Введение в p-адический анализ

и. рочев

17 апреля 2020 г.

Оглавление

Вместо предисловия

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

В основном я буду 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.

Дополнительные сведения можно почерпнуть, например, в книжке

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

Возможно, имеет смысл добавить:

- хорошие примеры на арифметические операции с p-адическими числами (в стандартном представлении);
- 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 (разрезание квадрата на равновеликие треугольники; из $a_1, \dots, a_n \in \mathbb{Q}$, $a_1^k + \dots + a_n^k \in \mathbb{Z}$ при всех $k \in \{1, \dots, n\}$ следует, что все $a_j \in \mathbb{Z}$);

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) существует постоянная $C > 0$, такая что для любых $x, y \in F$ выполнено

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

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

Замечание 1.2. Это определение не совсем стандартно. Обычно вместо свойства 3 требуют, чтобы выполнялось *неравенство треугольника*

$$\|x + y\| \leqslant \|x\| + \|y\|. \tag{1.1}$$

Понятно, что из неравенства треугольника следует свойство 3 с постоянной $C = 2$. Ниже мы увидим (предложение 1.11), что верно и обратное. Неравенство треугольника позволяет определить метрику $d(x, y) = \|x - y\|$. Вообще, любая норма задаёт топологию стандартным образом (в качестве базы топологии берутся открытые шары), причём эта топология метризуема (норму можно заменить на эквивалентную, удовлетворяющую нер-ву треугольника; см. ниже).

Пример 1.3. Если $F \subseteq \mathbb{C}$, то можно взять $\|\cdot\| = |\cdot|$ (обычный модуль).

Пример 1.4. На любом поле можно ввести *тривиальную норму*

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

Упражнение 1.5. Доказать, что если поле F конечно, то на нём не существует нетривиальной (т. е. не являющейся тривиальной) нормы.

Упражнение 1.6. Привести пример бесконечного поля, на котором есть только тривиальная норма.

Лемма 1.7. *Для любой нормы верно* $\|\pm 1\| = 1$ ($\implies \|-x\| = \|x\|$). □

Лемма 1.8. *Если* $n, m \in \mathbb{N}_0$, $n \leqslant 2^m$, *то* $\|x_1 + x_2 + \cdots + x_n\| \leqslant C^m \max\limits_{1 \leqslant k \leqslant n} \|x_k\|$. □

Следствие 1.9. $\|x_1 + \cdots + x_n\| \leqslant (2n)^{c_0} \max\limits_{1 \leqslant k \leqslant n} \|x_k\|$, *где* $c_0 = \log_2 C$. □

Следствие 1.10. $\|n\| \leqslant (2n)^{c_0}$. □

Предложение 1.11. *Если в определении 1.1 постоянная* $C = 2$, *то норма удовлетворяет неравенству треугольника* (1.1).

Доказательство. В нашем случае $c_0 = 1$. Пусть $x, y \in F$, $n \in \mathbb{N}$.

$$\|x + y\|^n = \|x^n + nx^{n-1}y + \cdots\| \leqslant 2(n+1) \max_{0 \leqslant k \leqslant n} \left\| \binom{n}{k} x^k y^{n-k} \right\|$$
$$\leqslant 2(n+1) \max_{0 \leqslant k \leqslant n} \left(2\binom{n}{k} \|x\|^k \|y\|^{n-k} \right) \leqslant 4(n+1)\big(\|x\| + \|y\|\big)^n.$$

Устремляем $n \to \infty$. □

Замечание 1.12. Пример $F \subseteq \mathbb{C}$, $\|\cdot\| = |\cdot|^\alpha$, $\alpha > 1$, показывает, что постоянную $C = 2$ в предложении 1.11 нельзя увеличить.

Следствие 1.13. *Отображение* $\|\cdot\| : F \to [0, +\infty)$ *«непрерывно» на* F, *т. е. для произвольных* $x_0 \in F$ *и* $\varepsilon > 0$ *существует* $\delta > 0$, *такое что из* $\|x - x_0\| < \delta$ *следует* $\big|\|x\| - \|x_0\|\big| < \varepsilon$.

Доказательство. Если $C \leqslant 2$, то всё следует из неравенства треугольника:

$$\big|\|x\| - \|y\|\big| \leqslant \|x - y\|.$$

Если же $C > 2$, то можно рассмотреть отображение $\|\cdot\|_1 = \|\cdot\|^{\log_C 2}$, которое является нормой на F с постоянной 2. □

Замечание 1.14. Из следствия 1.13 следует, что открытые шары действительно можно взять в качестве базы некоторой топологии.

Замечание 1.15. Аналогично и в других ситуациях предложение 1.11 позволяет всё свести к случаю с неравенством треугольника.

Упражнение 1.16. Док-ть стандартные арифметические свойства пределов (пределы суммы, разности, произведения, частного).

В дальнейшем нас в основном будет интересовать случай $C = 1$.

Определение 1.17. Если в определении 1.1 постоянная $C = 1$, то норма называется *неархимедовой*. Норма, не являющаяся неархимедовой, называется *архимедовой*. Соответствующее нормированное поле также будем называть (не)архимедовым.

Пример 1.18. Тривиальная норма на любом поле является неархимедовой.

Пример 1.19 (основной для нас)**.** Пусть p — простое число. На $\mathbb{Q}$ можно ввести *p-адическую норму*

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

Легко проверить, что это неархимедова норма.

Замечание 1.20. Можно было бы взять $A^{-\nu_p(x)}$ с произвольной постоянной $A > 1$. Выбор $A = p$ 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.

Пример 1.21 (функциональный аналог предыдущего примера)**.** Пусть $F = K(T)$, где K — некоторое поле, T — переменная. Фиксируем произвольный неприводимый многочлен $p(T) \in K[T]$. Тогда для $R(T) \neq 0$ можно положить $\|R\| = \mathrm{e}^{-\nu_p(R)}$. Если $p(T) = T - a$, $a \in K$, то $\nu_p(R) = \operatorname{ord}_{T=a} R(T)$ («порядок нуля» в точке a). По аналогии можно рассмотреть порядок в «бесконечно удалённой точке»:

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

Лемма 1.22. *Если норма неархимедова и $\|x\| \neq \|y\|$, то $\|x + y\| = \max\{\|x\|, \|y\|\}$.* □

Следствие 1.23. *Пусть норма неархимедова, $x_1, \ldots, x_n \in F$, причём $\|x_1\| > \max\limits_{2 \leqslant k \leqslant n} \|x_k\|$. Тогда $\|x_1 + \cdots + x_n\| = \|x_1\|$.* □

Следствие 1.24. *Пусть норма неархимедова, $x, y, z \in F$. Тогда (по крайней мере) два числа из $\|x - y\|, \|x - z\|, \|y - z\|$ равны. Неформально: в поле F (точнее, в соответствующем метрическом пространстве) все треугольники равнобедренные.* □

Лемма 1.25. *Пусть норма неархимедова, $a \in F$, $r > 0$. Рассмотрим открытый шар $B_r(a) = \{x \in F \mid \|x - a\| < r\}$. Тогда если $b \in B_r(a)$, то $B_r(b) = B_r(a)$. Аналогичное утверждение справедливо и для замкнутых шаров $B_r[a] = \{x \in F \mid \|x - a\| \leqslant r\}$. Неформально: любая точка шара является его центром.* □

Следствие 1.26. *Пусть норма неархимедова. Тогда если какие-то два шара пересекаются, то один является подмножеством другого.* □

Упражнение 1.27. Доказать, что в неархимедовом нормированном поле любой (открытый или замкнутый) шар (с положительным радиусом) является одновременно открытым и замкнутым множеством.

Лемма 1.28. *Норма является неархимедовой тогда и только тогда, когда для всех $n \in \mathbb{N}$ выполнено $\|n\| \leqslant 1$.*

Доказательство. $\boxed{\Longleftarrow}$ Пусть $x, y \in F$, $n \in \mathbb{N}$.

$$\|x+y\|^n \leqslant \big(2(n+1)\big)^{c_0} \max_{0\leqslant k\leqslant n} \left\| \binom{n}{k} x^k y^{n-k} \right\| \leqslant \big(2(n+1)\big)^{c_0} \big(\max\{\|x\|, \|y\|\}\big)^n.$$

Устремляем $n \to \infty$. □

Следствие 1.29. *Продолжение неархимедовой нормы (на «бóльшее» поле $K \supseteq F$) всегда неархимедово.* □

Упражнение 1.30. Пусть характеристика поля F положительна. Доказать, что любая норма на F является неархимедовой.

1.2 Эквивалентные нормы. Теорема Островского

Определение 1.31. Нормы $\|\cdot\|_1$ и $\|\cdot\|_2$ на поле F называются эквивалентными, если для любой посл-ти $\{x_n\}_{n=1}^{\infty} \subseteq F$ 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 1.32. Если $\|\cdot\|$ — норма на F, $\alpha > 0$, то $\|\cdot\|^\alpha$ — эквивалентная норма. (Если в определении нормы требовать нер-во треугольника, то нужно ограничение $\alpha \in (0, 1]$, чтобы (гарантированно) получилась норма.)

