Seminar 9 – 08.12.2021

Ex. 1 : Determinați elementele inversabile ale monoidului $(\mathbb{Z}_m, \cdot)$.

$\mathcal{U}(\mathbb{Z}_m) = \{\hat{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$.

Rez :

Th : Fie $a, b \in \mathbb{N}$, $(a, b) = d$. Atunci există $k, l \in \mathbb{Z}$ a.î.
$d = a \cdot k + b \cdot l$ (Algoritmul lui Euclid)

„$\supseteq$" Fie $\hat{a} \in \mathbb{Z}_m$ cu $(a, m) = 1 \xRightarrow{Th} \exists\, k, l \in \mathbb{Z}$ a.î.
$a \cdot k + m \cdot l = 1$.

În $\mathbb{Z}_m$: $\hat{a} \cdot \hat{k} + \underset{\hat{0}}{\underset{\shortparallel}{\hat{m}}} \cdot \hat{l} = \hat{1} \Rightarrow \hat{a} \cdot \hat{k} = \hat{1} \Rightarrow \hat{a} \in \mathcal{U}(\mathbb{Z}_m)$
$(\hat{a}^{-1} = \hat{k})$

„$\subseteq$" Fie $\hat{a} \in \mathcal{U}(\mathbb{Z}_m) \Rightarrow \exists\, \hat{b} \in \mathcal{U}(\mathbb{Z}_m) \subseteq \mathbb{Z}_m$ a.î. $\hat{a} \cdot \hat{b} = \hat{1}$.

Noi vrem să arătăm că $(a, m) = 1$.

Pp. că $(a, m) = d > 1$. $\Rightarrow a = d \cdot a_1$, $m = d \cdot m_1$, $(a_1, m_1) = 1$.

$\hat{a} \cdot \hat{b} = \hat{1} \Rightarrow \hat{d} \cdot \hat{a}_1 \cdot \hat{b} = \hat{1} \;\Big|\cdot \hat{m}_1 \Rightarrow \hat{m}_1 \cdot \hat{d} \cdot \hat{a}_1 \cdot \hat{b} = \hat{m}_1$

$\hat{0} = \hat{m}_1 \Rightarrow m \mid m_1$

$m \mid m_1 \Leftrightarrow d \cdot m_1 \mid m_1 \Leftrightarrow d \mid 1$ abs.

Ex. 2: Scrieți tablele grupurilor $(\mathbb{Z}_4, +)$ și $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Sunt ele izomorfe? Justificați.

Rez: $\mathbb{Z}_4$

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

$\mathbb{Z}_2 \times \mathbb{Z}_2$

$+$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$
$(\hat{0},\hat{0})$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$
$(\hat{0},\hat{1})$	$(\hat{0},\hat{1})$	$(\hat{0},\hat{0})$	$(\hat{1},\hat{1})$	$(\hat{1},\hat{0})$
$(\hat{1},\hat{0})$	$(\hat{1},\hat{0})$	$(\hat{1},\hat{1})$	$(\hat{0},\hat{0})$	$(\hat{0},\hat{1})$
$(\hat{1},\hat{1})$	$(\hat{1},\hat{1})$	$(\hat{1},\hat{0})$	$(\hat{0},\hat{1})$	$(\hat{0},\hat{0})$

Fie $(G,+)$ un grup, e elem. neutru, $x \in G$.

$$\mathrm{ord}(x) = \begin{cases} \min\{k \in \mathbb{N}^* \mid k \cdot x = e\}, & \text{dacă } \exists k \in \mathbb{N}^* \text{ a.î. } k\cdot x = e \\ \infty, & \text{dacă } kx \neq e, \forall k \in \mathbb{N}^* \end{cases}$$

$$\boxed{(G,\cdot) \longrightarrow x^k = e}$$

În $\mathbb{Z}_4$: $\mathrm{ord}(\hat{0}) = 1$, $\mathrm{ord}(\hat{1}) = 4$, $\mathrm{ord}(\hat{2}) = 2$, $\mathrm{ord}(\hat{3}) = 4$

În $\mathbb{Z}_2 \times \mathbb{Z}_2$: $\mathrm{ord}(\hat{0},\hat{0}) = 1$, $\mathrm{ord}(\hat{1},\hat{0}) = 2$, $\mathrm{ord}(\hat{0},\hat{1}) = 2$,
$\mathrm{ord}(\hat{1},\hat{1}) = 2$.

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

Obs.: Un grup cu 4 elemente este izomorf fie cu $\mathbb{Z}_4$, fie cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Temă: Fie mulțimile:

$G_1 = \left\{ I_2, A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$

$G_2 = \{1, -1, i, -i\}$

$G_3 = \left\{ e, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \right\}$

$G_4 = U(\mathbb{Z}_{12})$.

a. Arătați că $(G_1, \cdot)$, $(G_2, \cdot)$, $(G_3, \circ)$, $(G_4, \cdot)$ sunt grupuri (comutative)

b. Decideți care grupuri sunt izo cu $\mathbb{Z}_4$ și care cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Obs.: $|\mathbb{Z}_m| = m$, $U(\mathbb{Z}_m) = \{\hat{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$.

