

Летняя математическая школа ЛНМО

Поставы, 2022г.

Алгебраическая геометрия и теория чисел

**In nature, poisonous creatures
will develop bright colors to
warn others of their toxicity**



**Graduate Texts
in Mathematics**

Robin Hartshorne

**Algebraic
Geometry**

 Springer

*Конспект по материалам лекций, прочитанных М.И. Магиным
11-му математическому классу*



Лаборатория непрерывного
математического образования

Алгебраическая геометрия и теория чисел

Содержание

1. Нормированные поля	2
1.1 Нормированное поле. Неархимедовы нормы.	2
2. p-адические числа	4
2.1 Кольцо целых p -адических чисел.	4
2.2 Локализация и поле частных колца.	6
2.3 Поле p -адических чисел, как поле частных колца \mathbb{Z}_p	9
2.4 Сходимость в поле p -адических чисел	10
2.5 Лемма Гензеля:	14
2.6 Пополнение метрических пространств.	16
2.7 Пополнение нормированного поля.	17
3. Введение в алгебраическую геометрию	19
3.1 Квадратичные формы и квадратики	19

1. Нормированные поля

1.1 Нормированное поле. Неархимедовы нормы.

Здесь и в дальнейшем будем полагать F полем, хотя многие вещи работают и для кольца (а для области целостности существует единственное продолжение на поле частных).

Definition 1. Нормой (нормированием, абсолютным значением) на поле F называют отображение $\|\cdot\|: F \rightarrow \mathbb{R}_{>0}$, удовлетворяющее следующим свойствам:

1. $\|x\| = 0 \Leftrightarrow x = 0$.
2. $\forall x, y \in F \quad \|xy\| = \|x\|\|y\|$.
3. $\exists C > 0: \forall x, y \in F:$

$$\|x + y\| \leq C \cdot \max(\|x\|, \|y\|)$$

Пара $(F, \|\cdot\|)$ называется нормированным полем.

Remark 1. Тем, кто уже до этого видел определение нормы, это определение может показаться странным, так как обычно вместо третьего свойства требуют неравенство треугольника:

$$\forall x, y \in F \quad \|x + y\| \leq \|x\| + \|y\|$$

Ясно, что третье свойство следует из неравенства треугольника с $C = 2$. Ниже мы покажем и обратную импликацию.

Ясно, что любая норма задаёт метрику $d(x, y) = \|x - y\|$, а любая метрика индуцирует топологию стандартным образом.

Example 1. Если $F \leq \mathbb{C}$, то подходит $|\cdot|$ (модуль комплексного числа). Если $F \leq \mathbb{R}$ или $F \leq \mathbb{Q}$, то подходит $|\cdot|$.

Example 2. На любом поле можно ввести тривиальную норму (иногда соответствующую ей метрику называют метрикой лентяя):

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

Theorem 1. Если в определении 1 постоянная C равна 2, то норма удовлетворяет неравенству треугольника.

Доказательство. Сначала отметим, что если $n, m \in \mathbb{N}$, $n \leq 2^m$, то в случае произвольной постоянно C выполняется оценка:

$$\|x_1 + x_2 + \dots + x_n\| \leq C^m \cdot \max_{1 \leq k \leq n} \|x_k\|$$

В самом деле, достаточно просто расписать дерево неравенств.

Отсюда следует неравенство

$$\|x_1 + \dots + x_n\| \leq (2n)^{c_0} \max_{1 \leq k \leq n} (\|x_k\|), \quad c_0 = \log_2 C$$

В самом деле, $(2n)^{\log_2 C} = C \cdot n^{\log_2 C}$. Это также даёт удобную оценку: $\|n\| \leq (2n)^{c_0}$.

Теперь заметим, что в нашем случае $c_0 = \log_2 C = \log_2 2 = 1$, а значит, мы можем провести вот такую оценку:

$$\begin{aligned} \|x+y\|^n &= \|(x+y)^n\| = \left\| \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \right\| \leq 2(n+1) \max_{0 \leq k \leq n} \left\| \binom{n}{k} x^k y^{n-k} \right\| \leq 2(n+1) \max_{0 \leq k \leq n} \left(2 \binom{n}{k} \|x\|^k \|y\|^{n-k} \right) \leq \\ &\leq 4(n+1)(\|x\| + \|y\|)^n \end{aligned}$$

Преобразуем это неравенство

$$\left(\frac{\|x+y\|}{\|x\| + \|y\|} \right)^n \leq 4(n+1) \Leftrightarrow \frac{\|x+y\|}{\|x\| + \|y\|} \leq 4^{\frac{1}{n}} \cdot (n+1)^{\frac{1}{n}}$$

В пределе при $n \rightarrow \infty$ получаем:

$$\frac{\|x+y\|}{\|x\| + \|y\|} \leq 1 \Leftrightarrow \|x+y\| \leq \|x\| + \|y\|$$

□

Remark 2. Пример $F = \mathbb{C}$ с нормой $\|\cdot\| = |\cdot|^\alpha$, $\alpha > 1$ показывает, что константу $C = 2$ нельзя улучшить.

Remark 3. Тем самым, мы показали, что норму можно понимать, как функтор из категории \mathcal{Field} в категорию \mathcal{Metr} .

Corollary 1. Норма непрерывна.

Definition 2. Нормы, с постоянной $C = 1$ в определении 1 называют неархимедовыми. Нормы, не являющиеся неархимедовыми, называют архимедовыми.

Example 3. Тривиальная норма на любом поле F является неархимедовой.

Definition 3. Ясно, что любое $x \in \mathbb{Q}$ представимо в виде $x = p^n \cdot \frac{a}{b}$, где $a, b \in \mathbb{Z}$, $a \not\equiv p$, $b \not\equiv p$, $a \in \mathbb{Z}$. В таком случае число n называют p -адическим показателем числа x и обозначают $v_p(x)$.

Definition 4. (Самое важное)

Пусть p — простое число. Тогда норму

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

на поле \mathbb{Q} называют p -адической нормой.

Remark 4. Ясно, что подходит $r^{-v_p(x)}$, где $r > 1$, но p брать удобно, так как для $x \in \mathbb{Q}^*$ справедлива формула произведения

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

Lemma 1. Если норма неархимедова, то для x, y : $\|x\| \neq \|y\|$ выполняется $\|x+y\| = \max\{\|x\|, \|y\|\}$.

Corollary 2. Рассмотрим $(F, \|\cdot\|)$, где норма $\|\cdot\|$ неархимедова. Тогда, если $b \in B_r(a)$, то $B_r(a) = B_r(b)$.

Corollary 3. (Забавное)

Если на поле F введена неархимедова норма F , то $\forall x, y, z \in F$ по крайней мере два числа из $\|x-y\|$, $\|x-z\|$, $\|y-z\|$ равны.

Иными словами, в метрическом пространстве (F, d) ($d(x, y) = \|x-y\|$) все треугольники равнобедренные.

2. p -адические числа

2.1 Кольцо целых p -адических чисел.

Прежде чем давать какие-либо определения, рассмотрим следующий мотивирующий пример. Рассмотрим сравнение $x^2 \equiv 2 \pmod{7^n}$, $n \in \mathbb{N}$. Если $n = 1$, то ясно, что

$$x_0 \equiv \pm 3 \pmod{7}$$

Теперь рассмотрим $n = 2$. $x^2 \equiv 2 \pmod{7^2} \Rightarrow x^2 \equiv 2 \pmod{7}$, а значит, решения сравнения с $n = 2$ надо искать в виде $x_0 + 7t_1$.

Займемся поиском решений вида $x_1 = 3 + 7t_1$. Подставим:

$$(3 + 7t_1)^2 \equiv 2 \pmod{7^2} \Leftrightarrow 9 + 6 \cdot 7t_1 + 7^2 t_1^2 \equiv 2 \pmod{7^2} \Rightarrow 1 + 6t_1 \equiv 0 \pmod{7} \Rightarrow t_1 \equiv 1 \pmod{7}$$

Отсюда имеем решение $x_1 \equiv 3 + 7 \cdot 1 \pmod{7^2}$.

