Введение в p-адический анализ

рочев и. п.

31 октября 2026 г.

Оглавление

Оглавление i

Как бы предисловие 1

1 Нормированные поля. Нормы на $\mathbb{Q}$ 2
- 1.1 Нормированное поле. Неархимедова норма . . . 2
- 1.2 Эквивалентные нормы. Теорема Островского . . . 6

2 Пополнение нормированного поля. Поле p-адических чисел 9
- 2.1 Пополнение нормированного поля . . . 9
- 2.2 Поле p-адических чисел . . . 11

3 Теорема о слабой аппроксимации 17

4 Последовательности и ряды 19

5 Лемма Гензеля 22

6 Компактность кольца целых чисел 27

7 Лемма Гаусса 30

8 Сведения из теории алгебраических чисел 32
- 8.1 Конечные и алгебраические расширения полей . . . 32
- 8.2 Конечные поля . . . 35
- 8.3 Норма в конечных расширениях . . . 36

9 Продолжение нормы на алгебраическое замыкание 37
- 9.1 Нормы на векторных пространствах . . . 37
- 9.2 Продолжение нормы на алгебраическое замыкание . . . 39

10 Полное алгебраически замкнутое расширение 43

11 Арифметика конечных расширений 45

A Программа осеннего семестра 53

Как бы предисловие

Цель курса — познакомиться с теорией аналитических функций p-адического аргумента (неархимедовым аналогом стандартного курса комплексного анализа).

В основном я планирую опираться на две книжки:

- N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*. Graduate Texts in Mathematics, **58**, 2nd ed., Springer-Verlag, New York, 1984.
- Y. Amice. *Les nombres p-adiques*. Presses Universitaires de France, Paris, 1975.

Теорема о слабой аппроксимации (гл. 3) и лемма Гензеля (гл. 5) списаны из книжки

- S. Lang. *Algebraic number theory*. Graduate Texts in Mathematics, **110**, 2nd ed., Springer-Verlag, New York, 1994.

Дополнительные сведения можно почерпнуть, например, в книжке

- З. И. Боревич, И. Р. Шафаревич. *Теория чисел*. Любое издание.

Возможно, имеет смысл добавить:

- описание группы корней из 1 (Amice, § 2.4);
- разложение Малера для $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$;
- интересные приложения p-адики для подогрева интереса (например, теорему Monsky про разрезание квадрата на равновеликие треугольники);
- ещё что-нибудь.

Глава 1

Нормированные поля. Нормы на $\mathbb{Q}$

1.1 Нормированное поле. Неархимедова норма

Пусть F — некоторое поле (впрочем, определение работает и для кольца; причём для целостного кольца существует единственное продолжение на поле частных).

Определение 1.1. *Норма* (*нормирование*, *абсолютное значение*) на F — это отображение $\|\cdot\| : F \to [0, +\infty)$ со свойствами:

1) $\|x\| = 0 \iff x = 0$;

2) $\|xy\| = \|x\| \cdot \|y\|$;

3) $\|x + y\| \leqslant \|x\| + \|y\|$ (неравенство треугольника).

Пара $(F, \|\cdot\|)$ (или просто F, если понятно, какая норма имеется в виду) называется *нормированным полем* (или *полем с нормой*).

Пример 1.2. Если $F \subseteq \mathbb{C}$, то можно взять $\|\cdot\| = |\cdot|$ (обычный модуль).

Пример 1.3. На любом поле можно ввести *тривиальную норму*

$$\|x\| = \begin{cases} 0, & x = 0, \\ 1, & x \neq 0. \end{cases}$$

Упражнение 1.4. Доказать, что если поле F конечно, то на нём не существует нетривиальной (т. е. не являющейся тривиальной) нормы.

Упражнение 1.5. Придумать пример бесконечного поля, на котором есть только тривиальная норма. (На самом деле все такие поля легко описываются, но доказательство не очень тривиально.)

Лемма 1.6. *Для любой нормы верно* $\|\pm 1\| = 1$ ($\implies \|-x\| = \|x\|$). □

Следствие 1.7. *Функция* $d(x, y) = \|x - y\|$ *является метрикой на* F. *Соответственно, можно говорить о топологии и пределах.*

Упражнение 1.8. Доказать стандартные арифметические свойства пределов (пределы суммы, разности, произведения, частного).

В дальнейшем нас в основном будут интересовать так называемые неархимедовы нормы.

Определение 1.9. Если норма удовлетворяет неравенству

$$\|x + y\| \leqslant \max\{\|x\|, \|y\|\}$$

(ультраметрическое неравенство), то она называется *неархимедовой*. Норма, не являющаяся неархимедовой, называется *архимедовой*. Соответствующее нормированное поле также будем называть (не)архимедовым.

Пример 1.10. Тривиальная норма на любом поле является неархимедовой.

Для нетривиального примера неархимедовой нормы понадобится одно понятие.

Фиксируем простое число p. Каждое ненулевое рациональное число r можно представить в виде

$$r = p^{\alpha}\frac{u}{v}, \qquad \alpha, u, v \in \mathbb{Z}, \quad p \nmid uv.$$

Определение 1.11. Число α называется *p-адическим показателем* числа r. Обозначение: $\nu_p(r) = \alpha$.

Замечание 1.12. Корректность определения следует из основной теоремы арифметики.

Также положим формально $\nu_p(0) = +\infty$.

Основные свойства p-адического показателя:

1) $\nu_p(x) \in \mathbb{Z} \cup \{+\infty\}$, причём $\nu_p(x) = +\infty \iff x = 0$;

2) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$;

3) $\nu_p(x + y) \geqslant \min\{\nu_p(x), \nu_p(y)\}$; причём

3′) если $\nu_p(x) < \nu_p(y)$, то $\nu_p(x + y) = \nu_p(x) = \min\{\nu_p(x), \nu_p(y)\}$.

Арифметика:

- $\nu_p(r) < 0 \iff$ знаменатель числа r делится на p;
- $\nu_p(r) \geqslant 0 \iff$ знаменатель числа r не делится на p;
- $r \in \mathbb{Z} \iff$ для всех p выполнено $\nu_p(r) \geqslant 0$.

Теперь можно привести содержательный пример неархимедовой нормы (основной для нас).

Пример 1.13. Пусть p — простое число. На $\mathbb{Q}$ можно ввести *p-адическую норму*

$$|x|_p = p^{-\nu_p(x)} = \begin{cases} 0, & x = 0, \\ p^{-\nu_p(x)}, & x \neq 0. \end{cases}$$

Из свойств p-адического показателя следует, что это неархимедова норма.

Замечание 1.14. Можно было бы взять $c^{\nu_p(x)}$ с произвольной постоянной $c \in (0,1)$. Выбор $c = p^{-1}$ обусловлен тем, что тогда для любого $x \in \mathbb{Q}^*$ справедлива *формула произведения*

$$|x| \prod_p |x|_p = 1,$$

где произведение берётся по всем простым числам.

Относительно этой нормы «маленькими» являются числа, у которых числитель делится на большую степень p, а «большие» числа — это те, у которых знаменатель делится на большую степень p.

Также бывает полезен критерий целочисленности: $r \in \mathbb{Z} \iff \forall p \quad |r|_p \leqslant 1$.

Пример 1.15 («функциональный» аналог примера 1.13)**.** Пусть $F = k(T)$, где k — некоторое поле, T — переменная. Фиксируем неприводимый многочлен $p(T) \in k[T]$. Тогда для $R(T) \in F^*$ можно положить $\|R\|_p = \mathrm{e}^{-\nu_p(R)\deg p}$. В частности, если $p(T) = T - a$, то $\nu_p(R) = \operatorname{ord}_{T=a} R(T)$ — порядок в точке a. По аналогии можно рассмотреть порядок в «бесконечно удалённой точке», которому соответствует норма

$$\|P/Q\|_\infty = \mathrm{e}^{\deg P - \deg Q}.$$

Можно проверить, что здесь тоже есть формула произведения

$$\|R\|_\infty \prod_p \|R\|_p = 1,$$

где произведение берётся по всем унитарным неприводимым многочленам $p(T)$.

Из свойства 3′ p-адического показателя следует, что если $|x|_p > |y|_p$, то

$$|x+y|_p = |x|_p = \max\{|x|_p, |y|_p\}.$$

На самом деле аналогичное утверждение справедливо для произвольной неархимедовой нормы.

Лемма 1.16. *Если норма неархимедова и $\|x\| > \|y\|$, то $\|x+y\| = \|x\|$.*

Доказательство. С одной стороны, $\|x+y\| \leqslant \|x\|$.

С другой стороны, $\|x\| = \|(x+y)-y\| \leqslant \max\{\|x+y\|, \|y\|\}$, то есть $\|x\| \leqslant \|x+y\|$ или $\|x\| \leqslant \|y\|$. Поскольку $\|x\| > \|y\|$, то $\|x\| \leqslant \|x+y\|$. □

Следствие 1.17. *Пусть норма неархимедова, $x_1, \ldots, x_n \in F$, причём $\|x_1\| > \|x_k\|$ при $k > 1$. Тогда $\|x_1 + \cdots + x_n\| = \|x_1\|$.* □

Упражнение 1.18. Пусть норма неархимедова, $\lim\limits_{n\to\infty} x_n = a$, причём $a \neq 0$. Доказать, что $\|x_n\| = \|a\|$ при всех достаточно больших n.

Рассмотрим несколько забавных «геометрических» свойств, следующих из ультраметрического неравенства. (То, что метрика порождена нормой, неважно, и аналогичные утверждения справедливы в любом ультраметрическом пространстве.)

Лемма 1.19. *Пусть норма неархимедова, $x, y, z \in F$. Тогда (по крайней мере) два из трёх чисел $\|x-y\|, \|y-z\|, \|z-x\|$ равны. Неформально: в поле F (точнее, в соответствующем метрическом пространстве) все треугольники равнобедренные.* □

Обозначение 1.20. Пусть $a \in F$, $R > 0$. *Открытый шар* с центром a и радиусом R:

$$B_R(a) = \{x \in F : \|x - a\| < R\}.$$

Замкнутый шар:

$$B_R[a] = \{x \in F : \|x - a\| \leqslant R\}.$$

Упражнение 1.21. Доказать, что в неархимедовом нормированном поле любой (открытый или замкнутый) шар (с положительным радиусом) является одновременно открытым и замкнутым множеством (в топологическом смысле).

Лемма 1.22. *Пусть норма неархимедова. Тогда если $b \in B_R(a)$, то $B_R(b) = B_R(a)$. Аналогично для замкнутых шаров. Неформально: любая точка шара является его центром.*

Доказательство. $b \in B_R(a) \iff \|b - a\| < R \iff a \in B_R(b)$, поэтому достаточно доказать, что $B_R(b) \subseteq B_R(a)$.

Если $x \in B_R(b)$, то

$$\|x - a\| = \|(x - b) + (b - a)\| \leqslant \max\{\|x - b\|, \|b - a\|\} < R,$$

то есть $x \in B_R(a)$. □

Следствие 1.23. *Пусть норма неархимедова. Тогда если какие-то два шара пересекаются, то один является подмножеством другого.* □

Докажем полезный критерий неархимедовости нормы.

Лемма 1.24. *Норма является неархимедовой тогда и только тогда, когда для всех $n \in \mathbb{N}$ выполнено $\|n\| \leqslant 1$.*

Доказательство. Допустим, что $\|n\| \leqslant 1$ при $n \in \mathbb{N}$. Пусть $x, y \in F$, $n \in \mathbb{N}$. Имеем

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

Извлекаем корень n-й степени и устремляем $n \to \infty$. □

Следствие 1.25. *Продолжение неархимедовой нормы (на «бóльшее» поле $K \supseteq F$) всегда неархимедово.* □

Упражнение 1.26. Пусть характеристика поля F положительна. Доказать, что любая норма на F является неархимедовой.

Упражнение 1.27. Пусть функция $f : F \to [0, +\infty)$ удовлетворяет свойствам:

1) $f(xy) = f(x)f(y)$;

2) $f(x + y) \leqslant 2\max\{f(x), f(y)\}$.

Доказать, что выполнено неравенство треугольника $f(x + y) \leqslant f(x) + f(y)$.

Простой пример применения

Утверждение 1.28. *Пусть* $P(z) = z^n + a_1 z^{n-1} + \cdots + a_n \in \mathbb{Z}[z]$, $\alpha \in \mathbb{Q}$, $P(\alpha) = 0$. *Тогда* $\alpha \in \mathbb{Z}$.

Доказательство. Ключевая идея: $\alpha \in \mathbb{Z} \iff \forall p \quad |\alpha|_p \leqslant 1$.

Арифметическая задача свелась к аналитической: если коэффициенты (унитарного) многочлена «небольшие», то и корни у него «небольшие».

Поскольку $P(\alpha) = 0$, то

$$\alpha^n = -\sum_{k=1}^{n} a_k \alpha^{n-k},$$

поэтому найдётся $k \in \{1, \dots, n\}$, такое что

$$|\alpha^n|_p \leqslant |a_k \alpha^{n-k}|_p,$$

откуда

$$|\alpha|_p \leqslant \sqrt[k]{|a_k|_p} \leqslant 1. \qquad \square$$

Утверждение можно усилить: $|\alpha|_p \leqslant 1 \iff |\alpha|_p < p$ (поскольку для $\alpha \in \mathbb{Q}^*$ имеем $|\alpha|_p = p^n$, где $n \in \mathbb{Z}$), поэтому достаточно, чтобы для всех простых p и всех $k \in \{1, \dots, n\}$ выполнялось

$$\sqrt[k]{|a_k|_p} < p \iff |a_k|_p < p^k \iff \nu_p(a_k) > -k,$$

то есть p может входить в знаменатель a_k в степени не больше $k - 1$. Скажем, вместо $a_2 \in \mathbb{Z}$ достаточно потребовать, чтобы знаменатель $a_2 \in \mathbb{Q}$ был бесквадратным.

В частности, достаточно, чтобы выполнялось $k! a_k \in \mathbb{Z}$ $(k = 1, \dots, n)$. Учитывая формулы Ньютона, отсюда сразу следует симпатичное утверждение: если $x_1, \dots, x_n \in \mathbb{Q}$, причём $x_1^k + \cdots + x_n^k \in \mathbb{Z}$ при всех $k = 1, \dots, n$, то все $x_i \in \mathbb{Z}$.

1.2 Эквивалентные нормы. Теорема Островского

Определение 1.29. Нормы $\|\cdot\|_1$ и $\|\cdot\|_2$ на поле F называются эквивалентными, если для любой последовательности $x_n \in F$ выполнено

$$\lim_{n\to\infty} \|x_n\|_1 = 0 \iff \lim_{n\to\infty} \|x_n\|_2 = 0.$$

Обозначение: $\|\cdot\|_1 \sim \|\cdot\|_2$.

Пример 1.30. Если $\|\cdot\|$ — норма на F, $\alpha \in (0, 1]$, то $\|\cdot\|^\alpha$ — эквивалентная норма. Нужно только проверить неравенство треугольника, которое сводится к неравенству

$$(x + y)^\alpha \leqslant x^\alpha + y^\alpha$$

при $x, y \geqslant 0$. Если $x = y = 0$, то очевидно; иначе:

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

Заметим, что для обычного модуля $|\cdot|$ на $F \subseteq \mathbb{C}$ нельзя взять $\alpha > 1$, поскольку должно выполняться $|1 + 1|^\alpha \leqslant |1|^\alpha + |1|^\alpha$.

Теорема 1.31. *Если $\|\cdot\|_1 \sim \|\cdot\|_2$, то найдётся $\alpha > 0$, такое что $\|\cdot\|_2 = \|\cdot\|_1^\alpha$.*

Доказательство. Если обе нормы тривиальны, то утверждение тривиально.

Допустим, что норма $\|\cdot\|_1$ нетривиальна. Тогда найдётся $a \in F$ с $\|a\|_1 > 1$.

Поскольку $\|a^{-n}\|_1 \to 0$, то $\|a^{-n}\|_2 \to 0$. Следовательно, $\|a\|_2 > 1$, поэтому $\|a\|_2 = \|a\|_1^\alpha$ для некоторого $\alpha > 0$.

Докажем, что для всех $x \in F^*$ выполнено $\|x\|_2 = \|x\|_1^\alpha$.

Допустим обратное. Тогда найдётся $b \in F^*$, такое что $\|b\|_2 < \|b\|_1^\alpha$, т. е. $\|b\|_2 = \theta\|b\|_1^\alpha$, где $\theta \in (0,1)$. Для $n \in \mathbb{N}$ найдём $m_n \in \mathbb{Z}$, такое что $\|a\|_1^{m_n} \leqslant \|b\|_1^n < \|a\|_1^{m_n+1}$. Тогда для всех $n \in \mathbb{N}$ выполнено $1 \leqslant \|b^n a^{-m_n}\|_1 < \|a\|_1$, однако $\|b^n a^{-m_n}\|_2 = \theta^n \|b^n a^{-m_n}\|_1^\alpha \to 0$. Противоречие с эквивалентностью. □

Упражнение 1.32. Пусть $\|\cdot\|_1$ и $\|\cdot\|_2$ — нормы на F. Доказать эквивалентность условий:

1) $\|\cdot\|_1 \sim \|\cdot\|_2$;
2) $\|\cdot\|_1$ и $\|\cdot\|_2$ порождают одну и ту же топологию на F (это стандартное определение эквивалентности норм);
3) $\{x \in F : \|x\|_1 < 1\} = \{x \in F : \|x\|_2 < 1\}$;
4) $\{x \in F : \|x\|_1 \leqslant 1\} = \{x \in F : \|x\|_2 \leqslant 1\}$;
5) множества последовательностей Коши для $\|\cdot\|_1$ и $\|\cdot\|_2$ совпадают.

Лемма 1.33. *Пусть для некоторых $n_0 \in \mathbb{N}$, $n_0 > 1$, и $\alpha \geqslant 0$ выполнено $\|n_0\| \leqslant n_0^\alpha$. Тогда для всех $n \in \mathbb{N}$ верно $\|n\| \leqslant n^\alpha$.*

Доказательство. Пусть $n = a_k n_0^k + a_{k-1} n_0^{k-1} + \dots + a_0$, $a_i \in \{0, 1, \dots, n_0 - 1\}$, $a_k > 0$. Тогда

$$\|n\| \leqslant C_1 \sum_{i=0}^{k} \|n_0\|^i \leqslant C_1 \sum_{i=0}^{k} n_0^{\alpha i} \leqslant C_1 (k+1) n_0^{k\alpha} \leqslant C_1 n^\alpha \left(\frac{\ln n}{\ln n_0} + 1 \right),$$

где $C_1 = \max\{\|1\|, \dots, \|n_0 - 1\|\}$.

Применим доказанное к n^N (где n фиксировано, N — растущий параметр):

$$\|n\|^N \leqslant C_2 N n^{\alpha N}, \quad C_2 = C_2(n).$$

Извлекая корень N-й степени и устремляя $N \to \infty$, получаем требуемое. □

Следствие 1.34 (уточнение леммы 1.24)**.** *Если существует целое $n > 1$, такое что $\|n\| \leqslant 1$, то норма неархимедова.* □

Теорема 1.35 (Островский, 1916)**.** *Любая нетривиальная норма на $\mathbb{Q}$ эквивалентна либо $|\cdot|$, либо $|\cdot|_p$ для некоторого простого p.*

Замечание 1.36. На самом деле в архимедовом случае верно гораздо больше: любое поле с архимедовой нормой изометрически изоморфно некоторому подполю $\mathbb{C}$ с нормой, эквивалентной обычному модулю.

Доказательство теоремы Островского. Два случая:

1) Норма неархимедова. В этом случае найдётся простое p с $\|p\| < 1$ (иначе норма тривиальна).

   Если бы было два таких простых $p \neq q$, то мы бы имели: $1 = \text{н.о.д.}(p, q) = ap + bq$, откуда $1 \leqslant \max\{\|p\|, \|q\|\} < 1$ — противоречие. Значит, для всех простых $q \neq p$ выполнено $\|q\| = 1$, а тогда $\|\cdot\| = \|p\|^{\nu_p(\cdot)} \sim |\cdot|_p$.

