Seminar 10

13.12.2021

Exc Să se arate că un grup cu 4 elemente este izomorf ori cu $(\mathbb{Z}_4,+)$ ori cu $(\mathbb{Z}_2\times\mathbb{Z}_2,+)$.

Dem Fie $(G,\cdot)$ un grup cu $|G|=4$.

① Dc G are un element de ordin 4 $\rightsquigarrow G$ e ciclic $\xrightarrow[\text{Sg}]{\text{vezi}}$ $(G,\cdot)\simeq(\mathbb{Z}_4,+)$ (au "aceleași" tablă)

② $(\forall)\, x\in G$ $\text{ord}(x)\neq 4$. Lagrange $\Rightarrow \text{ord}(x)\mid 4 \Rightarrow \text{ord}\, x\in\{1,2\}$.

Dar $\boxed{\text{ord}(x)=1 \Leftrightarrow x=1_G}$ $\Rightarrow (\forall)\, x\in G\setminus\{1_G\}$ $\text{ord}(x)=2$.

$\Rightarrow x^2=1_G$ $(\forall)\, x\in G \Rightarrow G$ e abelian ; $G=\{1_G,x,y,z\}$ (vezi Sg, Sg)

$z=xy$ (deoarece $x\neq y\neq 1_G$ distincte 2 câte 2 : $xy\neq x \rightsquigarrow y\neq 1_G$; $xy\neq y \Leftrightarrow x\neq 1_G$; $xy=1_G \Rightarrow y=x^{-1}=x$ $\lightning$ $\Rightarrow xy\neq 1_G$) $\Rightarrow$

$\Rightarrow G=\langle x,y\rangle \underset{\text{grupuri}}{\overset{\text{izom.}}{\simeq}} (\mathbb{Z}_2\times\mathbb{Z}_2,+)$

$1_G \xmapsto{\varphi} (\hat{0},\hat{0})$
$x \xmapsto{\varphi} (\hat{1},\hat{0})$
$y \xmapsto{\varphi} (\hat{0},\hat{1})$
$xy \xmapsto{\varphi} (\hat{1},\hat{1})$

$\varphi(x\cdot y)=\varphi(x)+\varphi(y)$ φ e morfism de grupuri! (Exc.) verificați

φ e bijecție

$\Rightarrow \varphi$ e izom. de grupuri.

Exc! Un grup cu 6 elemente este izomorf cu $(\mathbb{Z}_6,+)$ sau $(S_3,\circ)$.
abelian nonabelian

(Exc!) Fie p un nr. prim. Să se arate că un grup G cu p elemente este izomorf cu $(\mathbb{Z}_p,+)$.

Dem Fie $(G,\cdot)$ un grup $|G|=p\geq 2$. Fie $x\in G\setminus\{1_G\} \Rightarrow \text{ord}(x)\neq 1$ $\Rightarrow$

T. Lagrange $\Rightarrow \text{ord}(x)\mid |G|=p$

$\Rightarrow \text{ord}(x)=p$. $\Rightarrow$ $G=\langle x\rangle=\{1_G,x,x^2,\dots,x^{p-1}\}$

Fie $\varphi: G\longrightarrow(\mathbb{Z}_p,+)$ $\varphi(x^k)=\hat{k}$ $(\forall)\ k=\overline{0,p-1}$ $(x^0=1_G)$ atunci φ este morfism de grupuri bijectiv (= izom. de gr.)

f morf. de grupuri: $f(x^i \cdot x^j) = f(x^i) + f(x^j)$ (0) $\forall\ i,j \in \{0,\dots,p-1\}$

$f(x^i) + f(x^j) = \hat{i} + \hat{j} = \widehat{i+j}$

$f(x^i \cdot x^j) = f(x^{i+j})$ (*)

$\widehat{i+j}$ dc $i+j \le p-1$ (1)

dc $i+j > p \Rightarrow f(x^{i+j}) = f(x^p \cdot x^{i+j-p})$

$= f(1 \cdot x^{i+j-p}) = f(x^{i+j-p}) = \widehat{i+j-p} = \widehat{i+j}$ (2)

$i+j-p < p$

$0 \le i,j < p$

Dim (*), (1) și (2) $\Rightarrow$ (0)

Ordinul unui element

$(G, \cdot)$ → grup.

Exc 1 Dacă $\text{ord}(x) = n < \infty$ atunci $k \in \mathbb{Z}$ a.î. $x^k = 1_G \iff n \mid k$.

