Seminar 9 - 06.12.2021

Ex. 1: Elementele inversabile ale monoidului $(\mathbb{Z}_n, \cdot)$ sunt $\mathcal{U}(\mathbb{Z}_n) = \{ \hat{a} \in \mathbb{Z}_n \mid \underset{\text{cmmdc}}{(a,n)} = 1 \}$

Teoremă: Fie $a, b \in \mathbb{N}$, $d = (a,b)$. Atunci există $m, n \in \mathbb{Z}$ a.î. $a \cdot m + b \cdot n = d$. ($m, n$ se det. cu ajutorul Alg. lui Euclid).

Rez:

„$\supseteq$" $(a,n) = 1 \xrightarrow{TR} \exists\, k, l \in \mathbb{Z}$ a.î. $ak + nl = 1$.

În $\mathbb{Z}_n$: $\widehat{ak} + \underbrace{\widehat{nl}}_{=\hat{0}} = \hat{1} \Rightarrow \hat{a} \cdot \hat{k} = \hat{1} \Rightarrow \hat{a} \in \mathcal{U}(\mathbb{Z}_n)$

$(\hat{a}^{-1} = \hat{k})$

$\mathcal{U}(\mathbb{Z}_n)$ = mulțimea elementelor inversabile din $\mathbb{Z}_n$ (unități)

„$\subseteq$" Fie $\hat{a} \in \mathcal{U}(\mathbb{Z}_n)$. Vrem să arătăm că $(a,n) = 1$.

Pp. că $(a,n) = d > 1 \Rightarrow a = d \cdot a_1$, $n = d \cdot n_1$, $(a_1, n_1) = 1$.

$\hat a \in U(\mathbb{Z}_m) \Rightarrow \exists\ \hat b \in \mathbb{Z}_m$ a.î. $\hat a \cdot \hat b = \hat 1$

$$\hat d \cdot \hat a_1 \cdot \hat b = \hat 1 \quad \Big| \cdot \hat m_1$$

$$\underbrace{\hat m_1 \cdot \hat d}_{\hat m = \hat 0} \cdot \hat a_1 \cdot \hat b = \hat m_1 \Rightarrow \left.\begin{array}{l} \hat m_1 = \hat 0 \Rightarrow m \mid m_1 \\ \text{Dar } m = d \cdot m_1 \\ \quad 0 < m_1 < m \end{array}\right\} \text{abs.}$$

$\Rightarrow$ Pp. făcută este falsă $\Rightarrow (a, m) = 1$.

Exemplu: $U(\mathbb{Z}_{12}) = \{ \hat a \in \mathbb{Z}_{12} \mid (a, 12) = 1 \}$
$= \{ \hat 1, \hat 5, \hat 7, \widehat{11} \}$

	$\hat 1$	$\hat 2$	$\hat 3$	$\hat 4$	$\hat 5$	$\hat 6$	$\hat 7$	$\hat 8$	$\hat 9$	$\widehat{10}$	$\widehat{11}$
$\hat 2$	$\hat 2$	$\hat 4$	$\hat 6$	$\hat 8$	$\widehat{10}$	$\hat 0$	$\hat 2$	$\hat 4$	$\hat 6$	$\hat 8$	$\widehat{10}$
$\hat 9$	$\hat 9$	$\hat 6$	$\hat 3$	$\hat 0$	$\hat 9$	$\hat 6$	$\hat 3$	$\hat 0$	$\hat 9$	$\hat 6$	$\hat 3$

$$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

$|U(\mathbb{Z}_n)| = \varphi(n)$.

$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$

$a_i \in \mathbb{N}^*$, p_i prime

Definiție: Fie $(G, \cdot)$ un grup, e elem. neutru în G, $x \in G$.

$$ord(x) = \begin{cases} \min\{k \in \mathbb{N}^* / x^k = e\}, & \text{dacă există} \\ \infty, & \text{dacă } x^k \neq e, \forall k \neq 0 \end{cases}$$

$(G, +)$ grup, $ord(x) = \begin{cases} \min\{k \in \mathbb{N}^* / k \cdot x = e\} \\ \infty \end{cases}$

Exemple: $(\mathbb{Z}_{12}, \cdot)$

Puterile lui $\hat{2}$: $\hat{2}, \hat{4}, \hat{8}, \hat{4}, \hat{8}, \hat{4}, \hat{8} \ldots$

$ord(\hat{2}) = \infty$

Puterile lui $\hat{5}$: $\hat{5}$, $\hat{5}^2 = \hat{1}$ $\Rightarrow$ $ord(\hat{5}) = 2$.

Ex. 2: Scrieți tabelele grupurilor $(\mathbb{Z}_4, +)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Sunt aceste grupuri izomorfe?

