Semimar 8

24.11.2020

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 a.î. $|G|=4$.

① Dc G are un element de ordin 4 $\rightsquigarrow$ G e ciclic $\overset{C8}{\rightsquigarrow} (G,\cdot)\simeq(\mathbb{Z}_4,+)$

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

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

$\Rightarrow x^2=1_G\ (\forall)\, x\in G \underset{\boxed{S7}}{\Longrightarrow}$ G e abelian ; $G=\{1_G, x, y, z\}$ deoarece $xy\neq x\neq y$, $xy \neq 1_G$ (distincte două câte 2), $z = xy$

$\Rightarrow x=x^{-1}$

$\left(xy=x \Rightarrow y=1_G\ \text{\textit{ₓ}}\right.$; $xy=y \Rightarrow x=1_G$ ✗ ; $xy=1_G \Rightarrow x=y^{-1}=y$ ✗ $\left.\right)$

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

$1_G \longmapsto (\hat{0},\hat{0})$

$x \longmapsto (\hat{1},\hat{0})$

$y \longmapsto (\hat{0},\hat{1})$

$x\cdot y \longmapsto (\hat{1},\hat{1})$

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

Exc (greu) Un grup cu 8 elemente este izomorf cu:

- abelian: $(\mathbb{Z}_8,+)$ sau $(\mathbb{Z}_2\times\mathbb{Z}_4,+)$ sau $(\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,+)$
- neabelian: $(D_4,\cdot)$ sau grupul cuaternionilor

D_4 = grupul diedral de ordin 4

Ordinul unui element $(G,\cdot)$ grup

$$ord(x)=\begin{cases}\infty, & \text{dacă } x^n\neq 1_G\ (\forall)\, n\in\mathbb{N}^*\\ t, & \text{dacă } x^t=1_G,\ t\in\mathbb{N}^* \text{ și } t \text{ cel mai mic cu proprietatea (număr natural nenul)}\end{cases}$$

Exc 2 Dc $ord(x)=n<\infty$ atunci $k\in\mathbb{Z}$, $x^k=1 \Leftrightarrow n\mid k$.

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

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

$x^k=1 \Rightarrow x^{na+r}=1 \Rightarrow x^{na}\cdot x^r=1 \Rightarrow (x^n)^a\cdot x^r=1 \underset{ord(x)=n}{\Rightarrow} x^r=1$ ($(x^n)^a=1$), $(0<r<n)$ contradicție cu def $ord(x)$.

Exc 3 Fie G un grup și $x\in G$ $ord(x)=n<\infty$. Arătați că $(\forall)\, k\in\mathbb{N}$ $ord(x^k)=\frac{n}{(n,k)}$, unde (n,k) repr. c.m.m.d.c. al lui n și k.

Fie $(n,k)=d$. Vreau $\operatorname{ord}(x^k)=\frac{n}{d}=n_1$. ✓

$\left(n=dn_1;\ k=dk_1;\ (n_1,k_1)=1\right)$

$(x^k)^{n_1}=x^{kn_1}=x^{dk_1n_1}=x^{k_1(dn_1)}=x^{nk_1}=(x^n)^{k_1}=1.$

A mai rămas de arătat că n_1 este cel mai mic natural nenul a.î. $(x^k)^{n_1}=1$. $\operatorname{ord}(x)=n$

Pp prin. reducere la absurd că $(\exists)\ 0<t<n_1$ a.î. $(x^k)^t=1$. $\Rightarrow x^{kt}=1$

$\Rightarrow n\mid kt \Rightarrow kt=n\cdot a$ cu un $a\in\mathbb{Z}$

Exc 2

$dk_1t=dn_1\cdot a \Rightarrow k_1t=n_1a. \Rightarrow n_1\mid k_1t$ $\quad (n_1,k_1)=1$ $\Rightarrow \boxed{n_1\mid t} \Rightarrow$

$n_1\le t$ ✗ (deoarece $t>0$)

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

Exc 4 (aplicații la Exc 3) Calculați $\operatorname{ord}(\hat{144})$ în $(\mathbb{Z}_{1000},+)$; $\operatorname{ord}(\hat{36})$ în $(\mathbb{Z}_{1000},+)$; $\operatorname{ord}(\hat{75})$ în $(\mathbb{Z}_{500},+)$.