При $n = 3$ мы получим $x_2 = x_1 + 7^2 t_2$ и подставляя

$$(3 + 7 + 7^2 t_2)^2 \equiv 2 \pmod{7^3}$$

мы найдём $t_2 \equiv 2 \pmod{7}$, а значит,

$$x_2 \equiv 3 + 7 \cdot 1 + 7^2 \cdot 2 \pmod{7^3}$$

Продолжая этот процесс, получим последовательность $x_0, x_1, x_2, \dots, x_n, \dots$ со свойствами

$$x_0 \equiv 3 \pmod{7}, \quad x_n \equiv x_{n-1} \pmod{7^n}, \quad x_n^2 \equiv 2 \pmod{7^{n+1}}$$

Процесс построения этой последовательности может напомнить внимательному читателю процесс вычисления $\sqrt{2}$ при помощи приближения рациональными числами. Там мы тоже строим последовательность рациональных чисел r_1, r_2, \dots, r_n , квадраты которых становятся сколь угодно близки к 2, например, $|r_n^2 - 2| < 1/10^n$.

Если мы зафиксируем простое число p будем считать два целых числа близкими, если их разность делится на достаточно большую степени p (то есть, близкими в смысле p -адической метрики):

$$d_p(x, y) = \|x - y\|_p = p^{-v_p(x-y)}$$

В конкретном примере выше,

$$\forall \varepsilon > 0 \exists N: \forall n \geq N \ d_7(x_n^2, 2) < \varepsilon$$

Как мы помним, задание последовательности рациональных чисел $\{r_n\}$ определяет вещественное число $\sqrt{2}$. Проводя аналогию, здесь мы также можем предположить, что последовательность $\{x_n\}$ определяет некоторое число α совершенно новой природы.

Заметим также, что если у нас есть такая последовательность рациональных чисел $\{r'_n\}$, что $\forall \varepsilon > 0 \exists N: \forall n > N \ |r_n - r'_n| < \varepsilon$, то её пределом также будет $\sqrt{2}$ (и в этом смысле определение корректно). Соответственно, здесь нам также будет естественно предположить, что последовательность $\{x'_n\}$, для которой $x_n \equiv x'_n \pmod{7^{n+1}}$ определяет то же самое число α .

Remark 5. В общем, во всей этой аналогии мы просто заменили метрику на p -адическую.

Definition 5. Пусть p — некоторое простое число. Последовательность целых чисел $\{x_n\}$, обладающих свойством

$$x_n \equiv x_{n-1} \pmod{p^n} \quad \forall n \geq 1$$

определяет новый объект, называемый p -адическим числом. Две последовательности $\{x_n\}$ и $\{x'_n\}$ определяют одно и то же целое p -адическое число, когда $x_n \equiv x'_n \pmod{p^{n+1}} \quad \forall n \geq 0$.

То есть, целые p -адические числа — предел по p -адическое норме целых.

Множество всех целых p -адических чисел мы будем обозначать через \mathbb{Z}_p .

Обычные целые числа (не p -адические) будем с этого момента называть целыми рациональными.

Заметим, что каждому целому рациональному числу x можно сопоставить целое p -адическое число, определяемое последовательностью $\{x, x, x, \dots\}$. Такое целое p -адическое число мы будем обозначать той же буквой x . Таким образом, мы получили естественное вложение $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ (инъективность вполне очевидна).

Remark 6. Канонический способ задания p -адического числа.

Пусть целое p -адическое число задается последовательностью $\{x_n\}$. Обозначим наименьшее неотрицательное число, сравнимое с x_n по модулю p^{n+1} за $\overline{x_n}$.

$$x_n \equiv \overline{x_n} \pmod{p^{n+1}}, \quad 0 \leq \overline{x_n} < p^{n+1}$$

Ясно, что

$$\overline{x_n} \equiv x_n \equiv x_{n-1} \equiv \overline{x_{n-1}} \pmod{p^n}$$

То есть, последовательность $\{\overline{x_n}\}$ определяют то же целое p -адическое число, что и $\{x_n\}$. Заметим, что если две последовательности $\{\overline{x_n}\}$ и $\{\overline{y_n}\}$ определяют одно и то же целое p -адическое число, то в силу

$$\overline{x_n} \equiv \overline{y_n} \pmod{p^{n+1}}, \quad 0 \leq \overline{x_n} < p^{n+1}, \quad 0 \leq \overline{y_n} < p^{n+1}$$

мы имеем $\overline{x_n} = \overline{y_n}$, то есть, такое представление единственно. Его мы и будем называть каноническим представлением.

Заметим, что $\overline{x^n} \equiv \overline{x_{n-1}} \pmod{p^n}$, а так как $0 \leq \overline{x_n} < p^{n+1}$, вся каноническая последовательность имеет вид

$$\{a_0, a_0 + a_1p, a_0 + a_1p + a_2p^2, \dots\}, \quad 0 \leq a_i < p$$

С другой стороны, ясно, что каждая последовательность такого вида задаёт некоторое целое p -адическое число.

Ясно, что операции сложения и умножения на p -адических числах определяются поточечными операциями с соответствующими последовательностями.

Все свойства операций очевидны, значит, \mathbb{Z}_p — коммутативное кольцо. Поймём что-нибудь про множество обратимых элементов кольца.

Theorem 2. Целое p -адическое число α , определяемое последовательностью $\{x_0, x_1, \dots, x_n, \dots\}$ я тогда и только тогда, когда $x_0 \not\equiv 0 \pmod{p}$.

Доказательство. Пусть $\alpha \in \mathbb{Z}_p^*$. Тогда существует такое целое p -адическое число β , что $\alpha\beta = 1$.

Пусть β определяется последовательностью $\{y_n\}$. Тогда

$$x_n y_n \equiv 1 \pmod{p^{n+1}}$$

В частности, $x_0 y_0 \equiv 1 \pmod{p} \Rightarrow x_0 \not\equiv 0 \pmod{p}$. И обратно, так как $x_0 \not\equiv 0 \pmod{p}$ и $x_n \equiv x_{n-1} \pmod{p^n}$ мы имеем

$$x_n \equiv x_{n-1} \equiv \dots \equiv x_0 \pmod{p} \Rightarrow x_n \not\equiv 0 \pmod{p}$$

Значит, так как p — простое, $\forall n \exists y_n: x_n y_n \equiv 1 \pmod{p^{n+1}}$.

$$x_n \equiv x_{n-1} \pmod{p^n}, \quad x_n y_n \equiv x_{n-1} y_{n-1} \pmod{p^n} \Rightarrow y_n \equiv y_{n-1} \pmod{p^n}$$

а значит, $\{y_n\}$ определяет некоторое целое p -адическое число β .

Таким образом, $\alpha\beta = 1 \Rightarrow \alpha \in \mathbb{Z}_p^*$. □

Theorem 3. Любое отличное от нуля целое p -адическое число α можно единственным образом представить в виде

$$\alpha = p^m \cdot \varepsilon, \quad \varepsilon \in \mathbb{Z}_p^*, \quad m \in \mathbb{N}$$

Доказательство. Если $\alpha \in \mathbb{Z}_p^*$, то равенство справедливо при $m = 0$.

Пусть теперь $\alpha \notin \mathbb{Z}_p^*$ и $\{x_n\} \rightarrow \alpha$. Тогда, по предыдущей теореме $x_0 \equiv 0 \pmod{p}$. Так как $\alpha \neq 0$, $\exists N \in \mathbb{N}: \forall n \geq N \quad x_n \not\equiv 0 \pmod{p^{n+1}}$. Пусть m — наименьший индекс, для которого

$$x_m \not\equiv 0 \pmod{p^{m+1}}$$

Заметим, что в таком случае $\forall s \geq 0$

$$x_{m+s} \equiv x_{m-1} \equiv 0 \pmod{p^m} \Rightarrow y_s = \frac{x_{m+s}}{p^m} \in \mathbb{Z}$$

$$p^m y_s - p^m y_{s-1} = x_{m+s} - x_{m+s-1} \equiv 0 \pmod{p^{m+s}} \Rightarrow y_s \equiv y_{s-1} \pmod{p^s}$$

То есть, последовательность $\{y_s\}$ тоже определяет некоторое p -адическое число $\varepsilon \in \mathbb{Z}_p$. Заметим, что $y_0 = x_m/p^m \not\equiv 0 \pmod{p} \Rightarrow \varepsilon \in \mathbb{Z}_p^*$.

