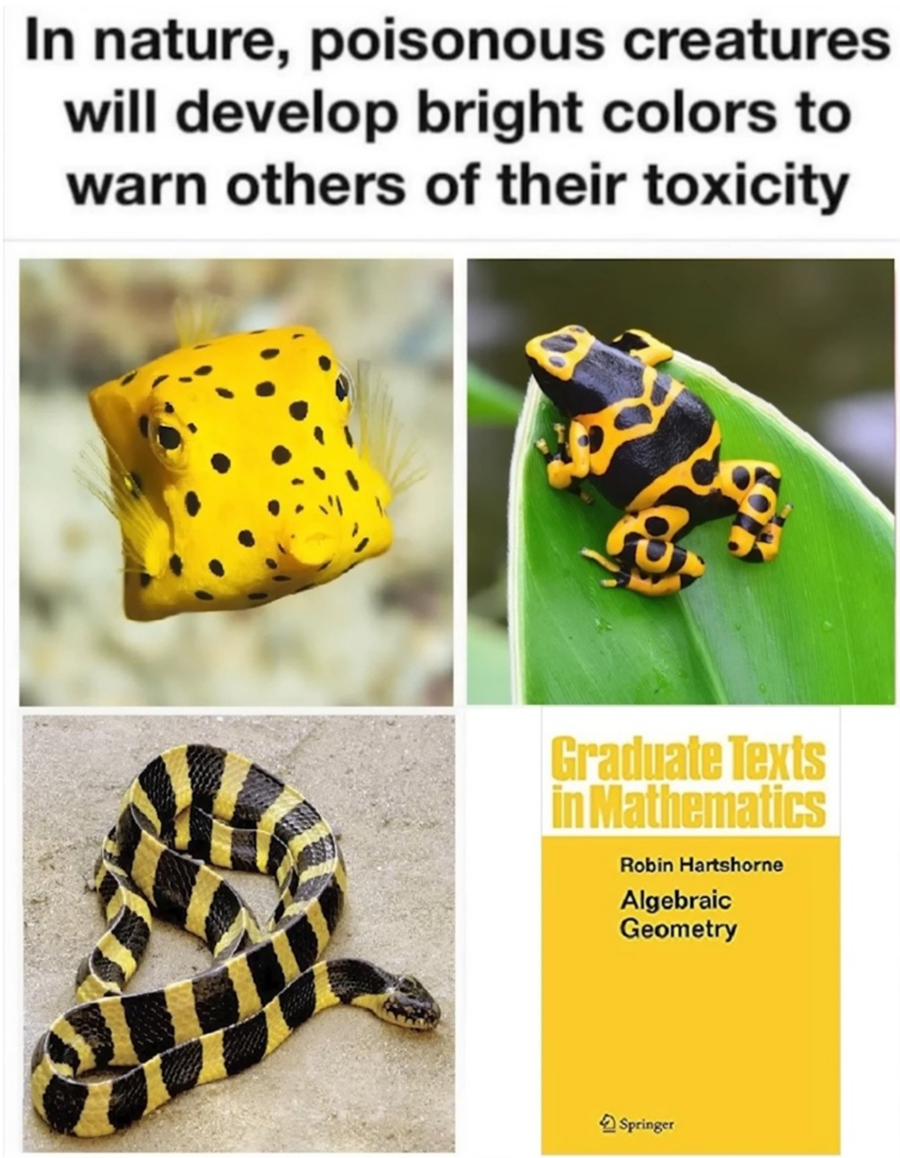
Летняя математическая школа ЛНМО

Поставы, 2022г.

Алгебраическая геометрия и теория чисел



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

1.1 Нормированное поле. Неархимедовы нормы.

Здесь и вдальнейшем 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 $\|\cdot\|\colon F \to \mathbb{R}_{>0}$, удовлетворяющее следующим свойствам:*

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

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

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:

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

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 выполняется оценка:

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

Тогда мы можем провести оценки следующим образом:

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

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 $n \to \infty$ 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 $\mathcal{F}ield$ в категорию $\mathcal{M}etr$.

