$|$Curs 7$|$

17.11.2020

Subgrupul generat de o mulțime

Def Fie $(G,\cdot)$ grup și $\emptyset \neq A \subseteq G$. Subgrupul lui G generat de mulțimea A se notează cu $\langle A \rangle$ și reprezintă

$$\langle A \rangle \overset{def}{:=} \{ a_1^{\pm 1} a_2^{\pm 1} \ldots a_n^{\pm 1} \mid a_1, \ldots, a_n \in A,\ n \geq 1 \} \leq G.$$

$\ni 1_G$

Prin definiție $\langle \emptyset \rangle = \{1_G\}$.

Obs 1) $G = \langle G \rangle$

2) Dacă $A = \{a\}$ $\quad \langle \{a\} \rangle \overset{not}{=} \langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$ $\left(1_G = a^0 \right)$; $\langle a \rangle \leftarrow$ s.n. subgrupul ciclic generat de a. ($\overset{not}{\not\!\!\!}\ aG$)

Exemple

1) $G = (\mathbb{Z}, +)$ $\quad \langle n \rangle = n\mathbb{Z} = \{ kn \mid k \in \mathbb{Z} \}$; $\boxed{G = \langle 1 \rangle = 1\mathbb{Z}.}$ (G este grup ciclic)

2) $G = (\mathbb{Z}_{10}, +)$ $\quad \langle \hat{2} \rangle = \hat{2}\mathbb{Z}_{10} = \{ k \cdot \hat{2} \mid k \in \mathbb{Z} \} = \{ \hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8} \}$

$\mathbb{Z}_{10} = \langle \hat{1} \rangle = \langle \hat{3} \rangle = \langle \hat{7} \rangle = \langle \hat{9} \rangle$ $\quad$ ($(\mathbb{Z}_{10}, +)$ este grup ciclic)

3) $G = U(\mathbb{Z}_8, \cdot) = \{ \hat{1}, \hat{3}, \hat{5}, \hat{7} \}$ $\quad \langle \hat{5} \rangle = \{ \hat{1}, \hat{5} \}$ $\quad \langle \hat{3} \rangle = \{ \hat{1}, \hat{3} \}$ $\quad \langle \hat{7} \rangle = \{ \hat{1}, \hat{7} \}$

$\langle \hat{1} \rangle = \{ \hat{1} \}$ $\Rightarrow$ G nu e ciclic

$\langle \{ \hat{3}, \hat{5} \} \rangle \ni \hat{3}, \hat{5}, \hat{3} \cdot \hat{5} = \hat{7}, \hat{3}^2 = \hat{1} \Rightarrow G = \langle \{ \hat{3}, \hat{5} \} \rangle = \langle \{ \hat{3}, \hat{7} \} \rangle = \langle \{ \hat{5}, \hat{7} \} \rangle$

Teoremă Fie G un grup și $A \subseteq G$. Atunci $\langle A \rangle$ este un subgrup al lui G conținut în orice subgrup al lui G care conține pe A. Mai mult,

$$\langle A \rangle = \bigcap_{\substack{H \leq G \\ H \supseteq A}} H$$

($\langle A \rangle$ = intersecția tuturor subgrupurilor lui G care-l conțin pe A)

Cor Fie $(G,\cdot)$ un grup abelian (com) și $A=\{a_1,\dots,a_n\} \subseteq G$. Atunci

$$\langle A \rangle \overset{not}{=} \langle a_1,\dots,a_n \rangle = \{a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} \mid k_1,\dots,k_n \in \mathbb{Z}\}.$$

Exc $8\mathbb{Z} \cap 4\mathbb{Z} = 8\mathbb{Z}$; $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$; $m\mathbb{Z} \cap n\mathbb{Z} = \text{cmmmc}(m,n)\mathbb{Z}$.

Def Spunem că grupul $(G,\cdot)$ este generat de submulțimea A dacă $G=\langle A \rangle$. G s.n. ciclic dacă $(\exists)$ $A \subseteq G$ cu $|A|=1$ a.î. $G=\langle A \rangle$. Grupul s.n. finit generat dacă $(\exists)$ $A \subseteq G$ cu $|A| < \infty$ a.î. $G=\langle A \rangle$.

Obs 1) $(\mathbb{Z},+)$ e ciclic; $(\mathbb{Z}_n,+)$ e ciclic

2) Un grup ciclic e abelian

3) Un grup finit e evident finit generat.

4) Exc! $(\mathbb{Q},+)$ nu este grup finit generat.

$(S_n, \circ) \to$ grup $\quad S_n = \{ f : \{1,2,\dots,n\} \to \{1,2,\dots,n\} \mid f$ bijecție $\}$ $\quad |S_n| = n!$

Dc $\sigma \in S_n$ atunci σ se. mai scrie $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$

$S_3 = \{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \}$

$e \overset{\text{not}}{=} 1_{S_3}$, $\overset{\text{not}}{=} (12)$, $\overset{\text{not}}{=} (13)$, $\overset{\text{not}}{=} (23)$, $\overset{\text{not}}{=} (123)$, $\overset{\text{not}}{=} (132)$

$(12) \circ (13) = \underset{f}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}} \circ \underset{g}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$ (1)

$(f \circ g)(1) = f(g(1)) = f(3) = 3$

$\Rightarrow (S_3, \circ)$ nu e grup comutativ

$(13) \circ (12) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$ (2)

$(12)H = \big($ unde $H = \langle (13) \rangle = \{e, (13)\} \big) = \{ (12) \circ e, (12) \circ (13) \} = \{ (12), (132) \}$

$H(12) = \{ e \circ (12), (13) \circ (12) \} = \{ (12), (123) \}$.

