5.12.2021

Tutoriat 7

Ordinul unui element. Grupuri ciclice. Indicatorul lui Euler

<u>Reamintire</u>: Dacă G este un grup finit, atunci ordinul lui G (notat $|G|$) este numărul de elemente al grupului.

<u>Ordinul unui element</u>

Fie G grup, $g \in G$. Definim ORDINUL LUI g ÎN G astfel:

a) G grup multiplicativ: $ord(g)$ = cel mai mic număr $\underline{n}$ pentru care $\boxed{g^n = 1}$

b) G grup aditiv: $o(g)$ = ——"—— pt. care $\underline{ng = 0}$

Practic: $g \in G$. $\underbrace{g \cdot g \cdot \ldots \cdot g}_{n} = 1$. Cât este n, atât e ordinul lui g in G

$\underbrace{g + g + \ldots + g}_{n} = 0$

<u>Propoziție-Definiție</u>

- g are <u>ordin finit</u> dacă:
  $\exists n \in \mathbb{Z}^*$ a.î. $g^n = 1$ (sau $ng = 0$)
- g are <u>ordin infinit</u> (adică $o(g) = \infty$) dacă
  $g^n = 1 \Leftrightarrow n = 0$ ($ng = 0 \Leftrightarrow n = 0$)

<u>Observații</u>

1) G grup, $g \in G$, $o(g) = n \geq 1$.
Atunci, pt. $m \in \mathbb{N}$ a.î. $g^m = 1 \Rightarrow n \mid m$

<u>Ex</u>: $(\mathbb{Z}_5, \cdot)$ $o(\hat{4}) = 2$ $\quad 2 \mid 20$

$\hat{4} \cdot \hat{4} = \hat{16} = \hat{1}$

$\hat{4}^{20} = \hat{1}$ $\quad \left(\hat{4}^{20} = (\hat{4}^2)^{10} = \hat{1}^{10} = \hat{1} \right)$

2) G grup, $g \in G$. Atunci
$o(g) = |\langle g \rangle|$ (cardinalul / ordinul subgrupului generat de g)

<u>Propoziție</u> G finit, $g \in G$. Atunci:

- $o(g) \mid |G|$
- $g^{|G|} = 1$

<u>Indicatorul lui Euler</u>: $\varphi(m)$

$\varphi(m) \stackrel{def}{:=}$ numărul întregi $1 \le k \le m$ primi cu m

$\varphi(m) = |\{a \in \{1, 2, \ldots, m-1\} \mid (m, a) = 1\}|$

Ciurmă
$(\mathbb{Z}_6, \cdot)$
$\mathbb{Z}_6 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$
$U(\mathbb{Z}_6) = \{\hat{1}, \hat{5}\}$
$(1, 6) = 1 = (5, 6)$

<u>Precizare</u>: $U(\mathbb{Z}_m) = \{\hat{b} \in \mathbb{Z}_m \mid (m, b) = 1\}$
$\varphi(m) = |U(\mathbb{Z}_m)|$

<u>Teorema lui Euler</u>: Fie $a, m \in \mathbb{N}^*$, $(a, m) = 1$. Atunci
$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

<u>Mica teoremă a lui Fermat</u>
$$a^{p-1} \equiv 1 \pmod{p}$$, unde $p \in \mathbb{N}^*$ prim, $a \in \mathbb{N}^*$, $p \nmid a$

<u>Observații</u>: $g \in G$, $o(g) = m \geq 1$, $k \in \mathbb{N}^*$

1) $o(g^k) = \dfrac{m}{(m, k)}$ $\quad \left(o(k \cdot g) = \dfrac{m}{(m, k)} \right)$

2) g^k generator pt $\langle g \rangle \Leftrightarrow (m, k) = 1$

3) Nr. generatori în $(\mathbb{Z}_m, +)$ este $\varphi(m)$

<u>Ex 3)</u>: $(\mathbb{Z}_8, +)$
Generatorii: $\hat{1}, \hat{3}, \hat{5}, \hat{7}$ $\quad \left(\varphi(8) = |\{\hat{b} \in \mathbb{Z}_8 \mid (8, b) = 1\}| = |\{1, 3, 5, 7\}| \right)$

Grupuri ciclice

Grup ciclic : grup generat de un singur element.

