Exemple

1) $(G,\cdot)$ grup și $g \in G \Rightarrow \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$

Dacă $\operatorname{ord} g = n \Rightarrow \langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$

Pt. proba grea din examen

2) În S_n, $T = \{\tau \in S_n \mid \tau$ este transpoziție$\}$

$\langle T \rangle = S_n$ (pt. că orice permutare e produs de transpoziții)

$D = \{\gamma \in S_n \mid \gamma = (a, b, c)$ ciclu de lungime 3$\}$

$\langle D \rangle = ?$

$\langle D \rangle = A_n = \{\sigma \in S_n \mid \sigma$ permutare pară$\}$

σ - pară $\Leftrightarrow \sigma$ este produsul unui număr par de transpoziții

$\sigma \in A_n \Rightarrow \exists\, \tau_1, \dots, \tau_{2k}$ transpoziții a.î. $\sigma = \tau_1 \cdot \tau_2 \cdot \ldots \cdot \tau_{2k} = (\tau_1 \tau_2)(\tau_3 \tau_4) \ldots (\tau_{2k-1} \ldots$

Dem. că orice produs de 2 transpoziții e un produs de cicluri de lungime 3

$(i, j) \cdot (k, l) = (i, k, j) \cdot (i, k, l)$

$(i, j) \cdot (j, k) = (i, k, j)^2$

$\Rightarrow \forall\, \sigma \in A_n$, σ e un produs de cicluri de lungime 3

$\Rightarrow A_n \subseteq \langle D \rangle$

Dacă $\sigma \in \langle D \rangle \Rightarrow \sigma$ este un produs de permutări pare $\Rightarrow \sigma \in A_n$

$\Rightarrow \langle D \rangle = A_n$

CURS 5 — 27.03.2018

Grupuri ciclice

$(G, \cdot)$ grup

$\emptyset \neq X \subseteq G \Rightarrow \langle X \rangle = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \mid n \in \mathbb{N}^*, \forall\, i = \overline{1,n}, x_i \in X, \varepsilon_i = \pm 1\}$ - subgrupul generat de X

În particular, dacă $X = \{x\} \Rightarrow \langle X \rangle \overset{not}{=} \langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$

Def: Spunem că grupul $(G, \cdot)$ este ciclic, dacă:

$\exists\, x \in G$ a.î. $G = \langle x \rangle$

În aceste condiții, vom spune că x este un generator pentru G.

Exemple:

1) $(\mathbb{Z}, +)$ este ciclic, generat de 1 sau de -1

$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

2) $(\mathbb{Z}_n, +)$ este ciclic, $\mathbb{Z}_n = \langle \hat{1} \rangle$

$\hat{a} \in \mathbb{Z}_n$ cu $(a, n) = 1 \Rightarrow \operatorname{ord} \hat{a} = n \overset{n \cdot \hat{a} = \hat{0}}{\Rightarrow} \langle \hat{a} \rangle = \{k \cdot \hat{a} \mid k \in \mathbb{Z}\} = \{\hat{0}, \hat{a}, 2\hat{a}, \dots, (n-1) \cdot \hat{a}\}$

$\operatorname{ord} \hat{a} = n \Rightarrow \forall\, i < j$ cu $i, j \in \{0, \dots, n-1\}$, $i \cdot \hat{a} \neq j \cdot \hat{a}$

$\Rightarrow |\langle \hat{a} \rangle| = n \Rightarrow \langle \hat{a} \rangle = \mathbb{Z}_n$

$n = 9$, $\hat{0} = \hat{9}$

$\langle \hat{2} \rangle = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{1}, \hat{3}, \hat{5}, \hat{7}\} = \mathbb{Z}_9$ ($5 \cdot \hat{2}$, $6 \cdot \hat{2}$, $7 \cdot \hat{2}$, $8 \cdot \hat{2}$)

3) Dacă p - prim impar, atunci $(U(\mathbb{Z}_p), \cdot)$ grup ciclic.