Из сравнения

$$p^m y_s = x_{m+s} \equiv x_s \pmod{p^{s+1}}$$

следует, что $\alpha = p^m \cdot \varepsilon$. Покажем теперь единственность. Предположим, что $\alpha = p^k \xi$, $k \geq 0$, $\xi \in \mathbb{Z}_p^*$. Пусть $\{z_s\} \rightarrow \xi$.

$$p^m y_s \equiv p^k z_s \pmod{p^{s+1}} \quad \forall s \geq 0$$

Так как ε и ξ — обратимые элементы кольца, по предыдущей теореме $y_s \not\equiv 0 \pmod{p}$, $z_s \not\equiv 0 \pmod{p}$. Подставим в предыдущее сравнения $s = m$:

$$p^m y_m \equiv p^k z_m \not\equiv 0 \pmod{p^{m+1}} \Rightarrow k \leq m$$

Так как мы можем проделать то же самое абсолютно симметрично для k , мы также имеем $k \geq m$, а значит $k = m$. То есть, мы получили, что $y_{m+s} \equiv z_{m+s} \pmod{p^{s+1}}$, а так как $y_{s+1} \equiv y_s \pmod{p^{s+1}}$, $z_{s+1} \equiv z_s \pmod{p^{s+1}}$, мы имеем $z_s \equiv y_s \pmod{p^{s+1}} \quad \forall s \geq 0 \Rightarrow \varepsilon = \xi$. \square

Corollary 4. \mathbb{Z}_p — область целостности.

Доказательство. Упражнение в листочке. \square

Теперь ясно, что число m в представлении $\alpha = p^m \varepsilon$ — p -адический показатель α ($v_p(\alpha)$).

В терминах p -адического показателя легко выразить свойства делимости p -адических чисел.

Corollary 5. Целое p -адическое число α делится на целое p -адическое число β тогда и только тогда, когда $v_p(\alpha) \geq v_p(\beta)$.

Резюмируя всё это, мы получили, что в кольце \mathbb{Z}_p всего один (с точностью до ассоциированности) простой элемент — число p , а все остальные (отличные от нуля) — его степени, домноженные на обратимые.

2.2 Локализация и поле частных колца.

Вообще, эта тема совершенно никак не относится к программе курса, но, прочитать всё равно надо.

Идея: уметь обращаться набор элементов кольца универсальным образом.

Remark 7. Отметим, что обратимый элемент не может являться делителем нуля, поэтому, если мы хотим обращать делители нуля, все элементы, которые в произведении с ним дают 0 должны перейти в 0. Кроме того, если два элемента обратимы, то их произведение обратимо. Кроме того, если мы добавим в множество, которое хотим обращать единицу, то ничего не изменится, так как умножение на единицу ничего не меняет.

Таким образом, будем заниматься обращением множеств, замкнуты относительно умножения и содержат единицу (будем называть такие множества мультипликативными).

Тут можно рассказать, с чего бы это называется локализацией, но как-то лень, если время останется, расскажу.

Definition 6. Пусть S — мультипликативное подмножество кольца R . Локализацией кольца R в S называется кольцо $S^{-1}R$ вместе с локализационным гомоморфизмом $\lambda_s: R \rightarrow S^{-1}R$, удовлетворяющее свойствам

1. $\forall s \in S \lambda_s(s)$ обратим в $S^{-1}R$.
2. Для любого гомоморфизма $\varphi: R \rightarrow A$, при котором $\varphi(s) \in A^*$ для всех $s \in S$ существует единственный гомоморфизм $\psi: S^{-1}R \rightarrow A$ такой, что $\psi \circ \lambda_s = \varphi$. Иными словами, коммутативна диаграмма

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & A \\ & \searrow \lambda_s & \nearrow \psi \\ & S^{-1}R & \end{array}$$

Как и всегда, определение объекта через универсальное свойство ничего не говорит о существовании объекта, поэтому сейчас мы будем больно и мучительно строить локализацию.

Построение локализации:

Определим отношение \sim на множестве $R \times S$ по правилу

$$(r_1, s_1) \sim (r_2, s_2) \iff ss_2r_1 = ss_1r_2$$

Remark 8. Здесь мы домножаем на s как раз за тем, чтоб делители нуля ушли в ноль.

Statement 1. \sim — отношение эквивалентности.

Доказательство. Рефлексивность и симметричность очевидны.

Самое неприятное — транзитивность.

Пусть $(r_1, s_1) \sim (r_2, s_2)$ и $(r_2, s_2) \sim (r_3, s_3)$, то есть

$$sr_1s_2 = sr_2s_1, \quad s'r_2s_3 = s'r_3s_2, \quad s, s' \in S$$

Домножим первое равенство $s's_3$, а второе ss_1 , получим

$$sr_1s_2 = sr_2s_1 \rightarrow s's_3sr_1s_2 = s's_3sr_2s_1, \quad s'r_2s_3 = s'r_3s_2 \rightarrow ss_1s'r_2s_3 = ss_1s'r_3s_2$$

Остается заметить, что

$$ss's_2 \in S \Rightarrow (r_1, s_1) \sim (r_3, s_3)$$

то есть, транзитивность доказана. □

Теперь, положим $S^{-1}R = R \times S / \sim$. Класс эквивалентности, содержащий представитель (r, s) будем обозначать $\frac{r}{s}$.

Определим локализационный гомоморфизм $\lambda_s: R \rightarrow S^{-1}R$ формулой $\lambda_s(r) = \frac{r}{1}$.

Теперь, научимся складывать дроби.

Theorem 4. Пусть S — мультипликативное подмножество кольца R . Определим на $S^{-1}R$ операции следующим образом

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_2 s_1}, \quad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_1 r_2 + s_2 r_1}{s_1 s_2}$$

Тогда $S^{-1}R$ — локализация R в мультипликативном подмножестве S с локализационным гомоморфизмом λ_s (как написано выше).

Доказательство. Докажем сначала, что наше определение сложения и умножения не зависит от выбора представителя.

Пусть выполняются равенства

$$\frac{r'_1}{s'_1} = \frac{r_1}{s_1} \leftrightarrow s r_1 s'_1 = s r'_1 s_1, \quad \frac{r'_2}{s'_2} = \frac{r_2}{s_2} \leftrightarrow s' r_2 s'_2 = s' r'_2 s_2$$

Перемножим последние равенства

$$s s' r_1 s'_1 r_2 s'_2 = s s' r'_1 s_1 r'_2 s_2$$

Отсюда имеем

$$\frac{r_1 r_2}{s_1 s_2} = \frac{r'_1 r'_2}{s'_1 s'_2}$$

Далее, будет некоторая **боль**, а именно, надо доказать

$$\frac{r_1 s_2 + r_2 s_1}{s_1 s_2} = \frac{r'_1 s'_2 + r'_2 s'_1}{s'_1 s'_2}$$

Если Вы немного помедитируете на формулы ниже, станет понятно, почему это так:

$$s s' (r_1 s_2 + r_2 s_1) s'_1 s'_2 = s s' (s_1 s_2 s'_1 s'_2 + r_2 s_1 s'_1 s'_2) = s s' (r'_1 s_2 s_1 s'_2 + r'_2 s_1 s'_2 s_2) = s s' (r'_1 s'_2 + r'_2 s'_1) s_1 s_2$$

Вообще, честно говоря, также нужно доказывать ассоциативность сложения, коммутативность и дистрибутивность. Давайте непосредственно проверим ассоциативность сложения

$$\left(\frac{r_1}{s_1} + \frac{r_2}{s_2} \right) + \frac{r_3}{s_3} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} + \frac{r_3}{s_3} = \frac{r_1 s_2 s_3 + r_2 s_1 s_3 + r_3 s_1 s_2}{s_1 s_2 s_3}$$

$$\frac{r_1}{s_1} + \left(\frac{r_2}{s_2} + \frac{r_3}{s_3} \right) = \frac{r_1}{s_1} + \frac{r_2 s_3 + r_3 s_2}{s_2 s_3} = \frac{r_1 s_2 s_3 + r_2 s_3 s_1 + r_3 s_2 s_1}{s_1 s_2 s_3}$$

Нейтральным элементом по сложению будет $\frac{0}{1} = \frac{0}{s}$, обратным по сложению к $\frac{r}{s}$ — $-\frac{r}{s}$. Нейтральным элементом по умножению $-\frac{1}{1} = \frac{s}{s}$. Проверим свойства локализации:

$$\lambda_s(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = 1$$

то есть, первое свойство выполнено.

Пусть $\varphi: R \rightarrow A$ — такой гомоморфизм колец, что $\varphi(s) \in A^* \forall s \in S$. Определим отображение $\psi: S^{-1}R \rightarrow A$ равенством $\psi(\frac{r}{s}) = \varphi(r)\varphi(s)^{-1}$.

