Фактор-кольцо

Опр. K – кольцо, L – идеал кольца K $(K, +, \cdot)$

K/L – фактор-кольцо K по идеалу L

$\{a + L\}$ (классы вычетов по NN)

1) $(a+L)+(b+L) = (a+b)+L$

2) $(a+L)\cdot(b+L) = (a\cdot b)+L$

Пример.

$\mathbb{Z}$, $L = \{0, \pm 3, \pm 6\}$

$0 + L = L$

$1 + L = \{1, 4, -2, 7, -5, \dots\}$

$2 + L = \{2, 5, -1, 8, -4, \dots\}$

$\mathbb{Z}/L = \{(0+L), (1+L), (2+L)\} \cong \mathbb{Z}_3$

Делители нуля

Опр. $a, b \in K$, $a \cdot b = 0$, $a \neq 0$, $b \neq 0$

a – левый делитель нуля

b – правый делитель нуля

$(K, +, \cdot)$ $a, b \in K$, $a \cdot b = e_+$, $a \neq e_+$, $b \neq e_+$

Опр. K – коммут. кольцо делителя нуля

Пример.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, $+$, $\cdot$

$2 \cdot 3 = 0$

$3 \cdot 4 = 0$

$\Rightarrow$ $2, 3, 4$ } делители нуля

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, $+$, $\cdot$

Делителей нуля нет.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

L. делитель нуля R. делитель нуля

Опр. K – коммут. кольцо без делителей нуля = целостное кольцо.

Теорема. K – целостное $\leftrightarrow$ $ac = bc$, $c \neq 0 \Rightarrow a = b$ $\Rightarrow$

$\Rightarrow$ $ac = bc \Rightarrow ac - bc = 0 \Rightarrow (a-b)c = 0 \Rightarrow$ ($c \neq 0$)

$\Rightarrow a - b = 0 \Rightarrow a = b$ ■

$\Leftarrow$ $ac = bc$, $c \neq 0 \Rightarrow a = b$

$ab = 0$, $a \neq 0$, $b \neq 0$?!?!?! – против. ■

a – обратим. $\exists a^{-1}$: $a \cdot a^{-1} = a^{-1} \cdot a = 1 = e$.

$a^{-1}a = 1$ $\quad ab = 0$

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

$0 = b$

Опр. $U(K) = \{a \in K : \exists a^{-1} \in K\}$ – мн-во обратим. эл.

Пример.

$U(\mathbb{Z}) = \{\pm 1\}$

$U(\mathbb{R}) = \mathbb{R}^*$

$U(\mathbb{Z}_6) = \{1, 5\}$

$U(\mathbb{Z}_5) = \{1, 2, 3, 4\} = \mathbb{Z}_5^*$

$1 \cdot 1 = 1$ $\quad 2 \cdot 3 = 1$ $\quad 4 \cdot 4 = 1$

Теорема. K – коммут. кольцо с единицей

$U(K)$ – группа по 2й операции

Опр. Поле – коммут. кольцо с единицей, у которого все ненулевые элементы обратимы. „P"

$U(P) = P^*$

P^* – мультипликативная группа поля

Пример.

$\mathbb{Z}$ – кольцо цел. чисел.

$\mathbb{Q}$ – поле рацион. чисел.

$\mathbb{R}$ – поле вещественных чисел.

$\mathbb{C}$ – поле комплексных чисел.

$M_{n\times n}$ – кольцо квадратных матриц.

$P[x]$ – кольцо многочленов.

$\mathbb{Z}[i] = \{a+bi,\ a,b\in\mathbb{Z}\}$ – кольцо Гауссовых чисел.

