представление действительных чисел в виде бесконечных десятичных дробей, докажите, что множество действительных чисел полно относительно евклидова расстояния, т. е.что любая последовательность Коши, состоящая из действительных чисел, имеет предел.

4. Докажите, что следующие метрические пространства не являются полными, и постройте их пополнения:

1) $\mathbb{R}$ с расстоянием $d(x, y) = |\operatorname{arctg} x - \operatorname{arctg} y|$;

2) $\mathbb{R}$ с расстоянием $d(x, y) = |e^x - e^y|$.

5. Докажите, что метрическое пространство полно тогда и только тогда, когда любая последовательность вложенных замкнутых шаров $\{B_n\}$, $B_1 \supset B_2 \supset B_3 \supset \ldots$, радиусы которых стремятся к нулю, имеет единственную общую точку.

§ 2. Нормированные поля

Рациональные и действительные числа являются основными примерами алгебраической структуры под названием поле. *Поле* F — это множество с двумя бинарными операциями, которые обычно называются *сложением* и *умножением* и которые удовлетворяют основным свойствам этих операций для чисел. Именно,

1) $a + b = b + a$ для любых $a, b \in F$ (коммутативность сложения);

2) $a + (b + c) = (a + b) + c$ для любых $a, b, c \in F$ (ассоциативность сложения);

3) существует такой элемент $0 \in F$, что $0 + a = a$ для любого $a \in F$ (существование нуля);

4) для любого элемента $a \in F$ существует такой элемент $-a \in F$, что $a + (-a) = 0$ (существование обратного по сложению);

5) $a \cdot b = b \cdot a$ для любых $a, b \in F$ (коммутативность умножения);

6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ для любых $a, b, c \in F$ (ассоциативность умножения);

7) существует такой элемент $1 \in F$, что $1 \cdot a = a$ для любого $a \in F^\times = F \setminus 0$ (существование единицы);

8) для любого элемента $a \in F^\times$ существует такой элемент $a^{-1} \in F^\times$, что $a \cdot a^{-1} = 1$ (существование обратного по умножению);

9) $a \cdot (b + c) = a \cdot b + a \cdot c$ для любых $a, b, c \in F$ (дистрибутивность);

10) $0 \neq 1$.

Алгебраическая структура с одной бинарной операцией, удовлетворяющей свойствам 1)—4), называется *абелевой* (*или коммутативной*) *группой*. Соответственно множество F с операцией сложения называется *аддитивной группой* поля F, а множество $F^\times$ с операцией умножения называется *мультипликативной группой* поля F. Важным свойством поля является то, что оно не содержит *делителей нуля*, т. е. таких элементов $a, b \in F^\times$, что $a \cdot b = 0$ (см. упражнение 6).

Определение 2.1. Пусть F является полем. *Нормой* на F называется отображение из F во множество неотрицательных действитель-

ных чисел, которое обозначается $\|\cdot\|$ и удовлетворяет следующим свойствам:

1) $\|x\| = 0$ тогда и только тогда, когда $x = 0$;

2) $\|xy\| = \|x\|\|y\|$ для любых $x, y \in F$;

3) $\|x + y\| \leqslant \|x\| + \|y\|$ для любых $x, y \in F$ (*неравенство треугольника*).

Норма называется *тривиальной*, если $\|0\| = 0$ и $\|x\| = 1$ для всех $x \neq 0$.

Заметим, что для любого $n \in \mathbb{N}$ мы имеем

$$n \cdot 1 := \underbrace{1 + \ldots + 1}_{n} \in F.$$

Мы будем обозначать этот элемент тем же самым символом n, что и соответствующее натуральное число.

Предложение 2.2. *Для любых $x, y \in F$ справедливы следующие утверждения*:

a) $\|1\| = \|-1\| = 1$;

b) $\|x\| = \|-x\|$;

c) $\|x \pm y\| \geqslant |\|x\| - \|y\||$;

d) $\|x - y\| \leqslant \|x\| + \|y\|$;

e) $\|x/y\| = \|x\|/\|y\|$;

f) $\|n\| \leqslant n$ *для любого* $n \in \mathbb{N}$.

Доказательство.

a) Мы имеем $\|1\| = \|(\pm 1) \cdot (\pm 1)\| = \|\pm 1\|^2 \Rightarrow \|\pm 1\| = 1$.

b) Мы имеем $\| - x\| = \|(-1) \cdot x\| = 1 \cdot \|x\|$.

c) Утверждение следует из п. b) и неравенства треугольника для нормы (см. Упражнение 7).

d) Утверждение следует из п. b) и неравенства треугольника.

e) Утверждение следует из п. a) и свойства 2) нормы.

f) Утверждение следует по индукции из п. a) и неравенства треугольника. □

Пусть $d(x, y) = \|x - y\|$. Из определения 2.1 и предложения 2.2 немедленно следует, что d является функцией расстояния; в самом деле, из свойства 1) определения 2.1 следует, что $d(x, y) = 0$ тогда и только тогда, когда $x = y$, симметричность следует из утверждения 2.2 b), а неравенство треугольника из утверждения 2.2 d). В такой ситуации мы будем говорить, что расстояние *индуцировано* нормой $\|\cdot\|$, и будем рассматривать $(F, \|\cdot\|)$ как метрическое пространство.

Определение 2.3. Говорят, что последовательность $\{a_n\}$ элементов из F

1) *ограничена*, если существует такая константа $C > 0$, что

$$\|a_n\| \leqslant C \quad \text{для любого } n;$$

2) *является бесконечно малой*, если

$$\lim_{n\to\infty} \|a_n\| = 0,$$

т. е. для любого $\varepsilon > 0$ существует такое N, что для всех $n > N$ выполняется неравенство $\|a_n\| < \varepsilon$;

3) является *последовательностью Коши*, если

$$\lim_{n,m\to\infty} \|a_n - a_m\| = 0,$$

т. е. для любого $\varepsilon > 0$ существует такое N, что для всех n, $m > N$ выполняется неравенство $\|a_n - a_m\| < \varepsilon$;

4) *сходится* к $a \in F$ (мы пишем $a = \lim\limits_{n\to\infty} a_n$), если

$$\lim_{n\to\infty} \|a_n - a\| = 0,$$

т. е. для любого $\varepsilon > 0$ существует такое N, что для всех $n > N$ выполняется неравенство $\|a_n - a\| < \varepsilon$.

Из определения следует, что любая бесконечно малая последовательность сходится к 0, а из неравенства треугольника следует, что любая сходящаяся последовательность является последовательностью Коши: пусть $\lim\limits_{n\to\infty} a_n = a$, тогда

$$\|a_n - a_m\| = \|a_n - a + a - a_m\| \leqslant \|a_n - a\| + \|a - a_m\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

для n, $m > N$, где N выбран из определения предела для $\varepsilon/2$. В частности, каждая бесконечно малая последовательность является последовательностью Коши. Свойства, приведенные ниже, доказываются такими же стандартными рассуждениями.

1. Каждая последовательность Коши ограничена.

2. Пусть $\{a_n\}$ — последовательность Коши и $\{n_1, n_2, \ldots\}$ — возрастающая последовательность натуральных чисел. Если подпоследовательность $a_{n_1}, a_{n_2}, \ldots$ бесконечно малая, то и сама последовательность $\{a_n\}$ бесконечно мала.

3. Если $\{a_n\}$ и $\{b_n\}$ — бесконечно малые последовательности, тогда последовательность $\{a_n \pm b_n\}$ также бесконечно мала. Если последовательность $\{a_n\}$ бесконечно мала, а $\{b_n\}$ ограничена, то последовательность $\{a_n b_n\}$ бесконечно мала.

Следующее простое утверждение часто бывает полезно.

Предложение 2.4. *Неравенство* $\|x\| < 1$ *выполняется тогда и только тогда, когда* $\lim\limits_{n\to\infty} x^n = 0$.

Доказательство. Пусть $\|x\| < 1$. Так как $\|x^n\| = \|x\|^n$, мы получаем

$$\lim_{n\to\infty} \|x^n\| = 0,$$

т. е. $\lim\limits_{n\to\infty} x^n = 0$. Наоборот, если $\|x\| \geqslant 1$, то для всех положительных n имеем $\|x^n\| \geqslant 1$ и, таким образом, $0 \neq \lim\limits_{n\to\infty} x^n$. □

Определение 2.5. Будем говорить, что две метрики d_1 и d_2 на F *эквивалентны*, если любая последовательность является последовательностью Коши в метрике d_1 в том и только в том случае, когда она является последовательностью Коши в метрике d_2. Будем говорить, что две нормы $\|\cdot\|_1$ и $\|\cdot\|_2$ эквивалентны ($\|\cdot\|_1 \sim \|\cdot\|_2$), если они индуцируют эквивалентные метрики.

Предложение 2.6. *Пусть $\|\cdot\|_1$ и $\|\cdot\|_2$ — две нормы на поле F. Для того, чтобы эти нормы были эквивалентны необходимо и достаточно существование такого положительного действительного числа α, что*

$$\|x\|_2 = \|x\|_1^{\alpha} \quad \textit{для любого } x \in F. \tag{2.1}$$

Доказательство. Пусть $\|\cdot\|_1 \sim \|\cdot\|_2$. Если норма $\|\cdot\|_1$ тривиальна, то согласно упражнению 9 норма $\|\cdot\|_2$ также тривиальна и следовательно, равенство (2.1) выполнено для любого α.

Если норма $\|\cdot\|_1$ нетривиальна, то можно выбрать такой элемент $a \in F$, что $\|a\|_1 \neq 1$. Заменяя, если надо, a на $1/a$, можно считать, что $\|a\|_1 < 1$. Положим

$$\alpha = \frac{\log\|a\|_2}{\log\|a\|_1}.$$

Так как нормы эквивалентны, из упражнения 10 следует, что $\|a\|_2 < 1$, значит, оба логарифма отрицательны и $\alpha > 0$.

Покажем, что число α удовлетворяет условию (2.1). Рассмотрим сначала такой $x \in F$, что $\|x\|_1 < 1$; случаи $\|x\|_1 > 1$ и $\|x\|_1 = 1$ будут следовать из упражнения 10. Рассмотрим множество

$$S = \{r = m/n\colon m,\ n \in \mathbb{N},\ \|x\|_1^r < \|a\|_1\}. \tag{2.2}$$

Для любого $r \in S$ имеем $\|x\|_1^m < \|a\|_1^n$, поэтому $\left\|\dfrac{x^m}{a^n}\right\|_1 < 1$. Тогда из упражнения 10 получаем

$$\left\|\frac{x^m}{a^n}\right\|_2 < 1,$$

поэтому $\|x\|_2^m < \|a\|_2^n$ и $\|x\|_2^r < \|a\|_2$. Поменяв местами $\|\cdot\|_1$ и $\|\cdot\|_2$ и повторив то же самое рассуждение, мы видим, что

$$S = \{r = m/n\colon m,\ n \in \mathbb{N},\ \|x\|_2^r < \|a\|_2\}. \tag{2.3}$$

Логарифмируя, можно переписать условия (2.2) и (2.3) следующим образом:

$$r > \frac{\log\|a\|_1}{\log\|x\|_1}, \qquad r > \frac{\log\|a\|_2}{\log\|x\|_2}, \tag{2.4}$$

так как все логарифмы, присутствующие в этих формулах, отрицательны. Но тогда мы получаем

$$\frac{\log\|a\|_1}{\log\|x\|_1} = \frac{\log\|a\|_2}{\log\|x\|_2},$$

потому что в противном случае между этими двумя числами нашлось бы какое-то рациональное число r и было бы выполнено только одно из условий (2.4). Таким образом,

$$\frac{\log\|x\|_2}{\log\|x\|_1} = \frac{\log\|a\|_2}{\log\|a\|_1} = \alpha,$$

что и требовалось доказать. □

Теперь мы опишем все нормы на $\mathbb{Q}$, эквивалентные абсолютному значению $|\cdot|$.

Предложение 2.7. *Функция* $\|x\| = |x|^\alpha$, $\alpha > 0$, *является нормой на* $\mathbb{Q}$ *тогда и только тогда, когда* $\alpha \leqslant 1$. *В этом случае она эквивалентна норме* $|\cdot|$.

Доказательство. Пусть $\alpha \leqslant 1$. Первые два свойства нормы очевидны, поэтому нужно проверить только неравенство треугольника. Предположим, что $|y| \leqslant |x|$. Тогда

$$|x+y|^\alpha \leqslant (|x|+|y|)^\alpha = |x|^\alpha\left(1+\frac{|y|}{|x|}\right)^\alpha \leqslant$$
$$\leqslant |x|^\alpha\left(1+\frac{|y|}{|x|}\right) \leqslant |x|^\alpha\left(1+\frac{|y|^\alpha}{|x|^\alpha}\right) = |x|^\alpha + |y|^\alpha.$$

Первое неравенство следует из того, что $t^\alpha \leqslant t$, если $t \geqslant 1$, а второе — из того, что $t^\alpha \geqslant t$, если $0 \leqslant t \leqslant 1$.

С другой стороны, если $\alpha > 1$, то неравенство треугольника не выполняется: например, $|1+1|^\alpha = 2^\alpha > |1|^\alpha + |1|^\alpha = 2$. □

Определение 2.8. Норма называется *неархимедовой*, если для всех x и y выполнено неравенство

$$\|x+y\| \leqslant \max(\|x\|, \|y\|).$$

Замечание 2.9. Очевидно, что из неархимедова свойства нормы следует неравенство треугольника. Мы будем называть это свойство *сильным неравенством треугольника*.

Расстояние, индуцированное неархимедовой нормой, называется *ультраметрикой*. Вместо неравенства треугольника для обычной функции расстояния

$$d(x, z) \leqslant d(x, y) + d(y, z),$$

выполняется сильное неравенство треугольника

$$d(x, z) \leqslant \max(d(x, y), d(y, z)).$$

Соответствующие метрические пространства называются *ультраметрическими пространствами*.

Следующая теорема дает необходимое и достаточное условие того, чтобы норма была неархимедовой.

Предложение 2.10. *Следующие утверждения эквивалентны*:

a) *норма* $\|\cdot\|$ *неархимедова*;

b) $\|n\| \leqslant 1$ *для любого целого числа* n.

Доказательство. a) $\Rightarrow$ b). Докажем это по индукции.

База индукции. Очевидно, что $\|1\| = 1 \leqslant 1$.

Шаг индукции. Пусть $\|k\| \leqslant 1$ для всех $k \in \{1, \ldots, n-1\}$; докажем, что $\|n\| \leqslant 1$.

Заметим, что $\|n\| = \|(n-1)+1\| \leqslant \max\{\|n-1\|, 1\} = 1$.

Из неравенства $\|1\| = 1 \leqslant 1$ и предположения индукции получаем $\|n\| \leqslant 1$ для всех $n \in \mathbb{N}$. Так как $\|-n\| = \|n\|$, мы заключаем, что $\|n\| \leqslant 1$ для всех $n \in \mathbb{Z}$.

b) $\Rightarrow$ a). Имеем

$$\|x+y\|^n = \|(x+y)^n\| = \left\|\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\right\| \leqslant \sum_{k=0}^{n}\left\|\binom{n}{k}\right\|\|x\|^k\|y\|^{n-k} \leqslant$$

$$\leqslant \sum_{k=0}^{n}\|x\|^k\|y\|^{n-k} \leqslant (n+1)[\max(\|x\|, \|y\|)]^n.$$

Поэтому для каждого натурального числа n выполняется неравенство

$$\|x+y\| \leqslant \sqrt[n]{n+1}\max(\|x\|, \|y\|).$$

Устремляя n к ∞, получаем

$$\|x+y\| \leqslant \max(\|x\|, \|y\|).$$

Здесь мы пользовались тем, что $\binom{n}{k}$ — целое число, и хорошо известным пределом

$$\lim_{n\to\infty}\sqrt[n]{n+1} = 1. \qquad \square$$

Это утверждение помогает объяснить разницу между архимедовыми и неархимедовыми нормами. Его можно переформулировать следующим образом: норма является архимедовой, если она обладает *свойством Архимеда*: *для данных* $x, y \in F$, $x \neq 0$, *существует такое натуральное число* n, *что* $\|nx\| > \|y\|$.

Легко видеть, что свойство Архимеда эквивалентно существованию целых чисел, имеющих сколь угодно большую норму:

$$\sup\{\|n\| : n \in \mathbb{Z}\} = +\infty. \tag{2.5}$$

Мы оставляем читателю проверить, что норма архимедова (т. е. не является неархимедовой) тогда и только тогда, когда выполняется условие (2.5) (упражнение 11).

Неархимедово свойство имеет и другие удивительные следствия.

Предложение 2.11. *Если элементы a и x неархимедова поля F удовлетворяют неравенству $\|x - a\| < \|a\|$, то $\|x\| = \|a\|$.*

Доказательство. Согласно сильному неравенству треугольника

$$\|x\| = \|x - a + a\| \leqslant \max(\|x - a\|, \|a\|) = \|a\|.$$

С другой стороны,

$$\|a\| = \|a - x + x\| \leqslant \max(\|x - a\|, \|x\|).$$

Если бы выполнялось неравенство $\|x - a\| > \|x\|$, то получилось бы, что $\|a\| \leqslant \|x - a\|$, а это противоречит условию. Значит, $\|x - a\| \leqslant \|x\|$ и $\|a\| \leqslant \|x\|$. Поэтому $\|x\| = \|a\|$, что и завершает доказательство. □

Это утверждение можно сформулировать в геометрических терминах следующим образом: *любой треугольник в ультраметрическом пространстве является равнобедренным, причем длина основания не превосходит длин боковых сторон.*

Доказательство следующего удивительного свойства мы оставляем читателю (упражнение 12).

Предложение 2.12. *Если норма $\|\cdot\|$ на поле F неархимедова, то любая точка замкнутого шара $\overline{B(a, r)} = \{x: \|x - a\| \leqslant r\}$ в F является его центром.*

Завершая этот параграф, покажем, что архимедова и неархимедова нормы не могут быть эквивалентны.

Предложение 2.13. *Две эквивалентные нормы ($\|\cdot\|_1 \sim \|\cdot\|_2$) на поле F либо обе архимедовы, либо обе неархимедовы.*

Доказательство. Из упражнения 10 следует, что если $\|\cdot\|_1 \sim \|\cdot\|_2$, то для любого целого n имеем $\|n\|_1 > 1$ тогда и только тогда, когда $\|n\|_2 > 1$. Отсюда и из предложения 2.10 следует, что либо обе нормы неархимедовы, либо обе архимедовы. □

Упражнения

6. Докажите, что поле не содержит делителей нуля.

7. Используя неравенство треугольника для нормы на поле F (п. 3 определения 2.1), докажите, что

$$\big|\|x\| - \|y\|\big| \leqslant \|x \pm y\| \quad \text{для любых } x, y \in F.$$

8. Докажите, что в любом нормированном поле выполняются следующие утверждения:

1) каждая последовательность Коши ограничена;

2) пусть $\{a_n\}$ — последовательность Коши и $\{n_1, n_2, \ldots\}$ — возрастающая последовательность натуральных чисел, тогда если подпоследовательность $a_{n_1}, a_{n_2}, \ldots$ бесконечно малая, то и сама последовательность $\{a_n\}$ бесконечно мала;

3) если последовательности $\{a_n\}$ и $\{b_n\}$ бесконечно малы, то и последовательность $\{a_n \pm b_n\}$ бесконечно мала: если последовательность $\{a_n\}$ бесконечно мала, а последовательность $\{b_n\}$ ограничена, то последовательность $\{a_n b_n\}$ бесконечно мала.

9. Докажите, что если $\|\cdot\|_1 \sim \|\cdot\|_2$ и норма $\|\cdot\|_1$ тривиальна, то норма $\|\cdot\|_2$ также тривиальна.

10. Докажите, что если $\|\cdot\|_1 \sim \|\cdot\|_2$, то $\|x\|_1 < 1$ тогда и только тогда, когда $\|x\|_2 < 1$; $\|x\|_1 > 1$ тогда и только тогда, когда $\|x\|_2 > 1$, и $\|x\|_1 = 1$ тогда и только тогда, когда $\|x\|_2 = 1$.

11. Докажите, что норма $\|\cdot\|$ архимедова тогда и только тогда, когда

$$\sup\{\|n\| : n \in \mathbb{Z}\} = +\infty.$$

12. Докажите, что если норма $\|\cdot\|$ на поле F неархимедова, то любая точка замкнутого шара $\overline{B(a, r)} = \{x : \|x - a\| \leqslant r\}$ в F является его центром (и то же самое для открытого шара $B(a, r) = \{x : \|x - a\| < r\}$).

13. Докажите, что если норма $\|\cdot\|$ неархимедова, то $\|\cdot\|^\alpha$ также неархимедова норма для любого $\alpha > 0$. (Сравните с предложением 2.7 для евклидова абсолютного значения на $\mathbb{Q}$.)

§ 3. Построение пополнения нормированного поля

В этом параграфе мы, исходя из произвольного нормированного поля F (не обязательно полного по его норме $\|\cdot\|$), построим другое поле $\bar{F}$, содержащее F, и снабдим его нормой (индуцированной нормой $\|\cdot\|$ на F) таким образом, что поле $\bar{F}$ будет *полным* нормированным полем.

Как мы уже видели (§ 1), в случае рациональных чисел с обычной (евклидовой) нормой процедура пополнения приводит к полю действительных чисел $\mathbb{R}$. Ту же самую процедуру мы позже (см. § 4) применим к полю $\mathbb{Q}$, снабженному совершенно другой нормой, и в результате получим p-адические числа. Главную роль в процедуре пополнения будут играть последовательности Коши: именно классы эквивалентных последовательностей Коши будут объявлены элементами поля $\bar{F}$. Поэтому мы начнем с обсуждения последовательностей Коши, состоящих из элементов произвольного нормированного поля F.

Последовательности Коши можно складывать, вычитать и перемножать (упражнение 14), поэтому множество всех последовательностей

Коши в $(F, \|\cdot\|)$, обозначаемое $\{F\}$, является коммутативным кольцом. Единичным элементом по сложению является последовательность

$$\bar{0} = \{0, 0, 0, \ldots\},$$

а единичным элементом по умножению является последовательность

$$\bar{1} = \{1, 1, 1, \ldots\}.$$

Ясно, что множество $\{F\}$ не является полем, так как оно содержит делители нуля:

$$\{1, 0, 0, \ldots\}\{0, 1, 0, 0, \ldots\} = \bar{0}.$$

Для каждого $a \in F$ последовательность

$$\bar{a} = \{a, a, a \ldots\}$$

лежит в $\{F\}$. Следовательно, $\{F\}$ содержит подкольцо, изоморфное полю F. Рассмотрим множество P всех бесконечно малых последовательностей. Очевидно, что P является подмножеством множества $\{F\}$. Более того, P является *идеалом* в $\{F\}$ (т. е. таким подкольцом, что для всех $p \in P$ и для всех $a \in F$ выполнено включение $ap \in P$). В самом деле, если последовательности $\{a_n\}$ и $\{b_n\}$ лежат в P, то и последовательность $\{a_n \pm b_n\}$ также лежит в P. И если последовательность $\{a_n\}$ лежит в P, а последовательность $\{b_n\}$ ограничена (в частности, является последовательностью Коши), то $\{a_n b_n\}$ также лежит в P (упражнение 8 (3)).

Положим $\bar{F} = \{F\}/P$. Элементами этого множества являются классы эквивалентных последовательностей Коши из $(F, \|\cdot\|)$, причем две последовательности *эквивалентны*, если их разность есть бесконечно малая последовательность. Заметим, что постоянные последовательности

$$\bar{a} = \{a, a, a, \ldots\},$$

где $a \in F$, принадлежат разным классам в $\bar{F}$ для разных a. Будем обозначать класс, содержащий последовательность $\{a_n\}$, через (a_n); (a_n) является элементом множества $\bar{F}$. Будем рассматривать F как подмножество множества $\bar{F}$, отождествляя $a \in F$ с $(\bar{a}) \in \bar{F}$.

Теорема 3.1. *Множество $\bar{F}$ является полем.*

Доказательство. Определим операции на $\bar{F}$ следующим образом: если $\{a_n\} \in A$, а $\{b_n\} \in B$, то $A + B = (a_n + b_n)$ и $AB = (a_n \cdot b_n)$. Из упражнения 15 следует, что эти операции не зависят от выбора представителей. Легко проверить, что множество $\bar{F}$ с такими операциями является коммутативным кольцом с единичным элементом по сложению $(\bar{0})$ и единичным элементом по умножению $(\bar{1})$. Докажем, что $\bar{F}$ является полем. Пусть A —

класс эквивалентности из $\bar{F}$, отличный от нулевого класса $(\bar{0}) = P$. Пусть также $\{a_n\}$ — любая последовательность Коши из A. Так как последовательность $\{a_n\}$ не является бесконечно малой, найдутся такие положительные числа c и N, что

$$\|a_n\| > c \quad \text{для любого } n \geqslant N.$$

Рассмотрим последовательность $\{a_n^*\}$, определенную формулой

$$a_n^* = \begin{cases} 0, & \text{если } 1 \leqslant n \leqslant N-1, \\ 1/a_n, & \text{если } n \geqslant N. \end{cases}$$

Мы утверждаем, что эта последовательность является последовательностью Коши. Действительно, если $n, m \geqslant N$, то

$$0 \leqslant \|a_m^* - a_n^*\| = \left\| \frac{1}{a_m} - \frac{1}{a_n} \right\| = \frac{\|a_m - a_n\|}{\|a_m\| \cdot \|a_n\|} \leqslant c^{-2}\|a_m - a_n\|,$$

отсюда и вытекает нужное нам утверждение, так как $\{a_n\}$ является последовательностью Коши. Обозначим класс эквивалентности, содержащий последовательность $\{a_n^*\}$, через A^{-1}. Тогда

$$\{a_n\}\{a_n^*\} = \{\underbrace{0, \ldots, 0}_{N-1}, 1, 1, 1 \ldots\},$$

причем разность последовательности Коши в правой части и $\bar{1}$ есть бесконечно малая последовательность

$$\{\underbrace{-1, \ldots, -1}_{N-1}, 0, 0, 0 \ldots\}.$$

Таким образом, $AA^{-1} = (\bar{1})$, что доказывает, что $\bar{F}$ является полем. □

Теперь мы продолжим норму $\|\cdot\|$ с F на $\bar{F}$.

Определение 3.2. Для любого $A \in \bar{F}$ положим

$$\|A\| = \lim_{n\to\infty} \|a_n\|,$$

где $\{a_n\}$ — любая последовательность Коши из A.

Для того чтобы убедиться в том, что эта норма определена корректно, мы должны показать, что этот предел существует и не зависит от выбора последовательности Коши $\{a_n\}$ из A. Из упражнения 7 имеем

$$\big|\|a_n\| - \|a_m\|\big| \leqslant \|a_n - a_m\|,$$

откуда следует, что последовательность действительных чисел $\{\|a_n\|\}$ является последовательностью Коши относительно абсолютного значения.

Так как множество действительных чисел $\mathbb{R}$ полно, предел, определяющий норму $\|\cdot\|$, существует. Возьмем другую последовательность $\{a'_n\} \in A$. Из того же самого неравенства имеем

$$0 \leqslant \lim_{n\to\infty} \big|\|a_n\| - \|a'_n\|\big| \leqslant \lim_{n\to\infty} \|a_n - a'_n\| = 0,$$

отсюда $\lim\limits_{n\to\infty} \|a_n\| = \lim\limits_{n\to\infty} \|a'_n\|$.

Предложение 3.3. *Функция $\|\cdot\|$ является нормой на $\bar{F}$.*

Доказательство. Нужно проверить три свойства из определения 2.1.

1) Если $A = (\bar{0})$, тогда последовательность $\{a_n\}$ бесконечно мала и $\|A\| = 0$. Если же $A \neq (\bar{0})$, то найдутся такие положительные числа c и N, что для всех $n \geqslant N$ имеем $\|a_n\| \geqslant c > 0$. Отсюда $\|A\| > 0$.

2) По свойствам вещественных пределов

$$\|AB\| = \lim_{n\to\infty} \|a_n b_n\| = \lim_{n\to\infty} \|a_n\|\|b_n\| = \lim_{n\to\infty} \|a_n\| \lim_{n\to\infty} \|b_n\| = \|A\|\|B\|.$$

3) Аналогично получаем $\|A + B\| \leqslant \|A\| + \|B\|$. □

Теперь мы можем определить ограниченные и бесконечно малые последовательности, а также последовательности Коши по норме $\|\cdot\|$ в $\bar{F}$.

Теорема 3.4. *Поле $\bar{F}$ полно по норме $\|\cdot\|$, и F является всюду плотным подмножеством множества $\bar{F}$.*

Доказательство. Докажем сначала второе утверждение. Пусть $A \in \bar{F}$ и $\{a_m\}$ — последовательность Коши элементов поля F, представляющая A. Для каждого фиксированного натурального числа n рассмотрим постоянную последовательность $\bar{a}_n$. Тогда последовательность $\{a_m - a_n\}_{m=1}^{\infty}$ представляет $A - (\bar{a}_n)$. Из того, что $\{a_n\}$ является последовательностью Коши, получаем

$$\lim_{n\to\infty} \|A - (\bar{a}_n)\| = \lim_{n,m\to\infty} \|a_m - a_n\| = 0. \tag{3.1}$$

Это доказывает, что множество F всюду плотно в $\bar{F}$. Теперь предположим, что $\{A_n\} = \{A_1, A_2, \ldots\}$ — последовательность Коши элементов поля $\bar{F}$. Так как F всюду плотно в $\bar{F}$, для каждого A_n существует такой элемент $a_n \in F$, что

$$\|A_n - (\bar{a}_n)\| < \frac{1}{n}. \tag{3.2}$$

Тогда последовательность $\{A_n - (\bar{a}_n)\}$ бесконечно мала и, следовательно, является последовательностью Коши в $\bar{F}$. Имеем

$$\{(\bar{a}_n)\} = \{A_n\} - \{A_n - (\bar{a}_n)\},$$

отсюда $\{(\bar{a}_n)\}$ — последовательность Коши в $\bar{F}$, но так как все ее элементы принадлежат полю F, то и сама последовательность $\{a_n\}$ является последовательностью Коши в F. Обозначим класс эквивалентности, содержащий $\{a_n\}$, через A (в наших обозначениях $(a_n) \in \bar{F}$). Из соотношений (3.1) и (3.2) следует, что последовательности $\{A - (\bar{a}_n)\}$ и $\{A_n - (\bar{a}_n)\}$ в $\bar{F}$ бесконечно малы, а значит, и их разность

$$\{A - A_n\} = \{A - (\bar{a}_n)\} - \{A_n - (\bar{a}_n)\}$$

есть бесконечно малая последовательность элементов поля $\bar{F}$. Отсюда вытекает, что

$$\lim_{n\to\infty} \|A - A_n\| = 0,$$

но это в точности означает, что $A = \lim\limits_{n\to\infty} A_n$. □

Предложение 3.5. *Арифметические операции продолжаются с F на $\bar{F}$ по непрерывности, т.е. если*

$$A = \lim_{n\to\infty} (\bar{a}_n), \quad B = \lim_{n\to\infty} (\bar{b}_n),$$

то

$$A + B = \lim_{n\to\infty} (\bar{a}_n + \bar{b}_n), \quad A \cdot B = \lim_{n\to\infty} (\bar{a}_n \cdot \bar{b}_n).$$

Доказательство. См. упражнение 16. □

Упражнения

14. Докажите, что если $\{a_n\}$ и $\{b_n\}$ — последовательности Коши, то последовательности $\{a_n + b_n\}$, $\{a_n - b_n\}$ и $\{a_n b_n\}$ также являются последовательностями Коши.

15. Докажите, что если $\{a_n\} \sim \{a'_n\}$ и $\{b_n\} \sim \{b'_n\}$ — две пары эквивалентных последовательностей Коши, то $\{a_n \pm b_n\} \sim \{a'_n \pm b'_n\}$ и $\{a_n \cdot b_n\} \sim \{a'_n \cdot b'_n\}$.

16. Докажите предложение 3.5.

§ 4. Поле p-адических чисел $\mathbb{Q}_p$

Абсолютная величина $|\cdot|$ является основным примером нормы на поле рациональных чисел $\mathbb{Q}$. Индуцированная ею метрика $d(x, y) = |x - y|$ — это обычное евклидово расстояние на числовой прямой, и, как было объяснено в § 1, результатом пополнения по этой норме является поле действительных чисел $\mathbb{R}$.

Возникает следующий вопрос: действительно ли евклидово расстояние между рациональными числами является наиболее «естественным»? Существует ли другой способ описать «близость» между рациональными числами? Оказывается, что ответ на этот вопрос положительный.

Новый способ измерения расстояния между рациональными числами возникает из следующей «арифметической» конструкции.