Если $\frac{r'}{s'} = \frac{r}{s}$, то по определению

$$\frac{r'}{s'} = \frac{r}{s} \Leftrightarrow r's = rs', \quad s'' \in S \Rightarrow \varphi(s'')\varphi(r')\varphi(s) = \varphi(s'')\varphi(r)\varphi(s')$$

Домножим на $\varphi(s'')^{-1}\varphi(s')^{-1}\varphi(s')^{-1}$, получим

$$\varphi(r')\varphi(s')^{-1} = \varphi(r)\varphi(s)^{-1}$$

а значит, ψ определён корректно. Так как $\varphi(1) = 1$, имеем $\varphi = \psi \circ \lambda_S$. Ясно, что ψ — гомоморфизм.

Равенство $\varphi = \psi \circ \lambda_S$ однозначно задаёт $\psi(\frac{r}{1}) = \varphi(r)$. Так как ψ должен быть гомоморфизмом,

$$\varphi(r) = \psi(\frac{r}{1}) = \psi(\frac{r}{s} \cdot \frac{s}{1}) = \psi(\frac{r}{s}) \cdot \varphi(s)$$

Так как по условию $\varphi(s) \in A^*$, имеем $\psi(\frac{r}{s}) = \varphi(r)\varphi(s)^{-1}$, что завершает доказательство. \square

ПРИМЕРЫ ЛОКАЛИЗАЦИИ:

1. Для $s \in R$ положим $\langle s \rangle = \{s^n \mid n \in \mathbb{N}\}$. Локализация $\langle s \rangle^{-1}R$ обозначается через R_s и называется главной локализацией в элементе s (по аналогии с главным идеалом).
2. Если P — простой идеал кольца R , то $R \setminus P$ является мультипликативным подмножеством. В этом случае локализация $R_P = (R \setminus P)^{-1}R$ называется локализацией R в простом идеале P . R_P является локальным кольцом (т.е. кольцом с единственным максимальным идеалом).
3. S — множество всех элементов R , не являющийся делителями нуля. Тогда $S^{-1}R$ называется полным кольцом частных кольца R . Это максимальная локализация, для которой гомоморфизм локализации инъективен.

Если R — область целостности, то $\{0\}$ — простой идеал. Локализация в этом идеале, очевидно, будет полем, которое называется полем частных кольца R .

Иными словами, поле частных — это полное кольцо частных области целостности. Локализационный гомоморфизм — это универсальное вложение в следующем смысле:

Lemma 2. Пусть R — область целостности, а $S = R \setminus \{0\}$. Тогда $F = S^{-1}R$ является полем, а гомоморфизм локализации $\lambda_S: R \rightarrow F$ инъективен, а λ_S удовлетворяет следующему универсальному свойству: для любого поля K и мономорфизма $R \rightarrow K$ существует единственный мономорфизм $\psi: F \rightarrow K$, что $\varphi = \psi \circ \lambda_S$.

2.3 Поле p -адических чисел, как поле частных кольца \mathbb{Z}_p .

Как мы уже выяснили, кольцо \mathbb{Z}_p — область целостности, его можно вложить в поле частных, используя конструкцию локализации.

В нашем случае это сводится к рассмотрению дробей α/p^k , где $\alpha \in \mathbb{Z}_p$, $k \geq 0$.

Definition 7. Дробь вида α/p^k , где $\alpha \in \mathbb{Z}_p$, а $k \geq 0$ называется дробным p -адическим числом или просто p -адическим числом.

Remark 9. Две дроби α/p^k и β/p^m определяют одно и то же p -адическое число, если $\alpha p^m = \beta p^k$.

Definition 8. Полем p -адических чисел \mathbb{Q}_p называется поле частных кольца целых p -адических чисел \mathbb{Z}_p .

Theorem 5. Всякое p -адическое число $\xi \neq 0$ единственным образом представляется в виде

$$\xi = p^m \cdot \varepsilon, \quad m \in \mathbb{Z}, \quad \varepsilon \in \mathbb{Z}_p^*$$

Доказательство. Пусть $\xi = \alpha/p^k$, $\alpha \in \mathbb{Z}_p$. По теореме 3 α можно представить в виде $p^\ell \varepsilon$, $\ell \geq 0, \varepsilon \in \mathbb{Z}_p^*$. Тогда $\xi = p^m \varepsilon$, $m = \ell - k$.

Единственность вытекает из единственности представления для 3. \square

2.4 Сходимость в поле p -адических чисел

Мы уже много раз говорили об аналогии между p -адическими числами и вещественными. В случае вещественных, они определяются последовательностями рациональных и являются пределами этих последовательностей.

Неформально мы уже обсуждали, почему это так в случае p -адических чисел, давайте теперь поймем, почему это так формально.

Теперь, после того как мы доопределили p -адический показатель на \mathbb{Q}_p , мы можем вводить на \mathbb{Q}_p (заметьте, уже не на \mathbb{Q}) знакомое нам p -адическое нормирование (и, соответственно, p -адическую метрику).

Definition 9. Последовательность p -адических чисел $\{\xi_n\}$ называется сходящейся к p -адическому числу ξ если

$$\lim_{n \rightarrow \infty} v_p(\xi_n - \xi) = \infty$$

Remark 10. Ясно, что эквивалентно сходимость можно определять, как

$$\lim_{n \rightarrow \infty} \{\xi_n\} = \xi \Leftrightarrow \lim_{n \rightarrow \infty} \|\xi_n - \xi\| = 0$$

то есть, как и обычно, начиная с некоторого довольно большого номера, p -адические числа становятся сколь угодно близки к пределу.

Рассмотрим сначала для удобства некоторые свойства p -адического показателя:

1. $v_p(\alpha\beta) = v_p(\alpha) + v_p(\beta)$.
2. $v_p(\alpha + \beta) \geq \min(v_p(\alpha), v_p(\beta))$.
3. $v_p(\alpha + \beta) = \min(v_p(\alpha), v_p(\beta))$, $\alpha \neq \beta$.

Для поля \mathbb{Q}_p справедливы все стандартные свойства пределов. Докажем, например, что при $\{\xi_n\} \rightarrow \xi$, $\xi \in \mathbb{Z}_p^*$ выполняется $\{1/\xi_n\} \rightarrow 1/\xi$.

Сначала отметим, что, начиная с некоторого места $v_p(\xi_n - \xi) > v_p(\xi)$, откуда $v_p(\xi_n) = \min(v_p(\xi_n - \xi), v_p(\xi)) = v_p(\xi) \Rightarrow v_p(\xi_n) \neq \infty \Rightarrow \xi_n \neq 0$, то есть, на него в самом деле можно делить.

Далее мы имеем

$$v_p\left(\frac{1}{\xi_n} - \frac{1}{\xi}\right) = v_p(\xi - \xi_n) - v_p(\xi_n) - v_p(\xi) = v_p(\xi_n - \xi) - 2v_p(\xi) \xrightarrow{n \rightarrow \infty} \infty$$

Теперь, для доказательства факта, который мы хотели формализовать, нам нужно понять, как вводятся сравнения на кольце целых p -адических чисел. Сравнения в кольце целых p -адических чисел

определяются также, как и в кольце целых чисел, то есть $\alpha \equiv \beta \pmod{\gamma} \Leftrightarrow (\alpha - \beta) \div \gamma$.

Если $\gamma = p^n \varepsilon$, $\varepsilon \in \mathbb{Z}_p^*$, то всякое сравнение по модулю γ равносильно сравнению по модулю p^n , а значит, достаточно рассматривать только такие (в этом случае).

Theorem 6. *Всякое целое p -адическое число сравнимо с целым рациональным числом по модулю p^n . Два целых рациональных числа тогда и только тогда сравнимы по модулю p^n в кольце \mathbb{Z}_p^* , когда они сравнимы по этому модулю в кольце \mathbb{Z} .*

Доказательство. Докажем сначала, что если α — целое p -адическое число, определяемое последовательностью $\{x_n\}$, то

$$\alpha \equiv x_{n-1} \pmod{p^n}$$

Как целое p -адическое число, x_n определяется последовательностью $\{x_n, x_n, \dots, x_n, \dots\}$. Тогда последовательность, определяющая целое p -адическое число $\alpha - x_n$ выглядит следующим образом

$$\{x_0 - x_{n-1}, x_1 - x_{n-1}, \dots, 0, x_n - x_{n-1}, \dots\}$$

Из того, что всякое целое p -адическое число α представимо в виде

$$\alpha = p^k \cdot \varepsilon, \varepsilon \in \mathbb{Z}_p^*$$

следует, что целое p -адическое число α , определяемое последовательностью $\{y_n\}$ делится на p^ℓ тогда и только тогда, когда $x_n \equiv 0 \pmod{p^{n+1}} \forall n = 0, 1, \dots, k-1$. Тогда, сравнение $\alpha \equiv x_n \pmod{p^n}$ равносильно сравнениям

$$x_k - x_{n-1} \equiv 0 \pmod{p^{k+1}}, k = 0, 1, \dots, n-1$$

а эти сравнения выполнены по определению p -адических чисел.