Dem "$\Leftarrow$" $n \mid k \Rightarrow k = n \cdot a$, $a \in \mathbb{Z}$ $\quad x^k = x^{n \cdot a} = (x^n)^a = 1_G^a = 1_G$. ($\text{ord}(x) = n$)

"$\Rightarrow$" Pp. rod. la abs. că $n \nmid k \Rightarrow k = n \cdot a + r$ cu $0 < r < n$

$x^k = 1_G \Rightarrow x^{n \cdot a + r} = 1_G \Rightarrow (x^n)^a \cdot x^r = 1_G \Rightarrow x^r = 1_G$ $\quad (0 < r < n)$ ↯

↯ ($\text{ord}(x) = n$) $\Rightarrow$ Pp. e falsă $\Rightarrow n \mid k$.

Exc 2 Fie $(G, \cdot)$ un grup și $x \in G$ a.î. $\text{ord}(x) = n < \infty$. Arătați că:

$(\forall)\ k \in \mathbb{N}$ $\quad \text{ord}(x^k) = \dfrac{n}{(n,k)}$, unde (n,k) repr. c.m.m.d.c. dintre n și k.

Aplicații: **Exc 3** Calculați $\text{ord}(\hat{144})$ în $(\mathbb{Z}_{1000}, +)$; $\text{ord}(\hat{33})$ în $(\mathbb{Z}_{311}, +)$

$\text{ord}(\hat{75})$ în $(\mathbb{Z}_{500}, +)$.

Exc 4 Det. elem. de ordin 8 din $(\mathbb{Z}_6 \times \mathbb{Z}_{10}, +)$, elementele de ordin 4 din $(\mathbb{Z}_{12} \times \mathbb{Z}_{15}, +)$ și elementele de ordin 6 din $(\mathbb{Z}_{12} \times \mathbb{Z}_{36}, +)$

Fie $(n,k) = d$. $\Rightarrow n = dn_1$, $k = dk_1$ $\quad (n_1, k_1) = 1$.

Vrem să arăt $\text{ord}(x^k) = \dfrac{n}{d} = n_1$.

- $(x^k)^{n_1} = x^{kn_1} = x^{dk_1 n_1} = (x^{dn_1})^{k_1} = (x^n)^{k_1} = (1_G)^{k_1} = 1_G$
- A mai rămas de arătat că n_1 este cel mai mic nr. natural nenul a.î. $(x^k)^{n_1} = 1_G$.

Pp. prin reducere la absurd că $(\exists)\ 0<t<m_1$ a.î. $(x^k)^t = 1_G \Rightarrow$

$\Rightarrow x^{kt} = 1_G \xrightarrow{\text{Exc 1}} m \mid kt \Rightarrow k\cdot t = m\cdot a \quad a\in\mathbb{Z}$

$\ord(x)$

$d k_1 \cdot t = d\cdot m_1 \cdot a \Rightarrow k_1 t = m_1 a \Rightarrow$

$\Rightarrow \begin{matrix} m_1 \mid k_1 t \\ (m_1, k_1) = 1 \end{matrix} \Rightarrow m_1 \mid t \Rightarrow m_1 \le t$ (m_1 nenul)

$0<t<m_1$

$\Rightarrow$ pp. e falsă $\Rightarrow$

$\Rightarrow \ord(x^k) = m_1 \left(= \frac{m}{(m,k)}\right)$

Exc 3 $(\mathbb{Z}_m, +) = \langle \hat{1} \rangle \quad \ord(\hat{1}) = m \quad \ord(\hat{k}) \overset{\text{Exc 2}}{=} \frac{m}{(m,k)}$

$\hat{k} = \underbrace{\hat{1}+\hat{1}+\dots+\hat{1}}_{k \text{ ori}}$

$\hat{1}$ în $(\mathbb{Z}_{1000}, +) \quad \ord(\widehat{144}) = \frac{1000}{(1000,144)} = \frac{1000}{2^3} = 125$

$\hat{1}$ în $(\mathbb{Z}_{311}, +) \quad \ord(\widehat{33}) = \frac{311}{(33,311)} = \frac{311}{1} = 311$

Exc 3.1 Fie $U_{36} = \{ z\in\mathbb{C} \mid z^{36} = 1 \}$ $\left((U_{36}, \cdot) \simeq (\mathbb{Z}_{36}, +) \right)$

$U_{36} = \{ \cos\frac{2k\pi}{36} + i\sin\frac{2k\pi}{36} \mid k = 0,\dots,35 \} = \{ \underbrace{1}_{z_0}, x_1, x_1^2, \dots, x_1^{35} \}$,

$\begin{cases} z^m = 1 \Rightarrow z_k = \cos\frac{2k\pi}{m} + i\sin\frac{2k\pi}{m} & k\in\{0,1,\dots,m-1\} \\ \text{Moivre: } z_1^k = \left(\cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}\right)^k = \left(\cos\frac{2k\pi}{m} + i\sin\frac{2k\pi}{m}\right) = z_k \\ z_1^m = 1 \end{cases}$

unde $x_1 = \cos\frac{2\pi}{36} + i\sin\frac{2\pi}{36}$. $\quad U_{36} = \langle x_1 \rangle$

Calculați $\ord\left(\cos\frac{2\cdot 18\pi}{36} + i\sin\frac{2\cdot 18\pi}{36}\right)$ în $(U_{36}, \cdot)$!