$\mathbb{Z}_n=\langle\hat{1}\rangle$ $\quad \operatorname{ord}(\hat{1})=n$ $\quad \operatorname{ord}(\hat{k})\overset{\text{Exc3}}{=}\frac{n}{(n,k)}$

în $\mathbb{Z}_{1000}$ $\quad \operatorname{ord}(\hat{144})=\frac{1000}{(144,1000)}=\frac{1000}{2^3}=5^3=125$

$\text{in}(\mathbb{Z}_{100},+)$ $\quad \text{ord}(\hat{36}) = \frac{100}{(36,100)} = 25.$

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

$U_{36} = \langle \underbrace{\cos\frac{\pi}{18} + i\sin\frac{\pi}{18}}_{z_1} \rangle$ $\quad z_1 = \cos\frac{2\pi}{36} + i\sin\frac{2\pi}{36}$

$= \{1, z_1, z_1^2, \dots, z_1^{35}\}$

$\text{ord}(z_1^{18}) = \frac{\text{ord}(z_1)}{(\text{ord}(z_1), 18)} = \frac{36}{(36,18)} = 2.$ $\quad (\underline{\text{Verificare}}: z_1^{18} \overset{\text{Moivre}}{=\!=} \cos\pi + i\sin\pi = -1. \quad \text{ord}(-1) = 2)$

Fie $U(\mathbb{Z}_m, \cdot)$ $\to$ grup cu $\varphi(m)$ elemente.

$U(\mathbb{Z}_{31}, \cdot) = \mathbb{Z}_{31}^*$ $\quad$ Cine e $\underbrace{2020^{2020}}$ in $\mathbb{Z}_{31}^*$?

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

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

$\equiv 5^{10} \pmod{31} \equiv 25^5 \pmod{31}$

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

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

$\equiv 5 \pmod{31}$

$\text{ord}(\hat{5}^{2020})$ in $U(\mathbb{Z}_{31}, \cdot)$

$$\text{ord}(\hat{5}^{2020}) = \frac{\text{ord}(\hat{5})}{(2020, \text{ord}(\hat{5}))} = \frac{3}{1} = 3$$

Euler $\Rightarrow 5^{30} \equiv 1 \pmod{31} \Rightarrow \hat{5}^{30} = \hat{1} \Rightarrow \text{ord}(\hat{5}) \mid 30.$

$5^2 \equiv 25 \pmod{31}$ $\quad 5^3 \equiv 125 \equiv 1 \pmod{31} \Rightarrow \hat{5}^3 = \hat{1} \Rightarrow \boxed{\text{ord}(\hat{5}) = 3}$ $(\cdot)$

$(\cdot) \rightsquigarrow (*)$ $\quad 2020^{2020} \equiv 5^{2020} \pmod{31} \equiv 5^{3 \cdot 673 + 1} \pmod{31} \equiv 5 \pmod{31}.$

Exc 5 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 $\mathbb{Z}_{12} \times \mathbb{Z}_{36}$.

Exc 6 Fie G_1, G_2 2 grupuri, $x \in G_1$, $y \in G_2$ a.î. $\text{ord}(x) = n < \infty$ și $\text{ord}(y) = m < \infty$. Atunci $\text{ord}((x,y)) = [n,m]$, unde $(x,y) \in G_1 \times G_2$ (grupul produs direct).

Fie $[n,m] = t \rightsquigarrow \boxed{t \cdot d = n \cdot m}$, unde $d = (n,m)$. $\rightsquigarrow \boxed{t = d n_1 m_1}$

$d = (n,m) \Rightarrow n = d n_1$, $m = d m_1$, $(n_1, m_1) = 1$

$$(x,y)^t = (x^t, y^t) = (x^{d n_1 m_1}, y^{d n_1 m_1}) = (x^{n \cdot m_1}, y^{m \cdot n_1}) = (1_{G_1}, 1_{G_2})$$

$x^{n \cdot m_1} = (x^n)^{m_1}$, $\quad y^{m \cdot n_1} = (y^m)^{n_1}$

Fie $k \in \mathbb{N}^*$ a.î. $(x,y)^k = (1_{G_1}, 1_{G_2}) \Rightarrow \begin{cases} x^k = 1_{G_1} \Rightarrow n \mid k \\ y^k = 1_{G_2} \Rightarrow m \mid k \end{cases} \Rightarrow [n,m] \mid k$

t ; $k \neq 0 \Rightarrow k \geq t$

$\Rightarrow$ t e cel mai mic nr. nat. nenul a.î. $(x,y)^t = (1_{G_1}, 1_{G_2}) \Rightarrow \text{ord}((x,y)) = t$.