Teorema de structură a grupurilor ciclice

G grup ciclic, atunci

a) $G \simeq (\mathbb{Z}, +)$, G infinit

b) $G \simeq (\mathbb{Z}_n, +)$, G finit. $|G| = n$

Lema chineză a resturilor

Fie $m, n \in \mathbb{N}^*$, $(m,n)=1$. Atunci

$$\varphi : \mathbb{Z}_{mn} \xrightarrow{\sim} \mathbb{Z}_m \times \mathbb{Z}_n, \quad \varphi(\underset{\mathbb{Z}_{mn}}{\hat{x}}) = (\underset{\mathbb{Z}_m}{\bar{x}}, \underset{\mathbb{Z}_n}{\bar{\bar{x}}}) \quad \text{izo.}$$

$$\left(\underset{\mathbb{Z}_6}{\hat{0}} \neq \hat{0} \in \mathbb{Z}_5 \right)$$

Sfaturi pentru a arăta că două grupuri (nu) sunt izomorfe:

- TFI / PUGF (vezi Tutorial 6)
- Sunt grupuri
  - comutative ambele ?? ($|G| = 6 \Rightarrow G \simeq \mathbb{Z}_6$, G comutativ; $G \simeq S_3$ (grup de permutări) G necomutat.)
  - ciclice
  - ordinele elementelor se păstrează

Exercitii

1) **Exercitiul 3:** Fie $\underbrace{G = \mathbb{Z}_2 \times \mathbb{Z}_4}_{}$ $(G,+)$ produsul direct al grupurilor ciclice $(\mathbb{Z}_2, +)$ si $(\mathbb{Z}_4, +)$.

(a) Calculaţi ordinele elementelor grupului G. (0,5 puncte)

(b) Arătaţi că grupul G nu este izomorf cu grupul $(\mathbb{Z}_8, +)$ si nici cu produsul direct de grupuri $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. (1 punct)

(c) Fie $H = \{(\hat{0}, \bar{0}), (\hat{0}, \bar{2})\}$. Arătaţi că H este subgrup normal in G si exista un izomorfism de grupuri $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. (1 punct)

Sol a) $|G| = 8 \Rightarrow \forall g \in G,\ o(g) \mid 8 \Rightarrow o(g) \in \{1, 2, 4, 8\}$

$G = \{(\hat{0},\bar{0}), (\hat{0},\bar{1}), (\hat{0},\bar{2}), (\hat{0},\bar{3}), (\hat{1},\bar{0}), (\hat{1},\bar{1}), (\hat{1},\bar{2}), (\hat{1},\bar{3})\}$

$\hat{x} \in \mathbb{Z}_2$

$\bar{y} \in \mathbb{Z}_4$

$(\hat{x},\bar{y}) + (\hat{x},\bar{y}) = (\hat{0},\bar{0})$

Elem. neutru al. lui G: $(\hat{0},\bar{0})$

Elem. de ordin

1: $(\hat{0},\bar{0})$

2: $(\hat{1},\bar{2}), (\hat{0},\bar{2}), (\hat{1},\bar{0})$

4: $(\hat{0},\bar{1}), (\hat{0},\bar{3}), (\hat{1},\bar{1}), (\hat{1},\bar{3})$

$4(\hat{x},\bar{y}) = (\hat{0},\bar{0})$

Varianta fără a scrie elem. lui G

$\mathbb{Z}_2$, $\hat{x}$: ordin 1: $\hat{0}$; ordin 2: $\hat{1}$

$\mathbb{Z}_4$, $\bar{y}$: ordin 1: $\hat{0}$; ordin 2: $\hat{2}$; ordin 4: $\hat{1}, \hat{3}$