$\neq$

Def Fie $(G, \cdot)$ un grup și $H \leq G$. Pe G definim următoarele rel. binare:

1) "$\equiv_s (\text{mod } H)$": $x \equiv_s y \,(\text{mod } H) \iff x^{-1} y \in H$ ($\equiv_s (\text{mod } H)$ s.n. congruența la stânga modulo H)

2) "$\equiv_d (\text{mod } H)$": $x \equiv_d y \,(\text{mod } H) \iff x y^{-1} \in H$ ($\equiv_d (\text{mod } H)$ s.n. — " — dreapta — " —)

Teoremă Fie $(G,\cdot)$ un grup și $H \leq G$. Atunci cele 2 congruențe modulo H (anterior definite) sunt relații de echivalență pe G. Clasele de echivalență ale $\equiv_s (\mathrm{mod}\, H)$ sunt submulțimile lui G de forma $xH = \{xy \mid y \in H\}$; clasele de echivalență ale $\equiv_d (\mathrm{mod}\, H)$ sunt submulțimile lui G de forma $Hx = \{yx \mid y \in H\}$. Mulțimea factor a lui $\equiv_s (\mathrm{mod}\, H)$ (resp $\equiv_d (\mathrm{mod}\, H)$) se notează cu $(G/H)_s$ (resp. $(G/H)_d$) și $|(G/H)_s| = |(G/H)_d|$. Acest cardinal comun s.n indicele lui H în G și se notează cu $[G:H]$.

Obs 1) $(G/H)_s$ și $(G/H)_d$ pot fi diferite (chiar dacă au același cardinal).
De exemplu pt $G = S_3$, $H = \langle (13) \rangle$

$(G/H)_s = \{(12)H, (13)H, (23)H\}$

$(G/H)_d = $ Exc! $= \{H(12), H(13), H(23)\}$

• $(12)H = \{(12), (132)\}$

•• $(13)H = \{(13), e\} = H$.

∴ $(23)H = \{(23)\circ e, (23)\circ(13)\} = \{(23), (123)\}$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}}_{(23)} \circ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}_{(13)} = \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{(123)}.$$

$$[G:H] = 3 \left(= \frac{6}{2} = \frac{|G|}{|H|} \right)$$

2) Dacă G e abelian atunci $xH = Hx$ $(\forall) x \in G$ și prin urmare $(G/H)_s = (G/H)_d$.

3) Fie $G = S_3$, $H = \langle (123) \rangle = \{ \underset{\substack{\shortparallel \\ (123)\circ(123)\circ(123)}}{e}, (123), \underset{\substack{\shortparallel \\ (123)\circ(123)}}{(132)} \}$. Atunci $(G/H)_s = (G/H)_d$

Def Fie $(G, \cdot)$ un grup și $H \leq G$. Dacă $(G/H)_s = (G/H)_d$ $((\forall)\, x \in G \ \ xH = Hx)$ atunci H s.n. subgrup normal al lui G și se notează cu $H \trianglelefteq G$.

În această situație ($H \trianglelefteq G$) notăm mulțimea $(G/H)_s = (G/H)_d$ cu G/H.

Teorema lui Lagrange Fie G un grup finit și $H \leq G$. Atunci

$$|G| = |H| \cdot [G:H]$$

În particular, $|H|$ divide $|G|$.

Dem "$\equiv_s (\mathrm{mod}\, H)$" rel. de echiv. pe G $\Rightarrow$ $|G| = \sum |C| = |H| \cdot |(G/H)_s|$

$|(G/H)_s| \overset{def}{=} [G:H]$.

C - clasă de echiv. a lui $\equiv_s (\mathrm{mod}\, H)$

$$C = xH \xleftarrow[\text{bij}]{f} H$$
$$xa = f(a) \xleftarrow{f} a$$

$$\boxed{|C| = |H|}$$

Def Fie $(G, \cdot)$ un grup și $x \in G$ un element al său.

$$\mathrm{ord}(x) \overset{def}{=} \begin{cases} \infty, & \text{dacă } x^n \neq 1 \ (\forall)\, n \geq 1. \\ \min\{ n \in \mathbb{N}^* \mid x^n = 1 \} & \text{dacă } (\exists)\, t \geq 1 \text{ a.î. } x^t = 1. \end{cases}$$

ordinul lui x = s.n.

Obs 1) $(G,\cdot)$ grup și $x \in G$ $\mathrm{ord}(x) = n < \infty \Rightarrow |\langle x \rangle| = n$.

2) $(G,\cdot)$ grup finit și $x \in G \Rightarrow \mathrm{ord}(x) < \infty$ și $\mathrm{ord}(x) \mid |G|$ ⟸ (Lagrange)