Corollary 1. *Норма непрерывна.*

Definition 2. *Нормы, с постойнной $C = 1$ 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 $a, b \in \mathbb{Z}$, $a \not\vdots\, p$, $a \not\vdots\, p$, а $n \in \mathbb{Z}$. В таком случае число n называют p-адическим показателем числа x и обозначают $\upsilon_p(x)$.*

Definition 4. ***(Самое важное)***
Пусть p — простое число. Тогда норму

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

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

Remark 4. Ясно, что подоходит $r^{-\upsilon_p(x)}$, 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.

1.2 Эквивалентные нормы.

Пока не знаю, буду ли рассказывать.

1.3 Пополнение метрических пространств.

Definition 5. *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 2. *$(\mathcal{F}(X), d_\infty)$ — 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 $0 \le |f(x) - g(x)| \le \sup = 0$, 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

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

Мы знаем, что:

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

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

$$d_\infty(f, h) - \varepsilon = \sup\{|f(x) - h(x)|, x \in X\} - \varepsilon \le |f(x_0) - h(x_0)| \le$$

$$\le |f(x_0) - g(x_0)| + |g(x_0) - h(x_0)| \le d_\infty(f, g) + d_\infty(g, h)$$

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

□

Lemma 3. $\mathcal{F}(X)$ *— полно.*

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

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

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

Definition 6. *Пусть (X, d_X) — метрическое пространство, $\mathcal{F}(X)$ — множество ограниченных функций из X в $\mathbb{R}$. Построим изометрическое вложение $k : X \to \mathcal{F}(X)$ 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

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

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*

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

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

$$d_\infty(d_x - d_{x_0}, d_y - d_{x_0}) = \sup_z |d_x(z) - d_{x_0}(z) - d_y(z) + d_{x_0}(z)| =$$

$$= \sup_z \big(d_X(x,z) - d_X(z,y)\big) \le d_X(x,y)$$

где равенство достигается при $z = y$.

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

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

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

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

□

Remark 5. Пополнение метрического пространства **единственно** с точностью до изометрии.

Remark 6. Выражение $X \subseteq \overline{X}$ тоже подразумевается с точностью до изометрии.

1.4 Пополнение нормированного поля.

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

Definition 7. *Пополнением нормированного поля* $(F_0, \|\cdot\|_0)$ *называется нормированное поле* $(F, \|\cdot\|)$, *уловлетворяющее следующим свойствам*

1. *Существует вложение* $i\colon F_0 \hookrightarrow F$, *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,* $\forall x, \varepsilon > 0\ \exists x_0 \in F_0 \colon \|x - i(x_0)\| < \varepsilon$.

Example 4. *Из курса анализа ясно, что* $(\mathbb{R}, |\cdot|)$ — *пополнение* $(\mathbb{Q}, |\cdot|)$.

Theorem 2. *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 $\|\{x_n\}\| = \lim\limits_{n\to\infty} \|x_n\|_0$.

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

$$|\|x_n\|_0 - \|x_m\|_0| \le \|x_n - x_m\|_0$$

Ясно, что остальные свойства нормы также выполняются.

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

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

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 $\lim \|x_n\|_0 > 0 \Rightarrow \forall n \ge n_0\ \|x_n\|_0 > \delta > 0$ для некоторого δ.
Тогда в качестве $[\{x_n\}]^{-1}$ возьмем класс $[\{y_n\}]$, где

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

Осталось проверить, что мы получили пополнение.
В качестве вложения возьмем $i(x) = [(x, x, \ldots)]$. Ясно, что $i(F_0)$ плотно в F, так как, если $X = [\{x_n\}] \in F$, то $i(x_n) \to X$ в пространстве $(F, \|\cdot\|)$.
Теперь проверим полноту. Пусть $X^{(n)} = [(x_1^{(n)}, x_2^{(n)}, \ldots)] \in F$ — последовательность Коши. Возьмем такую последовательность $k_n \in \mathbb{N}$, что

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

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

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

Устремим K к бесконечности и получим

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

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 $\{x_n\} \to x,\ x \in F^*$, то для достаточно больших n $\|x_n\| = \|x\|$.