2) Норма архимедова. Тогда найдётся $n_0 \in \mathbb{N}$: $\|n_0\| > 1$. Можно записать $\|n_0\| = n_0^\alpha$ для некоторого $\alpha > 0$.

   Из леммы 1.33 легко вывести, что $\|\cdot\| = |\cdot|^\alpha$ (лемму можно переформулировать следующим образом: функция

   $$f(n) = \max\left\{\frac{\ln\|n\|}{\ln n}, 0\right\}$$

   на $\mathbb{N} \setminus \{1\}$ в каждой точке принимает наибольшее значение). □

Глава 2

Пополнение нормированного поля. Поле p-адических чисел

2.1 Пополнение нормированного поля

Определение 2.1. *Пополнением* нормированного поля $(F_0, \|\cdot\|_0)$ будем называть нормированное поле $(F, \|\cdot\|)$ со следующими свойствами:

1) существует вложение $\iota : F_0 \hookrightarrow F$, сохраняющее норму, т. е. $\|\iota(x)\| = \|x\|_0$;
2) F полно как метрическое пространство, т. е. всякая последовательность Коши сходится;
3) $\iota(F_0)$ плотно в F, т. е. для произвольных $x \in F$ и $\varepsilon > 0$ найдётся $x_0 \in F_0$, такое что $\|x - \iota(x_0)\| < \varepsilon$.

Пример 2.2. $(\mathbb{R}, |\cdot|)$ — пополнение $(\mathbb{Q}, |\cdot|)$.

Теорема 2.3. *Для любого нормированного поля $(F_0, \|\cdot\|_0)$ существует пополнение.*

Набросок доказательства. Пусть A — множество всех последовательностей Коши $(x_n)_{n=1}^{\infty}$ в $(F_0, \|\cdot\|_0)$. На нём естественным образом определены операции сложения и умножения, а также можно ввести «норму» (полунорму) $\|(x_n)\| = \lim\limits_{n\to\infty} \|x_n\|_0$. Существование последнего предела следует из неравенства треугольника

$$\big|\|x_n\|_0 - \|x_m\|_0\big| \leqslant \|x_n - x_m\|_0$$

и фундаментальности последовательности (x_n). Легко видеть, что эта «норма» удовлетворяет свойствам

$$\|(x_n) \cdot (y_n)\| = \|(x_n)\| \cdot \|(y_n)\|,$$
$$\|(x_n) + (y_n)\| \leqslant \|(x_n)\| + \|(y_n)\|.$$

Далее, введём на A отношение эквивалентности:

$$(x_n) \sim (y_n) \iff \lim_{n\to\infty} \|x_n - y_n\|_0 = 0.$$

Легко проверить, что отношение $\sim$ уважает арифметические операции и «норму»:

1) если $(x_n) \sim (u_n)$ и $(y_n) \sim (v_n)$, то $(x_n + y_n) \sim (u_n + v_n)$ и $(x_n y_n) \sim (u_n v_n)$;

2) если $(x_n) \sim (y_n)$, то $\|(x_n)\| = \|(y_n)\|$.

В качестве искомого поля F возьмём множество $A/\sim$ всех классов эквивалентности $[(x_n)]$. При этом свойства отношения $\sim$ позволяют естественным образом индуцировать арифметические операции и «норму» с A на F: $[(x_n)] + [(y_n)] = [(x_n + y_n)]$, $[(x_n)] \cdot [(y_n)] = [(x_n y_n)]$, $\|[(x_n)]\| = \|(x_n)\|$.

Проверим, что $(F, \|\cdot\|)$ — нормированное поле. Нетривиально только существование обратного по умножению элемента.

Если $[(x_n)] \neq 0$, то $\lim\|x_n\|_0 > 0$. Следовательно, при $n \geqslant n_0$ выполнено $\|x_n\|_0 \geqslant \delta > 0$, и в качестве $[(x_n)]^{-1}$ можно взять $[(y_n)]$, где

$$y_n = \begin{cases} 1, & n < n_0, \\ 1/x_n, & n \geqslant n_0. \end{cases}$$

(Легко проверить, что эта последовательность фундаментальна.)

Замечание. С алгебраической точки зрения поле F — это факторкольцо кольца A по (максимальному) идеалу сходящихся к 0 последовательностей.

Проверим теперь, что получилось действительно пополнение. В качестве вложения возьмём $\iota(x) = [(x, x, x, \ldots)]$. При этом плотность $\iota(F_0)$ в F проверить легко: если $X = [(x_n)] \in F$, то $\iota(x_n) \to X$ в $(F, \|\cdot\|)$.

Осталось проверить полноту.

Для начала заметим, что всякая последовательность Коши вида $\iota(x_n)$, $x_n \in F_0$, имеет предел $[(x_1, x_2, \ldots)] \in F$.

Пусть теперь $X_n \in F$ — произвольная последовательность Коши. Для каждого n найдём $x_n \in F_0$, такое что $\|X_n - \iota(x_n)\| < \frac{1}{n}$. Последовательность $\iota(x_n)$ фундаментальна, поэтому имеет предел $X \in F$. Легко видеть, что $\lim X_n = X$. □

Упражнение 2.4. Доказать, что любые два пополнения изометрически изоморфны (т. е. существует изоморфизм, сохраняющий норму).

Будем дальше считать, что $F_0 \subseteq F$, отождествляя F_0 с $\iota(F_0)$.

В неархимедовом случае, который представляет для нас особый интерес, можно сказать кое-что дополнительное.

Лемма 2.5. *Пусть $(F, \|\cdot\|)$ — пополнение неархимедова поля $(F_0, \|\cdot\|_0)$. Тогда:*

1) *$(F, \|\cdot\|)$ неархимедово;*

2) *множество значений $\|\cdot\|$ совпадает с множеством значений $\|\cdot\|_0$.*

Доказательство. Первое утверждение следует из критерия неархимедовости.

Пусть $x \in F^*$. Найдём $x_0 \in F_0$, такое что $\|x - x_0\| < \|x\|$. Тогда

$$\|x\| = \|x - (x - x_0)\| = \|x_0\| = \|x_0\|_0.$$ □

2.2 Поле p-адических чисел

Фиксируем простое число p.

Определение 2.6. Пополнение поля $\mathbb{Q}$ относительно p-адической нормы $|\cdot|_p$ называется *полем p-адических чисел*. Обозначение: $(\mathbb{Q}_p, |\cdot|_p)$ (т. е. продолжение p-адической нормы на $\mathbb{Q}_p$ также обозначается через $|\cdot|_p$).

Продолжим на $\mathbb{Q}_p$ показатель $\nu_p(\cdot)$ с помощью равенства $|\alpha|_p = p^{-\nu_p(\alpha)}$. При этом по-прежнему $\nu_p(\alpha) \in \mathbb{Z}$ при $\alpha \neq 0$.

В этом параграфе мы получим альтернативное описание p-адических чисел, с которым удобнее работать, чем с классами эквивалентности последовательностей Коши.

Определение 2.7. p-адическое число α называется *целым*, если $|\alpha|_p \leqslant 1$, причём если $|\alpha|_p = 1$, то α называется *p-адической единицей*. Обозначения: $\mathbb{Z}_p$ — множество (всех) целых p-адических чисел, $\mathbb{Z}_p^\times$ — множество (всех) p-адических единиц.

Лемма 2.8. *$\mathbb{Z}_p$ — подкольцо поля $\mathbb{Q}_p$ с 1, а $\mathbb{Z}_p^\times$ — мультипликативная группа кольца $\mathbb{Z}_p$, причём $\mathbb{Z}_p$ и $\mathbb{Z}_p^\times$ замкнуты (в топологическом смысле). ($\Longrightarrow$ $\mathbb{Z}_p$ и $\mathbb{Z}_p^\times$ полны как метрические пространства.)* □

Для $\alpha, \beta \in \mathbb{Q}_p$ и $n \in \mathbb{Z}$ будем писать $\alpha \equiv \beta \pmod{p^n}$, если $\nu_p(\alpha - \beta) \geqslant n$. Эквивалентно: $|\alpha - \beta|_p \leqslant p^{-n}$, $\frac{\alpha-\beta}{p^n} \in \mathbb{Z}_p$. Легко видеть, что для $\alpha, \beta \in \mathbb{Z}$ и $n \geqslant 0$ это совпадает с обычной сравнимостью целых чисел по модулю p^n.

Сначала разберёмся с кольцом целых p-адических чисел $\mathbb{Z}_p$.

Лемма 2.9. *Для любого $\alpha \in \mathbb{Z}_p$ найдётся (единственное) $a \in \{0, 1, \dots, p-1\}$, такое что $\alpha \equiv a \pmod{p}$.*

Доказательство. Поскольку $\mathbb{Q}$ плотно в $\mathbb{Q}_p$, найдётся $u/v \in \mathbb{Q}$, такое что $|\alpha - u/v|_p \leqslant p^{-1}$, или $\alpha \equiv u/v \pmod{p}$. При этом $|u/v|_p \leqslant 1$, т. е. $(v, p) = 1$ (считаем, что дробь несократима), поэтому найдётся $a \in \{0, 1, \dots, p-1\}$, удовлетворяющее сравнению $va \equiv u \pmod{p}$. Тогда $\alpha \equiv u/v \equiv a \pmod{p}$. Единственность очевидна. □

Теорема 2.10. *Любое целое p-адическое число α можно единственным образом представить как сумму ряда вида*

$$\alpha = \sum_{n=0}^{\infty} a_n p^n, \quad a_n \in \{0, 1, \dots, p-1\}.$$

И обратно: каждый такой ряд сходится к некоторому целому p-адическому числу. При этом $\alpha \in \mathbb{Z}_p^\times \iff a_0 \neq 0$.

Доказательство. Будем строить последовательность a_n последовательно.

Положим $\alpha_0 = \alpha$. По лемме 2.9, найдётся $a_0 \equiv \alpha_0 \pmod{p}$.

Рассмотрим $\alpha_1 = \frac{\alpha_0 - a_0}{p} \in \mathbb{Z}_p$. Можно найти $a_1 \equiv \alpha_1 \pmod{p}$. Тогда

$$\alpha_2 = \frac{\alpha_1 - a_1}{p} = \frac{\alpha - a_0 - a_1 p}{p^2} \in \mathbb{Z}_p.$$

И так далее.

Пусть уже построены $a_0, a_1, \dots, a_{n-1}$, такие что

$$\alpha \equiv a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \pmod{p^n},$$

или

$$\alpha_n := \frac{\alpha - (a_0 + a_1 p + \cdots + a_{n-1} p^{n-1})}{p^n} \in \mathbb{Z}_p.$$

Найдём $a_n \equiv \alpha_n \pmod{p}$. Тогда

$$\alpha_{n+1} = \frac{\alpha_n - a_n}{p} = \frac{\alpha - (a_0 + a_1 p + \cdots + a_n p^n)}{p^{n+1}} \in \mathbb{Z}_p,$$

или

$$\alpha \equiv a_0 + a_1 p + \cdots + a_n p^n \pmod{p^{n+1}}.$$

В итоге получаем $\alpha = \sum_{n=0}^{\infty} a_n p^n$.
Сходимость произвольного такого ряда следует из полноты $\mathbb{Z}_p$: при $M \geqslant N$ имеем

$$\left| \sum_{n=N}^{M} a_n p^n \right|_p \leqslant p^{-N} \xrightarrow[N\to\infty]{} 0.$$

Единственность: если $a_n = a'_n$ при $n < n_0$ и $a_{n_0} \neq a'_{n_0}$, то при $N \geqslant n_0$ имеем

$$\left| \sum_{n=0}^{N} a_n p^n - \sum_{n=0}^{N} a'_n p^n \right|_p = \left| \sum_{n=n_0}^{N} (a_n - a'_n) p^n \right|_p = p^{-n_0} \not\to 0.$$

Беря $a'_n = 0$ и переходя к пределу при $N \to \infty$, получаем

$$\left| \sum_{n=n_0}^{\infty} a_n p^n \right|_p = p^{-n_0}, \quad a_{n_0} \neq 0.$$

В частности, $\alpha \in \mathbb{Z}_p^\times \iff a_0 \neq 0$. □

Следствие 2.11. *$\mathbb{N}_0$ плотно в $\mathbb{Z}_p$.* □

Следствие 2.12. *Множество $\mathbb{Z}_p$ имеет мощность континуум (следовательно, $\mathbb{Q}_p \neq \mathbb{Q}$, так что $\mathbb{Q}$ не полно относительно p-адической нормы).* □

Замечание 2.13. «Цифры» a_n можно брать из произвольного множества $S \subseteq \mathbb{Z}_p$, обладающего свойством: для любого $\alpha \in \mathbb{Z}_p$ найдётся единственное $a \in S$, такое что $\alpha \equiv a \pmod{p}$. С важным примером такого множества (представители Тейхмюллера) мы встретимся позже (см. пример 4.2). Более того, для каждой цифры a_n можно брать своё множество S_n.

Замечание 2.14. $\mathbb{Z}_p$ — факториальное кольцо с единственным простым (неприводимым) элементом p (с точностью до ассоциированности). При этом делимость устроена очень просто: $\beta \mid \alpha \iff \nu_p(\beta) \leqslant \nu_p(\alpha) \iff |\beta|_p \geqslant |\alpha|_p$.

Упражнение 2.15. Доказать, что всякое $\alpha \in \mathbb{Z}_p$ можно единственным образом представить в виде

$$\alpha = \sum_{n=0}^{\infty} a_n (-p)^n, \quad a_n \in \{0, 1, \dots, p-1\}.$$

При этом ряд конечен (т. е. $a_n = 0$ при $n \geqslant n_0$) тогда и только тогда, когда $\alpha \in \mathbb{Z}$.

Если $\alpha \in \mathbb{Q}_p^*$, то $\alpha = p^{v_p(\alpha)}\varepsilon$, где $\varepsilon \in \mathbb{Z}_p^\times$, так что для $\mathbb{Q}_p$ получаем аналогичное описание.

Теорема 2.16. *Любое $\alpha \in \mathbb{Q}_p^*$ можно единственным образом представить в виде*

$$\alpha = \sum_{n \geqslant n_0}^{\infty} a_n p^n, \quad n_0 \in \mathbb{Z},\ a_n \in \{0, 1, \dots, p-1\},\ a_{n_0} \neq 0. \tag{2.1}$$

И обратно: каждый такой ряд сходится к некоторому ненулевому p-адическому числу. При этом $v_p(\alpha) = n_0$. □

Представление (2.1) называется стандартным представлением p-адического числа α, а числа a_n — его стандартными p-адическими цифрами. Это аналог бесконечной десятичной дроби для вещественных чисел, поэтому по аналогии иногда используют запись $\alpha = \dots a_2 a_1 a_0 . a_{-1} \dots a_{n_0}$.

Рассмотрим несколько примеров на арифметические операции с такими рядами (достаточно ограничиться целыми p-адическими числами):

$$\begin{aligned}
&(1 + 0\cdot 5 + 3\cdot 5^2 + \cdots) - (2 + 4\cdot 5 + 1\cdot 5^2 + \cdots) = \\
&\qquad = (-1) + (-4)\cdot 5 + 2\cdot 5^2 + \cdots = 4 + (-5)\cdot 5 + 2\cdot 5^2 + \cdots = \\
&\qquad\qquad = 4 + 0\cdot 5 + 1\cdot 5^2 + \cdots, \\
&(2 + 3\cdot 5 + 1\cdot 5^2 + \cdots)\cdot(3 + 4\cdot 5 + 0\cdot 5^2 + \cdots) = \\
&\qquad = 6 + 17\cdot 5 + 15\cdot 5^2 + \cdots = 1 + 18\cdot 5 + 15\cdot 5^2 + \cdots = \\
&\qquad\qquad = 1 + 3\cdot 5 + 18\cdot 5^2 + \cdots = 1 + 3\cdot 5 + 3\cdot 5^2 + \cdots, \\
&\frac{1}{1 + 2\cdot 5 + 3\cdot 5^2 + \cdots} = 1 - (2\cdot 5 + 3\cdot 5^2 + \cdots) + (2\cdot 5 + 3\cdot 5^2 + \cdots)^2 - \cdots = \\
&\qquad\qquad = 1 + (-2)\cdot 5 + 1\cdot 5^2 + \cdots = 1 + 3\cdot 5 + 0\cdot 5^2 + \cdots, \\
&\frac{1}{2 + 1\cdot 5 + 4\cdot 5^2 + \cdots} = \frac{3}{3\cdot(2 + 1\cdot 5 + 4\cdot 5^2 + \cdots)} = \frac{3}{1 + 4\cdot 5 + 2\cdot 5^2 + \cdots} = \cdots = \\
&\qquad\qquad = 3 + 3\cdot 5 + 4\cdot 5^2 + \cdots.
\end{aligned}$$

(Также можно делить «уголком».)

Теорема 2.17. *Стандартное представление p-адического числа α является периодическим (т. е. последовательность цифр периодична) тогда и только тогда, когда $\alpha \in \mathbb{Q}$.*

Без ограничения общности можно считать, что $\alpha \in \mathbb{Z}_p$. Сначала разберёмся с чисто периодическим случаем.

Теорема 2.18. *Стандартное представление $\alpha \in \mathbb{Z}_p$ является чисто периодическим тогда и только тогда, когда $\alpha = -u/v$, где $u \in \mathbb{Z}$, $v \in \mathbb{N}$, $0 \leqslant u \leqslant v$, $p \nmid v$ (т. е. одновременно $\alpha \in [-1, 0] \cap \mathbb{Q}$ и $\alpha \in \mathbb{Z}_p$). При этом длина (наименьшего) периода — это показатель числа p по модулю знаменателя v, т. е. наименьшее $T \in \mathbb{N}$, такое что $p^T \equiv 1 \pmod{v}$ (в предположении, что дробь несократима, т. е. $(u, v) = 1$).*

Доказательство. Допустим, что последовательность цифр a_n чисто периодическая, т. е. для некоторого $T \in \mathbb{N}$ имеем $a_{n+T} = a_n$ при всех $n \geqslant 0$. Тогда

$$\sum_{n=0}^{\infty} a_n p^n = \sum_{n=0}^{T-1} a_n p^n \cdot (1 + p^T + p^{2T} + \cdots) = -\frac{\sum_{n=0}^{T-1} a_n p^n}{p^T - 1}.$$

При этом $0 \leqslant \sum_{n=0}^{T-1} a_n p^n \leqslant p^T - 1$. Если привести дробь к несократимому виду $-u/v$, то получим $v \mid p^T - 1$.

Обратно, пусть $\alpha = -u/v$, где $0 \leqslant u \leqslant v$, $p \nmid v$. Если $p^T \equiv 1 \pmod{v}$, то α можно записать в виде

$$\alpha = -\frac{A}{p^T - 1}, \quad 0 \leqslant A \leqslant p^T - 1.$$

Записав $A = \sum_{n=0}^{T-1} a_n p^n$ (представление в p-ичной системе счисления), можно повторить предыдущие выкладки в обратную сторону. □

Пример 2.19. $-1 = (p-1) + (p-1) \cdot p + (p-1) \cdot p^2 + \cdots = \sum_{n=0}^{\infty} (p-1)p^n$.

Из теоремы 2.18 сразу следует, что периодичность влечёт рациональность.

В обратную сторону можно доказывать по-разному.

Первое доказательство. Если $\alpha \in \mathbb{Z}$, $\alpha \geqslant 0$, то утверждение очевидно ($a_n = 0$ при $n \geqslant n_0$).