Предложение 1.33. *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 $x \in F^*$, такое что $\|x\|_2 < \|x\|_1^\alpha$, т. е. $\|x\|_2 = \theta\|x\|_1^\alpha$, где $\theta \in (0, 1)$. Для $n \in \mathbb{N}$ определим $m_n = \left\lfloor \dfrac{n \ln\|x\|_1}{\ln\|a\|_1} \right\rfloor \in \mathbb{Z}$, так что $\|a\|_1^{m_n} \leqslant \|x\|_1^n < \|a\|_1^{m_n+1}$. Тогда для всех $n \in \mathbb{N}$ выполнено $1 \leqslant \|x^n a^{-m_n}\|_1 < \|a\|_1$, но $\|x^n a^{-m_n}\|_2 = \theta^n \|x^n a^{-m_n}\|_1 \to 0$. Противоречие с эквивалентностью. □

Упражнение 1.34. Пусть $\|\cdot\|_1$ и $\|\cdot\|_2$ — нормы на F. Проверить эквивалентность следующих 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) $\{x \in F \mid \|x\|_1 < 1\} = \{x \in F \mid \|x\|_2 < 1\}$;

4) $\{x \in F \mid \|x\|_1 \leqslant 1\} = \{x \in F \mid \|x\|_2 \leqslant 1\}$;

5) множества последовательностей Коши для $\|\cdot\|_1$ и $\|\cdot\|_2$ совпадают.

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. Два случая:

1) Норма неархимедова. В этом случае найдётся простое p с $\|p\| < 1$. Если бы было два таких простых $p \neq q$, то мы бы имели: $1 = (p, q) = ap + bq$, следовательно, $1 \leqslant \max\{\|p\|, \|q\|\} < 1$, т. е. противоречие. Значит, такое простое единственно, а тогда $\|\cdot\| \sim |\cdot|_p$.

2) Норма архимедова. Для простоты будем считать, что есть нер-во треугольника.

   Докажем сначала вспомогательное утверждение (возможно, имеет смысл сформулировать его в виде отдельной леммы): если для некоторых $n_0 \in \mathbb{N}$, $n_0 > 1$, и $\alpha \geqslant 0$ выполнено $\|n_0\| \leqslant n_0^\alpha$, то для всех $n \in \mathbb{N}$ верно $\|n\| \leqslant n^\alpha$.

   Действительно, пусть $n = a_s n_0^s + a_{s-1} n_0^{s-1} + \cdots + a_0$, $a_i \in \{0, 1, \ldots, n_0 - 1\}$, $a_s > 0$. Тогда

   $$\|n\| \leqslant C_1(s+1)\big(\max\{\|n_0\|, 1\}\big)^s \leqslant C_1(s+1)n_0^{s\alpha} \leqslant C_1 n^\alpha\left(\frac{\ln n}{\ln n_0} + 1\right),$$

   где $C_1 = \max\limits_{1 \leqslant k \leqslant n_0 - 1} \|k\|$. Применяя доказанное для n^N и устремляя $N \to \infty$, получаем требуемое.

   Поскольку норма архимедова, то найдётся $n_0 \in \mathbb{N}$ с $\|n_0\| > 1$. Тогда $\|n_0\| = n_0^\alpha$ для некоторого $\alpha > 0$. Тогда из доказанного выше вспомогательного утверждения легко получить, что $\|\cdot\| = |\cdot|^\alpha$ (функция $f(n) = \max\left\{\frac{\ln\|n\|}{\ln n}, 0\right\}$ в каждой точке принимает наибольшее значение). □

Следствие 1.37 (уточнение леммы 1.28)**.** *Если существует целое $n > 1$, такое что $\|n\| \leqslant 1$, то норма неархимедова.* □

Глава 2

Пополнение нормированного поля. Поле p-адических чисел

2.1 Пополнение нормированного поля

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

1) существует вложение $i\colon F_0 \to F$, сохраняющее норму, т. е. $\|i(x)\| = \|x\|_0$;

2) $\left(F, \|\cdot\|\right)$ полно, т. е. каждая последовательность Коши сходится;

3) $i(F_0)$ плотно в F, т. е. для любых $x \in F$, $\varepsilon > 0$ найдётся $x_0 \in F_0$, такое что $\|x - i(x_0)\| < \varepsilon$.

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

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

Доказательство. Будем считать, что есть неравенство треугольника.

Пусть A — множество всех последовательностей Коши $(x_n)_{n=1}^{\infty}$ в $\left(F_0, \|\cdot\|_0\right)$. На нём естественным образом можно определить операции сложения и умножения, а также ввести «норму» $\|(x_n)\| = \lim\limits_{n\to\infty} \|x_n\|_0$. Существование последнего предела следует из неравенства треугольника $\left|\|x_n\|_0 - \|x_m\|_0\right| \leqslant \|x_n - x_m\|_0$ и того, что последовательность (x_n) фундаментальна. 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 следующие свойства отношения $\sim$:

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 $[(x_n)]$. Приведённые выше свойства позволяют естественным образом индуцировать операции сложения и умножения, а также «норму» с A на F, именно: $[(x_n)] + [(y_n)] = [(x_n + y_n)]$, $[(x_n)] \cdot [(y_n)] = [(x_n y_n)]$, $\|[(x_n)]\| = \|(x_n)\|$.

Проверим, что $\left(F, \|\cdot\|\right)$ — 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 $\|x_n\|_0 \geqslant \delta > 0$. Тогда в качестве $[(x_n)]^{-1}$ можно взять $[(y_n)]$, где

$$y_n = \begin{cases} 0, & n < n_0, \\ 1/x_n, & n \geqslant n_0. \end{cases}$$

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

Осталось проверить полноту. Пусть $X^{(n)} = \left[\left(x_1^{(n)}, x_2^{(n)}, \ldots\right)\right] \in F$ — последовательность Коши. Возьмём последовательность $k_n \in \mathbb{N}$, такую что

$$\sup_{k,l \geqslant k_n} \left\|x_k^{(n)} - x_l^{(n)}\right\|_0 \leqslant \frac{1}{n}.$$

Покажем, что в качестве предела $X^{(n)}$ можно взять $X = \left[\left(x_{k_n}^{(n)}\right)\right]$.

Пусть $N \geqslant k_n$, $M \geqslant k_m$, $K \geqslant \max\{k_n, k_m\}$. Переходя в неравенстве

$$\left\|x_N^{(n)} - x_M^{(m)}\right\|_0 \leqslant \left\|x_N^{(n)} - x_K^{(n)}\right\|_0 + \left\|x_K^{(n)} - x_K^{(m)}\right\|_0 + \left\|x_K^{(m)} - x_M^{(m)}\right\|_0 \leqslant \frac{1}{n} + \left\|x_K^{(n)} - x_K^{(m)}\right\|_0 + \frac{1}{m}$$

к пределу при $K \to \infty$, получаем

$$\left\|x_N^{(n)} - x_M^{(m)}\right\|_0 \leqslant \left\|X^{(n)} - X^{(m)}\right\| + \frac{1}{n} + \frac{1}{m}.$$

Отсюда легко вывести, что $x_{k_n}^{(n)}$ — посл-ть Коши (нужно взять $N = k_n$, $M = k_m$), а её класс эквивалентности действительно является искомым пределом (тут нужно аккуратно порассуждать с $\varepsilon > 0$). □

Упражнение 2.4. Док-ть, что любые два пополнения изометрически изоморфны.

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

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

Лемма 2.5. *Пусть $\left(F, \|\cdot\|\right)$ — (произвольное) неархимедово нормированное поле. Если последовательность $x_n \in F$ сходится к $x \in F^*$, то для всех достаточно больших n выполнено $\|x_n\| = \|x\|$.* □

Лемма 2.6. *Пусть $\left(F, \|\cdot\|\right)$ — пополнение неархимедова поля $\left(F_0, \|\cdot\|_0\right)$. Тогда:*

1) *$\left(F, \|\cdot\|\right)$ неархимедово;*

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

2.2 Поле p-адических чисел

Пусть p — простое число.

Определение 2.7. Пополнение поля $\mathbb{Q}$ относительно p-адической нормы $|\cdot|_p$ называется *полем p-адических чисел*. Обозначение: $\mathbb{Q}_p$.

Продолжение p-адической нормы на $\mathbb{Q}_p$ также будем обозначать через $|\cdot|_p$. Также продолжим на $\mathbb{Q}_p$ показатель $\nu_p(\alpha) = -\frac{\ln|\alpha|_p}{\ln p}$, так что равенство $|\alpha|_p = p^{-\nu_p(\alpha)}$ теперь справедливо для всех $\alpha \in \mathbb{Q}_p^*$. При этом по-прежнему $\nu_p(\alpha) \in \mathbb{Z}$. Дополнительно положим $\nu_p(0) = +\infty$.

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

Определение 2.8. p-адическое число α называется *целым*, если $|\alpha|_p \leqslant 1$. 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 2.9. *$\mathbb{Z}_p$ — замкнутое (в топологическом смысле) подкольцо поля $\mathbb{Q}_p$, причём $\mathbb{Q}_p$ — поле частных, а $\mathbb{Z}_p^\times$ — мультипликативная группа кольца $\mathbb{Z}_p$.* □

Также 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: $|\alpha - \beta|_p \leqslant p^{-n}$, $\frac{\alpha-\beta}{p^n} \in \mathbb{Z}_p$.

Упражнение 2.10. Проверить, что для $\alpha, \beta \in \mathbb{Z}$, $n \geqslant 0$ это совпадает с обычной сравнимостью целых чисел по модулю p^n.