Пусть $p \in \mathbb{N}$ — произвольное простое число. Определим отображение $|\cdot|_p$ на $\mathbb{Q}$ следующим образом:

$$|x|_p = \begin{cases} \dfrac{1}{p^{\operatorname{ord}_p x}}, & \text{если } x \neq 0, \\ 0, & \text{если } x = 0, \end{cases} \tag{4.1}$$

где

$$\operatorname{ord}_p x = \begin{cases} \text{наибольшая степень числа } p, \text{ которая делит } x, \text{ если } x \in \mathbb{Z}, \\ \operatorname{ord}_p a - \operatorname{ord}_p b, \text{ если } x = a/b,\ a,\ b \in \mathbb{Z},\ b \neq 0. \end{cases}$$

Замечания. 1. Заметим, что функция $|\cdot|_p$ может принимать только «дискретное» множество значений, а именно $\{p^n,\ n \in \mathbb{Z}\} \cup \{0\}$.

2. Если $a, b \in \mathbb{N}$, то $a \equiv b \pmod{p^n}$ тогда и только тогда, когда $|a - b|_p \leqslant 1/p^n$.

Предложение 4.1. *Отображение $|\cdot|_p$ является неархимедовой нормой на $\mathbb{Q}$.*

Доказательство. Свойство 1) из определения 2.1 очевидно, а свойство 2) следует из равенства

$$\operatorname{ord}_p(xy) = \operatorname{ord}_p(x) + \operatorname{ord}_p(y).$$

Проверим свойство 3). Если $x = 0$ или $y = 0$, то свойство 3) очевидно, поэтому предположим, что $x,\ y \neq 0$. Пусть $x = a/b$ и $y = c/d$. Тогда имеем

$$x + y = \frac{ad + bc}{bd},$$

$$\operatorname{ord}_p(x+y) = \operatorname{ord}_p(ad+bc) - \operatorname{ord}_p(bd) \geqslant \min(\operatorname{ord}_p(ad),\ \operatorname{ord}_p(bc)) - \operatorname{ord}_p b - \\ - \operatorname{ord}_p d = \min(\operatorname{ord}_p a - \operatorname{ord}_p b,\ \operatorname{ord}_p c - \operatorname{ord}_p d) = \min(\operatorname{ord}_p x,\ \operatorname{ord}_p y).$$

Таким образом,

$$|x + y|_p = \frac{1}{p^{\operatorname{ord}_p(x+y)}} \leqslant \max(p^{-\operatorname{ord}_p x},\ p^{-\operatorname{ord}_p y}) = \\ = \max(|x|_p,\ |y|_p) \leqslant |x|_p + |y|_p.$$

Заметим, что попутно мы доказали, что норма $|\cdot|_p$ неархимедова. □

Замечания. 1. Позднее мы увидим, что поле $\mathbb{Q}$ не полно по норме $|\cdot|_p$.

2. Норма $|\cdot|_{p_1}$ не эквивалентна норме $|\cdot|_{p_2}$, если p_1 и p_2 — различные простые числа (действительно, для последовательности $x_n = (p_1/p_2)^n$ имеем $|x_n|_{p_1} \to 0$, но $|x_n|_{p_2} \to \infty$).

Теперь мы готовы определить основной объект этой книги. Зафиксируем простое число p. Определим $\mathbb{Q}_p$ как пополнение поля $\mathbb{Q}$ по p-адической

норме $|\cdot|_p$, определенной соотношением (4.1). В соответствии с определением 3.2, p-адическая норма продолжается на $\mathbb{Q}_p$, и $(\mathbb{Q}_p, |\cdot|_p)$ является полным нормированным полем. Будем называть $\mathbb{Q}_p$ *полем p-адических чисел*. Элементами поля $\mathbb{Q}_p$ являются классы эквивалентных последовательностей Коши рациональных чисел относительно p-адической нормы. Ранее было показано, что $\mathbb{Q}$ можно отождествить с подполем $\mathbb{Q}_p$, состоящим из классов эквивалентности, содержащих постоянные последовательности Коши.

Для произвольного $a \in \mathbb{Q}_p$ возьмем последовательность Коши $\{a_n\}$, представляющую a. Тогда по определению

$$|a|_p = \lim_{n\to\infty} |a_n|_p.$$

Таким образом, множество значений отображения $|\cdot|_p$ на $\mathbb{Q}_p$ совпадает с множеством значений отображения $|\cdot|_p$ на $\mathbb{Q}$, а именно с $\{p^n,\ n \in \mathbb{Z}\} \cup \{0\}$. Это совсем не похоже на поведение абсолютной величины, которая при продолжении с $\mathbb{Q}$ на $\mathbb{R}$ принимает все неотрицательные действительные значения. Более того, если $|a|_p \neq 0$, то последовательность норм $\{|a_n|_p\}$ должна стабилизироваться, если n достаточно велико!

В каждом классе эквивалентных последовательностей Коши, определяющем некоторый элемент поля $\mathbb{Q}_p$, содержится единственный *канонический* представитель. Для того чтобы его построить, нам потребуется следующая лемма.

Лемма 4.2. *Если $x \in \mathbb{Q}$ и $|x|_p \leqslant 1$, то для любого i существует такое целое число $\alpha \in \mathbb{Z}$, что $|\alpha - x|_p \leqslant p^{-i}$. Число α можно выбрать принадлежащим множеству $\{0, 1, 2, \ldots, p^i - 1\}$, причем из этого множества оно выбирается единственным образом.*

Доказательство. Пусть $x = a/b$, где a и b взаимно просты (обозначается $(a, b) = 1$). Так как $|x|_p \leqslant 1$, число p не делит b; следовательно, b и p^i взаимно просты. Поэтому существуют такие целые числа m и n, что $mb + np^i = 1$. Положим $\alpha = am$. Тогда

$$|\alpha - x|_p = |am - a/b|_p = |a/b|_p|mb - 1|_p \leqslant$$
$$\leqslant |mb - 1|_p = |np^i|_p = |n|_p(1/p^i) \leqslant 1/p^i.$$

Наконец, используя сильное неравенство треугольника, к целому α можно прибавить число, кратное p^i, чтобы получить целое число между 0 и p^i, для которого по-прежнему $|\alpha - x|_p \leqslant p^{-i}$. □

Теорема 4.3. *Каждый класс эквивалентности $a \in \mathbb{Q}_p$, удовлетворяющий неравенству $|a|_p \leqslant 1$, содержит ровно одну такую последовательность Коши $\{a_i\}$, что*

1) $a_i \in \mathbb{Z}$, $0 \leqslant a_i < p^i$ *для* $i = 1, 2, \ldots$

2) $a_i \equiv a_{i+1} \pmod{p^i}$ *для* $i = 1, 2, \ldots$

Доказательство. Пусть $\{b_i\}$ — последовательность Коши. Мы хотим найти эквивалентную ей последовательность $\{a_i\}$, удовлетворяющую условиям 1) и 2). Для каждого $j = 1, 2, \ldots$ выберем такое натуральное число $N(j)$, что

$$|b_i - b_{i'}|_p \leqslant p^{-j} \quad \text{для любых } i, i' \geqslant N(j).$$

Заметим, что последовательность $N(j)$ можно выбрать строго возрастающей, поэтому $N(j) \geqslant j$.

Далее заметим, что $|b_i|_p \leqslant 1$, если $i \geqslant N(1)$, так как для всех $i' \geqslant N(1)$ выполняются неравенства

$$|b_i|_p \leqslant \max(|b_{i'}|_p, |b_i - b_{i'}|_p) \leqslant \max(|b_{i'}|_p, 1/p),$$

поэтому

$$|b_{i'}|_p \to |a|_p \leqslant 1 \quad \text{при } i' \to \infty.$$

Применяя лемму 4.2, можно найти целые числа a_j, $0 \leqslant a_j < p^j$ такие, что

$$|a_j - b_{N(j)}|_p \leqslant \frac{1}{p^j}.$$

Покажем, что $a_j \equiv a_{j+1} \pmod{p^j}$ и $(b_i) \sim (a_j)$.

Сначала докажем первое утверждение:

$$\begin{aligned}|a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \leqslant \\ &\leqslant \max(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p) \leqslant \\ &\leqslant \max(1/p^{j+1}, 1/p^j, 1/p^j) = 1/p^j,\end{aligned}$$

поэтому $a_j \equiv a_{j+1} \pmod{p^j}$.

Чтобы доказать второе утверждение, возьмем произвольное j; тогда для $i \geqslant N(j)$ имеем

$$\begin{aligned}&|a_i - b_i|_p = |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \leqslant \\ &\leqslant \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p) \leqslant \max(1/p^j, 1/p^j, 1/p^j) = 1/p^j.\end{aligned}$$

Следовательно,

$$|a_i - b_i|_p \to 0 \quad \text{при } i \to \infty.$$

Теперь докажем единственность. Пусть $\{a'_i\}$ — другая последовательность, удовлетворяющая условиям теоремы, но $a_{i_0} \neq a'_{i_0}$ для некоторого i_0. Тогда $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}}$, так как a_{i_0} и a_{i_1} заключены между 0 и p^{i_0}. Тогда из условия 2) следует, что для $i > i_0$ выполняются соотношения

$$a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \pmod{p^{i_0}},$$

т. е. $a_i \not\equiv a'_i \pmod{p^{i_0}}$. Но это в точности означает, что

$$|a_i - a'_i|_p > \frac{1}{p^{i_0}} \quad \text{для любого } i \geqslant i_0,$$

откуда вытекает, что $(a_i) \not\sim (a'_i)$. □

Если $a \in \mathbb{Q}_p$ и $|a|_p \leqslant 1$, то члены a_i последовательности из предыдущей теоремы удобно записывать следующим образом:

$$a_i = d_0 + d_1 p + \ldots + d_{i-1} p^{i-1},$$

где все d_i являются целыми числами из множества $\{0, 1, \ldots, p-1\}$. Наше условие 2) в точности означает, что

$$a_{i+1} = d_0 + d_1 p + \ldots + d_{i-1} p^{i-1} + d_i p^i,$$

причем «p-адические цифры» от d_0 до d_{i-1} являются теми же самыми, что и для a_i. Таким образом, a представляется сходящимся (по p-адической норме, разумеется) рядом

$$a = \sum_{n=0}^{\infty} d_n p^n,$$

который можно рассматривать как число, записанное по основанию p и бесконечно продолжающееся влево, или содержащее бесконечно много p-адических цифр. В дальнейшем мы будем записывать

$$a = \ldots d_n \ldots d_2 d_1 d_0$$

и называть эту запись *каноническим p-адическим разложением* или *канонической формой* числа a.

Если $|a|_p > 1$, то мы можем домножить a на некоторую степень числа p (именно, на $p^m = |a|_p$) и получить p-адическое число $a' = a p^m$, которое уже удовлетворяет неравенству $|a'|_p \leqslant 1$.

Тогда можно записать

$$a = \sum_{n=-m}^{\infty} d_n p^n, \tag{4.2}$$

причем $d_{-m} \neq 0$ и $b_i \in \{0, 1, 2, \ldots, p-1\}$. Тем самым мы представили данное p-адическое число a в виде дроби по основанию p, содержащей бесконечно много p-адических цифр перед запятой и конечное число цифр после нее:

$$a = \ldots d_n \ldots d_2 d_1 d_0, d_{-1} \ldots d_{-m}; \tag{4.3}$$

это представление называется *каноническим p-адическим разложением* числа a.

Очевидно, что норма p-адического числа определяется индексом первого ненулевого коэффициента в его каноническом разложении. Более

того, *порядок*, определенный в начале § 4 для рациональных чисел, можно продолжить на все p-адические числа: для числа a из (4.3) имеем $\operatorname{ord}_p(x) = -m$ и $|a|_p = p^{-\operatorname{ord}_p(a)} = p^m$.

Замечание 4.4. Единственность представления, которую гарантирует теорема 4.3, отсутствует в случае представления чисел бесконечными дробями по основанию g, о котором шла речь в § 1, например

$$1{,}0000\ldots = 0{,}9999\ldots$$

В p-адическом случае не бывает таких исключительных ситуаций. Если два p-адических разложения сходятся к одному и тому же p-адическому числу, то они совпадают, т. е. все их цифры совпадают.

Определение 4.5. *Целым p-адическим числом*, называется такое число $a \in \mathbb{Q}_p$, что его каноническое разложение содержит только неотрицательные степени числа p.

Множество целых p-адических чисел обозначается $\mathbb{Z}_p$:

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \right\}.$$

Легко видеть (упражнение 18), что $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leqslant 1\}$.

Теорема 4.6. *Каждая бесконечная последовательность целых p-адических чисел содержит сходящуюся подпоследовательность.*

Доказательство. Напомним, что *подпоследовательность* $\{x_{n_k}\}$ последовательности $\{x_n\}$ задается такой последовательностью натуральных чисел $\{n_k\}$, что $n_1 < n_2 < n_3 < \ldots$

Пусть $\{x_k\}$ — последовательность элементов $\mathbb{Z}_p$. Запишем каноническое разложение каждого члена $x_k = \ldots a_2^k a_1^k a_0^k$. Так как цифры a_0^k могут принимать только конечное число значений (именно, $0, 1, \ldots, p-1$), можно найти такое $b_0 \in \{0, 1, \ldots, p-1\}$ и такую бесконечную подпоследовательность $\{x_{0k}\}$ последовательности $\{x_k\}$, что первая цифра всех чисел x_{0k} равна b_0. Точно так же находим $b_1 \in \{0, 1, \ldots, p-1\}$ и подпоследовательность $\{x_{1k}\}$ последовательности $\{x_{0k}\}$, для которой две первые цифры всегда равны $b_1 b_0$. Продолжая эту процедуру, мы получим такую последовательность $b_0, b_1, b_2, \ldots$ и такую последовательность последовательностей

$$\begin{array}{l} x_{00}, x_{01}, x_{02}, \ldots, x_{0s}, \ldots \\ x_{10}, x_{11}, x_{12}, \ldots, x_{1s}, \ldots \\ x_{20}, x_{21}, x_{22}, \ldots, x_{2s}, \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

что каждая последовательность является подпоследовательностью предыдущей и каждый элемент n-й строки оканчивается на $b_n \ldots b_1 b_0$. Для

каждого $j = 0, 1, \ldots$ имеем

$$x_{jj} \in \{x_{j-1,j}, x_{j-1,j+1}, \ldots\}.$$

Таким образом, диагональная последовательность $x_{00}, x_{11}, \ldots$ является подпоследовательностью исходной последовательности и, очевидно, сходится к $\ldots b_3 b_2 b_1 b_0$. □

Замечание 4.7. Этот результат можно расширить на ограниченные последовательности (см. упражнение 22). Эта теорема верна и для ограниченных последовательностей действительных чисел. Помните ли вы, как она доказывается? Попробуйте доказать эту теорему аналогичным образом для последовательности вещественных чисел $0 \leqslant x_n \leqslant 1$, используя представление чисел x_n в виде бесконечных десятичных дробей.

Упражнения

17. Какова мощность множества $\mathbb{Z}_p$? Ответ обоснуйте.

18. Докажите, что $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leqslant 1\}$.

19. Найдите p-адические нормы и p-адические разложения следующих чисел:

1) $15, -1, -3$ в $\mathbb{Q}_5$;

2) $6!$ в $\mathbb{Q}_3$;

3) $1/3!$ в $\mathbb{Q}_3$.

20. Найдите p-адическое разложение числа $1/p$. Сделайте то же самое для числа $1/p^k$.

21. Найдите p-адическое разложение числа $1/2$, если p — простое нечетное число.

22. Докажите, что каждая ограниченная последовательность элементов поля $\mathbb{Q}_p$ содержит сходящуюся подпоследовательность.

§ 5. Арифметические операции в $\mathbb{Q}_p$

Отметим, что p-адическое разложение позволяет нам производить арифметические операции над элементами поля $\mathbb{Q}_p$, подобно тому как это было в случае $\mathbb{R}$. Более того, вскоре мы увидим, что производить арифметические операции над элементами поля $\mathbb{Q}_p$ даже легче, чем над действительными числами! Положим

$$a = \sum_{n=-m}^{\infty} a_n p^n, \quad b = \sum_{n=-m}^{\infty} b_n p^n,$$

где a_n и b_n — p-адические цифры, причем $a_{-m} \neq 0$, но, возможно, одна или несколько первых цифр $b_{-m}, b_{-m+1}, \ldots$ равны 0. Тогда правая часть

равенства

$$a \pm b = \sum_{n=-m}^{\infty} (a_n \pm b_n) p^n$$

является сходящимся рядом; однако он, вообще говоря, не будет канонической формой (4.2). Приведение к каноническому виду, описанному в теореме 4.3, соответствует обычной процедуре сложения (или вычитания) «столбиком», которую надо применить к p-адическим числам, записанным в виде (4.3), причем здесь, как и в случае десятичных дробей, используется система переноса в соседний разряд.

Чтобы проиллюстрировать алгоритм сложения, найдем каноническое p-адическое разложение числа -1 в $\mathbb{Q}_p$. Имеем $1 = \ldots 00001$. Пусть число $a = \ldots a_3 a_2 a_1 a_0$ удовлетворяет соотношению $1 + a = 0$ (тогда $a = -1$). Начиная справа, имеем $1 + a_0 = 0$, но, так как $a_0 \in \{0, 1, \ldots, p-1\}$, единственный способ достичь требуемого состоит в том, чтобы найти a_0 из соотношения $1 + a_0 = p$, а затем перенести единицу влево. Таким образом $a_0 = p - 1$. Продолжая эту процедуру, мы видим, что все a_n равны $p - 1$, т. е.

$$-1 = \ldots (p-1)(p-1)(p-1).$$

Умножение выполняется похожим образом. Пусть заданы канонические разложения чисел a и b:

$$a = \sum_{n=-m}^{\infty} a_n p^n, \quad b = \sum_{n=-k}^{\infty} b_n p^n.$$

Перемножая ряды и приводя подобные члены, получаем

$$ab = \sum_{n=-m-k}^{\infty} u_n p^n,$$

где

$$u_{-m-k} = a_{-m} b_{-k},$$
$$u_{-m-k+1} = a_{-m+1} b_{-k} + a_{-m} b_{-k+1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Снова этот ряд, вообще говоря, не является канонической формой, но метод теоремы 4.3 позволяет нам привести его к каноническому виду. Это соответствует обычной процедуре умножения «столбиком», которую надо применить к p-адическим числам, записанным в виде (4.3).

Чтобы проиллюстрировать деление, предположим, что даны два числа $a, b \in \mathbb{Q}_p$, причем $b \neq 0$. Не теряя общности, можно предположить, что

$b \in \mathbb{Z}_p$, $b = \ldots b_2 b_1 b_0$, причем $b_0 \neq 0$. Пусть p-адическое число a имеет вид

$$a = \ldots a_3 a_2 a_1 a_0, a_{-1} \ldots a_{-k}.$$

Так как $b_0 \neq 0$ и кольцо вычетов $\mathbb{Z}/p\mathbb{Z}$ является полем для простого числа p, всегда можно найти такое $c_{-k} \in \{0, 1, \ldots, p-1\}$, что $c_{-k} b_0 \equiv a_{-k} \pmod p$. Продолжая обычную процедуру деления (перенося, если надо, 1 влево), мы получим частное a/b в канонической форме.

Из сказанного выше вытекает, что если $a = \ldots a_2 a_1 a_0$ — целое p-адическое число, причем $a_0 \neq 0$, то обратное по умножению число $1/a$ также является целым p-адическим! (Хотя это свойство целых p-адических чисел, на первый взгляд, может показаться удивительным, оно оказывается довольно удобным.)

С другой стороны, из того, что

$$p \cdot \sum_{i=0}^{\infty} a_i p^i = a_0 p + a_1 p^2 + \ldots \neq 1 + 0p + 0p^2 + \ldots,$$

следует, что p не имеет обратного по умножению в $\mathbb{Z}_p$ (разумеется, p имеет обратный элемент в $\mathbb{Q}_p$ (упражнение 20)). Похожие рассуждения показывают, что целое p-адическое число, у которого первая цифра a_0 равна 0, не имеет обратного по умножению в $\mathbb{Z}_p$. Резюмируем вышесказанное в следующем предложении.

Предложение 5.1. *Целое p-адическое число*

$$a = \ldots a_1 a_0 \in \mathbb{Z}_p$$

имеет обратное по умножению в $\mathbb{Z}_p$ тогда и только тогда, когда $a_0 \neq 0$.

Обозначим группу обратимых элементов кольца $\mathbb{Z}_p$ через $\mathbb{Z}_p^\times$. Тогда

$$\mathbb{Z}_p^\times = \left\{ \sum_{i=1}^{\infty} a_i p^i : a_0 \neq 0 \right\}.$$

Эта группа также называется группой *p-адических единиц*. Согласно упражнению 23

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x|_p = 1\}.$$

Следующее утверждение немедленно следует из определения p-адической нормы и упражнения 23.

Предложение 5.2. *Пусть x — p-адическое число, имеющее норму p^{-n}. Тогда число x может быть записано в виде произведения $x = p^n u$, где $u \in \mathbb{Z}_p^\times$.*

Заметим, что арифметические операции в $\mathbb{Q}_p$ расширяют обычные операции над натуральными числами (записанными по основанию p). Знакомые нам алгоритмы просто неограниченно продолжаются.

Вот несколько примеров арифметических операций в $\mathbb{Q}_7$:

$$\ldots 263 \times \ldots 154 = \ldots 455;$$
$$\ldots 30{,}2 - \ldots 56{,}4 = \ldots 40{,}5;$$
$$\ldots 421 : \ldots 153 = \ldots 615.$$

Упражнения

23. Докажите, что $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x|_p = 1\}$.

24. Пусть число $a \in \mathbb{Q}_p$ имеет каноническое p-адическое разложение

$$\ldots a_n \ldots a_2 a_1 a_0, a_{-1} \ldots a_{-m}.$$

Какое каноническое разложение имеет число $-a$?

25. Целые числа 2, 3, 4 обратимы в $\mathbb{Z}_5$. Найдите 5-адические разложения обратных к ним. Найдите разложение числа $1/3$ в $\mathbb{Z}_7$.

26. Найдите 4 цифры канонических разложений следующих p-адических чисел:

1) $\ldots 1246 \times \ldots 6003$ в $\mathbb{Q}_7$;
2) $1 : \ldots 1323$ в $\mathbb{Q}_5$;
3) $900 - \ldots 312{,}3$ в $\mathbb{Q}_{11}$;

27. Найдите p-адическую норму числа $(p^n)!$.

28*. Найдите p-адическую норму числа $n!$.

§ 6. p-адическое разложение рациональных чисел

Каждое целое рациональное число является также целым p-адическим числом (просто запишите его в системе по основанию p). Однако целые p-адические числа есть и среди рациональных дробей! Мы видели, что

$$-1 = (p-1)\sum_{i=0}^{\infty} p^i,$$

поэтому

$$\sum_{i=0}^{\infty} p^i = \frac{1}{1-p}, \qquad \frac{1}{1-p} = \ldots 1111,$$

а это число является элементом кольца $\mathbb{Z}_p$. Заметим, что p-адическое разложение этого целого p-адического числа бесконечно! Упражнение 31 содержит необходимое и достаточное условие конечности p-адического разложения.

Следующая теорема показывает, что среди всех канонических p-адических разложений можно выделить разложения рациональных чисел точно таким же способом, как мы выделяем разложения рациональных чисел среди всех десятичных разложений вещественных чисел.

Теорема 6.1. *Каноническое p-адическое разложение* (4.3) *представляет рациональное число тогда и только тогда, когда оно с некоторого момента является периодическим влево.*

Доказательство. Предположим, что каноническое p-адическое разложение, начиная с некоторого момента, является периодическим. Умножая (если надо) данное p-адическое число x на некоторую степень числа p и вычитая рациональное число, можно считать, что $x \in \mathbb{Z}_p$ и x_0 имеет периодическое разложение вида

$$x = x_0 + x_1 p + x_2 p^2 + \ldots + x_{k-1} p^{k-1} + x_0 p^k + x_1 p^{k+1} \ldots$$

Число $a = x_0 + x_1 p + x_2 p^2 + \ldots + x_{k-1} p^{k-1}$ является целым рациональным, и поэтому x можно представить в виде

$$a(1 + p^k + p^{2k} + \ldots) = a\frac{1}{1 - p^k},$$

следовательно, число x является рациональным.

Обратно, предположим, что

$$\frac{a}{b} = \sum_{i \geqslant 0} x_i p^i \in \mathbb{Z}_p.$$

Можно считать, что числа a и b являются целыми взаимно простыми и что b не делится на p. Запишем p-адическое разложение числа a/b:

$$\frac{a}{b} = x_0 + x_1 p + x_2 p^2 + \ldots + x_{n-1} p^{n-1} + \ldots$$

и положим $A_n = x_0 + x_1 p + x_2 p^2 + \ldots + x_{n-1} p^{n-1}$, $0 \leqslant A_n \leqslant p^n - 1$. Так как A_n является целым рациональным числом,

$$\frac{a}{b} = A_n + p^n \frac{r_n}{b},$$

причем r_n — целое число. Тогда $r_n = (a - A_n b)/p^n$ и имеет место следующая оценка:

$$\frac{a - (p^n - 1)b}{p^n} \leqslant r_n \leqslant \frac{a}{p^n}.$$

Если n достаточно велико, то $-b \leqslant r_n \leqslant 0$, а это означает, что r_n принимает только конечное число значений. Теперь мы можем записать

$$x = A_n + p^n \frac{r_n}{b} = A_{n+1} + p^{n+1} \frac{r_{n+1}}{b} = A_n + x_n p^n + p^{n+1} \frac{r_{n+1}}{b}.$$

Отсюда вытекает, что $r_n = x_n b + pr_{n+1}$ для всех n. Так как r_n принимает только конечное количество значений, существуют такой индекс m и такое натуральное число P, что $r_m = r_{m+P}$; отсюда

$$x_m b + pr_{m+1} = x_{m+P} b + pr_{m+P+1}, \tag{6.1}$$

поэтому

$$(x_m - x_{m+P})b = p(r_{m+P+1} - r_{m+1}).$$

Так как $(b, p) = 1$, число p делит $x_m - x_{m+P}$. Но и x_m, и x_{m+P} являются цифрами из множества $\{0, 1, \ldots, p-1\}$, поэтому $x_m = x_{m+P}$. Если подставить это равенство в (6.1), то мы увидим, что $r_{m+1} = r_{m+P+1}$. Повторив вышеизложенное рассуждение, получим, что

$$r_n = r_{n+P} \quad \text{и} \quad x_n = x_{n+P} \quad (n \geqslant m).$$

Таким образом, не только последовательность цифр x_n, но и последовательность числителей r_n имеет период длины P, если $n \geqslant m$. □

Возникает такой вопрос: можно ли по p-адическому разложению рационального числа определить его знак? Ответ на этот вопрос положительный, и он дан в упражнении 30.

Упражнения

29. Докажите, что

1) $\mathbb{Z}_p \cap \mathbb{Q} = \{a/b \in \mathbb{Q}\colon p \nmid b\}$,

2) $\mathbb{Z}_p^\times \cap \mathbb{Q} = \{a/b \in \mathbb{Q}\colon p \nmid ab\}$.

30*. Пусть $r \in \mathbb{Q}$. Докажите, что существует такое число $k \geqslant 1$, что p-адическое разложение числа rp^k может быть представлено в виде $\ldots aaaaab$, где фрагменты a и b содержат одинаковое количество цифр. Докажите, что неравенство $r > 0$ эквивалентно неравенству $b > a$ в обычном смысле (как для целых чисел, записанных в системе по основанию p).

31. Докажите, что p-адическое разложение числа $a \in \mathbb{Q}_p$ обрывается (т. е. $a_i = 0$ для всех i, начиная с некоторого N) тогда и только тогда, когда a является *положительным* рациональным числом, знаменатель которого является степенью числа p.

§ 7. Лемма Гензеля и сравнения

Попробуем извлечь $\sqrt{6}$ в $\mathbb{Q}_5$; это означает, что мы хотим найти такую последовательность 5-адических цифр $a_0, a_1, a_2, \ldots, 0 \leqslant a_i \leqslant 4$, что

$$(a_0 + a_1 \times 5 + a_2 \times 5^2 + \ldots)^2 = 1 + 1 \times 5. \tag{7.1}$$

Из (7.1) получаем $a_0^2 \equiv 1 \pmod 5$, откуда $a_0 = 1$ или 4. Если $a_0 = 1$, то

$$2a_1 \times 5 \equiv 1 \times 5 \pmod{5^2} \implies 2a_1 \equiv 1 \pmod 5 \implies a_1 = 3.$$

На следующем шаге имеем

$$1 + 1 \times 5 \equiv (1 + 3 \times 5 + a_2 \times 5^2)^2 \equiv 1 + 1 \times 5 + 2a_2 \times 5^2 \pmod{5^3},$$

откуда следует, что $2a_2 \equiv 0 \pmod 5$ и, таким образом, $a_2 = 0$.

Итак, мы получаем ряд

$$a = 1 + 3 \times 5 + 0 \times 5^2 + \ldots,$$

где все a_i, начиная с a_1, определены однозначно.

Если мы возьмем $a_0 = 4$, то получим решение

$$-a = 4 + 1 \times 5 + 4 \times 5^2 + 0 \times 5^3 + \ldots$$

С другой стороны, несложно убедиться в том, что в $\mathbb{Q}_5$ существуют числа, из которых невозможно извлечь квадратный корень (например, $2 + 1 \times 5$).

Изложенный выше метод решения уравнений (таких как $x^2 - 6 = 0$ в $\mathbb{Q}_5$) можно обобщить с помощью очень важного утверждения, которое называется «леммой Гензеля».

Обобщая замечание 2, предшествующее предложению 4.1, будем говорить, что числа a и $b \in \mathbb{Q}_p$ *сравнимы* по модулю p^n, и записывать

$$a \equiv b \pmod{p^n},$$

если $|a - b|_p \leqslant 1/p^n$.

Теорема 7.1 (лемма Гензеля). *Пусть $F(x) = c_0 + c_1 x + \ldots + c_n x^n$ — многочлен с целыми p-адическими коэффициентами. Пусть*

$$F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \ldots + nc_n x^{n-1}$$

— производная многочлена $F(x)$. Предположим, что p-адическое число $\bar{a}_0$ удовлетворяет сравнению $F(\bar{a}_0) \equiv 0 \pmod p$, причем $F'(\bar{a}_0) \not\equiv \not\equiv 0 \pmod p$. Тогда существует единственное целое p-адическое число a, такое что $F(a_0) = 0$ и $a \equiv \bar{a}_0 \pmod p$.

Доказательство. Доказательство существования числа a состоит в построении канонического p-адического разложения $a = b_0 + b_1 p + + b_2 p^2 + \ldots$ по индукции. На k-м шаге индукции, используя p-адическую модификацию метода Ньютона (см. замечание сразу после этого доказательства), мы получим k-е приближение числа a, имеющее вид $a_k = b_0 + \ldots + b_k p^k$. Каждое a_k будет корнем многочлена $F(x)$ только «по модулю p^{k+1}» (т. е. $F(a_k) \equiv 0 \pmod{p^{k+1}}$). В пределе при $k \to \infty$ мы получим число a, которое будет «настоящим» корнем многочлена F.

Более точно, докажем индукцией по k следующее утверждение:
$S(k)$: *существует такое целое p-адическое число вида*

$$a_k = b_0 + b_1 p + \ldots + b_k p^k$$

(*цифры b_i лежат в множестве* $\{0, 1, \ldots, p-1\}$ *для всех i*), *что*

$$F(a_k) \equiv 0 \pmod{p^{k+1}} \quad \text{и} \quad a_k \equiv \bar{a}_0 \pmod{p}.$$

База индукции очевидна: возьмем b_0 равным первой p-адической цифре числа $\bar{a}_0$, тогда получим $a_0 \equiv \bar{a}_0$ и $F(a_0) \equiv 0 \pmod{p}$.

Теперь выполним шаг индукции, т. е. докажем, что из $S(k-1)$ следует $S(k)$. Для этого положим $a_k = a_{k-1} + b_k p^k$, где цифра b_k (пока неизвестная) удовлетворяет неравенству $0 \leqslant b_k < p$. Распишем $F(a_k)$, игнорируя слагаемые, кратные p^{k+1}:

$$F(a_k) = F(a_{k-1} + b_k p^k) = \sum_{i=0}^{n} c_i (a_{k-1} + b_k p^k)^i =$$

$$= \sum_{i=0}^{n} c_i (a_{k-1}^i + i a_{k-1}^{i-1} b_k p^k + \text{ слагаемые, кратные } p^{k+1}) \equiv$$

$$\equiv F(a_{k-1}) + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}.$$

Так как по предположению индукции $F(a_{k-1}) \equiv 0 \pmod{p^k}$, выражение для $F(a_k)$ можно переписать в виде

$$F(a_k) \equiv \alpha_k p^k + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}$$

для некоторого целого $\alpha_k \in \{0, 1, \ldots, p-1\}$. Таким образом, мы получаем следующее уравнение для неизвестной цифры b_k:

$$\alpha_k + b_k F'(a_{k-1}) \equiv 0 \pmod{p},$$

которое легко решается при условии $F'(a_{k-1}) \not\equiv 0 \pmod{p}$. Но это условие, конечно же, выполнено, так как $a_{k-1} \equiv \bar{a}_0 \pmod{p}$, и поэтому

$$F'(a_{k-1}) \equiv F'(\bar{a}_0) \not\equiv 0 \pmod{p}.$$

Разделив на $F'(a_{k-1})$, мы находим требуемую цифру b_k:

$$b_k = \frac{-\alpha_k}{F'(a_{k-1})} \pmod{p},$$

для которой выполнено сравнение $F(a_k) \equiv 0 \pmod{p^{k+1}}$. Тем самым, шаг индукции завершен.