combinaţii naturale ($o(\hat{x},\bar{y}) = [o(\hat{x}), o(\bar{y})]$)

b) $\cdot\ \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_4}_{G} \not\cong \mathbb{Z}_8$

ordine 1, 2, 4 | ordine posibile 1, 2, 4, 8

$o(g) = 1 \Rightarrow g = \bar{\bar{0}}$

$o(g) = 2 \Rightarrow g = \bar{\bar{4}}$

$o(g) = 4 \Rightarrow g \in \{\bar{\bar{2}}, \bar{\bar{6}}\}$

$o(g) = 8 \Rightarrow g \in U(\mathbb{Z}_8) = \{\bar{\bar{1}}, \bar{\bar{3}}, \bar{\bar{5}}, \bar{\bar{7}}\}$

Cum Z_8 are și elemente de ordin 8 (precum 1, 3, 5, 7), iar grupul G are elemente de ordin maxim 4, atunci grupurile G și Z_8 nu sunt izomorfe.

$\cdot\ \mathbb{Z}_2 \times \mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

ordinul maxim in $\mathbb{Z}_2 \times \mathbb{Z}_4 = 4$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\hat{0},\hat{0},\hat{0}), (\hat{0},\hat{0},\hat{1}), (0,1,0), (1,0,0), (0,1,1), (1,0,1), (1,1,0), (1,1,1)\}$

$\hat{x} \in \mathbb{Z}_2$

ordin maxim = 2

$\Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

c) (c) Fie $H = \{(\hat{0},\bar{0}), (\hat{0},\bar{2})\}$. Arătaţi că H este subgrup normal in G si există un izomorfism de grupuri $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. (1 punct)

$H \leq G$: $\left.\begin{array}{l} (\hat{0},\bar{0})-(\hat{0},\bar{0}) \in H \\ (\hat{0},\bar{2})-(\hat{0},\bar{0}) \in H \\ (\hat{0},\bar{0})-(\hat{0},\bar{2}) \in H \\ (\hat{0},\bar{0}) \in H \end{array}\right\} \Rightarrow H \leq G$

$H \trianglelefteq G$: H subgrup normal în $G \iff \forall x \in G, \forall h \in H$, $xhx^{-1} \in H$ $(x+h+x^{-1} \in H)$ Teorie

Obs: G grup comutativ $\Rightarrow$ oricare subgrup e normal

Calcul: Fie $(\hat{x},\bar{y}) \in \mathbb{Z}_2 \times \mathbb{Z}_8$

$(\hat{x},\bar{y}) + (\hat{0},\bar{2}) + (-\hat{x},-\bar{y}) \overset{G \text{ comut.}}{=} \underbrace{(\hat{x},\bar{y}) + (-\hat{x},-\bar{y})}_{(\hat{0},\bar{0})} + (\hat{0},\bar{2}) \in H$

Deci $H \trianglelefteq G$

Vrem: $\mathbb{Z}_2 \times \mathbb{Z}_4 / H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ (sumă a TFI)

Caut $f : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ surj, $\operatorname{Ker} f = \{(\hat{x},\bar{y}) \mid f((\hat{x},\bar{y})) = (\hat{0},\hat{0})\} = H$

$f((\hat{x},\bar{y})) = (\hat{x},\hat{y})$ surj.

$f((\hat{1},\bar{3})) = (\hat{1},\hat{3}) = (\hat{1},\hat{1})$

Ker f = ?

