Опр. Казваме, че множеството G с бинарна операция $*$ е група, ако:

1) $*$ е асоциативна — $\forall a,b,c \in G$

$$(a*b)*c = a*(b*c)$$

2) $*$ има неутрален елемент (единичен, нулев) —

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

3) Всеки ел. в G е обратим —

$$\forall a \in G \ \exists a^{-1} \in G : \ a*a^{-1} = a^{-1}*a = \underline{e}$$

Ако $*$ е комутативна ($\forall a,b \in G \quad a*b = b*a$) казваме, че групата е абелева (комутативна)

Зад. 1) Неутралният ел. е единствен

e', e'' – неутр. $\quad e' * e'' = \begin{cases} e'' \\ e' \end{cases}$

2) обратният ел. е единствен

$a \to a', a''$ са му обратни $\quad \overset{(\quad\quad)}{a' * \underset{(\quad\quad)}{a * a''}} = \begin{cases} a' \\ a'' \end{cases}$

Пр – $\forall$ лин. простр. с $+$; неутрален 0; обратен на a е $(\underline{-a})$
(абел. гр.) противоположен

– $\mathbb{N}, +$ не е група

– $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}; +$ е група (абел.)

неутр. → 1 – $\{-1, 1\}, \cdot$ да (абел.)

– $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}, \mathbb{C}^* = \mathbb{C} \setminus \{0\}; \cdot$ – абел. гр.

- $GL_n(F) = \{A \in M_n(F) \mid A$ - обратима $\}$

(F - поле   обратима $\Leftrightarrow$ неособена ($\det \neq 0$))

- A - обратима $\rightarrow \exists A' \in M_n(F)$: $\boxed{A}\boxed{A'} = \boxed{A'}\boxed{A} = E$

  Ако $\exists A'$, тя е единствена $\rightarrow A^{-1}$
- $E \in GL_n(F)$ - неутр. ел. (единична)
- умн. на матр. е асоциативно
- $(A^{-1})^{-1} = A \in GL_n(F)$
- $GL_n(F)$ затв. отн. $\cdot \Leftrightarrow \cdot$ е бинарна опер.

  $A, B \in GL_n(F) \rightarrow \exists (AB)^{-1} = B^{-1}A^{-1} \rightarrow AB \in GL_n(F)$

(обща линейна група) не е абелева

Зоб. $f : X \to Y$

$\forall x \mapsto \exists!\, y = f(x)$

$\left(F \subseteq X \times Y = \{(x,y) \mid x \in X,\ y \in Y\} \right.$

$F = \{(x, f(x)) \mid x \in X\}$ релация

$\left. (x, y_1), (x, y_2) \Rightarrow y_1 = y_2 \to \right.$ функция$)$

f - инективна: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

f - сюрективна: $\forall y \in Y \ \exists x \in X \ f(x) = y$

f - биективна, ако е инект. и сюрект.

$id_X : X \to X$ идентитет на X

$x \mapsto x$

$f : X \to \underline{Y}$, $g : \underline{Y} \to Z \to g \circ f : X \to Z$ (композиция на f и g (произведение))

„след" $x \mapsto g(f(x))$

- $f: X \to Y \Rightarrow f \circ id_X = id_Y \circ f = f$
- $f: X \to Y$ - обратима, ако $\exists g: Y \to X$: $\left| \begin{array}{l} f \circ g = id_Y \\ g \circ f = id_X \end{array} \right.$

- f - биекция $\Leftrightarrow$ f - обратима
- f - обратима, g е единствена; бележим я с f^{-1}

Пр. Ω - множ.

$S(\Omega) = \{ f: \Omega \to \Omega \mid f \text{ - биекция} \}$

- затв. отн. $\circ$ $\left((f \circ g)^{-1} = g^{-1} \circ f^{-1} \right)$
- id_Ω - ед. ел.
- $\circ$ е асоциат.
- $f^{-1} \in S(\Omega)$ - обратният на f

група (не е абел.)

