

Кольца и Поля

Кольцо

R - кольцо

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

Св-ва операции

1) по ассоциативности это абелева группа

2) дистрибутивность

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

Пр. кольца:

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

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

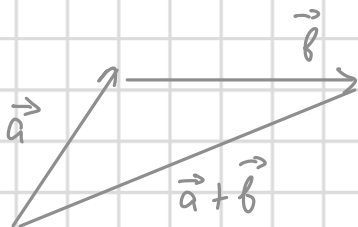
5) $\mathbb{Z}[x]$ — многочлены с целыми коэфф. со слож. и умнож.

6) $\text{Func}(\overset{X}{\xrightarrow{u}}, \overset{Y}{\xrightarrow{v}})$ с поточечным сложением и умножением

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

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

7) Геом. векторы со слож. и векторным умнож.

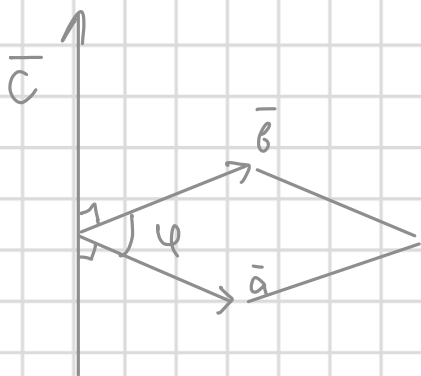


$$\overrightarrow{a \times b}:$$

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

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

3) $\vec{a}_1, \vec{b}_2, \vec{c}_3$ образуют правую тройку (\vec{c} перп. ко направлению \vec{a} и \vec{b})



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

Сначала проверим $(f+g) \circ h$

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

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

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

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

$$\left. \begin{array}{l} f \circ h = x^2 \\ g \circ h = x^2 \end{array} \right\} \Rightarrow 2x^2 = x^2 + x^2$$

Теперь проверим $h \circ (f+g)$

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

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

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

$$\Rightarrow 2x^2$$

Свойства из опр. кольца

$$1) 0 \cdot x = 0$$

$$\text{доказ.: } \triangleright yx = (0+y)x = 0x + yx \quad \text{сокр. т.к. все др.-ти взаимно просты}$$

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

$$2) (-x)y = (-xy) \quad \text{и т.д.}$$

Если кольцо коммутативно то это ассоциативное

кольцо

Если кольцо коммутативно то это коммутативное кольцо

Пром. век-ры не коммутативны и не ассоциативны

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

векторное произведение

Если есть нейтр. эл. то умножение : ноз комбо с единицей

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

Поле

Опр.: Поле - коммутативное и ассоциативное комбо с единицей в котором каждый ненулевой эл. обратим

Пр. поля: \mathbb{Q}, \mathbb{R}

\mathbb{Z} - не поле

Замечание: комбо 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

$$1^{-1} = 1$$

$x \in \overset{\text{комбо}}{K} - \overset{\text{ноз.}}{\text{злепитель}} \text{ нуля, если } \exists \underset{\text{ноз.}}{y} \in K : xy = 0$

0 - тривиальный элемент нуля

$x \neq 0$ - нетривиальный элемент нуля

^{нестр. ген. идеал}
Пр.: $\nexists \text{ Func } (X, \mathbb{R}), \text{ где } |x| > 1$

Операции: $+$, \cdot ноль и единица

$$\emptyset \neq Y \subseteq X \quad f(x) = \begin{cases} 0, & x \in Y \\ 1, & x \notin Y \end{cases}$$

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

$$f \cdot g \equiv 0$$

$\uparrow \quad \uparrow$
нестривительные генераторы идеала

Лемма:

\emptyset идеал не имеет нестривительных генераторов идеала

Док-во:

$$\triangleright \quad \begin{matrix} \text{нестр. ген. идеал} \\ a \cdot b = 0 \end{matrix} \quad \begin{matrix} \text{нестр. ген. идеал} \\ \exists b^{-1} \end{matrix}$$

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

$a = 0$ противоречие
 a — трив. ген.

Опр.: $\overset{\text{подк.}}{L} \subseteq \overset{\text{кольцо}}{R}$ наз. подкольцом если:

- 1) L — аддитивная подгруппа группы R
- 2) L замкнуто относительно умножения

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

Опр.: \mathbb{F} - поле

$K \subseteq F$ - подполе если:

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

Пр.: $\mathbb{Q} \leq \mathbb{R}$

Порядок кольца / поле $R = |R|$ ^{кон-во эл.}

Кольцо вычетов

\mathbb{Z} ^{остатки} $x-y : n$ $x-y \in n\mathbb{Z}$
 $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}$ $\mathbb{Z} / n\mathbb{Z}$
вычеты = остатки

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

можно ли сказать что $a_1 a_2 \equiv b_1 b_2 \pmod{n}$?