($\hat{a}$ - generator pentru $U(\mathbb{Z}_p) \Rightarrow$ spunem că a este o rădăcină primitivă modulo p)

4) $(U(\mathbb{Z}_8),\cdot)$ nu e ciclic

$U(\mathbb{Z}_8)=\{\hat{1},\hat{3},\hat{5},\hat{7}\}$, $\forall \hat{x}\in U(\mathbb{Z}_8)$, $x^2=1 \Rightarrow$

$\Rightarrow \forall \hat{x}\in U(\mathbb{Z}_8)$, $|\langle x\rangle| \in \{1,2\} \Rightarrow \langle \hat{x}\rangle \neq U(\mathbb{Z}_8)$

5) Grupul lui Klein nu e ciclic.

6) $(\mathbb{Q},+)$ nu e ciclic

Pp. că $\exists \frac{a}{b}\in\mathbb{Q}$, $a,b\in\mathbb{Z}$, $b>0$ a.î $\mathbb{Q}=\langle \frac{a}{b}\rangle$

$\Rightarrow \mathbb{Q}=\{\frac{ka}{b} \mid k\in\mathbb{Z}\}$

$\frac{a}{2b}\in\mathbb{Q} \Rightarrow \exists k\in\mathbb{Z}$ a.î $\frac{a}{2b}=\frac{ka}{b} \Rightarrow a=0 \Rightarrow \mathbb{Q}=\langle 0\rangle=\{0\}$ contradicție

$\forall \underset{n\geq 2}{n\in\mathbb{N}^*}$, $U_n=\{z\in\mathbb{C} \mid z^n=1\} \leq (\mathbb{C}^*,\cdot)$

$z^n=1 \Rightarrow z=z_k=\cos\frac{2k\pi}{n}+i\cdot\sin\frac{2k\pi}{n}$, $k=\overline{0,n-1}$

$\Rightarrow \forall z\in U_n$, $\exists k=\overline{0,n-1}$ a.î $z=z_1^k$ | $[r(\cos\alpha+i\sin\alpha)]^m=r^m(\cos m\alpha+i\sin m\alpha)$

Propoziție

Fie $G=\langle x\rangle$ un grup ciclic.

a) $|G|=n<\infty \iff \operatorname{ord} x=n$. În aceste condiții, $G=\{1,x,x^2,\dots,x^{n-1}\}$

b) G este infinit $\iff \operatorname{ord} x=\infty$.

În aceste condiții $G=\{x^k \mid k\in\mathbb{Z}\}$ și dacă $l\neq k \Rightarrow x^l\neq x^k$

Dem:

a) „$\Leftarrow$" Pp. că $\operatorname{ord}(x)=n<\infty \Rightarrow \langle x\rangle=\{1,x,x^2,\dots,x^{n-1}\}$ } $\Rightarrow |G|<n \Rightarrow$

Pp. că $|G|\neq n$, $G=\langle x\rangle$

$\Rightarrow \exists i,j\in\{0,\dots,n-1\}$ a.î $i<j$ și $x^i=x^j \Rightarrow x^{j-i}=1 \Rightarrow \operatorname{ord}(x)\leq j-i\leq n-1<n$ contradicție

„$\Rightarrow$" Pp. că $\operatorname{ord}(x)\neq n$

Din „$\Leftarrow$" $\Rightarrow |G|=|\langle x\rangle|\neq n$ contradicție

b) temă

Teoremă

Orice două grupuri ciclice de același cardinal sunt izomorfe.