Симетрична група на Ω

$\Omega = \{1, 2, \dots, n\}$ $\qquad S_n = S(\Omega)$ — симетрична група от ред $n!$

$\sigma \in S_n$; $\sigma : \Omega \to \Omega$ $\qquad \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$

пермутация на $1, 2, \dots, n$

Опр. Множество R с две бинарни операции $+, \cdot$ е пръстен, ако

1) $(R, +)$ — абелева група (4 св-ва)

- $\forall a, b, c \in R \quad (a+b)+c = a+(b+c)$ асоц.
- $\exists 0 \in R : \forall a \in R \quad a+0 = 0+a = a$ (съществуване на неутр. ел.)
- $\forall a \in R \ \exists (-a) \in R : a+(-a) = (-a)+a = 0$ (съществуване на противоп.)
- $\forall a, b \in R \quad a+b = b+a$ (комутативност)

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

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

$a(b+c) = ab + ac$ дистрибутивност

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

Опр. R - пръстен

1) R - комутативен пръстен, ако

$\forall a,b \in R \quad ab = ba$ (комутативност на $\cdot$)

2) R - пръстен с единица

$\exists e \in R : \forall a \in R \quad ea = ae = a$ (съществуване на единичен елемент)

3) $a \in R$ е обратим, ако $\exists a' : aa' = a'a = e$
(R трябва да е пръстен с единица)

Зад. Ако a' $\exists$, то a' е единствено; бележим a^{-1} $\to$ обратен на a

4) $a \overset{\neq 0}{\in} R$ е делител на нулата, ако

$\exists b \overset{\neq 0}{\in} R \; : \; \underset{(\text{ляв})}{ab = 0} \quad \underset{(\text{десен})}{(ba = 0)}$

(При ляв и десен b може да е различно!

5) R - област на цялост, ако R е комутативен пръстен с единица без делители на нулата

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

7) R е поле, ако R е комутативно тяло

Тв. R - пр. с 1, $a \in R$ - обратим $\Rightarrow$ a не е делител на 0

Д-во Нека a е делител на 0 $\Rightarrow$ $\exists b \overset{\neq 0}{\in} R: ab = 0$

$0 \overset{\text{д}}{=} a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = eb = b \Rightarrow b = 0 \uparrow \perp$

Заб. R - тяло или поле $\Rightarrow$ R няма делители на 0

Заб. R - поле $\Leftrightarrow$ R - комутативен пръстен с 1, в който $\forall$ ненулев е обратим.

Заб. Всяко поле е област

Тв R - пр. с 1, $a \in R$ $\Rightarrow$ $a.0 = 0.a = 0$

Д-во $a = 1.a = (1+0)a = 1.a + 0.a = a + 0.a \xrightarrow[\text{отляво}]{+(-a)} 0a = 0$

Тв. R - пр. с 1; $R^* = \{a \in R \mid \exists b \in R \mid ab = ba = e\}$

(множ. от обратимите ел.)

Тогава $(R^*, \cdot)$ е група

Д-во – затвореност $a_1, a_2 \in R^*$ $\exists b_1, b_2 \in R$: $\begin{cases} a_1b_1 = b_1a_1 = e \\ a_2b_2 = b_2a_2 = e \end{cases}$

$$(a_1a_2)(b_2b_1) = (b_2b_1)(a_1a_2) = e \to a_1a_2 \in R^*$$

$(b_1b_2 \in R)$

– асоц. $\Leftarrow$ асоц. на $\cdot$ в R

– ед. ел. $\Leftarrow$ ед. ел. в R

– всеки ел. е обратим $\Leftarrow$ b удовлетв. равенството и $b \in R^*$ (равенството е изп. за a)

Сл./Заб. – b е единствено; $b = a^{-1}$ – обратен на a

– $(a^{-1})^{-1} = a$; $(ab)^{-1} = b^{-1}a^{-1}$

– $M_n(F)$ – пръстен с 1 (не е комутативен)

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

Пр. – $\mathbb{Z}$ – област

– $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ – полета

– Тяло – Тяло на кватернионите – – числа

– Факт: Всяко крайно тяло е поле

– $\{a, b\}$, $a = 0$, $b = 1$

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

– поле с 2 елемента

Зад. Пре ЛП
- Л.К.
- ЛО
- подпространство
- сума и $\oplus$
- линейни изобр.

