Повторение:

Опр: Кольцо – мн-во с 2-мя бинарными операциями „+" и „·" со св-ми: 1) По сложению (относительно „+") – это абелева группа (нейтральный эл-т – „0", обратный эл-т к „a" – это „–a")

2) $a(b+c) = ab + ac$ и $(b+c)a = ba + ca$ $\forall a, b, c$ из кольца.

Опр: Поле – коммутативное ассоциативное кольцо с 1, где все эл-ты обратимы, кроме 0. ($\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$)

Опр: Поле – коммутативное ассоциативное кольцо $\mathbb{K}$, где $1 \neq 0$, и все ненулевые элементы обратимы. ($\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$)

Опр: Норма на поле $\mathbb{K}$ – это отображение $\|\cdot\| : \mathbb{K} \to [0, +\infty)$, т.ч.

1) $\|x\| = 0 \iff x = 0$
2) $\|xy\| = \|x\|\|y\| \quad \forall x, y \in \mathbb{K}$
3) $\|x + y\| \leq \|x\| + \|y\|$

Например, модуль на $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – норма на поле.

Св-во: $\|1\| = 1$, $\|-1\| = 1$

□ $\|1\| = \|1 \cdot 1\| = \|1\|\|1\| = \|1\|^2 \Rightarrow \|1\| = 1$

$1 = \|1\| = \|(-1)\cdot(-1)\| = \|-1\|^2 \Rightarrow \|-1\| = 1$ ▨

Вопрос: На любом ли поле можно ввести какую-нибудь норму?

($\forall \nexists$)

Лирическое отступление: Какие бывают поля?

Бесконечные и конечные. Пример (интересный факт) конечное поле может содержать только p^n эл-тов, где p - простое.

Устроено это примерно так: $\forall \alpha \in \mathbb{F}_{p^n}$

$\alpha = \lambda_0 + \lambda_1\theta + \lambda_2\theta^2 + \dots + \lambda_{n-1}\theta^{n-1}$, а $\theta^n = a_{n-1}\theta^{n-1} + \dots + a_1\theta + a_0$,

т.к. $\theta^n - a_{n-1}\theta^{n-1} - \dots - a_1\theta - a_0$ - неприводимый мн-член.

Утв: Мультипликативная группа конечного поля - циклическая.

□ $q = p^n$. Если $\mathbb{F}_q^*$ - не циклическая, то $\exists$ натуральное $n < q-1$, т.ч. $\forall x \in \mathbb{F}_q^*: x^n = 1$ ↯ ■

Тогда ясно, что на $\forall$ конечном поле нельзя ввести нетривиальную норму.

($\|0\| = 0$, возьмем порождающий a: $\|a^{q-1}\| = \|a\|^{q-1} = 1 \Rightarrow$ $\|a\| = 1 \Rightarrow$ норма тривиальная)

Ну а вообще нельзя ввести нетривиальную норму на конечных полях и их алг. расширениях. То есть на большинстве полей можно ввести что-то интересное.

Вот, например, есть интересная норма на $\mathbb{Q}$ – p-адическая.

Опр. p – какое-то простое число. Тогда $\forall x \in \mathbb{Q}$:

$$|x|_p = \begin{cases} 0, & x = 0 \\ p^{-\nu_p(x)}, & x \in \mathbb{Q}^* \end{cases}$$

(Если $x \neq 0$, то $x = p^\alpha \frac{a}{b}$ так, что $p \nmid ab$), тогда $\nu_p(x) = \alpha$)

Почему норма: 1) $|x|_p = 0 \Leftrightarrow x = 0$ – верно

2) $|ab|_p = \left|p^\alpha \frac{m_1}{n_1} p^\beta \frac{m_2}{n_2}\right|_p = \left|p^{\alpha+\beta} \frac{m_1 m_2}{n_1 n_2}\right|_p = p^{-(\alpha+\beta)} = p^{-\alpha} \cdot p^{-\beta} =$

$= |a|_p |b|_p$

3) $|x+y|_p = \left|p^\alpha \frac{a_1}{b_1} + p^\beta \frac{a_2}{b_2}\right|_p \overset{(\alpha \leq \beta)}{=} \left|p^\alpha \left(\frac{a_1}{b_1} + p^{\beta-\alpha} \frac{a_2}{b_2}\right)\right|_p =$

