Пръстени

Опр. R - пръстен, ако:

0/ Имаме бинарни опер. $+$ и $\cdot$

1/ $(R, +)$ — абелева гр.

2/ $\forall a,b,c \in R \quad (ab)c = a(bc)$

3/ $\forall a,b,c \in R \quad a(b+c) = ab + ac$

$(a+b)c = ac + bc$

Заб. $(R, +)$ - адитивна група на R

Св-ва: 1/ $0, -a$ са единствени

2/ $\forall a \in R \quad 0.a = 0$

Опр. R - пр.

1/ R - комутативен пръстен, ако $\forall a, b \in R \quad ab = ba$

2/ $1 \in R$ е единичен, ако $\forall a \in R \quad 1.a = a.1 = a$

(1 е единствен)

3/ R е пръстен с единица, ако има единичен ел.

4/ Ако R е пр. с 1 казваме, че $a \in R$ е обратим, ако $\exists a^* : aa^* = a^*a = 1$

(a^* е единствен и го бележим с a^{-1})

5) $a \in R$ е делител на нулата, ако $\exists\, a', a'' \in R$: $aa' = a''a = 0$ (Ако само $aa' = 0$ - a е лев делител; аналогично за $a''a = 0$ - десен делител)

6) Област на цялост е комутативен пр. с 1 без делители на 0

7) Тяло е пръстен с 1, в който $\forall$ ненулев ел. е обратим

8) Поле е комутативно тяло

Зад Ако R е ком. пр. с 1, то

$R^* = \{a \in R \mid \exists b \in R : ab = ba = 1\}$ с $\cdot$ е група

мултипликативна група на R

$\left((a^{-1})^{-1} = a\ ;\ (ab)^{-1} = b^{-1}a^{-1}\right)$

Зад. $\mathbb{Z}_n$, $\mathbb{Z}_n^* = \{\bar{a} \mid (a,n)=1\}$, $|\mathbb{Z}_n^*| = \varphi(n)$

$\forall \underbrace{\bar{a} \in \mathbb{Z}_n^*}_{(a,n)=1}$ $\bar{a}^{\varphi(n)} = \bar{1}$ (Лагранж) $\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Тв (Ойлер-Ферма) $\forall a \in \mathbb{Z} : (a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Зад. Ако $a \in R$ - обратим $\Rightarrow$ a не е делител на 0

Ако a е делител на 0 $\Rightarrow$ a не е обратим

ТВ (теорема на Уилсън) p - просто $\iff (p-1)! + 1 \equiv 0 \pmod p$

Забел. $a, p-a$; $p-a \equiv -a$; $a(p-a) \equiv -a^2$

Д-во (2) $\iff \bar{1} . \bar{2} \dots \overline{(p-1)} = -\bar{1}$ в $\mathbb{Z}_p$

($\Leftarrow$ очевидно; Ако $p = ab$, $1 < a \le p-1$, то $a \mid p \mid (p-1)! + 1$

$a \mid (p-1)!$ $\quad a \mid 1$)

$\bar{a} = \bar{a}^{-1}$

$\Downarrow$

$\bar{a}^2 = \bar{1} \iff a^2 \equiv 1 \iff p \mid a^2 - 1 = (a-1)(a+1) \iff p \mid a-1$ или $p \mid a+1$

$\iff a \equiv \pm 1 \pmod p \iff \bar{a} = \pm \bar{1}$ $\quad (-\bar{1} = \overline{p-1})$

$\bar{2} . \bar{3} \dots \overline{p-2} = \underbrace{\bar{1} \dots \bar{1}}_{\frac{p-3}{2}} = \bar{1}$

Считаме, че $p > 2$ ($p = 2$ очев.)

$\bar{1} . \bar{2} \dots \overline{p-1} = \bar{1} . \underbrace{\bar{2} \dots \overline{p-2}}_{\bar{1}} . \overline{p-1} = \overline{p-1} = -\bar{1}$

Пр. 1/ $\mathbb{Z}$ - област ; $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$

2/ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ - полета ; $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

3/ $M_n(F)$ - пр. с 1 (не е комутативен и има дел. на 0)

$$(M_n(F))^* = GL_n(F)$$

Зад. $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

F - поле (тяло) $F^* = F \setminus \{0\}$

4/ $\mathbb{Z}_p$ - поле за p - просто

5/ $\mathbb{Z}_n$ - ком. пр. с 1 и има дел. на 0 за n - съставно

Идеал. Фактор-пръстен. Теорема за ХММ

<u>Опр.</u> $\boxed{K \subseteq R}$ е подпръстен ($K < R$), ако

K е пръстен относно опер. $+$ и $\circ$ на R

<u>Зад.</u> $\Leftrightarrow$ $\forall a,b \in K \quad a-b,\ ab \in K$

<u>Зад.</u> подполе: $\forall a,b \in K \quad a-b, \underbrace{ab,\ b^{-1}}_{ab^{-1}} (b \neq 0) \in K$

<u>Опр.</u> $I \lhd R$ идеал на R, ако:

1) $\forall i_1, i_2 \in I \quad i_1 - i_2 \in I \quad \left(\Leftrightarrow \overset{\text{нормална подгрупа}}{(I,+) \lhd (R,+)}\right)$