Rez:

$\mathbb{Z}_4$

+	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{0}$	$\hat{1}$	$\hat{2}$

$ord(\hat{0}) = 1$

$ord(\hat{2}) = 2$

$ord(\hat{1}) = 4$

$ord(\hat{3}) = 4$

$$\left.\begin{array}{l} \widehat{3k} = \hat{0} \text{ în } \mathbb{Z}_4 \\ (3,4) = 1 \end{array}\right\} \Rightarrow \hat{k} = \hat{0}$$

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

$(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ = grupul lui Klein

$$\operatorname{ord}(\hat{0},\hat{1}) = \operatorname{ord}(\hat{1},\hat{0}) = \operatorname{ord}(\hat{1},\hat{1}) = 2$$

$$(\mathbb{Z}_2 \times \mathbb{Z}_2, +) \not\cong (\mathbb{Z}_4, +)$$

Obs: Fie G un grup cu 4 elemente. Atunci G este izomorf cu $(\mathbb{Z}_4, +)$ sau cu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

Exemple: $(\{1, i, i^2, i^3\}, \cdot) \cong (\mathbb{Z}_4, +)$

$\mathcal{U}(\mathbb{Z}_{12}) = \{\hat{1}, \hat{5}, \hat{7}, \hat{11}\}$ $\hat{5}, \hat{5}^2 = \hat{1}$

$(\mathcal{U}(\mathbb{Z}_{12}), \cdot) \leq (\underline{\mathbb{Z}_{12}, \cdot})$ $\hat{7}, \hat{7}^2 = \hat{1}$

subgrup monoid

$ord(\hat{5}) = 2$ $ord(\hat{11}) = 2$

$ord(\hat{7}) = 2$

$(\mathcal{U}(\mathbb{Z}_{12}), \cdot) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

Obs: Fie G un grup finit, $|G| = n$, $x \in G$ de ordin finit. Atunci $ord(x) \mid n$.

Mai mult, $\forall x \in G$, $x^n = e$.

Ex. 3: Scrieți toate subgrupurile lui $(\mathbb{Z}_6, +)$.

$\mathbb{Z}_6 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$

- $\{\hat{0}\}$, $\mathbb{Z}_6$
- $\{\hat{0}, \hat{3}\}$
- $\{\hat{0}, \hat{2}, \hat{4}\}$

$\{\hat{0}, \hat{5}, \hat{4}, \hat{1}, \hat{2}, \hat{3}\} = \mathbb{Z}_6$.

Obs.: Fie G un grup finit și $H \leq G$ (subgrup).
Atunci $|H| \mid |G|$.

Ex. 4: Fie $(G, \cdot)$ un grup și $x \in G$ elem. de ordin finit, $ord(x) = m$. Arătați că $\forall\, k \in \mathbb{N}$, $ord(x^k) = \dfrac{m}{(m,k)}$.

Rez: $(m,k) = d$, $m = d \cdot m_1$, $k = d \cdot k_1$, $(m_1, k_1) = 1$.

$\dfrac{m}{(m,k)} = \dfrac{m}{d} = m_1$.

$ord(x^k) = m_1 \left\langle \begin{array}{l} (x^k)^{m_1} = e \quad \checkmark \\ m_1 \text{ este minim cu această propr.} \end{array} \right.$

$(x^k)^{m_1} = x^{k \cdot m_1} = x^{k_1 \cdot d \cdot m_1} = x^{k_1 \cdot m} = (x^m)^{k_1} = e^{k_1} = e$

Putem presupune că $0 \leq k < m$. Astfel din T.î.R
$k = mc + r$, $0 \leq r < m$, $x^k = x^{mc+r} = x^{mc} \cdot x^r = x^r$

Pp. că $\exists\, m < m_1$ a. î. $(x^k)^m = e$.

$$\Rightarrow \left.\begin{array}{l} x^{km} = e \\ \operatorname{ord}(x) = n \end{array}\right\} \Rightarrow n \mid k \cdot m$$

$$\left.\begin{array}{l} d \cdot n_1 \mid d \cdot k_1 \cdot m \Rightarrow n_1 \mid k_1 \cdot m \\ (n_1, k_1) = 1 \end{array}\right\} \Rightarrow$$

$$\left.\begin{array}{l} \Rightarrow n_1 \mid m \quad \text{abs.} \\ 0 < m < n_1 \end{array}\right| \Rightarrow \text{Pp. este falsă} \Rightarrow n_1 \text{ minim.}$$

$$\Rightarrow \operatorname{ord}(x^k) = n_1 = \frac{n}{(n, k)}.$$

Obs: Im $(\mathbb{Z}_n, +)$, $\operatorname{ord}(\hat{1}) = n$.

$$\boxed{\underset{\hat{k} \in \mathbb{Z}_n}{\operatorname{ord}(\hat{k})} = \operatorname{ord}(k \cdot \hat{1}) = \frac{n}{(n, k)}}$$

Ex. 5 : Fie $(G, \cdot)$ un grup, $a, b \in G$ cu propr. că $ab = ba$, $\operatorname{ord}(a) = n < \infty$, $\operatorname{ord}(b) = m < \infty$.

Arătați că $\operatorname{ord}(ab) = [m, n]$

! $\quad (ab)^{mn} \underset{(ab = ba)}{\overset{!}{=}} a^{mn} \cdot b^{mn} = (a^n)^m \cdot (b^m)^n = e$.

$\Rightarrow \operatorname{ord}(ab) \mid mn$.

ex. $\left\langle \begin{array}{l} (ab)^{[m,n]} = e \\ [m,n] \text{ este cel mai mic cu această propr.} \end{array} \right.$