$= \left| \frac{p^\alpha (a_1 b_2 + a_2 b_1 p^{\beta-\alpha})}{b_1 b_2} \right|_p \leq p^{-\alpha} = \max(|x|_p, |y|_p) \leq$

$\leq |x|_p + |y|_p$

Как видим, вместо классического неравенства Δ имеем

$$= \left| \frac{p^{\max(\alpha_1+\beta_2,\alpha_2+\beta_1)}(a_1b_2+a_2b_1p)}{b_1b_2} \right|_p \leq p^{-\max(\alpha_1+\beta_2,\alpha_2+\beta_1)} = \max(|x|_p,|y|_p) \leq$$

$$\leq |x|_p + |y|_p$$

Как видим, вместо классического неравенства Δ выполнено более сильное неравенство: $\|a+b\| \leq \max(\|a\|,\|b\|)$. Нормы, где такое неравенство выполнено называются неархимедовыми (а где не выполнено, соответственно, архимедовыми). Так, например обычный модуль – архимедова норма на $\mathbb{Q}$, а $|\cdot|_p$ – неархимедова. Поля с архимедовой/неархимедовой нормой называются, соответственно, архимедовыми/неархимедовыми.

$\alpha \in \mathbb{Z}_p \Rightarrow \alpha \equiv a \pmod{p-1}$

Интересные свойства в неархимедовых полях (в $\mathbb{Q}$ с нормой $|\cdot|_p$, частности)

Утв 1: Если $\|x\| \neq \|y\| \Rightarrow \|x+y\| = \max\{\|x\|, \|y\|\}$

□ Б.о.о. $\|x\| < \|y\| \Rightarrow \|x+y\| \leq \|y\|$.

$y = (x+y)+(-x) \Rightarrow \|y\| \leq \max\{\|x+y\|, \|x\|\} \neq \|x\|$, т.к. иначе противоречие с $\|x\| < \|y\|$. $\Rightarrow \max\{\|x+y\|, \|x\|\} = \|x+y\| \Rightarrow$

$\left.\begin{array}{l} \|y\| \leq \|x+y\| \\ \|x+y\| \leq \|y\| \end{array}\right\} \Rightarrow \|x+y\| = \|y\| = \max\{\|x\|, \|y\|\}$ ■

Следствие: $\|x_1\| > \|x_i\|$ $(i = 2, \dots, n)$, тогда $\|x_1 + \dots + x_n\| = \|x_1\|$

Следствие 2: Из чисел $\|x-y\|, \|y-z\|, \|z-x\|$ хотя бы два равны. (т.е. все Δ-ки равнобедренные)

□ $x - z = (x-y) + (y-z)$. Если $\|x-y\| = \|y-z\|$, то всё, если нет, то по усл. $\|x-z\| = \max\{\|x-y\|, \|y-z\|\}$ ☑

Опр: $B_R(a) = \{x \in \mathbb{K} : \|x-a\| < R\}$

Утв. $B_R(a) = B_R(b)$ $\forall b \in B_R(a)$ ($\forall$ точка шара - центр шара)

□ $b \in B_R(a) \Leftrightarrow \|a-b\| < R \Leftrightarrow a \in B_R(b)$ ⇒ Из симметрии достаточно д-ть, что $B_R(b) \subseteq B_R(a)$. Пусть $x \in B_R(b)$, т.е. $\|x-b\| < R$. Тогда $(x-a) = (x-b) + (b-a)$ и $\|x-a\| \le \max\{\|x-b\|, \|b-a\|\} < R$ ☑

Следствие: $\forall$ 2 шара либо не пересекаются, либо один содержится в другом.

$\alpha \in \mathbb{Z}_p \Rightarrow \alpha \equiv a \pmod{p}$

Теорема: Норма неархимедова $\Leftrightarrow \forall n: \|\underbrace{1+\ldots+1}_{n}\| \le 1$.