Докажем теперь, что для двух целых рациональных p -адических чисел x и y сравнимость по модулю p^n в кольце \mathbb{Z}_p равносильна сравнимости по модулю p^n в кольце \mathbb{Z} .

Положим $x - y = p^m a$, $a \not\equiv 0 \pmod{p}$. Тогда, в кольце \mathbb{Z} сравнение $x \equiv y \pmod{p^n}$ равносильно условию $n \leq m$. С другой стороны, так как $a \not\equiv 0 \pmod{p}$, соответствующее ему целое p -адическое число обратимо в \mathbb{Z}_p^* , а значит, для числа $x - y$ есть представление в виде $p^m \alpha$, $\alpha \in \mathbb{Z}_p^*$, а значит, $v_p(x - y) = m$, то есть, $n \leq v_p(x - y)$, а в \mathbb{Z}_p это равносильно сравнению $x \equiv y \pmod{p^n}$, так как $v_p(p^n) = n$. \square

Theorem 7. *Если целое p -адическое число α определяется последовательностью $\{x_n\}$, то эта последовательность сходится к α . Произвольное p -адическое число ξ является пределом последовательности рациональных чисел.*

Доказательство. Как мы понимаем из предыдущей теоремы, если $\alpha \in \mathbb{Z}_p$ определяется последовательностью $\{x_n\}$, то $\alpha \equiv x_{n-1} \pmod{p^n}$, а это по определению влечёт $v_p(x_n - \alpha) \geq n + 1$. Значит, $v_p(x_n - \alpha) \xrightarrow{n \rightarrow \infty} \infty$, а это по определению означает, что $\{x_n\}$ стремится к α .

Теперь рассмотрим дробное p -адическое число $\xi = \alpha/p^k$.

$$v_p\left(\frac{x_n}{p^k} - \xi\right) = v_p\left(\frac{x_n - \alpha}{p^k}\right) = v_p(x_n - \alpha) - k \xrightarrow{n \rightarrow \infty} \infty$$

а значит, $\xi = \lim_{n \rightarrow \infty} \{y_n\}$, где $\{y_n\} = \{x_n/p^k\}$.

\square

Definition 10. Последовательность p -адических чисел $\{\xi_n\}$ называется ограниченной, если все значения $\|\xi\|_n$ ограничены сверху.

Theorem 8. (Лемма Больцано-Вейерштрасса для поля p -адических чисел)

Из всякой ограниченной последовательности p -адических чисел можно извлечь сходящуюся подпоследовательность.

Доказательство. Наверное, не успеваю рассказать. Можно прочитать в книге ШАФАРЕВИЧА (ССЫЛКУ). \square

Оказывается (хоть это и не особенно неожиданно), для p -адических чисел справедлив критерий Коши, то есть

Theorem 9. (Критерий Коши) Пусть нам дана последовательность $\{\xi_n\}$, $\xi_n \in \mathbb{Q}_p$. Тогда она сходится тогда и только тогда, когда

$$\lim_{n,m \rightarrow \infty} v_p(\xi_m - \xi_n) = \infty$$

Доказательство. Заметим, что из условия

$$\lim_{n,m \rightarrow \infty} v_p(\xi_m - \xi_n) = \infty$$

следует, что $\exists n_0: v_p(\xi_m - \xi_{n_0}) \geq 0 \ \forall m \geq n_0$. Но тогда, по свойству $v_p(\alpha + \beta) \geq \min(v_p(\alpha), v_p(\beta))$. мы имеем

$$v_p(\xi_m) = v_p((\xi_m - \xi_{n_0}) + \xi_{n_0}) \geq \min(0, v_p(\xi_{n_0}))$$

а отсюда следует ограниченность. Значит, по предыдущей теореме, из неё можно извлечь сходящуюся попоследовательность $\{\xi_{n_i}\}$ с пределом ξ . Значит, по определению сходимости $\exists N \in \mathbb{N}: \forall n, m \geq N \ v_p(\xi_m - \xi_n) \geq M$ и $v_p(\xi_{n_i} - \xi) \geq M$ Тогда

$$v_p(\xi_m - \xi) \geq \min(v_p(\xi_m - \xi_{n_i}), v_p(\xi_{n_i} - \xi)) \geq M \text{ for all } m \geq N$$

а значит $\lim_{m \rightarrow \infty} v_p(\xi_m - \xi) = \infty$, то есть, последовательность $\{\xi_m\}$ сходящаяся. \square

В поле p -адических чисел этому признаку можно придать и более сильную форму. А именно, если для последовательности $\{\xi_n\}$ выполнено

$$\lim_{m,n \rightarrow \infty} v_p(\xi_m - \xi_n) = \infty$$

то мы имеем и

$$\lim_{n \rightarrow \infty} v_p(\xi_{n+1} - \xi_n) = \infty$$

Оказывается, что верно и обратное следствие. Действительно, если $\forall n \geq N \ v_p(\xi_{n+1} - \xi_n) \geq M$, то в силу того, что $v_p(\alpha + \beta) \geq \min(v_p(\alpha), v_p(\beta))$ из равенства

$$\xi_m - \xi_n = \sum_{i=n}^{m-1} (\xi_{i+1} - \xi_i), \quad m > n \geq N$$

вытекает и оценка

$$v_p(\xi_m - \xi_n) \geq \min_{i \in \{n, \dots, m-1\}} v_p(\xi_{i+1} - \xi_i) \geq M \Rightarrow v_p(\xi_m - \xi_n) \rightarrow \infty$$

Theorem 10. Для сходимости последовательности p -адических чисел $\{\xi_n\}$ необходимо и достаточно, чтоб $\lim_{n \rightarrow \infty} v_p(\xi_{n+1} - \xi_n) = \infty$.

Ясно, что благодаря теории пределов мы можем определить секвенциальную непрерывность (непрерывность по Гейне) для функций p -адического аргумента.

К тому же, ясны стандартные арифметические свойства непрерывных функций, из которых следует, например, что многочлен непрерывен.

Definition 11. Если последовательность частичных сумм $s_n = \sum_{i=0}^n \alpha_i$ ряда

$$\sum_{i=0}^{\infty} \alpha_i = \alpha_0 + \alpha_1 + \dots + \alpha_n + \dots$$

с p -адическими членами сходится к p -адическому числу α , то будем говорить, что ряд сходится и его сумма равна α .

Из теоремы 10 можно легко получить критерий сходимости рядов из p -адических чисел.

Theorem 11. (Критерий сходимости рядов с p -адическими членами)

Для сходимости ряда $\sum \alpha_n$ с p -адическими членами необходимо и достаточно, чтоб $\|\alpha_n\|_p \xrightarrow{n \rightarrow \infty} 0$ (или, что равносильно, $v_p(\alpha_n) \xrightarrow{n \rightarrow \infty} \infty$).

Доказательство. Действительно, мы имеем цепочку

$$s_n = \sum_{k=1}^n \alpha_k \text{ — сходится} \Leftrightarrow \lim_{n \rightarrow \infty} \|s_{n+1} - s_n\|_p = 0 \Leftrightarrow \lim_{n \rightarrow \infty} \left\| \sum_{k=0}^{n+1} \alpha_k - \sum_{k=0}^n \alpha_k \right\|_p = \lim_{n \rightarrow \infty} \|\alpha_{n+1}\|_p = 0$$

□

Ясно, что как и в случае вещественного анализа, сходящиеся p -адические ряды можно складывать, умножать на константу. Также справедлива следующая теорема:

Theorem 12. При любой перестановке членов сходящегося p -адического ряда его сходимость не нарушается и сумма не меняется.

Доказательство. Упражнение в листочке.