Пусть $\alpha = -m$, $m \in \mathbb{N}$. Возьмём $N \in \mathbb{N}$, такое что $p^N \geqslant m$. Тогда

$$\alpha = (p^N - m) - p^N = \sum_{n=0}^{N-1} a_n p^n + \sum_{n=N}^{\infty} (p-1)p^n.$$

Пусть $\alpha \in \mathbb{Q} \cap \mathbb{Z}_p$, причём $\alpha \notin \mathbb{Z}$. Запишем $\alpha = m + \beta$, где $m \in \mathbb{Z}$, $\beta \in (-1, 0)$. Согласно теореме 2.18, имеем $\beta = \sum_{n=0}^{\infty} b_n p^n$, где $b_{n+T} = b_n$, $n \geqslant 0$, причём не все цифры равны 0 (так как $\beta \neq 0$) и не все цифры равны $p-1$ (так как $\beta \neq -1$). Прибавление m «испортит» лишь конечное число цифр. Действительно, если $p^N \geqslant |m|$, то

$$\sum_{n=0}^{N+T-1} b_n p^n + m \geqslant p^N + m \geqslant 0,$$

$$\sum_{n=0}^{N+T-1} b_n p^n + m \leqslant \sum_{n=0}^{N+T-1} (p-1)p^n - p^N + m \leqslant \sum_{n=0}^{N+T-1} (p-1)p^n.$$

Следовательно, при $n \geqslant N + T$ цифры не меняются. □

Замечание 2.20. Из первого доказательства и теоремы 2.18 следует, что длина периода для $\alpha = u/v \in \mathbb{Q} \cap \mathbb{Z}_p$, $(u, v) = 1$, равна показателю числа p по модулю знаменателя v.

Второе доказательство. Пусть $\alpha = u/v$, $p \nmid v$. Будем раскладывать α в ряд, как в доказательстве теоремы 2.10. При этом для всех $n \in \mathbb{N}_0$ выполнено $\alpha_n = u_n/v$, $u_n \in \mathbb{Z}$.

Действительно, это верно для $n = 0$. Если это справедливо для какого-то n, то имеем $u_n/v \equiv a_n \pmod{p}$, или $u_n \equiv v a_n \pmod{p}$, поэтому

$$\alpha_{n+1} = \frac{u_n/v - a_n}{p} = \frac{u_{n+1}}{v},$$

где

$$u_{n+1} = \frac{u_n - va_n}{p} \in \mathbb{Z}.$$

При этом

$$\alpha_n = \frac{\alpha - (a_0 + a_1 p + \cdots + a_{n-1}p^{n-1})}{p^n},$$

откуда

$$|\alpha_n| < |\alpha| + 1 = \text{const},$$

поэтому α_n может принимать лишь конечное число значений.

Следовательно, для некоторых $n_0 < n_1$ выполнено $\alpha_{n_0} = \alpha_{n_1}$, откуда получаем, что $a_{n+T} = a_n$ при $n \geqslant n_0$, где $T = n_1 - n_0$. □

Заметим, что оба доказательства конструктивны, причём для вычислений удобнее использовать второй подход. Разберём пример.

Пример 2.21. Рассмотрим $\frac{37}{126} \in \mathbb{Q}_3$. Поскольку $126 = 3^2 \cdot 14$, то сначала разберёмся с $\frac{37}{14} \in \mathbb{Z}_3$.

1) Первый способ:

$$\begin{aligned}
\frac{37}{14} &= 3 - \frac{5}{14} = 3 - \frac{260}{3^6 - 1} = 3 + \frac{2 + 2\cdot 3 + 1\cdot 3^2 + 0\cdot 3^3 + 0\cdot 3^4 + 1\cdot 3^5}{1 - 3^6} \\
&= 3 + (2 + 2\cdot 3 + 1\cdot 3^2 + 0\cdot 3^3 + 0\cdot 3^4 + 1\cdot 3^5)\sum_{k=0}^{\infty} 3^{6k} \\
&= 2 + 0\cdot 3 + 2\cdot 3^2 + (0 + 0\cdot 3 + 1\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 1\cdot 3^5)\sum_{k=0}^{\infty} 3^{6k+3} \\
&= \overline{122100}202.
\end{aligned}$$

2) Вычисляем цифры последовательно (фактически делим $37 = 1 + 0\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3$ на $14 = 2 + 1\cdot 3 + 1\cdot 3^2$ «уголком»):

$$\begin{aligned}
\alpha_0 &= \frac{37}{14} \equiv 2 \pmod 3 && \Longrightarrow && a_0 = 2, \\
\alpha_1 &= \frac{37/14 - 2}{3} = \frac{3}{14} \equiv 0 \pmod 3 && \Longrightarrow && a_1 = 0, \\
\alpha_2 &= \frac{3/14 - 0}{3} = \frac{1}{14} \equiv 2 \pmod 3 && \Longrightarrow && a_2 = 2, \\
\alpha_3 &= \frac{1/14 - 2}{3} = \frac{-9}{14} \equiv 0 \pmod 3 && \Longrightarrow && a_3 = 0, \\
\alpha_4 &= \frac{-9/14 - 0}{3} = \frac{-3}{14} \equiv 0 \pmod 3 && \Longrightarrow && a_4 = 0, \\
\alpha_5 &= \frac{-3/14 - 0}{3} = \frac{-1}{14} \equiv 1 \pmod 3 && \Longrightarrow && a_5 = 1,
\end{aligned}$$

$$\begin{aligned}
\alpha_6 &= \frac{-1/14-1}{3} = \frac{-5}{14} \equiv 2 \pmod 3 &&\Longrightarrow && a_6 = 2,\\
\alpha_7 &= \frac{-5/14-2}{3} = \frac{-11}{14} \equiv 2 \pmod 3 &&\Longrightarrow && a_7 = 2,\\
\alpha_8 &= \frac{-11/14-2}{3} = \frac{-13}{14} \equiv 1 \pmod 3 &&\Longrightarrow && a_8 = 1,\\
\alpha_9 &= \frac{-13/14-1}{3} = \frac{-9}{14} = \alpha_3 &&\Longrightarrow && a_n = a_{n-6},\ n \geqslant 9.
\end{aligned}$$

Заметим, что α_3 — это первое $\alpha_n \in (-1, 0)$, поэтому период начинается именно с a_3.

Окончательно имеем

$$\begin{aligned}
\frac{37}{126} &= 2\cdot 3^{-2} + 0\cdot 3^{-1} + 2 + (0 + 0\cdot 3 + 1\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 1\cdot 3^5)\sum_{k=0}^{\infty} 3^{6k+1}\\
&= \overline{1221002}.02.
\end{aligned}$$

Альтернативный подход (без подробностей)

Последовательность целых (рациональных) чисел $(b_n)_{n=1}^{\infty}$, для которой выполнено $b_{n+1} \equiv b_n \pmod{p^n}$, является последовательностью Коши в $\mathbb{Z}_p$, поэтому имеет предел $\lim b_n = \alpha \in \mathbb{Z}_p$. При этом две таких последовательности b_n и b'_n имеют один и тот же предел α тогда и только тогда, когда $b_n \equiv b'_n \equiv \alpha \pmod{p^n}$. Следовательно, если потребовать дополнительно $0 \leqslant b_n \leqslant p^n - 1$, то все пределы будут различны. Более того, для каждого $\alpha \in \mathbb{Z}_p$ легко найти такую последовательность b_n: если $\alpha = \sum_{i=0}^{\infty} a_i p^i$, то можно взять $b_n = \sum_{i=0}^{n-1} a_i p^i$. Фактически это значит, что $\mathbb{Z}_p$ можно задать как проективный предел:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

При этом получается целостное кольцо, поле частных которого есть $\mathbb{Q}_p$. (Подробнее про этот подход можно почитать, например, в Боревиче–Шафаревиче.)

Глава 3

Теорема о слабой аппроксимации

Неэквивалентные нормы порождают разные топологии. На самом деле ситуация гораздо интереснее.

Лемма 3.1. *Пусть $\|\cdot\|_1, \|\cdot\|_2$ — неэквивалентные нетривиальные нормы на F. Тогда найдётся $a \in F$, такое что $\|a\|_1 > 1 > \|a\|_2$.*

Доказательство. Заметим, что утверждение леммы симметрично относительно $\|\cdot\|_1$ и $\|\cdot\|_2$ (если $\|a\|_1 > 1 > \|a\|_2$, то $\|1/a\|_2 > 1 > \|1/a\|_1$).

Пусть для определённости найдётся последовательность $x_n \in F$, такая что $\|x_n\|_1 \not\to 0$ и $\|x_n\|_2 \to 0$. Переходя, если нужно, к подпоследовательности, будем считать, что для всех n выполнено $\|x_n\|_1 \geqslant \varepsilon > 0$. Поскольку норма $\|\cdot\|_1$ нетривиальна, то найдётся $b \in F$ с $\|b\|_1 > 1$. Тогда можно взять $a = b^m x_n$, где m выбрано так, что $\|b\|_1^m \varepsilon > 1$, а n достаточно велико. □

Лемма 3.2. *Пусть $\|\cdot\|_1, \dots, \|\cdot\|_n$ — попарно неэквивалентные нетривиальные нормы на F. Тогда найдётся $a \in F$, такое что $\|a\|_1 > 1$, $\|a\|_k < 1$ при $k = 2, \dots, n$.*

Доказательство. Доказываем индукцией по n. Случай $n = 2$ рассмотрен выше.

Пусть $n > 2$ и уже построено a_0, такое что $\|a_0\|_1 > 1$, $\|a_0\|_k < 1$ при $1 < k < n$. Если при этом $\|a_0\|_n < 1$, то всё замечательно. Допустим, что $\|a_0\|_n \geqslant 1$.

По лемме 3.1, найдётся $b \in F$, такое что $\|b\|_1 > 1 > \|b\|_n$.

Если $\|a_0\|_n = 1$, то можно взять $a = a_0^N b$ для достаточно большого N.

Если же $\|a_0\|_n > 1$, то сгодится $a = \frac{a_0^N}{1+a_0^N}\, b$. □

Теорема 3.3 (weak approximation theorem)**.** *Пусть $\|\cdot\|_1, \dots, \|\cdot\|_n$ — попарно неэквивалентные нетривиальные нормы на F, $x_1, \dots, x_n \in F$, $\varepsilon > 0$. Тогда найдётся $x \in F$, такое что $\|x - x_k\|_k < \varepsilon$ при $k = 1, \dots, n$.*

Доказательство. Сначала найдём $a_1, \dots, a_n \in F$, такие что $\|a_k\|_k > 1 > \|a_k\|_l$, $l \neq k$. Тогда можно взять

$$x = \frac{a_1^N}{1 + a_1^N}\, x_1 + \dots + \frac{a_n^N}{1 + a_n^N}\, x_n$$

при достаточно большом N. □

Пример 3.4. Если $F = \mathbb{Q}$, $\|\cdot\|_k$ — различные p-адические нормы, $x_k \in \mathbb{Z}$, то получаем слабый вариант китайской теоремы об остатках (нужное x будет рациональным, но не целым, вообще говоря). Для полноценной КТО нужна сильная аппроксимация, но это уже выходит за рамки спецкурса.

Упражнение 3.5. Пусть $a \in \mathbb{R}$ и для каждого простого p фиксировано $a_p \in \mathbb{Q}_p$. Доказать, что существует последовательность $x_n \in \mathbb{Q}$, такая что $\lim\limits_{n\to\infty} x_n = a$ в $\mathbb{R}$ и $\lim\limits_{n\to\infty} x_n = a_p$ в $\mathbb{Q}_p$ для всех p, т. е.

$$\lim_{n\to\infty} |x_n - a| = \lim_{n\to\infty} |x_n - a_p|_p = 0.$$

Глава 4

Последовательности и ряды в полных неархимедовых нормированных полях

В этой главе будем предполагать, что $(F, \|\cdot\|)$ — полное неархимедово нормированное поле (для лемм 4.3 и 4.7 полнота не нужна).

Лемма 4.1. *Пусть $a_n \in F$. Тогда:*

1) *последовательность a_n сходится тогда и только тогда, когда $\lim\limits_{n\to\infty} \|a_{n+1} - a_n\| = 0$ (без полноты поля F последнее условие равносильно фундаментальности);*
2) *ряд $\sum_{n=1}^{\infty} a_n$ сходится тогда и только тогда, когда $\lim\limits_{n\to\infty} \|a_n\| = 0$.* □

Пример 4.2. Пусть $\alpha \in \mathbb{Z}_p$. Рассмотрим последовательность $a_n = \alpha^{p^n}$, $n \geqslant 0$. При $n \geqslant 1$ имеем $a_n \equiv a_{n-1} \pmod{p^n}$. (Для $\alpha \in \mathbb{Z}$ это следует из теоремы Эйлера, а общий случай получается по непрерывности, поскольку $\mathbb{Z}$ плотно в $\mathbb{Z}_p$.) Следовательно, существует предел $\lim a_n =: \omega(\alpha) \in \mathbb{Z}_p$, который называется *представителем Тейхмюллера* для α (the *Teichmüller representative* of α). Несколько наблюдений:

1) $a_{n-1}^p = a_n \implies \big(\omega(\alpha)\big)^p = \omega(\alpha)$.
2) $a_n \equiv a_0 = \alpha \pmod{p} \implies \omega(\alpha) \equiv \alpha \pmod{p}$.
3) $\omega(0), \omega(1), \dots, \omega(p-1)$ попарно различны $\implies$ многочлен $x^p - x$ имеет p различных корней в $\mathbb{Q}_p$ (и даже в $\mathbb{Z}_p$).
4) $\omega(\alpha)$ — единственный корень многочлена $x^p - x$, такой что $\omega(\alpha) \equiv \alpha \pmod{p}$. (В частности, $\omega(\alpha) = \omega(\beta) \iff \alpha \equiv \beta \pmod{p}$.)
5) $\omega(\mathbb{Z}_p) = \{\omega(0), \omega(1), \dots, \omega(p-1)\}$ — полная система вычетов по модулю p в $\mathbb{Z}_p$.
6) Если $\alpha \in \mathbb{Z}_p^\times$, то $\big(\omega(\alpha)\big)^{p-1} = 1$.
7) $\omega\big(\omega(\alpha)\big) = \omega(\alpha)$.

8) $\omega(\alpha\beta) = \omega(\alpha)\,\omega(\beta)$.

9) $\omega(\alpha+\beta) \equiv \omega(\alpha) + \omega(\beta) \pmod{p}$.

Положим $\omega_0(\alpha) = \omega(\alpha)$, $\omega_n(\alpha) = \omega\left(\frac{\alpha-\omega_0(\alpha)-\omega_1(\alpha)p-\dots-\omega_{n-1}(\alpha)p^{n-1}}{p^n}\right)$ $(n \geqslant 1)$. Тогда

$$\alpha = \sum_{n=0}^{\infty} \omega_n(\alpha) p^n, \quad \omega_n(\alpha) \in \omega(\mathbb{Z}_p).$$

Это представление называется *разложением Тейхмюллера* (the *Teichmüller expansion*) для α, а $\omega_n(\alpha)$ — *цифрами Тейхмюллера* (the *Teichmüller digits*).

Поговорим немного о свойствах сходящихся рядов. В неархимедовом случае всё гораздо проще. Например, нет аналога теоремы Римана об условно сходящихся рядах.

Лемма 4.3. *Если ряд $\sum_{n=1}^{\infty} a_n$ сходится и его сумма равна S (дальше будем просто писать $\sum_{n=1}^{\infty} a_n = S$), то для любой биекции $\sigma\colon \mathbb{N} \to \mathbb{N}$ выполнено $\sum_{n=1}^{\infty} a_{\sigma(n)} = S$.*

Доказательство. Фиксируем $\varepsilon > 0$. Найдётся $N_1 \in \mathbb{N}$, такое что

$$\left\| \sum_{n=1}^{N_1} a_n - S \right\| \leqslant \varepsilon,$$
$$\|a_n\| \leqslant \varepsilon, \quad n \geqslant N_1.$$

Поскольку σ — биекция, найдётся $N_2 \in \mathbb{N}$, такое что $\{1, \dots, N_1\} \subseteq \{\sigma(1), \dots, \sigma(N_2)\}$. Пусть $N \geqslant N_2$. Тогда

$$\sum_{n=1}^{N} a_{\sigma(n)} - S = \left(\sum_{n=1}^{N_1} a_n - S \right) + \sum{}' a_n,$$

где в последней сумме все слагаемые имеют номер $n > N_1$. Следовательно,

$$\left\| \sum_{n=1}^{N} a_{\sigma(n)} - S \right\| \leqslant \varepsilon. \qquad \square$$

Таким образом, сходящийся ряд можно суммировать в произвольном порядке. Более того, его члены можно дополнительно группировать произвольным образом.

Лемма 4.4. *Пусть $\sum_{n=1}^{\infty} a_n = S$, $\mathbb{N} = \bigsqcup_{m=1}^{\infty} A_m$ (т. е. $\mathbb{N} = \bigcup_{m=1}^{\infty} A_m$, где $A_m \cap A_n = \varnothing$ при $m \neq n$). Тогда для каждого $m \in \mathbb{N}$ выражение $S_m = \sum_{n \in A_m} a_n$ определено (это конечная сумма либо сходящийся ряд), причём $\sum_{m=1}^{\infty} S_m = S$.* $\square$

Упражнение 4.5. Доказать лемму 4.4.

Важное следствие леммы 4.4 — возможность переставлять порядок суммирования в повторных рядах при условии сходимости соответствующих кратных рядов.

Будем писать $\sum_{m,n=1}^{\infty} a_{m,n} = S$, если для некоторой биекции $\sigma\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ выполнено $\sum_{k=1}^{\infty} a_{\sigma(k)} = S$ (согласно лемме 4.3, это не зависит от выбора σ).

Лемма 4.6. *Допустим, что $\sum_{m,n=1}^{\infty} a_{m,n} = S$. Тогда*

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} a_{m,n} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} a_{m,n} = S. \qquad \square$$

Как показывает пример

$$a_{m,n} = \begin{cases} 1, & n = m, \\ -1, & n = m+1, \\ 0 & \text{иначе}, \end{cases}$$

условие сходимости двойного ряда существенно. Просто заменить его требованием сходимости обоих повторных рядов нельзя.

Наконец, сходящиеся ряды можно перемножать ровно так же, как и абсолютно сходящиеся ряды в архимедовом случае.

Лемма 4.7. *Пусть* $\sum_{n=1}^{\infty} a_n = A$, $\sum_{n=1}^{\infty} b_n = B$. *Тогда* $\sum_{m,n=1}^{\infty} a_m b_n = AB$.

Доказательство. Пусть $k \mapsto \big(m(k), n(k)\big)$ — произвольная биекция $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

Найдётся постоянная $C \geqslant 1$, такая что $\max\{\|a_n\|, \|b_n\|\} \leqslant C$.

Фиксируем $\varepsilon > 0$. Найдётся $N_0 \in \mathbb{N}$, такое что

$$\left\| \sum_{m=1}^{N_0} a_m \cdot \sum_{n=1}^{N_0} b_n - A \cdot B \right\| \leqslant \varepsilon,$$
$$\max\{\|a_n\|, \|b_n\|\} \leqslant \varepsilon, \quad n \geqslant N_0.$$

Найдётся $K_0 \in \mathbb{N}$, такое что $\{1, \dots, N_0\} \times \{1, \dots, N_0\} \subseteq \{\sigma(1), \dots, \sigma(K_0)\}$.

Пусть $K \geqslant K_0$. Тогда

$$\sum_{k=1}^{K} a_{m(k)} b_{n(k)} = \sum_{m=1}^{N_0} \sum_{n=1}^{N_0} a_m b_n + \sum{}' a_m b_n,$$

где в последней сумме для всех слагаемых выполнено $\max\{m, n\} > N_0$. Тогда

$$\left\| \sum_{k=1}^{K} a_{m(k)} b_{n(k)} - AB \right\| \leqslant C\varepsilon. \qquad \square$$

Глава 5

Лемма Гензеля

Пусть $(F, \|\cdot\|)$ — полное неархимедово нормированное поле. По аналогии с $\mathbb{Q}_p$ введём *кольцо целых* поля F:

$$\mathbb{Z}_F = \{x \in F : \|x\| \leqslant 1\}.$$

Оно замкнуто (в топологическом смысле) $\Longrightarrow$ полно как метрическое пространство.

Теорема 5.1 (лемма Гензеля)**.** *Пусть $f(x) \in \mathbb{Z}_F[x]$, $\alpha_0 \in \mathbb{Z}_F$, причём $\|f(\alpha_0)\| < \|f'(\alpha_0)\|^2$. Тогда найдётся единственное $\alpha \in \mathbb{Z}_F$, удовлетворяющее условиям $f(\alpha) = 0$, $\|\alpha - \alpha_0\| < \|f'(\alpha_0)\|$.*

Доказательство. Положим $c = \frac{\|f(\alpha_0)\|}{\|f'(\alpha_0)\|^2} \in [0, 1)$.