$\square \Rightarrow$ очевидно

$\Leftarrow \|(x+y)^n\| = \|x+y\|^n \le \sum_{k=0}^{n} \|C_n^k x^k y^{n-k}\| \le (n+1)\left(\max\{\|x\|, \|y\|\}\right)^n$

$\|1+1+\ldots+1\| \le 1 \Rightarrow$

$\|x+y\| \le \sqrt[n]{n+1} \cdot \max\{\|x\|, \|y\|\} \xrightarrow{n\to\infty} \max\{\|x\|, \|y\|\}$ ☑

Продолжение нормы: $(\mathbb{K}_1, \|\cdot\|_1)$ и $(\mathbb{K}_2, \|\cdot\|_2)$

$\mathbb{K}_1 \subseteq \mathbb{K}_2$ так, что $\|\cdot\|_2$ на $\mathbb{K}_1$ совпадает с $\|\cdot\|_1$

Тогда если в таком смысле продолжить неарх. норму, то по прежнему получим неарх.

$\alpha \in \mathbb{Z}_p \Rightarrow \alpha \equiv a_0 + a_1 p + \dots$

Опр.: Последовательность $\{x_n\}$ фундаментальна по норме $\|\cdot\|$, если $\forall \varepsilon > 0 \ \exists N \in \mathbb{N}$, т.ч. $\forall m, n > N \ \|x_m - x_n\| < \varepsilon$. Если $\forall$ такая последовательность сходится, то поле с такой нормой называется полным.

Пример неполного: $(\mathbb{Q}, |\cdot|)$

~~Пополнением исходного поля ...~~

Пополнением исходного поля $(\mathbb{K}_1, \|\cdot\|_1)$ называется такое поле $(\mathbb{K}_2, \|\cdot\|_2)$, что

1) $\mathbb{K}_1 \subseteq \mathbb{K}_2$
2) $\|\cdot\|_2$ на $\mathbb{K}_1$ совпадает с $\|\cdot\|_1$
3) $(\mathbb{K}_2, \|\cdot\|_2)$ – полно
4) $\mathbb{K}_1$ всюду плотно в $\mathbb{K}_2$.

Пример: $\mathbb{R}$ – пополнение $(\mathbb{R}, |\cdot|)$ – пополнение $(\mathbb{Q}, |\cdot|)$

4) $|\cdot|_1$ вкладу плотно в $|\cdot|_2$.

Пример: $\mathbb{R}$ ~~не полно~~ $(\mathbb{R}, |\cdot|)$ – пополнение $(\mathbb{Q}, |\cdot|)$.

$(\mathbb{Q}, |\cdot|_p)$ – не полно.

Пополнение $(\mathbb{Q}, |\cdot|_p)$ называется полем p-адических чисел и обозначается $\mathbb{Q}_p$.

Мн-во значений нормы $|\cdot|_p$ на $\mathbb{Q}_p$ осталось прежним

($x_n = x + (x_n - x)$ ~~$\cdot |x_n - x|_p$~~ $\cdot |x_n - x|_p \to 0 \Rightarrow$ для большого n $|x|_p > |x_n - x|_p \Rightarrow |x_n|_p = \max\{|x|_p, |x_n - x|_p\} = |x|_p$).

Опр: Мн-во эл-тов $x \in \mathbb{Q}_p$, т.ч. $|x|_p \leq 1$ образуют кольцо, которое называется кольцом целых p-адических чисел $\mathbb{Z}_p$

Почему кольцо?: $x, y \in \mathbb{Z}_p \Rightarrow |x+y|_p \le \max\{|x|_p, |y|_p\} \le 1$.

$|xy|_p = |x|_p |y|_p \le 1$. Остальное очев.

В $\mathbb{Q}_p$ можно определить сравнения по степеням p:

$$\alpha \equiv \beta \pmod{p^n} \iff \frac{\alpha-\beta}{p^n} \in \mathbb{Z}_p, \text{ т.е. } \left|\frac{\alpha-\beta}{p^n}\right|_p \le 1$$

Лемма: $\forall \alpha \in \mathbb{Z}_p \ \exists!\ a \in \{0, 1, \dots, p-1\}$, т.ч. $\alpha \equiv a \pmod{p}$

В $\mathbb{Q}_p$ можно определить сравнения по степеням p:

$$\alpha \equiv \beta \pmod{p^n} \iff \frac{\alpha-\beta}{p^n} \in \mathbb{Z}_p, \text{ т.е. } \left|\frac{\alpha-\beta}{p^n}\right|_p \le 1$$

Лемма: $\forall \alpha \in \mathbb{Z}_p \ \exists!\ a \in \{0,1,\dots,p-1\}$, т.ч. $\alpha \equiv a \pmod{p}$

! - очев., т.к. $\{0,1,\dots,p-1\}$ — несравнимы друг с другом.