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

$$a_1 a_2 = (b_1 + k_1 n)(b_2 + k_2 n) = b_1 b_2 + n(b_1 k_2 + k_1 b_2 + k_1 k_2 n) \\ \Downarrow \\ a_1 a_2 \equiv b_1 b_2 \pmod{n}$$

^{кольцо вычетов}
 $\langle \mathbb{Z}_n, +, \cdot \rangle$ - ассоц., коммут., кольцо с 1

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

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

нестр. фн. мнрл $\Rightarrow \mathbb{Z}_4$ не нонл

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

кого \mathbb{Z} -нонл?

Теорема:

$$\mathbb{Z}_n - \text{нонл} \Leftrightarrow n - \text{простое число}$$

Док-во:

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

$$\triangleleft \bar{k} \text{ и } \bar{m} \neq 0$$

$$\bar{n} = \bar{0} = \overline{km} = \bar{k} \cdot \bar{m} \Rightarrow$$

$\bar{k} \cdot \bar{m}$ - нестр. фн. мнрл



Если n -простое \mathbb{Z}_n - не нонл

$$\triangleleft n - \text{простое}$$

$$\bar{a} \neq 0$$

$$0 \leq k\ell < n \Rightarrow k - \ell < n$$

$$\bar{0} \cdot \bar{a}, \bar{1} \cdot \bar{a}, \bar{2} \cdot \bar{a}, \bar{3} \cdot \bar{a}, \dots, \overline{(n-1)} \cdot \bar{a}$$

$$k > \ell; 0 \leq a \leq n-1$$

Покажем что вообще все n -пл \mathbb{Z}_n

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

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

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

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

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



$$k - \ell \not\equiv 0 \pmod{n}, a \not\equiv 0 \pmod{n} \Rightarrow \text{все } n$$

противоречие

разные

\Downarrow
есть $\bar{1}$

$$\triangle \mathbb{Z}_p$$

простое
число

$$\underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{p \text{ раз}} = \bar{0}$$

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

$$\underbrace{1 + 1 + \dots + 1}_n = 0 \quad \text{то такое число наз. характеристикой}$$

поле

(char)

Пр.: char $F = n$

char $\mathbb{Z}_p = p$

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

Лемма:

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

Доказ.

$$\triangle \underbrace{1 + 1 + \dots + 1}_{km} = 0 \Rightarrow \underbrace{(1 + 1 + \dots + 1)}_k \underbrace{(1 + 1 + \dots + 1)}_m = 0$$

$$1 + 1 + 1 + 1 + 1 + 1 = 0$$

нельзя перем. то же,

$$(1 + 1)(1 + 1 + 1) = 0$$

что F — поле

т.к. нулевой элемент не равен единице

$$\triangle \mathbb{Z}_p$$

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

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

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

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

Малая теорема Ферма:

$$a^p = a \pmod{p}$$

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

Док-во:

$$\triangle \quad \overline{a^p} = \overline{a} \quad \text{в поле } \mathbb{Z}_p$$

$$\overline{a} = \overbrace{1+1+\dots+1}^a = \overline{1} + \overline{1} + \dots + \overline{1}$$

$$\overline{a^p} = \overline{a}^p = (\overline{1} + \overline{1} + \dots + \overline{1})^p \stackrel{\text{в поле } \mathbb{Z}_p}{=} \underbrace{\overline{1}^p + \overline{1}^p + \overline{1}^p + \dots + \overline{1}^p}_a = \overline{a}$$

\sqrt{F} -поле

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

\mathbb{R}^2 - евклидова норма

Аксиомы:

- 1) Через любые 2 т. можно провести 1 прямую
- 2) Для любых двух точек a и b в \mathbb{R}^2 существует 1 прямая, соединяющая их
- 3) Любые две прямые либо параллельны, либо пересекаются в одной точке

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

$$C(0,1)$$

$$D(1,1)$$

прямые: $AC; BD; AB;$

$CD; AD; CB$

// прямые: $AC \parallel BD; AB \parallel CD;$

$AD \parallel CB$

$$A(0,0)$$

$$B(1,0)$$

Пр.: мн-во точек, удовлетв-щих урав-нию $ax + by = c$ где $a, b, c \in \mathbb{Z}$ и $a, b \neq 0$

$$AC : x = 0$$

$$AB : y = 0$$

$$AD : x + y = 1$$

$$BD : x = 1$$

$$CD : y = 1$$

$$CB : x + y = 1$$