Dem:

Vom demonstra că dacă $G=\langle x\rangle$ este ciclic $\Rightarrow G\simeq \begin{cases}(\mathbb{Z},+) & \text{, dacă } G \text{ este infinit}\\ (\mathbb{Z}_n,+) & \text{, dacă } |G|=n\end{cases}$

• Caz 1 : G - infinit $\Rightarrow G=\{x^k \mid k\in\mathbb{Z}\}$

$f:\mathbb{Z}\to G$, $f(k)=x^k \Rightarrow f(\mathbb{Z})=G \Rightarrow f$ surjectivă (1)

Fie $l,k\in\mathbb{Z}$ a.î $f(l)=f(k) \Rightarrow x^l=x^k \Rightarrow l=k \Rightarrow f$ injectivă (2)

$f(l+k)=x^{l+k}=x^l\cdot x^k=f(l)\cdot f(k)$, $\forall l,k\in\mathbb{Z} \Rightarrow f$ morfism (3)

Din (1)(2)(3) $\Rightarrow f$ izomorfism . Deci, $G\simeq(\mathbb{Z},+)$

• Caz 2 : $|G|=n \Rightarrow G=\{1,x,x^2,\dots,x^{n-1}\}$, $\operatorname{ord}(x)=n$

$f:\mathbb{Z}_n\to G$, $f(\hat{k})=x^k$

Dem. că f e bine definită : $\hat{k}=\hat{l} \overset{?}{\Longrightarrow} f(\hat{k})=f(\hat{l})$

$\hat{k}=\hat{l} \Rightarrow n\mid k-l \Rightarrow x^{k-l}=1 \Rightarrow x^k=x^l \Rightarrow f(\hat{k})=f(\hat{l})$

$\Rightarrow f$ e bine definită

f surjectivă - evident

Pp. $f(\hat{k})=f(\hat{l}) \Rightarrow x^k=x^l \Rightarrow x^{k-l}=1 \overset{\operatorname{ord}x=n}{\Longrightarrow} n\mid k-l \Rightarrow \hat{k}=\hat{l}$

$\Rightarrow f$ injectivă

f morfism - temă

$\Rightarrow f$ izomorfism $\Rightarrow G\simeq(\mathbb{Z}_n,+)$

Teoremă (subgrupurile unui grup ciclic)
Fie $(G,\cdot)$ un grup ciclic, $G=\langle x\rangle$ și $H\leq G$

a) $H\leq G \Leftrightarrow \exists\, d\in\mathbb{N}$ a.î. $H=\langle x^d\rangle$

b) Dacă G este infinit $\Rightarrow \forall\, d,e\in\mathbb{N}$ cu $d\neq e$ avem $\langle x^d\rangle \neq \langle x^e\rangle$

c) Dacă $|G|=n$ atunci $H\leq G \Leftrightarrow \exists\, d\in\mathbb{N}$ cu $d\mid n$ a.î. $H=\langle x^d\rangle$

În acest caz, dacă $d,e\mid n$ cu $d\neq e$, atunci $\langle x^d\rangle \neq \langle x^e\rangle$

Dem:

a) „$\Rightarrow$"

Caz 1: $H=\{1\} \Rightarrow H=\langle x^0\rangle$

Caz 2: $H\neq\{1\} \Rightarrow \exists\, h\in H, h\neq 1$; $G=\{x^k \mid k\in\mathbb{Z}\}$ $\Rightarrow \exists\, k\in\mathbb{Z}^*$ a.î. $h=x^k$, $H\leq G$ $\Rightarrow h^{-1}=x^{-k}\in H$

$\Rightarrow \exists\, k\in\mathbb{Z}^*$ a.î. $x^k, x^{-k}\in H \Rightarrow$

$\Rightarrow \exists\, k\in\mathbb{N}^*$ a.î. $x^k\in H$

Fie $d\in\mathbb{N}^*$ cel mai mic a.î. $x^d\in H$

$x^d\in H \Rightarrow \langle x^d\rangle \leq H$

Demonstrăm că $H\leq\langle x^d\rangle=\{(x^d)^l \mid l\in\mathbb{Z}\}=\{x^{dl}\mid l\in\mathbb{Z}\}$

Fie $y\in H \Rightarrow y\in G \Rightarrow \exists\, n\in\mathbb{Z}$ a.î. $y=x^n$

