Пръстени

D Нека $M \neq \emptyset$ с 2 бинарни операции: $+, \cdot$. M е пръстен, ако са изпълнени следните аксиоми:

1) $(M,+)$ – абелева група:
$$\begin{cases} a+b=b+a \\ (a+b)+c=a+(b+c) \\ \exists 0 : a+0=a, \forall a \\ \forall a \; \exists b_a : a+b_a=b_a+a=0 \end{cases}$$

2) асоциативност на умножението: $(ab)c=a(bc), \forall a,b,c \in M$

3) $a(b+c)=ab+ac$;
$(b+c)a=ba+ca$; $\forall a,b,c \in M$

Ако за $\forall a,b \in M \Rightarrow ab=ba$, M се нарича комутативен пръстен.

! При линейните пространства имаме 2 операции, но едната е външна.

Пример: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ – комутативни безкрайни пръстени.

D Нека M е пръстен и K е непразно подмножество на M. K е подпръстен $(K<M)$ на M, ако е пръстен относно същите операции.

Пример: некомутативен пръстен: $M_{n \times n}(\mathbb{R})$
краен пръстен: $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{(n-1)}\}$ → комутативен.
$M_{n \times n}(\mathbb{Z}_2)$ – краен некомутативен пръстен.

$\mathbb{Z}_6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

D M е пръстен с единица, ако $\exists e(1) : ea=ae=a, \forall a$.

Пример за пръстен без единица: $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} < \mathbb{Z}$

D M – пръстен с единица. Елементът a се нарича обратим, ако $\exists b \in M$:
$ab=ba=e$.
$M^* = \{x \in M \mid x \text{ – обратим}\}$
$\mathbb{Z}_6 \to \mathbb{Z}_6^* = \{\bar{1}, \bar{5}\}$
$M_{n \times n}(\mathbb{R}^*) = \{A \in M_{n \times n}(\mathbb{R}) \mid \det A \neq 0\} = GL(n, \mathbb{R})$.

Тв Ако M е пръстен с единица, то M^* е група относно умножението

Доказателство:
$\forall A,B,C \in M^* \to (AB)C=A(BC)$
$e \in M^* \to e \cdot e = e$
$\forall A,B \in M^* \Rightarrow \exists ! A^{-1}, B^{-1} \in M : AA^{-1}=A^{-1}A=e \Rightarrow A^{-1} \in M^*$
(аналогично с B)

$$\left.\begin{array}{l} (AB)(B^{-1}A^{-1})=e \\ (B^{-1}A^{-1}AB)=e \end{array}\right\} AB \in M^* \text{ и } (AB)^{-1} \in M \Rightarrow (M^*, \cdot) \Rightarrow$$

D M^* - мултипликативна група на пръстена M.

$\mathbb{Z}^* = \{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$

D M - пръстен. Елементите $a, b \in M$: $ab = 0$ и $a \neq 0 \neq b$ се наричат делители на 0.

Тв Делителите на нулата не могат да бъдат обратими елементи.

Доказателство:

a - делител на нулата $\Rightarrow \exists\, b \neq 0 : ab = 0$

$a \neq 0$.

Допускаме, че $\exists a^{-1} : aa^{-1} = a^{-1}a = e$.

$a^{-1}ab = eb = b$

$a^{-1} \cdot 0 = 0$ // ↯ $\Rightarrow \nexists a^{-1}$.

Свойства:

1) $\forall a \in M \Rightarrow a.0 = 0.a = 0$.
2) 0 е единствен
3) противоположният елемент е единствен.
4) Ако $\exists$ единичен елемент, то той е единствен.
5) обобщена асоциативност.

D F е поле, ако F е комутативен пръстен с единица, в който всеки ненулев елемент е обратим.

T В пръстена $\mathbb{Z}_n$ $\bar{a} \in \mathbb{Z}_n$ $(\bar{a} \neq \bar{0})$:

1) $\bar{a}$ е обратим $\Leftrightarrow (a, n) = 1$
2) $\bar{a}$ е делител на нулата $\Leftrightarrow (a, n) = d > 1$.