Рассмотрим рекуррентную последовательность (α_0 — из условия теоремы):

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}, \quad n \geqslant 0.$$

(«Метод Ньютона» aka «метод касательных».) Проверим, что она обладает следующими свойствами:

1) $\|\alpha_n - \alpha_0\| \leqslant c\|f'(\alpha_0)\| < \|f'(\alpha_0)\|$ (в частности, $\alpha_n \in \mathbb{Z}_F$);
2) $\|f'(\alpha_n)\| = \|f'(\alpha_0)\|$ (в частности, $f'(\alpha_n) \neq 0$, поэтому α_{n+1} определено);
3) $\|f(\alpha_n)\| \leqslant c^{2^n}\|f'(\alpha_0)\|^2$;
4) $\|\alpha_{n+1} - \alpha_n\| \leqslant c^{2^n}\|f'(\alpha_0)\|$.

Введём обозначения. Для $\alpha, \beta, \gamma \in F$ будем писать $\alpha = \beta + \mathcal{O}(\gamma)$, если $\|\alpha - \beta\| \leqslant \|\gamma\|$. Аналогично определим «о малое»: $\alpha = \beta + \mathfrak{o}(\gamma)$, если $\|\alpha - \beta\| < \|\gamma\|$.

Тогда справедливо утверждение (фактически формула Тейлора): если $P(x) \in \mathbb{Z}_F[x]$, $\alpha, \beta \in \mathbb{Z}_F$, то $P(\alpha + \beta) = P(\alpha) + P'(\alpha)\beta + \mathcal{O}(\beta^2) = P(\alpha) + \mathcal{O}(\beta)$.

Будем проверять свойства по индукции.

При $n = 0$ свойства 1 и 2 тривиальны, а свойство 3 следует из определения c.

Пусть α_n определено и удовлетворяет свойствам 1–3. Тогда определено α_{n+1}, причём

$$\|\alpha_{n+1} - \alpha_n\| = \frac{\|f(\alpha_n)\|}{\|f'(\alpha_n)\|} \leqslant c^{2^n}\|f'(\alpha_0)\|,$$

то есть свойство 4 (для этого n) также верно.

Из свойств 1_n и 4_n следует $\|\alpha_{n+1} - \alpha_0\| \leqslant c\|f'(\alpha_0)\|$, т. е. свойство 1_{n+1}.

Свойство 2_{n+1} следует из свойства 1_{n+1}, поскольку

$$f'(\alpha_{n+1}) = f'(\alpha_0) + \mathcal{O}(\alpha_{n+1} - \alpha_0) = f'(\alpha_0) + \mathfrak{o}\big(f'(\alpha_0)\big).$$

Проверяем свойство 3_{n+1}:

$$f(\alpha_{n+1}) = f(\alpha_n) + f'(\alpha_n)(\alpha_{n+1} - \alpha_n) + \mathcal{O}\big((\alpha_{n+1} - \alpha_n)^2\big) = \mathcal{O}\big((\alpha_{n+1} - \alpha_n)^2\big).$$

Осталось воспользоваться свойством 4_n.

Таким образом, все свойства проверены.

Из свойства 4 следует, что существует предел $\lim \alpha_n = \alpha$, причём из свойств 1 и 3 следует, что α искомое. Кроме того, из свойства 2 следует, что $\|f'(\alpha)\| = \|f'(\alpha_0)\|$.

Докажем единственность. Допустим противное: пусть найдётся $\beta \neq \alpha$, такое что $f(\beta) = 0$ и $\beta = \alpha_0 + \mathfrak{o}\big(f'(\alpha_0)\big)$. Тогда

$$0 = f(\beta) = f(\alpha) + f'(\alpha)(\beta - \alpha) + \mathcal{O}\big((\beta - \alpha)^2\big) = f'(\alpha)(\beta - \alpha) + \mathcal{O}\big((\beta - \alpha)^2\big),$$

откуда

$$\|f'(\alpha)\| \leqslant \|\beta - \alpha\| < \|f'(\alpha_0)\|,$$

что противоречит равенству $\|f'(\alpha)\| = \|f'(\alpha_0)\|$. □

Упражнение 5.2. Доказать, что на самом деле верно равенство $\|\alpha - \alpha_0\| = \frac{\|f(\alpha_0)\|}{\|f'(\alpha_0)\|}$.

Обратимся к случаю $F = \mathbb{Q}_p$. В этом случае лемму Гензеля можно сформулировать следующим образом.

Теорема 5.3. *Пусть $f(x) \in \mathbb{Z}_p[x]$, $\alpha_0 \in \mathbb{Z}_p$, $v_p\big(f'(\alpha_0)\big) =: e \in \mathbb{N}_0$. Допустим, что справедливо сравнение $f(\alpha_0) \equiv 0 \pmod{p^{2e+1}}$. Тогда найдётся единственное $\alpha \equiv \alpha_0 \pmod{p^{e+1}}$, такое что $f(\alpha) = 0$.* □

Упражнение 5.4. Проверить, что $\alpha = \sum_{n=0}^{\infty} a_n p^n$ можно искать с помощью следующей процедуры «подъёма решений»:

1) $\sum_{n=0}^{e} a_n p^n \equiv \alpha_0 \pmod{p^{e+1}}$;

2) если $b_N := \sum_{n=0}^{e+N-1} a_n p^n$ уже найдено для некоторого $N \in \mathbb{N}$, то a_{e+N} однозначно находится из сравнения

$$f(b_N) + f'(b_N) p^{e+N} a_{e+N} \equiv 0 \pmod{p^{2e+N+1}},$$

причём последнее сравнение равносильно сравнению

$$f(b_N) + f'(\alpha_0) p^{e+N} a_{e+N} \equiv 0 \pmod{p^{2e+N+1}}.$$

Замечание 5.5. На самом деле, зная b_N, можно найти сразу b_{2N} как решение сравнения $f(b_N) + f'(b_N)(b_{2N} - b_N) \equiv 0 \pmod{p^{2e+2N}}$.

Выделим особо случай $e = 0$ теоремы 5.3.

Теорема 5.6. *Пусть $f(x) \in \mathbb{Z}_p[x]$, $\alpha_0 \in \mathbb{Z}_p$, $f(\alpha_0) \equiv 0 \pmod{p}$, $f'(\alpha_0) \not\equiv 0 \pmod{p}$. Тогда найдётся единственное $\alpha \equiv \alpha_0 \pmod{p}$, такое что $f(\alpha) = 0$.* □

Разберём несколько поучительных примеров.

Пример 5.7. Возьмём многочлен $f(x) = x^p - x$. Пусть $\alpha_0 \in \mathbb{Z}_p$. Тогда $f(\alpha_0) \equiv 0 \pmod{p}$ (малая теорема Ферма), $f'(\alpha_0) = p\alpha_0^{p-1} - 1 \equiv -1 \not\equiv 0 \pmod{p}$, поэтому из леммы Гензеля следует существование (и единственность) корня многочлена $f(x)$ в шаре $x \equiv \alpha_0 \pmod{p}$. Мы снова построили представитель Тейхмюллера $\omega(\alpha_0)$ (см. пример 4.2).

Остановимся на извлечении квадратных корней. Ограничимся случаем $x^2 = \alpha$, где $\alpha \in \mathbb{Z}_p^\times$ (общий случай легко сводится к нему). Тогда если $x \in \mathbb{Q}_p$ — решение, то $|x|_p = 1$, т. е. $x \in \mathbb{Z}_p^\times$.

Лемма 5.8. *Пусть $p > 2$ — простое число, $\alpha = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p^\times$. Тогда уравнение $x^2 = \alpha$ разрешимо в $\mathbb{Q}_p$ в том и только том случае, если $\left(\frac{a_0}{p}\right) = 1$ (т. е. a_0 — квадратичный вычет по модулю p).*

Доказательство. Если $x = \sum_{n=0}^{\infty} x_n p^n$ — решение, то $x_0^2 \equiv a_0 \pmod{p}$, поэтому $\left(\frac{a_0}{p}\right) = 1$.

Обратно, пусть $\left(\frac{a_0}{p}\right) = 1$. Возьмём $\alpha_0 \in \mathbb{Z}$, удовлетворяющее условию $\alpha_0^2 \equiv a_0 \pmod{p}$. Применяем теорему 5.6 для многочлена $f(x) = x^2 - \alpha$. □

Лемма 5.9. *Пусть $\alpha \in 1 + 2\mathbb{Z}_2$. Тогда уравнение $x^2 = \alpha$ разрешимо в $\mathbb{Q}_2$ в том и только том случае, если $\alpha \equiv 1 \pmod{8}$.*

Доказательство. Аналогично, только придётся использовать теорему 5.3 при $e = 1$. □

Упражнение 5.10. С помощью лемм 5.8 и 5.9 доказать, что

$$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \begin{cases} C_2 \times C_2, & p > 2, \\ C_2 \times C_2 \times C_2, & p = 2, \end{cases}$$

где C_2 — циклическая группа порядка 2.

Пример 5.11. Рассмотрим уравнение $x^2 = -1$. Оно разрешимо в $\mathbb{Q}_5$, но не разрешимо в $\mathbb{R}$, $\mathbb{Q}_2$ и $\mathbb{Q}_3$. Отсюда следует, что поле $\mathbb{Q}_5$ не изоморфно ни одному из полей $\mathbb{R}$, $\mathbb{Q}_2$ и $\mathbb{Q}_3$ (даже в смысле обычного изоморфизма полей, без учёта нормы). (Более того, не существует (ненулевого) гомоморфизма из $\mathbb{Q}_5$ ни в одно из этих полей.)

Упражнение 5.12. Доказать, что поля $\mathbb{Q}_p$ при различных простых p не изоморфны друг другу и полю $\mathbb{R}$.

Аналогичные утверждения можно доказать и для корней более высокой степени. Альтернативный подход к извлечению корня m-й степени при $(m, p) = 1$ можно получить на основе формулы бинома Ньютона.

Лемма 5.13. *Пусть $m \in \mathbb{N}$, $(m, p) = 1$, $\alpha \in p\mathbb{Z}_p$. Тогда ряд $\sum_{n=0}^{\infty} \binom{1/m}{n} \alpha^n$ сходится в $\mathbb{Z}_p$, причём его сумма является (единственным) корнем уравнения $x^m = 1 + \alpha$, удовлетворяющим условию $x \equiv 1 \pmod{p}$.*

Замечание 5.14. $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$ — биномиальные многочлены.

Доказательство. При $\gamma \in \mathbb{N}_0$ имеем $\binom{\gamma}{n} \in \mathbb{Z}$, откуда $\left|\binom{\gamma}{n}\right|_p \leqslant 1$. Поскольку $\mathbb{N}_0$ плотно в $\mathbb{Z}_p$, то $\binom{\gamma}{n} \in \mathbb{Z}_p$ при всех $\gamma \in \mathbb{Z}_p$, в частности, при $\gamma = 1/m$.

Следовательно, ряд $\sum_{n=0}^{\infty} \binom{1/m}{n} \alpha^n$ сходится. Пусть S — его сумма. Тогда

$$S^m = \sum_{n_1,\ldots,n_m=0}^{\infty} \binom{1/m}{n_1} \cdots \binom{1/m}{n_m} \alpha^{n_1+\cdots+n_m} = \sum_{n=0}^{\infty} \left(\sum_{n_1+\cdots+n_m=n} \binom{1/m}{n_1} \cdots \binom{1/m}{n_m} \right) \alpha^n.$$

Эти равенства справедливы и для $\alpha \in (-1, 1) \subseteq \mathbb{R}$, причём в этом случае мы знаем, что $S^m = 1 + \alpha$. Из теоремы единственности для степенных рядов (можно также равенства рассматривать с точностью до $o(\alpha^N)$ при $\alpha \to 0$) следует, что это тождество, поэтому это верно и в $\mathbb{Q}_p$.

Итак, S — корень уравнения. При этом

$$S = 1 + \mathcal{O}(\alpha) = 1 + \mathcal{O}(p).$$

Единственность следует из леммы Гензеля. □

Замечание 5.15. Справедливо тождество (*свёртка Вандермонда*):

$$\sum_{n_1+\cdots+n_m=n} \binom{x_1}{n_1} \cdots \binom{x_m}{n_m} = \binom{x_1 + \cdots + x_m}{n}.$$

Для доказательства достаточно сравнить коэффициенты при z^n в левой и правой частях равенства

$$(1+z)^{x_1} \cdots (1+z)^{x_m} = (1+z)^{x_1+\cdots+x_m}.$$

Пример 5.16. Ряд $\sum_{n=0}^{\infty} \binom{1/2}{n} (7/9)^n$ сходится в $\mathbb{R}$ и в $\mathbb{Q}_7$, причём в $\mathbb{R}$ сумма ряда равна $+4/3$, а в $\mathbb{Q}_7$ его сумма равна $-4/3$.

Условие $(m, p) = 1$ в лемме 5.13 существенно, как показывает следующее упражнение.

Упражнение 5.17. Пусть $p > 2$ — простое число, $\alpha \in p\mathbb{Z}_p$. Доказать, что уравнение $x^p = 1 + \alpha$ разрешимо в $\mathbb{Q}_p$ тогда и только тогда, когда $\alpha \equiv 0 \pmod{p^2}$, причём в этом случае решение единственно.

Упражнение 5.18. Пусть $p > 2$ — простое число, $n \in \mathbb{N}$, $\alpha \in \mathbb{Z}_p^\times$. Доказать, что уравнение $x^n = \alpha$ разрешимо в $\mathbb{Q}_p$ тогда и только тогда, когда разрешимо сравнение

$$x^n \equiv \alpha \pmod{p^{\nu_p(n)+1}}.$$

Бонус: пример на подъём решений

Пример 5.19. Рассмотрим уравнение $x^2 + 1 = 0$ в $\mathbb{Q}_5$.

Пусть $x = \sum_{n=0}^{\infty} a_n 5^n$. Положим $x_n = \sum_{i=0}^{n-1} a_i 5^i \equiv x \pmod{5^n}$.

Смотрим по модулю 5: $x^2 + 1 \equiv 0 \pmod 5 \implies a_0^2 + 1 \equiv 0 \pmod 5 \implies a_0 \in \{2, 3\}$. Рассмотрим решение с $a_0 = 2$, то есть $x_2 = 2 + 5a_1$.

Смотрим по модулю 5^2:

$$\begin{gathered} x_2^2 + 1 \equiv 0 \pmod{5^2}, \\ 5 + 20a_1 \equiv 0 \pmod{5^2}, \\ 1 + 4a_1 \equiv 0 \pmod{5}, \\ a_1 = 1 \implies x_3 = 7 + 5^2 a_2. \end{gathered}$$

Смотрим по модулю 5^3:

$$\begin{gathered} 50 + 14 \cdot 5^2 a_2 \equiv 0 \pmod{5^3}, \\ 2 + 14a_2 \equiv 0 \pmod{5}, \\ a_2 = 2 \implies x_4 = 57 + 5^3 a_3. \end{gathered}$$

Пусть x_n найдено, $x_n^2 + 1 \equiv 0 \pmod{5^n}$. Ищем $x_{n+1} = x_n + 5^n a_n$:

$$\begin{gathered} x_n^2 + 2x_n \cdot 5^n a_n + 1 \equiv 0 \pmod{5^{n+1}}, \\ \frac{x_n^2 + 1}{5^n} + 2x_n a_n \equiv 0 \pmod{5}, \\ \frac{x_n^2 + 1}{5^n} + 4a_n \equiv 0 \pmod{5}, \\ a_n \equiv \frac{x_n^2 + 1}{5^n} \pmod{5}, \\ x_{n+1} \equiv x_n^2 + x_n + 1 \pmod{5^{n+1}}. \end{gathered}$$

Упражнение 5.20. В обозначениях примера 5.19 проверить рекуррентную формулу:

$$x_{2n} \equiv x_n + \frac{x_n(x_n^2 + 1)}{2} \pmod{5^{2n}}.$$

Упражнение 5.21. Вычислить корень уравнения $x^2 + 7 = 0$ в $\mathbb{Q}_2$, удовлетворяющий условию $x \equiv 1 \pmod 4$, с точностью $\mathcal{O}(2^6)$.

Глава 6

Компактность кольца целых чисел

Введём ряд соглашений и обозначений, которые будем пользовать и в дальнейшем.

Пусть $(F, \|\cdot\|)$ — произвольное неархимедово нормированное поле (возможно, неполное). Будем обозначить: $G_F = \{\|x\| : x \in F^*\}$, $\mathbb{Z}_F = \{x \in F : \|x\| \leqslant 1\}$ — кольцо целых, $\mathfrak{M}_F = \{x \in F : \|x\| < 1\}$ — единственный максимальный идеал кольца $\mathbb{Z}_F$ ($\mathfrak{M}_F$ состоит из всех необратимых элементов кольца $\mathbb{Z}_F$, поэтому содержит все собственные идеалы), $k_F = \mathbb{Z}_F/\mathfrak{M}_F$ — *поле вычетов* поля F (или кольца $\mathbb{Z}_F$, или нормы $\|\cdot\|$).

Пример 6.1. Для $F = \mathbb{Q}_p$: $G_F = p^{\mathbb{Z}} = \{p^n : n \in \mathbb{Z}\}$, $\mathbb{Z}_F = \mathbb{Z}_p$, $\mathfrak{M}_F = p\mathbb{Z}_p$, $k_F = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ (поле из p элементов).

Вкратце остановимся на том, как ведёт себя поле вычетов при продолжении нормы. Пусть $F_0 \subseteq F$. Тогда $\mathfrak{M}_{F_0} = \mathfrak{M}_F \cap \mathbb{Z}_{F_0} \subseteq \mathfrak{M}_F$, поэтому определено естественное вложение $\varphi : k_{F_0} \hookrightarrow k_F$, а именно: $\varphi(\alpha + \mathfrak{M}_{F_0}) = \alpha + \mathfrak{M}_F$. Удобно отождествлять k_{F_0} с его образом $\varphi(k_{F_0})$ и считать, что $k_{F_0} \subseteq k_F$.

Упражнение 6.2. Пусть F — пополнение F_0. Доказать, что $k_F = k_{F_0}$.

Всюду дальше предполагаем, что норма $\|\cdot\|$ нетривиальна, т. е. $G_F \neq \{1\}$.

Лемма 6.3. *Группа G_F либо плотна в $(0, +\infty)$, либо является циклической (в последнем случае говорят, что группа дискретна, потому что каждый её элемент является изолированным).*

Доказательство. Удобно «прологарифмировать» и свести к случаю (ненулевой) подгруппы $G \trianglelefteq \mathbb{R}$ (по сложению).

Рассмотрим

$$a = \inf\{g \in G : g > 0\}.$$

Если $a = 0$, то G содержит сколь угодно малые числа, поэтому всюду плотна.

Если $a > 0$, то $a \in G$ (иначе для любого $\varepsilon > 0$ выполнено $G \cap (a, a + \varepsilon) \neq \varnothing$ и G содержит сколь угодно малые числа), откуда $G = \langle a \rangle$ (для всякого $g \in G$ найдётся $n \in \mathbb{Z}$, такое что $na \leqslant g < (n+1)a$, откуда $0 \leqslant g - na < a$ и $g = na$). □

Лемма 6.4. *Пусть группа G_F дискретна. Тогда $\mathbb{Z}_F$ — кольцо главных идеалов. Более того, если $\mathfrak{M}_F = (\pi) = \pi\mathbb{Z}_F$, то всякий ненулевой идеал имеет вид $(\pi^n) = \mathfrak{M}_F^n$ для некоторого $n \in \mathbb{N}_0$.*

Доказательство. Пусть $G_F = \langle a \rangle$, $a \in (0,1)$. Фиксируем $\pi \in \mathbb{Z}_F$, такое что $\|\pi\| = a$.