Наконец, для $\alpha, \beta, \gamma \in \mathbb{Q}_p$ будем писать $\alpha = \beta + \mathcal{O}(\gamma)$, если $|\alpha - \beta|_p \leqslant |\gamma|_p$ (будем также использовать аналогичное обозначение для любого неархимедова нормированного поля). В частности, $\alpha = \beta + \mathcal{O}(p^n) \iff \alpha \equiv \beta \pmod{p^n}$. Можно до кучи ещё определить «о малое»: $\alpha = \beta + \mathfrak{o}(\gamma)$, если $|\alpha - \beta|_p < |\gamma|_p$. Возможно, лучше отложить эти обозначения на потом, когда они понадобятся.

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

Лемма 2.11. *Для любого $\alpha \in \mathbb{Z}_p$ найдётся (единственное) $a \in \{0, 1, \ldots, p-1\}$, такое что $\alpha \equiv a \pmod{p}$.* □

Теорема 2.12. *Любое целое p-адическое число α можно единственным образом представить как сумму ряда вида*

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

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

Следствие 2.13. *$\mathbb{N}_0$ плотно в $\mathbb{Z}_p$.* □

Следствие 2.14. *Множество $\mathbb{Z}_p$ имеет мощность континуум (следовательно, $\mathbb{Q}_p \neq \mathbb{Q}$, т. е. $\mathbb{Q}$ не полно относительно p-адической нормы).* □

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

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

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*

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

И обратно: каждый такой ряд сходится к некоторому p-адическому числу. При этом: если $a_{n_0} \neq 0$, то $v_p(\alpha) = n_0$. □

Замечание 2.17. Единственность надо понимать как единственность двусторонней последовательности $(a_n)_{n\in\mathbb{Z}}$, где полагаем $a_n = 0$ при $n < n_0$.

Представление (2.1) будем называть стандартным представлением (разложением, записью) p-адического числа α, а числа a_n — его (стандартными p-адическими) цифрами. Это аналог бесконечной десятичной дроби для вещественных чисел.

Замечание 2.18. Цифры a_n можно брать из любого множества $S \subseteq \mathbb{Z}_p$, обладающего свойством: для любого $\alpha \in \mathbb{Z}_p$ найдётся единственное $a \in S$, такое что $\alpha \equiv a \pmod p$. (Интересный пример такого множества можно найти в примере 4.2 далее.) Более того, для каждой цифры a_n можно брать своё множество S_n.

Здесь уместно разобрать несколько примеров с арифметическими операциями для таких рядов.

Теорема 2.19. *Последовательность цифр p-адического числа α является периодической тогда и только тогда, когда $\alpha \in \mathbb{Q}$.* □

(Нужно рассказать два доказательства: через геометрические прогрессии и непосредственное вычисление цифр.)

Альтернативный подход (без деталей)

Последовательность целых чисел $(b_n)_{n=1}^{\infty}$ со свойством $b_{n+1} \equiv b_n \pmod{p^n}$ является последовательностью Коши, 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 тогда и только тогда, когда $b_n \equiv b'_n \pmod{p^n}$. 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 $\alpha = \sum_{n=0}^{\infty} a_n p^n$, то можно взять $b_n = \sum_{i=0}^{n-1} a_i p^i$.

Это означает, 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 $\mathbb{Q}_p$.

Глава 3

Теорема о слабой аппроксимации

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

Лемма 3.1. *Пусть $\|\cdot\|_1, \|\cdot\|_2$ — нетривиальные нормы на F, $\|\cdot\|_1 \nsim \|\cdot\|_2$. 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 $\|a^{-1}\|_2 > 1 > \|a^{-1}\|_1$.

Пусть для определённости найдётся последовательность $x_n \in F$, такая что $\|x_n\|_1 \nrightarrow 0$, $\|x_n\|_2 \to 0$. Переходя, если нужно, к подпоследовательности, можно считать, что $\|x_n\|_1 \geqslant \varepsilon > 0$ для всех n. Поскольку норма $\|\cdot\|_1$ нетривиальна, то существует $b \in F$ 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. Пусть $\|a_0\|_n \geqslant 1$.

Возьмём $b \in F$, 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 $a_k \in F$, 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 вообще говоря будет рациональным, а не целым). 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.

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 $\sum\limits_{n=1}^{\infty} a_n$ 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 $a_n = \alpha^{p^n}$, $n \geqslant 0$. Для неё справедливы сравнения $a_n \equiv a_{n-1} \pmod{p^n}$, $n \geqslant 1$. (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). Легко проверить следующие свойства:

1) $\big(\omega(\alpha)\big)^p = \omega(\alpha)$;

2) $\omega(\alpha) \equiv \alpha \pmod{p}$;

3) $\omega\big(\mathbb{Z}_p\big) = \big\{\omega(0), \omega(1), \dots, \omega(p-1)\big\} = \big\{x \in \mathbb{Q}_p \mid x^p = x\big\}$, причём это множество содержит ровно p элементов, различных по модулю p (т. е. является «полной системой вычетов по модулю p»);

4) $\omega\big(\omega(\alpha)\big) = \omega(\alpha)$;

5) $\omega(\alpha\beta) = \omega(\alpha)\,\omega(\beta)$;

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

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

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

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

Упражнение 4.3. Пусть $\alpha, \beta \in \mathbb{Z}_p$, $\beta^p = \beta$, $\beta \equiv \alpha \pmod{p}$. Доказать, что $\beta = \omega(\alpha)$.

Поговорим немного о свойствах сходящихся рядов (члены рядов лежат в F). В неархимедовом случае всё немного проще. Например, нет аналога теоремы Римана об условно сходящихся рядах.

Лемма 4.4. *Если ряд* $\sum\limits_{n=1}^{\infty} a_n$ *сходится и его сумма равна* S *(дальше будем просто писать* $\sum\limits_{n=1}^{\infty} a_n = S$*), то для любой биекции* $\sigma : \mathbb{N} \to \mathbb{N}$ *выполнено* $\sum\limits_{n=1}^{\infty} a_{\sigma(n)} = S$. □

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

Лемма 4.5. *Пусть* $\sum\limits_{n=1}^{\infty} a_n = S$, $\mathbb{N} = \bigsqcup\limits_{m=1}^{\infty} A_m$ *(т. е.* $\mathbb{N} = \bigcup\limits_{m=1}^{\infty} A_m$, *где* $A_m \cap A_n = \varnothing$ *при* $m \neq n$*). Тогда для каждого* m *выражение* $\sum\limits_{n \in A_m} a_n$ *определено (это конечная сумма либо сходящийся ряд), причём* $\sum\limits_{m=1}^{\infty} \sum\limits_{n \in A_m} a_n = S$. □

Наконец, сходящиеся ряды можно перемножать ровно так же, как и абсолютно сходящиеся ряды с комплексными числами.

Лемма 4.6. *Пусть* $\sum\limits_{n=1}^{\infty} a_n = A$, $\sum\limits_{n=1}^{\infty} b_n = B$, $k \mapsto \big(m(k), n(k)\big)$ *— биекция* $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$. *Тогда* $\sum\limits_{k=1}^{\infty} a_{m(k)} b_{n(k)} = AB$. *(Будем писать* $\sum\limits_{m,n=1}^{\infty} a_m b_n = AB$.*)* □

Важное следствие леммы 4.5 — возможность переставлять порядок суммирования в повторных рядах при условии сходимости соответствующих кратных рядов.

Лемма 4.7. *Допустим, что* $\sum\limits_{m,n=1}^{\infty} a_{m,n} = S$. *Тогда* $\sum\limits_{m=1}^{\infty} \sum\limits_{n=1}^{\infty} a_{m,n} = \sum\limits_{n=1}^{\infty} \sum\limits_{m=1}^{\infty} a_{m,n} = S$. □

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. Заменить его требованием сходимости обоих повторных рядов нельзя.

Глава 5

Лемма Гензеля

Пусть $(F, \|\cdot\|)$ — полное неархимедово нормированное поле. Обозначим

$$\mathbb{Z}_F = B_1[0] = \{x \in F \mid \|x\| \leqslant 1\}$$

(«кольцо целых чисел» поля F). Это действительно кольцо, причём оно замкнуто (в топологическом смысле), т. е. является полным метрическим пространством.

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

Доказательство. Положим $c = \frac{\|f(\alpha_0)\|}{\|f'(\alpha_0)\|^2} < 1$. Рассмотрим последовательность, заданную рекуррентно: $\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$, $n \geqslant 0$ («метод Ньютона» aka «метод касательных»). По индукции легко проверить, что она обладает свойствами (проверять надо одновременно именно в таком порядке):

1) $\|\alpha_n - \alpha_0\| \leqslant c\|f'(\alpha_0)\| < \|f'(\alpha_0)\|$;
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) $\|\alpha_{n+1} - \alpha_n\| \leqslant c^{2^n}\|f'(\alpha_0)\|$.

Поэтому можно взять $\alpha = \lim \alpha_n$.

Чтобы доказать единственность, достаточно разложить по Тейлору в т. α. □

Замечание 5.2. Как видно из доказательства, на самом деле справедливо неравенство $\|\alpha - \alpha_0\| \leqslant \|f(\alpha_0)\| \,/\, \|f'(\alpha_0)\|$.