$f((\hat{x},\bar{y})) = (\hat{0},\hat{0}) \iff (\hat{x},\hat{y}) = (\hat{0},\hat{0})$

$\iff \begin{cases} x - 0 \ \vdots\ 2 \\ y - 0 \ \vdots\ 2 \end{cases} \iff \begin{cases} x = 2t \\ y = 2s \end{cases} \Rightarrow \begin{array}{l} \hat{x} = \hat{0} \\ y \in \{0,2,4,\dots\} \end{array}$

$\iff \operatorname{Ker} f = \{(\hat{0},\bar{0}), (\hat{0},\bar{2})\} = H$

$\overset{\text{TFI}}{\Longrightarrow} \exists \bar{f} : G/H \xrightarrow{\sim} \mathbb{Z}_2 \times \mathbb{Z}_2$, $\bar{f}(\overline{(\hat{x},\bar{y})}) = f((\hat{x},\bar{y}))$ izo

---

Ex. Bonus: $\mathbb{Z}_4 \not\simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2}_{\text{grupul lui Klein}}$

Sol: $\hat{1} \in \mathbb{Z}_4$, $o(\hat{1}) = 4$

Nu există $x \in \mathbb{Z}_2 \times \mathbb{Z}_2$ a.î. $o(x) = 4$ $\Rightarrow \mathbb{Z}_4 \not\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

$\boxed{\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3}$ (Lema chineză)

Problema 2. Se consideră grupul (aditiv) $G = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$.

(1) Aflați ordinele elementelor $(\widehat{4}, \overline{3})$, respectiv $(\widehat{3}, \overline{5})$. (5 pct.)

(2) Este adevărat că $(\widehat{4}, \overline{3}) \in \langle(\widehat{3}, \overline{5})\rangle$? Dar că $(\widehat{3}, \overline{5}) \in \langle(\widehat{4}, \overline{3})\rangle$? Justificați. (5 pct.)

(3) Formează $\{(\widehat{4}, \overline{3}), (\widehat{3}, \overline{5})\}$ un sistem de generatori pentru G? Justificați. (5 pct.)

(4) Este G grup ciclic? Justificați. (5 pct.)

(5) Este $G/\langle(\widehat{4}, \overline{3})\rangle$ grup ciclic? Justificați. (10 pct.)

Sol a) $G = \mathbb{Z}_9 \times \mathbb{Z}_{18}$

$m(\widehat{4}, \overline{3}) = (\widehat{0}, \overline{0})$

$o(\widehat{4}) = \frac{|\mathbb{Z}_9|}{(|\mathbb{Z}_9|, 4)} = \frac{9}{(9,4)} = 9$ în $\mathbb{Z}_9$

$o(\overline{3}) = \frac{18}{(18,3)} = \frac{18}{3} = 6$ $\mathbb{Z}_{18}$

Putem lua $m = [9, 6] = 18$

Deci $o((\widehat{4}, \overline{3})) = 18$ în G

$m(\widehat{3}, \overline{5}) = (\widehat{0}, \overline{0})$ $o(\widehat{3}) = 3$ în $\mathbb{Z}_9$ $o(\overline{5}) = \frac{18}{(18,5)} = \frac{18}{1} = 18$ în $\mathbb{Z}_{18}$

Luând $m = [3, 18] = 18 \Rightarrow o((\widehat{3}, \overline{5})) = 18$

b) $(\widehat{4}, \overline{3}) \overset{?}{\in} \langle(\widehat{3}, \overline{5})\rangle = \{m(\widehat{3}, \overline{5}) \mid m \in \mathbb{Z}\}$

Pp. $(\widehat{4}, \overline{3}) \in \langle(\widehat{3}, \overline{5})\rangle \Leftrightarrow \exists m$ a.î. $(\widehat{4}, \overline{3}) = (\widehat{3}m, \overline{5}m)$

presupun

$\Leftrightarrow \begin{cases} \widehat{3}m = \widehat{4} & \text{în } \mathbb{Z}_9 \\ \overline{5}m = \overline{3} & \text{în } \mathbb{Z}_{18} \end{cases}$

Cum $\nexists m$ a.î. $\widehat{3}m = \widehat{4}$ în $\mathbb{Z}_9 \Rightarrow (\widehat{4}, \overline{3}) \notin \langle(\widehat{3}, \overline{5})\rangle$ (calculați, luați m cum doriți)

Similar, $(\widehat{3}, \overline{5}) \notin \langle(\widehat{4}, \overline{3})\rangle$

c) Formează $\{(\widehat{4}, \overline{3}), (\widehat{3}, \overline{5})\}$ un sistem de generatori pentru G? Justificați.