Lemma 4. *Пусть* $(F, \|\cdot\|)$ *— пополнение неархимедова поля* $(F_0, \|\cdot\|_0)$*. Тогда*

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

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, рещения 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 $x_0, x_1, x_2, \ldots, x_n, \ldots$ со свойствами

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

Процесс построения этой последовательности может напонмить внимательному читателю процесс вычисления $\sqrt{2}$ при помощи приблиэения рациональными числами. Там мы тоже строим последовательность рациональых чисел $r_1, r_2, \ldots, r_n$, 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,

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

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 $\forall \varepsilon > 0\ N \colon \forall n > N\ |r_n - r'_n| < \varepsilon$, то её пределом также будет $\sqrt{2}$ (и в этом смысле определение корректно). Соответсвенно, 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 7. В общем, во всей этой аналогии мы просто заменили метрику на p-адическую.

Definition 8. *Пусть p — некоторое простое число. Последовательность целых чисел $\{x_n\}$, обладающих свойством*

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

определяет новый объект, называемый p-адическим числом. Две последовательности $\{x_n\}$ и $\{x'_n\}$ определяют одно и то же целое p-адическое число, когда $x_n \equiv x'_n \pmod{p^{n+1}}\ \forall n \geq 0$.
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-адиеческое число, определяемое последовательностью $\{x, x, x, \ldots\}$. Такое целое p-адическое число мы будем обозачать той же буквой x. Таким образом, мы получили естественное вложение $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ (инективность вполне очевидна).

Remark 8. **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 $\overline{x_n}$.

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

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

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

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

$$\{a_0,\ a_0 + a_1 p,\ a_0 + a_1 p + a_2 p^2, \ldots\}, \quad 0 \leq a_i < p$$

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

Доказательство. Путь $\alpha \in \mathbb{Z}_p^*$. 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, $x_0y_0 \equiv 1 \pmod p \Rightarrow x_0 \not\equiv 0 \pmod p$. И обратно, так как $x_0 \not\equiv 0 \pmod p$ и $x_n \equiv x_{n-1} \pmod{p^n}$ мы имеем

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

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

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

а значит, $\{y_n\}$ определяет некоторое целое p-адическое число β.
Таким образом, $\alpha\beta = 1 \Rightarrow \alpha \in \mathbb{Z}_p^*$. □

Theorem 4. *Любое отлчиное от нуля целое p-адическое число α можно представить в виде*

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

Доказательство. Если $\alpha \in \mathbb{Z}_p^*$, то равенство справедливо при $m = 0$.
Пусть теперь $\alpha \notin \mathbb{Z}_p^*$ и $\{x_n\} \to \alpha$. Тогда, по предыдущей теореме $x_0 \equiv 0 \pmod p$. Так как $\alpha \neq 0,\ \exists N \in \mathbb{N}\colon \forall n \geq N\ x_n \not\equiv 0 \pmod{p^{n+1}}$. Пусть m — наимеьший 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 $\{z_s\} \to \xi$.

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

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 $z_s \equiv y_s \pmod{p^{s+1}}\ \forall s \geq 0 \Rightarrow \varepsilon = \xi$. □

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

Доказательство. Упражнение в листочке. □

Теперь ясно, что число m в представлении $\alpha = p^m\varepsilon$ — p-адический показатель α ($\upsilon_p(\alpha)$).
В терминах p-адического показателя легко вырадать свойства делимости p-адических чисел.

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

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 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 (надеюсь, вы знаете, что это такое).
В нашем случае это сводится к рассмотрению дробей α/p^k, где $\alpha \in \mathbb{Z}_p,\ k \geq 0$.

Definition 9. *Дробь вида α/p^k, где $\alpha \in \mathbb{Z}_p$, а $k \geq 0$ называется дробным p-адмическим 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 10. *Полем p-адических чисел $\mathbb{Q}_p$ называется поле частных кольца целых p-адических чисел $\mathbb{Z}_p$.*

Theorem 5.

2.3 Поле p-адических чисел, как пополнение.