$\mathbb{Z}_p$ – поле

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

1. $\mathbb{Z}_n$, $n = a\cdot b$, $a\cdot b = 0 \Rightarrow a, b$ – делители нуля $\Rightarrow$
$\Rightarrow a, b$ не обратимы $\Rightarrow \mathbb{Z}_n$ – не поле

2. $\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$ $a \neq 0$

$0\cdot a = 0$, $1\cdot a = a$, $2a$, $3a$, $\dots$, $(p-1)a$ – все различны

▲ $ka = m\cdot a \Rightarrow k = m$

$\exists\, b: ba = 1 \Rightarrow b = a^{-1}$ ▲

Теорема. Малая теорема Ферма

$\forall\ a \neq 0 \pmod p$ $\quad a^{p-1} = 1 \pmod p$

▲ $\mathbb{Z}_p$ – поле $\Rightarrow$ $\mathbb{Z}_p^*$ – мультипликативная группа поля

$\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$

$\mathrm{Card}\ \mathbb{Z}_p^* = p-1$ $\quad \forall a\in\mathbb{Z}_p^*$ $\mathrm{Card}\ a$ – делитель $p-1$

$a^{\mathrm{Card}\ a} = 1 \Rightarrow (a^{\mathrm{Card}\ a})^{\alpha} = a^{\alpha\cdot\mathrm{Card}\ a} = a^{p-1} = 1$ ▲

Пример

$2^{1000} \pmod{17} = 2^{(16 \cdot 62 + 8)} \pmod{17} = 2^8 \pmod{17}$

$2^{16} = 1 \pmod{17}$

Характеристика поля

Опр. P_1 - подполе поля P

P_1 - подкольцо кольца P и P_1 - поле

P - расширение поля P_1

Пример.

$\mathbb{Q}$ - подполе $\mathbb{R}$, $\mathbb{R}$ - расширение $\mathbb{Q}$

Опр. P - простое поле (нет нетривиальных подполей)

Теорема. $\forall P$ - поле $\exists!$ простое подполе P_1

$P_1 \cong \mathbb{Q}$, $P_1 \cong \mathbb{Z}_p$

$\{e_+, e_\cdot, \dots\} \to \{0, 1, \dots\}$

$1 \in P_1 \Rightarrow 1+1 = 2 \in P_1 \Rightarrow 3 \in P$

1) $1+1+1+\dots+1 = 0$ $\quad P_1 \cong \mathbb{Z}_p$

2) $1+1+\dots+1+\dots$

$(1+1)^{-1}$, $(1+1+1)^{-1}$, $\dots$ $\quad \overbrace{(1+1+\dots+1)}^{k} \cdot \overbrace{(1+1+\dots+1)}^{m}{}^{-1} \to \frac{k}{m}$

$P_1 \cong \mathbb{Q}$

$P_1 \subseteq P$, $P_2 \subseteq P$, $P_3 \subseteq P$, $\dots$ $\quad P_1 \cap P_2 \cap \dots$ — самое простое подполе

Опр. P, у которого простое подполе $P_1 \cong \mathbb{Q}$

$\mathrm{Char}\, P = 0$

Опр. P, у которого простое подполе $P_1 \cong \mathbb{Z}_p$

$\mathrm{Char}\, P = p$

Кол-во элементов поля $= p^k$

$\{0, 1\} \cong \mathbb{Z}_2$ $\quad$ p – простое, k – натуральное

$\mathbb{Z}_p$ – поле

2, 3, 4, 5, ~~6~~, 7, 8, 9, ~~10~~, 11

Кольцо многочленов

$(a_0, a_1, a_2, \dots, a_n, \dots)$, $a_i \in A$ – кольцо

конечное число $a_i \neq 0$

$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$

$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$

$c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, …, $c_k = \sum_{i=0}^{k} a_i b_{k-i}$

Кольцо многочленов над кольцом A „$A[x]$"

Пример.

$\mathbb{Z}[x] = \{a_0 + a_1 x + a_2 x^2 + \dots, a_i \in \mathbb{Z}\}$

$\mathbb{Z}_2[x] = \{x, x+1, x^2+1, x^{10} + x + 1 \dots\}$