2) $\forall i \in I,\ \forall r \in R \quad \underset{\text{десен}}{\underline{ir}},\ \underset{\text{ляв}}{ri} \in I$

Зад. Всеки идеал е подпръстен

Пр. 1/ $I \lhd \mathbb{Z} \Rightarrow (I,+) < (\mathbb{Z},+) = \langle 1 \rangle$
$\Rightarrow \exists n \in \mathbb{Z}: I = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ ... и това наистина е идеал $\forall n$ ($n \in \mathbb{N}$)

2/ F - поле, $I \lhd F \Rightarrow I = \{0\}, F$

Зад. $I \lhd R$ и $a \in I$ е обратим (в частност е 1), то $I = R$ $(a \in I \Rightarrow 1 = a^{-1}a \in I \Rightarrow \forall b \ \ b = 1.b \in I)$

3) $M_2(F)$; $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in F \right\} \subseteq M_2(F)$
I е десен идеал, но не е лев

Нека R е пр. и $I \triangleleft R$

$(I,+) \triangleleft (R,+) \longrightarrow (R/I,+)$ факторгрупа абелева

$R/I = \{\underset{\bar{r}}{\underset{\shortparallel}{r+I}} \mid r \in R\}$; $r+I = \{r+i \mid i \in I\}$

$\bar{r}_1 + \bar{r}_2 = \overline{r_1+r_2}$ $\quad\Big|\quad$ $\bar{r}_1 = \bar{r}_2 \Leftrightarrow r_1 - r_2 \in I$ $\quad (r_1 \equiv r_2 \pmod{I})$

$\bar{r}_1 \cdot \bar{r}_2 := \overline{r_1 r_2}$

<u>Тв</u> $\cdot$ е коректна

<u>Д-во</u> $\bar{r}_1 = \bar{r}_1'$ и $\bar{r}_2 = \bar{r}_2'$ $\Rightarrow r_1 - r_1', \; r_2 - r_2' \in I$

$\Rightarrow \exists i_1, i_2 : \left| \begin{array}{l} r_1 = r_1' + i_1 \\ r_2 = r_2' + i_2 \end{array} \right.$ $\quad r_1 r_2 = r_1' r_2' + \underbrace{r_1' i_2 + i_1 r_2' + i_1 i_2}_{\in I}$

$\Rightarrow r_1 r_2 - r_1' r_2' \in I \Rightarrow \overline{r_1 r_2} = \overline{r_1' r_2'}$

Тв $(R/I, +, \cdot)$ е пръстен

$$\Big\{ (\bar{r}_1 \bar{r}_2)\bar{r}_3 = \overline{r_1 r_2}\,\bar{r}_3 = \overline{(r_1 r_2) r_3} = \overline{r_1 (r_2 r_3)} =$$

$$= \bar{r}_1\, \overline{r_2 r_3} = \bar{r}_1 (\bar{r}_2 \bar{r}_3), \text{ Аналог.}$$

$$\bar{r}_1 (\bar{r}_2 + \bar{r}_3) = \dots ; \quad (\bar{r}_1 + \bar{r}_2)\bar{r}_3 = \dots \Big)$$

Опр. R/I – факторпръстен на R по I

Зад. 1) R – ком. $\Rightarrow$ R/I – ком.

2) R – пр. с 1 $\Rightarrow$ R/I – пр. с 1

3) не е в. за дел. на 0

4) R – пр. с 1 и $a \in R^*$ $\Rightarrow$ $\bar{a} \in (R/I)^*$

Опр. 1) $\varphi: R_1 \to R_2$ е ХММ на пръстени, ако

- $\forall a, b \in R_1 \quad \varphi(a+b) = \varphi(a) + \varphi(b)$
- $\forall a, b \in R_1 \quad \varphi(ab) = \varphi(a)\varphi(b)$

Ако φ е и биекция $\to$ φ е изоморфизъм
$(R_1 \cong R_2)$

2) $\operatorname{Ker} \varphi = \{ r_1 \in R_1 \mid \varphi(r_1) = 0_{R_2} \}$

3) $\operatorname{Im} \varphi = \{ r_2 \in R_2 \mid \exists r_1 : \varphi(r_1) = r_2 \} = \varphi(R_1) =$
$= \{ \varphi(r_1) \mid r_1 \in R_1 \}$

Забел. 1) φ - ХМОМ $\Rightarrow \varphi(0_{R_1}) = 0_{R_2}$, $\varphi(-r_1) = -\varphi(r_1)$

$\varphi(a-b) = \varphi(a) - \varphi(b)$

(φ е ХОМ на групите $(R_1,+)$ и $(R_2,+)$)

2) Ако R_1 и R_2 са пр. с 1

φ е ХМОМ на групите R_1^* и R_2^* $\rightarrow \varphi(1_{R_1}) = 1_{R_2}$

Тв. 1) $\operatorname{Ker}\varphi \triangleleft R_1$

2) $\operatorname{Im}\varphi < R_2$ (подпръстен)

$$\left(\varphi(r_1') = r_2',\ \varphi(r_1'') = r_2'' \Rightarrow \begin{array}{l}\varphi(r_1' - r_1'') = r_2' - r_2'' \\ \varphi(r_1' r_1'') = r_2' r_2''\end{array}\right)$$