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

Следствие 5.3. *Пусть $f(x) \in \mathbb{Z}_p[x]$, $\alpha_0 \in \mathbb{Z}_p$. Допустим, что для некоторого $e \in \mathbb{N}_0$ выполнено $|f'(\alpha_0)|_p = p^{-e}$, $f(\alpha_0) \equiv 0 \pmod{p^{2e+1}}$. Тогда найдётся единственное $\alpha \in \alpha_0 + p^{e+1}\mathbb{Z}_p$, такое что $f(\alpha) = 0$.* □

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

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

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

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

Более того, 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 $e = 0$.

Следствие 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 $\alpha \in \alpha_0 + p\mathbb{Z}_p$, такое что $f(\alpha) = 0$.* □

Разберём несколько поучительных примеров (для $\mathbb{Q}_p$).

Пример 5.7 (снова представители Тейхмюллера, см. пример 4.2)**.** Рассмотрим многочлен $f(x) = x^p - x$. Пусть $\alpha_0 \in \mathbb{Z}_p$. Тогда $f(\alpha_0) \equiv 0 \pmod{p}$ (малая теорема Ферма), $f'(\alpha_0) = p\alpha_0^{p-1} - 1 \equiv -1 \not\equiv 0 \pmod{p}$, и следствие 5.6 даёт нам существование (и заодно единственность) корня многочлена $f(x)$ в шаре $x \equiv \alpha_0 \pmod{p}$. Мы снова построили представитель Тейхмюллера.

Обсудим теперь поподробнее извлечение квадратных корней.

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

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 $\alpha \equiv 1 \pmod{8}$.* □

Пример 5.10. 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).

Упражнение 5.11. Доказать подобным образом, что поля $\mathbb{Q}_{p_1}$ и $\mathbb{Q}_{p_2}$ при различных простых p_1, p_2 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. Разберём пример.

Лемма 5.12. *Пусть $m \in \mathbb{N}$, $(m, p) = 1$, $\alpha \in p\mathbb{Z}_p$. Тогда ряд $\sum\limits_{n=0}^{\infty} \binom{1/m}{n} \alpha^n$ сходится в $\mathbb{Z}_p$, причём его сумма является (единственным) корнем уравнения $x^m = 1 + \alpha$, удовлетворяющим условию $x \equiv 1 \pmod{p}$.* □

Пример 5.13. Ряд $\sum\limits_{n=0}^{\infty} \binom{1/2}{n} (7/9)^n$ сходится и 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 5.12 существенно.

Упражнение 5.14. 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 $\alpha \equiv 0 \pmod{p^2}$.

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: $G_F = \{\|x\| \mid x \in F^*\}$, $\mathbb{Z}_F = B_1[0] = \{x \in F \mid \|x\| \leqslant 1\}$ — кольцо целых чисел, $\mathfrak{M}_F = B_1(0) = \{x \in F \mid \|x\| < 1\}$ — (единственный) максимальный идеал кольца $\mathbb{Z}_F$, $k_F = \mathbb{Z}_F/\mathfrak{M}_F$ — *поле вычетов* поля F (или кольца $\mathbb{Z}_F$, или нормы $\|\cdot\|$).

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 $\varphi\colon\ k_{F_0} \to k_F$, 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 6.1. Пусть F — пополнение F_0. Доказать, что $k_F = k_{F_0}$. (*Указание*. Вспомнить доказательство леммы 2.11.)

Дальше предположим, что норма $\|\cdot\|$ нетривиальна, т. е. $G_F \neq \{1\}$.

Лемма 6.2. *Группа G_F дискретна $\iff$ $G_F = \langle a\rangle$ при некотором $a \in (0,1)$. В противном случае группа G_F плотна в $[0, +\infty)$.* □

Лемма 6.3. *Пусть группа G_F дискретна. Тогда $\mathbb{Z}_F$ — кольцо главных идеалов. Более того, любой ненулевой идеал имеет вид $\mathfrak{M}_F^n$ для некоторого $n \in \mathbb{N}_0$.* □

Определение 6.4. В условиях леммы 6.3: если $\mathfrak{M}_F = (\pi_F) = \pi_F\mathbb{Z}_F$, то элемент π_F называется *униформизующим элементом* кольца $\mathbb{Z}_F$.

Лемма 6.5. *Допустим, что поле F полно, группа G_F дискретна и поле вычетов k_F конечно. Тогда кольцо $\mathbb{Z}_F$ компактно.* □

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

Вернёмся к случаю $F = \mathbb{Q}_p$. В этом случае: $G_F = p^{\mathbb{Z}}$, $\mathfrak{M}_F = p\mathbb{Z}_p$, $k_F \cong \mathbb{F}_p$.

Следствие 6.7. *Кольцо $\mathbb{Z}_p$ компактно.* □

Следствие 6.8 (Hensel)**.** *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

Прежде чем обсуждать продолжение нормы на алгебраические расширения, разберём простой случай (чисто) трансцендентных расширений, интересный и сам по себе.

В этой главе $(F, \|\cdot\|)$ — 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 (т. е. получается настоящее продолжение).

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

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

Упражнение 7.2. Обобщить лемму Гаусса на многочлены от нескольких 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 НОД его коэффициентов; обозначение: $\operatorname{cont}(P)$. При этом $\operatorname{cont}(0) = 0$. Несложно убедиться, что для ненулевого многочлена P выполнено

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

поэтому из леммы 7.1 следует $\operatorname{cont}(PQ) = \operatorname{cont}(P) \operatorname{cont}(Q)$.

Упражнение 7.4. Доказать, что норму $\|\cdot\|$ можно продолжить на поле рациональных функций $F(z)$ с помощью формулы

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

То же самое верно для произвольного количества неизвестных.

Как и раньше, рассмотрим кольцо целых чисел $\mathbb{Z}_F = \{x \in F \mid \|x\| \leqslant 1\}$ поля F. Из леммы Гаусса получаем важное следствие для целочисленных многочленов.

Следствие 7.5. *Пусть $P(z), Q(z) \in F[z]$ — унитарные многочлены (т. е. старшие коэффициенты равны 1), причём $P(z)Q(z) \in \mathbb{Z}_F[z]$. Тогда $P(z), Q(z) \in \mathbb{Z}_F[z]$.* $\square$

Глава 8

Сведения из теории алгебраических чисел

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

S. Lang. *Algebra*. Любое издание.

Определение 8.1. Поле K называется *расширением* поля F, если $F \subseteq K$. Часто пишут: расширение K/F (это *не* фактор). Поле K можно рассмотреть как векторное пространство над полем F; его размерность $\dim_F K$ называется *степенью* расширения и обозначается через $[K : F]$. Если K — конечномерное векторное пространство над F, то расширение K/F называется *конечным*.

Утверждение 8.2. *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 $[L : F] = [L : K][K : F]$. Более того, если $\omega_1, \dots, \omega_n$ — базис K/F, $\theta_1, \dots, \theta_m$ — базис L/K, то всевозможные попарные произведения $\omega_\nu \theta_\mu$ образуют базис L/F.* □

Определение 8.3. 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 полем F, а его степень — *степенью* α над полем F. Обозначения: $P_\alpha(z)$, $\deg_F \alpha = \deg \alpha$.

Утверждение 8.4. *Пусть α алгебраическое над F. Тогда его минимальный многочлен определён однозначно и неприводим над F. Кроме того, для любого многочлена $P(z) \in F[z]$, такого что $P(\alpha) = 0$, выполнено $P_\alpha \mid P$.* □

Определение 8.5. Расширение K/F называется *алгебраическим*, если все элементы поля K являются алгебраическими над F.

Утверждение 8.6. *Любое конечное расширение является алгебраическим, причём степень любого элемента расширения не превосходит степени расширения.* □

Определение 8.7. Пусть K — расширение F, $\alpha_1, \dots, \alpha_n \in K$. Полем, *порождённым элементами* $\alpha_1, \dots, \alpha_n$ над полем F, называется наименьшее по включению подполе $L \subseteq K$, которое содержит F и все α_j. Обозначение: $L = F(\alpha_1, \dots, \alpha_n)$. В этом случае говорят, что L — *конечно порождённое* расширение F. Очевидно, что

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

Расширение вида $F(\alpha)$ называется *простым*.

Если α трансцендентно (т. е. не алгебраическое) над F, то $F(\alpha)$ изоморфно полю рациональных функций (от одного неизвестного) над F. Случай алгебраического α чуть более интересен.

Утверждение 8.8. *Пусть* $\deg_F \alpha = n$. *Тогда* $[F(\alpha) : F] = n$, *причём* $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ — *базис. Более того,* $F(\alpha) \cong F[z]/P_\alpha(z)F[z]$. □

Утверждение 8.9. *Расширение* K/F *конечно* $\iff$ $K = F(\alpha_1, \dots, \alpha_n)$, *где все* α_j *алгебраические над* F. □

Из утверждений 8.9 и 8.6 легко вывести, что множество алгебраических над F элементов (лежащих в каком-нибудь фиксированном расширении K) замкнуто относительно основных арифметических операций, т. е. является полем.

Утверждение 8.10. *Пусть* $P(z) \in F[z]$ — *унитарный неприводимый (над* F*) многочлен. Тогда найдётся некоторое расширение* K *поля* F, *в котором многочлен* $P(z)$ *имеет корень* α. *Более того, при этом* $P(z) = P_\alpha(z)$. □

Утверждение 8.11. *Для любого поля* F *существует такое расширение, в котором каждый непостоянный многочлен* $P(z) \in F[z]$ *имеет корень.* □

Утверждение 8.12. *Для любого поля* F *существует минимальное по включению расширение* A *со свойством из утверждения 8.11. При этом* A *является алгебраическим расширением поля* F *(другими словами,* A *состоит из корней всех непостоянных многочленов* $P(z) \in F[z]$*). Более того, поле* A *алгебраически замкнуто.* □

Определение 8.13. Расширение A из утверждения 8.12 называется *алгебраическим замыканием* поля F. Обозначение: F^{alg}. (*Замечание*. Можно доказать, что любые два алгебраических замыкания изоморфны.)