Sist. de gen: $X \subseteq G$ sist. de gen. $\Leftrightarrow \langle X\rangle = \{m_1x_1 + m_2x_2 + \dots + m_mx_m \mid m_i \in \mathbb{Z}, x_i \in X\} = G$

Pp. $\{(\widehat{4}, \overline{3}), (\widehat{3}, \overline{5})\}$ sist de gen $\Leftrightarrow \forall (\widehat{x}, \overline{y}) \in G$,

$(\widehat{x}, \overline{y}) = n(\widehat{4}, \overline{3}) + m(\widehat{3}, \overline{5})$, $n, m \in \mathbb{Z}$

Vom reveni cu detalii sâmbătă $\rightsquigarrow$ $\begin{cases} \widehat{x} = \widehat{4}n + \widehat{3}m \\ \overline{y} = \overline{3}n + \overline{5}m \end{cases}$ avem un sistem de ecuații în $\mathbb{Z}_{18}$ în m și n

$\begin{vmatrix} 4 & 3 \\ 3 & 5 \end{vmatrix} = 11$ (în $\mathbb{Z}_{18}$) $\in U(\mathbb{Z}_{18})$

$11^{-1} = 5$ (verificați)

$\Rightarrow n = \frac{\begin{vmatrix} x & 3 \\ y & 5 \end{vmatrix}}{11} = 5(5x - 3y) = 25x - 15y \overset{18}{=} 7x + 3y$

$m = \frac{\begin{vmatrix} 4 & x \\ 3 & y \end{vmatrix}}{11} = 5(4y - 3x) \overset{18}{=} 2y + 3x$

Cum avem soluții, $\langle(\widehat{4}, \overline{3}), (\widehat{3}, \overline{5})\rangle = G$

d) $\mathbb{Z}_9 \times \mathbb{Z}_{18}$ nu e ciclic

Avem $(9,18) = 9 < 9 \cdot 18 = |\mathbb{Z}_9 \times \mathbb{Z}_{18}|$

Fie $(\hat{a}, \bar{b}) \in \mathbb{Z}_9 \times \mathbb{Z}_{18}$. Atunci

$$k(\hat{a}, \bar{b}) = (k\hat{a}, k\bar{b})$$

De asemenea,

$$\left(\frac{9 \cdot 18}{9}\hat{a}, \frac{9 \cdot 18}{9}\bar{b}\right) = (\hat{0}, \bar{0})$$

Deci $\langle(\hat{a}, \bar{b})\rangle$ are ordin cel mult egal cu $\frac{9 \cdot 18}{9} < 9 \cdot 18$, așa că $\mathbb{Z}_9 \times \mathbb{Z}_{18}$ nu e ciclic

e) Știm de la punctul c) că $\langle(\hat{4}, \bar{3}), (\hat{3}, \bar{5})\rangle = G$

$$G/\langle(\hat{4}, \bar{3})\rangle = \frac{\langle(\hat{4}, \bar{3}), (\hat{3}, \bar{5})\rangle}{\langle(\hat{4}, \bar{3})\rangle} \underline{\underline{(\hat{4}, \bar{3}) \notin \langle(\hat{3}, \bar{5})\rangle}} \langle(\hat{3}, \bar{5})\rangle$$, deci este ciclic

Cum $\left.\begin{array}{l} o(\hat{3}, \bar{5}) = 18 \\ G/\langle(\hat{4}, \bar{3})\rangle \text{ finit} \end{array}\right| \Rightarrow G/\langle(\hat{4}, \bar{3})\rangle \simeq \mathbb{Z}_{18}$