Возьмём произвольный ненулевой идеал $\mathfrak{A} \trianglelefteq \mathbb{Z}_F$. Пусть

$$\max\{\|\alpha\| : \alpha \in \mathfrak{A} \setminus \{0\}\} = \|\alpha_0\| = a^n.$$

Если $\alpha \in \mathfrak{A}$, то $\|\alpha\| \leqslant \|\alpha_0\|$. Обратно: если $\|\alpha\| \leqslant \|\alpha_0\|$, то $\alpha = \alpha_0\beta$, где $\|\beta\| \leqslant 1$, т. е. $\beta \in \mathbb{Z}_F$, поэтому $\alpha \in \mathfrak{A}$. Следовательно,

$$\alpha \in \mathfrak{A} \iff \|\alpha\| \leqslant \|\alpha_0\| \iff \|\alpha\| \leqslant \|\pi^n\| \iff \alpha \in (\pi^n) = (\pi)^n.$$

В частности, $\mathfrak{M}_F = (\pi)$. □

Определение 6.5. В условиях леммы 6.4: если $\mathfrak{M}_F = (\pi)$, то π называется *униформизующим элементом* кольца $\mathbb{Z}_F$ (он определён с точностью до умножения на обратимый элемент кольца $\mathbb{Z}_F$).

Теорема 6.6. *Допустим, что поле F полно, группа G_F дискретна и поле вычетов k_F конечно. Тогда кольцо $\mathbb{Z}_F$ компактно.*

Доказательство. Доказательство аналогично доказательству компактности отрезка.

Допустим противное: найдётся открытое покрытие $\mathbb{Z}_F \subseteq \bigcup_{i \in I} U_i$, из которого нельзя выбрать конечное подпокрытие.

Пусть S — некоторая «полная система вычетов» по модулю идеала $\mathfrak{M}_F = \pi\mathbb{Z}_F$, то есть

$$\mathbb{Z}_F = \bigsqcup_{\alpha \in S} (\alpha + \pi\mathbb{Z}_F).$$

Поскольку $|S| = |k_F| < +\infty$, то найдётся $\alpha_0 \in S$, такое что для $\alpha_0 + \pi\mathbb{Z}_F$ нельзя выбрать конечное подпокрытие.

Аналогично, поскольку

$$\alpha_0 + \pi\mathbb{Z}_F = \bigcup_{\alpha \in S} (\alpha_0 + \alpha\pi + \pi^2\mathbb{Z}_F),$$

то найдётся $\alpha_1 \in S$, такое что для $\alpha_0 + \alpha_1\pi + \pi^2\mathbb{Z}_F$ нельзя выбрать конечное подпокрытие.

И так далее. В результате получим последовательность $\alpha_n \in S$, такую что при любом n для $\alpha_0 + \alpha_1\pi + \dots + \alpha_n\pi^n + \pi^{n+1}\mathbb{Z}_F$ нельзя выбрать конечное подпокрытие.

Пусть $\beta = \sum_{n=0}^{\infty} \alpha_n\pi^n \in \mathbb{Z}_F$. Найдётся $i \in I$, такое что $\beta \in U_i$. Но тогда при достаточно большом n выполнено

$$\alpha_0 + \alpha_1\pi + \dots + \alpha_n\pi^n + \pi^{n+1}\mathbb{Z}_F \subseteq U_i.$$

Противоречие. □

Упражнение 6.7. Доказать обратное утверждение: если кольцо $\mathbb{Z}_F$ компактно, то поле F полно, группа G_F дискретна и поле вычетов k_F конечно.

Следствие 6.8. *Кольцо $\mathbb{Z}_p$ компактно.* □

Следствие 6.9. *Пусть* $P_k(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$, $k = 1, \dots, m$. *Тогда следующие два условия эквивалентны*:

1) *система сравнений*

$$P_k(x_1, \dots, x_n) \equiv 0 \pmod{p^N}, \qquad k = 1, \dots, m,$$

разрешима (*в целых числах*) *для любого* $N \in \mathbb{N}$;

2) *система уравнений*

$$P_k(x_1, \dots, x_n) = 0, \qquad k = 1, \dots, m,$$

разрешима в $\mathbb{Z}_p$. □

Глава 7

Лемма Гаусса

В этой теме $(F, \|\cdot\|)$ — неархимедово нормированное поле (возможно, неполное).

Продолжим норму $\|\cdot\|$ на кольцо многочленов $F[z]$ по формуле

$$\left\| \sum_{n=0}^{d} c_n z^n \right\| = \max_{0 \leqslant n \leqslant d} \|c_n\|.$$

Заметим, что если $P(z) = c_0$ — постоянный многочлен, то $\|P\| = \|c_0\|$, поэтому конфликта обозначений не возникает, то есть получается настоящее продолжение.

Оказывается, это продолжение является настоящей нормой на кольце многочленов.

Лемма 7.1 (лемма Гаусса)**.** *Для любых многочленов $P(z), Q(z) \in F[z]$ выполнено*

$$\|PQ\| = \|P\| \cdot \|Q\|.$$

Первое доказательство. Если $P(z) = 0$ или $Q(z) = 0$, то утверждение очевидно, поэтому далее считаем, что $P(z) \neq 0$ и $Q(z) \neq 0$.

Пусть

$$P(z) = a_m z^m + \cdots + a_0,$$
$$Q(z) = b_n z^n + \cdots + b_0.$$

Тогда

$$P(z)Q(z) = c_{m+n} z^{m+n} + \cdots + c_0,$$

где $c_k = \sum_{i+j=k} a_i b_j$. Очевидно, что $\|c_k\| \leqslant \|P\| \cdot \|Q\|$, поэтому $\|PQ\| \leqslant \|P\| \cdot \|Q\|$.

Пусть $\|P\| = \|a_s\|$, $\|Q\| = \|b_t\|$, причём s и t наибольшие возможные. Тогда

$$c_{s+t} = a_s b_t + \sum_{\substack{i+j=s+t, \\ (i,j) \neq (s,t)}} a_i b_j,$$

где для каждого слагаемого в последней сумме выполнено $i > s$ или $j > t$, откуда $\|a_i b_j\| < \|P\| \cdot \|Q\| = \|a_s b_t\|$. Следовательно, $\|c_{s+t}\| = \|P\| \cdot \|Q\|$. □

Второе доказательство. Можно считать, что $\|P\| = \|Q\| = 1$ («максимальные» коэффициенты можно вынести за скобки). В частности, $P(z), Q(z) \in \mathbb{Z}_F[z]$.

Для каждого многочлена $A(z) \in \mathbb{Z}_F[z]$ определим его *редукцию* по модулю идеала $\mathfrak{M}_F$: $\overline{A}(z) = A(z) \bmod \mathfrak{M}_F \in k_F[z]$ (каждый коэффициент рассматривается по модулю идеала). Легко проверить, что получается гомоморфизм колец $\mathbb{Z}_F[z] \to k_F[z]$.

Поскольку $\|P\| = \|Q\| = 1$, то $\overline{P} \neq \overline{0}$ и $\overline{Q} \neq \overline{0}$, поэтому $\overline{PQ} = \overline{P} \cdot \overline{Q} \neq \overline{0}$ (поскольку кольцо $k_F[z]$ не имеет делителей нуля). Следовательно, $\|PQ\| = 1$. □

Замечание 7.2. Как видно из второго доказательства, лемма Гаусса справедлива для многочленов от произвольного множества переменных.

Замечание 7.3. Лемма 7.1 является уточнением классической леммы Гаусса о примитивных многочленах. Для многочлена $P(z) \in \mathbb{Z}[z]$ его *содержанием* называется наибольший общий делитель его коэффициентов; обозначение: $\operatorname{cont}(P)$. (При этом полагаем $\operatorname{cont}(0) = 0$.) Несложно убедиться, что для ненулевого многочлена P выполнено

$$\operatorname{cont}(P) = \prod_p |P|_p^{-1},$$

поэтому из леммы 7.1 получаем

$$\operatorname{cont}(PQ) = \operatorname{cont}(P)\operatorname{cont}(Q).$$

В частности, при $\operatorname{cont}(P) = \operatorname{cont}(Q) = 1$ получаем классическую формулировку леммы Гаусса (произведение примитивных многочленов является примитивным многочленом).

Упражнение 7.4. Проверить, что норму $\|\cdot\|$ можно продолжить на поле рациональных функций $F(z)$ по формуле

$$\left\|\frac{P(z)}{Q(z)}\right\| = \frac{\|P(z)\|}{\|Q(z)\|}.$$

(Аналогично для произвольного количества неизвестных.)

Упражнение 7.5. Для $R > 0$ положим

$$\left\|\sum_{n=0}^{d} c_n z^n\right\|_R = \max_{0 \leqslant n \leqslant d} \|c_n\| R^n.$$

Доказать, что для любых многочленов $P(z), Q(z) \in F[z]$ выполнено

$$\|PQ\|_R = \|P\|_R \cdot \|Q\|_R.$$

Упражнение 7.6. С помощью упражнений 7.4 и 7.5 построить пример неархимедова нормированного поля с $G_F = (0, +\infty)$.

Из леммы Гаусса следует важное следствие для целочисленных многочленов.

Следствие 7.7. *Пусть $P(z), Q(z) \in F[z]$ — унитарные многочлены, причём $P(z)Q(z) \in \mathbb{Z}_F[z]$. Тогда $P(z), Q(z) \in \mathbb{Z}_F[z]$.*

Доказательство. Имеем $\|P\| \geqslant 1$ и $\|Q\| \geqslant 1$, однако $\|P\| \cdot \|Q\| = \|PQ\| \leqslant 1$. Следовательно, $\|P\| = \|Q\| = 1$. □

Глава 8

Сведения из теории алгебраических чисел

8.1 Конечные и алгебраические расширения полей

Доказательства приводимых ниже утверждений (многие из них довольно простые) можно найти, например, в книжке

S. Lang. *Algebra*.

Определение 8.1. Поле K называется *расширением* поля F, если $F \subseteq K$. Принято писать: расширение K/F (это *не* фактор). Поле K можно рассмотреть как векторное пространство над полем F. Если оно конечномерно, то расширение K/F называется *конечным*. Размерность $\dim_F K$ этого пространства называется *степенью* расширения и обозначается через $[K : F]$.

Пример 8.2. $\mathbb{C}$ — конечное расширение $\mathbb{R}$ степени $[\mathbb{C} : \mathbb{R}] = 2$.

Теорема 8.3. *Рассмотрим «башню расширений» $F \subseteq K \subseteq L$. Расширение L/F конечно тогда и только тогда, когда конечны оба расширения K/F и L/K, причём в этом случае выполнено $[L : F] = [K : F] \cdot [L : K]$. Более того, если $\omega_1, \dots, \omega_n$ — базис K над F, $\Omega_1, \dots, \Omega_m$ — базис L над K, то всевозможные попарные произведения $\omega_i \Omega_j$ образуют базис L над F.*

Определение 8.4. Пусть K — расширение F. Элемент $\alpha \in K$ называется *алгебраическим над F*, если существует ненулевой многочлен $P(z) \in F[z]$, такой что $P(\alpha) = 0$. Унитарный такой многочлен наименьшей возможной степени называется *минимальным многочленом α над F*, а его степень — *степенью α над F*. Обозначения: $\mu_\alpha(z) = \mu_{\alpha,F}(z)$, $\deg \alpha = \deg_F \alpha$.

Лемма 8.5. *Пусть α алгебраичен над F. Тогда его минимальный многочлен (над F) определён однозначно и неприводим (над F). Кроме того, для любого многочлена $P(z) \in F[z]$, такого что $P(\alpha) = 0$, выполнено $\mu_\alpha(z) \mid P(z)$.*

Следствие 8.6. *Пусть $P(z) \in F[z]$ — унитарный неприводимый (над F) многочлен, $P(\alpha) = 0$. Тогда $P(z) = \mu_\alpha(z)$.*

Следствие 8.7. *Пусть α алгебраичен над F. Тогда его минимальный многочлен является минимальным для всех своих корней.*

Определение 8.8. Расширение K/F называется *алгебраическим*, если все элементы K являются алгебраическими над F.

Лемма 8.9. *Любое конечное расширение является алгебраическим, причём если K — конечное расширение F, $\alpha \in K$, то $\deg \alpha \leqslant [K : F]$.*

Определение 8.10. Пусть K — расширение F, $\alpha_1, \dots, \alpha_n \in K$. Через $F(\alpha_1, \dots, \alpha_n)$ обозначается наименьшее по включению подполе K, которое содержит F (как подполе) и все α_i. Если $K = F(\alpha_1, \dots, \alpha_n)$, то говорят, что поле K *порождено элементами* $\alpha_1, \dots, \alpha_n$ над полем F. Такие расширения называются *конечно порождёнными*. Расширение вида $F(\alpha)$ (то есть порождённое одним элементом) называется *простым*.

Очевидно, что

$$F(\alpha_1, \dots, \alpha_n) = \left\{ \frac{P(\alpha_1, \dots, \alpha_n)}{Q(\alpha_1, \dots, \alpha_n)} \ : \ P(\boldsymbol{z}), Q(\boldsymbol{z}) \in F[\boldsymbol{z}], Q(\boldsymbol{\alpha}) \neq 0 \right\}.$$

Кроме того, несложно видеть, что

$$F(\alpha_1, \dots, \alpha_n) = F(\alpha_1)(\alpha_2) \dots (\alpha_n),$$

поэтому для начала разберёмся с простыми расширениями.

Если α трансцендентен (то бишь не алгебраичен) над F, то $F(\alpha)$ изоморфно полю рациональных функций (от одного неизвестного) над F. Случай алгебраического α более интересен.

Теорема 8.11. *Пусть α алгебраичен над F, $\deg_F \alpha = n$. Тогда $F(\alpha)$ — конечное расширение F степени n, причём $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ — базис $F(\alpha)$ над F. Более того, $F(\alpha) \cong F[z]/\mu_\alpha(z)F[z]$ (с естественным изоморфизмом $P(\alpha) \leftrightarrow P(z) + \mu_\alpha(z)F[z]$).*

Следствие 8.12 (уточнение леммы 8.9)**.** *Если K — конечное расширение F, $\alpha \in K$, то $\deg \alpha$ делит $[K : F]$.*

Следствие 8.13. *Расширение K/F конечно тогда и только тогда, когда $K = F(\alpha_1, \dots, \alpha_n)$ для некоторых $\alpha_1, \dots, \alpha_n$, алгебраических над F.*

Следствие 8.14. *Пусть K — расширение F. Тогда множество всех алгебраических над F элементов поля K замкнуто относительно основных арифметических операций, то есть является полем.*

Теорема 8.15 (теорема о примитивном элементе)**.** *Если $\operatorname{char} F = 0$, то всякое конечное расширение поля F является простым.* (*Если $K = F(\theta)$, то θ называется* примитивным элементом *расширения.*)

Пример 8.16. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

Лемма 8.17. *Для любого поля F существует расширение K, в котором всякий непостоянный многочлен $P(z) \in F[z]$ раскладывается на линейные множители.*

Теорема 8.18. *Пусть K — расширение из леммы 8.17, A — поле всех алгебраических над F элементов поля K. Тогда A алгебраически замкнуто.*

Определение 8.19. Расширение A из теоремы 8.18 называется *алгебраическим замыканием* поля F. Обозначение: F^{alg} (также используется обозначение $\overline{F}$). (Можно доказать, что любые два алгебраических замыкания изоморфны.)

В дальнейшем будем считать, что зафиксировано некоторое алгебраическое замыкание F^{alg}, и все поля и корни многочленов будем брать из этого фиксированного поля (если не сказано противное).

Определение 8.20. Алгебраическое расширение K/F называется *сепарабельным*, если для любого $\alpha \in K$ его минимальный многочлен (над F) не имеет кратных корней.

Теорема 8.21 (теорема о примитивном элементе)**.** *Если K — сепарабельное конечное расширение F, то оно является простым.*

Пример 8.22 («контрпример»)**.** Пусть p — простое число. Тогда:

1) $\mathbb{F}_p(z^{1/p})$ — несепарабельное расширение $\mathbb{F}_p(z)$;
2) расширение $\mathbb{F}_p(x^{1/p}, y^{1/p})/\mathbb{F}_p(x, y)$ не имеет примитивного элемента (если $\alpha \in \mathbb{F}_p(x^{1/p}, y^{1/p})$, то $\alpha^p \in \mathbb{F}_p(x, y)$, откуда $\deg \alpha \leqslant p$; с другой стороны, $[\mathbb{F}_p(x^{1/p}, y^{1/p}) : \mathbb{F}_p(x, y)] = p^2$).

Теорема 8.23. *Если $K = F(\alpha_1, \ldots, \alpha_n)$ — конечное расширение F, то оно сепарабельно тогда и только тогда, когда минимальные многочлены всех порождающих α_i не имеют кратных корней.*

Определение 8.24. Поле F называется *совершенным*, если любой неприводимый над F многочлен не имеет кратных корней (то есть любое алгебраическое расширение F сепарабельно).

Лемма 8.25. *Поле F совершенно тогда и только тогда, когда либо $\operatorname{char} F = 0$, либо $\operatorname{char} F = p > 0$ и для любого $\alpha \in F$ найдётся $\beta \in F$, такое что $\alpha = \beta^p$.*

Лемма 8.26. *Любое конечное поле совершенно.*

Определение 8.27. Пусть $\alpha \in F^{\mathrm{alg}}$. Корни его минимального многочлена $\mu_\alpha(z)$ над F называются *сопряжёнными* к α (или с α) над F.

Лемма 8.28. *Многочлен $\mu_\alpha(z)$ является минимальным для всех сопряжённых к α.*

Определение 8.29. Пусть K, L — расширения F. Вложение полей $\sigma : K \to L$ называется вложением (поля K в поле L) *над полем F*, если σ тождественно на F, то есть $\sigma(\alpha) = \alpha$ для всех $\alpha \in F$.

Лемма 8.30. *Пусть K — алгебраическое расширение F, $\alpha \in K$. Тогда для любого вложения $\sigma : K \to F^{\mathrm{alg}}$ над F элемент $\sigma(\alpha)$ является сопряжённым к α над F.*

Лемма 8.31. *Пусть $\alpha \in F^{\mathrm{alg}}$, α' — любое его сопряжённое над F. Тогда существует единственное вложение $\sigma : F(\alpha) \to F^{\mathrm{alg}}$ над F, такое что $\sigma(\alpha) = \alpha'$, а именно: $\sigma\big(P(\alpha)\big) = P(\alpha')$, $P(z) \in F[z]$.*

Следствие 8.32. *Пусть $\alpha \in F^{\mathrm{alg}}$. Тогда количество вложений $F(\alpha) \to F^{\mathrm{alg}}$ над F равно количеству (различных) сопряжённых к α над F.*

Лемма 8.33. *Пусть $\alpha \in F^{\mathrm{alg}}$. Тогда любое вложение $F \to F^{\mathrm{alg}}$ можно продолжить до вложения $F(\alpha) \to F^{\mathrm{alg}}$, причём количество продолжений равно количеству сопряжённых к α над F.*

Следствие 8.34. *Пусть K — конечное расширение F. Тогда количество вложений $K \to F^{\mathrm{alg}}$ над F не превосходит $[K : F]$, причём равенство достигается тогда и только тогда, когда расширение K/F сепарабельно.*

Теорема 8.35. *Пусть K — алгебраическое расширение F. Тогда следующие условия эквивалентны:*

1) *Любое вложение $\sigma\colon K \to F^{\mathrm{alg}}$ над F является автоморфизмом поля K, то есть $\sigma(K) = K$.*
2) *Для любого вложения $\sigma\colon K \to F^{\mathrm{alg}}$ над F выполнено $\sigma(K) \subseteq K$;*
3) *Для любого $\alpha \in K$ все сопряжённые к α (над F) лежат в K.*

Если $K = F(\alpha_1, \dots, \alpha_n)$ — конечное расширение F, то эти условия эквивалентны тому, что все сопряжённые ко всем порождающим α_i лежат в K.

Определение 8.36. Алгебраическое расширение K/F, удовлетворяющее любому из условий теоремы 8.35, называется *нормальным*. Сепарабельное нормальное расширение называется *расширением Галуа*.

Определение 8.37. Пусть K/F — расширение Галуа. *Группой Галуа* этого расширения называется группа всех автоморфизмов поля K над F относительно операции композиции. Обозначение: $\mathrm{Gal}(K/F)$.