Теперь положим

$$a = b_0 + b_1 p + b_2 p^2 + \ldots$$

Заметим, что $F(a) = 0$, так как для всех k имеем

$$F(a) \equiv F(a_k) \equiv 0 \pmod{p^{k+1}}.$$

Единственность числа a вытекает из единственности последовательности $\{a_k\}$. □

Замечание 7.2. В методе Ньютона для вещественного случая, если $f'(a_{n-1}) \neq 0$, мы выбираем

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}.$$

Поправочный член очень похож на «поправочный член» из доказательства леммы Гензеля:

$$b_n p^n \equiv -\frac{\alpha_n p^n}{F'(a_{n-1})} \equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.$$

Однако лемма Гензеля в некотором смысле лучше, чем метод Ньютона в вещественном случае: в p-адическом случае сходимость к корню многочлена гарантируется универсальным условием на начальное приближение $\bar{a}_0$, причем вид этого условия не зависит от многочлена. В вещественном же случае метод Ньютона сходится, если начальное приближение достаточно близко к искомому корню, а это условие зависит от многочлена. Например, если $f(x) = x^3 - x$ и $a_0 = 1/\sqrt{5}$, то получится $a_1 = -1/\sqrt{5}$, $a_2 = 1/\sqrt{5}$ и т. д.

Напомним, что в теореме 4.3 каноническое разложение p-адического числа получается из последовательности сравнений. Лемма Гензеля подтверждает эту связь. Следующая теорема делает связь между p-адическими числами и сравнениями еще более очевидной.

Теорема 7.3. *Многочлен с целыми коэффициентами имеет корень в $\mathbb{Z}_p$ тогда и только тогда, когда он имеет целочисленный корень по модулю p^k для любого $k \geqslant 1$.*

Доказательство. Пусть $F(x)$ — многочлен с целочисленными коэффициентами. Пусть $a \in \mathbb{Z}_p$ является корнем этого многочлена, т. е.

$$F(a) = 0. \tag{7.2}$$

По теореме 4.3 существует такая последовательность целых чисел $\{a_1, a_2, \ldots, a_k, \ldots\}$, что

$$a \equiv a_k \pmod{p^k} \quad (a_k = b_0 + b_1 p + b_2 p^2 + \ldots + b_{k-1} p^{k-1}).$$

Тогда из соотношений $F(a_k) \equiv F(a) \pmod{p^k}$ и $F(a) = 0$ следует, что

$$F(a_k) \equiv 0 \pmod{p^k}. \tag{7.3}$$

Обратно, предположим, что сравнение (7.3) имеет целочисленное решение a_k для любого $k \geqslant 1$. Согласно теореме 4.6 последовательность $\{a_k\}$ содержит сходящуюся подпоследовательность $\{a_{k_i}\}$, $\lim\limits_{i\to\infty} a_{k_i} = a$. Покажем, что a является решением уравнения (7.2). Действительно, так как многочлен является непрерывной функцией, имеем

$$F(a) = \lim_{i\to\infty} F(a_{k_i})$$

(здесь мы пользуемся тем, что предел суммы равен сумме пределов и предел произведения равен произведению пределов, т. е. предложением 3.5). С другой стороны,

$$F(a_{k_i}) \equiv 0 \pmod{p^{k_i}}.$$

Таким образом, $\lim\limits_{i\to\infty} F(a_{k_i}) = 0$ и $F(a) = 0$. □

Практическое следствие теоремы 7.3 состоит в следующем. Если многочлен с целыми коэффициентами не имеет корней по модулю p, то он не имеет корней и в $\mathbb{Z}_p$. Обычно бывает несложно найти корни по модулю p, если они есть. Если корень по модулю p не является корнем производной по модулю p, то по лемме Гензеля можно найти корень в $\mathbb{Z}_p$.

Второе условие ($F'(\bar{a}_0) \equiv 0 \pmod{p}$) теоремы 7.1 существенно (см. упражнение 32).

Будем называть целое рациональное число a, не делящееся на p, *квадратичным вычетом по модулю* p, если сравнение

$$x^2 \equiv a \pmod{p}$$

имеет решение среди чисел $\{1, 2, \ldots, p-1\}$. В противном случае a называется *квадратичным невычетом*.

Предложение 7.4. *Целое рациональное число a, не делящееся на p, имеет в $\mathbb{Z}_p$ ($p \neq 2$) квадратный корень тогда и только тогда, когда a является квадратичным вычетом по модулю p.*

Доказательство. Пусть $P(x) = x^2 - a$, тогда $P'(x) = 2x$. Если a — квадратичный вычет, то

$$a \equiv a_0^2 \pmod{p}$$

для некоторого $a_0 \in \{1, 2, \ldots, p-1\}$. Значит, $P(a_0) \equiv 0 \pmod{p}$. Но

$$P'(a_0) = 2a_0 \not\equiv 0 \pmod{p},$$

так как $(a_0, p) = 1$. Следовательно, по лемме Гензеля существует решение, принадлежащее $\mathbb{Z}_p$. Обратно, если a — квадратичный невычет, то по теореме 7.3 многочлен $P(x)$ не имеет корней в $\mathbb{Z}_p$. □

Например, $\sqrt{-1}$ в $\mathbb{Z}_5$ существует, так как число $-1 + 5 = 4$ является квадратичным вычетом по модулю 5; в то же самое время $\sqrt{-1}$ в $\mathbb{Z}_3$ не

существует, так как число $-1+3=2$ является квадратичным невычетом по модулю 3.

Выясните, существует ли $\sqrt{p}$ в $\mathbb{Z}_p$?

Упражнения

32. Приведите пример многочлена с целыми коэффициентами, который имеет корень по модулю 2, но не имеет корней в $\mathbb{Z}_2$.

33. Докажите, что если $p \neq 2$, то p-адическая единица

$$u = c_0 + c_1 p + c_2 p^2 + \ldots$$

является квадратом в $\mathbb{Z}_p$ тогда и только тогда, когда c_0 является квадратичным вычетом по модулю p.

34. Докажите, что уравнение $x^3 - 1 = 0$ имеет решение $a \neq 1$ в $\mathbb{Z}_7$, и найдите три первые цифры его канонического разложения.

35. Докажите, что уравнение $x^5 - 1 = 0$ не имеет решений $a \neq 1$ в $\mathbb{Q}_7$. Вы должны объяснить, почему такие корни из 1, если бы они были, должны были бы лежать в $\mathbb{Z}_7$, а не просто в $\mathbb{Q}_7$!

§ 8. Алгебраические свойства целых p-адических чисел

Мы уже видели, что целые p-адические числа во многом отличаются от обычных целых чисел из множества $\mathbb{Z}$. Здесь мы увидим, что алгебраические свойства чисел из $\mathbb{Z}_p$ не хуже, а может быть, даже чем-то и лучше, чем свойства обычных целых чисел. Обычные целые числа образуют *коммутативное кольцо*, т. е. это множество с двумя бинарными операциями, которые называются, как и в случае поля, сложением и умножением, причем эти операции уловлетворяют свойствам 1)—6) и 9) из определения поля (§ 2). Коммутативное кольцо без делителей нуля называется *областью целостности*.

Непустое подмножество I кольца R называется *идеалом*, если оно является подгруппой в R по сложению и для любых $x \in I$ и $r \in R$ выполняется включение $r \cdot x \in I$.

Например, множество $m\mathbb{Z}$ всех целых чисел, делящихся на данное число m, является идеалом кольца $\mathbb{Z}$.

Идеал называется *максимальным*, если он не содержится ни в каком другом собственном идеале. В примере, приведенном выше, идеал $m\mathbb{Z}$ максимален тогда и только тогда, когда m является простым числом.

Идеал $I \subset R$ называется *главным*, если $I = rR = (r)$ для некоторого $r \in R$.

Для кольца R и идеала $I \subset R$ можно определить фактор R/I как множество смежных классов с операциями сложения и умножения, которые

определяются естественным образом. Если R — коммутативное кольцо с единицей, то R/I является полем тогда и только тогда, когда идеал I максимален. Например, $\mathbb{Z}/p\mathbb{Z}$ — это поле вычетов по модулю p, которое является единственным полем из p элементов. Для более подробного ознакомления см. [3], §3.5.

Предложение 8.1. *Кольцо $\mathbb{Z}_p$ является областью целостности.*

Доказательство. Это вытекает из того, что $\mathbb{Z}_p$ содержится в множестве $\mathbb{Q}_p$, которое является полем и поэтому не содержит делителей нуля. □

Пусть $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ — конечное поле из p элементов. Отображение

$$a = \sum_{i=0}^{\infty} a_i p^i \mapsto a_0 \pmod p$$

определяет гомоморфизм колец, который называется *приведением* mod p. Этот гомоморфизм сюръективен, и его ядро имеет вид

$$\{a \in \mathbb{Z}_p : a_0 = 0\} = \left\{\sum_{i=1}^{\infty} a_i p^i\right\} = \left\{p \sum_{i=0}^{\infty} a_{i+1} p^i\right\} = p\mathbb{Z}_p.$$

Так как фактор является полем, ядро $p\mathbb{Z}_p$ образует максимальный идеал в кольце $\mathbb{Z}_p$.

Следствие 8.2. *Кольцо $\mathbb{Z}_p$ содержит единственный максимальный идеал, а именно*

$$p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^{\times}.$$

Доказательство. Пусть I — другой максимальный идеал. Так как идеал $p\mathbb{Z}_p$ также максимальный, I обязан содержать какой-то элемент a из его дополнения, $a \in \mathbb{Z}_p^{\times}$. Так как I является идеалом, $1 = a \cdot a^{-1} \in I$ и тогда $I = \mathbb{Z}_p$. □

Предложение 8.3. *Кольцо $\mathbb{Z}_p$ является областью главных идеалов. Более точно, все идеалы кольца $\mathbb{Z}_p$ главные: $\{0\}$ и $p^k\mathbb{Z}_p$ для всех $k \in \mathbb{N}$.*

Доказательство. Пусть $I \neq \{0\}$ — какой-то идеал в $\mathbb{Z}_p$ и $0 \neq a \in I$ — элемент, имеющий максимальную норму (такой элемент существует, так как норма принимает дискретное множество значений). Пусть $|a|_p = p^{-k}$ для некоторого $k \in \mathbb{N}$. Тогда $a = \varepsilon p^k$, где ε является p-адической единицей. Следовательно, $p^k = \varepsilon^{-1} a \subset I$, а значит, $(p^k) = p^k\mathbb{Z}_p \subset I$. Наоборот, для любого $b \in I$ мы имеем $|b|_p = p^{-w} \leqslant p^{-k}$. Но тогда мы можем написать

$$b = p^w \varepsilon' = p^k p^{w-k} \varepsilon' \in p^k\mathbb{Z}_p.$$

Таким образом, $I \subset p^k\mathbb{Z}_p$, и, значит, $I = p^k\mathbb{Z}_p$. □

В §7 в качестве приложения леммы Гензеля мы рассмотрели существование квадратных корней в $\mathbb{Q}_p$. Другим применением этого утверждения является вопрос о примитивных корнях из единицы в $\mathbb{Q}_p$.

Напомним, что элемент поля ζ называется *корнем степени m из единицы*, если $\zeta^m = 1$; такой корень называется *примитивным*, если $\zeta^n \neq 1$ для $0 < n < m$.

Предложение 8.4. *Для любого простого числа p и любого натурального числа m, взаимно простого с p, в $\mathbb{Q}_p$ существует примитивный корень степени m из единицы тогда и только тогда, когда $m \mid (p-1)$. В этом случае каждый корень степени m из единицы является также корнем степени $(p-1)$. Все корни степени $(p-1)$ из единицы образуют циклическую подгруппу в $\mathbb{Z}_p^\times$ порядка $(p-1)$.*

Доказательство. Пусть $m \mid (p-1)$; тогда $p - 1 = km$ для некоторого $k \geqslant 1$, и, значит, каждый корень степени m из 1 является также и корнем степени $(p-1)$. Положим

$$f(x) = x^{p-1} - 1, \qquad f'(x) = (p-1)x^{p-2}.$$

Возьмем произвольное натуральное число $x_0 \in \mathbb{Z}_p^\times$ из отрезка $1 \leqslant x_0 \leqslant p-1$. Тогда

$$f(x_0) \equiv 0 \pmod{p} \quad \text{и} \quad f'(x_0) \not\equiv 0 \pmod{p},$$

так как $|f'(x_0)| = 1$. Следовательно, можно применить лемму Гензеля и получить в точности $(p-1)$ решение, которые являются корнями из 1 степени $(p-1)$. Первые цифры этих корней равны, соответственно, $1, 2, \ldots, p-1$. Обратно, если $\alpha \in \mathbb{Q}_p$ — какой-то корень из 1 степени m, $\alpha^m = 1$, то $|\alpha|_p = 1$, т. е. $\alpha \in \mathbb{Z}_p$. Пусть первая цифра числа α равна α_0. Тогда $\alpha_0^m \equiv 1 \pmod{p}$, и, значит, m делит $p-1$, где $p-1$ — порядок группы $(\mathbb{Z}/p\mathbb{Z})^\times$. Так как многочлен с коэффициентами в поле не может иметь корней больше, чем его степень ([3], Lemma 5.3.2), многочлен $x^{p-1} - 1$ не может иметь больше $(p-1)$ корня, и все его корни являются корнями из 1. Ясно, что корни из 1 образуют группу по умножению. Наконец, так как конечная подгруппа мультипликативной группы поля циклическая ([3], Lemma 7.1.6), группа корней из 1 степени $(p-1)$ является циклической подгруппой порядка $(p-1)$ в $\mathbb{Z}_p^\times$. □

Для нахождения корней из единицы степени p лемма Гензеля неприменима (почему?), мы вернемся к этому вопросу позже (теорема 18.9).

Корни из единицы степени $(p-1)$ тесно связаны с так называемой *функцией сигнум* $\operatorname{sgn}_p(x)$, которая определяется в следующей теореме.

Теорема 8.5. *Для любого $x \in \mathbb{Z}_p$ существует предел $\lim\limits_{n\to\infty} x^{p^n}$. Этот предел обозначается $\operatorname{sgn}_p(x)$ и обладает следующими свойствами:*

a) $\operatorname{sgn}_p(x)$ *зависит только от первой цифры* x_0 *канонического* p*-адического разложения числа* x;

b) $\operatorname{sgn}_p(xy) = \operatorname{sgn}_p(x) \cdot \operatorname{sgn}_p(y)$;

c) $\operatorname{sgn}_p(x) = 0$, *если* $x_0 = 0$, *и является корнем из* 1 *степени* $(p-1)$, *если* $x_0 \neq 0$.

Доказательство. Пусть $x_0 \in \{1, 2, \ldots, p-1\}$. Сначала мы покажем, что последовательность $\{x_0^{p^n}\}$ сходится. По теореме Эйлера

$$x_0^{\varphi(p^n)} \equiv 1 \pmod{p^n},$$

где φ — функция Эйлера: для натурального числа m значение $\varphi(m)$ равно количеству чисел, меньших m и взаимно простых с ним. Так как число p — простое, имеем $\varphi(p^n) = p^n - p^{n-1}$. Тогда

$$x_0^{p^n - p^{n-1}} \equiv 1 \pmod{p^n}, \quad x_0^{p^n} \equiv x_0^{p^{n-1}} \pmod{p^n},$$

и, следовательно,

$$|x_0^{p^n} - x_0^{p^{n-1}}|_p \leqslant \frac{1}{p^n}.$$

Так как $1/p^n \to 0$ при $n \to \infty$, последовательность $\{x_0^{p^n}\}$ является последовательностью Коши и, поскольку пространство $\mathbb{Z}_p$ полно, сходится к некоторому пределу в $\mathbb{Z}_p$, который мы обозначим

$$\operatorname{sgn}_p(x_0) = \lim_{n\to\infty} x_0^{p^n}.$$

Очевидно, что этот предел существует для $x_0 = 0$, поэтому функция $\operatorname{sgn}_p(x)$ определена для всех $x_0 \in \{0, 1, 2, \ldots, p-1\}$ и $\operatorname{sgn}_p(0) = 0$. Далее мы покажем, что этот предел существует для всех $x \in \mathbb{Z}_p$ и определяется первой цифрой x_0 числа x. Для этого нам понадобится следующая лемма.

Лемма 8.6. *Пусть* $x \in \mathbb{Z}_p$, *причем первая цифра числа* x *равна* x_0. *Тогда выполнено неравенство* $|x^p - x_0^p|_p \leqslant p^{-1}|x - x_0|_p$.

Доказательство. Пусть $x = x_0 + \alpha$, причем $|\alpha|_p \leqslant p^{-1}$. Тогда

$$x^p - x_0^p = \binom{p}{1}x_0^{p-1}\alpha + \binom{p}{2}x_0^{p-2}\alpha^2 + \ldots + \binom{p}{p}\alpha^p =$$
$$= (x - x_0)\left(\binom{p}{1}x_0^{p-1} + \binom{p}{2}x_0^{p-2}\alpha + \ldots + \binom{p}{p}\alpha^{p-1}\right).$$

Так как $\left|\binom{p}{j}x_0^{p-j}\alpha^{j-1}\right|_p \leqslant p^{-1}$ для $j \geqslant 1$, применяя сильное неравенство треугольника, получаем

$$|x^p - x_0^p|_p \leqslant p^{-1}|x - x_0|_p. \qquad \square$$

Применяя доказанную лемму, получаем

$$|x^{p^n} - x_0^{p^n}|_p \leqslant p^{-1}|x^{p^{n-1}} - x_0^{p^{n-1}}|_p \leqslant \ldots \leqslant p^{-n}|x - x_0|_p,$$

откуда следует, что предел $\lim\limits_{n\to\infty} x^{p^n}$ существует и равняется $\lim\limits_{n\to\infty} x_0^{p^n}$. Таким образом, мы определили $\operatorname{sgn}_p(x)$ для всех $x \in \mathbb{Z}_p$, доказав тем самым утверждение a). Утверждение b) вытекает из свойства пределов:

$$\lim_{n\to\infty} (xy)^{p^n} = \lim_{n\to\infty} (x^{p^n})(y^{p^n}) = \lim_{n\to\infty} x^{p^n} \lim_{n\to\infty} y^{p^n}.$$

Осталось показать, что если $x_0 \in \{1, 2, \ldots, p-1\}$, то $\operatorname{sgn}_p(x_0)$ является корнем из 1 степени $(p-1)$. Используя утверждение b) и малую теорему Ферма (которая является частным случаем теоремы Эйлера при $n = p$), получаем

$$\operatorname{sgn}_p^{p-1}(x_0) = \operatorname{sgn}_p(x_0^{p-1}) = \operatorname{sgn}_p(1) = 1.$$

Таким образом, значения функции $\operatorname{sgn}_p(x)$ являются решениями уравнения $y^p - y = 0$. Так как $\mathbb{Q}_p$ — поле, это уравнение не может иметь в $\mathbb{Q}_p$, а значит, и в $\mathbb{Z}_p$, больше p решений. Следовательно, значениями функции сигнум исчерпываются все решения этого уравнения. □

§ 9. Метрики и нормы на множестве рациональных чисел. Теорема Островского

Как мы уже видели, на поле $\mathbb{Q}$ можно ввести следующие нормы: во-первых, p-адическую норму $|\cdot|_p$ для каждого простого числа p, во-вторых, обычную абсолютную величину $|\cdot|$ (которая иногда обозначается $|\cdot|_\infty$, удобно считать, что $p = \infty$ является бесконечно большим простым числом). Здесь мы покажем, что на $\mathbb{Q}$ не существует других норм и, следовательно, единственно возможными пополнениями поля $\mathbb{Q}$ являются поля $\mathbb{Q}_p$ для всех простых p и $\mathbb{R} = \mathbb{Q}_\infty$.

Теорема 9.1 (теорема Островского). *Всякая нетривиальная норма $\|\cdot\|$ на $\mathbb{Q}$ эквивалентна норме $|\cdot|_p$ для некоторого простого числа p или $p = \infty$.*

Доказательство. Предположим сначала, что норма $\|\cdot\|$ архимедова, т. е. существует такое натуральное число n, что $\|n\| > 1$, и обозначим через n_0 минимальное число n, удовлетворяющее этому условию. Тогда $\|n_0\| = n_0^\alpha$ для некоторого положительного действительного числа α.

Запишем произвольное натуральное число n в системе с основанием n_0, т. е. в виде

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \ldots + a_s n_0^s,$$

где $0 \leqslant a_i < n_0$, $i = 0, \dots s$ и $a_s \neq 0$. Тогда

$$\|n\| \leqslant \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \dots + \|a_s n_0^s\| = \\ = \|a_0\| + \|a_1\| n_0^\alpha + \|a_2\| n_0^{2\alpha} + \dots + \|a_s\| n_0^{s\alpha}.$$

Так как все цифры a_i строго меньше n_0, имеем (согласно выбору n_0) $\|a_i\| \leqslant 1$. Следовательно,

$$\|n\| \leqslant 1 + n_0^\alpha + n_0^{2\alpha} + \dots + n_0^{s\alpha} \leqslant \\ \leqslant n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \dots + n_0^{-s\alpha}) \leqslant n^\alpha \left(\sum_{i=0}^{\infty} \left(\frac{1}{n_0^\alpha} \right)^i \right),$$

потому что $n \geqslant n_0^s$. Выражение в скобках является константой, не зависящей от n; обозначим ее C. Таким образом,

$$\|n\| \leqslant C n^\alpha \quad \text{для всех } n = 1, 2, \dots$$

Если применить это же рассуждение к n^N вместо n, то получим

$$\|n^N\| \leqslant C n^{N\alpha} \quad \Longrightarrow \quad \|n\| \leqslant \sqrt[N]{C} n^\alpha.$$

Зафиксировав n и перейдя к пределу при $N \to \infty$, получим

$$\|n\| \leqslant n^\alpha. \tag{9.1}$$

Докажем теперь обратное неравенство. Сначала заметим, что

$$n_0^{s+1} > n \geqslant n_0^s.$$

Так как

$$n_0^{(s+1)\alpha} = \|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leqslant \|n\| + \|n_0^{s+1} - n\|,$$

имеем

$$\|n\| \geqslant \|n_0^{s+1}\| - \|n_0^{s+1} - n\| \geqslant n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha,$$

потому что

$$\|n_0^{s+1} - n\| \leqslant (n_0^{s+1} - n)^\alpha,$$

как было доказано выше. Таким образом, так как $n \geqslant n_0^s$,

$$\|n\| \geqslant n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha = n_0^{(s+1)\alpha} \left[1 - \left(1 - \frac{1}{n_0} \right)^\alpha \right] = C' n_0^{(s+1)\alpha} \geqslant C' n^\alpha$$

для некоторой положительной константы C', не зависящей от n.

Как и выше, применим это неравенство к n^N. Извлекая корень N-й степени и переходя к пределу при $N \to \infty$, получаем

$$\|n\| \geqslant n^{\alpha}. \tag{9.2}$$

Из неравенств (9.1) и (9.2) следует, что $\|n\| = n^{\alpha}$ для всех $n \in \mathbb{N}$. Применяя свойство 2) из определения нормы, мы видим, что $\|x\| = |x|^{\alpha}$. Наконец, предложение 2.6 позволяет нам заключить, что данная норма эквивалентна абсолютной величине $|\cdot|$.

Теперь предположим, что норма $\|\cdot\|$ неархимедова, т.е. $\|n\| \leqslant 1$ для всех натуральных чисел n. Так как мы предположили, что норма $\|\cdot\|$ нетривиальна, можно найти число n_0, которое является минимальным среди всех натуральных чисел, удовлетворяющих неравенству $\|n\| < 1$. Заметим, что это число n_0 обязано быть простым, так как если бы оно было представимо в виде $n_0 = n_1 n_2$, где $n_1, n_2 < n_0$, то выполнялось бы равенство $\|n_1\| = \|n_2\| = 1$ и поэтому мы получили бы $\|n_0\| = \|n_1\|\|n_2\| = 1$. Обозначим это простое число n_0 через p.

Покажем, что если n не делится на p, то $\|n\| = 1$. Разделим n на p с остатком: $n = rp + s$, где $0 < s < p$. Из минимальности числа p вытекает, что $\|s\| = 1$. Мы имеем также $\|rp\| < 1$, так как $\|p\| < 1$ (по выбору p) и $\|r\| \leqslant 1$ (из неархимедовости нормы $\|\cdot\|$). Следовательно,

$$\|n - s\| < \|s\|,$$

и из предложения 2.11 мы получаем, что $\|n\| = \|s\| = 1$. Наконец, для данного $n \in \mathbb{Z}$ можно записать $n = p^v n'$, где p не делит n'. Отсюда

$$\|n\| = \|p\|^v \|n'\| = \|p\|^v.$$

Пусть $\rho = \|p\| < 1$. Тогда $\rho = (1/p)^{\alpha}$ для некоторого положительного действительного числа α. Таким образом,

$$\|n\| = |n|_p^{\alpha}.$$

Теперь легко показать (воспользовавшись свойством 2) из определения нормы), что то же самое соотношение будет выполнено, если вместо n подставить произвольное ненулевое рациональное число x. Применив предложение 2.6, получим $\|\cdot\| \sim |\cdot|_p$, чем завершается доказательство теоремы. □

Предложение 9.2 (формула произведения). *Пусть* $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$. *Тогда для любого* $x \in \mathbb{Q}^{\times}$ *выполняется равенство*

$$\prod_{p \leqslant \infty} |x|_p = 1,$$

где произведение берется по всем простым числам в $\mathbb{N}$, *включая «простое число на бесконечности»*.

Доказательство. Достаточно доказать эту формулу в случае, когда x является натуральным числом, для остальных чисел она будет следовать из мультипликативности нормы. Итак, пусть $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. Тогда $|x|_q = 1$, если $q \neq p_i$, $|x|_{p_i} = p_i^{-a_i}$ для $i = 1, \ldots, k$ и $|x| = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. Утверждение доказано. □

Эта формула устанавливает соотношение между нормами на $\mathbb{Q}$. Например, если мы знаем значения всех норм, кроме одной, то эта формула позволяет нам восстановить значение неизвестной нормы. Это оказывается очень важным в приложениях к алгебраической геометрии.

Предположим, что мы хотим найти корень многочлена в $\mathbb{Q}$. Очевидно, что если этот многочлен имеет корни в $\mathbb{Q}$, то он имеет корни в $\mathbb{R}$ и во всех полях $\mathbb{Q}_p$. Отсюда можно заключить, что если для некоторого $p \leqslant \infty$ многочлен не имеет корней в $\mathbb{Q}_p$, то этот многочлен не имеет корней и в $\mathbb{Q}$ (здесь «∞-адических» снова означает «вещественный»). Обратное утверждение представляется более интересным, но верно ли оно? Если многочлен имеет p-адические корни для всех p, включая ∞, то имеет ли он хотя бы один рациональный корень? Вот простой пример, когда обратное утверждение верно.

Предложение 9.3. *Число* $x \in \mathbb{Q}$ *является квадратом в* $\mathbb{Q}$ *тогда и только тогда, когда оно является квадратом в каждом поле* $\mathbb{Q}_p$, $p \leqslant \infty$.

Доказательство. Для любого $x \in \mathbb{Q}^\times$ имеем

$$x = \pm \prod_{p<\infty} p^{\operatorname{ord}_p(x)}.$$

Если число x является квадратом в $\mathbb{R}$, то оно положительно. В $\mathbb{Q}_p$ можно написать $x = p^{\operatorname{ord}_p(x)} u$, где $u \in \mathbb{Z}_p^\times$ (предложение 5.2). Если x является квадратом в $\mathbb{Q}_p$, то порядок $\operatorname{ord}_p(x)$ должен быть четным и $u = v^2$ для некоторой p-адической единицы $v \in \mathbb{Z}_p^\times$. Если мы перепишем наше исходное разложение, то увидим, что x является полным квадратом в $\mathbb{Q}$. □

Доказанный результат есть проявление так называемого *принципа «от локального к глобальному»*, который утверждает, что существование решений диофантова уравнения в $\mathbb{Q}$ (глобальных решений) может быть установлено путем изучения для каждого $p \leqslant \infty$ решений в $\mathbb{Q}_p$ (локальных решений). К сожалению, этот принцип не является универсальным, хотя он применим в некоторых важных случаях, например для квадратичных форм от нескольких переменных (теорема Минковского—Хассе).

Упражнения

36. Два поля F и K называются *изоморфными*, если существует такое отображение $\varphi: F \to K$, что

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

1) Докажите, что поля $\mathbb{Q}_p$ и $\mathbb{R}$ неизоморфны.

2*) Докажите, что если $p \neq q$ — два простых числа, то поля $\mathbb{Q}_p$ и $\mathbb{Q}_q$ неизоморфны.

37. Пусть $p \neq 2$ — простое число. Обозначим $(\mathbb{Q}_p^\times)^2 = \{a^2 : a \in \mathbb{Q}_p^\times\}$. Докажите, что факторгруппа $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ имеет порядок 4, и укажите представителя для каждого смежного класса.

§ 10. Отступление: что такое $\mathbb{Q}_g$, если число g не простое?

Для того чтобы еще раз оценить красоту p-адических чисел, давайте посмотрим, что получится, если вместо простого числа p взять составное число g. Чтобы воспользоваться для определения нормы $|\cdot|_g$ формулой (4.1), нужно более аккуратно определить $\mathrm{ord}_g(x)$, если x — рациональное число. Если $x \in \mathbb{Z}$, то $\mathrm{ord}_g(x)$ определяется, как и в случае простого числа, как максимальная степень числа g, которая делит x. Если же $x = a/b$, то определение порядка $\mathrm{ord}_g(x)$ отличается от случая $g = p$. Нам потребуется следующая лемма.

Лемма 10.1. *Пусть $x = a/b$, $a, b \in \mathbb{N}$, $(a, b) = 1$. Тогда существуют единственное такое целое число v и такая пара целых чисел a' и b', что $a/b = g^v a'/b'$, $g \nmid a'$ и $(a', b') = (g, b') = 1$.*

Доказательство. Если $g \nmid a$ и $(g, b) = 1$, то, очевидно, можно положить $v = 0$.

Если $g \mid a$, обозначим через g^φ ($\varphi \geqslant 1$) максимальную степень числа g, которая делит a. Положим $a' = ag^{-\varphi}$ и $b' = b$, тогда $g \nmid a'$ и $(a', b') = (g, b') = 1$. Кроме того, имеем

$$\frac{a}{b} = g^\varphi \frac{a'}{b'},$$

и остается положить $v = \varphi > 0$.

Теперь предположим, что $g \nmid a$ и $(g, b) > 1$. Тогда b можно представить в виде $b = b_1 b_2$ ($b_1, b_2 > 0$), причем все простые сомножители числа b_1 делят g и $(b_2, g) = 1$. Аналогично g можно представить в виде $g = g_1 g_2$ ($g_1, g_2 > 0$), так что все простые сомножители числа g_1 делят b_1, но $(g_2, b_1) = (g_2, b) = 1$. Существует минимальное натуральное число ψ для

которого $b_1 \mid g^\psi$ и, значит, $b_1 \mid g_1^\psi$. Тогда в правой части равенства

$$g^\psi \frac{a}{b} = \frac{g_1^\psi}{b_1} \frac{g_2^\psi}{b_2} a$$

частное g_1^ψ / b_1 является целым числом. Таким образом, если положить

$$a' = \frac{g_1^\psi}{b_1} g_2^\psi a \quad \text{и} \quad b' = b_2,$$

то получим

$$\frac{a}{b} = g^{-\psi} \frac{a'}{b'}, \quad g \nmid a', \quad (a', b') = (g, b') = 1,$$

и остается положить $v = -\psi < 0$. □

Теперь если $x = a/b$, то определим $\operatorname{ord}_g(x)$ как целое число v из леммы 10.1 и определим соответствующую норму $|a/b|_g = g^{-v}$. Однако эта норма не является мультипликативной, т. е. не удовлетворяет свойству 2) из определения 2.1. Например,

$$\left|\frac{1}{20}\right|_{10} = 10^2, \quad \left|\frac{1}{50}\right|_{10} = 10^2, \quad \text{но} \quad \left|\frac{1}{20} \cdot \frac{1}{50}\right|_{10} = \left|\frac{1}{1000}\right|_{10} = 10^3 < 10^2 \cdot 10^2.$$

Но конечно, если $g = p$ является простым числом, то это определение совпадает с определением 4.1.