□

Как мы знаем, в курсе вещественного (и комплексного) анализа это свойство характеризует абсолютно сходящиеся ряды. То есть, все сходящиеся p -адические ряды являются и абсолютно сходящимися, а значит, их можно и перемножать:

написать сюда произведение рядов

Теперь уже ясно, что если целое p -адическое число α определяется канонической последовательностью $\{x_n\}$, где

$$x_0 = a_0, \quad x_1 = a_0 + a_1 p, \quad x_2 = a_0 + a_1 p + a_2 p^2, \dots, \quad x_n = \sum_{k=0}^n a_k p^k$$

то, так как мы доказали, что эта последовательность сходится к α , а значит

$$\alpha = \lim_{n \rightarrow \infty} \{x_n\} = \lim_{n \rightarrow \infty} \sum_{k=0}^n a_k p^k = \sum_{k=0}^{\infty} a_k p^k, \quad 0 \leq a_i < p$$

Так как различные канонические последовательности определяют различные p -адические числа, такое представление единственно для каждого числа. Представление целых p -адических чисел рядами напоминает запись вещественных чисел в виде бесконечных десятичных дробей, то есть

$$\overline{0, a_1 \dots a_n \dots} = \sum_{k=1}^{\infty} a_k \left(\frac{1}{10} \right)^k, \quad 0 \leq a_i < 10$$

Рассмотрим теперь ряд

$$b_0 + b_1 p + b_2 p^2 + \dots + b_n p^n + \dots, \quad b_i \in \mathbb{Z}$$

то он будет сходящимся, так как $v_p(b_n p^n) \geq n$, и его сумма будет равна некоторому α .

Для того, что бы для этого α получить каноническое представление, достаточно заменить все b_i на $b_i \bmod p$, относя неполное частное на каждом шаге к следующему члену.

Это замечание актуально для действий в \mathbb{Z}_p , так как при сложении, вычитании и перемножении рядов вида $\sum a_k p^k$, $0 \leq a_i < p$, мы получаем ряды вида $\sum b_k p^k$, $b_k \in \mathbb{Z}$. Отметим, что в этом представлении, действия с p -адическими числами полностью аналогичны действиям с вещественными числами в десятичной записи.

Из теоремы (ссылка) следует, что целое p -адическое число, представленное в виде ряда обратимо тогда и только тогда, когда a_0 . Вместе с теоремой ([вставить ссылку](#)) это даёт следующую теорему:

Theorem 13. *Каждое отличное от нуля целое p -адическое число ξ однозначно записывается в виде*

$$\xi = p^m (a_0 + a_1 p + a_2 p^2 + \dots + a_n p^n + \dots)$$

где $m = v_p(\xi)$, $1 \leq a_0 \leq p-1$, $0 \leq a_n \leq p-1 \quad \forall n \geq 2$.

Заметим, что эта запись соответствует записи последовательности цифр, бесконечной влево, а именно

$$\alpha = \begin{cases} \dots a_{m+1} a_m \overbrace{00 \dots 0}^{m-1}_{(p)}, & m \geq 0 \\ \dots a_1 a_0 a_{-1} \dots a_{m(p)}, & m < 0 \end{cases}$$

p -АДИЧЕСКИЕ ЧИСЛА, КАК ПРОЕКТИВНЫЙ ПРЕДЕЛ:

Разобранное нами построение кольца целых p -адических чисел соответствует более общей алгебраической конструкции. А именно, мы на пальцах разобрали конструкцию проективного предела обратного спектра топологических пространств, групп, колец (не важно чего, в общем).

ПАРАГРАФ НА ДОРАБОТКЕ : (.

Так вот, из нашего построения ясно, что кольцо \mathbb{Z}_p является проективным пределом последовательности $\mathbb{Z}/p^n \mathbb{Z}$ с естественным отображением $\mathbb{Z}/p^n \mathbb{Z} \rightarrow \mathbb{Z}/p^m \mathbb{Z}$ «взятие остатка».

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

2.5 Лемма Гензеля:

Definition 12. *Числовым полем называют конечное расширение поля \mathbb{Q} .*

Example 4. *Например, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ — числовые поля. Поле \mathbb{R} не является конечным расширением \mathbb{Q} , а значит, это не числовое поле.*

Definition 13. Элемент α расширения поля \mathbb{Q} называется алгебраическим числом, если он является корнем ненулевого многочлена в $\mathbb{Q}[T]$.

Example 5. Например, $\frac{1}{2}, \sqrt{2}, i$ — алгебраические числа. Числа e, π не являются алгебраическими (доказательства представили Эрмит в 1873г. и Линдеманн в 1882г.).

Definition 14. Элемент α поля, являющегося расширением \mathbb{Q} называется алгебраическим целым, если он является корнем унитарного многочлена с целыми коэффициентами.

Definition 15. Все алгебраические целые элементы поля K образуют кольцо, которое принято называть кольцом целых поля K и обозначать \mathcal{O}_K .

Example 6. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$.

Definition 16. Пусть $(F, \|\cdot\|)$ — полное неархимедово нормированное поле. Обозначим за

$$\mathbb{Z}_F = B_1(0) = \{x \in F \mid \|x\| \leq 1\}$$

— «кольцо целых» чисел поля F .

Theorem 14. (Лемма Гензеля) Пусть $f(x) \in \mathbb{Z}_F[x]$, $\alpha_0 \in \mathbb{Z}_F$ и справедливо неравенство $\|f(\alpha_0)\| < \|f'(\alpha_0)\|^2$ (тут f' — формальная производная многочлена f). Тогда существует единственное $\alpha \in \mathbb{Z}_F$, такое, что $f(\alpha) = 0$ и $\|\alpha - \alpha_0\| < \|f'(\alpha_0)\|$.

Доказательство. Положим $c = \|f(\alpha_0)\|/\|f'(\alpha_0)\|^2 < 1$. Рассмотрим рекуррентно заданную последовательность

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

(«метод касательных Ньютона»).

Индукцией проверяется, что она обладает следующими свойствами:

1. $\|\alpha_n - \alpha_0\| < c\|f'(0)\| < \|f'(\alpha_0)\|$.
2. $\|f'(\alpha_n)\| = \|f'(\alpha_0)\|$.
3. $\|f(\alpha_n)\| \leq c^{2^n} \|f(\alpha_0)\|^2$.
4. $\|\alpha_n - \alpha_0\| \leq c^{2^n} \|f(\alpha_0)\|$.

А значит, можно взять $\alpha = \lim_{n \rightarrow \infty} \alpha_n$. Единственность следует из разложения многочлена по тейлору в точке α . \square

Corollary 6. (Важное:)

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

Кроме того, есть еще НАРОДНАЯ формулировка леммы Гензеля:

Theorem 15. Пусть f — многочлен с целыми (или целыми p -адическими коэффициентами), а m и k — целые числа, причем $0 \leq m \leq k$. Тогда, если r — целое число, такое, что

$$f(r) \equiv 0 \pmod{p^k}, \quad f'(r) \not\equiv 0 \pmod{p}$$

то существует такое целое s , что

$$f(s) \equiv 0 \pmod{p^{k+m}}, \quad r \equiv s \pmod{p^k}$$

и более того, s может быть выражено в явном виде, а именно,

$$s = r - f(r) \cdot a, \quad a = (f'(r))^{-1} \pmod{p^m}$$

2.6 Пополнение метрических пространств.

Definition 17. Пусть (X, d_X) — метрическое пространство, $\mathcal{F}(X)$ — множество всех ограниченных функций из X в \mathbb{R} . Тогда введём расстояние d_∞ между функциями $f, g \in \mathcal{F}(X)$:

$$d_\infty(f, g) \stackrel{\text{def}}{=} \sup\{|f(x) - g(x)|, x \in X\}$$

Заметим, что определение корректно, так как функции ограничены.

Lemma 3. $(\mathcal{F}(X), d_\infty)$ — метрическое пространство.

Доказательство. Проверим три аксиомы метрики:

1. Пусть $f = g$. Тогда $|f(x) - g(x)| = 0$ для всякого $x \in X$, так что $d_\infty(f, g) = 0$. Если же наоборот $d_\infty(f, g) = 0$, то $0 \leq |f(x) - g(x)| \leq \sup = 0$, а значит $f(x) = g(x)$ для всех $x \in X$, что и означает $f \equiv g$.
2. Так как $|f(x) - g(x)| = |g(x) - f(x)|$, то и $d_\infty(f, g) = d_\infty(g, f)$.
3. Рассмотрим три ограниченные функции $f, g, h \in \mathcal{F}(X)$, и покажем, что

$$d_\infty(f, g) + d_\infty(g, h) \geq d_\infty(f, h)$$

Мы знаем, что:

$$\forall x \in X : |f(x) - g(x)| + |g(x) - h(x)| \geq |f(x) - h(x)|$$

в силу неравенства треугольника для стандартной метрики на \mathbb{R} . Для всякого $\varepsilon > 0$ мы можем взять x_0 такой, что $|f(x_0) - h(x_0)| \geq \sup\{|f(x) - h(x)|, x \in X\} - \varepsilon$. Получаем, что

$$\begin{aligned} d_\infty(f, h) - \varepsilon &= \sup\{|f(x) - h(x)|, x \in X\} - \varepsilon \leq |f(x_0) - h(x_0)| \leq \\ &\leq |f(x_0) - g(x_0)| + |g(x_0) - h(x_0)| \leq d_\infty(f, g) + d_\infty(g, h) \end{aligned}$$

а раз это верно для любого $\varepsilon > 0$, то искомое неравенство доказано. □

Lemma 4. $\mathcal{F}(X)$ — полно.