Доказателство:

1) $(a, n) = 1 \Rightarrow \exists u, v \in \mathbb{Z} : au + nv = 1 \Rightarrow au \equiv 1 (n) \Rightarrow \bar{a}\bar{u} = \bar{1}$ в $\mathbb{Z}_n$.
$\Rightarrow \bar{u}$ е обратният на $\bar{a}$.

2) $(a, n) = d > 1 \Rightarrow a = da_1, n = dn_1, (a_1, n_1) = 1$.

$\Rightarrow \bar{a}\bar{n}_1 = \bar{a}_1 d \bar{n}_1 = \bar{a}_1 \bar{n} = \bar{a}_1 \bar{0} = \bar{0} \Rightarrow \bar{a}$ е делител на $\bar{0}$.

Следствия

1) $|\mathbb{Z}_n^*| = \varphi(n)$
2) $\mathbb{Z}$ е поле $\Leftrightarrow n$ е просто
3) $|\mathbb{Z}_n^*| = \varphi(n)$; $\bar{a} \in \mathbb{Z}_n^* \Rightarrow (a, n) = 1$

Разглеждаме $\mathbb{Z}_n^*$ и прилагаме следствието от теорема на Лагранж $\Rightarrow$

$\Rightarrow |\bar{a}|\,|\mathbb{Z}_n^*| \Leftrightarrow |\bar{a}|\,\varphi(n) \Leftrightarrow \bar{a}^{\varphi(n)} = e$

$\Rightarrow$ **Теорема на Ойлер**: Когато $(a, n) = 1$, $a^{\varphi(n)} \equiv 1 (n)$.

4) n - просто $\Rightarrow \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{\bar{0}\}$

$\bar{x}^2 = \bar{1} \Rightarrow \bar{x} \in \{\pm\bar{1}\} \equiv \{\bar{1}, \overline{n-1}\}$

$\Rightarrow$ единственият елемент от ред 2 е $\overline{-1}$.

$\Rightarrow (\overline{n-1})! = \bar{1}.\underbrace{\bar{2}.\ldots.\overline{n-1}}_{\text{ред.} > 2} \equiv -1\,(n)$

нито един от тях не съвпада с обратния си.

$\Rightarrow$ Можем да го разбием на двойки $(a, a^{-1}) \Rightarrow \bar{1}.\bar{3}.\ldots.\overline{(n-2)} = \bar{1}$

Т Теорема на Уилсън

За $\forall$ n - просто $\Rightarrow (n-1)! \equiv -1\,(n)$.

ТВ Нека $K \subset M$, M - пръстен.

$K < M \Leftrightarrow$ 1) $a-b \in K$ 2) $ab \in K$ $\forall a,b \in K$

Доказателство:

$\Leftarrow$) $a-b \in K \Rightarrow K$ е подгрупа на $(M,+)$.

$ab \in K \Rightarrow$ умножението е бинарна операция за K.

② и ③ са в сила за елементите на $M \Rightarrow$

$\Rightarrow$ и за елементите на K

$\Rightarrow K < M$.

$\Rightarrow$)

Полета. Характеристика на полета.

D Характеристика на поле F:

F има характеристика $k \neq 0$ ($\operatorname{char} F = k$), ако k е минималното естествено число, за което $k1 = \underbrace{1+\ldots+1}_{k\text{-пъти}} = 0$. $\operatorname{char} F = 0$, ако $\forall k \in \mathbb{N}$

$\Rightarrow k1 \neq 0$.

Забележка: $k = |1|$, $1 \in (F,+)$.

Т $\operatorname{char} F \in 0$ или просто число, за всяко поле F.

Доказателство:

Допускаме, че $\operatorname{char} F = m = ks$, $k>1$, $s>1 \Rightarrow 0 = m1 = ks1 =$

$= \underbrace{1+1+\ldots+1}_{k.s\text{ пъти}} = \underbrace{(1+\ldots+1)}_{s\text{ пъти}} + \ldots + \underbrace{(1+\ldots+1)}_{s\text{ пъти}} = \underbrace{s1+\ldots+s1}_{k\text{ пъти}} = (k1)(s1) = ab$

k пъти; k пъти; "a"; "b"; $a,b \neq 0$

$k,s < m \Rightarrow ab = 0 \Rightarrow a,b$ - делители на 0

F - поле и $a,b \in F \Rightarrow$ обратими

↯