Вообще говоря,

$$|ab|_g \leqslant |a|_g |b|_g, \tag{10.1}$$

поэтому отображение $|\cdot|_g$ является не нормой, а так называемой *псевдонормой* (см. упражнение 38). Тем не менее, функция $d(x, y) = |x - y|_g$ является метрикой, и можно рассмотреть пополнение поля $\mathbb{Q}$ по этой метрике. В результате пополнения получается кольцо $\mathbb{Q}_g$, которое, если число g составное, не является полем (см. упражнение 39).

Следующая теорема принадлежит Гензелю.

Теорема 10.2. *Если число $g = p_1 p_2 \ldots p_k$ является произведением различных простых чисел, то кольцо $\mathbb{Q}_g$ изоморфно прямой сумме p-адических полей: $\mathbb{Q}_g = \mathbb{Q}_{p_1} \oplus \ldots \oplus \mathbb{Q}_{p_k}$.*

Доказательство. Мы построим соответствующий изоморфизм в случае $g = 10$, $p_1 = 2$, $p_2 = 5$, но эта конструкция без затруднений переносится на общий случай.

Рассмотрим последовательность Коши рациональных чисел относительно $|\cdot|_{10}$. Она определяет 10-адическое число

$$A = \lim_{n \to \infty}^{(10)} a_n,$$

и из существования 10-адического предела вытекает существование 2-адического и 5-адического пределов, которые мы обозначим

$$A_2 = \overset{(2)}{\lim_{n\to\infty}} a_n, \quad A_5 = \overset{(5)}{\lim_{n\to\infty}} a_n$$

соответственно. Обратно, очевидно, что из существования пределов A_2 и A_5, очевидно, вытекает существование предела A. Легко видеть, что цифры чисел A_2 и A_5 не зависят от выбора последовательности Коши $\{a_n\}$, с помощью которой определялось число A.

В частности, для $A \in \mathbb{Q}_{10}$ существует каноническое разложение

$$A = \sum_{n=-f}^{\infty} b_n 10^n. \tag{10.2}$$

Чтобы найти цифры чисел A_2 и A_5, запишем

$$A_2 = \sum_{n=-f}^{\infty} (b_n 5^n) 2^n = \sum_{n=-f}^{\infty} c_n 2^n, \quad A_5 = \sum_{n=-f}^{\infty} (b_n 2^n) 5^n = \sum_{n=-f}^{\infty} d_n 2^n,$$

где коэффициенты c_n и d_n соответствующих канонических разложений получаются приведением к каноническому виду (теорема 4.3). Итак, имеем $A = \langle A_2, A_5 \rangle$, и из правил сложения, вычитания и умножения g-адических и p-адических пределов можно получить следующее утверждение: если $B = \langle B_1, B_2 \rangle$ — другое 10-адическое число ($B_2 \in \mathbb{Q}_2$ и $B_5 \in \mathbb{Q}_5$), тогда

$$A \pm B = \langle A_2 \pm B_2, A_5 \pm B_5 \rangle \quad \text{и} \quad AB = \langle A_2 B_2, A_5 B_5 \rangle.$$

Обратно, пусть даны произвольные числа $A_2 \in \mathbb{Q}_2$ и $A_5 \in \mathbb{Q}_5$. Покажем, что существует единственное такое число $A \in \mathbb{Q}_{10}$, что $A = \langle A_2, A_5 \rangle$. Для каждого $p = 2, 5$ пусть $\{a_n^{(p)}\}$ — такая последовательность рациональных чисел, что

$$A_p = \lim_{n\to\infty} a_n^{(p)} \quad \text{по норме } |\cdot|_p.$$

Вообще говоря, последовательность $\{a_n^{(p)}\}$ не обязана сходиться по норме $|\cdot|_q$, если $p \neq q$, и даже может не быть ограниченной по этой норме. Чтобы преодолеть эту трудность, рассмотрим последовательности

$$e_n^{(2)} = \frac{5^n}{2^n + 5^n}, \quad e_n^{(5)} = \frac{2^n}{2^n + 5^n}.$$

Легко видеть, что

$$\lim_{n\to\infty} e_n^{(p)} = \delta_{pq} \quad \text{по норме } |\cdot|_q, \quad \text{где} \quad \delta_{pq} = \begin{cases} 1, & \text{если } p = q, \\ 0, & \text{если } p \neq q. \end{cases}$$

Отсюда вытекает, что существует такая бесконечная подпоследовательность $e_{r_n}^{(p)}$, что

$$\lim_{n\to\infty}^{(q)} a_n^{(p)} e_{r_n}^{(p)} = \begin{cases} A_p, & \text{если } p = q, \\ 0, & \text{если } p \neq q. \end{cases}$$

Значит,

$$\lim_{n\to\infty}^{(10)} a_n^{(2)} e_{r_n}^{(2)} = \langle A_2, 0\rangle \quad \text{и} \quad \lim_{n\to\infty}^{(10)} a_n^{(5)} e_{r_n}^{(5)} = \langle 0, A_5\rangle.$$

Наконец, замечаем, что последовательность $a_n = a_n^{(2)} e_{r_n}^{(2)} + a_n^{(5)} e_{r_n}^{(5)}$ сходится к $\langle A_2, A_5\rangle = A$. □

Упражнения

38. Докажите, что если число g составное, то функция $|\cdot|_g$ является псевдонормой, т.е. она удовлетворяет свойствам 1) и 3) из определения 2.1, а также неравенству (10.1).

39. Докажите, что $\mathbb{Q}_{10}$ не является полем, предъявив делители нуля.

40*. Рассмотрим следующую последовательность натуральных чисел:

$$6,\ 76,\ 376,\ 9376,\ 109376\ldots$$

1) Докажите, что эту последовательность можно продолжить однозначно таким образом, чтобы получить 10-адическое число $\alpha = \ldots 109376$, удовлетворяющее уравнению $\alpha^2 = \alpha$.

2) Докажите, что уравнение $x^2 = x$ имеет в $\mathbb{Z}_{10}$ четыре корня, а именно 0, 1, α и β.

3) Найдите первые 6 цифр числа β.

4) Докажите, что $\mathbb{Z}_{10} \approx \mathbb{Z}_5 \oplus \mathbb{Z}_2$ (прямое произведение групп).

41. Докажите, что на $\mathbb{Q}_p$ не существует *отношения порядка* $>$, удовлетворяющего следующим свойствам:

1) если $x > y$, то $z + x > z + y$ для любого z;

2) если $x > 0$ и $y > 0$, то $xy > 0$;

3) если $x_n > 0$ и существует предел $\lim\limits_{n\to\infty} x_n = x$, то $x \geqslant 0$.

Глава 2

Топология пространства $\mathbb{Q}_p$ в сравнении с топологией $\mathbb{R}$

§ 11. Основные топологические свойства

Поле p-адических чисел во многом похоже на поле действительных чисел: оно является нормированным полем, полным по метрике, порожденной p-адической нормой (теорема 3.4). И поле $\mathbb{R}$, и поле $\mathbb{Q}_p$ являются пополнениями пространства $\mathbb{Q}$, оба содержат $\mathbb{Q}$ в качестве всюду плотного подмножества и поэтому являются сепарабельными пространствами. Поле $\mathbb{R}$ *локально компактно*, т. е. каждая точка содержится в некоторой компактной окрестности; то же самое, как мы скоро увидим, верно и для $\mathbb{Q}_p$ (теорема 11.9).

Сначала рассмотрим $\mathbb{R}$ и $\mathbb{Q}_p$ с точки зрения теории метрических пространств. Открытый шар $B(a, r)$ в $\mathbb{R}$ — это открытый интервал $|x - a| < r$. Открытый шар радиуса $r \in \mathbb{R}^+$ с центром в точке $a \in M$ можно определить для любого метрического пространства (M, d) следующим образом:

$$B(a, r) = \{x \in M: d(a, x) < r\}.$$

В пространстве $\mathbb{Q}_p$ открытыми шарами являются следующие множества:

$$B(a, r) = \{x \in \mathbb{Q}_p: |x - a|_p < r\},$$

и, так как p-адическая норма принимает дискретное множество значений $\{0, p^n; n \in \mathbb{Z}\}$, можно рассматривать только шары радиусов $r = p^n$, $n \in \mathbb{Z}$.

Напомним, что подмножество A метрического пространства M называется *открытым*, если для любой точки $x \in A$ существует шар $B(a, r) \subset A$, содержащий x. Множество $A \subset M$ называется *замкнутым*, если его дополнение $M \setminus A$ открыто.

Пусть $\mathcal{G}$ обозначает семейство всех открытых подмножеств пространства M, а $\mathcal{F}$ обозначает семейство всех замкнутых подмножеств пространства M. По определению каждый элемент семейства $\mathcal{F}$ является дополнением единственного элемента семейства $\mathcal{G}$ и наоборот. Открытые и замкнутые множества обладают следующими свойствами.

Предложение 11.1. 1) *Если $\mathcal{C} \subset \mathcal{G}$ — произвольный набор открытых множеств, то $\bigcup\limits_{G \in \mathcal{C}} G$ принадлежит $\mathcal{G}$. Если $G_1, \ldots, G_n \in \mathcal{G}$ — произвольный конечный набор открытых множеств, то $\bigcap\limits_{i=1}^{n} G_i$ принадлежит $\mathcal{G}$.*

2) *Если* $C \subset \mathcal{F}$ — *произвольный набор замкнутых множеств, то* $\bigcap_{F \in C} F$ *принадлежит* $\mathcal{F}$. *Если* $F_1, \ldots, F_n \in \mathcal{F}$ — *произвольный конечный набор замкнутых множеств, то* $\bigcup_{i=1}^{n} F_i$ *принадлежит* $\mathcal{F}$.

Доказательство мы оставляем читателю (упражнение 42).

Итак, семейство $\mathcal{G}$ замкнуто относительно произвольных объединений и конечных пересечений, а семейство $\mathcal{F}$ замкнуто относительно произвольных пересечений и конечных объединений. Семейство $\mathcal{G}$ открытых подмножеств метрического пространства определяет *топологию*. Понятия окрестности, предела, сходимости, непрерывности и т. д. можно определить в терминах топологии без привлечения метрики. В действительности понятие топологии является более общим и основывается только на свойствах из предложения 11.1 (еще, конечно, предполагается, что все пространство и пустое множество открыты). Вообще говоря, топологические пространства могут быть весьма «патологическими» и довольно сильно отличаться от пространств, в которых топология порождена метрикой.

Если M — топологическое пространство и $X \subset M$, то X можно превратить в топологическое пространство, задав на нем *индуцированную топологию*, объявляя пересечения открытых подмножеств пространства M с X открытыми множествами в X. В случае метрического пространства индуцированная топология получается ограничением метрики пространства M на X.

Возвращаясь к p-адическим числам, рассмотрим *сферу* в $\mathbb{Q}_p$:

$$S(a, r) = \{x \in \mathbb{Q}_p : |x - a|_p = r\}.$$

Следующий важный результат кажется удивительным.

Предложение 11.2. *Сфера* $S(a, r)$ *является открытым множеством в* $\mathbb{Q}_p$.

Доказательство. Пусть $x \in S(a, r)$, $\varepsilon < r$. Покажем, что $B(x, \varepsilon) \subset S(a, r)$. Пусть $y \in B(x, \varepsilon)$. Тогда $|x - y|_p < |x - a|_p = r$ и согласно предложению 2.11 $|y - a|_p = |x - a|_p = r$, а это в точности означает, что $y \in S(a, r)$. □

Этот факт кажется довольно странным, так как в $\mathbb{R}^n$ (в частности, в $\mathbb{R}$) сферы, конечно, не являются открытыми множествами! Давайте посмотрим, что следует из этого странного свойства.

Предложение 11.3. *Шары в* $\mathbb{Q}_p$ *являются одновременно открытыми и замкнутыми множествами.*

Доказательство. В любом метрическом пространстве любой шар $B(a, r)$ является открытым множеством, так как каждая точка $x \in B(a, r)$ содержится в шаре $B(a, r)$, который содержится в $B(a, r)$. Чтобы доказать

замкнутость шара $B(a, r)$, покажем, что его дополнение

$$C = \{x \in \mathbb{Q}_p : |x - a|_p \geqslant r\}$$

открыто. Но $C = S(a, r) \cup D$, где

$$D = \{x \in \mathbb{Q}_p : |x - a|_p > r\}.$$

Множество D открыто (это верно для любого метрического пространства). В самом деле, пусть $y \in D$. Тогда $|y - a|_p = r_1 > r$. Мы утверждаем, что открытый шар $B(y, r_1 - r)$ целиком лежит в D. Действительно, если бы это было неверно, то нашлась бы такая точка $x \in B(y, r_1 - r)$ что $|x - a|_p \leqslant r$. Но тогда

$$r_1 = |y - a|_p = |a - x + x - y|_p \leqslant |a - x|_p + |x - y|_p < r + r_1 - r = r_1,$$

что невозможно. Теперь утверждение следует из того, что объединение двух открытых множеств является открытым. □

Напомним, что точка $x \in M$ называется *граничной точкой* множества $A \subset M$, если любой открытый шар с центром в точке x содержит как точки, принадлежащие, так и точки, не принадлежащие A. Множество A является замкнутым тогда и только тогда, когда оно содержит все свои граничные точки. Из этого определения следует, что в $\mathbb{Q}_p$ сфера $S(a, r)$ не является границей открытого шара $B(a, r)$! Более того, из предложения 11.3 немедленно следует, что $B(a, r)$ не имеет границы вовсе! И конечно, замкнутый шар

$$\overline{B(a, p^n)} = \{x \in \mathbb{Q}_p : |x - a|_p \leqslant p^n\} = \\ = \{x \in \mathbb{Q}_p : |x - a|_p < p^{n+1}\} = B(a, p^{n+1}) \quad (11.1)$$

не является замыканием открытого шара $B(a, p^n)$!

Также из соотношения (11.1) следует, что все утверждения, которые мы доказали для открытых шаров, верны и для замкнутых шаров в $\mathbb{Q}_p$.

Вот еще одно парадоксальное свойство шаров в $\mathbb{Q}_p$. Хотя это утверждение предлагалось в качестве упражнения 12, для полноты изложения приведем его доказательство.

Предложение 11.4. *Если $b \in B(a, r)$, то $B(b, r) = B(a, r)$, иными словами, каждая точка шара является его центром.*

Доказательство. Пусть $x \in B(b, r)$. По нашему предположению

$$|a - b|_p < r, \quad |b - x|_p < r.$$

Применяя сильное неравенство треугольника, получаем

$$|a - x|_p = |(a - b) + (b - x)|_p \leqslant \max(|a - b|_p, |b - x|_p) < r,$$

следовательно, $B(b, r) \subset B(a, r)$. Так как условие $b \in B(a, r)$ эквивалентно условию $a \in B(b, r)$ (оба они записываются в виде $|a - b|_p < r$), точно так же получаем $B(a, r) \subset B(b, r)$, что окончательно доказывает совпадение этих двух шаров. □

Вот еще одно свойство шаров в $\mathbb{Q}_p$.

Предложение 11.5. *Два шара в $\mathbb{Q}_p$ имеют непустое пересечение тогда и только тогда, когда один из них содержится в другом, т.е.*

$$B(a, r) \cap B(b, s) \neq \varnothing \Rightarrow B(a, r) \subset B(b, s) \text{ или } B(a, r) \supset B(b, s).$$

Доказательство. Предположим, что $r \leqslant s$ и $y \in B(a, r) \cap B(b, s)$. Тогда из предложения 11.4 имеем $B(a, r) = B(y, r)$ и $B(b, s) = B(y, s)$. Но $B(y, r) \subset B(y, s)$, откуда следует требуемое включение. □

Предложение 11.6. *Сфера $S(a, r)$ является одновременно открытым и замкнутым множеством.*

Доказательство. Мы уже знаем (предложение 11.2), что множество $S(a, r)$ открыто. Кроме того, множество $\overline{B(a, r)}$ замкнуто, и, так как множество $B(a, r)$ открыто, его дополнение $\{x \in \mathbb{Q}_p : |x - a|_p \geqslant r\}$ замкнуто. Но сфера $S(a, r)$ является пересечением этих двух замкнутых множеств и поэтому замкнута. Заметим, что это доказательство замкнутости сферы работает во всех метрических пространствах. □

Множество всех шаров в $\mathbb{R}$ несчетно, так как несчетно множество всех положительных действительных чисел (теорема Кантора); то же самое верно для множества центров a и для множества радиусов ρ, поэтому, тем более, это верно для множества всех шаров $B(a, \rho)$. Однако для множества шаров в $\mathbb{Q}_p$ справедлив совершенно противоположный результат.

Предложение 11.7. *Множество всех шаров в $\mathbb{Q}_p$ счетно.*

Доказательство. Запишем центр шара $B(a, p^{-s})$ в каноническом виде

$$a = \sum_{n=-m}^{\infty} a_n p^n$$

и положим

$$a_0 = \sum_{n=-m}^{s} a_n p^n.$$

Ясно, что a_0 является рациональным числом и $|a - a_0| < p^{-s}$, т. е. $a_0 \in B(a, p^{-s})$. Тогда согласно предложению 11.4 мы получаем

$$B(a_0, p^{-s}) = B(a, p^{-s}).$$

Таким образом, как центры, так и радиусы образуют счетные множества. Следовательно, множество всех пар (a_0, s) счетно, что и доказывает счетность множества всех шаров в $\mathbb{Q}_p$. □

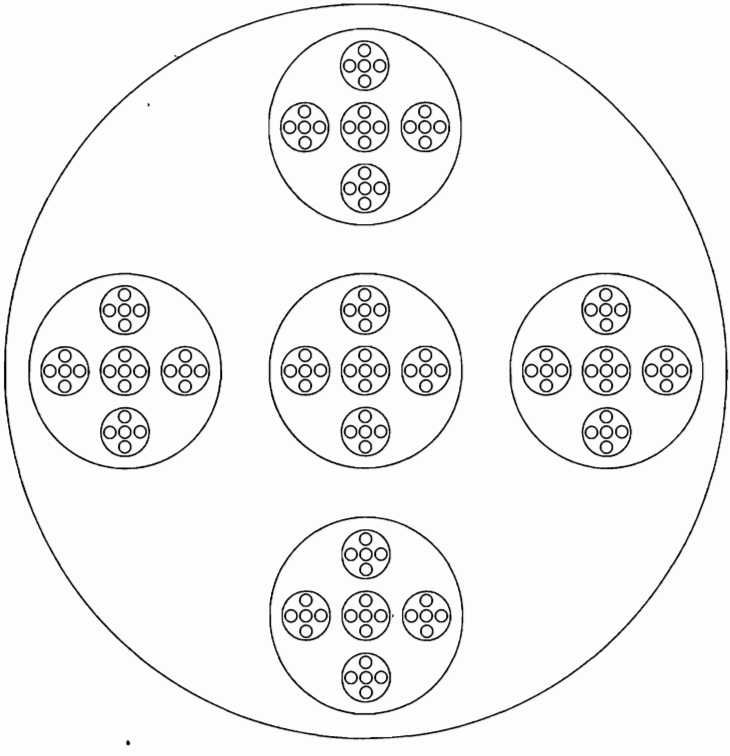
В обозначениях § 5 имеем

$$\mathbb{Z}_p = \overline{B(0,\ 1)} = B(0,\ p)$$

и

$$\mathbb{Z}_p^\times = S(0,\ 1) = (1 + p\mathbb{Z}_p) \cup (2 + p\mathbb{Z}_p) \cup \ldots \cup ((p-1) + p\mathbb{Z}_p).$$

Схематично это изображено на рисунке для $p = 5$. Сфера $\mathbb{Z}_5^\times$ является объединением четырех открытых шаров, что находится в полном согласии с предложением 11.2. Центральный шар представляет собой максимальный идеал $5\mathbb{Z}_5$ в кольце $\mathbb{Z}_5$.



Определение 11.8. Множество K в метрическом пространстве называется *секвенциально компактным*, если каждая бесконечная последовательность точек из K содержит подпоследовательность, сходящуюся к точке из K.

Согласно теореме Гейне—Бореля для метрических пространств это условие эквивалентно *компактности*. (Напомним, что множество K на-

зывается *компактным*, если любое открытое покрытие множества K содержит конечное подпокрытие.)

Как мы уже видели (теорема 4.6), пространство $\mathbb{Z}_p$ секвенциально компактно. Таким образом, пространство $\mathbb{Z}_p$ компактно, и согласно упражнению 22 отсюда следует компактность любого шара в $\mathbb{Q}_p$. Мы получаем следующий результат.

Теорема 11.9. *Пространство $\mathbb{Q}_p$ локально компактно.*

Вот еще одно довольно неожиданное утверждение.

Предложение 11.10. *Пространство $\mathbb{Z}_p$ полно.*

Доказательство. Так как любая последовательность Коши элементов пространства $\mathbb{Z}_p$ содержит подпоследовательность, сходящуюся к некоторому элементу пространства $\mathbb{Z}_p$, который мы обозначим a, и сама последовательность должна сходиться к тому же элементу a, что и доказывает полноту пространства $\mathbb{Z}_p$. □

Теорема 11.11. *Множество $\mathbb{N}$ плотно в $\mathbb{Z}_p$.*

Доказательство. Пусть $x = \ldots a_2 a_1 a_0 \in \mathbb{Z}_p$. Для каждого $n \in \mathbb{N}$ положим

$$x_n = \ldots 00 a_n a_{n-1} \ldots a_0 = \sum_{i=0}^{n} a_i p^i.$$

Тогда $x_n \in \mathbb{N}$ и $|x - x_n| < p^{-n}$, откуда вытекает требуемое утверждение. □

Определение 11.12. Топологическое пространство X называется *несвязным*, если его можно представить в виде объединения двух непересекающихся непустых открытых множеств. В противном случае пространство X называется *связным*.

Подмножество пространства X называется *связным*, если оно является связным пространством в индуцированной топологии.

Пространство X называется *вполне несвязным*, если все его связные подмножества исчерпываются пустым множеством и одноточечными множествами $\{a\}$ $(a \in X)$.

Пример 11.13. Любой интервал в $\mathbb{R}$ связен, т. е. не может быть представлен в виде объединения двух непустых непересекающихся открыто-замкнутых множеств.

Теорема 11.14. *Пространство $\mathbb{Q}_p$ вполне несвязно.*

Доказательство. Для каждого $a \in \mathbb{Q}_p$ и $n \in \mathbb{N}$ множество

$$U_n(a) = \{x \in \mathbb{Q}_p : |x - a|_p \leqslant p^{-n}\} = \{x \in \mathbb{Q}_p : |x - a|_p < p^{-n+1}\}$$

является открытой и замкнутой окрестностью точки a. Пусть $a \in A$, причем $A \neq \{a\}$. Тогда существует такое $n \in \mathbb{N}$, что $U_n(a) \cap A \neq A$. Таким образом,

$$A = (U_n(a) \cap A) \cup (\mathbb{Q}_p \setminus U_n(a) \cap A),$$

где множество $U_n(a)$ и его дополнение $\mathbb{Q}_p \setminus U_n(a)$ открыты и непусты; отсюда следует, что A не может быть связным. □

Вернемся к мультипликативной группе $\mathbb{Q}_p^\times$ поля $\mathbb{Q}_p$. Мы уже видели (упражнение 37), что если $p \neq 2$, то факторгруппа $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ имеет порядок 4 и изоморфна группе $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Для $p = 2$ факторгруппа $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ изоморфна группе $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, причем в качестве множества представителей можно взять $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

Теорема 11.15. *Подгруппа $(\mathbb{Q}_p^\times)^2$ группы $\mathbb{Q}_p^\times$ является открытым подмножеством в $\mathbb{Q}_p^\times$.*

Доказательство. Напомним, что p-адическое число $x \neq 0$ является квадратом тогда и только тогда, когда $x = p^{2n}u^2$ для некоторых $n \in \mathbb{Z}$ и $u \in \mathbb{Z}_p^\times$. Пусть $x \in (\mathbb{Q}_p^\times)^2$ и $y \in \mathbb{Q}_p$ выбраны так, что $|x - y|_p < p^{-2n}$. Тогда по свойству равнобедренного треугольника (см. предложение 2.11) имеем $|y|_p = |x|_p = p^{-2n}$, и, значит, $y = p^{2n}v$ для некоторого $v \in \mathbb{Z}_p^\times$. Отсюда получаем $|y - x|_p = p^{-2n}|v - u^2|_p < p^{-2n}$, следовательно, $|v - u^2| < 1$. Последнее неравенство означает, что первые цифры этих двух p-адических единиц совпадают. Но тогда из леммы Гензеля следует, что v также является квадратом в $\mathbb{Z}_p$, и поэтому $y \in (\mathbb{Q}_p^\times)^2$. □

Упражнения

42. Докажите предложение 11.1.

§ 12. Канторово множество

Этот параграф посвящен в основном вопросам вещественного анализа. Положим

$$C_0 = I = [0, 1],\ C_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right],$$

$$C_2 = \left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right], \ldots$$

Множество C_n является объединением 2^n отрезков, каждый из которых имеет длину 3^{-n}. Кроме того, имеют место включения $C_0 \supset C_1 \supset C_2 \supset \ldots$ Все множества C_n замкнуты, поэтому множество

$$C := \bigcap_{n=0}^{\infty} C_n \neq \varnothing$$

является замкнутым подмножеством единичного отрезка I.

Рассмотрим представление действительных чисел из отрезка $I = [0, 1]$ в виде бесконечных дробей по основанию 3. Заметим, что концевые точки отрезков, из которых состоит C_n, имеют два таких разложения, например,

$$\frac{2}{9} = 0{,}02 = 0{,}012222\ldots, \quad \frac{1}{3} = 0{,}1 = 0{,}022222\ldots,$$

причем одно из них не содержит цифру 1. Выбрав разложения концевых точек таким образом, чтобы они не содержали единиц, замечаем, что разложение любой точки из C в троичную дробь содержит только цифры 0 и 2, потому что остальные точки из C раскладываются в троичную дробь единственным образом, причем по построению их разложения не содержат единиц.

Обратно, каждая точка из I, разложение которой содержит только нули и двойки, принадлежит пересечению всех множеств C_n: если первая цифра — нуль, то точка принадлежит отрезку [0, 0,02222...], если же первая цифра — двойка, то точка принадлежит отрезку [0,2, 0,2222...], точно так же вторая цифра определяет, какому отрезку (левому или правому) из множества C_2 принадлежит наша точка и т. д.

Суммируя сказанное выше, получаем следующий результат

Предложение 12.1. *Троичное канторово множество C состоит из всех точек отрезка I, которые могут быть представлены в виде троичной дроби с помощью цифр* 0 *и* 2.

Доказательство следующего утверждения иллюстрирует очень важный метод в элементарной теории бесконечных множеств, так называемый диагональный процесс Кантора.

Предложение 12.2. *Канторово множество C несчетно.*

Доказательство. Это следует из канторовского диагонального процесса. Пусть множество C счетно, тогда занумеруем его точки и разложим их в троичную дробь:

$$x_1 = 0{,}a_{11}a_{12}\ldots, \qquad x_2 = 0{,}a_{21}a_{22}\ldots,$$

Рассмотрим точку $c = 0{,}c_1c_2\ldots$, которая строится следующим образом: $c_1 = \{0, 2\} \setminus a_{11}$, $c_2 = \{0, 2\} \setminus a_{22}$ и т. д. Тогда по предложению 12.1 c принадлежит множеству C, но не совпадает ни с одной точкой $(x_1, x_2, \ldots)$ из нашего списка. Итак, мы получили противоречие. □

Замечание 12.3. В нашей итерационной процедуре построения множества C на каждом шаге мы выкидываем среднюю треть из каждого остающегося отрезка. По этой причине C часто называют троичным канторовым множеством. Эту конструкцию можно модифицировать, выбрасывая, скажем, одну четвертую, или одну десятую, или еще какую-то часть остающихся отрезков. Таким образом можно построить множества с довольно парадоксальными свойствами, см. упражнение 51.

Определение 12.4. Множество называется *совершенным*, если оно замкнуто и не содержит изолированных точек.

Предложение 12.5. *Канторово множество C совершенно.*

Доказательство. Пусть $x \in C$ и S — произвольный интервал, содержащий x. Так как $x \in \bigcap_{n=0}^{\infty} C_n$, мы получаем, что $x \in C_n$. Пусть I_n — отрезок, входящий в C_n, который содержит x. Для достаточно большого n имеем $I_n \subset S$. Пусть x_n — концевая точка отрезка I_n, причем $x_n \neq x$. По построению множества C мы имеем $x_n \in C$ и $x_n \in S$. Таким образом, любой интервал S, содержащий точку x, содержит и другие точки из C, поэтому множество C совершенно. □

Далее мы увидим, что канторово множество является геометрической моделью множества целых p-адических чисел для любого простого числа p. Но сначала напомним некоторые определения, связанные с непрерывными отображениями метрических пространств.

Определение 12.6. Пусть (X, d) и (Y, ρ) — два метрических пространства. Тогда отображение $f: X \to Y$ называется

1) *непрерывным*, если для каждого открытого подмножества $V \subset Y$ его прообраз $f^{-1}(V)$ является открытым множеством в X;

2) *открытым*, если для любого открытого множества $U \subset X$ его образ $f(U)$ открыт в Y;

3) *гомеоморфизмом*, если оно непрерывно и биективно, причем обратное отображение также непрерывно;

4) *непрерывным в точке* x, если для любой окрестности A точки $f(x)$ в Y ее прообраз $f^{-1}(A)$ содержит окрестность точки x;

5) *равномерно непрерывным*, если для каждого $\varepsilon > 0$ существует такое $\delta > 0$, что $\rho(f(x_1), f(x_2)) < \varepsilon$, если $d(x_1, x_2) < \delta$.

Теорема 12.7. *Множество целых 2-адических чисел $\mathbb{Z}_2$ гомеоморфно канторову множеству C.*

Доказательство. Рассмотрим отображение $\psi: \mathbb{Z}_2 \to C$,

$$\sum_{i=0}^{\infty} a_i 2^i \overset{\psi}{\mapsto} \sum_{i=0}^{\infty} \frac{2a_i}{3^{i+1}}.$$

Покажем, что ψ является гомеоморфизмом. Сначала заметим, что из единственности представлений элементов множеств $\mathbb{Z}_2$ и C вытекает биективность отображения ψ.

Если $|x_1 - x_2| < 1/3^N$, то числа x_1 и x_2 принадлежат одному и тому же или соседним отрезкам, которые образуются при разбиении отрезка I на 3^N равных частей. Но так как отрезки, образующие C_N, не имеют общих концов, числа x_1 и x_2 лежат в одной и той же компоненте I_N множества C_N, и поэтому их первые N цифр совпадают.

Обратно, если первые N цифр чисел $x_1, x_2 \in C$ совпадают, то эти числа лежат в одной и той же компоненте I_N множества C_N. С другой стороны, первые N цифр 2-адических чисел y_1 и y_2 совпадают тогда и только тогда,

когда $|y_1 - y_2|_2 < 1/2^N$. Из того, что $1/2^N$ и $1/3^N$ стремятся к 0 при $N \to \infty$, следует, что отображения ψ и ψ^{-1} непрерывны. □

Следствие 12.8. *Канторово множество C вполне несвязно.*

Доказательство. Из предложения 11.14 следует, что пространство $\mathbb{Z}_2$ вполне несвязно. Поэтому по теореме 12.7 это же верно и для C. □

Определение 12.9. Подмножество $A \subset X$ называется *всюду плотным* в X, если его замыкание $\bar{A}$ совпадает с X. Подмножество $A \subset X$ называется *нигде не плотным* в X, если множество $X \setminus \bar{A}$ всюду плотно в X.

Из следствия 12.8 вытекает, что канторово множество не содержит никакого интервала (для замкнутого множества это эквивалентно свойству быть нигде не плотным).

Теперь рассмотрим $\mathbb{Z}_p$. Существует множество типа канторовского, гомеоморфное множеству $\mathbb{Z}_p$: это множество всех действительных чисел из отрезка $I = [0, 1]$, разложения которых по основанию $2p - 1$ содержат только четные цифры. Это множество строится при помощи процедуры, которая похожа на процедуру построения троичного канторова множества. Чтобы получить C_1, разделим I на $2p - 1$ равных частей и удалим каждый второй интервал. Легко видеть, что C_1 содержит те и только те точки из I, которые могут быть записаны в виде дроби по основанию $2p - 1$ $0{,}a_1a_2\ldots$, причем a_1 четно. Повторяя ту же самую процедуру для каждого из отрезков, составляющих C_1, мы получим замкнутое множество C_2, которое состоит из точек с четными двумя первыми цифрами a_1 и a_2, и так далее. Пересечение $C^p = \bigcap\limits_{n=0}^{\infty} C_n$ является множеством типа канторовского, которое несчетно и совершенно. Отображение

$$\sum_{i=0}^{\infty} a_i p^i \overset{\psi_p}{\mapsto} \sum_{i=0}^{\infty} \frac{2a_i}{(2p-1)^{i+1}}$$

из $\mathbb{Z}_p$ в C^p является гомеоморфизмом, что можно доказать примерно так же, как и теорему 12.7. Множество $\mathbb{Z}_5$ схематично изображено на с. 52.

