Кольца и Поля

Кольцо

R – кольцо

$\langle R, +, \cdot \rangle$

Св-ва операций

1) по сложению это абелева группа

2) двусторонняя дистрибутивность

$$a(b+c) = ab + ac \qquad (a+b)c = ac + bc$$

Пр. кольц:

1) нулевое кольцо $\{0\}$

2) кольцо с нулевым умножением

$$\forall x, y \in R \quad xy = yx = 0$$

3) $\langle \mathbb{Z}, +, \cdot \rangle, \langle \mathbb{R}, +, \cdot \rangle, \langle \mathbb{Q}, +, \cdot \rangle$

4) кольцо десятичных дробей

$3{,}51 \quad 0{,}687 \quad 25{,}03$

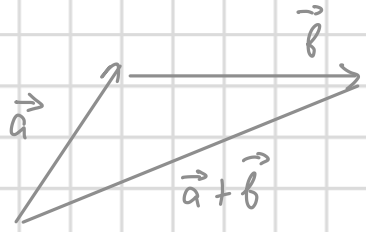
5) $\mathbb{Z}[x]$ – многочлены с целыми коэфф. со сложением и умнож.

6) $Func(\overset{\text{нз}}{X}, \overset{\text{в}}{Y})$ с поточечным сложением и умножением

$$\forall x \in X: \quad (f+g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

7) Геом. векторы со сложением и векторным умнож.

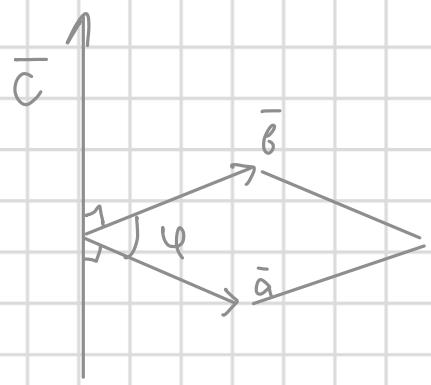


$\overrightarrow{a \times b}$:

1) $\vec{c} \perp \vec{a}$ и $\vec{c} \perp \vec{b}$

2) $|\vec{c}| = S_{\square} = |\vec{a}||\vec{b}| \cdot \sin\varphi$

3) $\vec{a}_1, \vec{b}_2, \vec{c}_3$ образуют правую тройку (с опр. по правилу правой руки)



Пр. не кольца $\langle \mathbb{Z}[x], +, \circ \rangle$

$\triangleleft$ дистрибутивность справа $(f+g)\circ h$

$\exists\ f = x \quad g = x \quad h = x^2$

$(f+g)\circ h = (2x)\circ x^2 = 2x^2 = (2x)(x^2)$ — $2x$ от x^2, подставим x^2 в x

$f\circ h = x \circ x^2 = x^2$

$g\circ h = x \circ x^2 = x^2$ $\Big\}$ $\Rightarrow 2x^2 = x^2 + x^2$

$\triangleleft$ дист. слева

$h \circ (f+g) = (2x)^2 = 4x^2$ ($f+g = 2x$)

$h\circ g = x^2 \circ x = x^2$

$h\circ f = x^2 \circ x = x^2$ $\Big\}$ $\Rightarrow 2x^2$

Следствия из опр. кольца

1) $0\cdot x = 0$

док-во: $\triangleright$ $yx = (0+y)x = 0x + yx$ сокращ. т.к. все эл.-ты кольца регулярны

$yx - yx = 0x + yx - yx \Leftrightarrow 0 = 0x$

2) $(-x)y = (-xy)$ и т.д.

если умнож. в кольце ассоциативно то это ассоциативное кольцо

если кольцо коммутативно то это коммутативное кольцо

Прим. вект-ры не коммутативно и не ассоциативно

$\bar{a} \times \bar{b} \neq -\bar{b} \times \bar{a}$ $\quad (\bar{a} \times \bar{b}) \times \bar{c} \neq \bar{a} \times (\bar{b} \times \bar{c})$

векторное произведение

Если есть нейтр. эл. по умножению: кол. называют с единицей

Пр.: $\langle 2\mathbb{Z}, +, \cdot \rangle$ – кольцо без единицы

Поле

Опр.: Поле – коммутативное и ассоциативное кольцо с единицей в котором каждый ненулевой эл. обратим

Пр. полей: $\mathbb{Q}$, $\mathbb{R}$

$\mathbb{Z}$ – не поле

Замечание: Кольцо из 1 эл не поле

Конечное поле $\mathbb{F}_2 = \mathbb{Z}_2$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$1^{-1} = 1$

