Seminar 9

Ex 1: Să se calculeze ordinele elem.:

a. $\hat{4}, \hat{5}, \hat{7}$ în $(\mathbb{Z}_{31}^*, \cdot)$

b. $\hat{5}, \hat{7}, \hat{25}$ în $(\mathbb{Z}_{30}, \cdot)$ ($U(\mathbb{Z}_{30}), \cdot$)

Rez:

a. $a^{p-1} \equiv 1 \pmod p$ p prim, $(a,p)=1$.

$\hat{4}^{30} = \hat{1} \Rightarrow \text{ord}(\hat{4}) \mid 30$.

$\hat{4}^2 = \hat{16}$

$\hat{4}^3 = \hat{64} = \hat{2}$

$\hat{4}^5 = \hat{32} = \hat{1} \Rightarrow \text{ord}(\hat{4}) = 5$.

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

$\hat{5}^2 = \hat{25}$

$\hat{5}^3 = \hat{125} = \hat{1} \Rightarrow \text{ord}(\hat{5}) = 3$.

$\hat{7}^{30} = \hat{1} \Rightarrow \text{ord}(\hat{7}) \mid 30$

$\hat{7}^2 = \hat{49} = \hat{18}$ $\quad \hat{7}^4 = \hat{35} = \hat{4}$

$\hat{7}^3 = \hat{7} \cdot \hat{18} = \hat{126} = \hat{2}$

$\hat{7}^5 = \hat{2} \cdot \hat{18} = \hat{36} = \hat{5}$

$=$

$\text{ord}(\hat{5}) = 3 \Leftrightarrow \text{ord}(\hat{7}^5) = 3 \Rightarrow \text{ord}(\hat{7}) = 15$

$\hat{5}^3 = \hat{1}$

$(\hat{7}^5)^3 = \hat{1} \Leftrightarrow \hat{7}^{15} = \hat{1} \Rightarrow \text{ord}(\hat{7}) \mid \hat{15}$

b. $(a,m)=1$, $a^{\varphi(m)} \equiv 1 \pmod m$

$\varphi(32) = \varphi(2^5) = 32\left(1-\frac{1}{2}\right) = 16.$

$\hat{5}^{16} = \hat{1} \Rightarrow \text{ord}(\hat{5}) \mid 16$

$\hat{5}^2 = \hat{25} = -\hat{7}$

$\hat{5}^4 = (-\hat{7})^2 = \hat{49} = \hat{17}$

$\hat{5}^8 = \hat{17}\cdot\hat{17} = \hat{1} \Rightarrow \text{ord}(\hat{5}) = 8$

$\hat{7}^{16} = \hat{1} \Rightarrow \text{ord}(\hat{7}) \mid 16.$

$\hat{7}^2 = \hat{49} = \hat{17}$

$\hat{7}^4 = \hat{1} \Rightarrow \text{ord}(\hat{7}) = 4.$

$\hat{25}^{16} = \hat{1} \Rightarrow \text{ord}(\hat{25}) \mid 16$

$\left.\begin{array}{l} \hat{25} = \hat{5}^2 \\ \text{ord}(\hat{5}) = 8 \end{array}\right\} \Rightarrow \text{ord}(\hat{25}) = 4.$ $\quad \left|\begin{array}{l} \hat{5}^8 = \hat{1} \\ (\hat{5}^2)^4 = \hat{1} \end{array}\right.$

Ex. 2 : Det. efectivele de ordin m în grupul specificat :

a. $m=2$, $(\mathbb{Q}^*, \cdot)$

b. $m=2$, $(\mathbb{Z}_4, +)$

c. $m=3$, $(\mathbb{Z}_{24}, +)$

d. $m=4$, $(\mathbb{C}^*, \cdot)$

Rez :

a. $x \in \mathbb{Q}^*$, $x^2 = 1 \Rightarrow x = \pm 1$

$x = 1$, $\text{ord}(1) = 1$

$\boxed{x=-1}$, $\text{ord}(-1) = 2$

b. $(\mathbb{Z}_4, +)$, $2\hat{x} = \hat{0} \Rightarrow \hat{x} = \hat{0}$ sau $\boxed{\hat{x} = \hat{2}}$

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

c. $(\mathbb{Z}_{24}, +)$, $3\hat{x} = \hat{0}$

$\text{ord}(\hat{x}) = \frac{m}{(m,x)}$, $\text{ord}(\hat{x}) = \frac{24}{(24,x)} = 3 \Rightarrow (24,x) = 8$

$(24, x) = 8 \iff \hat{x} \in \{\hat{8}, \hat{16}\}$

d. $x^4 = 1$ în $(\mathbb{C}^*, \cdot)$

$x^4 - 1 = 0 \iff (x-1)(x+1)(x^2+1) = 0$

$\boxed{i, -i.}$

Ex. 3: Fie $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, c \in \mathbb{R}^*, b \in \mathbb{R} \right\}$.

a. Să se arate că $(G, \cdot)$ grup.

b. Det. elementele de ordin 2 ale lui G.

c. Arătați că $A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}$ au ordinul 2, dar AB are ordinul ∞.

Rez:

a. Parte stabilă

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}$$

$a, c \in \mathbb{R}^*$

$d, f \in \mathbb{R}^*$

$ad, cf \in \mathbb{R}^*$

Asoc. OK

Elem. neutru: I_2

$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \Rightarrow A^{-1} = \frac{1}{ac}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} \in G$

b. $A^2 = I_2$, $A \neq I_2$.

$$A^2 - \mathrm{Tr}(A) \cdot A + \det A \cdot I_2 = O_2.$$

$\mathrm{Tr}(A) = a + c$

$\det A = ac$

$I_2 - (a+c)A + ac\, I_2 = O_2$

$(1+ac)\, I_2 = (a+c)\, A$

$$\begin{pmatrix} 1+ac & 0 \\ 0 & 1+ac \end{pmatrix} = \begin{pmatrix} a(a+c) & b(a+c) \\ 0 & c(a+c) \end{pmatrix}$$

$$\begin{cases} a^2+ac = 1+ac \\ c^2+ac = 1+ac \\ b(a+c)=0 \end{cases} \iff \begin{cases} a^2=1 \\ c^2=1 \\ b(a+c)=0 \end{cases}$$

I. $b=0$

$a^2=c^2$

$a=c$ sau $a=-c$

$\Downarrow a^2=1$.