$\ord(x_1^{18}) \overset{\text{Exc 2}}{=\!=} \frac{\ord x_1}{(\ord x_1, 18)} = \frac{36}{(36,18)} = \frac{36}{18} = 2$ $\quad x_1^{18} = \cos\pi + i\sin\pi = -1$ (sau $\ord(-1) = 2$)

$(\mathbb{Z}_m, +) \quad \ord(\hat{k}) = \frac{m}{(m,k)} \quad \ord(\hat{k}) = m \Longleftrightarrow (m,k) = 1$

Elementele de ordin m din $(\mathbb{Z}_m, +)$ (sau generatorii lui $(\mathbb{Z}_m, +)$) sunt $\{ \hat{k} \mid (k,m) = 1 \}$.

Exc 3.2 $U(\mathbb{Z}_m, \cdot)$ → grup cu $\varphi(m)$ elemente.

$U(\mathbb{Z}_{31}, \cdot) = \mathbb{Z}_{31} \setminus \{\hat{0}\}$ ($\varphi(31) = 31 - 1 = 30$) Calculați $\hat{2020}^{2020^{2020}}$ în $\mathbb{Z}_{31}$.

Euler $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

$2020 \equiv 5 \pmod{31}$

$m = 31, a = 5$ $5^{30} = 5^{\varphi(31)} \equiv 1 \pmod{31}$

$2020 = 30 \cdot 67 + 10$

$2020^{2020} \equiv 5^{2020} \pmod{31} \equiv 5^{30 \cdot 67 + 10} \pmod{31}$

$2020 \mid 30$ — 18 | 67 — 220 — 210 — 10

$\equiv (5^{30})^{67} \cdot 5^{10} \pmod{31} \equiv 5^{10} \pmod{31} \equiv 25^5 \pmod{31} \equiv -6^5 \pmod{31} \equiv$

$1 \equiv -36^2 \cdot 6 \pmod{31} \equiv -5^2 \cdot 6 \pmod{31} \equiv -25 \cdot 6 \pmod{31} \equiv 6^2 \pmod{31}$

$\equiv 5 \pmod{31}$.

$\hat{5}^{2020} = \hat{5}$ în $\mathbb{Z}_{31}$

$\operatorname{ord}(\hat{5}^{2020}) = \operatorname{ord}(\hat{5})$

$\operatorname{ord}(\hat{5}^{2020}) = ?$ în $U(\mathbb{Z}_{31}, \cdot)$?

Exc 2 $\Rightarrow$ $\dfrac{\operatorname{ord}(\hat{5})}{(2020, \operatorname{ord}(\hat{5}))} = \dfrac{3}{(2020, 3)} = \dfrac{3}{1} = 3$

Vreau $\operatorname{ord}(\hat{5})$ (folosesc definiția, știind că $\operatorname{ord}(\hat{5})$ în $(\mathbb{Z}_{31}, \cdot)$ $\operatorname{ord}(\hat{5}) \mid 30$)

$\hat{5}^2 = \hat{25}$ $\hat{5}^3 = \hat{125} = \hat{1}$ în $\mathbb{Z}_{31}$ $\Rightarrow$ $\boxed{\operatorname{ord}(\hat{5}) = 3}$

Exc Fie G_1, G_2 grupuri, $x \in G_1, y \in G_2$ a.î. $\operatorname{ord}(x) = n < \infty$ și $\operatorname{ord}(y) = m < \infty$. Atunci $\operatorname{ord}((x,y)) = [n,m]$, unde $(x,y) \in G_1 \times G_2$ (grupul produs direct).

Exc 4 e aplicație directă la ↑ și Exc 2.

Dem Fie $[n,m] = t \rightsquigarrow t \cdot d = n \cdot m$ $d = (n,m)$ $n = d n_1$, $(n_1, m_1) = 1$

$m = d m_1$

$t = d n_1 m_1$

$(x,y)^t = (x^t, y^t) = (x^{d n_1 m_1}, y^{d n_1 m_1}) =$

$= ((x^n)^{m_1}, (y^m)^{n_1}) = (1_{G_1}, 1_{G_2})$ (Exc 1)

Fie $k \in \mathbb{N}^*$ a.î. $(x,y)^k = (1_{G_1}, 1_{G_2}) \Rightarrow$ $\begin{cases} x^k = 1_{G_1} \Rightarrow n \mid k \\ y^k = 1_{G_2} \Rightarrow m \mid k \end{cases}$ (Exc 1) $\Rightarrow [n,m] \mid k$ (t'')

$\Longrightarrow_{k \neq 0}$ $t \leq k \Rightarrow t = \operatorname{ord}((x,y))$. ∎