Групи

Опр. G с $\boxed{\text{бинарна операция}}$ $*$ е група, ако:

1) $*$ е асоциативна

$\forall a,b,c \in G \quad (a*b)*c = a*(b*c)$

2) $*$ има неутрален ел.

$\exists e \in G : \forall a \in G \quad a*e = e*a = a$

3) Всеки ел. на G е обратим

$\forall a \in G \ \exists a' \in G : a*a' = a'*a = e$

Пр. 1) $+$; $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – гр.

$\mathbb{N}$ – не

2) $\cdot$; $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$; $\mathbb{R}^*, \mathbb{C}^*$

$\cdot$; $\{-1, 1\}$

3) V – ЛП ; $(V, +)$ – гр.

4) $GL_n(F) = \{A \in M_n(F) \mid \exists A' \in M_n(F) : AA' = A'A = E\}$

– $A, B \in GL_n(F) \Rightarrow \exists A', B' \in M_n(F) : \begin{array}{|l} AA' = A'A = E \\ BB' = B'B = E \end{array}$

$(AB)(B'A') = (B'A')(AB) = E$

$\Rightarrow AB \in GL_n(F)$

- $A, B, C \in GL_n(F) \subseteq M_n(F)$
  $\Rightarrow A(BC) = (AB)C$
- E - неутр. ел.; $EE = E \to E \in GL_n(F)$
  $\forall A \quad AE = EA = A \Leftarrow$ от $M_n(F)$
- $A \in GL_n(F) \to \exists A' \in M_n(F)$:
  $AA' = A'A = E \to A' \in GL_n(F)$
  $((A')' = A)$

F - поле: A - обр. $\Leftrightarrow A$ - неособена ($\det A \neq 0$)

A, B - обр. $\to \det A, \det B \neq 0 \to$

$$\det AB = \det A \cdot \det B \neq 0$$

F - не е поле - напр. $\mathbb{Z}$

<u>Деф.</u> Ако $\forall a, b \in G \quad a * b = b * a$,
G се нарича абелева (комутативна) гр.

<u>Деф.</u> Пр 1, 2, 3 - абелеви; Пр 4 - не

<u>Деф.</u> 1) Неутралният ел. е единствен

$$\left(e'e'' = \begin{cases} e'' & (e' \text{ - неутр.}) \\ e' & (e'' \text{ - неутр.}) \end{cases} \to e' = e'' \right)$$

2) Обратният ел. е единствен

$$\left(a', a'' \text{ - обр. на } a;\ (a'a)a'' = a'(aa'') = \begin{cases} a'' \\ a' \end{cases} \right)$$

Означаваме го с a^{-1}

3) Може да се док., че редът на скобите е

$a_1 a_2 \dots a_n$ няма значение

.... не ги пишем

Опр. R с бинарни опер. $+, \cdot$ е пръстен, ако

1) $(R, +)$ – абелева гр.

2) $\forall a, b, c \in R$

$(ab)c = a(bc)$

асоциативност на $\cdot$

3) $\forall a, b, c \in R$

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

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

Пр. 1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

2) $M_n(F)$

(F – пръстен)

Опр. R – пръстен

1) R – комутативен пръстен, ако

$\forall a, b \in R$

$ab = ba$

2) R – пръстен с 1, ако $\exists e \in R : \forall a \in R \ ae = ea = a$

Пр – пръстен без 1

$2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$

3) $a^{(\neq 0)} \in R$ – делител на нулата (ляв, десен), ако $\exists b', b'' \in R$, $b' \neq 0 \neq b''$: $\underbrace{ab' = 0}_{\text{ляв}} = \underbrace{b''a}_{\text{десен}}$

4) R – област, ако R – ком. пр. с 1, без дел. на 0

5) R – пр. с 1; $a \in R$ е обратим, ако $\exists b \in R$:

$ab = ba = 1$

6) R - тяло, ако R е пр. с 1, в който $\forall$ ненулев ел. е обратим

7) R - поле, ако е комутативно тяло

Зад. Поле - ком. пр. с 1, в който $\forall$ ненулев е обратим

ТВ 1) единичният ел. е единствен

2) Ако a е обратим и $a', a'' \in R$:

$aa' = a'a = aa'' = a''a = e \Rightarrow \underline{a' = a''}$

$a' = a''$ - обратен на a; a^{-1}

3) $\forall a \in R \quad a.0 = 0.a = 0$

$\left(\underset{\underset{aa}{\parallel}}{a(a+0)} = aa + a.0 \xrightarrow{+(-aa)} a.0 = 0 \right)$

4) a - обратим $\Rightarrow$ a не е делител на 0

$\left(\underset{b \neq 0}{ab = 0} \xrightarrow[\text{отляво}]{a^{-1}.} b = 0 \ ?! \right)$