В дальнейшем мы будем считать, что зафиксировано некоторое алгебраически замкнутое поле, и все поля и корни многочленов будем брать из этого фиксированного поля (если не сказано противное).

Определение 8.14. Алгебраическое расширение K/F называется *сепарабельным*, если для любого $\alpha \in K$ его минимальный многочлен (над F) не имеет кратных корней.

Утверждение 8.15 (теорема о примитивном элементе)**.** *Если* $\alpha \in F^{\text{alg}}$, K — *сепарабельное конечное расширение поля* $F(\alpha)$, *то расширение* K/F *является простым, т. е.* $K = F(\theta)$. *В частности, если* K — *сепарабельное конечное расширение* F, *то оно является простым.* □

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

Пример 8.17 («контрпример)**.** Пусть p — простое число. Тогда:

1) $\mathbb{F}_p(x^{1/p})$ — несепарабельное расширение $\mathbb{F}_p(x)$;

2) для расширения $\mathbb{F}_p(x^{1/p}, y^{1/p})/\mathbb{F}_p(x, y)$ нет примитивного элемента (поскольку для любого $\alpha \in \mathbb{F}_p(x^{1/p}, y^{1/p})$ выполнено $\alpha^p \in \mathbb{F}_p(x, y)$, откуда $\deg \alpha \leqslant p$; с другой стороны, $\left[\mathbb{F}_p(x^{1/p}, y^{1/p}) : \mathbb{F}_p(x, y)\right] = p^2$).

Определение 8.18. Поле F называется *совершенным*, если либо $\operatorname{char} F = 0$, либо $\operatorname{char} F = p$ и для любого $\alpha \in F$ уравнение $x^p = \alpha$ разрешимо в F.

Утверждение 8.19. *Поле совершенно тогда и только тогда, когда любое его алгебраическое (или конечное) расширение сепарабельно (т. е. любой неприводимый многочлен не имеет кратных корней).* □

Утверждение 8.20. *Любое конечное поле совершенно.* □

Определение 8.21. Пусть K, L — расширения F. Вложение $\sigma : K \to L$ называется вложением (поля K в поле L) *над полем* F, если σ тождественно на F, т. е. $\sigma(\alpha) = \alpha$ для всех $\alpha \in F$.

Определение 8.22. Пусть α алгебраическое над F. Корни его минимального многочлена (над F) называются *сопряжёнными* с α (над F).

Утверждение 8.23. *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 с α над F.* □

Утверждение 8.24. *Пусть α алгебраическое над F, 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 8.25. *Пусть $\alpha \in F^{\mathrm{alg}}$. Тогда количество вложений $F(\alpha) \to F^{\mathrm{alg}}$ над F равно количеству (различных) сопряжённых с α над F (в частности, оно не превосходит $\deg_F \alpha$).* □

Утверждение 8.26. *Более общо, 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 с α над F.* □

Следствие 8.27. *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.* □

Следствие 8.28. *Пусть $\alpha_1, \ldots, \alpha_n \in F^{\mathrm{alg}}$. Расширение $F(\alpha_1, \ldots, \alpha_n)$ поля F является сепарабельным тогда и только тогда, когда минимальные многочлены всех порождающих α_ν не имеют кратных корней.* □

Определение 8.29. Алгебраическое расширение K/F называется *нормальным*, если для любого вложения $\sigma : K \to F^{\mathrm{alg}}$ над F выполнено $\sigma(K) \subseteq K$. Сепарабельное нормальное расширение называется *расширением Галуа*.

Утверждение 8.30. *Пусть K — алгебраическое расширение F. Тогда следующие условия эквивалентны:*

1) *расширение K/F нормально;*

2) *любое вложение $\sigma\colon K \to F^{\mathrm{alg}}$ над F является автоморфизмом поля K, т. е. $\sigma(K) = K$;*

3) *для любого $\alpha \in K$ все сопряжённые с α (над F) лежат в K.*

Если расширение K/F конечно, то эти условия эквивалентны тому, что K является полем разложения некоторого многочлена над F, т. е. $K = F(\alpha_1, \dots, \alpha_m)$, где $\prod\limits_{k=1}^{m}(z - \alpha_k) \in F[z]$. □

Определение 8.31. Пусть K/F — расширение Галуа. *Группой Галуа* этого расширения называется группа всех автоморфизмов поля K над F относительно операции композиции. Обозначение: $\mathrm{Gal}(K/F)$.

Утверждение 8.32. *Если K/F — расширение Галуа, то $\bigl|\mathrm{Gal}(K/F)\bigr| = [K : F]$.* □

8.1 Конечные поля

Поговорим немного о конечных полях.

Пусть F — конечное поле, $\operatorname{char} F = p$. Тогда F является конечным расширением $\mathbb{F}_p$. Если $f = [F : \mathbb{F}_p]$, то $|F| = p^f$.

Утверждение 8.33. *Для любого $q = p^f$ 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 с точностью до изоморфизма, а если зафиксировать алгебраическое замыкание, то единственное в принципе) обозначается через $\mathbb{F}_q$.

Упражнение 8.34. Доказать, что $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$ тогда и только тогда, когда $q_2 = q_1^f$, $f \in \mathbb{N}$. При этом $f = [\mathbb{F}_{q_2} : \mathbb{F}_{q_1}]$.

Утверждение 8.35. *Пусть G — конечная подгруппа мультипликативной группы некоторого поля. Тогда G циклическая.* □

Следствие 8.36. *Группа $\mathbb{F}_q^*$ циклическая.* □

Утверждение 8.37. *Расширение $\mathbb{F}_{q^f}/\mathbb{F}_q$ является расширением Галуа, причём группа Галуа циклическая и порождена автоморфизмом $x \mapsto x^q$.* □

Следствие 8.38. *Допустим, что многочлен $P(z) \in \mathbb{F}_q[z]$ унитарный и неприводимый над $\mathbb{F}_q$, $\deg P = d$, $P(\alpha) = 0$. Тогда*

$$P(z) = \prod_{k=0}^{d-1}\bigl(z - \alpha^{q^k}\bigr).$$ □

Упражнение 8.39. Пусть $\alpha \in \mathbb{F}_q^{\mathrm{alg}}$. Доказать, что $\deg_{\mathbb{F}_q} \alpha$ — это минимальное $f \in \mathbb{N}$, такое что $\alpha^{q^f} = \alpha$.

Упражнение 8.40. 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 $\frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$, где μ — функция Мёбиуса.

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 следующими тремя 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 $\|\cdot\|_2$ будем называть *эквивалентными*, если существуют положительные постоянные a, b, такие что $a\|\cdot\|_1 \leqslant \|\cdot\|_2 \leqslant b\|\cdot\|_1$ (если норма $\|\cdot\|$ 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».

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

Лемма 9.2. *Пусть F локально компактно, V — конечномерное векторное пространство над F. Тогда любые две векторные нормы на V эквивалентны.* □

Замечание 9.3. Для тривиальной нормы док-во немного хитрее. Основная трудность — доказать, что $\inf\limits_{v \neq 0} \|v\|_V > 0$. Если допустить противное, то можно найти последовательность векторов $v_n \in V$, такую что $\|v_{n+1}\|_V < \frac{1}{2}\|v_n\|_V$. Легко доказать, что эти вектора линейно независимы. Пожалуй, это хорошее упражнение.

Следствие 9.4. *Пусть F локально компактно, K — алгебраическое расширение F. Тогда существует не более одного продолжения нормы $\|\cdot\|$ с F на K.* □

Следствие 9.5. *Пусть K — нормальное расширение локально компактного поля F. Допустим, что мы продолжили норму $\|\cdot\|$ с F на K. Тогда для любого автоморфизма $\sigma\colon K \to K$ над F выполнено $\|\sigma(\cdot)\| = \|\cdot\|$.* □

Следствие 9.6. *В условиях следствия 9.5 пусть $\alpha \in K$, α' — сопряжённое с α над F. Тогда $\|\alpha'\| = \|\alpha\|$.* □

9.2 Продолжение нормы на алгебраическое замыкание

Сейчас, используя результаты предыдущего параграфа, мы получим, как должно выглядеть продолжение нормы на F^{alg}, если оно существует. Для этого нам понадобится ещё одно понятие нормы.

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

Определение 9.7. 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 9.8. *Пусть $F \subseteq L \subseteq K$ (башня конечных расширений), $\alpha \in L$. Тогда*

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

□

Лемма 9.9. *Пусть $P_\alpha(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0 = (z-\alpha_1)\cdots(z-\alpha_n)$ — минимальный многочлен α (над F). Тогда*

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

□

До конца этой главы будем предполагать, что F локально компактно (если не сказано противное).