Более того, пространства $\mathbb{Z}_2$ и $\mathbb{Z}_p$ для любого простого числа p гомеоморфны. Чтобы это доказать, достаточно построить гомеоморфизм между двумя канторовыми множествами C^p и C. Но, как часто бывает в математике, обобщения делают задачу проще. Поэтому мы докажем более общий факт (теорему 12.12), а для этого нам понадобятся две леммы.

Лемма 12.10. *Пусть $A \subset \mathbb{R}$ — открытое множество. Тогда A является объединением не более чем счетной совокупности попарно непересекающихся интервалов.*

Доказательство. Как следует из [9], теорема 2.47, связными компонентами множества A являются интервалы. Затем, как это часто дела-

ется в анализе, мы воспользуемся тем, что множество $\mathbb{Q}$ всюду плотно в $\mathbb{R}$: каждая связная компонента множества A содержит рациональную точку, и, так как множество рациональных чисел счетно и компоненты множества A не пересекаются, множество связных компонент множества A не более чем счетно. □

Лемма 12.11. *Пусть $f: A \to B$ — монотонное взаимно однозначное отображение двух замкнутых подмножеств $\mathbb{R}$. Тогда f — гомеоморфизм.*

Доказательство. Заметим, что f^{-1} также является биекцией, поэтому достаточно доказать непрерывность монотонной биекции (которая обязательно будет строго монотонной). Пусть $c \in A$ — предельная точка множества A. Так как A замкнуто, существует такая монотонная последовательность точек из A (ее без потери общности можно считать строго возрастающей), что $\lim\limits_{n\to\infty} x_n = x$. Тогда $\{f(x_n)\}$ — строго возрастающая последовательность точек из множества B такая, что $f(x_n) < x$. Так как множество B замкнуто $\lim\limits_{n\to\infty} f(x_n) = L \in B$, $f(x_n) < L$ и, значит, $L \leqslant f(x)$. Если предположить, что $L < f(x)$, то получится, что $f^{-1}(L) < x$, и значит найдется такое x_n из нашей последовательности, для которого $f(x_n) > L$. А это противоречит показанному выше. Значит, $\lim\limits_{n\to\infty} f(x_n) = f(x)$. □

Теорема 12.12. *Любое компактное совершенное вполне несвязное подмножество $A \subset \mathbb{R}$ гомеоморфно канторову множеству C.*

Доказательство. Из компактности множества A следует его ограниченность; из того, что A вполне несвязно, можно заключить, что A нигде не плотно (и поэтому не содержит никакого интервала). Пусть $m = \inf A$ (точная нижняя грань) и $M = \sup A$ (точная верхняя грань). Мы построим такое строго монотонное отображение $F: [m, M] \to [0, 1]$, что $F(A) = C$. Множество $[m, M] \setminus A$ является объединением не более чем счетной совокупности попарно непересекающихся интервалов, не имеющих общих концов. Это множество интервалов не может быть конечным, так как A нигде не плотно. Обозначим это счетное множество интервалов через $\mathcal{I}$.

Сейчас мы построим биекцию между множеством $\mathcal{I}$ и множеством интервалов, которые образуют дополнение канторова множества C до отрезка $[0, 1]$. Возьмем один из интервалов, имеющих максимальную длину (их число конечно); обозначим его через I_1. Определим F на интервале I_1 как возрастающее линейное отображение, образ которого есть интервал $(1/3, 2/3)$. Рассмотрим интервалы I_{21} и I_{22}, имеющие максимальные длины и расположенные соответственно слева и справа от интервала I_1. Отобразим их линейно на интервалы $(1/9, 2/9)$ и $(7/9, 8/9)$ соответственно и т. д. Продолжая эту процедуру, мы получим строго монотонное взаимно однозначное отображение $[m, M] \setminus A \to [0, 1] \setminus C$. Чтобы в этом убедить-

ся, заметим, что максимальные длины интервалов, выбираемых на каждом шаге, убывают, и, так как для каждого интервала $I \subset [m, M] \setminus A$ существует только конечное количество интервалов в $[m, M] \setminus A$, длины которых превосходят $|I|$, рано или поздно мы дойдем до любого интервала из $\mathcal{I}$. Итак, мы построили биекцию между множеством интервалов $\mathcal{I}$ в $[m, M] \setminus A$ и множеством их образов в $[0, 1] \setminus C$ при отображении F, причем эта биекция сохраняет порядок следования интервалов, т. е. интервал A расположен левее интервала B тогда и только тогда, когда интервал $F(A)$ расположен левее интервала $F(B)$. Таким образом, отображение $F\colon [m, M] \setminus A \to [0, 1] \setminus C$ взаимно однозначно. Это отображение по построению строго монотонно на каждом интервале из $\mathcal{I}$, и если точки x и y $(x < y)$ принадлежат разным интервалам, то $F(x) < F(y)$, так как отображение F сохраняет порядок следования интервалов. Отображение F можно продолжить по непрерывности на множество E концевых точек выкинутых интервалов. Получившееся отображение снова будет возрастающим. Для каждой точки $a \in A$ рассмотрим множество

$$L_a = \{x \in E\colon x < a\}$$

и положим $F(a) = \sup\{f(x);\ x \in L_a\}$. Так как $a = \sup(L_a)$ и функция F монотонно возрастает на $([m, M] \setminus A) \cup E$, отображение F продолжается на весь отрезок $[m, M]$ до монотонно возрастающей функции. Ограничивая F на A и применяя лемму 12.11, получаем требуемый гомеоморфизм между A и C. □

Следствие 12.13. *Пространства $\mathbb{Z}_2$ и $\mathbb{Z}_p$ гомеоморфны.*

Вот еще одно замечательное применение результатов, изложенных выше.

Теорема 12.14. *Существует непрерывное отображение единичного отрезка I на единичный квадрат I^2.*

Доказательство[1]. Рассмотрим отображение $f\colon C \to C^2$, описанное в упражнении 47. Это отображение является гомеоморфизмом, следовательно, оно непрерывно. Пусть $g\colon C \to I$ — композиция гомеоморфизма между C и $\mathbb{Z}_2$ и отображения, описанного в упражнении 45. Отображение g также непрерывно. Декартов квадрат этого отображения $g \times g\colon C^2 \to I^2$ является непрерывным сюръективным отображением. Тогда мы получаем непрерывное отображение $(g \times g) \circ f\colon C \to I^2$ канторова множества C на единичный квадрат I^2. Так как $C \subset I$, это отображение можно продолжить по линейности на интервалы, которые составляют дополнение множества C. Полученное отображение отрезка I на квадрат I^2 является искомым. □

[1] Эта конструкция принадлежит А. Шиндяпину.

Построенное отображение является разновидностью так называемой *кривой Пеано*, которая обычно строится путем итераций.

Упражнения

43. Докажите, что отображение непрерывно тогда и только тогда, когда оно непрерывно в каждой точке.

44. Докажите, что непрерывный образ связного множества связен.

45. Рассмотрим отображение $\varphi: \mathbb{Q}_p \to \mathbb{R}$, которое сопоставляет каждому p-адическому числу действительное число, записанное по основанию p, следующим образом:

$$\ldots b_2 b_1 b_0, b_{-1} b_{-2} \ldots b_{-k} \mapsto b_{-k} \ldots b_{-2} b_{-1}, b_0 b_1 b_2 \ldots$$

1) Докажите, что φ является непрерывным отображением $\mathbb{Q}_p$ на множество $\mathbb{R}_+$ всех неотрицательных действительных чисел.

2) Докажите, что φ отображает $\mathbb{Z}_p$ на отрезок $[0, 1]$.

3) Докажите, что отображение φ не взаимно однозначно.

46. Рассмотрим отображение $f: I \to I^2$ единичного отрезка I на единичный квадрат $I^2 = I \times I$, определенное следующим образом:

$$(0, x_1 x_2 x_3 x_4 \ldots) \mapsto (0, x_1 x_3 x_5 \ldots,\ 0, x_2 x_4 x_6 \ldots)$$

(чтобы определить это отображение корректно, мы запрещаем «хвост», состоящий из одних девяток). Докажите, что это отображение не является непрерывным.

47. Рассмотрим отображение $f: C \to C^2$ канторова множества C на его декартов квадрат, определенное следующим образом:

$$(0, x_1 x_2 x_3 x_4 \ldots) \mapsto (0, x_1 x_3 x_5 \ldots,\ 0, x_2 x_4 x_6 \ldots).$$

Докажите, что f — гомеоморфизм.

48. Пусть даны два счетных всюду плотных подмножества A и B единичного интервала $(0, 1)$. Постройте монотонно возрастающее отображение $\psi: (0, 1) \to (0, 1)$, переводящее A в B. Выведите отсюда, что подмножества A и B гомеоморфны.

49*. Пусть $A = \mathbb{Q} \cap [0, 1]$ и $B = \mathbb{Q} \cap (0, 1)$. Докажите, что A и B гомеоморфны.

50*. Существует ли непустое совершенное подмножество в $\mathbb{R}$, которое не содержит рациональных чисел?

51*. Модифицируйте конструкцию канторова множества C таким образом, чтобы получить множество положительной меры, гомеоморфное множеству C, т. е. такое подмножество отрезка $[0, 1]$ типа канторова множества, чтобы сумма длин интервалов его дополнения была строго меньше 1.

Глава 3
Математический анализ в $\mathbb{Q}_p$

§ 13. Последовательности и ряды

В этом параграфе мы рассмотрим основные свойства, связанные со сходимостью последовательностей и рядов в $\mathbb{Q}_p$. Мы уже отмечали основной результат: $\mathbb{Q}_p$ является полным метрическим пространством, поэтому любая последовательность Коши сходится. Последовательности Коши можно охарактеризовать следующим образом.

Теорема 13.1. *Последовательность $\{a_n\}$ элементов пространства $\mathbb{Q}_p$ является последовательностью Коши и, таким образом, сходится тогда и только тогда, когда*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0. \tag{13.1}$$

Доказательство. Если $\{a_n\}$ — последовательность Коши, то

$$\lim_{\substack{m\to\infty \\ n\to\infty}} |a_m - a_n|_p = 0.$$

В частности, если положить $m = n + 1$, то получим (13.1). Это верно для последовательностей Коши в любом метрическом пространстве.

Обратное утверждение в $\mathbb{R}$, конечно, неверно (приведите пример). Однако в ультраметрических пространствах оно верно. В самом деле, пусть выполнено условие (13.1). Это означает, что для любого $\varepsilon > 0$ существует такое натуральное число N, что для любого $n > N$ выполняется неравенство

$$|a_{n+1} - a_n|_p < \varepsilon.$$

Возьмем любые $m > n > N$ и, применяя к выражению $|a_m - a_n|_p$ сильное неравенство треугольника, получим

$$\begin{aligned} |a_m - a_n|_p &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + \ldots - a_n|_p \leqslant \\ &\leqslant \max(|a_m - a_{m-1}|_p, |a_{m-1} - a_{m-2}|_p, \ldots, |a_{n+1} - a_n|_p) < \varepsilon, \end{aligned}$$

что и требовалось доказать. □

Теперь рассмотрим ряд $\sum\limits_{i=1}^{\infty} a_i$ в $\mathbb{Q}_p$. Будем говорить, что ряд *сходится*, если последовательность его частичных сумм $S_n = \sum\limits_{i=1}^{n} a_i$ сходится в $\mathbb{Q}_p$, и что ряд *сходится абсолютно*, если сходится вещественный ряд $\sum\limits_{i=1}^{\infty} |a_i|_p$.

Как и в случае $\mathbb{R}$, из неравенства треугольника следует, что абсолютно сходящийся ряд сходится.

Предложение 13.2. *Если ряд $\sum |a_i|_p$ сходится в $\mathbb{R}$, то ряд $\sum a_i$ сходится в $\mathbb{Q}_p$.*

Доказательство. Так как ряд $\sum |a_i|_p$ сходится, последовательность его частичных сумм является последовательностью Коши, т. е. для любого $\varepsilon > 0$ существует такое натуральное число N, что для всех n, m, удовлетворяющих неравенству $m > n > N$, выполняется неравенство

$$\sum_{i=n+1}^{m} |a_i|_p < \varepsilon.$$

Применяя неравенство треугольника, получаем

$$|S_m - S_n|_p = \left|\sum_{i=n+1}^{m} a_i\right|_p \leqslant \sum_{i=n+1}^{m} |a_i|_p < \varepsilon,$$

откуда следует, что последовательность $\{S_n\}$ является последовательностью Коши, и поэтому ряд $\sum a_i$ сходится в $\mathbb{Q}_p$. □

Как обычно, мы ожидаем, что в $\mathbb{Q}_p$ дела со сходимостью рядов обстоят лучше. И действительно, следующий результат является следствием теоремы 13.1.

Предложение 13.3. *Ряд $\sum\limits_{n=1}^{\infty} a_n$ $(a_n \in \mathbb{Q}_p)$ сходится в $\mathbb{Q}_p$ тогда и только тогда, когда $\lim\limits_{n\to\infty} a_n = 0$; в этом случае*

$$\left|\sum_{n=1}^{\infty} a_n\right|_p \leqslant \max_n |a_n|_p.$$

Доказательство. Сходимость рассматриваемого ряда эквивалентна сходимости последовательности его частичных сумм $S_n = \sum\limits_{i=1}^{n} a_i$. Но $a_n = S_{n+1} - S_n$. Поэтому из теоремы 13.1 следует, что $\{a_n\}$ стремится к 0 тогда и только тогда, когда ряд $\sum\limits_{n=1}^{\infty} a_n$ сходится.

Теперь предположим, что ряд $\sum\limits_{n=1}^{\infty} a_n$ сходится. Если $\sum\limits_{n=1}^{\infty} a_n = 0$, то доказывать нечего. Если же это не так, то, поскольку $a_n \to 0$, из упражнения 52

следует, что существует натуральное число N, удовлетворяющее условиям

$$\left|\sum_{n=1}^{\infty} a_n\right|_p = \left|\sum_{n=1}^{N} a_n\right|_p$$

и, следовательно, используя предложение 2.11, получаем

$$\max\{|a_n|_p;\ 1 \leqslant n \leqslant N\} = \max_n |a_n|_p.$$

Из сильного неравенства треугольника имеем

$$\left|\sum_{n=1}^{N} a_n\right|_p \leqslant \max\{|a_n|_p;\ 1 \leqslant n \leqslant N\} = \max_n |a_n|_p,$$

что и требовалось доказать. □

Аналогичное утверждение для $\mathbb{R}$ *неверно*. Наиболее известный пример расходящегося вещественного ряда с общим членом, стремящимся к нулю, — гармонический ряд $\sum \frac{1}{n}$. Впрочем, существуют и более тонкие примеры, скажем, $\sum\left(\frac{1}{n}\right)\ln n$ или $\sum\limits_{p \text{ простое}} \frac{1}{p}$.

Определение 13.4. Ряд $\sum\limits_{n=0}^{\infty} a_n$ сходится *безусловно*, если для любой перестановки его членов $a_n \to a'_n$ ряд $\sum\limits_{n=0}^{\infty} a'_n$ также сходится.

Очевидно, что из безусловной сходимости вытекает обычная сходимость. Однако в $\mathbb{Q}_p$ верно и обратное.

Теорема 13.5. *Если ряд $\sum\limits_{n=0}^{\infty} a_n$ сходится, то он сходится безусловно и его сумма не зависит от перестановки членов.*

Доказательство. Пусть $\varepsilon > 0$ — произвольное положительное действительное число. Пусть также N — такое натуральное число, что для всех $n > N$ выполнены неравенства $|a_n|_p < \varepsilon$, $|a'_n|_p < \varepsilon$ и

$$\left|\sum_{n=1}^{\infty} a_n - \sum_{n=1}^{N} a_n\right|_p < \varepsilon. \tag{13.2}$$

Положим $S = \sum\limits_{n=1}^{N} a_n$, $S' = \sum\limits_{n=1}^{N} a'_n$ и обозначим через S_1 и S'_1 соответственно сумму всех членов из S, для которых $|a_n|_p > \varepsilon$, и сумму всех членов из S', для которых $|a'_n|_p > \varepsilon$. Ясно, что S_1 и S'_1 содержат одни и те же члены, поэтому $S_1 = S'_1$. Сумма S отличается от суммы S_1 членами, удовлетворяющими неравенству $|a_n|_p < \varepsilon$, и точно так же S' отличается от S'_1 членами,

удовлетворяющими неравенству $|a'_n|_p < \varepsilon$. Таким образом, $|S - S_1|_p < \varepsilon$ и $|S' - S'_1|_p < \varepsilon$, поэтому $|S - S'|_p < \varepsilon$. Сопоставляя эти результаты с (13.2), получаем

$$\left|\sum_{n=1}^{\infty} a_n - \sum_{n=1}^{N} a'_n\right|_p < \varepsilon.$$

Так как $\varepsilon \to 0$ и $N \to \infty$, мы видим, что ряд $\sum\limits_{n=1}^{\infty} a'_n$ сходится и

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} a'_n,$$

что и требовалось доказать. □

В вещественном случае ситуация совершенно иная. Там перестановка членов ряда может изменить сумму и даже сделать ряд расходящимся. Однако перестановки членов ни на что не влияют, если ряд сходится абсолютно (по теореме Дирихле; помните ли вы, как она доказывается?). Теорема 13.5 кажется еще более удивительной, так как следующее утверждение верно не только в вещественном, но и в p-адическом случае.

Теорема 13.6. *В пространстве $\mathbb{Q}_p$ существует ряд $\sum\limits_{n=1}^{\infty} a_n$, который сходится, но не сходится абсолютно.*

Доказательство. Рассмотрим следующий ряд, составленный из повторяющихся членов: 1; p повторяется p раз; p^2 повторяется p^2 раз; и т.д. Очевидно, что члены этого ряда стремятся к 0, поэтому он сходится. Однако

$$\sum_{n=1}^{\infty} |a_n|_p = 1 + p \cdot p^{-1} + p^2 \cdot p^{-2} + \ldots = \infty,$$

что и утверждалось. □

Следующий результат связан с перестановкой порядка суммирования в двойных рядах, довольно тонким вопросом в вещественном случае.

Теорема 13.7. *Рассмотрим такие p-адические числа b_{ij}, $i, j = 1, 2, \ldots$, что для любого $\varepsilon > 0$ существует натуральное число $N = N(\varepsilon)$, для которого*

$$\max(i, j) \geqslant N \Rightarrow |b_{ij}| < \varepsilon.$$

Тогда оба ряда

$$\sum_i \left(\sum_j b_{ij}\right) \quad \text{и} \quad \sum_j \left(\sum_i b_{ij}\right)$$

сходятся и их суммы равны.

Доказательство. По предложению 13.3 внутренние ряды $\sum_j b_{ij}$ и $\sum_i b_{ij}$ сходятся (первый — для всех i, второй — для всех j). Кроме того, для всех $i \geqslant N$ имеем

$$\left|\sum_j b_{ij}\right|_p \leqslant \max_j |b_{ij}|_p < \varepsilon,$$

и точно так же для всех $j \geqslant N$ имеем

$$\left|\sum_i b_{ij}\right|_p < \varepsilon.$$

Отсюда следует сходимость обоих двойных рядов. Чтобы доказать равенство их сумм, напишем

$$\left|\sum_{i=1}^{\infty}\left(\sum_{j=1}^{\infty} b_{ij}\right) - \sum_{i=1}^{N}\left(\sum_{j=1}^{N} b_{ij}\right)\right|_p = \left|\sum_{i=1}^{N}\left(\sum_{j=N+1}^{\infty} b_{ij}\right) + \sum_{i=N+1}^{\infty}\left(\sum_{j=1}^{\infty} b_{ij}\right)\right|_p < \varepsilon,$$

что может выполняться для любого ε лишь в том случае, когда суммы обоих рядов равны. □

По сути, это еще один вариант результата о перестановках членов в рядах.

Упражнения

52. Пусть $\lim_{n\to\infty} a_n = a$ в $\mathbb{Q}_p$. Докажите, что либо $\lim_{n\to\infty} |a_n|_p = 0$, либо существует такое натуральное число N, что $|a_n|_p = |a|_p$ для всех $n \geqslant N$.

53. Докажите, что последовательность $a_n = 2^{3^n}$ сходится в $\mathbb{Q}_3$, и найдите ее предел.

54 («гармоническая» последовательность).

1) Покажите, что последовательность $1, 1/2, 1/3, \ldots$ не имеет предела в $\mathbb{Q}_p$, но содержит сходящуюся подпоследовательность.

2*) Докажите, что множество $\{1, 1/2, 1/3, \ldots\}$ плотно в $\{x \in \mathbb{Q}_p : |x|_p \geqslant 1\}$.

55. Докажите, что $\sum_{n=1}^{\infty} n! \cdot n = -1$ в $\mathbb{Q}_p$ для любого p.

56. Используя идеи предыдущего упражнения, докажите, что в $\mathbb{Q}_p$ для любого простого числа p имеют место равенства

$$\sum_{n=1}^{\infty} n^2 \cdot (n+1)! = 2; \quad \sum_{n=1}^{\infty} n^5 \cdot (n+1)! = 26.$$

§ 14. p-адические степенные ряды

Формальным степенным рядом называется выражение вида

$$f(X) = \sum_{n=0}^{\infty} a_n X^n,$$

где $a_n \in \mathbb{Q}_p$, а X — переменная. Множество всех степенных рядов от X с коэффициентами в кольце R обозначается $R[[X]]$, а множество многочленов через $R[X]$.

Для данных $x \in \mathbb{Q}_p$ и $f \in \mathbb{Q}_p[[X]]$ можно рассмотреть соответствующий числовой ряд $f(x)$, равный $\sum\limits_{n=0}^{\infty} a_n x^n$. Как мы уже знаем, он сходится тогда и только тогда, когда $|a_n x^n|_p \to 0$.

Как и в архимедовом случае (степенные ряды с коэффициентами в $\mathbb{R}$ или $\mathbb{C}$), определим «радиус сходимости»

$$r = \frac{1}{\limsup |a_n|_p^{1/n}}. \tag{14.1}$$

Напомним, что верхним пределом $\limsup$ последовательности называется точная верхняя грань (sup) множества ее предельных точек. Таким образом, в случае $0 < r < \infty$ для любого $C > 1/r$ существует только конечное количество чисел $|a_n|_p^{1/n}$, больших C. Следующее утверждение оправдывает термин «радиус сходимости».

Предложение 14.1. *Предположим, что* $0 < r < \infty$. *Тогда ряд*

$$\sum_{n=0}^{\infty} a_n x^n$$

сходится, если $|x|_p < r$, *и расходится, если* $|x|_p > r$.

Доказательство. Пусть сначала $|x|_p < r$. Положим $|x|_p = (1-\varepsilon)r$. Тогда

$$|a_n x^n|_p = (r|a_n|_p^{1/n})^n (1-\varepsilon)^n.$$

Так как существует только конечное количество таких n, что $|a_n|_p^{1/n} > \dfrac{1}{r - (1/2)\varepsilon r}$, имеем

$$\lim_{n\to\infty} |a_n x^n|_p \leqslant \lim\left(\frac{(1-\varepsilon)r}{(1-\varepsilon/2)r}\right)^n = \lim_{n\to\infty}\left(\frac{1-\varepsilon}{1-\varepsilon/2}\right)^n = 0.$$

Аналогично, если $|x|_p > r$, то запишем $|x|_p = (1+\varepsilon)r$. Тогда

$$|a_n x^n|_p = (r|a_n|_p^{1/n})^n (1+\varepsilon)^n.$$

Так как существует только конечное количество таких n, что $|a_n|_p^{1/n} > \frac{1}{r + (1/2)\varepsilon r}$, имеем

$$\limsup_{n\to\infty} |a_n x^n|_p \geqslant \lim\left(\frac{(1+\varepsilon)r}{(1+\varepsilon/2)r}\right)^n = \lim_{n\to\infty}\left(\frac{1+\varepsilon}{1+\varepsilon/2}\right)^n \neq 0. \qquad \square$$

Что происходит на «границе» $|x|_p = r$? В архимедовом случае ($\mathbb{R}$ или $\mathbb{C}$) поведение степенного ряда на границе интервала или круга сходимости может быть довольно сложным. Например, радиус сходимости обычного логарифмического степенного ряда $\ln(1+x) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$ равен 1. Если $|x| = 1$, то при $x = -1$ ряд расходится, а при $x = 1$ — сходится (не абсолютно).

В неархимедовом случае поведение степенного ряда во всех точках $|x|_p = r$ одинаково, потому что ряд сходится тогда и только тогда, когда $|a_n x^n|_p \to 0$, а это условие зависит только от нормы $|x|_p$, но не от конкретного значения x.

Рассмотрим тот же самый пример $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$. Мы имеем

$$|a_n|_p = p^{\operatorname{ord}_p n} \quad \text{и} \quad \lim_{n\to\infty} |a_n|_p^{1/n} = 1$$

(упражнение 57). Этот ряд сходится при $|x|_p < 1$ и расходится при $|x|_p > 1$. Если же $|x|_p = 1$, то $|a_n x^n|_p = p^{\operatorname{ord}_p n} \geqslant 1$, и поэтому для всех таких x ряд расходится.

Лемма 14.2. *Любой ряд $f(X) \in \mathbb{Z}_p[[X]]$ сходится в $\{x \in \mathbb{Q}_p : |x|_p < 1\}$.*

Доказательство. Пусть $|x|_p < 1$ и $f(x) = \sum_{n=0}^{\infty} a_n x^n$. Так как для любого $n \geqslant 0$ выполняется неравенство $|a_n|_p \leqslant 1$, имеем $|a_n x^n|_p \leqslant |x|_p^n \to 0$ при $n \to \infty$, откуда и следует сходимость ряда. $\square$

Пример 14.3. Зафиксируем некоторое $a \in \mathbb{Z}_p$. Положим

$$f_a(X) = \sum_{n=0}^{\infty}\binom{a}{n}X^n \in \mathbb{Z}_p[[X]].$$

Здесь

$$\binom{a}{n} = \frac{a(a-1)\dots(a-n+1)}{n!} \quad \text{и} \quad f_a(X) := (1+X)^a.$$

Лемма 14.4. *Если $a \in \mathbb{Z}_p$ и $n \geqslant 0$, то $\binom{a}{n} \in \mathbb{Z}_p$.*

Доказательство. Для каждого $n \geqslant 0$ рассмотрим

$$P_n(X) = \frac{X(X-1)\dots(X-n+1)}{n!} \in \mathbb{Q}[X].$$

Как и любой многочлен, P_n определяет непрерывное отображение $\mathbb{Q}_p \to \to \mathbb{Q}_p$. Если m, n — натуральные числа, $\binom{m}{n} \in \mathbb{N}$, то для $a \in \mathbb{N}$ имеем

$$P_n(a) = \binom{a}{n} \in \mathbb{N}.$$

Таким образом, непрерывная функция P_n отображает $\mathbb{N}$ в $\mathbb{N}$. Тогда по непрерывности она переводит замыкание множества $\mathbb{N}$ в замыкание множества $\mathbb{N}$. Но по теореме 11.11 множество $\mathbb{N}$ плотно в $\mathbb{Z}_p$; это означает, что P_n отображает $\mathbb{Z}_p$ в $\mathbb{Z}_p$. □

Замечание 14.5. Несложно показать непосредственно, что если $m \in \mathbb{Z}$, то $\binom{m}{n} \in \mathbb{Z}$. Как это сделать?

Следующий результат очень похож на соответствующее утверждение из вещественного анализа.

Лемма 14.6. *Пусть $f(x) = \sum a_n x^n$, $a_n \in \mathbb{Q}_p$, — p-адический степенной ряд, областью сходимости которого является открытый и замкнутый шар $D \subset \mathbb{Q}_p$. Тогда $f\colon D \to \mathbb{Q}_p$ является непрерывной функцией на D.*

Доказательство. Мы покажем, что функция f непрерывна в каждой точке $x \in D$, $x \neq 0$, а случай $x = 0$ оставим читателю (упражнение 59). Пусть $|x - x'|_p < \delta$, где $\delta < |x|_p$ будет выбрано позже. Тогда $|x|_p = |x'|_p$ по свойству равнобедренного треугольника. Мы имеем

$$|f(x) - f(x')|_p = \left|\sum_{n=0}^{\infty}(a_n x^n - a_n x'^n)\right|_p \leqslant \max_n |a_n x^n - a_n x'^n|_p =$$
$$= \max_n(|a_n|_p(x - x')(x^{n-1} + x^{n-2}x' + \ldots + x'^{n-1}))|_p.$$

Но

$$|x^{n-1} + x^{n-2}x' + \ldots + x'^{n-1}|_p \leqslant \max_{1 \leqslant i \leqslant n} |x^{n-i}x'^{i-1}|_p = |x|_p^{n-1}.$$

Таким образом,

$$|f(x) - f(x')|_p \leqslant \max_n(|x - x'|_p |a_n|_p |x|_p^{n-1}) < \frac{\delta}{|x|_p} \max_n(|a_n|_p |x|_p^n).$$

Так как числа $|a_n x^n|_p$ ограничены при $n \to \infty$, получаем $|f(x) - f(x')|_p < \varepsilon$ для подходящего δ. □

Предложение 14.7. *Радиус сходимости степенного ряда*

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$$

совпадает с радиусом сходимости его производной

$$Df(X) = \sum_{n=1}^{\infty} na_n X^{n-1},$$

т.е. $r_f = r_{Df}$.

Доказательство. Для любого $n \in \mathbb{N}$ имеем $|n|_p \leqslant 1$. Тогда

$$r_{Df} = \limsup_{n\to\infty} |na_n|_p^{1/n-1} = \limsup_{n\to\infty} |na_n|_p^{1/n} = \limsup_{n\to\infty} |a_n|_p^{1/n} = r_f,$$

что и требовалось доказать. □

Следующий пример показывает, что поведение степенного ряда на границе может отличаться от поведения его производной. Степенной ряд $f(X) = \sum\limits_{n=0}^{\infty} X^{p^n}$ имеет радиус сходимости, равный 1, и расходится при $|x|_p = 1$, в то время как его производная $Df(X) = \sum\limits_{n=1}^{\infty} p^n X^{p^n-1}$ сходится для $|x|_p = 1$ (так как ряд $\sum\limits_{n=1}^{\infty} p^n$ сходится).

Упражнения

57. Докажите, что $\lim\limits_{n\to\infty} p^{\mathrm{ord}_p n/n} = 1$.

58. Пусть

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$$

— степенной ряд и $r = 1/\limsup |a_n|_p^{1/n}$. Докажите, что если $r = 0$, то $f(x)$ сходится тогда и только тогда, когда $x = 0$, а если $r = \infty$, то $f(x)$ сходится для всех $x \in \mathbb{Q}_p$.

59. Докажите непрерывность степенного ряда $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$, имеющего положительный радиус сходимости, в точке $x = 0$.

60. Докажите, что

$$\mathrm{ord}_p(n!) = \frac{n - S_n}{p - 1},$$

где S_n — сумма цифр числа n, записанного по основанию p.

§ 15. Некоторые элементарные функции

§ 15.1. p-адический логарифм. Рассмотрим следующий степенной ряд:

$$\log(1 + X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}. \tag{15.1}$$

Так как все коэффициенты этого ряда являются рациональными числами, сам ряд принадлежит кольцу $\mathbb{Q}[[X]]$. Как мы уже видели, соответствующий степенной ряд в $\mathbb{Q}_p$, который мы будем обозначать $\ln_p(1+x)$, чтобы не путать с логарифмом по основанию p, и называть *p-адическим логарифмом*, сходится при $|x|_p < 1$. (Мы сохраним обозначение $\log(1+x)$ для соответствующего числового степенного ряда в $\mathbb{R}$.)

Аналогично, определим ряд

$$\ln_p(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n},$$

который сходится при $x \in B = \{x \in \mathbb{Z}_p : |x-1|_p < 1\} = 1 + p\mathbb{Z}_p$.