Сега
пораждане (от множ. $X \to \langle X \rangle$)
Подгрупи, подпръстени, подполе, подтяло
декартово произв.
хомоморфизми

Зад/Деф $g \in G$ - гр.,

$\cdot$

$$g^n = \begin{cases} \underbrace{g \cdot g \cdot \ldots \cdot g}_{n} & n \in \mathbb{N} \\ \underbrace{g^{-1} \ldots g^{-1}}_{-n} & n < 0 \\ e & n = 0 \end{cases}$$

Може да се докаже, че

$(g^m)^n = g^{mn}$; $g^m \cdot g^n = g^{m+n}$

$+$

$$\left.\begin{matrix} \underbrace{g + g + \ldots + g}_{n} \\ \underbrace{(-g) + (-g) + \ldots + (-g)}_{-n} \\ 0 \end{matrix}\right\} \begin{matrix} \mathbb{Z} \quad G \\ n \cdot g \end{matrix}$$

(означение)

$m(ng) = (mn)g$; $mg + ng = (m+n)g$

Пр. U, V — ЛП над F

$W := U \times V$; $(u_1, v_1) + (u_2, v_2) = (u_1 + u_2, v_1 + v_2)$

ЛП над F $\quad \lambda(u, v) = (\lambda u, \lambda v)$

$\bar{U} = U \times \{\theta_V\}$, $\bar{V} = \{\theta_U\} \times V$; $\bar{U} \cong U$, $\bar{V} \cong V$

$W = \bar{U} \oplus \bar{V}$; $\bar{U}, \bar{V}$ — подпростр. на W

Опр. Под X е подмножество на множ. от вид X, което също е от вид X, относно операциите на множеството (понякога); Пишем $<$

Тв. 1/ G — гр. $H < G \iff H \subseteq G$ и $\left|\begin{array}{l} \forall h_1, h_2 \in H \quad h_1 h_2 \in H \\ e_G \in H \\ \forall h \in H \quad h^{-1} \in H \end{array}\right.$

$\iff H \subseteq G$ и $\left|\begin{array}{l} \forall h_1, h_2 \in H \quad h_1 h_2 \in H \\ \forall h \in H \quad h^{-1} \in H \end{array}\right.$ $\iff$

$\Leftrightarrow H \subseteq G$ и $\forall h_1, h_2 \in H \quad h_1^{-1}h_2 \in H \quad (h_1 h_2^{-1} \in H)$

Заб. При $+$; $h_1^{-1}h_2 \to (-h_1)+h_2 \quad (h_1+(-h_2)=h_1-h_2)$

Заб. $+$ — адитивни и почти винаги е комутативна

$\cdot$ — мултипликативни — общия случай

2) R — пръстен; $K < R$ (подпръстен) $\Leftrightarrow K \subseteq R$ и

$\forall k_1, k_2 \in K \quad k_1 - k_2,\ k_1 k_2 \in K$

3) R — поле (тяло); $K < R \Leftrightarrow K \subseteq R$ и $k_1 - k_2,\ k_1 k_2^{-1} \in K \ (k_2 \neq 0)$

Пораждане

— G — гр.; $g \in G \quad \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$

- G - гр. ; $a, b \in G$ $\quad \langle a, b \rangle = \{a^{i_1} b^{j_1} a^{i_2} b^{j_2} \ldots a^{i_n} b^{j_n} \mid i_k, j_k \in \mathbb{Z},\ n \in \mathbb{N} \cup \{0\}\}$ $\ni e$

$\left(\left(a^{i_1} b^{j_1} \ldots a^{i_n} b^{j_n}\right)^{-1} = b^{-j_n} a^{-i_n} \ldots b^{-j_1} a^{-i_1} \right)$

думи в език с азбука $\{a, a^{-1}, b, b^{-1}\}$; $\cdot$ - конкатенация

Зад. V - ЛП ; $X \subseteq V$

$$\ell(X) = \underbrace{\{\text{ЛК на вектори от } X\}}_{\text{е Лподпр.} \to \supseteq} \overset{\subseteq}{=} \bigcap_{X \subseteq U < V} U$$

Опр. A е от тип α и $X \subseteq A$, Множеството

Породено от X е $\langle X \rangle = \bigcap\limits_{X \subseteq B < A} B$ $\quad$ (B е от тип α) - е от тип α също