$x \in \underset{\text{кольцо}}{R}$ – нетр. делитель нуля, если $\exists\, y \in R$: $xy = 0$

0 – тривиальный делитель нуля

$x \neq 0$ – нетривиальный делитель нуля

Пр.: $\exists$ $Func(X, \mathbb{R})$, (нетрив. дел. нуля) такие, что $|x| > 1$

операции: $+, \cdot$ поточечные

$\emptyset \neq Y \subsetneq X$

$$f(x) = \begin{cases} 0, & x \in Y \\ 1, & x \notin Y \end{cases}$$

$$g(x) = \begin{cases} 1, & x \notin Y \\ 0, & x \in Y \end{cases}$$

$f \cdot g \equiv 0$

↑ ↑

нетривиальные делители нуля

Лемма:

В поле нет нетривиальных делителей нуля

Док-во:

▷ $ab = 0$ (*) $\Rightarrow \exists b^{-1}$

a — нетрив. дел. нуля

$\cdot b^{-1}$

$a = 0 \cdot b^{-1} = 0$

$a = 0$ противоречие ◀

a — трив. дел.

Опр.: $L \subseteq R$ (подкольцо, кольцо) наз. подкольцом если:

1) L — аддитивная подгруппа группы R

2) L замкнуто отн. умножения

Пр. подкольца: $2\mathbb{Z} \subseteq \mathbb{Z}$

Опр.: $\exists$ F – поле

$K \subseteq F$ – подполе если:

1) K – подкольцо F
2) $\forall x \neq 0 \in K : x^{-1} \in K$
3) $1 \in K$ единица поля $\in$ подполе

Пр.: $\mathbb{Q} \leq \mathbb{R}$ (подполе)

Порядок кольца/поля $R = |R|$ (кол-во эл.)

Кольцо вычетов

$\mathbb{Z}$ $x - y \vdots n$ $\quad x - y \in n\mathbb{Z}$

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ (остаток) $\quad \mathbb{Z}/n\mathbb{Z}$

вычеты = остатки

$a_1 \equiv b_1 \pmod n$

$a_2 \equiv b_2 \pmod n$

Верно, что $a_1 + a_2 \equiv b_1 + b_2 \pmod n$

можем ли сказать что $a_1 a_2 \equiv b_1 b_2 \pmod n$?

$a_1 = b_1 + k_1 n \qquad a_2 = b_2 + k_2 n$

$a_1 a_2 = (b_1 + k_1 n)(b_2 + k_2 n) = b_1 b_2 + n(b_1 k_2 + k_1 b_2 + k_1 k_2 n)$

$\Downarrow$

$a_1 a_2 \equiv b_1 b_2 \pmod n$

$\langle \mathbb{Z}_n, +, \cdot \rangle$ (кольцо вычетов) – ассоц., коммут., кольцо с 1

$\triangleleft \langle \mathbb{Z}_4, +, \cdot \rangle$

$\bar{2} \cdot \bar{1} = \bar{2}$

нетр. дел. нуля $\Rightarrow$ $\mathbb{Z}_4$ не поле

$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$

Когда $\mathbb{Z}$ – поле?

Теорема:

$\mathbb{Z}_n$ – поле $\Leftrightarrow$ n – простое число

Док-во:

$\triangleright$ $\exists\, n = km \quad 1 < k, m < n$

$\triangleleft$ $\bar{k}$ и $\bar{m} \neq 0$ $\quad \bar{n} = \bar{0} = \overline{km} = \bar{k} \cdot \bar{m} \Rightarrow$

$\bar{k}, \bar{m}$ – нетрив. дел. нуля

$\Lleftarrow$

если n-сост $\mathbb{Z}_n$ – не поле

$\triangleleft$ n – простое $\quad \bar{a} \neq 0$ $\quad 0 \leq k\ell < n \Rightarrow k - \ell < n$

$\bar{0} \cdot \bar{a}, \bar{1} \cdot \bar{a}, \bar{2} \cdot \bar{a}, \bar{3} \cdot \bar{a}, \ldots, \overline{(n-1)} \cdot \bar{a}$ $\quad k > \ell;\ 0 \leq a \leq n-1$