Следствие 9.10. *Пусть K — нормальное конечное расширение F. Допустим, что мы продолжили норму $\|\cdot\|$ с F на K. Тогда для всех $\alpha \in K$ выполнено*

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

□

Таким образом, если продолжение нормы на F^{alg} существует, то оно должно задаваться формулой

$$\|\alpha\| = \left\|\mathrm{N}_F^K(\alpha)\right\|^{\frac{1}{[K:F]}} \tag{9.1}$$

(заметим, что $\mathrm{N}_F^K(\alpha) \in F$), где K — какое-то нормальное конечное расширение F, содержащее α (например, сгодится поле разложения минимального многочлена α).

Из леммы 9.8 следует, что выражение в правой части равенства (9.1) на самом деле не зависит от выбора конечного расширения K (необязательно нормального), содержащего α. Наша ближайшая цель — доказать, что эта формула действительно определяет искомое продолжение нормы на F^{alg}.

Теорема 9.11. *Пусть F локально компактно. Тогда существует единственное продолжение нормы $\|\cdot\|$ с F на F^{alg}, причём это продолжение можно задать с помощью формулы*

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

Более того, справедлива формула

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

где K — (произвольное) конечное расширение $F(\alpha)$.

Доказательство. □

Глава 10

Аналитические функции: начало

Всюду в этой главе $(F, \|\cdot\|)$ — полное неархимедово поле с нетривиальной нормой. Позже мы потребуем ещё алгебраическую замкнутость, но на первых порах она нам не нужна. Основные для нас примеры:

- поле $\mathbb{Q}_p$ и его конечные расширения (есть локальная компактность);
- поле $\mathbb{C}_p$ (пополнение $\mathbb{Q}_p^{\mathrm{alg}}$; есть алгебраическая замкнутость).

10.1 Степенные ряды. Радиус сходимости

Рассмотрим степенной ряд $S(z) = \sum\limits_{n=0}^{\infty} c_n z^n \in F[\![z]\!]$. Если $z \in F$, то, как мы знаем, сходимость ряда равносильна условию

$$\lim_{n\to\infty} \|c_n z^n\| = \lim_{n\to\infty} \bigl(\|c_n\| \cdot \|z\|^n\bigr) = 0.$$

Радиусом сходимости ряда $S(z)$ называется величина $R(S) \in [0, +\infty]$, определяемая равенством

$$R(S) = \sup\Bigl\{r \geqslant 0 \;\Big|\; \lim_{n\to\infty} \|c_n\| r^n = 0\Bigr\}.$$

Из определения видно, что $R = R(S)$ обладает следующим свойством: ряд сходится при $\|z\| < R$ и расходится при $\|z\| > R$. (Заметим, что если группа G_F дискретна, то это условие не определяет R однозначно.) Кроме того, справедлива *формула Коши–Адамара*

$$R(S) = \frac{1}{\limsup\limits_{n\to\infty} \|c_n\|^{1/n}}\,.$$

Что касается случая $\|z\| = R$, то бывает и так, и эдак, однако ситуация разительно отличается от архимедова случая: не бывает такого, что для каких-то z (с $\|z\| = R$) ряд сходится, а для других расходится.

Если $R \in G_F$, т. е. найдётся $z \neq 0$, такое что $\|z\| = R$, то условие сходимости ряда при $\|z\| = R$ имеет вид

$$\lim_{n\to\infty} \|c_n\| R^n = 0.$$

Если последнее условие выполняется для какого-то $R > 0$ (необязательно $R \in G_F$), то условимся писать $R(S) \geqslant R^+$.

10.2 Аналитические в шаре функции

Пусть $B = B_R[a]$ — некоторый (замкнутый) шар. (Следует помнить, что B является одновременно открытым и замкнутым множеством.) В дальнейшем под B мы будем понимать не просто подмножество поля F, но шар с фиксированными центром a (любая точка шара является его центром) и радиусом R (если группа G_F дискретна, то шары с разными радиусами могут совпадать).

Определение 10.1. Функция $f\colon B \to F$ называется *строго аналитической в шаре B*, если найдётся степенной ряд $S(z) = \sum\limits_{n=0}^{\infty} c_n z^n \in F[\![z]\!]$ с $R(S) \geqslant R^+$, такой что $f(z) = S(z-a)$ при $z \in B$.

Замечание 10.2. Чуть ниже (см. теорему 10.8) мы увидим, что на самом деле понятие строго аналитической в шаре функции не зависит от выбора центра a.

Множество всех строго аналитических в B функций будем обозначать через $\mathcal{A}(B)$. Несложно проверить, что это алгебра над полем F (нетривиальна только проверка условия $R(S) \geqslant R^+$ для произведения).

Лемма 10.3. *Пусть $S(z) = \sum\limits_{n=0}^{\infty} c_n z^n \in F[\![z]\!] \setminus \{0\}$, причём $R(S) > 0$. Тогда найдётся $\varepsilon > 0$, такое что $S(z) \neq 0$ при $0 < |z| \leqslant \varepsilon$.* □

Следствие 10.4. *В определении 10.1 коэффициенты c_n степенного ряда S однозначно восстанавливаются по функции f.* □

Лемма 10.5. *Пусть $f(z) = \sum\limits_{n=0}^{\infty} c_n (z-a)^n \in \mathcal{A}(B)$, $z_0 \in B$. Тогда существует производная*

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0},$$

причём $f'(z_0) = \sum\limits_{n=1}^{\infty} n c_n (z_0 - a)^{n-1}$. □

Следствие 10.6. *Пусть $f(z) = \sum\limits_{n=0}^{\infty} c_n (z-a)^n \in \mathcal{A}(B)$. Тогда f бесконечно дифференцируема в B, причём*

$$f^{(k)}(z) = k! \sum_{n=k}^{\infty} \binom{n}{k} c_n (z-a)^{n-k}.$$

В частности, $f^{(k)}(a) = k! c_k$. □

Следствие 10.7. *Если $\operatorname{char} F = p > 0$, $f \in \mathcal{A}(B)$, то $f^{(p)}(z) = 0$ при $z \in B$.* □

Если $\operatorname{char} F = 0$, то получаем

$$\frac{f^{(k)}(z)}{k!} = \sum_{n=k}^{\infty} \binom{n}{k} c_n (z-a)^{n-k}.$$

Условимся считать это равенство определением выражения $f^{(k)}(z)/k!$ при $k \geqslant p$, если $\operatorname{char} F = p > 0$.

Для $b \in B$ будем обозначить

$$T_b(z) = T_b[f](z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(b)}{n!}\, z^n.$$

Теорема 10.8. *Пусть $f \in \mathcal{A}(B)$, $b \in B$. Тогда $R(T_b) \geqslant R^+$, причём при $z \in B$ справедливо равенство $f(z) = T_b(z-b)$.* □

Следствие 10.9. *$R(T_b)$ не зависит от $b \in B$.* □

Теорема 10.10 (теорема единственности)**.** *Пусть $f \in \mathcal{A}(B)$, $f(z) = 0$ при всех $z \in Z \subseteq B$, причём множество Z имеет предельную точку. Тогда функция f тождественно равна нулю (на B).* □

Следствие 10.11. *Допустим, что поле F локально компактно. Если $f \in \mathcal{A}(B)$, причём f не является тождественно нулевой, то множество нулей f в B конечно.* □

Ниже мы увидим, что следствие 10.11 верно и без предположения о локальной компактности (см. следствие 12.3).

Для $f \in \mathcal{A}(B)$ будем обозначить

$$\|f\|_{a,R} = \max_{n \geqslant 0} \left\| \frac{f^{(n)}(a)}{n!} \right\| R^n.$$

Легко видеть, что $\|\cdot\|_{a,R}$ — векторная норма на $\mathcal{A}(B)$ (причём неархимедова). Более того, несложно показать, что она мультипликативна, т. е. $\|fg\|_{a,R} = \|f\|_{a,R} \cdot \|g\|_{a,R}$ (обобщение леммы Гаусса). Кроме того, для любого $r \in F^*$ очевидно тождество

$$\|f\|_{0,R} = \|f_r\|_{0,R/\|r\|},$$

где $f_r(z) = f(rz)$.

Упражнение 10.12. Доказать, что $\|f\|_{b,R}$ не зависит от $b \in B$.

Теорема 10.13. *Алгебра $\mathcal{A}(B)$ является полным метрическим пространством относительно нормы $\|\cdot\|_{a,R}$ (точнее, относительно соответствующей метрики), причём сходимость по этой норме влечёт равномерную сходимость на B. Более того, для любого $n \in \mathbb{N}_0$ дифференциальный оператор $\frac{1}{n!}\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^n : \mathcal{A}(B) \to \mathcal{A}(B)$ является непрерывным линейным оператором (с нормой R^{-n}).* □

Следствие 10.14. *Пусть $f_n \in \mathcal{A}(B)$, $n \in \mathbb{N}$, причём $\lim\limits_{n\to\infty} \|f_n\|_{a,R} = 0$. Тогда для бесконечного произведения*

$$f(z) = \prod_{n=1}^{\infty} \bigl(1 + f_n(z)\bigr) = \lim_{N\to\infty} \prod_{n=1}^{N} \bigl(1 + f_n(z)\bigr)$$

выполнено $f \in \mathcal{A}(B)$. □

Начиная с этого момента и до конца главы можно предполагать, что поле F алгебраически замкнуто. Это гарантирует плотность группы G_F в $[0,+\infty)$, а также алгебраическую замкнутость поля вычетов k_F (в частности, k_F бесконечно). Для большинства утверждений алгебраическая замкнутость не нужна, и я буду явно указывать, какие именно дополнительные свойства используются в доказательствах.