Exc 5 $\{(\hat{k},\bar{l}) \in \mathbb{Z}_6 \times \mathbb{Z}_{10} \mid \text{ord}((\hat{k},\bar{l})) = 8\}$.

Exc 6 $\rightsquigarrow$ $\text{ord}((\hat{k},\bar{l})) = [\text{ord}(\hat{k}), \text{ord}(\bar{l})] = 8 = 2^3 \Rightarrow$ $\text{ord}(\hat{k}) = 8$ sau $\text{ord}(\bar{l}) = 8$

Lagrange $\Rightarrow$ $\begin{cases} \text{ord}(\hat{k}) \mid 6 & (1) \\ \text{ord}(\bar{l}) \mid 10 & (2) \end{cases}$

$\not\exists$ (1) $\not\exists$ (2)

$\Rightarrow$ Nu există elemente de ordin 8 în $\mathbb{Z}_6 \times \mathbb{Z}_{10}$.

$A = \{(\hat{k},\bar{l}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{15} \mid \text{ord}((\hat{k},\bar{l})) = 4\}$

Exc 6 $\rightsquigarrow$ $\text{ord}((\hat{k},\bar{l})) = [\text{ord}(\hat{k}), \text{ord}(\bar{l})] = 4$ (*)

Lagrange $\Rightarrow$ $\begin{cases} \text{ord}(\hat{k}) \mid 12 \\ \text{ord}(\bar{l}) \mid 15 \end{cases}$ $\Rightarrow$ $\text{ord}(\hat{k}) = 4$ și $\text{ord}(\bar{l}) = 1$

$\text{ord}(\hat{k}) = 4$ sau $\text{ord}(\bar{l}) = 4$

(*) $\Rightarrow$ $(\text{ord}(\hat{k}), \text{ord}(\bar{l}) \in \{1,2,4\})$

$\text{ord}(\bar{l}) = 1 \Rightarrow \bar{l} = \bar{0}$ în $\mathbb{Z}_{15}$

$4 = \text{ord}(\hat{k}) = \frac{12}{(12,k)} \Rightarrow (12,k) = 3 \underset{k<12}{\Rightarrow} k \in \{3,9\}$

Deci $A = \{(\hat{3}, \bar{0}), (\hat{9}, \bar{0})\}$.

$B = \{(\hat{k}, \bar{\ell}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{36} \mid ord((\hat{k}, \bar{\ell})) = 6\}$

Exc 6 $\Rightarrow$ $ord((\hat{k}, \bar{\ell})) = [ord(\hat{k}), ord(\bar{\ell})] = 6$

Lagrange $\Rightarrow$ $\begin{cases} ord(\hat{k}) \mid 12 \\ ord(\bar{\ell}) \mid 36 \end{cases}$ $\Rightarrow$

$(ord(\hat{k}), ord(\bar{\ell})) \in \{(1,6), (2,6), (3,6), (6,6), (2,3), (6,3), (3,2), (6,2), (6,1)\}$

$ord(\hat{k}) = \frac{12}{(12,k)}$ $\quad ord(\bar{\ell}) = \frac{36}{(36,\ell)}$

TEMĂ !!

$ord(\bar{\ell}) = 1 \iff \bar{\ell} = \bar{0}$ in $\mathbb{Z}_{36}$

$ord(\bar{\ell}) = 2 \Rightarrow \dots$

$ord(\bar{\ell}) = 3 \Rightarrow \dots$

$ord(\bar{\ell}) = 6 \Rightarrow \dots$

$ord(\hat{k}) = 1 \iff \hat{k} = \hat{0}$ in $\mathbb{Z}_{12}$

$ord(\hat{k}) = 2 \Rightarrow (12,k) = 6 \Rightarrow \hat{k} \in \{\hat{6}\}$

$ord(\hat{k}) = 3 \Rightarrow (12,k) = 4 \Rightarrow \hat{k} \in \{\hat{4}, \hat{8}\}$

$ord(\hat{k}) = 6 \Rightarrow (12,k) = 2 \Rightarrow \hat{k} \in \{\hat{2}, \hat{10}\}$