Доказательство. Пусть f_n — фундаментальная последовательность функций. Тогда $\forall x_0 \in X : \{f_n(x_0)\}$ — также фундаментальная последовательность, так как $|f_n(x_0) - f_m(x_0)| \leq \sup\{|f_n(x) - f_m(x)|, x \in X\}$. Следовательно,

$$\forall x_0 \in X : \exists \lim_{n \rightarrow \infty} f_n(x_0)$$

и сходимость по всем точкам равномерна, так как не зависит от выбора точки x_0 . Иными словами,

$$\exists f(x) : \forall \varepsilon > 0 : \exists N : \forall n > N : d_\infty(f_n, f) < \varepsilon$$

где $f(x_0)$ определяется как предел $\lim_{n \rightarrow \infty} f_n(x_0)$. Так что $f(x)$ — функция, являющаяся пределом искомой последовательности функций. □

Definition 18. Пусть (X, d_X) — метрическое пространство, $\mathcal{F}(X)$ — множество ограниченных функций из X в \mathbb{R} . Построим изометрическое вложение $k : X \rightarrow \mathcal{F}(X)$ следующим образом:

1. Если X — ограничено, то определим $k(x) = d_x$, где

$$\forall y \in X : d_x(y) \stackrel{\text{def}}{=} d_X(x, y)$$

Функция d_x ограничена, так как X ограничено. Заметим также, что

$$d_\infty(d_x, d_y) = \sup_z |d_x(z) - d_y(z)| = \sup_z (d_X(x, z) - d_X(z, y)) \leq d_X(x, y)$$

однако равенство достигается при $z = y$, так что $d_\infty(d_x, d_y) = d_X(x, y)$, а значит вложение изометрическое.

2. Пусть X , возможно, не ограничено. Тогда определим $k(x) = d_x - d_{x_0}$ для некоторой фиксированной точки $x_0 \in X$, где

$$\forall y \in X : (k(x))(y) \stackrel{\text{def}}{=} d_x(y) - d_{x_0}(y) = d_X(x, y) - d_X(y, x_0)$$

что есть ограниченная функция, так как $\forall y \in X : d_X(x, y) - d_X(y, x_0) \leq d_X(x, x_0)$. Заметим, что это аналогичным образом будет изометрическим вложением:

$$\begin{aligned} d_\infty(d_x - d_{x_0}, d_y - d_{x_0}) &= \sup_z |d_x(z) - d_{x_0}(z) - d_y(z) + d_{x_0}(z)| = \\ &= \sup_z (d_X(x, z) - d_X(z, y)) \leq d_X(x, y) \end{aligned}$$

где равенство достигается при $z = y$.

Любое метрическое пространство (X, d_X) имеет пополнение $(\bar{X}, d_{\bar{X}})$, то есть такое метрическое пространство \bar{X} , что выполнено:

1. $X \subseteq \bar{X}$
2. X — всюду плотно в \bar{X}
3. $d_{\bar{X}}|_X = d_X$, то есть вложение из X в \bar{X} является изометрическим
4. $(\bar{X}, d_{\bar{X}})$ — полно.

Доказательство. Возьмём изометрическое вложение Куратовского $k : X \rightarrow \mathcal{F}(X)$, и возьмём его замыкание в топологическом пространстве $\mathcal{F}(X)$ с топологией, индуцированной метрикой d_∞ — назовём это замыкание \bar{X} . Заметим, что

1. $X \subseteq \bar{X}$ естественным образом
2. X всюду плотно в \bar{X} , так как любое множество всюду плотно в своём замыкании
3. Вложение X в \bar{X} изометрическое, так как оно изометрическое и во всё пространство $\mathcal{F}(x)$
4. \bar{X} полно как замкнутое подмножество полного пространства.

□

Remark 11. Пополнение метрического пространства **единственно** с точностью до изометрии.

Remark 12. Выражение $X \subseteq \bar{X}$ тоже подразумевается с точностью до изометрии.

2.7 Пополнение нормированного поля.

Теперь мы умеем пополнять метрические пространства, но нам никто не гарантирует, что при пополнении поля по норме получится поле.

Definition 19. Пополнением нормированного поля $(F_0, \|\cdot\|_0)$ называется нормированное поле $(F, \|\cdot\|)$, удовлетворяющее следующим свойствам

1. Существует вложение $i : F_0 \hookrightarrow F$, сохраняющее норму (изометрическое), то есть $\|i(x)\| = \|x\|_0$.
2. $(F, \|\cdot\|)$ полно, как метрическое пространство.
3. $i(F_0)$ всюду плотно в F , то есть, $\forall x, \varepsilon > 0 \exists x_0 \in F_0 : \|x - i(x_0)\| < \varepsilon$.

Example 7. Из курса анализа ясно, что $(\mathbb{R}, |\cdot|)$ — пополнение $(\mathbb{Q}, |\cdot|)$.

Theorem 16. Для любого нормированного поля существует пополнение.

Доказательство. Будем рассматривать случай нормы с неравенством треугольника.

Пусть \mathfrak{A} — множество всех последовательностей Коши $\{x_n\}_{n=1}^\infty$ в пространстве $(F_0, \|\cdot\|_0)$.

На \mathfrak{A} можно естественным образом определить операции сложения и умножения (поточечно), а также ввести норму $\|\cdot\|$, как $\|\{x_n\}\| = \lim_{n \rightarrow \infty} \|x_n\|_0$.

Это определение корректно, так как предел всегда существует в силу неравенства треугольника и того, что $\{x_n\}$ — последовательность Коши

$$|\|x_n\|_0 - \|x_m\|_0| \leq \|x_n - x_m\|_0$$

Ясно, что остальные свойства нормы также выполняются.

Введём на \mathfrak{A} отношение эквивалентности \sim :

$$\{x_n\} \sim \{y_n\} \Leftrightarrow \lim_{n \rightarrow \infty} \|x_n - y_n\|_0 = 0$$

Нетрудно заметить, что это отношение эквивалентности «уважает» арифметические действия и норму, то есть

1. $\{x_n\} \sim \{u_n\}, \{y_n\} \sim \{v_n\} \Rightarrow \{x_n + y_n\} \sim \{u_n + v_n\}, \{x_n y_n\} \sim \{u_n v_n\}$.
2. $\{x_n\} \sim \{y_n\} \Rightarrow \|\{x_n\}\| = \|\{y_n\}\|$.

В качестве поля F возьмем фактормножество \mathfrak{A}/\sim . Приведенные выше свойства естественно индуцируют арифметические операции и норму с A на F :

- $[\{x_n\}] + [\{y_n\}] = [\{x_n + y_n\}]$.
- $[\{x_n\}] \cdot [\{y_n\}] = [\{x_n \cdot y_n\}]$.
- $\|[\{x_n\}]\| = \|\{x_n\}\|$.

Аксиомы кольца вполне очевидны, проверим существование обратного по умножению элемента. Если $[\{x_n\}] \neq 0$, то $\lim \|x_n\|_0 > 0 \Rightarrow \forall n \geq n_0 \ \|x_n\|_0 > \delta > 0$ для некоторого δ .

Тогда в качестве $[\{x_n\}]^{-1}$ возьмем класс $[\{y_n\}]$, где

$$y_n = \begin{cases} 0, & n < n_0 \\ \frac{1}{x_n}, & n \geq n_0 \end{cases}$$

Осталось проверить, что мы получили пополнение.

В качестве вложения возьмем $i(x) = [(x, x, \dots)]$. Ясно, что $i(F_0)$ плотно в F , так как, если $X = [\{x_n\}] \in F$, то $i(x_n) \rightarrow X$ в пространстве $(F, \|\cdot\|)$.