Теорема 10.15. *Допустим, что поле вычетов k_F бесконечно и $R \in G_F$. Тогда справедливы равенства*

$$\|f\|_{a,R} = \max_{z\in B}\|f(z)\| = \max_{\|z-a\|=R}\|f(z)\|.$$

(*В частности, оба максимума достигаются.*)

Доказательство. С помощью линейной замены общий случай можно свести к случаю $a = 0$, $R = 1$, т. е. $B = \mathbb{Z}_F$. Более того, обрубив ряд в нужном месте и домножив на подходящий множитель, всё можно свести к случаю, когда $f(z) \in \mathbb{Z}_F[z]$, причём $\|f\|_{0,1} = 1$. Но в этом случае утверждение очевидно: нужно найти $\overline{\alpha} \in k_F^*$, такое что $\overline{f}(\overline{\alpha}) \neq \overline{0}$. □

Следствие 10.16 (принцип максимума)**.** *В условиях теоремы 10.15 справедливо равенство*

$$\max_{z\in B}\|f(z)\| = \max_{\|z-a\|=R}\|f(z)\|,$$

причём если $\|f\|_{a,R} > \|f(a)\|$, то для всех $b \in B_R(a)$ выполнено

$$\|f(b)\| < \max_{z\in B}\|f(z)\|.$$ □

Следствие 10.17 (неравенства Коши)**.** *В условиях теоремы 10.15 для любого $n \in \mathbb{N}_0$ справедливо неравенство*

$$\left\|\frac{f^{(n)}(a)}{n!}\right\| \leqslant \max_{z\in B}\|f(z)\| \cdot R^{-n}.$$ □

Определение 10.18. Функция $f : F \to F$ называется *целой*, если она является строго аналитической в любом шаре; равносильно: существует степенной ряд $S(z) \in F[\![z]\!]$ с $R(S) = +\infty$, такой что $f(z) = S(z)$.

Следствие 10.19 (теорема Лиувилля)**.** *Допустим, что поле вычетов k_F бесконечно. Тогда любая ограниченная целая функция является постоянной.* □

Теорема 10.20. *Допустим, что группа G_F плотна в $[0,+\infty)$. Тогда (для произвольного $R > 0$) справедливо равенство*

$$\|f\|_{a,R} = \sup_{z\in B}\|f(z)\|.$$

Более того, если $R \in G_F$, то выполнено

$$\|f\|_{a,R} = \sup_{\|z-a\|<R}\|f(z)\| = \sup_{\|z-a\|=R}\|f(z)\|.$$ □

Следствие 10.21 (снова теорема Лиувилля)**.** *Допустим, что группа G_F плотна в $[0,+\infty)$. Тогда любая ограниченная целая функция является постоянной.* □

Пример 10.22 («контрпример» к теореме Лиувилля для $\mathbb{Q}_p$)**.** Приведём пример ненулевой целой функции $f(z)$ над полем $\mathbb{Q}_p$, удовлетворяющей условию

$$\lim_{|z|_p \to +\infty} \big|f(z)\big|_p = 0.$$

Для этого рассмотрим многочлен $P(z) = 1 - z^{p-1}$. Легко видеть, что

$$\big|P(z)\big|_p = \begin{cases} 1, & |z|_p < 1, \\ |z|_p^{p-1}, & |z|_p > 1, \end{cases}$$
$$\max_{|z|_p = 1} \big|P(z)\big|_p = p^{-1}.$$

Рассмотрим последовательность многочленов

$$P_N(z) = \prod_{n=1}^{N} \big(P(p^n z)\big)^{k_n},$$

где натуральные числа k_n удовлетворяют рекуррентному соотношению

$$k_N = (p-1) \sum_{n=1}^{N-1} n k_{N-n} + N,$$

Несложно проверить, что при $N \geqslant m \geqslant 0$ выполнено

$$\max_{|z|_p = p^m} \big|P_N(z)\big|_p = p^{-m}.$$

Следовательно, в качестве искомой целой (см. следствие 10.14) функции годится

$$f(z) = \lim_{N \to \infty} P_N(z) = \prod_{n=1}^{\infty} \big(P(p^n z)\big)^{k_n}.$$

Упражнение 10.23. Обобщить предыдущий пример на произвольное локально компактное поле. (Таким образом, следствия 10.19 и 10.21 охватывают все случаи, когда справедлива теорема Лиувилля.)

Теорема 10.24 (теорема Вейерштрасса)**.** *Допустим, что выполнены условия теоремы 10.15 или теоремы 10.20. Пусть* $f_n(z) \rightrightarrows\limits_{n\to\infty} f(z)$ *при* $z \in B$, *причём* $f_n \in \mathcal{A}(B)$, $n \in \mathbb{N}$. *Тогда* $f \in \mathcal{A}(B)$. *Более того, для любого* $k \in \mathbb{N}_0$ *выполнено* $\dfrac{f_n^{(k)}(z)}{k!} \rightrightarrows\limits_{n\to\infty} \dfrac{f^{(k)}(z)}{k!}$ *при* $z \in B$. □

Пример 10.25 («контрпример» к теореме Вейерштрасса для $\mathbb{Q}_p$)**.** Вспомним представителей Тейхмюллера (см. пример 4.2): $\omega(z) = \lim\limits_{n\to\infty} z^{p^n}$. Легко видеть, что сходимость равномерная на $\mathbb{Z}_p$, однако $\omega \notin \mathcal{A}\big(\mathbb{Z}_p\big)$, поскольку $\omega(z) = 0$ при $|z|_p < 1$.

Введём обозначение

$$\mathcal{R}(B) = \{f(z) \in F(z) \mid f \text{ не имеет полюсов в } B\}.$$

Элементы $\mathcal{R}(B)$ можно рассматривать как функции из B в F.

Теорема 10.26. *Допустим, что поле* F *алгебраически замкнуто. Тогда справедливо включение* $\mathcal{R}(B) \subseteq \mathcal{A}(B)$, *причём* $\mathcal{R}(B)$ *плотно в* $\mathcal{A}(B)$ *в топологии равномерной сходимости.* □

Замечание 10.27. Утверждение теоремы 10.26 можно положить в основу определения аналитических функций для множеств, не являющихся шарами.

Глава 11

Экспонента и логарифм

11.1 Экспонента и логарифм

Будем предполагать, что F — полное неархимедово нормированное поле характеристики 0, поле вычетов k_F которого имеет характеристику $p > 0$ (т. е. $\|p\| < 1$). Примеры: поле p-адических чисел $\mathbb{Q}_p$, его конечные расширения и пополнение $\mathbb{C}_p$ его алгебраического замыкания.

Для определённости будем считать, что $\|p\| = p^{-1}$, а также определим показатель $\nu\colon F \to \mathbb{R} \cup \{+\infty\}$ стандартным образом:

$$\|\alpha\| = p^{-\nu(\alpha)}.$$

Рассмотрим функции ($z \in F$)

$$E(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!},$$
$$L(z) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(z-1)^n}{n}.$$

Некоторые простейшие свойства:

1) Ряд для $E(z)$ сходится $\iff z \in B_0 = B_{p^{-1/(p-1)}}(0) = \{z \in F \mid \nu(z) > 1/(p-1)\}$, причём $E'(z) = E(z)$, $z \in B_0$.

2) Ряд для $L(z)$ сходится $\iff z \in U_0 = B_1(1) = \{z \in F \mid \|z-1\| < 1\}$, причём $L'(z) = 1/z$, $z \in U_0$.

3) Для произвольных $x, y \in B_0$ выполнено $E(x+y) = E(x)E(y)$. В частности, справедливо равенство $E(z)E(-z) = 1$ (так что $E(z) \neq 0$).

4) Для произвольных $u, v \in U_0$ выполнено $L(uv) = L(u) + L(v)$.

5) Если $z \in B_0$, то $E(z) \in 1 + B_0$, $L(1+z) \in B_0$, причём справедливы равенства $L\big(E(z)\big) = z$, $E\big(L(1+z)\big) = 1 + z$.

Пара слов про доказательства. Для проверки тождеств проще всего воспользоваться тем, что аналитическая функция с нулевой производной является постоянной. Для проверки последнего тождества дифференцировать нужно функцию $(1+z)E\big(-L(1+z)\big)$. Можно также проделать манипуляции с рядами и проапеллировать к вещественному случаю, как в доказательстве леммы 5.12. Для доказательства аналитичности композиций учесть, что если $v(z) = 1/(p-1) + \varepsilon$, $n \in \mathbb{N}$, то

$$v\left(\frac{z^n}{n}\right) \geqslant v\left(\frac{z^n}{n!}\right) = n\,v(z) - \frac{n - S_p(n)}{p-1} \geqslant \frac{1}{p-1} + n\varepsilon. \qquad \square$$

Следствие 11.1. *Функции E и L являются взаимно обратными изоморфизмами аддитивной группы B_0 и мультипликативной группы $1 + B_0$.* $\square$

Следствие 11.2. *Уравнение $L(z) = 0$ имеет единственное решение $z = 1$ (кратности один) в шаре $1 + B_0$ (для любого поля F).* $\square$

Следствие 11.3. *Уравнение $L(z) = 0$, $z \in 1 + p\mathbb{Z}_p$, имеет единственное решение $z = 1$, если $p > 2$, и два решения $z = \pm 1$, если $p = 2$.* $\square$

Следствие 11.4. *В поле $\mathbb{Q}_2$ справедливо равенство*

$$\sum_{n=1}^{\infty} \frac{2^n}{n} = 0. \qquad \square$$

Следствие 11.5. *Группа корней из 1 в $\mathbb{Q}_p$ конечна и имеет порядок* $\begin{cases} p-1, & p > 2, \\ 2, & p = 2. \end{cases}$ $\square$

Теорема 11.6. *Все решения уравнения $L(z) = 0$ в шаре U_0 (для произвольного поля F) — это в точности корни уравнений $z^{p^n} = 1$, $n = 0, 1, 2, \ldots$, причём все решения имеют кратность один. Кроме того, если z — примитивный корень степени p^n из 1, $n \in \mathbb{N}$, то*

$$v(z-1) = \frac{1}{\varphi(p^n)} = \frac{1}{p^{n-1}(p-1)}.$$

Доказательство. Пусть $L(z) = 0$, $z \in U_0$.