$|U(\mathbb{Z}_m)| = \varphi(m)$

$(\mathbb{Z}_m, \cdot)$ monoid $\longrightarrow$ $(U(\mathbb{Z}_m), \cdot)$ grup

Ex. 3: Fie $(G, \cdot)$ un grup, $a, b \in G$ de ordin finit, $ord(a) = n$
$ord(b) = m$. Arătați că dacă $ab = ba$ și $(m, n) = 1$, atunci
$ord(ab) = m \cdot n$.

Rez: $ord(ab) = m \cdot n$ < $(ab)^{m \cdot n} = e$
mn minim cu această prop.

$$(ab)^{mn} \overset{ab=ba}{=} a^{m \cdot n} \cdot b^{m \cdot n} = (\underbrace{a^n}_{=e})^m \cdot (\overbrace{b^m}^{=e})^n = e^m \cdot e^n = e$$

e (deoarece $ord(a) = n$)

Obs.: Dacă $x^k = e$ pt. un anumit $k \in \mathbb{N}^*$, atunci $ord(x) \mid k$.

Pp. că $ord(ab) = k$. Cum $(ab)^{mn} = e \Rightarrow k \mid mn$.

$(ab)^k = e \Rightarrow a^k \cdot b^k = e \Rightarrow a^k = b^{-k}$.

$$a^k = b^{-k} \Big|^{m} \Rightarrow a^{mk} = b^{-mk} \Rightarrow b^{-mk} = e \Rightarrow n \mid mk.$$

$$\left.\begin{array}{l} \left.\begin{array}{l} n \mid mk \\ (n,m)=1 \end{array}\right\} \Rightarrow n \mid k \\ \text{Analog, obţinem } m \mid k \end{array}\right\} \Rightarrow \left.\begin{array}{l} [n,m] \mid k \\ (n,m)=1 \end{array}\right\} \Rightarrow nm \mid k.$$

Reminder: $a, b \in \mathbb{N}$, $a \cdot b = [a,b] \cdot (a,b)$.

$$\left.\begin{array}{l} k \mid nm \\ nm \mid k \end{array}\right\} \Rightarrow k = nm. \Rightarrow \operatorname{ord}(ab) = nm.$$

Contraexemplu: În S_3 considerăm $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ şi

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$\operatorname{ord}(\tau) = 2$, $\operatorname{ord}(\sigma) = 3$, $(2,3) = 1$.

$\rho = \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\rho^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$ord(\tau \circ \sigma) = 2$.

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

$(m,k) = $ cmmdc (m,k).

Rez: $ord(x^k) = \dfrac{m}{(m,k)} = m_1$ $\begin{cases} (x^k)^{m_1} = e \\ m_1 \text{ este minim cu această propr.} \end{cases}$

Fie $d = (m,k)$. $\Rightarrow m = d \cdot m_1$, $k = d \cdot k_1$, $(m_1, k_1) = 1$.

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

$\left[(x^k)^{\frac{m}{(m,k)}} = x^{\frac{k \cdot m}{(m,k)}} = x^{[m,k]} = e \quad (m \mid [m,k]) \right]$

Obs: Putem presupune că $0 \le k < n$.

Dim T.Î.R: $k = n \cdot c + r$, $0 \leq r < n$

$$x^k = x^{n \cdot c + r} = x^{n \cdot c} \cdot x^r = x^r$$

$$(x^k)^{n_1} = e \Rightarrow ord(x^k) \mid n_1.$$

Fie $ord(x^k) = m$, $m \mid n_1$

$$\left.\begin{array}{l} x^{km} = e \\ ord(x) = n \end{array}\right\} \Rightarrow n \mid km \Rightarrow d \cdot n_1 \mid d \cdot k_1 \cdot m \Rightarrow n_1 \mid k_1 \cdot m \quad (n_1, k_1) = 1 \Rightarrow$$

$$\Rightarrow \left.\begin{array}{l} n_1 \mid m \\ m \mid n_1 \end{array}\right\} \Rightarrow m = n_1.$$

! Obs.: Fie $(G, \cdot)$ un grup finit, $|G| = n$, $x \in G$.
Atunci $ord(x) < \infty$ și mai mult $ord(x) \mid n$.
În particular, $x^n = e$, $\forall x \in G$.
$H = \langle x \rangle = \{x^k \mid k \in \mathbb{Z}\} \leq G \Rightarrow |H| \leq n$.

Exemplu: $(\mathbb{Z}_6, \cdot)$ monoid

$(\mathcal{U}(\mathbb{Z}_6), \cdot)$ grup, $\mathcal{U}(\mathbb{Z}_6) = \{\hat{1}, \hat{5}\}$

$\text{ord}(\hat{1}) = 1$, $\text{ord}(\hat{5}) = 2$.

$\hat{2}^1 = \hat{2}$, $\hat{2}^2 = \hat{4}$, $\hat{2}^3 = \hat{2}$, $\hat{2}^4 = 4$

$\hat{2}^k \in \{\hat{2}, \hat{4}\}$, $\forall k \in \mathbb{N}^*$.

$a^k \mod n$ <
- n prim, $a^{p-1} \equiv 1$
- $(a,m) = 1 : a^{\varphi(m)} \equiv 1$.
- $(a,m) \neq 1$

$a^{a^{b^b}} \mod m \equiv a^r$

$(a,m) = 1$, $a^{\varphi(m)} \equiv 1$, $a^{b^b} \equiv r \mod \varphi(m)$

$(a,m) > 1 \rightsquigarrow a^1, a^2, a^3, \ldots$ (seamănă cu pb. cu ultima cifră)