Теперь проверим полноту. Пусть $X^{(n)} = [(x_1^{(n)}, x_2^{(n)}, \dots)] \in F$ — последовательность Коши. Возьмем такую последовательность $k_n \in \mathbb{N}$, что

$$\sup_{k, \ell \geq k_n} \|x_k^{(n)} - x_\ell^{(n)}\|_0 < \frac{1}{n}$$

Покажем, что в качестве предела можно взять $X = [\{x_{k_n}^{(n)}\}]$. Пусть $N \geq k_n$, $M \geq k_m$, $K \geq \max\{k_n, k_m\}$.

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

Устремим K к бесконечности и получим

$$\|x_N^{(n)} - x_M^{(m)}\|_0 \leq \|X^{(n)} - X^{(m)}\| + \frac{1}{n} + \frac{1}{m}$$

Положим $N = k_n$, $M = k_m$ и получим, что $x_{k_n}^{(n)}$ — последовательность Коши, а её класс эквивалентности — искомый предел. \square

Далее отождествим $i(F_0)$ с F_0 и будем считать, что $F \subseteq F$.

В неархимедовом случае можно сказать даже несколько больше.

Пусть $(F, \|\cdot\|)$ — неархимедово нормированное поле. Если $\{x_n\} \rightarrow x$, $x \in F^*$, то для достаточно больших n $\|x_n\| = \|x\|$.

Lemma 5. Пусть $(F, \|\cdot\|)$ — пополнение неархимедова поля $(F_0, \|\cdot\|_0)$. Тогда

1. $(F, \|\cdot\|)$ неархимедово.
2. $\text{Im}(\|\cdot\|) = \text{Im}(\|\cdot\|_0)$.

3. Введение в алгебраическую геометрию

3.1 Квадратичные формы и квадрики

Definition 20. Пусть X — коммутативное кольцо и даны наборы коэффициентов $\{a_i\} \in X$, $\{b_i\} \in X$, $c \in X$. Если $\exists j: 1 \leq j \leq n$, $a_j \neq 0$. Квадратичной функцией (*не формой*) будем называть функцию вида

$$f(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij} x_i x_j + \sum_{i=1}^n b_i x_i + c$$

Если X — аффинное пространство (мы будем считать, что векторное над полем K), то квадрикой мы будем называть множество нулей такой функции $X \rightarrow K$, то есть, множество вида

$$K = \{x \in X \mid f(x) = f(x_1, \dots, x_n) = 0\}$$

Example 8. Эллипс, парабола и гипербола — известные вам квадрики на плоскости.

Remark 13. Заметим, что если нам дана квадрика M , заданная, как множество нулей функции f и мы сменили систему координат, то в новой системе координат M также будет являться квадрикой, то есть, найдётся такая квадратичная функция f' , множеством нулей которой будет M .

Часто нас будет интересовать, как выглядят квадрики над кольцом целых чисел, то есть, как решать диофантово уравнение $f(x_1, \dots, x_m) = 0$. Эта задача весьма сложная, поэтому для начала попытаемся понять, как пытаться решать такие уравнения над полем \mathbb{Q} .

Example 9. Опишем все пифагоровы тройки, то есть, такие все тройки $(X, Y, Z) \in \mathbb{Z}^3$, что

$$X^2 + Y^2 = Z^2$$

Заметим, что достаточно описывать только тройки, где $\gcd(X, Y, Z) = 1$, так как, если мы умножим все три числа на какое-то целое число, то мы вновь получим пифагорову тройку.

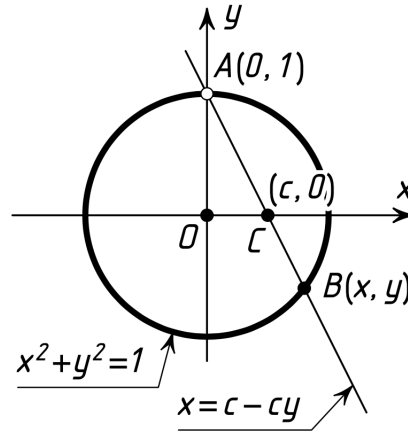
Более того, достаточно рассматривать только тройки попарно взаимно простых чисел, так как

$$X : p, Y : p \Rightarrow X^2 + Y^2 = Z^2 : p$$

Заметим, что при $Z = 0$ мы имеем решение $(0, 0, 0)$, дальше будем рассматривать случаи $Z \neq 0$. Поделим на z и получим уравнение

$$x^2 + y^2 = 1$$

То есть, мы свели задачу к перечислению всех рациональных точек на окружности. Некоторые рациональные точки $(0, \pm 1)$, $(\pm 1, 0)$. Выберем из них, например, точку $A = (0, 1)$. Проведем всевозможные прямые через точку A (кроме горизонтальных). Каждая такая прямая ℓ пересечет окружность еще в одной точке $B(x, y)$ и ось абсцисс в точке $C(c, 0)$.



Таким образом, пересекая, мы получаем взаимнооднозначное соответствие между точками окружности и точками прямой.

Причем, это соответствие сохраняет рациональность точек. Прямая, проходящая через точки A и C определяется уравнением $y = c - cy$. Подставим это в уравнение окружности

$$(c - cy)^2 + y^2 = 1 \Rightarrow (c^2 + 1)y^2 - 2c^2y + c^2 - 1 = 0$$

откуда мы имеем, что либо $y = 1$, либо $y = \frac{c^2 - 1}{c^2 + 1}$, при $x = c - cy = \frac{2c}{c^2 + 1}$. Остается заметить, что если $c \in \mathbb{Q}$, то $(x, y) \in \mathbb{Q}^2$. Обратное всегда вытекает. Если координаты двух точек рациональны, то уравнение соединяющей их прямой можно записать так, чтобы оно имело рациональные коэффициенты. Если две прямые задаются уравнениями с рациональными коэффициентами, то точка их пересечения (если она существует) имеет рациональные координаты. То есть, каждое рациональное решение, кроме $(0, 1)$ можно получить

$$x = \frac{2c}{c^2 + 1}, \quad y = \frac{c^2 - 1}{c^2 + 1}$$

где $c \in \mathbb{Q}$.

Подставим $c = m/n$, где $\gcd(m, n) = 1$, тогда

$$x = \frac{2c}{c^2 + 1} = \frac{2mn}{m^2 + n^2}, \quad y = \frac{c^2 - 1}{c^2 + 1} = \frac{m^2 - n^2}{m^2 + n^2}$$

Теперь будем искать все целые решения, выполним обратную подстановку:

$$\frac{X}{Z} = \frac{2mn}{m^2 + n^2}, \quad \frac{Y}{Z} = \frac{m^2 - n^2}{m^2 + n^2}, \quad m^2 + n^2 \neq 0$$

Вспомним, что числа (X, Y, Z) взаимно просты, а значит, дроби в левых частях несократимы. Если бы мы знали, что дроби, стоящие в правых частях тоже несократимы, то мы бы положили $X = 2mn$, $Y = m^2 - n^2$, $Z = m^2 + n^2$, но, к сожалению, они бывают сократимы. Но, они могут быть сократимы только на 2. Действительно, если p — простое число, не равное двум и $p \mid 2mn$. Так как $\gcd(m, n) = 1$, если $p \mid m$, то $p \nmid n \Rightarrow m^2 + n^2 \not\equiv 0 \pmod{p}$, а значит, дробь X/Z несократима. Рассмотрим теперь вторую дробь. Если p — простое число, не равное двум и $p \mid m^2 - n^2$, $p \mid m^2 + n^2$, то $p \mid 2m^2$ и $p \mid 2n^2$. Так как $\gcd(m, n) = 1$, это влечёт $p = 2$. Итак, мы наконец нашли взаимнопростые натуральные решения

$$X = mn, \quad Y = \frac{m^2 - n^2}{2}, \quad Z = \frac{m^2 + n^2}{2}$$

при $\gcd(m, n) = 1$ и нечетных m, n , а также

$$X = 2mn, \quad Y = m^2 - n^2, \quad Z = m^2 + n^2$$

при взаимнопростых m и n , одно из которых четно. Любые целые положительные решения мы получим умножением этих решений на натуральное число. Теперь заметим, что формулы для четного и нечетного случаев на самом деле совпадают. Если

$$X = pq, \quad Y = \frac{p^2 - q^2}{2}, \quad Z = \frac{p^2 + q^2}{2}$$

— решение, вычисленное по формулам для первого случая, где $\gcd(p, q) = 1$ и числа p и q оба нечетны, то те же решения мы получим и по вторым формулам, только подставляя

$$m = \frac{p + q}{2}, \quad n = \frac{p - q}{2}$$

разве что с точностью до того, что X и Y поменяются местами.