Лемма 8.38. *Если K/F — расширение Галуа, то $|\mathrm{Gal}(K/F)| = [K : F]$.*

8.2 Конечные поля

Пусть F — конечное поле, $\mathrm{char}\, F = p$. Тогда F содержит подполе $\mathbb{F}_p$ из p элементов.

Лемма 8.39. *F является конечным расширением $\mathbb{F}_p$. Если $[F : \mathbb{F}_p] = n$, то $|F| = p^n$.*

Лемма 8.40. *Для любого $q = p^n$ существует единственное подполе $\mathbb{F}_p^{\mathrm{alg}}$ из q элементов. Оно состоит из всех корней многочлена $z^q - z$.*

Поле из q элементов (единственное, если зафиксировать алгебраическое замыкание) обозначается через $\mathbb{F}_q$.

Упражнение 8.41. Доказать, что $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$ тогда и только тогда, когда $q_2 = q_1^n$, $n \in \mathbb{N}$. При этом $[\mathbb{F}_{q_2} : \mathbb{F}_{q_1}] = n$.

Лемма 8.42. *Пусть G — конечная подгруппа мультипликативной группы некоторого поля. Тогда G циклическая.*

Следствие 8.43. *Группа $\mathbb{F}_q^*$ циклическая.*

Теорема 8.44. *Расширение $\mathbb{F}_{q^n}/\mathbb{F}_q$ является расширением Галуа с циклической группой Галуа, порождённой автоморфизмом $x \mapsto x^q$.*

Следствие 8.45. *Пусть $P(z) \in \mathbb{F}_q[z]$ — унитарный неприводимый над $\mathbb{F}_q$ многочлен, $\deg P = n$, $P(\alpha) = 0$. Тогда*

$$P(z) = \prod_{i=0}^{n-1} \left(z - \alpha^{q^i}\right).$$

Упражнение 8.46. Пусть $\alpha \in \mathbb{F}_q^{\mathrm{alg}}$. Доказать, что $\deg_{\mathbb{F}_q} \alpha$ — это наименьшее $n \in \mathbb{N}$, такое что $\alpha^{q^n} = \alpha$.

Упражнение 8.47. Доказать, что для любого $n \in \mathbb{N}$ справедливо разложение

$$z^{q^n} - z = \prod P(z),$$

где произведение берётся по всем унитарным неприводимым (над $\mathbb{F}_q$) многочленам $P(z) \in \mathbb{F}_q[z]$ с условием $\deg P(z) \mid n$. Вывести отсюда, что количество унитарных неприводимых многочленов степени n равно $\frac{1}{n}\sum_{d \mid n} \mu(d) q^{n/d}$, где μ — функция Мёбиуса.

8.3 Норма в конечных расширениях

Пусть K — конечное расширение F. Каждому $\alpha \in K$ сопоставим линейный (над F) оператор $T_\alpha : K \to K$ по правилу $T_\alpha(x) = \alpha x$. Легко видеть, что это соответствие уважает арифметические операции и инъективно, то есть получаем вложение поля K в алгебру линейных операторов (линейное над F).

Определение 8.48. Определитель $\det T_\alpha$ оператора T_α называется *нормой α относительно расширения K/F*. Обозначения: $\mathrm{N}_F^K(\alpha) = \mathrm{N}_{K/F}(\alpha) = \mathrm{N}(\alpha)$.

Непосредственно из определения видно, что эта норма обладает свойствами:

1) $\mathrm{N}_F^K(\alpha) \in F$;
2) $\mathrm{N}_F^K(\alpha) = 0 \iff \alpha = 0$;
3) $\mathrm{N}_F^K(\alpha\beta) = \mathrm{N}_F^K(\alpha)\,\mathrm{N}_F^K(\beta)$;
4) если $\alpha \in F$, то $\mathrm{N}_F^K(\alpha) = \alpha^{[K:F]}$.

Последнее свойство — частный случай следующего утверждения.

Лемма 8.49. *Пусть $F \subseteq K \subseteq L$ — башня конечных расширений, $\alpha \in K$. Тогда*

$$\mathrm{N}_F^L(\alpha) = \big(\mathrm{N}_F^K(\alpha)\big)^{[L:K]}.$$

Доказательство. Пусть $\omega_1, \dots, \omega_n$ — базис K над F, A — матрица оператора $T_\alpha|_K$ в этом базисе, $\Omega_1, \dots, \Omega_m$ — базис L над K. В качестве базиса L над F возьмём

$$\omega_1\Omega_1, \dots, \omega_n\Omega_1, \omega_1\Omega_2, \dots, \omega_n\Omega_2, \dots, \omega_1\Omega_m, \dots, \omega_n\Omega_m.$$

Легко видеть, что матрица оператора T_α в этом базисе блочно-диагональная вида

$$\begin{pmatrix} A & O & \cdots & O \\ O & A & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A \end{pmatrix},$$

откуда получаем требуемое. □

Лемма 8.50. *Пусть $\mu_\alpha(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0 = (z - \alpha_1)\cdots(z - \alpha_n)$ — минимальный многочлен α (над F). Тогда*

$$\mathrm{N}_F^K(\alpha) = \big((-1)^n a_0\big)^{[K:F(\alpha)]} = (\alpha_1 \cdots \alpha_n)^{[K:F(\alpha)]}.$$

Доказательство. Можно считать, что $K = F(\alpha)$. Возьмём базис $1, \alpha, \dots, \alpha^{n-1}$. В этом базисе матрица оператора T_α равна

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix},$$

поэтому $\mathrm{N}_F^{F(\alpha)}(\alpha) = (-1)^n a_0 = \alpha_1 \cdots \alpha_n$. □

Глава 9

Продолжение нормы на алгебраическое замыкание

9.1 Нормы на векторных пространствах

Определение 9.1. Пусть $(F, \|\cdot\|)$ — нормированное поле, V — векторное пространство над F. *Нормой* на V называется отображение $\|\cdot\|_V : V \to [0, +\infty)$, обладающее свойствами:

1) $\|v\|_V = 0 \iff v = 0$;

2) $\|\alpha v\|_V = \|\alpha\| \cdot \|v\|_V$ для любых $\alpha \in F$, $v \in V$;

3) $\|v_1 + v_2\|_V \leqslant \|v_1\|_V + \|v_2\|_V$.

Две нормы $\|\cdot\|_1$ и $\|\cdot\|_2$ на V будем называть *эквивалентными*, если найдутся положительные постоянные A, B, такие что $A\|\cdot\|_1 \leqslant \|\cdot\|_2 \leqslant B\|\cdot\|_1$ (если норма $\|\cdot\|$ на F нетривиальна, то это эквивалентно тому, что нормы порождают одну и ту же топологию, а также тому, что сходимости по этим нормам эквивалентны).

Чтобы отличать новое понятие нормы от старого, будем говорить «векторная норма». Если K — расширение F, то любое продолжение нормы $\|\cdot\|$ на K будет векторной нормой на K.

Теорема 9.2. *Пусть F полно, V — конечномерное векторное пространство над F. Тогда любые две векторные нормы на V эквивалентны.*

Доказательство. Фиксируем базис $e_1, \dots, e_m$. Легко видеть, что функция

$$\|\alpha_1 e_1 + \dots + \alpha_m e_m\|_\infty = \max_{1 \leqslant i \leqslant n} \|\alpha_i\|$$

является векторной нормой. Докажем, что всякая векторная норма $\|\cdot\|_V$ эквивалентна $\|\cdot\|_\infty$.

Неравенство $\|\cdot\|_V \ll \|\cdot\|_\infty$ очевидно:

$$\|v\|_V = \|\alpha_1 e_1 + \dots + \alpha_n e_n\|_V \leqslant \sum_{i=1}^{n} \|\alpha_i\| \|e_i\|_V \leqslant B\|v\|_\infty, \quad B = \sum_{i=1}^{n} \|e_i\|_V.$$

Обратное неравенство $\|\cdot\|_\infty \ll \|\cdot\|_V$ будем доказывать индукцией по размерности m. Случай $m = 1$ тривиален. Пусть $m > 1$.

Допустим противное. Тогда для любого $n \in \mathbb{N}$ найдётся вектор

$$v_n = \alpha_{n,1}e_1 + \dots + \alpha_{n,m}e_m,$$

такой что $\|v_n\|_\infty > n\|v_n\|_V$. Перейдя, если нужно, к подпоследовательности и изменив нумерацию элементов базиса, можно считать, что $\|v_n\|_\infty = 1$, $\alpha_{n,m} = 1$. Тогда $\|v_n\|_V < 1/n$, поэтому $v_n \to 0$ по норме $\|\cdot\|_V$.

Пусть $W = Fe_1 + \dots + Fe_{m-1}$. По предположению индукции, найдётся положительная постоянная C, такая что для любого вектора $w \in W$ выполнено $\|w\|_\infty \leqslant C\|w\|_V$.

Фиксируем $i \in \{1, \dots, m-1\}$. Тогда для любых $n_1, n_2 \in \mathbb{N}$ имеем

$$\|\alpha_{n_1,i} - \alpha_{n_2,i}\| \leqslant \|v_{n_1} - v_{n_2}\|_\infty \leqslant C\|v_{n_1} - v_{n_2}\|_V < C\left(\frac{1}{n_1} + \frac{1}{n_2}\right).$$

Следовательно, последовательность $\alpha_{n,i} \in F$, $n \in \mathbb{N}$, фундаментальна, поэтому существует предел $\alpha_i = \lim\limits_{n\to\infty} \alpha_{n,i} \in F$.

Положим $v = \alpha_1 e_1 + \dots + \alpha_{m-1}e_{m-1} + e_m \neq 0$. Тогда $v_n \to v$ по норме $\|\cdot\|_\infty$, но $\|\cdot\|_V \ll \|\cdot\|_\infty$, поэтому $v_n \to v$ и по норме $\|\cdot\|_V$, что противоречит тому, что $v_n \to 0$ по норме $\|\cdot\|_V$. □

Следствие 9.3. *Пусть F полно, K — алгебраическое расширение F. Тогда существует не более одного продолжения нормы $\|\cdot\|$ с F на K.*

Доказательство. Пусть $\|\cdot\|_1$ и $\|\cdot\|_2$ — продолжения нормы на K. Возьмём любое $\alpha \in K$. Нормы $\|\cdot\|_{1,2}$ являются векторными нормами на $F(\alpha)$, поэтому найдутся положительные постоянные A, B, такие что для любого $n \in \mathbb{N}$ выполнено

$$A\|\alpha^n\|_1 \leqslant \|\alpha^n\|_2 \leqslant B\|\alpha^n\|_1,$$
$$\sqrt[n]{A}\,\|\alpha\|_1 \leqslant \|\alpha\|_2 \leqslant \sqrt[n]{B}\,\|\alpha\|_1.$$

Устремляя $n \to \infty$, получаем $\|\alpha\|_1 = \|\alpha\|_2$. □

Следствие 9.4. *Допустим, что F полно и существует продолжение нормы $\|\cdot\|$ с F на F^{alg}. Пусть $\alpha \in F^{\mathrm{alg}}$, α' — любое сопряжённое к α над F. Тогда $\|\alpha'\| = \|\alpha\|$.*

Доказательство. Рассмотрим вложение $\sigma\colon F(\alpha) \to F^{\mathrm{alg}}$ над F, такое что $\sigma(\alpha) = \alpha'$. Легко видеть, что функция $v(x) = \|\sigma(x)\|$ — норма на $F(\alpha)$, причём для $x \in F$ имеем $v(x) = \|x\|$. Тогда $v(x) = \|x\|$ для всех $x \in F(\alpha)$, в частности, $\|\alpha'\| = v(\alpha) = \|\alpha\|$. □

Следствие 9.5. *Допустим, что F полно и существует продолжение нормы $\|\cdot\|$ с F на F^{alg}. Пусть K — конечное расширение F. Тогда для всех $\alpha \in K$ выполнено*

$$\left\|\mathrm{N}_F^K(\alpha)\right\| = \|\alpha\|^{[K:F]}.$$

Доказательство. Воспользуемся равенством

$$\mathrm{N}_F^K(\alpha) = (\alpha_1 \cdots \alpha_n)^{[K:F(\alpha)]},$$

где $\alpha_1, \dots, \alpha_n$ — все корни минимального многочлена α над F (с учётом кратностей). Для всех i имеем $\|\alpha_i\| = \|\alpha\|$, поэтому

$$\left\|\mathrm{N}_F^K(\alpha)\right\| = \|\alpha\|^{[F(\alpha):F]\cdot[K:F(\alpha)]} = \|\alpha\|^{[K:F]}.$$ □

Упражнение 9.6. Пусть K — конечное расширение полного поля F. Допустим, что существует продолжение нормы $\|\cdot\|$ с F на K. Доказать, что K также полно.

9.2 Продолжение нормы на алгебраическое замыкание

Пусть F полно. Тогда если продолжение нормы на F^{alg} существует, то оно должно задаваться формулой

$$\|\alpha\| = \left\|\mathrm{N}_F^K(\alpha)\right\|^{\frac{1}{[K:F]}},$$

где K — (произвольное) конечное расширение $F(\alpha)$ (заметим, что $\mathrm{N}_F^K(\alpha) \in F$). При этом последнее выражение на самом деле не зависит от выбора расширения K:

$$\left\|\mathrm{N}_F^K(\alpha)\right\|^{\frac{1}{[K:F]}} = \left\|\mathrm{N}_F^{F(\alpha)}(\alpha)\right\|^{\frac{[K:F(\alpha)]}{[K:F]}} = \left\|\mathrm{N}_F^{F(\alpha)}(\alpha)\right\|^{\frac{1}{[F(\alpha):F]}}.$$

Теорема 9.7. *Пусть $(F, \|\cdot\|)$ — полное нормированное поле. Тогда существует единственное продолжение нормы $\|\cdot\|$ с F на F^{alg}, а именно:*

$$\|\alpha\| = \left\|\mathrm{N}_F^{F(\alpha)}(\alpha)\right\|^{\frac{1}{[F(\alpha):F]}}.$$

Более того, для любого конечного расширения $K \supseteq F(\alpha)$ справедлива формула

$$\|\alpha\| = \left\|\mathrm{N}_F^K(\alpha)\right\|^{\frac{1}{[K:F]}}.$$

Напомним, что топологическое пространство называется локально компактным, если любая его точка имеет предкомпактную окрестность. Любое поле с тривиальной нормой локально компактно. Если норма нетривиальна, то локальная компактность поля F эквивалентна компактности единичного замкнутого шара $B_1[0] = \{\alpha \in F : \|\alpha\| \leqslant 1\}$. Например, поля $\mathbb{R}$ и $\mathbb{Q}_p$ локально компактны.

Мы докажем теорему в предположении, что F — локально компактное неархимедово поле с нетривиальной нормой (для тривиальной нормы утверждение тривиально).

Доказательство теоремы для частного случая. Мы уже доказали, что если продолжение существует, то оно должно задаваться указанными формулами, а также то, что последнее выражение не зависит от K. Кроме того, очевидно, что при $\alpha \in F$ эти формулы дают то, что нужно. Остаётся проверить выполнение свойств нормы.

Неравенство $\|\alpha\| > 0$ при $\alpha \neq 0$ очевидно.

Пусть $\alpha, \beta \in F^{\mathrm{alg}}$. Возьмём $K = F(\alpha, \beta)$. Тогда

$$\|\alpha\beta\| = \left\|\mathrm{N}_F^K(\alpha\beta)\right\|^{\frac{1}{[K:F]}} = \left\|\mathrm{N}_F^K(\alpha)\,\mathrm{N}_F^K(\beta)\right\|^{\frac{1}{[K:F]}} = \|\alpha\| \cdot \|\beta\|.$$

Основная сложность — это проверка ультраметрического неравенства

$$\|\alpha + \beta\| \leqslant \max\{\|\alpha\|, \|\beta\|\}.$$

Легко видеть, что оно равносильно такому утверждению: если $\|\gamma\| \leqslant 1$, то $\|1 + \gamma\| \leqslant 1$.

Возьмём $\gamma \in F^{\mathrm{alg}}$, $\|\gamma\| \leqslant 1$, и рассмотрим расширение $K = F(\gamma)$, $m = [K : F]$. Фиксируем базис $1, \gamma, \ldots, \gamma^{m-1}$.

Пусть C — матрица оператора $T_\gamma : x \mapsto \gamma x$. Тогда $\|\det C\| \leqslant 1$. Нам нужно доказать, что $\|\det(I + C)\| \leqslant 1$.

Введём векторную норму $\|\cdot\|_\infty$ на алгебре матриц $A = (a_{i,j}) \in F^{m\times m}$:

$$\|A\|_\infty = \max\|a_{i,j}\|.$$

Ключевую роль в доказательстве нужного неравенства играет следующее утверждение.

Ключевая лемма. $\sup\limits_{n\in\mathbb{N}_0} \|C^n\|_\infty < +\infty$.

Прежде чем доказывать ключевую лемму, выведем из неё нужное неравенство. Пусть $\|C^n\|_\infty \leqslant M$. Тогда для любого $n \in \mathbb{N}$ имеем

$$\|(I+C)^n\|_\infty = \left\|\sum_{k=0}^{n}\binom{n}{k}C^k\right\|_\infty \leqslant \max_k\|C^k\|_\infty \leqslant M,$$

поэтому

$$\|\det(I+C)\|^n = \left\|\det\big((I+C)^n\big)\right\| \leqslant M^m = \text{const}.$$

Извлекая корень n-й степени и устремляя $n \to \infty$, получаем требуемое.

Осталось доказать лемму. Допустим противное. Тогда $\|C^n\|_\infty \to +\infty$ для некоторой последовательности $n = n_k \to \infty$. В дальнейшем под n понимаем n_k.

Пусть $\|C^n\|_\infty = \|a_n\|$, $a_n \in F$. Тогда $\|a_n^{-1}C^n\|_\infty = 1$. В силу компактности единичного шара можно выделить сходящуюся подпоследовательность $a_n^{-1}C^n \to A$.

Легко видеть, что предельная матрица A обладает свойствами:

1) $\det A = 0$;

2) $\|A\|_\infty = 1$ $(\implies A \neq O)$;

3) $AC = CA$.

Поскольку $\det A = 0$, найдётся ненулевой вектор-столбец $v \in F^m$, такой что $Av = 0$. Но тогда

$$AC^i v = C^i A v = 0, \quad i = 0, 1, \dots, m-1.$$

Пусть вектору $v = (v_0\, v_1\, \dots\, v_{m-1})^\mathsf{T}$ отвечает элемент $\alpha = v_0 + v_1\gamma + \dots + v_{m-1}\gamma^{m-1} \in K^*$. Тогда векторам $C^i v$ соответствуют $T_\gamma^i\alpha = \gamma^i\alpha$. Поскольку элементы $\gamma^i\alpha$ образуют базис поля K (над F), то векторы $C^i v$ образуют базис F^m. Но тогда $A = O$. Противоречие. □

Из леммы Гаусса и теоремы 9.7 можно вывести следующий результат о существовании продолжения неархимедовой нормы.

Теорема 9.8. *Пусть K — (произвольное) расширение F, $\|\cdot\|$ — неархимедова норма на F. Тогда норму $\|\cdot\|$ можно продолжить на K.*

Набросок доказательства. Стандартное рассуждение с леммой Цорна позволяет свести общий случай к случаю простого расширения $K = F(\theta)$.

Если элемент θ трансцендентен, то $F(\theta)$ изоморно полю рациональных функций, и существование продолжения следует из леммы Гаусса.

Допустим, что θ алгебраичен, и пусть $\mu_\theta(z)$ — его минимальный многочлен над F. Далее, пусть C — пополнение поля F. Тогда норму $\|\cdot\|$ можно продолжить на алгебраическое замыкание C^{alg}. Фиксируем $\omega \in C^{\text{alg}}$, такое что $\mu_\theta(\omega) = 0$. Тогда существует вложение $\sigma : K \hookrightarrow C^{\text{alg}}$ над F, такое что $\sigma(\theta) = \omega$. В качестве искомого продолжения годится $\|\alpha\| = \|\sigma(\alpha)\|$. □

В заключение приведём идею доказательства теоремы 9.7 в общем случае.