Теорема 15.1. *p-адический логарифм удовлетворяет основному свойству*

$$\ln_p(xy) = \ln_p(x) + \ln_p(y).$$

Доказательство. Следующее тождество:

$$\mathbf{log}(1+X) + \mathbf{log}(1+Y) - \mathbf{log}(1+X+Y+XY) = 0 \qquad (15.2)$$

выполнено для формальных степенных рядов. Можно проверить непосредственно (разложив в ряды и перегруппировав члены), что все коэффициенты получающегося в результате ряда равны 0. Однако можно это проверить и по-другому. Заметим, что ряд (15.1) определяет вещественный логарифм, который удовлетворяет соотношению (15.2). Это означает, что ряд, стоящий в левой части равенства (15.2), обращается в 0 для всех действительных чисел X и Y из интервала $(-1, 1)$. Поэтому после приведения подобных членов (которое не влияет на сходимость и сумму соответствующего вещественного ряда, так как он сходится абсолютно) левая часть записывается в виде $\sum c_{n,m} X^n Y^m$ и все $c_{n,m}$ равны 0. Возьмем любые $\alpha, \beta \in p\mathbb{Z}_p$, тогда $\alpha + \beta + \alpha\beta \in p\mathbb{Z}_p$ и то же самое можно сказать про

$$\ln_p(1+\alpha) + \ln_p(1+\beta) - \ln_p(1+\alpha)(1+\beta).$$

Так как все рассматриваемые ряды сходятся, можно, применяя теорему 13.7, перегруппировать члены и переписать левую часть в виде $\sum c_{n,m} \alpha^n \beta^m$, причем все $c_{n,m}$ равны 0, откуда и вытекает требуемое утверждение. □

§ 15.2. *p*-адическая экспонента. Теперь рассмотрим степенной ряд

$$\mathbf{exp}(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

Соответствующий вещественный степенной ряд сходится всюду. Рассмотрим этот степенной ряд в $\mathbb{Q}_p$; он называется *p-адической экспонентой* и обозначается $\exp_p(x)$. Следующая теорема может сначала показаться странной.

Теорема 15.2. *p-адическая экспонента* $\exp_p(x)$ *сходится в круге* $D_p = \{x \in \mathbb{Q}_p : |x|_p < r_p\}$, *где* $r_p = p^{-1/(p-1)}$, *и расходится во всех остальных точках* $\mathbb{Q}_p$.

Доказательство. Сначала найдем радиус сходимости r_p этого степенного ряда по формуле (14.1). В данном случае $a_n = 1/n!$. Используя упражнение 60, получаем

$$\left|\frac{1}{n!}\right|_p = p^{\frac{n-S_n}{p-1}}.$$

Из формулы

$$r_p = \frac{1}{\limsup |a_n|_p^{1/n}}$$

(используя то, что r_p является степенью числа p) получаем соотношение

$$\operatorname{ord}_p r_p = \liminf \frac{1}{n} \operatorname{ord}_p a_n = \liminf\left(-\frac{n-S_n}{n(p-1)}\right) = -\frac{1}{p-1}$$

(последнее равенство выполнено, так как

$$\lim_{n\to\infty}\left(-\frac{n-S_n}{n}\right) = -1 + \lim_{n\to\infty}\frac{S_n}{n} = -1),$$

и тогда $r_p = p^{-1/(p-1)}$. Теперь посмотрим, что будет при $|x|_p = p^{-1/(p-1)}$, т.е. $\operatorname{ord}_p(x) = 1/(p-1)$. Можно написать

$$\operatorname{ord}_p(a_n x^n) = -\frac{n-S_n}{p-1} + \frac{n}{p-1} = \frac{S_n}{p-1}.$$

Если $n = p^m$, то $S_n = 1$ и $\operatorname{ord}_p(a_{p^m} x^{p^m}) = 1/(p-1)$, поэтому

$$\lim_{n\to\infty} |a_n x^n|_p \neq 0 \quad \text{для} \quad |x|_p = p^{-1/(p-1)},$$

и ряд расходится при $|x|_p = p^{-1/(p-1)}$. □

Замечание 15.3. Если $p = 2$, то радиус сходимости равен $1/2$, поэтому $\exp_2(x)$ сходится в $4\mathbb{Z}_2$.

Если $p > 2$, то радиус сходимости равен $p^{-1/(p-1)}$. Однако p-адическая норма не может принимать такое значение, и так как $1/p < p^{-1/(p-1)} < 1$, ряд $\exp_p(x)$ сходится в $p\mathbb{Z}_p$.

Предложение 15.4. *Если точки x и y принадлежат области сходимости* D_p *p-адической экспоненты, то* $\exp_p(x+y) = \exp_p(x)\exp_p(y)$.

Доказательство. Так как это верно для формальных степенных рядов, то доказательство аналогично доказательству предложения 15.1. □

Предложение 15.5. *Если* $x \in D_p = \{|x|_p < p^{-1/(p-1)}\}$, *то*

$$|\exp_p(x) - 1|_p < 1,$$

т.е. $\exp_p(x)$ *принадлежит области определения функции* $\ln_p(x)$ *и*

$$\ln_p(\exp_p(x)) = x. \tag{15.3}$$

Наоборот, если $x \in D_p$, *то*

$$|\ln_p(1+x)|_p < p^{-\frac{1}{p-1}}$$

и

$$\exp_p(\ln_p(1+x)) = 1 + x. \tag{15.4}$$

Доказательство. Соотношения (15.3) и (15.4) следуют из соответствующих соотношений для формальных степенных рядов, поэтому достаточно проверить, что все рассматриваемые ряды сходятся.

Если $x \in D_p$, то ряд $\exp_p(x)$ сходится и по предложению 13.3

$$|\exp_p(x) - 1|_p \leqslant \max_n \left|\frac{x^n}{n!}\right|_p.$$

Используя результат упражнения 60, получаем

$$\left|\frac{x^n}{n!}\right|_p < p^{-\frac{n}{p-1}} p^{\operatorname{ord}_p(n!)} < p^{-\frac{n}{p-1}} p^{\frac{n}{p-1}} = 1.$$

Поэтому $|\exp_p(x) - 1|_p < 1$, как и утверждалось.

Чтобы доказать вторую часть, надо оценить $\operatorname{ord}_p(n)$.

Лемма 15.6. *Справедливо равенство* $\operatorname{ord}_p(n) - \dfrac{n}{p-1} \leqslant \dfrac{-1}{p-1}$.

Доказательство леммы. Для $n = 1$ и $n = p$ имеем равенство. Если $1 < n < p$, то $\operatorname{ord}_p(n) = 0$ и имеет место строгое неравенство. Для $p > n$ имеет место следующая оценка сверху для $\operatorname{ord}_p(n)$ (ср. упражнение 57 выше):

$$\operatorname{ord}_p(n) \leqslant \frac{\log n}{\log p}.$$

Тогда

$$\frac{n-1}{p-1} - \operatorname{ord}_p(n) \geqslant \frac{n-1}{p-1} - \frac{\log n}{\log p}. \tag{15.5}$$

Положим

$$f(x) = \frac{x-1}{p-1} - \frac{\log x}{\log p}.$$

Мы имеем $f(p) = 0$ и $f'(x) > 0$ для $x > p$. Это означает, что функция f возрастает, в частности, при $n > p$ имеет место неравенство

$$\frac{n-1}{p-1} - \frac{\log n}{\log p} > 0;$$

сопоставляя это неравенство с (15.5), получаем требуемое утверждение. □

Пусть снова $x \in D_p$. Тогда

$$|\ln_p(1+x)|_p \leqslant \max_n \left|\frac{x^n}{n}\right|_p.$$

Применяя лемму, получаем

$$\left|\frac{x^n}{n}\right|_p < p^{-\frac{n}{p-1}} p^{\operatorname{ord}_p(n)} \leqslant p^{-\frac{1}{p-1}},$$

откуда $|\ln_p(1+x)|_p < p^{-\frac{1}{p-1}}$. □

Пример 15.7. Пусть $p = 2$. Тогда $-1 \in \{x \in \mathbb{Z}_2 \colon |x-1|_2 < 1\}$, так как $|-1-1|_2 = 1/2 < 1$. Таким образом, 2-адический логарифм $\ln_2(-1)$ можно вычислить с помощью степенного ряда

$$\ln_2(-1) = \ln_2(1-2) = -\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots\right).$$

С другой стороны, имеем

$$0 = \ln_2(1) = \ln_2(-1) + \ln_2(-1) = 2\ln_2(-1),$$

откуда $\ln_2(-1) = 0$. Это означает, что при $n \to \infty$ сумма

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots + \frac{2^n}{n}$$

становится все ближе и ближе (по 2-адической норме) к 0, т. е. делится на сколь угодно большие степени двойки, если n достаточно велико. Более точно, для каждого M существует такое n, что

$$2^M \mid \left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots + \frac{2^n}{n}\right).$$

Можете ли вы оценить максимальную степень двойки, которая делит

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots + \frac{2^n}{n}?$$

§ 16. Можно ли p-адический степенной ряд продолжить аналитически?

Предположим, что нам дана функция, заданная степенным рядом в некотором круге. Можно ли эту функцию «естественным» образом продолжить на бо́льшую область? В вещественном случае ответ утвердительный: даже несмотря на то, что степенной ряд $\log(x+1)$ расходится при $x > 1$, существует бесконечно гладкая функция $\log$, определенная для всех положительных чисел. Способ продолжения в состоит в следующем: мы выбираем внутри круга сходимости некоторую точку α, находим степенное разложение нашей функции в этой точке и таким образом продолжаем нашу функцию в круг сходимости нового ряда. К сожалению, этот метод в случае $\mathbb{Q}_p$ не работает.

Предложение 16.1. *Пусть*

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]],$$

и пусть $\alpha \in D$, где D — круг сходимости ряда f. Для $m \geqslant 0$ положим

$$b_m = \sum_{n=m}^{\infty} \binom{n}{m} a_n \alpha^{n-m}, \tag{16.1}$$

$$g(X) = \sum_{m=0}^{\infty} b_m (X-\alpha)^m. \tag{16.2}$$

Тогда

1) *ряд* (16.1) *сходится для всех m, поэтому b_m корректно определено для каждого m;*

2) *круг сходимости ряда $g(X)$ совпадает с D;*

3) *$g(\lambda) = f(\lambda)$ для всех $\lambda \in D$.*

Доказательство.

Так как $\alpha \in D$, для каждого m имеем

$$\left|\binom{n}{m} a_n \alpha^{n-m}\right|_p \leqslant |a_n \alpha^{n-m}|_p = |\alpha|_p^{-m} |a_n \alpha^n|_p \to 0,$$

потому что $\binom{n}{m} \in \mathbb{Z}$. Значит ряд $f(x)$ сходится в точке α. Тем самым утверждение 1) доказано.

Теперь, если $\lambda \in D$, то

$$f(\lambda) = \sum_{n=0}^{\infty} a_n (\lambda - \alpha + \alpha)^n = \sum_{n=0}^{\infty} \sum_{m \leqslant n} \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m. \tag{16.3}$$

Последнее разложение очень похоже на частичную сумму ряда $g(x)$, надо только поменять порядок суммирования. Чтобы обосновать законность смены порядка суммирования, покажем, что этот двойной ряд сходится «равномерно». Сначала сделаем так, чтобы оба индекса принимали бесконечное количество значений.

Положим

$$\beta_{n,m} = \begin{cases} \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m, & \text{если } m \leqslant n, \\ 0, & \text{если } m > n. \end{cases}$$

Мы хотим показать, что $\beta_{m,n} \to 0$ равномерно относительно обоих индексов, т. е. мы хотим найти такое число N, что если $m > N$ или $n > N$, то $|\beta_{m,n}|_p < \varepsilon$. Имеет место следующая оценка:

$$|\beta_{m,n}|_p = \left| \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m \right|_p \leqslant |a_n \alpha^{n-m} (\alpha - \lambda)^m|_p.$$

Можно найти такую точку $r_1 \in D$, что $r = |r_1|_p \geqslant \max(|\alpha|_p, |\lambda|_p)$. (Возьмем, например, $r_1 = \alpha$ или $r_1 = \lambda$ в зависимости от того, какое из чисел α и λ имеет бóльшую норму.) Тогда по построению $|\alpha|_p^m \leqslant r^m$, и

$$|\lambda - \alpha|_p^{n-m} \leqslant \max(|\alpha|_p, |\lambda|_p)^{n-m} \leqslant r^{n-m}$$

по построению и неархимедову свойству нормы; поэтому

$$|\beta_{n,m}|_p \leqslant |a_n \alpha^{n-m} (\lambda - \alpha)^m|_p \leqslant |a_n|_p r^n,$$

причем последнее выражение стремится к 0, когда $n \to \infty$ независимо от m, т. е.

$$\forall \varepsilon > 0 \ \exists N \colon \forall n > N \ |\beta_{m,n}|_p < \varepsilon,$$

а это половина нужного нам утверждения. Далее, если $m > N$, то

$$\text{либо } n \geqslant m \Rightarrow n > N \Rightarrow |\beta_{m,n}|_p < \varepsilon,$$

$$\text{либо } n < m \Rightarrow \beta_{m,n} = 0, \ \text{ поэтому } |\beta_{m,n}|_p = 0 < \varepsilon.$$

Теперь мы можем применить теорему 13.7 и поменять порядок суммирования в соотношении (16.3):

$$f(\lambda) = \sum_{n=0}^{\infty} \sum_{m \leqslant n} \binom{n}{m} a_n a^{n-m} (\lambda - a)^m = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \beta_{n,m} =$$

$$= \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \beta_{n,m} = \sum_{m=0}^{\infty} \sum_{n=m}^{\infty} \binom{n}{m} a_n a^{n-m} (\lambda - a)^m = g(\lambda).$$

Мы взяли произвольное $\lambda \in D$ и получили, что ряд g сходится в точке λ; поэтому g сходится во всем круге D. Заметим, что f и g участвуют в этих рассуждениях симметрично, поэтому можно, начав с g, построить f. Отсюда следует, что ряд f сходится тогда же, когда сходится g, что и требовалось доказать. □

Итак, нам не удается продолжить функцию, заданную p-адическим степенным рядом, так, как это делают в вещественном случае. Возникает вопрос: продолжение какого рода мы хотим получить? В вещественном случае функция называется аналитической, если она определяется степенным рядом в некоторой окрестности каждой точки своей области определения. Рассмотрим функцию, определенную в $\mathbb{Z}_p$ и равную 1 на $p\mathbb{Z}_p$ и 0 на $\mathbb{Z}_p \setminus p\mathbb{Z}_p = \mathbb{Z}_p^\times$. Так как оба эти множества открыты, наша функция f может быть записана в виде степенного ряда (константы) в некоторой окрестности каждой точки из $\mathbb{Z}_p$, но эта функция совсем не похожа на «аналитическую»! Поэтому перед тем как ставить вопрос об аналитическом продолжении, нужно правильно определить аналитическую функцию.

§ 17. Нули p-адических степенных рядов

В следующей теореме речь идет о функциях $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$, заданных степенными рядами $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$, которые сходятся для всех $x \in \mathbb{Z}_p$. Такие функции характеризуются тем, что соответствующий ряд сходится для $|x|_p = 1$, т.е.

$$\lim_{n\to\infty} a_n = 0.$$

Теорема 17.1 (теорема Штрассмана). *Пусть*

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$$

— ненулевой степенной ряд (т.е. не все его коэффициенты равны нулю). Предположим, что $\lim\limits_{n\to\infty} a_n = 0$ *и тогда ряд* $f(x)$ *сходится при всех* $x \in \mathbb{Z}_p$. *Пусть* N *— натуральное число, которое определяется следующим образом*:

1) $|a_N|_p = \max |a_n|_p$,

2) $|a_n|_p < |a_N|_p$ *при* $n > N$. *Тогда функция* $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ *имеет не более* N *нулей.*

Замечание 17.2. Так как $a_n \to 0$, норма $|a_n|_p$ принимает максимальное значение на конечном множестве индексов $n_1, n_2, \ldots, n_k$; тогда $N = n_k$, где n_k — максимальный из индексов чисел a_n, имеющих максимальную норму.

Доказательство теоремы 17.1. Доказательство проводится индукцией по N.

База индукции. При $N = 0$ наше предположение означает, что $|a_0|_p > |a_n|_p$ для всех $n > 0$. Мы хотим доказать, что $f(x)$ не имеет нулей в $\mathbb{Z}_p$. Если

$$0 = f(x) = a_0 + a_1 x + a_2 x^2 + \ldots,$$

то

$$|a_0|_p = |a_1 x + a_2 x^2 + \ldots| \leqslant \max_{n \geqslant 1} |a_n x^n|_p \leqslant \max_{n \geqslant 1} |a_n|_p < |a_0|_p,$$

и тем самым мы получили противоречие.

Шаг индукции. В явном виде выделим множитель, соответствующий одному из нулей, и покажем, что частное также является степенным рядом, для которого число N строго меньше. Предположим, что

$$|a_N|_p = \max_n |a_n|_p \quad \text{и} \quad |a_n| < |a_N|_p \quad \text{для } n > N,$$

и пусть $f(\alpha) = 0$ для некоторого $\alpha \in \mathbb{Z}_p$. Возьмем произвольное число $x \in \mathbb{Z}_p$. Тогда

$$f(x) = f(x) - f(\alpha) = \sum_{n=1}^{\infty} a_n (x^n - \alpha^n) = (x - \alpha) \sum_{n=1}^{\infty} \sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}.$$

По теореме 13.7 можно поменять порядок суммирования: полагая $k = n - j - 1$, получаем

$$f(x) = (x - \alpha) \sum_{j=0}^{\infty} b_j x^j = (x - \alpha) g_1(x), \qquad \text{где } b_j = \sum_{k=0}^{\infty} a_{j+1+k} \alpha^k.$$

Мы имеем

$$|b_j|_p \leqslant \max |a_{j+1+k}|_p \leqslant |a_N|_p \quad \text{для всех } j \text{ от } 0 \text{ до } \infty,$$

так как элемент a_N имеет максимальную норму. Далее,

$$|b_{N-1}|_p = |a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \ldots|_p = |a_N|_p,$$

и если $j > N$, то

$$|b_j|_p \leqslant \max_{k \geqslant 0} |a_{j+k+1}|_p \leqslant \max_{j \geqslant N+1} |a_j|_p < |a_N|.$$

Итак, элемент b_{N-1} имеет максимальную норму, а нормы всех последующих элементов строго меньше. Применяя к функции g_1 предположение индукции, получаем, что количество нулей этой функции не превосходит $N - 1$, поэтому максимально возможное количество нулей функции f равно N, а именно, $N - 1$ нулей функции g_1 и α. □

Теорема Штрассмана имеет несколько следствий.

Следствие 17.3. *Пусть $f(X) = \sum a_n X^n$ — степенной ряд, сходящийся в $\mathbb{Z}_p$. Пусть также $\alpha_1, \alpha_2, \ldots, \alpha_m$ — все нули функции $f(X)$ в $\mathbb{Z}_p$. Тогда существует степенной ряд $g(x)$, сходящийся в $\mathbb{Z}_p$, но не имеющий там нулей и такой, что*

$$f(X) = (X - \alpha_1)\ldots(X - \alpha_m)g(X).$$

Доказательство. Как и при доказательстве теоремы 17.1, можно написать

$$f(X) = (X - \alpha_1)g_1(X),$$

причем ряд $g_1(X)$ сходится в $\mathbb{Z}_p$ и имеет там не более $m - 1$ нулей. Продолжая этот процесс, мы выделим все m нулей и получим $g_m(X) = g(X)$. □

Следствие 17.4. *Пусть $f(X) = \sum a_n X^n$ — степенной ряд, сходящийся в $p^m\mathbb{Z}_p$ для некоторого $m \in \mathbb{Z}$. Тогда $f(X)$ имеет в $p^m\mathbb{Z}_p$ конечное число нулей. Это число не превосходит числа N, которое определяется из соотношений*

$$|p^{mN}a_N|_p = \max_n |p^{mn}a_n|_p \quad \text{и} \quad |p^{mn}a_n|_p < |p^{mN}a_N|_p \quad \text{для } n > N.$$

Доказательство. Положим $g(X) = f(p^m X) = \sum a_n p^{mn} X^n$. Так как ряд f сходится в $p^m\mathbb{Z}_p$, ряд g сходится в $\mathbb{Z}_p$. Теперь утверждение вытекает из теоремы 17.1. □

Пример 17.5. Пусть $f(X) = \sum\limits_{n=0}^{\infty} p^n X^n$. Найдем область сходимости $f(X)$ и количество нулей. Радиус сходимости вычисляется по формуле (14.1), где $|a_n|_p = |p^n|_p = p^{-n}$: $r = p$. При $|x|_p = p$ имеем

$$|p^n x^n|_p = |p^n|_p |x|_p^n = p^{-n+n} = 1,$$

а это выражение не стремится к 0. Таким образом, ряд сходится при

$$\{|x|_p < p\} = \{|x|_p \leqslant 1\} = \mathbb{Z}_p.$$

Последовательность $|p^n|_p = p^{-n}$ убывает, поэтому элемент $p^0 = 1$ имеет максимальную норму. Непосредственное примененяя теорему Штрассмана, мы получаем, что $N = 0$, т.е. степенной ряд $f(X)$ не имеет нулей в своей области сходимости. Конечно, это можно было увидеть и напрямую, так как в области сходимости имеет место обычная формула суммы бесконечной геометрической прогрессии и $f(X) = (1 - pX)^{-1}$.

Следствие 17.6. *Рассмотрим два p-адических степенных ряда*

$$f(X) = \sum_{n \geqslant 0} a_n X^n, \quad g(X) = \sum_{n \geqslant 0} b_n X^n,$$

сходящихся в $p^m\mathbb{Z}_p$. Если существует бесконечно много таких чисел $\alpha \in p^m\mathbb{Z}_p$, что $f(\alpha) = g(\alpha)$, то $a_n = b_n$ для всех $n \geqslant 0$.

Доказательство. Применим следствие 17.4 к разности $f(X) - g(X)$. Она имеет бесконечно много нулей в $p^m\mathbb{Z}_p$ и поэтому представляется нулевым рядом. Таким образом, все коэффициенты рядов $f(X)$ и $g(X)$ равны, т. е. $a_n = b_n$ для всех $n \geqslant 0$. □

Это свойство аналогично соответствующим свойствам степенных рядов с вещественными или комплексными коэффициентами.

Следствие 17.7. *Пусть степенной ряд $f(X) = \sum\limits_{n\geqslant 0} a_n X^n$ сходится в $p^m\mathbb{Z}_p$. Если функция $f(x)$ периодическая, т. е. существует такая константа $\tau \in p^m\mathbb{Z}_p$, что $f(x+\tau) = f(x)$ для всех $x \in p^m\mathbb{Z}_p$, то $f(X) = \mathrm{const}$.*

Доказательство. Легко видеть, что функция $f(x) - f(0)$ равна нулю в точках вида τn для всех $n \in \mathbb{Z}$. Так как $\tau \in p^m\mathbb{Z}_p$, а $p^m\mathbb{Z}_p$ является идеалом, то $n\tau \in p^m\mathbb{Z}_p$. Таким образом, функция $f(x) - f(0)$ имеет бесконечно много нулей в $p^m\mathbb{Z}_p$, откуда следует, что $f(X) - f(0) = 0$, т. е. $f(X) = \mathrm{const}$. □

Этот результат неверен в классическом случае, когда функции синус и косинус являются периодическими и «целыми», т. е. задаются степенными рядами, сходящимися во всех точках. Причиной различия является, конечно, то обстоятельство, что в случае $\mathbb{R}$ или $\mathbb{C}$, если τ — период, то все точки вида $n\tau$ не могут принадлежать ограниченному интервалу или кругу.

Следствие 17.8. *Пусть $f(X) = \sum\limits_{n\geqslant 0} a_n X^n$ — p-адический степенной ряд, который является целым, т. е. сходится при всех $x \in \mathbb{Q}_p$. Тогда функция $f(x)$ имеет не более чем счетное множество нулей. Более того, если множество нулей бесконечно, то оно образует такую последовательность $\{z_n\}$, что $|z_n|_p \to \infty$ при $n \to \infty$.*

Доказательство. Множество нулей в каждом ограниченном круге $p^m\mathbb{Z}_p$, $m \in \mathbb{Z}$, конечно. □

Упражнения

61. Используя теорему Штрассмана, покажите, что при $p \neq 2$ равенство $\ln_p(x) = 0$ выполняется тогда и только тогда, когда $x = 1$. Покажите, что при $p = 2$ равенство $\ln_p(x) = 0$ выполняется тогда и только тогда, когда $x = \pm 1$.

62. Найдите область сходимости и скажите все, что можете, о нулях следующих p-адических степенных рядов:

1) $\sum p^{-n} X^n$,

2) $\sum n! X^n$.

63. С помощью степенных рядов определите p-адические аналоги синуса и косинуса и найдите их области сходимости. Покажите, что если $p \equiv 1 \pmod 4$, то существует такое $i \in \mathbb{Q}_p$, что $i^2 = -1$ и для всех x из общей области сходимости выполняется следующее классическое соотношение:

$$\exp_p(ix) = \cos_p(x) + i \sin_p(x).$$

§ 18. Дальнейшие свойства p-адических экспонент и логарифмов

Рассмотрим область сходимости ряда $\exp_p$, которая имеет вид

$$D_p = \{x \in \mathbb{Z}_p : |x|_p < p^{-\frac{1}{p-1}}\}.$$

Как мы уже видели в § 15, если $p \neq 2$, то $D_p = p\mathbb{Z}_p$ и $D_2 = 4\mathbb{Z}_2$. Отображения

$$\exp_p : D_p \to 1 + D_p \quad \text{и} \quad \ln_p : 1 + D_p \to D_p$$

взаимно обратны (предложение 15.5). Основные свойства экспоненциальной и логарифмической функций можно сформулировать на языке теории групп следующим образом.

Предложение 18.1. *Функция p-адический логарифм определяет изоморфизм групп*

$$\ln_p : 1 + D_p \to D_p,$$

где $1 + D_p$ рассматривается как группа по умножению, а D_p — как группа по сложению; обратным изоморфизмом является отображение $\exp_p$.

Доказательство. Сначала проверим, что $1 + D_p$ является мультипликативной подгруппой группы $\mathbb{Z}_p$. Это вытекает из того, что D_p является идеалом в $\mathbb{Z}_p$: если $x, y \in D_p$, то $x + y + xy \in \mathbb{Z}_p$ и, следовательно, $(1 + x)(1 + y) \in 1 + D_p$. Оставшаяся часть является прямым следствием предложения 15.5. □

Следствие 18.2. *Мультипликативная группа $1 + D_p$ не имеет кручения, т.е. не существует такого числа $x \in 1 + D_p$, $x \neq 1$, что $x^m = 1$ для некоторого натурального числа m.*

Доказательство. Аддитивная группа D_p не имеет кручения, так как в поле $\mathbb{Q}_p$ из соотношения $my = 0$ следует, что $y = 0$, откуда и вытекает требуемое утверждение. □

Замечания. 1. Первое утверждение означает, что функция $\ln_p$ определяет взаимно однозначное соответствие между группами $1 + D_p$ и D_p, причем образ произведения равен сумме образов. В частности, отображение $\ln_p$ инъективно, т. е. не существует двух чисел в $1 + D_p$, у которых

значения $\ln_p$ были бы равны. Заметим, что $1 + D_p$ является максимальным кругом, в котором отображение $\ln_p$ инъективно. Действительно, для $p \neq 2$ множество $1 + D_p$ является областью сходимости функции $\ln_p$, поэтому достаточно рассмотреть случай $p = 2$. Как мы уже видели (пример 15.7), $|-1 - 1|_2 = 1/2$, поэтому число -1 лежит в множестве $1 + 2\mathbb{Z}_2$, являющемся областью определения функции $\ln_2$, но не лежит в множестве $1 + D_2 = 1 + 4\mathbb{Z}_2$, являющемся областью определения функции $\exp_2$. С другой стороны, $\ln_2(1) = \ln_2(-1) = 0$, поэтому, как только мы покидаем $1 + D_2$, инъективность пропадает.

2. Этот изоморфизм аналогичен тому, который имеет место в вещественном случае, когда log и exp определяют взаимно обратные изоморфизмы между группой положительных действительных чисел по умножению и группой всех действительных чисел по сложению.

Но оказывается, и это особенно интересно, что экспонента является изометрией! Чтобы это доказать, нам понадобится следующее предложение.

Предложение 18.3. *Для любого $x \in D_p$ имеют место следующие соотношения*:

1) $|\exp_p(x)|_p = 1$;

2) $|\ln_p(1 + x)|_p = |x|_p$;

3) $|1 - \exp_p(x)|_p = |x|_p$.

Доказательство. Для любого натурального числа $n \geqslant 1$ имеем $S_n \geqslant 1$ (сумма p-адических цифр числа n). Тогда

$$\operatorname{ord}_p(n!) = \frac{n - S_n}{p - 1} \leqslant \frac{n - 1}{p - 1}.$$

С другой стороны, $\operatorname{ord}_p(n) \leqslant \operatorname{ord}_p(n!)$. Пусть $r_p = p^{-\frac{1}{p-1}}$ — радиус круга D_p. Тогда

$$|n|_p \geqslant |n!|_p \geqslant p^{-\frac{n-1}{p-1}} = r_p^{n-1}$$

и

$$\left|\frac{x^n}{n}\right|_p \leqslant \left|\frac{x^n}{n!}\right|_p \leqslant \left(\frac{|x|_p}{r_p}\right)^{n-1} |x|_p < |x|_p < 1$$

при $n \geqslant 2$ и $0 < |x|_p < r_p$.

Свойство равнобедренного треугольника (предложение 2.11) можно переформулировать следующим образом:

$$|a|_p > |b|_p \Rightarrow |a + b|_p = |a|_p \qquad (\textit{побеждает сильнейший!})$$

Можно написать

$$\exp_p(x) = 1 + x + \sum_{n=2}^{\infty} \frac{x^n}{n!}.$$

Так как

$$|1|_p = 1 \quad \text{и} \quad \left| x + \sum_{n=2}^{\infty} \frac{x^n}{n!} \right|_p < 1,$$

имеем $|\exp_p(x)|_p = 1$. Аналогично получаем

$$|\ln_p(1+x)|_p = |x|_p \quad \text{и} \quad |1 - \exp_p(x)|_p = |x|_p,$$

что и требовалось доказать. □

Замечание 18.4. Попутно мы получили более короткое доказательство оценок из предложения 15.5.

Следствие 18.5. *Отображения*

$$\exp_p\colon D_p \to 1 + D_p \quad \textit{и} \quad \ln_p\colon 1 + D_p \to D_p$$

являются изометриями.

Доказательство. Пусть $x, y \in D_p$. Тогда

$$|\exp_p(x) - \exp_p(y)|_p = |\exp_p(y)|_p |\exp_p(x-y) - 1|_p = \\ = |\exp_p(x-y) - 1|_p = |x-y|_p,$$

откуда следует изометричность экспоненты. Так как $\exp_p(\ln_p(1+x)) = 1 + x$, имеем

$$|\ln_p(1+x) - \ln_p(1+y)|_p = |(1+x) - (1+y)|_p = |x-y|_p,$$

откуда следует изометричность логарифма. □

В завершение этого параграфа покажем, что $\exp_p(x)$ и $\ln_p(x)$ удовлетворяют тем же самым дифференциальным уравнениям, что и их вещественные аналоги:

$$\exp_p'(x) = \exp_p(x) \quad \text{и} \quad \ln_p'(x) = \frac{1}{x}$$

в соответствующих областях сходимости.

Сначала напомним определение производной (в контексте p-адического анализа).

Определение 18.6. Пусть $X \subset \mathbb{Q}_p$, $a \in X$ — предельная точка множества X. Функция $f\colon X \to \mathbb{Q}_p$ называется *дифференцируемой в точке* a, если существует производная $f'(a)$ функции f в точке a, равная

$$\lim_{x \to a} \frac{f(x) - f(a)}{x - a}.$$

Функция $f\colon X \to \mathbb{Q}_p$ называется *дифференцируемой на множестве* X, если $f'(a)$ существует в каждой точке $a \in X$.

Заметим, что определение производной имеет смысл, так как $\mathbb{Q}_p$ является нормированным полем. Производная обладает следующими стандартными свойствами.

1. Хорошо известные правила дифференцирования суммы, произведения, частного и композиции переносятся без каких-либо затруднений.

2. Как следствие, производная многочлена $P(x) = \sum\limits_{i=0}^{n} a_i x^i$ равна $P'(x) = \sum\limits_{i=1}^{n} i a_i x^{i-1}$.

3. Рациональные функции (частное двух многочленов) дифференцируемы.

4. Дифференцируемые функции непрерывны.

Мы уже доказали (см. предложение 14.7), что если $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$ — степенной ряд, то его формальная производная $Df(X) = \sum\limits_{n=1}^{\infty} n a_n X^{n-1}$ имеет тот же самый радиус сходимости, что и сам ряд. Как и в вещественном или комплексном случае, формальный степенной ряд $Df(X)$ представляет производную $f'(x)$ в области сходимости.