Din teorema împărțirii cu rest $\rightsquigarrow \exists\, q,r\in\mathbb{Z}$ a.î. $n=dq+r$ și $0\leq r<d$

$\Rightarrow y=x^{dq}\cdot x^r \Rightarrow x^r=(x^{dq})^{-1}\cdot y$; $y\in H$, $x^{dq}\in H$ $\Rightarrow x^r\in H$, $r<d$ $\Rightarrow r\notin\mathbb{N}^* \Rightarrow r=0 \Rightarrow d\mid n \Rightarrow y\in\langle x^d\rangle$

$\Rightarrow H\leq\langle x^d\rangle$

$\Rightarrow H=\langle x^d\rangle$

„$\Leftarrow$" $H=\langle x^d\rangle \Rightarrow H\leq G$

b), c) → temă (facultativ)

Exemple

1) (Subgrupurile lui $\mathbb{Z}$)

$H\leq\mathbb{Z}$, $H\leq G \Leftrightarrow \exists\, d\in\mathbb{N}$ a.î. $H=\langle d\cdot 1\rangle=\langle d\rangle=d\cdot\mathbb{Z}$

2) (Subgrupurile lui $\mathbb{Z}_n$)

$H\leq\mathbb{Z}_n$, $H\leq\mathbb{Z}_n \Leftrightarrow \exists\, d\mid n$ a.î. $H=\langle d\cdot\hat{1}\rangle=\langle\hat{d}\rangle=d\cdot\mathbb{Z}_n$

3) Subgrupurile lui $\mathbb{Z}_{12}$

$d\mid 12 \Leftrightarrow d\in\{1,2,3,4,6,12\}$

$d=1$: $1\cdot\mathbb{Z}_{12}=\mathbb{Z}_{12}$

$d=2$: $2\cdot\mathbb{Z}_{12}=\{\hat{0},\hat{2},\hat{4},\hat{6},\hat{8},\hat{10}\}$

$d=3$: $3\cdot\mathbb{Z}_{12}=\{\hat{0},\hat{3},\hat{6},\hat{9}\}$

$d=4$: $4\cdot\mathbb{Z}_{12}=\{\hat{0},\hat{4},\hat{8}\}$

$d=6$: $6\cdot\mathbb{Z}_{12}=\{\hat{0},\hat{6}\}$

Relații de echivalență induse de un subgrup

$x, y \in \mathbb{Z}_n \Leftrightarrow n \mid y - x \Leftrightarrow y - x \in n\mathbb{Z}$ x

Def: Fie $(G, \cdot)$ grup și $H \leq G$. Pe G definim relațiile:

a) $x \rho_H y \Leftrightarrow x^{-1} \cdot y \in H$

b) $x \rho'_H y \Leftrightarrow y \cdot x^{-1} \in H$

Propoziție

Relațiile ρ_H și ρ'_H sunt relații de echivalență pe G

Dem:

Pt. ρ_H

- reflexivă: $\forall x \in G, x \rho_H x$

Fie $x \in G, x^{-1} \cdot x = 1 \in H \Rightarrow x \rho_H x \ ; \forall x \in G$

$\Rightarrow \rho_H$ este reflexivă

- tranzitivă

Fie $x, y, z \in G$ cu $x \rho_H y$ și $y \rho_H z \Rightarrow$

$\Rightarrow x^{-1} y \in H, y^{-1} z \in H \Rightarrow (x^{-1} y)(y^{-1} z) \in H \Rightarrow x^{-1} z \in H \Rightarrow x \rho_H z$

- simetrică

Fie $x, y \in G$ cu $x \rho_H y \Rightarrow x^{-1} \cdot y \in H \Rightarrow (x^{-1} \cdot y)^{-1} \in H \Rightarrow y^{-1} x \in H \Rightarrow y \rho_H x$

$H \leq G$

Def: ρ_H s.n. relație de echivalență la stânga indusă de H

ρ'_H s.n. relație de echivalență la dreapta indusă de H.