Покажем это вновь все эл-ты $\mathbb{Z}_n$

$\exists\, \bar{k} \cdot \bar{a} = \bar{\ell} \cdot \bar{a}$

$\bar{k} \cdot \bar{a} - \bar{\ell} \cdot a = \bar{0}$

$(\overline{k - \ell})\, \bar{a} = 0$

$\Downarrow$

есть $\bar{1}$

$(k - \ell)\, a \equiv 0 \pmod n$

$(k - \ell)\, a \ \vdots\ n \in \mathbb{P}$

$\Downarrow$

$k - \ell \not\vdots\ n,\ a \not\vdots\ n \Rightarrow$ все эл. разные

противоречие

$\forall \mathbb{Z}_p$ (p — простое число) $\quad \underbrace{\bar{1} + \bar{1} + \ldots + \bar{1}}_{p \text{ раз}} = \bar{0}$

если F — поле и n — такое наим. натур-ое число, что

$\underbrace{1 + 1 + \ldots + 1}_{n} = 0$ то такое число наз. характеристикой поля (char)

Пр.: $\operatorname{char} F = n$

$\operatorname{char} \mathbb{Z}_p = p$

$\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = 0$

Лемма:

если $\operatorname{char} F > 0 \Rightarrow \operatorname{char} F \in \mathbb{P}$

Док-во

▷ $\underbrace{1 + 1 + \ldots + 1}_{km} = 0 \Rightarrow \left(\underbrace{1 + \ldots + 1}_{k}\right)\left(\underbrace{1 + \ldots + 1}_{m}\right) = 0$

$1 + 1 + 1 + \ldots + 1 = 0$ противоречие тому, что

$(1 + 1)(1 + \ldots + 1) = 0$ это F — поле ◀

Т.к. получили натур. делитель

$\forall \mathbb{Z}_p$

$$(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{p-k}$$

$$C_p^k = \frac{p!}{k!(p-k)!} = \frac{(p-k+1)(p-k+2)\dots p}{k!} \vdots p$$

$$(a+b)^p = a^p + b^p$$

$$(x+y)^3 = x^3 + y^3 \quad в \ \mathbb{Z}_3$$

Малая теорема Ферма:

$$a^p = a \pmod p$$

если $\left(НОД(a,p) = 1 \quad a^{p-1} \equiv 1 \pmod p\right)$

Док-во:

$\triangleright$ $\overline{a^p} = \bar{a}$ в поле $\mathbb{Z}_p$

$$\bar{a} = \overline{\underbrace{1+1 \dots +1}_{a}} = \bar{1} + \bar{1} + \dots + \bar{1}$$

(в поле $\mathbb{Z}_p$)

$$\overline{a^p} = \bar{a}^p = (\bar{1}+\bar{1}+\dots+\bar{1})^p = \underbrace{\bar{1}^p + \bar{1}^p + \bar{1}^p \dots + \bar{1}^p}_{a} = \bar{a}$$

($\bar{1}^p = \bar{1}$, $\bar{1}^p = \bar{1}$ ...) $\blacktriangleleft$

$\forall F$ – поле

$$F \times F = \{(x,y) \mid x \in F, y \in F\} = F^2$$

$\mathbb{R}^2$ – декартова плоскость

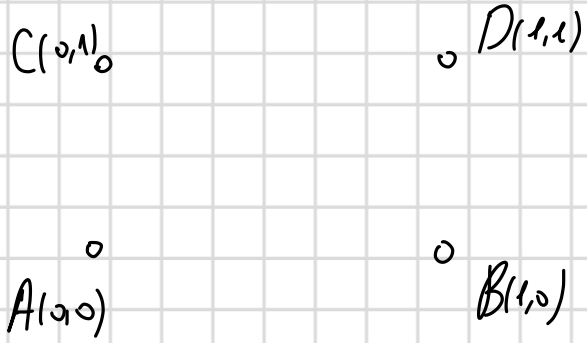
Аксиомы:

1) через любые 2 т. проходит только 1 прямая

2) Для каждой прямой и $\notin$ ей т. сущ. ровно 1 прямая пересекающаяся с данной

3) существуют 3 точки не лежащие на 1 прямой

$\mathbb{F} = \mathbb{Z}_2 \quad \mathbb{Z}_2 \times \mathbb{Z}_2$



прямые: $AC; BD; AB; CD; AD; CB$

$\parallel$ прямые: $AC \parallel BD$; $AB \parallel CD$; $AD \parallel CB$

Пр.: мн-во точек, удов. ур-ию $ax + by = c$, где хотя бы один из коэфф. $\neq 0$

$AC: x = 0$ $\quad AB: y = 0$ $\quad AD: 1x + 1y = 0$

$BD: x = 1$ $\quad CD: y = 1$ $\quad CB: x + y = 1$