Предложение 18.7. *Рассмотрим степенной ряд*

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]],$$

и предположим, что ряд $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$ *сходится в открытом шаре* $U \subset \mathbb{Q}_p$. *Тогда функция* $f(x)$ *дифференцируема в* U *и для всех* $x \in U$ *выполняется равенство*

$$f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}.$$

Более того, функция $f(x)$ *имеет в* U *производные всех порядков, которые раскладываются в ряды следующим образом*:

$$f^{(k)}(x) = k! \sum_{n=k}^{\infty} \binom{n}{k} a_n x^{n-k}.$$

Коэффициенты исходного степенного ряда можно вычислить по следующим формулам:

$$a_k = \frac{f^{(k)}(0)}{k!}.$$

Теперь мы можем вычислить производные функций $\exp_p$ и $\ln_p$ с помощью разложений в степенные ряды.

Предложение 18.8. 1. *Функция* $\exp_p$ *дифференцируема в* D_p *и*

$$\exp'_p(x) = \exp_p(x).$$

2. *Функция* $\ln_p$ *дифференцируема в* $1 + p\mathbb{Z}_p$ *и*

$$\ln'_p(x) = \frac{1}{x}.$$

Доказательство. Действительно,

$$\exp'_p(x) = \sum_{n=1}^{\infty} \frac{nx^{n-1}}{n!} = \sum_{n=1} \frac{x^{n-1}}{(n-1)!} = \exp_p(x).$$

Аналогично

$$\ln'_p(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{n(x-1)^{n-1}}{n} = \sum_{n=1}^{\infty} (-1)^{n-1}(x-1)^{n-1} = \frac{1}{x},$$

как и утверждалось. □

Теперь с помощью p-адических логарифмов определим, какие примитивные корни из единицы степени p можно извлечь в $\mathbb{Z}_p$.

Теорема 18.9. *Примитивные корни из единицы степени* p^n *не принадлежат* $\mathbb{Q}_p$, *за исключением случая* $p = 2$, *а* $n = 1$.

Доказательство. Пусть $p \neq 2$ и $x^{p^n} = 1$. Тогда $|x|_p = 1$, т.е. $x \in \mathbb{Z}_p$, и первая цифра x_0 числа x удовлетворяет сравнению $x_0^{p^n} \equiv 1 \pmod p$. Однако порядок каждого элемента мультипликативной группы $(\mathbb{Z}/p\mathbb{Z})^\times$ должен делить порядок самой группы, т.е. число $(p-1)$. Отсюда следует, что $x_0 = 1$ и $x \in 1 + p\mathbb{Z}_p$. Из инъективности функции $\ln_p$ (предложение 18.1) следует, что единственным корнем уравнения $\ln_p(x) = 0$ является $x = 1$. Так как $x^{p^n} = 1$, получаем

$$0 = \ln_p(1) = \ln_p(x^{p^n}) = p^n \ln_p(x), \text{ значит, } \ln_p(x) = 0,$$

откуда $x = 1$.

Однако в случае $p = 2$ имеем $\ln_2(-1) = \ln_2(1) = 0$ (см. пример 15.7), и аналогичные рассуждения показывают, что, хотя $x = -1$ является нетривиальным квадратным корнем из 1 в $\mathbb{Q}_2$, в $\mathbb{Q}_2$ не существует нетривиальных корней из единицы степени 2^n при $n > 1$. □

Глава 4
p-адические функции

§ 19. Локально постоянные функции

В заключительной части наших лекций мы изучим p-адические функции p-адического переменного. Напомним определение 12.6 для случая $X = \mathbb{Z}_p$, $Y = \mathbb{Q}_p$, если два последних пространства снабжены p-адической метрикой.

Определение 19.1. Функция $f: \mathbb{Z}_p \to \mathbb{Q}_p$ называется *непрерывной в точке* $a \in \mathbb{Z}_p$, если для любого $\varepsilon > 0$ существует такое $\delta > 0$, что для любого $x \in \mathbb{Z}_p$, удовлетворяющего неравенству $|x - a|_p < \delta$, выполнено неравенство $|f(x) - f(a)|_p < \varepsilon$.

Функция $f: \mathbb{Z}_p \to \mathbb{Q}_p$ называется *непрерывной*, если она непрерывна в каждой точке $a \in \mathbb{Z}_p$.

Функция $f: \mathbb{Z}_p \to \mathbb{Q}_p$ называется *равномерно непрерывной*, если для любого $\varepsilon > 0$ существует такое $\delta > 0$, что для любых x, $y \in \mathbb{Z}_p$, удовлетворяющих неравенству $|x - y|_p < \delta$, выполнено неравенство $|f(x) - f(y)|_p < \delta$.

Пример 19.2. Так как пространство $\mathbb{Z}_p$ вполне несвязно, *характеристическая функция* любого шара $U \in \mathbb{Z}_p$, имеющая вид

$$\xi_U(x) = \begin{cases} 1, & \text{если } x \in U, \\ 0, & \text{если } x \in \mathbb{Z}_p \setminus U \end{cases}$$

непрерывна. Это очевидно, так как сам шар U и его дополнение $\mathbb{Z}_p \setminus U$ являются открытыми множествами.

Это понятие можно обобщить следующим образом.

Определение 19.3. Функция $f: \mathbb{Z}_p \to \mathbb{Q}_p$ называется *локально постоянной*, если для каждого $x \in \mathbb{Z}_p$ существует такая окрестность $U_x \ni x$ (например, шар с центром в точке x радиуса p^{-m} для некоторого $m \in \mathbb{N}$, $\{y \in \mathbb{Z}_p : |x - y|_p < p^{-m}\}$), что функция f постоянна в U_x.

Замечание 19.4. Локально постоянными функциями на $\mathbb{R}$ или на интервале (или на любом связном пространстве) являются константы и только они.

Предложение 19.5. *Локально постоянные функции непрерывны.*

Доказательство. Очевидно из определения. □

Следующее утверждение вытекает из компактности пространства $\mathbb{Z}_p$ (теорема 4.6).

Предложение 19.6. *Пусть $f: \mathbb{Z}_p \to \mathbb{Q}_p$ — локально постоянная функция. Тогда $\mathbb{Z}_p$ можно представить в виде конечного объединения*

$$\mathbb{Z}_p = \bigcup_{i=1}^{k} U_{x_i}$$

таких попарно непересекающихся шаров, что функция f постоянна в каждом из этих шаров. В частности, множество $\{f(x): x \in \mathbb{Z}_p\}$ всех значений функции f состоит из конечного числа элементов.

Доказательство. Рассмотрим множество всех шаров U_x из определения локально постоянной функции. Все такие шары образуют открытое покрытие пространства $\mathbb{Z}_p$. Так как пространство $\mathbb{Z}_p$ компактно, это покрытие содержит конечное подпокрытие $U_{x_1}, \ldots, U_{x_k}$. Напомним, что два шара в ультраметрическом пространстве либо не пересекаются, либо один содержится в другом, поэтому, если удалить шары, содержащиеся в других шарах, получится покрытие пространства $\mathbb{Z}_p$ попарно не пересекающимися шарами. □

Следствие 19.7. *Любая локально постоянная функция, определенная на $\mathbb{Z}_p$, равномерно непрерывна.*

Доказательство. Пусть p^{-m_i} — радиус шара U_{x_i}, $i = 1, 2, \ldots, k$, и $m = \max\limits_i m_i$. Покажем, что $\delta = p^{-m}$ является искомым для любого $\varepsilon > 0$. В самом деле, пусть $|x - y|_p < p^{-m}$. Так как $x \in U_{x_i}$ для некоторого i и каждая точка шара является его центром, можно считать, что $x = x_i$. Тогда $|x_i - y|_p < p^{-m} \leqslant p^{-m_i}$, т. е. $f(y) = f(x_i) = f(x)$. □

Множество $\mathbb{Z}_p$ содержит подмножество $\mathbb{N}$ натуральных чисел и подмножество $\mathbb{Z}$ целых чисел, которые плотны в $\mathbb{Z}_p$ (теорема 11.11), поэтому иногда мы будем рассматривать функции из $\mathbb{N}$ в $\mathbb{Q}_p$, из $\mathbb{Z}$ в $\mathbb{Q}_p$ и, вообще, из $E \to \mathbb{Q}_p$, где $E \subset \mathbb{Z}_p$.

Определение 19.8. Пусть E — подмножество пространства $\mathbb{Z}_p$, не обязательно компактное. Функция $f: E \to \mathbb{Q}_p$ называется *кусочно постоянной на E*, если существует такое натуральное число t, что

$$f(x) = f(x_0) \quad \text{для всех таких } x, x_0 \in E, \text{ что } |x - x_0|_p \leqslant p^{-t}.$$

Наименьшее целое число t, для которого выполнено это условие, называется *порядком* функции f.

Из определения ясно, *что кусочно постоянная функция равномерно непрерывна и локально постоянна на E.*

Для каждого натурального числа t построим разбиение множества E следующим образом. Положим $\mathbb{N}_t = \{0, 1, 2, \ldots, p^t - 1\}$. Для каждого $x \in \mathbb{Z}_p$ напишем каноническое разложение

$$x = x_0 + x_1 p + \ldots + x_{t-1} p^{t-1} + \ldots$$

и положим

$$N_x = x_0 + x_1 p + \ldots + x_{t-1} p^{t-1}. \tag{19.1}$$

Тогда $N_x \in \mathbb{N}_t$ и

$$|x - N_x|_p \leqslant p^{-t}. \tag{19.2}$$

Для каждого $N \in \mathbb{N}_t$ положим

$$E(N) = E \cap U(N, t), \quad \text{где } U(N, t) = \{x \in \mathbb{Z}_p : |x - N|_p \leqslant p^{-t} < p^{-t+1}\}.$$

Мы уже видели, что каждое число $x \in \mathbb{Z}_p$ принадлежит некоторому шару $U(N, t)$, и, так как для любых $N, M \in \mathbb{N}_t$ выполнено неравенство $|N - M|_p > p^{-t}$, шары $U(N, t)$ попарно не пересекаются. Таким образом, получаем разбиение множества E:

$$E = \bigcup_{N=0}^{p^t-1} E(N). \tag{19.3}$$

Теперь мы можем доказать следующую довольно неожиданную теорему.

Теорема 19.9. *Любая кусочно постоянная функция на $\mathbb{N}$ или $\mathbb{Z}_p$ является периодической.*

Доказательство. Пусть $E = \mathbb{N}$ или $\mathbb{Z}_p$, и пусть $f: E \to \mathbb{Q}_p$ — кусочно постоянная функция порядка t. Рассмотрим описанное выше разбиение (19.3) множества E. Если $x, y \in E(N)$, то, применяя сильное неравенство треугольника, имеем $|x - y|_p = |(x - N) + (N - y)|_p \leqslant p^{-t}$, следовательно, $f(x) = f(y)$. Заметим, что если $x \in E(N)$, то $x + p^t \in E(N)$. Таким образом,

$$f(x + p^t) = f(x) \quad \text{для всех } x \in E,$$

т. е. функция f является периодической. □

В вещественном анализе есть теорема, которая утверждает, что всякая функция, непрерывная на отрезке, может быть равномерно приближена с любой точностью кусочно постоянной функцией. Аналогичный результат имеет место и для p-адических функций. Здесь даже есть дополнительное преимущество: в p-адическом случае кусочно постоянные функции непрерывны.

Теорема 19.10. *Пусть $E = \mathbb{N}$ или $\mathbb{Z}_p$. Функция $f: E \to \mathbb{Q}_p$ равномерно непрерывна на E тогда и только тогда, когда для каждого натурального числа s существуют такое натуральное число $t = t(s)$ и такая кусочно постоянная функция $S: E \to \mathbb{Q}_p$ порядка не выше t, что*

$$|f(x) - S(x)|_p \leqslant p^{-s} \quad \textit{для любого } x \in E. \tag{19.4}$$

Доказательство. Предположим, что функции f и S удовлетворяют неравенству (19.4). Если x_0 удовлетворяет неравенству

$$|x - x_0|_p \leqslant p^{-t},$$

то

$$S(x) = S(x_0), \quad |f(x) - S(x)|_p \leqslant p^{-s}, \quad |f(x_0) - S(x_0)|_p \leqslant p^{-s},$$

и тогда

$$|f(x) - f(x_0)|_p = |(f(x) - S(x)) - (f(x_0) - S(x_0)|_p \leqslant p^{-s},$$

откуда следует равномерная непрерывность функции f.

Обратно, предположим, что функция f равномерно непрерывна на E. Тогда для любого натурального числа s существует такое натуральное число $t = t(s)$, что

$$|f(x) - f(x_0)|_p \leqslant p^{-s}, \quad \text{если } x, x_0 \in E \text{ и } |x - x_0|_p \leqslant p^{-t}. \tag{19.5}$$

Определим функцию $S: E \to \mathbb{Q}_p$ следующим образом:

$$S(x) = f(N_x), \quad \text{если } x \in E,$$

где число N_x определяется соотношением (19.1). Тогда S является кусочно постоянной функцией порядка не выше t. Из неравенств (19.2) и (19.5) имеем

$$|f(x) - S(x)|_p = |f(x) - f(N_x)|_p \leqslant p^{-s},$$

что и требовалось доказать. □

Упражнения

В первых трех задачах предполагается, что число x является элементом кольца $\mathbb{Z}_p$ и записано в каноническом виде

$$x = x_0 + x_1 p + x_2 p^2 + \ldots,$$

где коэффициенты x_n являются p-адическими цифрами $0, 1, 2, \ldots, p - 1$.

64. Определите, являются ли следующие функции равномерно непрерывными на $\mathbb{N}$ или непрерывными на $\mathbb{Z}_p$:

1) $f(x) = x_0 + x_1 x_2$;

2) $f(x) = P(x_0, x_1, x_3)$, где P — многочлен с коэффициентами в $\mathbb{Z}_p$;

3) $f(x) = \begin{cases} 1, & \text{если } x_0 = 0, \\ x/x_0, & \text{если } x_0 \neq 0. \end{cases}$

65. Являются ли какие-то функции из упражнения 64 локально постоянными или кусочно постоянными? Ответ обоснуйте.

66. Какие из следующих двух функций $f(x) = \sum_{n=0}^{\infty} x_n$; $f(x) = \sum_{n=0}^{\infty} x_n n!$ непрерывны? локально постоянны на $\mathbb{N}$?

67. Пусть функция $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ определяется следующим образом:

$$f(x) = \begin{cases} 0, & \text{если } x = 0, \\ 1/|x|_p, & \text{если } x \neq 0. \end{cases}$$

Является ли функция f непрерывной? локально постоянной на $\mathbb{Z}_p$?

§ 20. Непрерывные и равномерно непрерывные функции

Пусть $E \subset \mathbb{Z}_p$ и $x_0 \in E$ — предельная точка множества E. Перечислим некоторые свойства функций, непрерывных на E.

Теорема 20.1. *Пусть* $f\colon E \to \mathbb{Q}_p$, $g\colon E \to \mathbb{Q}_p$.

1) *Функция f непрерывна в точке $x_0 \in E$ тогда и только тогда, когда для любой такой последовательности $\{x_n\}$, что $\lim\limits_{n\to\infty} x_n = x_0$, выполняется равенство*

$$\lim_{n\to\infty} f(x_n) = f(x_0).$$

2) *Если функции f и g непрерывны в точке $x_0 \in E$, то функции $f+g$, $f-g$ и fg также непрерывны в этой точке. Если, кроме того, $g(x_0) \neq 0$, то функция f/g также непрерывна в точке x_0.*

Доказательство, точно такое же, как и в вещественном случае, мы оставляем читателю. Теперь приведем несколько примеров разрывных функций.

Пример 20.2. Пусть функция $f\colon \mathbb{N} \to \mathbb{Q}_p$ определяется следующей формулой:

$$f(x) = \frac{1}{x-c},$$

где $c \in \mathbb{Z}_p$. Если $c \notin \mathbb{N}$, то знаменатель не обращается в нуль на $\mathbb{N}$ и по теореме 20.1 функция f непрерывна на $\mathbb{N}$ (но не равномерно непрерывна — можете ли вы это доказать?). Однако функция f не ограничена на $\mathbb{N}$. Действительно, так как c является целым p-адическим числом, существуют такие натуральные числа x, что норма $|x-c|_p$ сколь угодно мала, и поэтому норма $|f(x)|_p$ сколь угодно велика. Если $c \in \mathbb{N}$, то функция f разрывна в точке c.

Пример 20.3. Следующие примеры используют специфику p-адических чисел и, на первый взгляд, не похожи на примеры из вещественного анализа. Однако, оказывается, вещественные аналоги у этих примеров все-таки есть. Мы вернемся к этому вопросу в § 21. Рассмотрим такую бесконечно малую последовательность целых p-адических чисел $\{a_n\}$, что $a_n \neq 0$ для всех n. По этой последовательности построим две функции $f_1: \mathbb{Z}_p \to \mathbb{Q}_p$ и $f_2: \mathbb{Z}_p \to \mathbb{Q}_p$ следующим образом:

$$f_1(x) = \begin{cases} a_x, & \text{если } x \in \mathbb{N}, \\ 0, & \text{если } x \notin \mathbb{N} \text{ (но } x \in \mathbb{Z}_p), \end{cases}$$

$$f_2(x) = \begin{cases} a_x, & \text{если } x \in \mathbb{N}, \\ 1, & \text{если } x \notin \mathbb{N} \text{ (но } x \in \mathbb{Z}_p). \end{cases}$$

Обе функции f_1 и f_2 разрывны в точках из $\mathbb{N}$. Чтобы в этом убедиться, возьмем произвольное число $x \in \mathbb{N}$, тогда $\lim\limits_{n\to\infty}(x + p^n) = x$ и

$$\lim_{n\to\infty} f_1(x + p^n) = \lim_{n\to\infty} a_{x+p^n} = 0,$$

так как вторая последовательность является подпоследовательностью бесконечно малой последовательности. Однако $f_1(x) = a_x \neq 0$, и аналогичное утверждение верно для f_2.

Докажем, что функция f_1 непрерывна во всех точках $x \in \mathbb{Z}_p \setminus \mathbb{N}$. В самом деле, возьмем любую последовательность $x_n \to x$, и пусть $\{x_{r_n}\}$ — подпоследовательность, содержащаяся в $\mathbb{N}$. Тогда $a_{x_{r_n}} \to 0$, как подпоследовательность бесконечно малой последовательности, и, следовательно, $f_1(x_n) \to 0$.

Функция f_2 разрывна во всех точках множества $\mathbb{Z}_p$. Действительно, если $x \in \mathbb{Z}_p \setminus \mathbb{N}$, возьмем такую последовательность $\{x_n\}$, состоящую из натуральных чисел, что $x_n \to x$. Тогда $f_2(x_n) \to 0$, но $f_2(x) = 1 \neq 0$.

Так как множество $\mathbb{Z}_p$ компактно, имеет место следующая теорема (ср. [9], теорема 4.19).

Теорема 20.4. *Каждая функция $f: \mathbb{Z}_p \to \mathbb{Q}_p$, непрерывная на $\mathbb{Z}_p$, равномерно непрерывна и ограничена.*

Докажем теперь следующую важную теорему. Мы воспользуемся ею в случае $E = \mathbb{N}$ (тогда замыкание $\overline{E}$ совпадает с $\mathbb{Z}_p$).

Теорема 20.5. *Пусть E — подмножество множества $\mathbb{Z}_p$, а $\overline{E}$ — его замыкание. Пусть функция $f: E \to \mathbb{Q}_p$ равномерно непрерывна на E. Тогда существует единственная функция $F: \overline{E} \to \mathbb{Q}_p$, равномерно непрерывная и ограниченная на $\overline{E}$ и такая, что*

$$F(x) = f(x), \text{ если } x \in E.$$

Доказательство. Пусть $X \in \bar{E}$. Тогда в E существует такая последовательность $\{x_n\}$, что

$$x_n \to X \quad \text{при } n \to \infty. \tag{20.1}$$

(Представляет интерес только случай $X \notin E$.) Так как функция f равномерно непрерывна на E, для любого натурального числа s существует другое натуральное число $t = t(s)$, для которого выполняется неравенство (19.5). Согласно соотношению (20.1) существует такое натуральное число $N = N(t)$, что

$$|x_n - X|_p \leqslant p^{-t} \quad \text{при } n \geqslant N.$$

Тогда для $n, m \geqslant N$ имеем

$$|x_m - x_n|_p = |(x_m - X) - (x_n - X)|_p \leqslant p^{-t}$$

и из (19.5) получаем

$$|f(x_m) - f(x_n)|_p \leqslant p^{-s}.$$

Это означает, что $\{f(x_n)\}$ — p-адическая последовательность Коши. Пусть $L = \lim\limits_{n\to\infty} f(x_n)$ — ее предел.

Легко видеть, что этот предел не зависит от выбора последовательности $x_n \to X$. Действительно, пусть $\{x'_n\}$ — другая последовательность и $x'_n \to X$. Тогда последовательность $\{x_n - x'_n\}$ бесконечно мала и, так как функция f равномерно непрерывна, последовательность $\{f(x_n) - f(x'_n)\}$ также бесконечно мала; но отсюда следует, что

$$L = \lim_{n\to\infty} f(x'_n).$$

Таким образом, функция $F\colon \bar{E} \to \mathbb{Q}_p$, заданная формулой

$$F(X) = \lim_{n\to\infty} f(x_n)$$

при $X \in \bar{E}$ и $X = \lim\limits_{n\to\infty} x_n$, $x_n \in E$, определена корректно.

Покажем, что функция F равномерно непрерывна на $\bar{E}$. Пусть пара точек X и X_0 из $\bar{E}$ удовлетворяет неравенству $|X - X_0|_p \leqslant p^{-t}$. Выберем в E точки x и x_0 так, чтобы выполнялись неравенства

$$|x - X|_p \leqslant p^{-t}, \quad |x_0 - X_0|_p \leqslant p^{-t},$$
$$|f(x) - F(X)|_p \leqslant p^{-s}, \quad |f(x_0) - F(X_0)|_p \leqslant p^{-s}.$$

Тогда

$$|x - x_0|_p = |(x - X) + (X - X_0) - (x_0 - X_0)|_p \leqslant p^{-t},$$

и из (19.5) имеем $|f(x) - f(x_0)|_p \leqslant p^{-s}$. Таким образом,

$$|F(X) - F(X_0)|_p = |-(f(x) - F(X)) + (f(x) - f(x_0)) + (f(x_0) - F(X_0))|_p \leqslant p^{-s},$$

тем самым, равномерная непрерывность F на $\bar{E}$ доказана.

Докажем, наконец, что функция F ограничена на $\bar{E}$. Действительно, в противном случае нашлась бы такая бесконечная последовательность $\{X_n\} \subset \bar{E}$, что

$$\lim_{n\to\infty} |F(X_n)|_p = \infty. \tag{20.2}$$

Так как E, а значит, и $\bar{E}$, являются подмножествами компактного множества $\mathbb{Z}_p$, найдется такая подпоследовательность $\{X_{r_n}\}$, что существует предел

$$X_0 = \lim_{n\to\infty} X_{r_n}.$$

Поскольку все члены этой подпоследовательности принадлежат $\bar{E}$, а множество $\bar{E}$ замкнуто, $X_0 \in \bar{E}$. Как мы уже знаем, функция F равномерно непрерывна на $\bar{E}$, а значит, и непрерывна в точке X_0. Отсюда получаем

$$\lim_{n\to\infty} F(X_{r_n}) = F(X_0),$$

что противоречит условию (20.2).

Чтобы доказать единственность функции F, предположим, что существует другая функция F^* с теми же свойствами. Тогда разность $F - F^*$ равномерно непрерывна на $\bar{E}$ и тождественно равна нулю на E. Так как множество E плотно в $\bar{E}$, по непрерывности функция $F - F^*$ также тождественно равна нулю на $\bar{E}$. □

§ 21. Точки разрыва и теорема Бэра о категории

Функция f_1 из примера 20.3 имеет близкий аналог в вещественном анализе, это так называемая *функция Римана* $r\colon \mathbb{R} \to \mathbb{R}$, которая определяется следующим образом:

$$r(x) = \begin{cases} 1/q, & \text{если число } x \text{ рациональное, } x = p/q,\ (p, q) = 1, \\ 0, & \text{если число } x \text{ иррациональное.} \end{cases}$$

Эта функция непрерывна во всех иррациональных точках и разрывна во всех рациональных. Функция f_2 из примера 20.3 также имеет действительный аналог (см. упражнение 68) — функцию, разрывную во всех точках множества $\mathbb{R}$. Другим примером функции, разрывной во всех точках множества $\mathbb{R}$, является характеристическая множества рациональных чисел или *функция Дирихле*:

$$\chi_{\mathbb{Q}}(x) = \begin{cases} 1, & \text{если число } x \text{ рациональное,} \\ 0, & \text{если число } x \text{ иррациональное.} \end{cases}$$

Возникает естественный вопрос: существует ли вещественная функция, разрывная во всех иррациональных точках и непрерывная во всех

рациональных? Аналогичный вопрос: существует ли p-адическая функция, разрывная во всех точках из $\mathbb{Z}_p \setminus \mathbb{N}$ и непрерывная во всех точках из $\mathbb{N}$? Ответ на оба эти вопроса отрицательный. Причина этого — теорема Бэра о категории, которая верна для любого полного метрического пространства.

Пусть (X, ρ) — метрическое пространство. Пусть $\mathcal{G}$ обозначает семейство всех открытых подмножеств множества X, а $\mathcal{F}$ обозначает семейство всех замкнутых подмножеств множества X. По определению (см. § 11) каждый элемент из $\mathcal{F}$ является дополнением единственного элемента из $\mathcal{G}$ и наоборот. Напомним, что множество $\mathcal{G}$ замкнуто по отношению к любым объединениям и конечным пересечениям, а множество $\mathcal{F}$ замкнуто относительно любых пересечений и конечных объединений (предложение 11.1). Легко построить примеры, в которых счетное пересечение открытых множеств не является открытым и счетное пересечение замкнутых множеств не замкнуто. Однако такие множества настолько важны в анализе, что им даны специальные названия.

Определение 21.1. Множество $A \subset X$ называется *множеством типа* $\mathcal{G}_\delta$, если его можно представить в виде счетного пересечения открытых множеств; множество $A \subset X$ называется *множеством типа* $\mathcal{F}_\sigma$, если его можно представить в виде счетного объединения замкнутых множеств.

Теорема 21.2. *Пусть (X, ρ) и (Y, d) — два метрических пространства и $f: X \to Y$ — любое отображение. Тогда множество всех точек, в которых отображение f непрерывно, является множеством типа $\mathcal{G}_\delta$.*

Доказательство. Пусть $A \subset X$. Определим *колебание функции f на множестве A* как элемент расширенного множества действительных чисел $\mathbb{R} \cup \infty$, заданный следующим образом:

$$\omega(A) = \sup\{d(f(x), f(y)): x, y \in A\}.$$

Для $x_0 \in X$ определим *колебание функции f в точке x_0*, полагая

$$\omega(x_0) = \lim_{\delta \to 0} \omega(B(x_0, \delta)).$$

Лемма 21.3. *Пусть $f: X \to Y$ и $\varepsilon > 0$. Тогда множество*

$$W_\varepsilon = \{x \in X: \omega(x) < \varepsilon\}$$

открыто.

Доказательство леммы 21.3. Пусть $x_0 \in W_\varepsilon$. Пусть $\omega(x_0) < \varepsilon$. Это означает, что существует такое $\delta > 0$, что для любых $x, y \in B(x_0, \delta)$ выполнено неравенство $d(f(x), f(y)) < \varepsilon_1 < \varepsilon$. Пусть $z \in B(x_0, \delta/2)$. Если $z_1, z_2 \in B(z, \delta/2)$, то $z_1, z_2 \in B(x_0, \delta)$ и поэтому

$$d(f(z_1), f(z_2)) < \varepsilon_1.$$

Отсюда следует, что $\omega(B(z, \delta/2)) \leqslant \varepsilon_1 < \varepsilon$. Но тогда $\omega(z) < \varepsilon$ и множество W_ε открыто. □

Чтобы завершить доказательство теоремы, заметим, что

$$\{x: \omega(x) = 0\} = \bigcap_{n=1}^{\infty} W_{1/n},$$

поэтому (см. упражнение 72) множество всех точек непрерывности отображения f имеет тип $\mathcal{G}_\delta$. □

Следствие 21.4. *Множество точек разрыва любой функции $f: X \to Y$ имеет тип $\mathcal{F}_\sigma$.*

Доказательство. См. упражнение 71. □

Теорема 21.5 (теорема Бэра о категории). *Пусть (X, ρ) — полное метрическое пространство, и пусть $S = \bigcup_{n=1}^{\infty} S_n$, причем все множества S_n нигде не плотны в X. Тогда множество $X \setminus S$ всюду плотно в X. В частности, множество X нельзя представить в виде счетного объединения нигде не плотных множеств.*

Доказательство. Пусть B_0 — непустой шар в X. Чтобы доказать, что мнжество $X \setminus S$ всюду плотно, покажем, что $X \setminus S \cap B_0 \neq \varnothing$. Построим по индукции такую последовательность вложенных шаров $B_n = B_n(x_n, r_n)$, что $r_n < 1/n$ и

$$\overline{B_{n+1}} \subset B_n \setminus \overline{S_{n+1}}.$$

Чтобы убедится в том, что это возможно, заметим, что $B_n \setminus \overline{S_{n+1}} \neq \varnothing$, так как множество S_{n+1}, а значит, и множество $\overline{S_{n+1}}$ нигде не плотны. Тогда возьмем какую-нибудь точку $x_{n+1} \in B_n \setminus \overline{S_{n+1}}$. Поскольку множество $\overline{S_{n+1}}$ замкнуто, имеем

$$\operatorname{dist}(x_{n+1}, S_{n+1}) > 0,$$

поэтому можно выбрать требуемый шар B_{n+1}. Последовательность $\{x_n\}$ является последовательностью Коши, так как для любых $n, m > N$ выполняется неравенство

$$\rho(x_n, x_m) \leqslant \rho(x_n, x_N) + \rho(x_N, x_m) < \frac{2}{N}.$$

Так как пространство X полно, существует такая точка x, что $x_n \to x$. Но для всех n точка x_{n+1} принадлежит $\overline{B_{n+1}}$, поэтому

$$x \in \bigcap_{n=1}^{\infty} \overline{B_n} \subset B_0 \cap (X \setminus S),$$

что и требовалось доказать. □

Теперь мы готовы доказать следующую теорему.

Теорема 21.6. *Не существует функции $f\colon \mathbb{R} \to \mathbb{R}$, непрерывной во всех рациональных точках и разрывной во всех иррациональных точках.*

Доказательство. Согласно следствию 21.4, достаточно доказать, что множество всех иррациональных чисел не является множеством типа $\mathcal{F}_\sigma$. Предположим обратное: пусть $\mathbb{R} \setminus \mathbb{Q} = \bigcup\limits_{n=1}^{\infty} F_n$, причем все множества F_n замкнуты. Тогда каждое множество F_n нигде не плотно, так как в противном случае нашелся бы интервал, в котором F_n было бы плотно, а это невозможно, поскольку, будучи замкнутым множеством, F_n содержало бы этот интервал, что противоречит тому, что $\mathbb{R} \setminus \mathbb{Q}$ не содержит никакого интервала.

Далее заметим, что множество $\mathbb{Q}$ имеет тип $\mathcal{F}_\sigma$, так как оно является объединением счетного числа точек, которые, конечно же, являются замкнутыми множествами. Таким образом, мы представили множество $\mathbb{R}$, которое является полным метрическим пространством, в виде счетного объединения нигде не плотных множеств, что противоречит теореме Бэра о категории. □

Упражнение 73 содержит p-адический аналог этого утверждения.

Упражнения

68. Постройте функцию $f\colon \mathbb{R} \to \mathbb{R}$, которая напоминает функцию f_2 из примера 20.3, и докажите, что она разрывна в каждой точке.

69. Пусть X — метрическое пространство. Докажите, что

1) если множество F замкнуто, то оно имеет тип $\mathcal{G}_\delta$;

2) если множество G открыто, то оно имеет тип $\mathcal{F}_\sigma$.

70. Постройте множество, которое принадлежит $\mathcal{F}_\sigma \cap \mathcal{G}_\delta$, но не является ни открытым, ни замкнутым.

71. Докажите, что если множество A имеет тип $\mathcal{F}_\sigma$, то его дополнение $X \setminus A$ имеет тип G_δ и наоборот.

72. Докажите, что функция f непрерывна в точке x_0 тогда и только тогда, когда $\omega(x_0) = 0$.

73. Докажите, что не существует функции $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$, которая была бы непрерывна во всех точках из $\mathbb{N}$, но разрывна во всех точках из $\mathbb{Z}_p \setminus \mathbb{N}$.

§ 22. Дифференцируемость p-адических функций

Теорема Лагранжа о среднем значении является краеугольным камнем дифференциального исчисления. Она утверждает, что для каждой пары точек $x \neq y$ из области определения дифференцируемой функции f суще-

ствует такая точка ζ, лежащая *между* точками x и y, что

$$f(y) - f(x) = f'(\zeta)(y - x). \tag{22.1}$$

Таким образом, если $f'(x) = 0$ для всех x, то из равенства (22.1) следует, что $f(x) = f(y)$.