В архимедовом случае всё просто, поскольку есть только два полных архимедовых нормированных поля: $\mathbb{R}$ и $\mathbb{C}$ (см. замечание 1.36).

В неархимедовом случае теорему можно вывести из следующего обобщения леммы Гензеля. Напомним, что для многочлена $P(x) \in \mathbb{Z}_F[x]$ через $\overline{P}(x)$ обозначается его редукция по модулю идеала $\mathfrak{M}_F$: $\overline{P}(x) = P(x) \bmod \mathfrak{M}_F \in k_F[x]$.

Теорема 9.9. *Пусть F — полное неархимедово нормированное поле, $P(x), A_0(x), B_0(x) \in \mathbb{Z}_F[x]$, причём $\overline{P}(x) = \overline{A_0}(x)\overline{B_0}(x)$, н.о.д.$(\overline{A_0}(x), \overline{B_0}(x)) = \overline{1}$, $\overline{A_0}(x) \neq \overline{0}$. Тогда найдутся $A(x), B(x) \in \mathbb{Z}_F[x]$, удовлетворяющие условиям: $P(x) = A(x)B(x)$, $\overline{A}(x) = \overline{A_0}(x)$, $\overline{B}(x) = \overline{B_0}(x)$, $\deg A(x) = \deg \overline{A}(x)$.*

В случае $A_0(x) = x - \alpha_0$ теорема эквивалентна следующему частному случаю леммы Гензеля: если $\|P(\alpha_0)\| < 1$, $\|P'(\alpha_0)\| = 1$, то найдётся $\alpha \in \alpha_0 + \mathfrak{M}_F$, такое что $P(\alpha) = 0$.

Как мы видели, основная сложность в доказательстве теоремы 9.7 — это показать, что из $\|\gamma\| \leqslant 1$ следует $\|1 + \gamma\| \leqslant 1$. Учитывая явную формулу для $\mathrm{N}_F^K(\cdot)$, несложно понять, что это эквивалентно следующему утверждению.

Лемма 9.10. *Пусть F — полное неархимедово нормированное поле, $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in F[x]$ — унитарный неприводимый многочлен, причём $a_0 \in \mathbb{Z}_F$. Тогда $P(x) \in \mathbb{Z}_F[x]$.*

Доказательство. Допустим противное, и пусть $\|a_k\| = \|a_l\| = \|P\| > 1$, причём k и l — соответственно наименьший и наибольший индексы, удовлетворяющие этому условию (так что $0 < k \leqslant l < n$).

Рассмотрим многочлен $Q(x) = a_l^{-1}P(x) \in \mathbb{Z}_F[x]$. Имеем

$$\overline{Q}(x) = x^k(x^{l-k} + \dots + \overline{a_k a_l^{-1}}).$$

Применяя теорему 9.9 ($A_0(x) = x^k$, $B_0(x) = x^{l-k} + \dots + a_k a_l^{-1}$), получаем, что многочлен $Q(x)$ имеет нетривиальный делитель степени k, что противоречит неприводимости $P(x)$. □

Для доказательства теоремы 9.9 понадобится следующее утверждение («непрерывность» деления с остатком), верное для произвольного неархимедова F. (Здесь и ниже полагаем $\deg 0 = -\infty$.)

Лемма 9.11. *Пусть $A(x) \in F[x]$, $B(x) \in \mathbb{Z}_F[x]$, причём многочлен $B(x)$ унитарный. Разделим $A(x)$ на $B(x)$ с остатком: $A(x) = B(x)Q(x) + R(x)$, $\deg R(x) < \deg B(x)$. Тогда $\max\{\|Q\|, \|R\|\} \leqslant \|A\|$.*

Доказательство. Можно считать, что $\|A\| = 1$, а в этом случае утверждение очевидно. □

Пусть многочлены $A_0(x)$ и $B_0(x)$ удовлетворяют условиям теоремы 9.9. Можно считать, что многочлен $A_0(x)$ унитарный. Найдутся многочлены $U(x), V(x) \in \mathbb{Z}_F[x]$, такие что

$$\overline{A_0}(x)\overline{U}(x) + \overline{B_0}(x)\overline{V}(x) = \overline{1}.$$

Положим

$$\varepsilon = \|A_0U + B_0V - 1\| < 1.$$

Ключевую роль в доказательстве теоремы играет следующая лемма.

Лемма 9.12. *Для любого многочлена $R(x) \in F[x]$ найдутся многочлены $S(x), T(x) \in F[x]$, удовлетворяющие условиям: $\deg S(x) \leqslant \max\{\deg R(x) - \deg A_0(x), \deg B_0(x) - 1\}$, $\deg T(x) < \deg A_0(x)$, $\max\{\|S\|, \|T\|\} \leqslant \|R\|$, $\|A_0S + B_0T - R\| \leqslant \varepsilon\|R\|$.*

Доказательство. Положим $W = 1 - A_0U - B_0V$. Тогда $R = R \cdot 1 = A_0RU + B_0RV + RW$, причём $\|RW\| = \|R\| \cdot \|W\| = \varepsilon\|R\|$.

Поделим RV и RW с остатком на A_0. Обозначим остатки через T и W_0 соответственно. Тогда для некоторого многочлена S имеем

$$R = A_0S + B_0T + W_0.$$

Используя это равенство и лемму 9.11 (а также равенство $\|S\| = \|A_0S\|$), несложно убедиться, что многочлены $S(x)$ и $T(x)$ искомые. □

Теперь уже несложно доказать теорему 9.9. Для этого построим две последовательности многочленов $A_n(x), B_n(x) \in \mathbb{Z}_F[x]$ (где многочлены A_0 и B_0 — из условия теоремы). При этом можно считать, что $\deg B_0 = \deg \overline{B_0} \leqslant \deg P - \deg A_0$ (как и выше, считаем, что многочлен A_0 унитарный).

Пусть A_n и B_n уже построены. Применим лемму 9.12 к многочлену $R = R_n = P - A_n B_n$. Обозначим через S_n, T_n соответствующие многочлены из леммы и положим $A_{n+1} = A_n + T_n$, $B_{n+1} = B_n + S_n$.

Обозначим

$$\varepsilon_1 = \max\{\varepsilon, \|P - A_0 B_0\|\} < 1.$$

С помощью индукции можно проверить свойства:

- многочлен A_n унитарный, $\deg A_n = \deg A_0$, $\deg B_n \leqslant \deg P - \deg A_0$;
- $\|P - A_n B_n\| \leqslant \varepsilon_1^{n+1}$;
- $\max\{\|A_{n+1} - A_n\|, \|B_{n+1} - B_n\|\} \leqslant \varepsilon_1^{n+1}$ (в частности, $\max\{\|A_n - A_0\|, \|B_n - B_0\|\} \leqslant \varepsilon_1$).

Следовательно, многочлены $A = \lim A_n$, $B = \lim B_n$ искомые.

Оставляем детали проверки заинтересованному читателю.

Глава 10

Полное алгебраически замкнутое расширение

Для нужд p-адического анализа хотелось бы иметь полное и алгебраически замкнутое расширение поля $\mathbb{Q}$ (с нормой, продолжающей p-адическую норму $|\cdot|_p$) — неархимедов аналог поля комплексных чисел. В отличие от архимедова случая, алгебраическое замыкание поля $\mathbb{Q}_p$ на эту роль не годится.

Теорема 10.1 (без доказательства)**.** *Пусть F — локально компактное неархимедово поле с нетривиальной нормой. Тогда его алгебраическое замыкание F^{alg} неполно.* □

К счастью, не всё так плохо.

Теорема 10.2. *Пополнение алгебраически замкнутого нормированного поля алгебраически замкнуто.*

Доказательство. Для простоты ограничимся неархимедовым случаем.

Пусть Ω — пополнение K, причём K алгебраически замкнуто.

Возьмём непостоянный многочлен

$$P(z) = z^m + a_{m-1}z^{m-1} + \cdots + a_0 \in \Omega[z].$$

Найдётся последовательность многочленов

$$P_n(z) = z^m + a_{n,m-1}z^{m-1} + \cdots + a_{n,0} \in K[z],$$
$$\|P_n - P\| \xrightarrow[n\to\infty]{} 0.$$

Поскольку K алгебраически замкнуто, каждый из P_n раскладывается на линейные множители:

$$P_n(z) = \prod_{k=1}^{m}(z - \rho_{n,k}), \quad \rho_{n,k} \in K.$$

Наша цель — построить последовательность Коши ρ_{n,k_n} из корней многочленов P_n.

Положим $k_1 = 1$. Если k_n уже выбрано, то в качестве $\rho_{n+1,k_{n+1}}$ возьмём (произвольный) корень P_{n+1}, ближайший к ρ_{n,k_n}.

Поскольку $\|P_n - P\| \to 0$, то коэффициенты многочленов P_n ограничены, поэтому ограничены и все их корни: $\|\rho_{n,k}\| \leqslant A$ (см. доказательство утверждения 1.28). Будем считать, что $A \geqslant 1$.

Поскольку

$$P_{n+1}(\rho_{n,k_n}) - P_n(\rho_{n,k_n}) = P_{n+1}(\rho_{n,k_n}) = \prod_{k=1}^{m}(\rho_{n,k_n} - \rho_{n+1,k}),$$

то

$$\left\|\rho_{n,k_n} - \rho_{n+1,k_{n+1}}\right\|^m \leqslant \left\|P_{n+1}(\rho_{n,k_n}) - P_n(\rho_{n,k_n})\right\| \leqslant \|P_{n+1} - P_n\| \cdot A^{m-1} \to 0, \quad n \to \infty.$$

Следовательно, последовательность ρ_{n,k_n} фундаментальна, поэтому существует предел $\rho = \lim \rho_{n,k_n} \in \Omega$.

Имеем

$$P(\rho) = \lim_{n\to\infty} P_n(\rho_{n,k_n}) = 0,$$

то есть многочлен P имеет корень в Ω. □

Упражнение 10.3. Доказать теорему 10.2 для архимедовых полей.

Итого, имеем цепочку (башню) расширений

$$\mathbb{Q} \underset{\text{пополнение}}{\subseteq} \mathbb{Q}_p \subseteq \mathbb{Q}_p^{\text{alg}} \underset{\text{пополнение}}{\subseteq} \mathbb{C}_p,$$

где через $\mathbb{C}_p$ обозначено пополнение алгебраического замыкания поля $\mathbb{Q}_p$. Согласно теореме 10.2, $\mathbb{C}_p$ и будет искомым полным алгебраически замкнутым расширением $\mathbb{Q}$. (Легко видеть, что $\mathbb{C}_p$ — минимальное такое расширение. При этом каждое расширение в цепочке однозначно с точностью до изометрического изоморфизма.)

Упражнение 10.4. Найти группу $G_{\mathbb{C}_p}$ и поле вычетов $k_{\mathbb{C}_p}$ (последнее — с точностью до изоморфизма).

Глава 11

Арифметика конечных расширений

Для простоты всюду в этой главе F — локально компактное неархимедово поле с нетривиальной нормой $\|\cdot\|$.

Напомним, что локальная компактность F означает компактность $\mathbb{Z}_F$ (если норма нетривиальна), которая эквивалентна тому, что поле F полно, группа G_F дискретна (то есть циклическая) и поле вычетов k_F конечно.

Фиксируем конечное расширение K поля F степени $[K : F] = n$.

Возьмём какой-нибудь базис K над F и рассмотрим векторную норму $\|\cdot\|_\infty$. Относительно этой нормы K локально компактно. Поскольку норма $\|\cdot\|$ эквивалентна $\|\cdot\|_\infty$, то K локально компактно и по норме $\|\cdot\|$. Следовательно, поле K полно (ср. с упражнением 9.6), группа G_K дискретна, и поле вычетов k_K конечно (что несложно доказать и непосредственно).

Целое замыкание кольца целых

Определение 11.1. Пусть $A \subseteq B$ — коммутативные ассоциативные кольца с 1 (причём единичный элемент 1 общий). Элемент $b \in B$ называется *целым над* A, если b является корнем некоторого унитарного многочлена $P(z) = z^m + a_{m-1}z^{m-1} + \cdots + a_0 \in A[z]$, Можно доказать, что множество всех элементов B, целых над A, является кольцом. Оно называется *целым замыканием* кольца A в кольце B.

Лемма 11.2. *Пусть $\alpha \in K$. Тогда следующие условия эквивалентны:*

1) *α цел над $\mathbb{Z}_F$;*
2) *$\mu_\alpha(z) \in \mathbb{Z}_F[z]$ (где $\mu_\alpha(z)$ — минимальный многочлен α над F);*
3) *$\alpha \in \mathbb{Z}_K$.*

(*Таким образом, $\mathbb{Z}_K$ — целое замыкание $\mathbb{Z}_F$ в K.*)

Доказательство. Докажем импликации $1 \implies 2 \implies 3 \implies 1$.

$1 \implies 2$. Пусть $P(\alpha) = 0$, где $P(z) \in \mathbb{Z}_F[z]$ унитарный. Тогда $P(z) = \mu_\alpha(z)Q(z)$ для некоторого $Q(z) \in F[z]$. По следствию 7.7 из леммы Гаусса, имеем $\mu_\alpha(z) \in \mathbb{Z}_F[z]$.

$2 \Longrightarrow 3$. Из явных формул $\|\alpha\| = \left\|\mathrm{N}_F^{F(\alpha)}(\alpha)\right\|^{1/n}$ и $\mathrm{N}_F^{F(\alpha)}(\alpha) = \pm\mu_\alpha(0)$ получаем $\|\alpha\| \leqslant 1$, то есть $\alpha \in \mathbb{Z}_K$.

$3 \Longrightarrow 1$. Рассмотрим минимальный многочлен α над F:

$$\mu_\alpha(z) = z^m + a_{m-1}z^{m-1} + \cdots + a_0 = \prod_{i=1}^{m}(z - \alpha_i), \quad \alpha_k \in F^{\mathrm{alg}}.$$

Тогда $\|\alpha_i\| = \|\alpha\| \leqslant 1$ для всех i, поэтому $\|a_i\| \leqslant 1$ для всех i, то есть $\mu_\alpha(z) \in \mathbb{Z}_F[z]$. □

Индекс ветвления

Из формулы

$$\|\alpha\| = \left\|\mathrm{N}_F^{F(\alpha)}(\alpha)\right\|^{1/n}$$

получаем $G_F \subseteq G_K \subseteq G_F^{1/n}$. Поскольку группа G_F циклическая, найдётся натуральное число $e \mid n$, такое что $G_K = G_F^{1/e}$. Эквивалентно: $\|\pi_K\| = \|\pi_F\|^{1/e}$, где π_F и π_K — униформизующие элементы колец $\mathbb{Z}_F$ и $\mathbb{Z}_K$ соответственно.

Определение 11.3. Число $e = e_{K/F}$ называется *индексом ветвления* расширения K/F.

Если $F \subseteq K \subseteq L$ — башня конечных расширений, то очевидно, что $e_{L/F} = e_{K/F} \cdot e_{L/K}$.

Определение 11.4. Расширение K/F называется *неразветвлённым*, если $e_{K/F} = 1$, и *вполне разветвлённым*, если $e_{K/F} = [K : F]$.

Определение 11.5. Многочлен $P(z) = z^m + a_{m-1}z^{m-1} + \ldots + a_0 \in \mathbb{Z}_F[z]$ будем называть *многочленом Эйзенштейна* над F, если все $a_i \in \mathfrak{M}_F$, причём $a_0\mathbb{Z}_F = \mathfrak{M}_F$.

Следующая теорема описывает все вполне разветвлённые расширения F.

Теорема 11.6.

1) *Если K — вполне разветвлённое расширение F, то $K = F(\pi_K)$, где π_K — (произвольный) униформизующий элемент кольца $\mathbb{Z}_K$, причём минимальный многочлен π_K над F является многочленом Эйзенштейна над F.*

2) *Если $P(z)$ — многочлен Эйзенштейна над F, то $P(z)$ неприводим над F. Более того, если $P(\pi) = 0$, $\pi \in F^{\mathrm{alg}}$, то $K = F(\pi)$ — вполне разветвлённое расширение F, причём π — униформизующий элемент кольца $\mathbb{Z}_K$.*

Доказательство.

1) Для краткости обозначим $\pi = \pi_K$. Рассмотрим его минимальный многочлен

$$\mu_\pi(z) = z^m + a_{m-1}z^{m-1} + \cdots + a_0 = \prod_{i=1}^{m}(z - \pi_i).$$

Имеем $\|a_0\| = \|\pi\|^m = \|\pi_F\|^{m/n}$, откуда $m/n \in \mathbb{N}$, то есть $m = [F(\pi) : F] \geqslant n = [K : F]$. Следовательно, $K = F(\pi)$ и $m = n$. Поскольку $\|\pi_i\| = \|\pi\| < 1$ для всех i, то $\|a_i\| < 1$ для всех i (теорема Виета), причём $\|a_0\| = \|\pi_F\|$, то есть a_0 — униформизующий элемент кольца $\mathbb{Z}_F$. Значит, $\mu_\pi(z)$ — многочлен Эйзенштейна над F.

2) Допустим противное: $P(z) = A(z)B(z)$, где

$$A(z) = z^k + a_{k-1}z^{k-1} + \dots + a_0 \in F[z],$$
$$B(z) = z^l + b_{l-1}z^{l-1} + \dots + b_0 \in F[z].$$

По следствию из леммы Гаусса, имеем $A(z), B(z) \in \mathbb{Z}_F[z]$. Следовательно, можно рассмотреть редукцию по модулю идеала $\mathfrak{M}_F$:

$$z^{k+l} = \overline{P}(z) = \overline{A}(z)\overline{B}(z) \in k_F[z],$$

откуда $\overline{A}(z) = z^k$, $\overline{B}(z) = z^l$. В частности, $a_0, b_0 \in \mathfrak{M}_F$, откуда $P(0) = a_0 b_0 \in \mathfrak{M}_F^2$ — противоречие с определением многочлена Эйзенштейна.

Если $P(\pi) = 0$, $\deg P = n$, то $\|\pi\| = \|\pi_F\|^{1/n}$, откуда $e = e_{K/F} \geqslant n$. Поскольку $e \mid n$, то $e = n$ и π — униформизующий элемент кольца $\mathbb{Z}_K$. □

Упражнение 11.7. Пусть K — вполне разветвлённое расширение F степени n, причём $p \nmid n$, где $p = \operatorname{char} k_F$ (если $p \nmid e_{K/F}$, то расширение K/F называется *слабо разветвлённым*). Доказать, что найдётся униформизующий элемент кольца $\mathbb{Z}_K$, минимальный многочлен которого над F имеет вид $z^n + a_0$. Другими словами, найдутся униформизующие элементы π_F и π_K, такие что $\pi_F = \pi_K^n$. (*Указание.* Использовать лемму Гензеля.)

Упражнение 11.8. Пусть p — простое число, $a \in \mathbb{Z}_p$, причём $\nu_p(a) = 1$. Доказать, что многочлен $P(z) = z^p - (1 + a)$ неприводим над $\mathbb{Q}_p$, причём если $P(\alpha) = 0$, $\alpha \in \mathbb{Q}_p^{\text{alg}}$, то $\mathbb{Q}_p(\alpha)$ — вполне разветвлённое расширение $\mathbb{Q}_p$. (*Указание.* Рассмотреть $P(z + 1)$.)

Поля вычетов

Напомним (см. главу 6), что есть естественное вложение полей вычетов $k_F \hookrightarrow k_K$ $(a + \mathfrak{M}_F \mapsto a + \mathfrak{M}_K)$, поэтому удобно считать, что k_K — расширение k_F.

Дальше для краткости будем обозначить $\overline{\alpha} = \alpha \bmod \mathfrak{M}_K = \alpha + \mathfrak{M}_K \in k_K$, $\alpha \in \mathbb{Z}_K$.

Лемма 11.9. $[k_K : k_F] \leqslant [K : F]$.

Доказательство. Очевидно. Действительно, пусть $\overline{\alpha_1}, \dots, \overline{\alpha_m} \in k_K$ линейно независимы над k_F, $\alpha_i \in \mathbb{Z}_K$. Докажем, что $\alpha_1, \dots, \alpha_m$ линейно независимы над F.