(∃) - $\exists \frac{u}{v} \in \mathbb{Q}$, т.ч. $|\alpha - \frac{u}{v}|_p < \frac{1}{p}$, т.к. $\mathbb{Q}$ плотно в $\mathbb{Q}_p$. $\Rightarrow$

$\frac{u}{v} = \underset{\mathbb{Z}_p}{\alpha} + \underset{\mathbb{Z}_p,\ \text{т.к. } |\cdot|_p<1}{\left(\frac{u}{v} - \alpha\right)} \in \mathbb{Z}_p \Rightarrow p \nmid v$ ($\frac{u}{v}$ несократима) $\Rightarrow$

$\exists a$, т.ч. $u \equiv av \pmod{p} \Rightarrow \frac{u}{v} - a = \frac{u-av}{v} \equiv 0 \pmod{p}$

$\Rightarrow \alpha \equiv \frac{u}{v} \equiv a \pmod{p}$ □

$\mathbb{Z}_p$ $\mathbb{Z}_p$, т.к. $|\cdot|_p \le 1$

$\exists\, a$, т.к. $u \equiv av \pmod{p} \Rightarrow \quad \frac{u}{v} - a = \frac{u - av}{v} \equiv 0 \pmod{p}$

$\Rightarrow \alpha \equiv \frac{u}{v} \equiv a \pmod{p}$ ☒

Теорема: $\forall\, \alpha \in \mathbb{Z}_p$ $\exists!$ представление в виде ряда $\alpha = \sum\limits_{n=0}^{\infty} a_n p^n$, $a_n \in \{0, 1, \dots, p-1\}$ и $\forall$ такой ряд сходится и эл-ту из $\mathbb{Z}_p$.

□ $\{x_n\} = \left\{\sum\limits_{k=0}^{n} a_k p^k\right\} \Rightarrow |x_n - x_m|_p = \left|\sum\limits_{k=m+1}^{n} a_k p^k\right|_p \le p^{-(m+1)}$.

Т.к. $\mathbb{Q}_p$ - полное $\Rightarrow$ сходится. (и. эл-ту $\sum\limits_{k=0}^{+\infty} a_k p^k$) и этот эл-т лежит в $\mathbb{Z}_p$. (С какого-то момента норма не меняется).

$\alpha \in \mathbb{Z}_p \Rightarrow \alpha \equiv a_0 \pmod{p}$

$\alpha_1 = \frac{\alpha - a_0}{p} \in \mathbb{Z}_p \Rightarrow \exists\, a_1 \equiv \alpha_1 \pmod{p}$

$\vdots$

$\alpha_{n+1} = \frac{\alpha - (a_0 + a_1 p + \ldots + a_n p^n)}{p^{n+1}} \in \mathbb{Z}_p \Rightarrow \alpha_{n+1} \equiv a_{n+1} \pmod{p}$

Вот и разложение. □

p

Вот и разложение. ☐

Следствие: $\mathbb{N}$ плотно в $\mathbb{Z}_p$

Следствие: $\mathbb{Z}_p$ – континуально.

Если $\alpha \in \mathbb{Q}_p$ и $|\alpha|_p = p^k$, то $|p^k \alpha|_p = |p^k|_p |\alpha|_p =$

$= 1 \Rightarrow p^k \alpha \in \mathbb{Z}_p$ и $p^k \alpha = \sum_{n=0}^{+\infty} a_n p^n \Rightarrow \alpha = \sum_{n=0}^{+\infty} a_n p^{n-k}$ и

так представляется $\forall$ p-адическое число. $\left(\frac{a_0}{p^k} + \frac{a_1}{p^{k-1}} + \ldots + a_k + \right.$

$\left. + a_{k+1} p + \ldots \right)$