Для p-адических функций это неверно: существуют непостоянные функции, производные которых тождественно равны нулю, поэтому теорему о среднем значении вряд ли можно распространить на p-адический случай, даже если убрать из формулировки слово «между», которое не имеет смысла для p-адических чисел. Следующий пример показывает, что происходит в p-адическом случае.

Пример 22.1. Пусть $E \subset \mathbb{Z}_p$ — подмножество без изолированных точек, и пусть f — локально постоянная функция на E. Тогда для каждого $a \in E$ существует такое $\varepsilon > 0$, что если $x \in E$ удовлетворяет неравенству $|x - a|_p < \varepsilon$, то $f(x) = f(a)$. Таким образом,

$$\frac{f(x) - f(a)}{x - a} = 0, \quad \text{если } |a - x|_p < \varepsilon,$$

поэтому функция f дифференцируема на E и $f'(a) = 0$ для всех $a \in E$!

Из этого примера видно, что существует достаточно широкий класс непостоянных функций, производные которых равны нулю. Этот результат противоположен не только результатам вещественного анализа, но и свойствам аналитических функций, т. е. функций, которые задаются степенными рядами. Действительно, пусть $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$, $x \in \mathbb{R}$, и E — область сходимости этого степенного ряда. Тогда если функция f' тождественно равна нулю, то все ее производные также тождественно равны нулю и по предложению 18.7 все коэффициенты a_k степенного ряда равны нулю при $k \geqslant 1$, поэтому $f(x) = a_0$, т. е. функция является константой.

Как мы уже видели, множество функций $\{f\colon \mathbb{Z}_p \to \mathbb{Q}_p\colon f' = 0\}$, также называемых *псевдоконстантами*, содержит локально постоянные функции. Следующий пример опровергает естественное предположение о том, что все псевдоконстанты являются локально постоянными.

Пример 22.2. Существует инъективная (и, таким образом, не локально постоянная) функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, производная которой тождественно равна нулю.

Доказательство. Пусть $x = \sum\limits_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$; положим

$$f(x) = \sum_{n=0}^{\infty} a_n p^{2n}.$$

Тогда если числа

$$x = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p \quad \text{и} \quad y = \sum_{n=0}^{\infty} b_n p^n \in \mathbb{Z}_p$$

удовлетворяют неравенству $|x - y|_p = p^{-j}$ для некоторого $j = 0, 1, 2, \ldots$, то

$$a_0 = b_0, \quad a_1 = b_1, \quad \ldots, \quad a_{j-1} - b_{j-1}, \quad a_j \neq b_j$$

и поэтому $|f(x) - f(y)|_p = p^{-2j}$. Таким образом, имеем

$$|f(x) - f(y)|_p = |x - y|_p^2 \quad \text{для всех } x, y \in \mathbb{Z}_p.$$

Отсюда мы заключаем, что функция f инъективна (из равенства $f(x) = f(y)$ следует, что $x = y$) и

$$\left|\frac{f(x) - f(y)}{x - y}\right|_p = |x - y|_p \to 0 \quad \text{при } y \to x,$$

т. е. $f' = 0$ тождественно. □

Этот пример приводит нас к определению условия Гёльдера для функций.

Определение 22.3. Пусть $E \subset \mathbb{Z}_p$ и $\alpha > 0$. Функция $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ *удовлетворяет условию Гёльдера порядка* α, если существует такая константа $M > 0$, что для всех $x, y \in E$ имеет место неравенство

$$|f(x) - f(y)|_p \leqslant M|x - y|_p^{\alpha}.$$

Функция из примера 22.2 удовлетворяет условию Гёльдера порядка 2. Заметим, что если функция удовлетворяет условию Гёльдера порядка больше 1, то $f' = 0$, поэтому в вещественном случае f является константой.

В вещественном анализе имеет место теорема Ролля, которая утверждает, что если функция $f\colon [a, b] \to \mathbb{R}$ непрерывна на отрезке $[a, b]$, дифференцируема на интервале (a, b) и $f(a) = f(b)$, то найдется такая точка $\zeta \in (a, b)$, что $f'(\zeta) = 0$. Вот пример, который показывает, что для p-адических функций теорема Ролля, вообще говоря, не имеет места.

Пример 22.4. Рассмотрим функцию $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$, заданную формулой

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

Мы имеем $f(0) = f(1) = 0$, $f'(x) = px^{p-1} - 1$. Кроме того, так как $|f'(x) + 1|_p \leqslant 1/p$, т. е. $f'(x) \in -1 + p\mathbb{Z}_p$, имеем $f'(x) \neq 0$ для всех $x \in \mathbb{Z}_p$.

Еще одно отличие p-адических функций от вещественных обнаруживается, когда мы рассматриваем локальную обратимость (непрерывно) дифференцируемых функций. В вещественном анализе верно следующее: если

для такой функции f выполнено неравенство $f'(x_0) \neq 0$, то функция f локально обратима в некоторой окрестности точки x_0. Для p-адических функций это, вообще говоря, неверно, как показывает следующий поразительный пример.

Пример 22.5. Существует такая дифференцируемая функция $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$, что $f'(x) = 1$ для всех $x \in \mathbb{Z}_p$, но $f(p^n) = f(p^n - p^{2n})$ для всех $n \in \mathbb{N}$, поэтому функция f не инъективна ни в какой окрестности точки 0.

Для каждого $n \in \mathbb{N}$ положим $B_n = \{x \in \mathbb{Z}_p : |x - p^n|_p < p^{-2n}\}$. Если $x \in B_n$, то $|x|_p = p^{-n}$ («побеждает сильнейший»), поэтому все круги B_i попарно не пересекаются. Положим

$$f(x) = \begin{cases} x - p^{2n}, & \text{если } n \in \mathbb{N},\ x \in B_n, \\ x, & \text{если } x \in \mathbb{Z}_p \setminus \bigcup\limits_n B_n. \end{cases}$$

Так как $p^n \in B_n$, имеем $f(p^n) = p^n - p^{2n}$. С другой стороны, легко проверить, что $p^n - p^{2n}$ не лежит ни в каком круге B_m. Отсюда следует, что $f(p^n - p^{2n}) = p^n - p^{2n}$, т. е. функция f не инъективна ни в какой окрестности нуля.

Чтобы доказать, что $f' = 1$, рассмотрим функцию $g(x) = x - f(x)$,

$$g(x) = \begin{cases} p^{2n}, & \text{если } n \in \mathbb{N},\ x \in B_n, \\ 0, & \text{если } x \in \mathbb{Z}_p \setminus \bigcup\limits_n B_n. \end{cases}$$

Так как функция $g(x)$ локально постоянна на $\mathbb{Z}_p \setminus \{0\}$, имеем $g' = 0$ на $\mathbb{Z}_p \setminus \{0\}$, поэтому достаточно проверить, что $g'(0) = 0$. Пусть $x \in \mathbb{Z}_p$, $x \neq 0$, тогда

$$\left|\frac{g(x) - g(0)}{x}\right|_p = \begin{cases} \dfrac{|p^{2n}|_p}{|x|_p} = p^{-n}, & \text{если } n \in \mathbb{N},\ x \in B_n, \\ 0, & \text{если } x \text{ не лежит ни в каком шаре } B_m. \end{cases}$$

Поэтому $g'(0) = \lim\limits_{x \to 0} g(x)/x = 0$. Таким образом, $f'(x) = 1$ для всех $x \in \mathbb{Z}_p$.

§ 23. Непрерывно дифференцируемые функции и изометрии пространства $\mathbb{Q}_p$

В вещественном анализе непрерывно дифференцируемыми функциями называются такие дифференцируемые функции, производные которых непрерывны. Как мы уже видели (пример 22.5), для p-адических функций этого условия для локальной обратимости не достаточно. Оказывается, этой проблемы можно избежать, если усилить определение *непрерывно дифференцируемой* функции в p-адическом случае.

Определение 23.1. Пусть E — непустое подмножество пространства $\mathbb{Q}_p$ без изолированных точек и $f: E \to \mathbb{Q}_p$. *Первой разделенной разностью* $\Phi_1 f$ для функции f называется функция двух переменных x и y, заданная формулой

$$\Phi_1 f(x, y) = \frac{f(x) - f(y)}{x - y} \quad (x, y \in E, x \neq y),$$

определенная на множестве $E \times E \setminus \Delta$, где диагональ Δ — это множесто вида $\Delta = \{(x, x): x \in E\}$. Будем говорить, что функция f *непрерывно дифференцируема* (или C^1-гладкая) в точке $a \in E$, если существует предел

$$\lim_{(x,y)\to(a,a)} \Phi_1 f(x, y).$$

Иными словами, функция f является C^1-гладкой в точке a, если она дифференцируема в точке a и для любого $\varepsilon > 0$ существует такое $\delta > 0$, что если $|x - a|_p < \delta$ и $|y - a|_p < \delta$, $(x, y) \in E \times E \setminus \Delta$, то

$$\left|\frac{f(x) - f(y)}{x - y} - f'(a)\right|_p < \varepsilon. \tag{23.1}$$

Будем говорить, что функция f является C^1-гладкой на E, если она C^1-гладкая во всех точках $a \in E$.

Замечания. 1) Из неравенства (23.1) следует, что всякая C^1-гладкая на E функция имеет непрерывную производную на E. Обратное неверно. Действительно, пусть f — функция из примера 22.5. Тогда

$$\lim_{n\to\infty} \frac{f(p^n) - f(p^n - p^{2n})}{p^{2n}} = 0 \neq 1 = f'(0).$$

2) Для вещественных функций непрерывность производной f' гарантирует существование предела

$$\lim_{(x,y)\to(a,a)} \frac{f(x) - f(y)}{x - y}$$

(предел берется по всем $x, y \in [a, b]$, для которых $x \neq y$), потому что

$$\frac{f(x) - f(y)}{x - y} = f'(\zeta)$$

для некоторого числа ζ между x и y по теореме о среднем.

Теперь рассмотрим C^1-гладкие p-адические функции с точки зрения локальной обратимости. Легко установить локальную инъективность.

Предложение 23.2. *Пусть E — непустое подмножество пространства $\mathbb{Q}_p$ без изолированных точек и функция $f: E \to \mathbb{Q}_p$ является C^1-гладкой в некоторой точке $a \in E$. Если $f'(a) \neq 0$, то существует такая окрестность U точки a, что*

$$|f(x) - f(y)|_p = |f'(a)|_p |x - y|_p \quad (x, y \in E \cap U).$$

Другими словами, функция $f/f'(a)$ является изометрией в некоторой окрестности точки a. В частности, функция f инъективна в окрестности точки a.

Доказательство. По определению C^1-гладких функций существует такое $\delta > 0$, что для любых $x \neq y$, удовлетворяющих неравенствам $|x - a|_p < \delta$ и $|y - b|_p < \delta$, выполнено неравенство

$$\left|\frac{f(x) - f(y)}{x - y} - f'(a)\right|_p < |f'(a)|_p.$$

Тогда по свойству равнобедренного треугольника получаем

$$\frac{|f(x) - f(y)|_p}{|x - y|_p} = |f'(a)|_p. \qquad \square$$

Возникает вопрос: все ли изометрии пространства $\mathbb{Q}_p$ сюръективны? Для многих знакомых нам метрических пространств (например, $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^3$, гиперболическая плоскость) это верно. Однако этим свойством обладают не все метрические пространства, как показывает следующий простой пример.

Рассмотрим множество $E = \{x \in \mathbb{R}: x \geqslant 0\}$ с обычным евклидовым расстоянием $d(x, y) = |x - y|$. Тогда сдвиг $f(x) = x + 1$, очевидно, является изометрией, но не сюръективной.

Тем не менее, все изометрии пространства $\mathbb{Q}_p$ сюръективны, потому что это пространство обладает следующими двумя свойствами.

1) Пространство $\mathbb{Q}_p$ локально компактно.

2) Любой сдвиг $x \mapsto x + a$ ($a \in \mathbb{Q}_p$) является взаимно однозначной изометрией пространства $\mathbb{Q}_p$.

Сначала мы докажем, что нужным нам свойством обладают *компактные* метрические пространства.

Предложение 23.3. *Любая изометрия компактного метрического пространства на себя сюръективна.*

Доказательство. Пусть (X, d) — компактное метрическое пространство, а $f: X \to X$ — его изометрия. Предположим, что отображение f не сюръективно, т.е. существует такая точка $y \in X$, что $y \notin f(X)$. Тогда легко видеть, что существует такой открытый шар $B(y, r)$, что $B(y, r) \not\subset f(X)$. В самом деле, в противном случае нашлась бы такая последовательность $y_n \to y$, что $y_n = f(x_n)$. Поскольку пространство X компактно, последовательность $\{x_n\}$ содержит такую сходящуюся подпоследовательность $\{x_{n_k}\}$, что $\lim\limits_{k\to\infty} x_{n_k} = x \in X$. Так как $\lim\limits_{k\to\infty} y_{n_k} = y$ и отображение f непрерывно (как и любая изометрия), получаем, что $f(x) = y$, что противоречит предположению. Итак, требуемый открытый шар $B(y, r)$ существует.

Теперь достаточно доказать, что любая изометрия компактного метрического пространства «попадает» в любой открытый шар. Чтобы сде-

лать это более ясным, введем понятие *емкости*. Зафиксируем некоторое действительное число $r > 0$ и рассмотрим всевозможные покрытия пространства X шарами радиуса r. Каждое такое покрытие содержит конечное подпокрытие. Назовём *минимальное* количество шаров радиуса r, покрывающих пространство X, *емкостью* и обозначим ее через $h(X, r)$. Образ $f(X)$ компактного пространства X компактен ([9], теорема 4.14). Сейчас мы докажем, что емкость не меняется при изометриях.

Лемма 23.4. *Если $f: X \to X$ — изометрия компактного метрического пространства на себя и $r > 0$, то $h(X, r) = h(f(X), r)$.*

Доказательство леммы. Пусть $X \subset B_1 \cup B_2 \cup \ldots \cup B_N$ — покрытие пространства X, состоящее из N шаров радиуса r. Поскольку отображение f является изометрией, оно инъективно, и поэтому отображает X на $f(X)$ взаимно однозначно. Таким образом, f отображает каждый шар

$$B_i = B(x_i, r) = \{x \in X: d(x, x_i) < r\}$$

на шар, лежащий в пространстве $f(X)$ и имеющий вид

$$f(B_i) = \{x \in f(X): d(x, f(x_i)) < r\} = B(f(x_i), r).$$

Тогда

$$f(X) \subset f(B_1) \cup f(B_2) \cup \ldots \cup f(B_N)$$

и $h(f(X), r) \leqslant h(X, r)$. Но если применить то же самое рассуждение к отображению $f^{-1}: f(X) \to X$, то получим $h(X, r) \leqslant h(f(X), r)$, что и доказывает лемму. □

Вернемся к доказательству предложения 23.3. Напомним, что согласно нашему исходному предположению изометрия $f: X \to X$ не сюръективна; поэтому существует открытый шар $B(y, r)$, не пересекающийся с $f(X)$. Пусть $h = h(X, r/2)$ и

$$B_1 \cup B_2 \cup \ldots \cup B_h \supset X \tag{23.2}$$

— минимальное покрытие пространства X шарами радиуса $r/2$. Заметим, что если шар B_i содержит точку y, то $B_i \cap f(X) = \varnothing$. Это означает, что если мы из покрытия (23.2) выкинем шар B_i, то оставшиеся шары по-прежнему будут покрывать пространство $f(X)$. Таким образом, $h(f(X), r/2) < h(X, r/2)$, что противоречит лемме 23.4[1]. □

[1] Предложение 23.3 можно доказать, не используя понятие емкости. Рассмотрим последовательность точек y, $f(y)$, $f(f(y))$, $f(f(f(y)))$, ... Поскольку пространство X компактно, существуют такие два члена этой последовательности $f^m(y)$ и $f^n(y)$ $(m > n)$, что $d(f^m(y), f^n(y)) < r$. Но тогда $d(f^{m-n}(y), y) = d(f^m(y), f^n(y)) < r$, что противоречит тому, что $B(y, r) \cap f(X) = \varnothing$. — *Прим. перев.*

Теорема 23.5. *Любая изометрия пространства $\mathbb{Q}_p$ сюръективна.*

Доказательство. Пусть $f: \mathbb{Q}_p \to \mathbb{Q}_p$ — изометрия, не являющаяся сюръективной. Если $f(0) = a$, то $g(x) = f(x) - a$ — также несюръективная изометрия пространства $\mathbb{Q}_p$. Тогда существует точка $y \notin g(\mathbb{Q}_p)$. Пусть $|y|_p = r$. Поскольку отображение g является изометрией и $g(0) = 0$, оно отображает замкнутый шар $\overline{B} = \overline{B(0, 2r)}$ на себя и $y \notin g(\overline{B})$. Так как $\overline{B}$ — компактное метрическое пространство, полученный результат противоречит предложению 23.3. □

Упражнения

74. Пусть функция $f: \mathbb{Z}_p \to \mathbb{Z}_p$ определяется следующей формулой:

$$f\left(\sum_{n=0}^{\infty} a_n p^n\right) := \sum_{n=0}^{\infty} a_n p^{n^2}.$$

Докажите, что $f' = 0$, т. е. f — псевдоконстанта.

75*. Пусть функция $f: \mathbb{Z}_p \to \mathbb{Z}_p$ определяется следующей формулой:

$$f\left(\sum_{n=0}^{\infty} a_n p^n\right) := \sum_{n=0}^{\infty} a_n p^{n!}.$$

Докажите, что функция f инъективна, $f' = 0$ и f удовлетворяет условию Гёльдера порядка α для любого положительного числа α.

76. Пусть функция $f: \mathbb{Z}_p \to \mathbb{Z}_p$ определяется следующей формулой:

$$f\left(\sum_{n=0}^{\infty} a_n p^n\right) := \sum_{n=0}^{\infty} a_n^2 p^n.$$

Докажите, что функция f непрерывна.

§ 24. Интерполирование

Пусть $a_1, a_2, \ldots$ — последовательность элементов пространства $\mathbb{Q}_p$. Ее можно рассмотреть как функцию $f: \mathbb{N} \to \mathbb{Q}_p$, заданную формулой $f(n) = a_n$. Так как множество $\mathbb{N}$ плотно в $\mathbb{Z}_p$, из теоремы 20.5 следует, что существует не более одной такой непрерывной функции $F: \mathbb{Z}_p \to \mathbb{Q}_p$, что $F(n) = f(n)$ для всех $n \in \mathbb{N}$. Если такая функция F существует, то будем говорить, что последовательность $\{a_n\}$ *может быть интерполирована*. Конечно, аналогичное определение можно дать для двусторонних последовательностей, и для последовательностей вида $a_0, a_1, \ldots$

Если функция $f(n) = a_n$ равномерно непрерывна на $\mathbb{N}$, то из теоремы 20.5 непосредственно следует, что последовательность $\{a_n\}$ может быть

интерполирована. Обратно, предположим, что $f(n) = a_n$ может быть интерполирована непрерывной функцией $F: \mathbb{Z}_p \to \mathbb{Q}_p$. Тогда по теореме 20.4 функция F равномерно непрерывна на $\mathbb{Z}_p$, а значит, и на $\mathbb{N}$. Таким образом, последовательность $a_1, a_2, \ldots$ элементов пространства $\mathbb{Q}_p$ может быть интерполирована тогда и только тогда, когда для любого $\varepsilon > 0$ найдется такое N, что

$$\text{если } |n - m|_p \leqslant p^{-N}, \text{ то } |a_n - a_m|_p < \varepsilon. \tag{24.1}$$

Оказывается, не обязательно рассматривать все положительные числа n, m, для которых $|n - m|_p \leqslant p^{-N}$. Достаточно проверить условие (24.1) только для таких чисел n, m, которые отличаются на достаточно большую степень числа p. Более точно, имеет место следующее утверждение.

Предложение 24.1. *Пусть $a_1, a_2, \ldots$ — последовательность элементов пространства $\mathbb{Q}_p$. Она может быть интерполирована тогда и только тогда, когда для любого $\varepsilon > 0$ существует такое N, что*

$$\textit{если } n = m + p^N, \textit{ то } |a_n - a_m|_p < \varepsilon. \tag{24.2}$$

Доказательство. Если функция $f(n) = a_n$ равномерно непрерывна, то для любого $\varepsilon > 0$ существует такое N, что выполняется условие (24.1). В частности, это верно для $n = m + p^N$, так как в этом случае $|n - m|_p \leqslant p^{-N}$. Покажем, что из более слабого, на первый взгляд, условия (24.2) следует равномерная непрерывность. Для данного $\varepsilon > 0$ найдем N, для которого выполняется условие (24.2). Возьмем $n, m \in \mathbb{N}$, удовлетворяющие неравенству $|n - m|_p \leqslant p^{-N}$. Тогда $n - m$ делится на p^N, поэтому $n = m + bp^N$ для некоторого $b \in \mathbb{N}$. Мы имеем

$$a_n - a_m = \sum_{j=1}^{b} (a_{m+jp^N} - a_{m+(j-1)p^N}).$$

Из нашего условия (24.2) следует, что p-адическая норма каждого слагаемого меньше ε. Применяя сильное неравенство треугольника, получаем $|a_n - a_m|_p < \varepsilon$. □

В некотором смысле равномерная непрерывность последовательности $\{a_n\}$ противоположна свойству быть последовательностью Коши. Следующее простое утверждение дает нам множество примеров *не* равномерно непрерывных последовательностей, которые, следовательно, не могут быть интерполированы.

Предложение 24.2. *Пусть $\{a_n\}$ — непостоянная последовательность Коши, состоящая из p-адических чисел. Тогда она не может быть интерполирована.*

Доказательство. Предположим, что последовательность $\{a_n\}$ может быть интерполирована непрерывной функцией $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$, $f(n) = a_n$. Так как $\mathbb{N}$ плотно в $\mathbb{Z}_p$, для любого $x \in \mathbb{Z}_p \setminus \mathbb{N}$ существует последовательность натуральных чисел n_k, сходящаяся к x. Последовательность $\{a_n\}$ является последовательностью Коши и поэтому сходится к некоторому числу $c \in \mathbb{Q}_p$. Тогда и последовательность $\{a_{n_k}\}$ сходится к тому же самому пределу, и по непрерывности имеем $f(x) = \lim\limits_{k\to\infty} a_{n_k} = c$. Далее, так как множество $\mathbb{Z}_p \setminus \mathbb{N}$ также плотно в $\mathbb{Z}_p$, для любого $n \in \mathbb{N}$ существует такая последовательность $x_k \in \mathbb{Z}_p \setminus \mathbb{N}$, что $n = \lim\limits_{k\to\infty} x_k$. Тогда $a_n = f(n) = \lim\limits_{k\to\infty} f(x_k) = c$, т. е. $\{a_n\}$ является постоянной последовательностью, и, таким оборазом, получили противоречие. □

Для полноты изложения докажем несколько свойств равномерно непрерывных функций (некоторыми из них мы уже пользовались в теореме 20.5).

Предложение 24.3. *Пусть $E \subset \mathbb{Z}_p$ и функции $f\colon E \to \mathbb{Q}_p$ и $g\colon E \to \mathbb{Q}_p$ равномерно непрерывны на E. Тогда функции $f + g$, $f - g$ и fg также равномерно непрерывны на E.*

Доказательство. Для любого натурального числа s существует такое натуральное число t, что из неравенства $|x - y|_p \leqslant p^{-t}$ следует, что

$$|f(x) - f(y)|_p \leqslant p^{-s} \quad \text{и} \quad |g(x) - g(y)|_p \leqslant p^{-s}.$$

По теореме 20.5 функции f и g ограничены на $\overline{E}$ и, следовательно, на $E \subset \overline{E}$, т. е. существует такое натуральное число u, что $|f(x)|_p \leqslant p^u$ и $|g(x)|_p \leqslant p^u$. Пусть x, $y \in E$, причем $|x - y|_p \leqslant p^{-t}$. Тогда

$$\big|(f(x) \pm g(x)) - (f(y) \pm g(y))\big|_p = |(f(x) - f(y)) \pm (g(x) - g(y))|_p \leqslant p^{-s},$$

$$\big|f(x)g(x) - f(y)g(y)\big|_p = \big|f(x)(g(x) - g(y)) + (f(x) - f(y))g(y)\big|_p \leqslant p^{-t+u}. \quad \square$$

Следствие 24.4. *Любой многочлен $P(x)$ с коэффициентами в $\mathbb{Q}_p$ равномерно непрерывен на любом подмножестве $E \subset \mathbb{Z}_p$.*

Доказательство. Это следует из того, что функции $f(x) = c$ и $f(x) = x$ равномерно непрерывны на любом подмножестве $E \subset \mathbb{Q}_p$. □

Следствие 24.5. *Пусть*

$$\binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!}$$

— биномиальный коэффициент, где $n \in \mathbb{N}$ и $x \in \mathbb{Z}_p$. Тогда функция $P_n(x) = \binom{x}{n}$ равномерно непрерывна на $\mathbb{Z}_p$ и $\left|\binom{x}{n}\right|_p \leqslant 1$, т.е. $\binom{x}{n} \in \mathbb{Z}_p$.

Доказательство. Поскольку $P_n(x) = \binom{x}{n}$ — многочлен с рациональными коэффициентами, он равномерно непрерывен на $\mathbb{Z}_p$ по след-

ствию 24.4. Пусть $x \in \mathbb{Z}_p$. Тогда существует такая последовательность $\{x_m\} \subset \mathbb{N}$, что $x = \lim\limits_{m\to\infty} x_m$. По непрерывности многочлена $P_n(x)$ имеем

$$\lim_{m\to\infty} \binom{x_m}{n} = \binom{x}{n}.$$

Поскольку каждое число $\binom{x_m}{n}$ является целым рациональным, имеет место неравенство $\left|\binom{x_m}{n}\right|_p \leqslant 1$. Поэтому $\left|\binom{x}{n}\right|_p = \lim\limits_{m\to\infty}\left|\binom{x_m}{n}\right|_p \leqslant 1$, т. е. $\binom{x}{n} \in \mathbb{Z}_p$. □

(Сравните это доказательство с доказательством леммы 14.4, где мы доказали лишь, что $\binom{x}{n} \in \mathbb{Z}_p$ для любого $x \in \mathbb{Z}_p$.)

Теперь рассмотрим p-адическую показательную функцию. Наша цель состоит в том, чтобы выяснить, для каких p-адических чисел $a \in \mathbb{Q}_p$ последовательность $1, a, a^2, a^3, \ldots$ может быть интерполирована. В результате интерполяции получится непрерывная «показательная» функция $f(x) = a^x$.

Теорема 24.6. *Последовательность* $1, a, a^2, a^3, \ldots$ *может быть интерполирована тогда и только тогда, когда* $a \in 1 + p\mathbb{Z}_p$.

Доказательство. Нам понадобится следующая оценка.

Лемма 24.7. *Пусть* $0 < \varepsilon < 1$. *Тогда из неравенства* $|y - 1|_p \leqslant \varepsilon$ *вытекает неравенство* $|y^p - 1|_p \leqslant \tau|y - 1|_p$, *где* $\tau = \max(\varepsilon, p^{-1}) < 1$.

Доказательство леммы. Положим $y = 1 + a$, тогда $|a|_p \leqslant \varepsilon$ и

$$y^p - 1 = \binom{p}{1}a + \binom{p}{2}a^2 + \ldots + \binom{p}{p}a^p =$$
$$= (y-1)\left(\binom{p}{1} + \binom{p}{2}a + \ldots + \binom{p}{p}a^{p-1}\right).$$

Мы имеем $\left|\binom{p}{j}a^{j-1}\right|_p \leqslant p^{-1}$ для $j = 1, \ldots, p-1$ и $|a^{p-1}|_p \leqslant \varepsilon^{p-1} \leqslant \varepsilon$. Следовательно, $|y^p - 1|_p \leqslant \tau|y - 1|_p$, где $\tau = \max(\varepsilon, p^{-1})$. □

Из теоремы 8.5 следует, что

1) $\lim\limits_{n\to\infty} a^{p^n} = 1$, тогда и только тогда, когда
2) $a \in 1 + p\mathbb{Z}_p$.

Чтобы завершить доказательство, воспользуемся предложением 24.1. Последовательность $1, a, a^2, \ldots$ может быть интерполирована тогда и только тогда, когда $|a^{j+p^n} - a^j|_p$ стремится к 0 равномерно по j. Заметим, что если $|a|_p < 1$, то последовательность $\{a^n\}$ стремится к 0 и, таким образом, по предложению 24.2 не может быть интерполирована. Поэтому можно считать, что $|a|_p = 1$. Тогда

$$|a^{j+p^n} - a^j|_p = |a|_p^j|a^{p^n} - 1|_p = |a^{p^n} - 1|_p,$$

а последнее выражение стремится к 0 равномерно по j тогда и только тогда, когда выполняется условие 1), а вместе с ним и 2). □

Функция

$$a^x = \lim_{n \to x} a^n \quad (x \in \mathbb{Z}_p,\ a \in 1 + p\mathbb{Z}_p)$$

обладает следующими свойствами, которые мы оставляем без доказательства: для всех $x, y \in \mathbb{Z}_p$ и любого $a \in 1 + p\mathbb{Z}_p$ верно, что

1) $a^x \in 1 + p\mathbb{Z}_p$,
2) $a^{x+y} = a^x a^y$,
3) $a^{-x} = (a^x)^{-1}$,
4) $\exp_p(px) = (\exp_p p)^x$,
5) $(a^x)'_{x=0} = \ln_p(a)$,
6) $a^x = \sum_{n=0}^{\infty} \binom{x}{n} (a-1)^n$.

Свойство 4) устанавливает соотношение между функцией a^x и p-адической экспонентой, определенной в § 15.2. По теореме 15.2 ряд, определяющий функцию $\exp_p(x)$, расходится в точке $x = 1$. Однако ряд для $\exp_p(px)$ при $p \geqslant 3$ и ряд для $\exp_p(4x)$ при $p = 2$ аналитичны в $\mathbb{Z}_p$. Следовательно, число, аналогичное e, не принадлежит $\mathbb{Q}_p$, но числа e^p при $p \geqslant 3$ и e^4 при $p = 2$ принадлежат $\mathbb{Q}_p$! Таким образом, число e лежит в алгебраическом расширении поля $\mathbb{Q}_p$ степени p, если $p \geqslant 3$, и степени 4, если $p = 2$.

Упражнения

77. Докажите, что для каждого $j \in \mathbb{N}$ p-адическая последовательность $1^j, 2^j, 3^j, \ldots$ может быть интерполирована.

78. Докажите, что для каждого $j \in \mathbb{N}$ p-адическая последовательность

$$\left[\frac{1}{p^j}\right], \left[\frac{2}{p^j}\right], \left[\frac{3}{p^j}\right], \ldots$$

может быть интерполирована.

79. Докажите, что p-адическая последовательность $n \mapsto (-1)^n$ может быть интерполирована тогда и только тогда, когда $p = 2$.

Список литературы

[1] Боревич З. И., Шафаревич И. Р. Теория чисел. М.: Наука, 1964.

[2] Gouvêa F. Q. p-adic Numbers: An Introduction. 2nd edition. Springer-Verlag: Berlin—Heidelberg—New York. Universitext. 2000.

[3] Herstein I. N. Topics in Algebra. 2nd edition. John Wiley & Sons: New York—Chichester—Brisbane—Toronto—Singapore, 1975.

[4] Кириллов А. А., Гвишиани А. Д. Теоремы и задачи функционального анализа. М.: Наука, 1979.

[5] Кириллов А. А. Что такое число? М.: Наука, 1993.

[6] Коблиц Н., p-адические числа p-адический анализ и дзета-функции. М.: Мир, 1982.

[7] Mahler K. p-adic Numbers and their Functions. Cambridge University Press, 1973.

[8] Robert A. M. A Course in p-adic Analysis. Springer-Verlag: Berlin—Heidelberg—New York, 2000.

[9] Рудин У. Основы математического анализа. М.: Мир, 1976.

[10] Schikoff W. H. Ultrametric Calculus, An Introduction to p-adic Analysis. Cambridge University Press, Cambridge Studies in Adv. Math. 4, 1984.

Светлана Борисовна Каток

p-адический анализ в сравнении с вещественным

Редактор: Васильева О. А.
Художник: Сопова У.

Лицензия ИД № 01335 от 24.03.2000 г. Подписано в печать 15.05.2004 г. Формат 60 × 90 1/16. Бумага офсетная № 1. Печать офсетная. Печ. л. 7. Тираж 1000 экз.
Заказ №193т
Издательство Московского центра непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. 241—72—85.

Отпечатано с готовых диапозитивов во ФГУП «Полиграфические ресурсы».

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга», Большой Власьевский пер., д. 11. Тел. 241—72—85. E-mail: biblio@mccme.ru