$a=c=1$ sau $a=c=-1$

II. $a+c=0$

$a=1 \Rightarrow c=-1$

$a=-1 \Rightarrow c=1$

$\det(I_2)=1 \Rightarrow -I_2, \pm\begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}, b\in\mathbb{R}$.

c. $A=\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$, $B=\begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}$ - au ordin 2.

$$AB=\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}:=C$$

$$C^2=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$C^3=\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

$\vdots$

$C^m=\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ (dem. prin ind.)

$$C^{m+1}=\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & m+1 \\ 0 & 1 \end{pmatrix}$$

$C^m=I_2 \iff m=0$

$\det(C)=\infty$.

Ex 4: Fie $G = \{A \in \mathcal{M}_2(\mathbb{Z}) \mid A = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\}$ și $H = \{A \in G \mid A = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}\}$.

a. $(G, \cdot)$ monoid comutativ.

b. $(H, +)$ subgrup al lui $(G, +)$.

c. funcția $f: H \to \mathbb{Q}$, $f\left(\begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}\right) = (-1)^m$ este morfism între grupurile $(H, +)$ și $(\mathbb{Q}^*, \cdot)$.

Rez:

a. $A = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$, $B = \begin{pmatrix} c & 2d \\ d & c \end{pmatrix}$

$$AB = \begin{pmatrix} ac + 2bd & 2ad + 2bc \\ ad + bc & ac + 2bd \end{pmatrix} \in G.$$

$BA = AB$.

Asoc. OK. Elem. neutru: I_2

b. $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $B = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \in H$

$A + B \in H$. OK.

Elem. simetrizabil: $-A \in H$.

c. $f: H \to \mathbb{Q}$, $f(mI_2) = (-1)^m$ morfism între $(H, +)$ și $(\mathbb{Q}^*, \cdot)$.

$A, B \in H$, $A = aI_2$, $B = bI_2$.

$f(A + B) = f(A) \cdot f(B)$.

$f(A + B) = f((a+b)I_2) = (-1)^{a+b}$

$f(A) \cdot f(B) = (-1)^a \cdot (-1)^b = (-1)^{a+b}$

$\operatorname{Im} f = \{-1, 1\}$.

Elem. neutru $\operatorname{Im}(\mathbb{Q}^*, \cdot)$: 1.

$\text{Ker} f = ?$

$\text{Ker} f = \{ A \in H \mid f(A) = 1 \} = \{ aI_2 \mid (-1)^a = 1 \} =$

$= \{ 2k I_2 \mid k \in \mathbb{Z} \} = 2H.$

Teorema fundamentală de izomorfism

$f : G \to H$ morfism $\quad G/\text{Ker} f \simeq \text{Im} f.$

$f : H \to \mathbb{Q}^*$, $\text{Ker} f = 2H$, $\text{Im} f = \{-1, 1\}$.

$H/2H \simeq \{-1, 1\} \simeq \mathbb{Z}_2.$

Obs: Există un izomorfism de grupuri între $(H, +)$ și $(\mathbb{Z}, +)$.

$H/2H \simeq \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_2.$

$\therefore$ În general, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$

Ex: Fie $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(a) =$ restul împărțirii lui a la n, unde $n \in \mathbb{N}$, $n \geq 2$. $\quad f(a) = \hat{a}$.

Arătați că f este morfism de grupuri între $(\mathbb{Z}, +)$ și $(\mathbb{Z}_n, +)$ (endomorfism). Calculați $\text{Im} f$ și $\text{Ker} f$.

Ex. 5: Fie $(S_3, \circ)$ grupul permutărilor.

a. Care sunt subgrupurile (normale) ale lui S_3?

b. Calculați grupurile factor corespunzătoare.

Rez:

$S_3 = \{ e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2) \}.$

a. Subgrupuri: $\{e\}$, S_3, $\langle (1\,2) \rangle$, $\langle (1\,3) \rangle$, $\langle (2\,3) \rangle$, $\langle (1\,2\,3) \rangle = \langle (1\,3\,2) \rangle$

$\langle (1\,2), (1\,3) \rangle = \{ e, (1\,2), (1\,3), (1\,3\,2), (1\,2\,3), (2\,3) \} = S_3$

$H = \langle (1\ 2) \rangle$ nu este normal

$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$

$H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$

$H = \{e, (1\ 2)\}$.

$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$

$(1\ 3)H,\ H,\ (2\ 3)H$

$(S_3/H)_s = \{\hat{e}, (\hat{1}\ 3), (\hat{2}\ 3)\}$.

$|(S_3/H)_d| = |(S_3/H)_d|$

$H = \langle (1\ 2\ 3) \rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$.

$(1\ 2)\ H = \{(1\ 2), (2\ 3), (3\ 1)\}$.

$H(1\ 2) = \{(1\ 2), (2\ 3), (3\ 1)\}$.

H normal.

T. Lagrange: $|S_3| = |H| \cdot |S_3 : H|$

$\Rightarrow |S_3 : H| = 2 \Rightarrow$ H normal

$S_3/H = \{\hat{e}, (\hat{1}\ 2)\}$

$(S_3/H, \circ)$ grup