Obs: $\rho_H(x) = \{y \in G \mid x \rho_H y\} = \{y \in G \mid x^{-1} y \in H\} = x \cdot H = \{x \cdot h \mid h \in H\}$

$\rho'_H(x) = H \cdot x$

$G/\rho_H = \{xH \mid x \in G\}$; $xH = yH \Leftrightarrow x^{-1} y \in H$

$G/\rho'_H = \{Hx \mid x \in G\}$; $Hx = Hy \Leftrightarrow yx^{-1} \in H$

Exemplu:

$G = D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$H = \{1, s\}$

$rH = \{s, sr^3\}$, $Hr = \{r, sr\}$

$G/\rho_H = \{\underbrace{\{1, s\}}_{1 \cdot H}, \underbrace{\{r, sr^3\}}_{r \cdot H}, \underbrace{\{r^2, sr^2\}}_{r^2 \cdot H}, \underbrace{\{r^3, sr\}}_{r^3 \cdot H}\}$

Teoremă

Fie $(G, \cdot)$ grup și $H \leq G$.

a) $|G/\rho_H| = |G/\rho'_H| \overset{not}{=} |G : H|$

Dacă G este finit $\Rightarrow |G| = |H| \cdot |G : H|$

Dem:

a) $F: G/\rho_H \longrightarrow G/\rho'_H$, $F(xH) = H \cdot x^{-1}$

bine că F e bine definită

$xH = yH \Rightarrow y = y \cdot 1 \in xH \Rightarrow \exists h \in H$ a.i. $y = xh$

$\Rightarrow H \cdot y^{-1} = H \cdot (xh)^{-1} = H \cdot h x^{-1}$
H parte stabilă $\Rightarrow Hh \subseteq H$ $\Rightarrow H \cdot y^{-1} \subseteq H \cdot x^{-1}$

Analog: $H \cdot x^{-1} \subseteq H \cdot y^{-1}$

$\Rightarrow F(xH) = F(yH)$

$\Rightarrow F$ este bine definită

Fie $F' : G/\rho'_H \longrightarrow G/\rho_H$, $F'(Hx) = x^{-1} \cdot H$

Analog, se arată că F' este bine definită

Prin calcul avem $F \circ F' = 1_{G/\rho'_H}$ și $F' \circ F = 1_{G/\rho_H}$

$\Rightarrow F$ bijectivă $\Rightarrow |G/\rho_H| = |G/\rho'_H|$

b) G-finit $\rightarrow G/\rho_H = \{x_1H, x_2H, \dots, x_kH\}$ - o mulțime cu k elemente

unde $k = |G:H|$

Fie $\varphi : H \longrightarrow xH$ funcția definită prin $\varphi(h) = xh$

$\varphi(h_1) = \varphi(h_2) \overset{x^{-1}}{\Rightarrow} xh_1 = xh_2 \Rightarrow h_1 = h_2$

$\Rightarrow \varphi$ injectivă
φ-surjectivă (evident) $\Rightarrow \varphi$ bijectivă

$\Rightarrow \forall x \in G, |H| = |xH|$

$\Rightarrow |x_1H| = |x_2H| = \dots = |x_kH| = |H|$

G/ρ_H este o partiție pt. $G \Rightarrow |G| = |x_1H| + |x_2H| + \dots + |x_kH| = k \cdot |H| = |G:H| \cdot |H|$

Def: Numărul $|G:H|$ s.n. indicele lui H în G

(Corolar (T. lui Lagrange))

Dacă G - grup finit și $x \in G \Rightarrow \operatorname{ord} x \mid |G|$

Dem:

$\operatorname{ord} x = |\langle x \rangle|$
$|G| = |\langle x \rangle| \cdot |G : \langle x \rangle|$
$\Rightarrow \operatorname{ord} x \mid |G|$