Запишем $z = 1 + x$, $v(x) > 0$. Если $v(x) > 1/(p-1)$, то утверждение сразу следует из следствия 11.2. Допустим, что $v(x) \leqslant 1/(p-1)$.

Имеем

$$z^p = 1 + \binom{p}{1}x + \cdots + \binom{p}{p-1}x^{p-1} + x^p,$$

откуда

$$v(z^p - 1) \geqslant \min\big\{v(x) + 1, p\,v(x)\big\} = p\,v(x) = p\,v(z-1).$$

Продолжая в том же духе, найдётся $n \in \mathbb{N}$, такое что $v\big(z^{p^n} - 1\big) > 1/(p-1)$. При этом

$$L\big(z^{p^n}\big) = p^n L(z) = 0.$$

Следовательно, $z^{p^n} = 1$.

Обратно, пусть $z^{p^n} = 1$. Основная трудность — доказать, что $z \in U_0$.

Это несложно увидеть, заметив, что в поле вычетов k_F выполнено

$$\overline{z}^{p^n} = \overline{1} = \overline{z}^{p^f - 1},$$

где $f = f_{\mathbb{Q}_p(z)/\mathbb{Q}_p}$, откуда $\overline{z} = \overline{1}$, что и требуется. Найти $v(z-1)$ несколько сложнее.

Случай $n = 0$ тривиален, поэтому пусть $n > 0$, причём n наименьшее возможное. Тогда $(z-1)$ — корень многочлена

$$\frac{(x+1)^{p^n} - 1}{(x+1)^{p^{n-1}} - 1}.$$

Легко проверить, что это многочлен Эйзенштейна над полем $\mathbb{Q}_p$, откуда всё следует. □

11.2 Теорема Скулема–Малера–Леха

Теорема 11.7 (the Skolem–Mahler–Lech theorem[1])**.** *Пусть F — произвольное поле характеристики 0, $\{a_n\}_{n \geqslant 0} \subseteq F$ — линейная рекуррентная последовательность над F, т. е. последовательность, удовлетворяющая рекуррентному соотношению вида*

$$a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_d a_{n-d} = 0, \quad n \geqslant d,$$

с некоторыми фиксированными $c_i \in F$, $1 \leqslant i \leqslant d$. Тогда множество

$$\{n \in \mathbb{N}_0 \mid a_n = 0\}$$

является объединением конечного числа (бесконечных) арифметических прогрессий и некоторого конечного множества. Более того, если это множество бесконечно, то либо $a_n = 0$ при всех $n \geqslant n_0$, либо характеристический многочлен

$$\lambda^d + c_1 \lambda^{d-1} + \cdots + c_d \tag{11.1}$$

имеет два различных корня (в F^{alg}), отношение которых является корнем из единицы.

Теорема названа в честь трёх математиков:

- Thoralf Albert Skolem (Туральф Альберт Скулем), 1934: $F = \mathbb{Q}$;
- Kurt Mahler, 1935: $F = \mathbb{Q}^{\mathrm{alg}}$;
- Christer Lech, 1953: произвольное F, $\operatorname{char} F = 0$.

Пример 11.8 («контрпример» для характеристики $p > 0$)**.** Пусть $F = \mathbb{F}_p(x)$, где x — переменная. Рассмотрим линейную рекурренту

$$a_n = (1+x)^n - 1 - x^n.$$

Несложно видеть, что

$$a_n = 0 \iff n = p^m, \ m \in \mathbb{N}_0.$$

Заметим, что для $F = \mathbb{F}_p^{\mathrm{alg}}$ утверждение теоремы о структуре множества нулей справедливо по тривиальной причине: в этом случае каждая линейная рекуррента периодическая (поскольку все a_n лежат в конечном поле $\mathbb{F}_p(c_1, \ldots, c_d, a_0, \ldots, a_{d-1})$).

[1] Ch. Lech. «A note on recurring series». *Ark. Mat.* **2**:5 (1953), 417–421; DOI:10.1007/bf02590997.

Замечание 11.9. Заметим, что последнее утверждение в теореме (про корни характеристического многочлена) не зависит от выбора алгебраического замыкания F^{alg} (поскольку любые два алгебраических замыкания изоморфны над F). Непосредственно это можно увидеть так. Поскольку $\operatorname{char} F = 0$, то количество различных корней многочлена $f(z)$ равно

$$\deg \frac{f(z)}{\gcd\bigl(f(z), f'(z)\bigr)}.$$

Поэтому то, что какие-то два (различных) корня $f(z)$ отличаются на корень n-й степени из 1, равносильно тому, что

$$\deg \frac{f_n(z)}{\gcd\bigl(f_n(z), f_n'(z)\bigr)} < \deg \frac{f(z)}{\gcd\bigl(f(z), f'(z)\bigr)},$$

где $f_n(z)$ — многочлен, корнями которого являются n-е степени корней многочлена $f(z)$ (с учётом кратностей). При этом $f_n(z)$ однозначно восстанавливается по $f(z)$ (по теореме Виета и теореме о симметрических многочленах), если положить старший коэффициент равным 1.

Мы ограничимся доказательством теоремы Скулема (для $F = \mathbb{Q}$). Общий случай можно доказать аналогично, если воспользоваться следующей теоремой Касселса[2] (без доказательства).

Теорема о вложении. *Пусть $F = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ — конечно порождённое расширение $\mathbb{Q}$, причём $\alpha_1 \cdots \alpha_n \neq 0$. Тогда существует бесконечно много простых чисел p, для которых существует вложение $i\colon F \hookrightarrow \mathbb{Q}_p$, такое что $i(\alpha_\nu) \in \mathbb{Z}_p^\times$, $1 \leqslant \nu \leqslant n$.* □

Доказательство теоремы Скулема

Не теряя общности, можно считать, что $c_d \neq 0$.

Фиксируем простое число p, такое что все $c_i \in \mathbb{Z}_p$, причём $|c_d|_p = 1$.

Пусть $\alpha_1, \dots, \alpha_m \in \mathbb{Q}_p^{\mathrm{alg}}$ — все различные корни характеристического многочлена (11.1). Тогда

$$a_n = \sum_{j=1}^{m} P_j(n)\alpha_j^n \tag{11.2}$$

для некоторых многочленов $P_j(z) \in \mathbb{Q}_p^{\mathrm{alg}}[z]$.

Рассмотрим поле $K = \mathbb{Q}_p(\alpha_1, \dots, \alpha_m)$. Пусть $f = f_{K/\mathbb{Q}_p}$ — степень поля вычетов расширения $K/\mathbb{Q}_p$, т. е. $k_K = \mathbb{F}_{p^f}$. Из условий на c_i следует (неплохо бы добавить ссылку), что $|\alpha_j|_p = 1$, поэтому $\left|\alpha_j^{p^f-1} - 1\right|_p < 1$.

Рассуждая так же, как при доказательстве теоремы 11.6, найдём $l \in \mathbb{N}_0$, такое что $\nu_p\left(\alpha_j^{p^l(p^f-1)} - 1\right) > 1/(p-1)$. Положим $D = p^l\bigl(p^f - 1\bigr)$. Согласно свойству 5 экспоненциальной и логарифмической функций, имеем

$$\alpha_j^D = E\Bigl(L\bigl(\alpha_j^D\bigr)\Bigr). \tag{11.3}$$

[2] J. W. S. Cassels. «An embedding theorem for fields». *Bull. Aust. Math. Soc.* **14**:2 (1976), 193–198; DOI:10.1017/s000497270002503x.

Фиксируем $r \in \{0, 1, \dots, D-1\}$. Для доказательства теоремы Скулема достаточно показать, что если $a_{r+Dn} = 0$ для бесконечно многих $n \in \mathbb{N}_0$, то $a_{r+Dn} = 0$ для всех $n \in \mathbb{N}_0$. (Из общих свойств линейных рекуррент следует, что в этом случае либо все многочлены P_j в представлении (11.2) нулевые, либо найдутся $i \neq j$, такие что $\alpha_i^D = \alpha_j^D$.)

Из равенства (11.3) и свойств экспоненты следует равенство $a_{r+Dn} = g(n)$, где

$$g(z) = \sum_{j=1}^{m} P_j(r + Dz)\, \alpha_j^r\, E\Big(zL\big(\alpha_j^D\big)\Big).$$

Функция g является строго аналитической в шаре $\mathbb{Z}_K$, поэтому из следствия 10.11 получаем требуемое.