Допустим противное:

$$a_1\alpha_1 + \dots + a_m\alpha_m = 0, \tag{11.1}$$

где $a_i \in F$ не все равны 0. Поделив на максимальный коэффициент, можно считать, что $\max\|a_i\| = 1$, в частности, $a_i \in \mathbb{Z}_F$. Рассматривая равенство (11.1) по модулю $\mathfrak{M}_K$, получаем линейную зависимость $\overline{\alpha_1}, \dots, \overline{\alpha_m}$ над k_F. □

Обозначение 11.10. $f_{K/F} = [k_K : k_F]$.

Если $F \subseteq K \subseteq L$ — башня конечных расширений, то очевидно, что $f_{L/F} = f_{K/F} \cdot f_{L/K}$.

Базис кольца целых

Пусть $e = e_{K/F}$, $f = f_{K/F}$.

Теорема 11.11. *Пусть π_K — униформизующий элемент кольца $\mathbb{Z}_K$, $\overline{\omega_1}, \dots, \overline{\omega_f}$ — базис k_K над k_F ($\omega_j \in \mathbb{Z}_K$). Тогда $\pi_K^i \omega_j$ $(0 \leqslant i \leqslant e-1, 1 \leqslant j \leqslant f)$ — базис $\mathbb{Z}_K$ как свободного $\mathbb{Z}_F$-модуля, то есть для любого $\alpha \in \mathbb{Z}_K$ существует единственное представление вида*

$$\alpha = \sum_{i=0}^{e-1} \sum_{j=1}^{f} a_{i,j} \pi_K^i \omega_j, \quad a_{i,j} \in \mathbb{Z}_F.$$

Доказательство. Фиксируем униформизующий элемент π_F кольца $\mathbb{Z}_F$. Справедливо равенство $\|\pi_F\| = \|\pi_K^e\|$, поэтому $\pi_F \mid \pi_K^e$ и $\pi_K^e \mid \pi_F$.

Пусть $\alpha \in \mathbb{Z}_K$. Разложим $\overline{\alpha} \in k_K$ по базису $\overline{\omega_1}, \dots, \overline{\omega_f}$:

$$\overline{\alpha} = \sum_{j=1}^{f} \overline{c_j} \cdot \overline{\omega_j}, \quad c_j \in \mathbb{Z}_F.$$

Тогда

$$\alpha \equiv \sum_{j=1}^{f} c_j \omega_j \pmod{\mathfrak{M}_K = \pi_K \mathbb{Z}_K},$$

то есть

$$\frac{\alpha - \sum_j c_j \omega_j}{\pi_K} \in \mathbb{Z}_K.$$

Повторяя этот процесс e раз, найдём $c_{i,j} \in \mathbb{Z}_F$, такие что

$$\alpha \equiv \sum_{i=0}^{e-1} \left(\sum_{j=1}^{f} c_{i,j} \omega_j \right) \pi_K^i \pmod{\pi_K^e \mathbb{Z}_K = \pi_F \mathbb{Z}_K},$$

откуда

$$\frac{\alpha - \sum_{i,j} c_{i,j} \pi_K^i \omega_j}{\pi_F} \in \mathbb{Z}_K.$$

Снова итерируя этот процесс, для произвольного $N \in \mathbb{N}$ можно найти $c_{i,j,k} \in \mathbb{Z}_F$, такие что

$$\alpha \equiv \sum_{k=0}^{N-1} \left(\sum_{i=0}^{e-1} \sum_{j=1}^{f} c_{i,j,k} \pi_K^i \omega_j \right) \pi_F^k \pmod{\pi_F^N \mathbb{Z}_K}.$$

Устремляя $N \to \infty$, получаем

$$\alpha = \sum_{i=0}^{e-1} \sum_{j=1}^{f} a_{i,j} \pi_K^i \omega_j,$$

где

$$a_{i,j} = \sum_{k=0}^{\infty} c_{i,j,k} \pi_F^k \in \mathbb{Z}_F.$$

Таким образом, элементы $\pi_K^i \omega_j$ $(0 \leqslant i \leqslant e-1, 1 \leqslant j \leqslant f)$ порождают $\mathbb{Z}_K$ как $\mathbb{Z}_F$-модуль. Осталось проверить линейную независимость.

Допустим противное:

$$\sum_{i=0}^{e-1} \sum_{j=1}^{f} a_{i,j} \pi_K^i \omega_j = 0,$$

где $a_{i,j} \in \mathbb{Z}_F$ не все равны 0. Можно считать, что $\max \|a_{i,j}\| = 1$. Пусть i_0 — наименьшее i, для которого найдётся j, такое что $\|a_{i,j}\| = 1$. Заметим, что если $i < i_0$, то для всех j верно $a_{i,j} \in \pi_F \mathbb{Z}_F \subseteq \pi_K^e \mathbb{Z}_K$. Следовательно,

$$\sum_{j=1}^{f} a_{i_0,j} \pi_K^{i_0} \omega_j \equiv 0 \pmod{\pi_K^{i_0+1}} \implies \sum_{j=1}^{f} \overline{a_{i_0,j}} \cdot \overline{\omega_j} = \overline{0},$$

то есть $\overline{\omega_j}$ линейно зависимы над k_F. Противоречие. □

Следствие 11.12. *В обозначениях теоремы 11.11 имеем: $\pi_K^i \omega_j$ $(0 \leqslant i \leqslant e-1, 1 \leqslant j \leqslant f)$ — базис K над F.* □

Следствие 11.13. $[K : F] = ef$. □

Следствие 11.14.

1) *Расширение K/F неразветвлено тогда и только тогда, когда $f_{K/F} = [K : F]$.*
2) *Расширение K/F вполне разветвлено тогда и только тогда, когда $f_{K/F} = 1$ (то есть когда $k_K = k_F$).* □

Неразветвлённые расширения

Пусть $k_F \cong \mathbb{F}_q$, $p = \operatorname{char} k_F$ ($\|p\| < 1$, q — степень p). Тогда $k_K \cong \mathbb{F}_{q^f}$, $f = f_{K/F}$.

Теорема 11.15. *Для любого $f \in \mathbb{N}$ существует единственное неразветвлённое расширение F_f поля F степени f, а именно: $F_f = F(\zeta)$, где ζ — (произвольный) примитивный корень из 1 степени $q^f - 1$. Более того, если K — произвольное конечное расширение F с $f_{K/F} = f$, то $F_f \subseteq K$, причём расширение K/F_f вполне разветвлено.*

Замечание 11.16. Примитивный корень из 1 степени N существует (в F^{alg}) тогда и только тогда, когда N не делится на $\operatorname{char} F$. Если $\operatorname{char} F > 0$, то $\operatorname{char} F = \operatorname{char} k_F = p \nmid q^f - 1$, так что ζ действительно существует. При этом расширение $F(\zeta)$ не зависит от выбора ζ.

Замечание 11.17. Итого имеем башню расширений $F \subseteq F_f \subseteq K$, где расширение F_f/F неразветвлённое, а расширение K/F_f вполне разветвлённое.

Доказательство теоремы. Сперва докажем, что неразветвлённое расширение степени f существует.

Рассмотрим какое-нибудь поле $\mathbb{F}_{q^f} \supseteq \mathbb{F}_q = k_F$. Имеем: $\mathbb{F}_{q^f}^* = \langle g \rangle$. Тогда $\mathbb{F}_{q^f} = k_F(g)$ и минимальный многочлен $\mu_g(z) \in k_F[z]$ элемента g над k_F имеет степень f.

Возьмём (любой) унитарный многочлен $\mu(z) \in \mathbb{Z}_F[z]$, такой что $\overline{\mu}(z) = \mu_g(z)$. Пусть $\mu(\alpha) = 0$, $\alpha \in F^{\mathrm{alg}}$. Рассмотрим $K = F(\alpha)$. Заметим, что $\alpha \in \mathbb{Z}_K$ (так как α цел над $\mathbb{Z}_F$).

Поскольку $\overline{\mu}(\overline{\alpha}) = \overline{0}$, то $[k_F(\overline{\alpha}) : k_F] = f$. Получаем:

$$[K : F] \geqslant [k_K : k_F] \geqslant [k_F(\overline{\alpha}) : k_F] = f \geqslant [K : F],$$

откуда $f_{K/F} = [K : F] = f$, то есть K — искомое неразветвлённое расширение.

Пусть K — произвольное неразветвлённое расширение F степени f. Тогда $k_K \cong \mathbb{F}_{q^f}$. Пусть $k_K^* = \langle \overline{\alpha} \rangle$, $\alpha \in \mathbb{Z}_K$.

Рассмотрим многочлен $P(z) = z^N - 1$, $N = q^f - 1$. Тогда $\overline{P(\alpha)} = \overline{0} \neq \overline{P'(\alpha)}$, откуда $\|P(\alpha)\| < 1 = \|P'(\alpha)\|^2$. По лемме Гензеля, найдётся $\zeta \in \overline{\alpha}$, такое что $P(\zeta) = 0$. При этом все степени $\overline{\zeta^i} = \overline{\alpha}^i \in k_K$, $0 \leqslant i < N$, различны, так что ζ — примитивный корень из 1 степени N, то есть $F(\zeta) \subseteq K$. Имеем:

$$f = [K : F] \geqslant [F(\zeta) : F] \geqslant [k_F(\overline{\zeta}) : k_F] = [k_F(\overline{\alpha}) : k_F] = f,$$

откуда $K = F(\zeta)$. Единственность и явный вид F_f установлены.

Наконец, пусть K — произвольное конечное расширение с $f_{K/F} = f$ (то есть $k_K \cong \mathbb{F}_{q^f}$).

Для некоторого $\alpha_0 \in \mathbb{Z}_K$ имеем $k_K^* = \langle \overline{\alpha_0} \rangle$. Пусть $\overline{\mu}(z)$ — минимальный многочлен $\overline{\alpha_0}$ над k_F (где $\mu(z) = z^f + \dots \in \mathbb{Z}_F[z]$). Заметим, что

$$\overline{\mu}(z) \mid z^{q^f} - z,$$

поэтому $\overline{\mu}(z)$ не имеет кратных корней. По лемме Гензеля, найдётся $\alpha \in \overline{\alpha_0}$, такое что $\mu(\alpha) = 0$. По доказанному выше, $F(\alpha)$ — неразветвлённое расширение F степени f, следовательно, $F_f = F(\alpha) \subseteq K$.

Рассматривая башню $F \subseteq F_f \subseteq K$, получаем $f_{K/F_f} = 1$, то есть расширение K/F_f вполне разветвлено. □

Лемма Краснера

Лемма 11.18 (лемма Краснера)**.** *Пусть $\alpha, \beta \in F^{\mathrm{alg}}$, причём минимальный многочлен α над F не имеет кратных корней, $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ — все сопряжённые к α над F ($n = \deg_F \alpha$). Допустим, что $\|\alpha - \beta\| \neq \|\alpha_i - \beta\|$ при всех $i = 2, \dots, n$. Тогда $\alpha \in F(\beta)$.*

Замечание 11.19. Обычно требуют $\|\alpha - \beta\| < \|\alpha_i - \beta\|$ или, эквивалентно, $\|\alpha - \beta\| < \|\alpha - \alpha_i\|$ (эквивалентность следует из равенства $\alpha - \beta = (\alpha - \alpha_i) + (\alpha_i - \beta)$). На самом деле лемма была доказана Островским до Краснера.

Доказательство леммы. Пусть $K = F(\beta)$. Допустим, что $\alpha \notin K$. Тогда $[K(\alpha) : K] > 1$, то есть $\deg \mu_{\alpha,K}(z) > 1$. Однако $\mu_{\alpha,K}(z) \mid \mu_{\alpha,F}(z)$, поэтому найдётся $i > 1$, такое что α_i является сопряжённым к α над K. Возьмём вложение $\sigma : K(\alpha) \to F^{\mathrm{alg}}$ над K, такое что $\sigma(\alpha) = \alpha_i$. Тогда $\sigma(\alpha - \beta) = \alpha_i - \beta$, поэтому $\|\alpha - \beta\| = \|\alpha_i - \beta\|$ (см. следствие 9.4). Противоречие. □

Непрерывность алгебраических функций

Теорема 11.20. *Для любых $n \in \mathbb{N}$, $M \geqslant 1$, $\varepsilon > 0$ существует $\delta = \delta(n, M, \varepsilon) > 0$, такое что справедливо следующее утверждение. Пусть $f(z), g(z) \in F[z]$ — унитарные многочлены степени n, $\|f\| \leqslant M$, $\|f - g\| \leqslant \delta$. Тогда для любого корня $\alpha \in F^{\mathrm{alg}}$ многочлена $f(z)$ найдётся корень $\beta \in F^{\mathrm{alg}}$ многочлена $g(z)$, такой что $\|\alpha - \beta\| \leqslant \varepsilon$. И обратно: для любого β найдётся α.*

Доказательство. Положим $\delta = \min\{M, (\varepsilon/M)^n\}$. Тогда $\|g\| \leqslant M$, так что условие симметрично относительно многочленов $f(z)$ и $g(z)$.

Аналогично доказательству утверждения 1.28 получаем $\|\alpha\| \leqslant M$, а тогда рассуждения из доказательства теоремы 10.2 дают

$$\|\alpha - \beta\| \leqslant \|f(\alpha) - g(\alpha)\|^{1/n} \leqslant (\delta M^n)^{1/n} \leqslant \varepsilon$$

для некоторого β. □

Следствие 11.21. *Если в условиях теоремы 11.20 все корни многочлена f различны, то при достаточно малом $\delta = \delta(f) > 0$ все корни $g(z)$ также различны и соответствие $\alpha \leftrightarrow \beta$ взаимно однозначно.* □

Следствие 11.22. *Пусть* $\operatorname{char} F = 0$, *$f(z) \in F[z]$ — унитарный неприводимый над F многочлен степени n. Тогда существует $\delta = \delta(f) > 0$, такое что если $g(z)$ — унитарный многочлен степени n, $\|f - g\| \leqslant \delta$, то $g(z)$ неприводим, причём можно так занумеровать корни α_i, β_i многочленов $f(z)$ и $g(z)$ соответственно, что $F(\alpha_i) = F(\beta_i)$ при всех i.*

Доказательство. По лемме Краснера, при достаточно малом $\varepsilon > 0$ будет выполнено $F(\alpha_i) \subseteq F(\beta_i)$. Но тогда

$$n = [F(\alpha_i) : F] \leqslant [F(\beta_i) : F] \leqslant n,$$

откуда $F(\alpha_i) = F(\beta_i)$ и $g(z)$ — минимальный многочлен для β_i. □

Следствие 11.23. *Пусть* $\operatorname{char} F = 0$. *Тогда для любого $n \in \mathbb{N}$ существует лишь конечное число расширений F степени n.*

Доказательство. По теореме 11.15, достаточно рассматривать вполне разветвлённые расширения, которые порождаются корнями многочленов Эйзенштейна. Поскольку множество многочленов Эйзенштейна фиксированной степени компактно, то из следствия 11.22 получаем требуемое. □

Упражнение 11.24. Описать все квадратичные расширения (расширения степени 2) поля $\mathbb{Q}_p$:

1) Если $p > 2$, то существует ровно три квадратичных расширения поля $\mathbb{Q}_p$, а именно: $\mathbb{Q}_p(\sqrt{a}\,)$, $\mathbb{Q}_p(\sqrt{p}\,)$, $\mathbb{Q}_p(\sqrt{ap}\,)$, где $a \in \{1, \dots, p-1\}$ — (произвольный) квадратичный невычет по модулю p.

2) Существует ровно семь квадратичных расширений поля $\mathbb{Q}_2$, а именно: $\mathbb{Q}_2(\sqrt{-1}\,)$, $\mathbb{Q}_2(\sqrt{\pm 3}\,)$, $\mathbb{Q}_2(\sqrt{\pm 2}\,)$, $\mathbb{Q}_2(\sqrt{\pm 6}\,)$.

Какие из этих расширений неразветвлённые?

Бонус: доказательство неполноты F^{alg}

Для полноты (no pun intended) изложения приведём набросок доказательства теоремы 10.1.

Фиксируем униформизующий элемент $\pi = \pi_F$ кольца $\mathbb{Z}_F$.

Для $n \in \mathbb{N}_0$ пусть ζ_n — примитивный корень из 1 степени $q^{2^n} - 1$, так что $K_n = F(\zeta_n)$ — неразветвлённое расширение F степени 2^n. Очевидно, что если $m < n$, то $K_m \subseteq K_n$.

Заметим, что расширение K_n/F нормально, причём если σ — нетривиальный автоморфизм K_n над F, то $\sigma(\zeta_n) \not\equiv \zeta_n \pmod{\mathfrak{M}}$, где $\mathfrak{M} = \mathfrak{M}_{K_n}$ (см. доказательство теоремы 11.15; это обобщение представителей Тейхмюллера).

Рассмотрим последовательность вида

$$\alpha_N = \sum_{n=0}^{N} \zeta_n \pi^{k_n} \in F^{\mathrm{alg}},$$

где целые $0 = k_0 < k_1 < k_2 < \cdots$ выберем позже. Она фундаментальна.

Заметим, что $\alpha_N \in K_N$. Предположим, что $F(\alpha_N) \neq K_N$. Тогда найдётся автоморфизм σ поля K_N над $F(\alpha_N)$, такой что $\sigma(\zeta_N) \neq \zeta_N$. Рассмотрим наименьшее $m \leqslant N$, для которого $\sigma(\zeta_m) \neq \zeta_m$. Тогда

$$\sigma(\alpha_N) = \sum_{n=0}^{N} \sigma(\zeta_n)\pi^{k_n} \not\equiv \sum_{n=0}^{N} \zeta_n \pi^{k_n} = \alpha_N \pmod{\pi^{k_m+1}},$$

что противоречит равенству $\sigma(\alpha_N) = \alpha_N$. Следовательно, $F(\alpha_N) = K_N$ (при любом выборе k_n).

Пусть $k_0, \ldots, k_n$ выбраны. Найдётся целое $k_{n+1} > k_n$, такое что α_n не удовлетворяет никакому сравнению вида

$$c_{2^n-1}\alpha_n^{2^n-1} + \cdots + c_0 \equiv 0 \pmod{\pi^{k_{n+1}}}, \quad c_i \in \mathbb{Z}_F,\ \max\|c_i\| = 1,$$

потому что иначе (по компактности) α_n было бы корнем ненулевого многочлена $P(z) \in F[z]$ степени не выше $2^n - 1$.

Предположим, что существует предел $\lim \alpha_n = \alpha \in F^{\mathrm{alg}}$. Тогда α удовлетворяет уравнению вида

$$c_m\alpha^m + \cdots + c_0 = 0, \quad c_i \in \mathbb{Z}_F,\ \max\|c_i\| = 1,$$

откуда

$$c_m\alpha_n^m + \cdots + c_0 \equiv 0 \pmod{\pi^{k_{n+1}}},$$

что противоречит выбору k_{n+1}, если $2^n - 1 \geqslant m$.

Приложение А

Программа осеннего семестра

1) Нормированные поля. Неархимедовы нормы. Эквивалентность норм. Нормы на поле рациональных чисел (теорема Островского).
2) Пополнение нормированного поля. Поле p-адических чисел. Стандартное представление p-адического числа.
3) Теорема о слабой аппроксимации.
4) Сходимость последовательностей и рядов в полных неархимедовых нормированных полях. Пример: представители Тейхмюллера.
5) Лемма Гензеля. Примеры: представители Тейхмюллера, извлечение корней.
6) Компактность кольца целых.
7) Лемма Гаусса и продолжение нормы на поле рациональных функций.
8) Существование и единственность продолжения нормы на алгебраическое замыкание; явный вид продолжения.
9) Построение полного алгебраически замкнутого расширения.
10) Целое замыкание кольца целых в конечном расширении.
11) Индекс ветвления и степень поля вычетов конечного расширения. Многочлены Эйзенштейна и вполне разветвлённые расширения. Неразветвлённые расширения. Описание произвольного конечного расширения в терминах неразветвлённых и вполне разветвлённых.
12) Лемма Краснера.
13) Непрерывность корней многочленов как функций от коэффициентов (непрерывность алгебраических функций).