Seminar 10 – 15.12.2021

Exc: Fie G și H două grupuri, $a \in G$, $b \in H$ de ordin finit, $ord(a) = m$, $ord(b) = n$. Arătați că $ord((a,b)) = [m,n]$, $(a,b) \in G \times H$.

$$\boxed{\text{În } (\mathbb{Z}_n, +),\ ord(\hat{k}) = \frac{n}{(n,k)}.}$$

Ex. 1: Determinați elementele de ordin 4, resp. 6 ale grupului $(\mathbb{Z}_{12} \times \mathbb{Z}_9, +)$

Rez: $(\hat{a}, \bar{b}) \in \mathbb{Z}_{12} \times \mathbb{Z}_9$, $ord(\hat{a}) = m$, $ord(\bar{b}) = n$.

$ord((\hat{a}, \bar{b})) = 4$

$[m,n] = 4 \Rightarrow (m,n) \in \{(4,4), (2,4), (4,2), (1,4), (4,1)\}$

$\hat{a} \in \mathbb{Z}_{12} \Rightarrow ord(\hat{a}) = m \mid 12$

$\bar{b} \in \mathbb{Z}_9 \Rightarrow ord(\bar{b}) = n \mid 9$

$\Rightarrow (m,n) = (4,1)$.

$ord(\hat{a}) = 4$, $\hat{a} \in \mathbb{Z}_{12}$

$4 = \frac{12}{(12, a)} \rightarrow (12, a) = 3 \Rightarrow \hat{a} \in \{\hat{3}, \hat{9}\}$

$a = 3k$, $(k, 4) = 1$.

$ord(\bar{b}) = 1$, $\bar{b} \in \mathbb{Z}_9$. $\Rightarrow \bar{b} = \bar{0}$

Am obținut 2 soluții : $(\hat{3}, \bar{0})$, $(\hat{9}, \bar{0})$

$ord(\hat{a}, \bar{b}) = 6$

$$\left.\begin{array}{l} [m, n] = 6 \\ m \mid 12 , n \mid 9 \end{array}\right\} \Rightarrow (m, n) \in \{(6, 1), (6, 3), (2, 3)\}$$

$[m, n] = 6 \Rightarrow \{(1, 6), (2, 6), (3, 6), (6, 6), (6, 3), (6, 2), (6, 1), (2, 3), (3, 2)\}$

I. $m = 6$, $n = 1$ $\Rightarrow \bar{b} = \bar{0}$.

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

$a = 2k$, $(k, 6) = 1$

$\underline{II}$. $m = 6$, $n = 3$

$m = 6 \Rightarrow \hat{a} \in \{\hat{2}, \hat{10}\}$.

$ord(\bar{b}) = 3 = \frac{9}{(9, b)} \Rightarrow (9, b) = 3 \Rightarrow \bar{b} \in \{\bar{3}, \bar{6}\}$. | 4 perechi

$\underline{III}$. $m = 2$, $n = 3$

$n = 3 \Rightarrow \bar{b} \in \{\bar{3}, \bar{6}\}$.

$m = 2 \Rightarrow ord(\hat{a}) = 2 = \frac{12}{(12, a)} \Rightarrow (12, a) = 6 \Rightarrow \hat{a} = \hat{6}$

Euler: $a^{\varphi(m)} \equiv 1 \mod m$ dacă $(a, m) = 1$.

Fermat: $a^{p-1} \equiv 1 \mod p$ dacă $p \nmid a$, p prim

Ex. 2: Calculați 2020^{2020} în $\mathbb{Z}_{29}$, $\mathbb{Z}_{21}$ și $\mathbb{Z}_{25}$.

a. $\widehat{2020}^{2020}$ în $\mathbb{Z}_{29}$, 29 prim, $29 \nmid 2020$.

$\widehat{2020} = \widehat{19}$. Suntem în condițiile Fermat. $\Rightarrow \widehat{19}^{28} = \hat{1}$

$\hat{19}^{28} = \hat{1}$

$\hat{19}^{2020} = \hat{19}^{28 \cdot c + r} = \hat{19}^{r} = \hat{19}^{4} = (-\hat{10})^{4} = \hat{100}^{2} = \hat{13}^{2} = \hat{169}$
$= \hat{24}$

$\hat{19} = -\hat{10}$

b. $\hat{2020}^{2020}$ în $\mathbb{Z}_{21}$.

$\hat{2020} = \hat{4}$, $(4, 21) = 1 \rightarrow$ Putem aplica Euler.

$\hat{4}^{\varphi(21)} = \hat{1}$, $\varphi(21) = 21\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 12$.

$\hat{4}^{12} = \hat{1}$

$\hat{4}^{2020} = \hat{4}^{4} = \hat{16}^{2} = (-\hat{5})^{2} = \hat{25} = \hat{4}$.

Obs.: $\hat{4}^{3} = \hat{64} = \hat{1}$

c. $\hat{2020}^{2020}$ în $\mathbb{Z}_{25}$

$\hat{2020} = \hat{20}$, $(20, 25) = 5 \neq 1$.

$\hat{20}$, $\hat{20}^2 = \hat{400} = \hat{0}$, $\hat{20}^k = \hat{0}$, $k \geq 2$.

$\hat{2020}^{2020} = \hat{0}$.

Ex. 3: $\hat{9}^{2021}$ în $\mathbb{Z}_{24}$ | $\mathbb{Z}_{30}$.

$(9, 24) = 3 \neq 1$.

$\hat{9}^2 = \hat{81} = \hat{9}$

$\hat{9}^2 = \hat{81} = \hat{21} = -\hat{9}$

$\hat{9}^3 = -\hat{81} = \hat{9}$.

$\hat{2}$ în $\mathbb{Z}_{12}$, $\hat{2}, \hat{4}, \hat{8}, \hat{4}, \hat{8}, \ldots$

$$\hat{2}^{2021} = \underbrace{\hat{2} \cdot \hat{2}^{2020}}_{\hat{8}} = \hat{2} \cdot \hat{4}^{1010} = \hat{8}$$

$5^{2^7} = 5^{128} \not| \; 25^7$

$(5, n) = 1 \leadsto$ Euler

$(5, n) \neq 1 \leadsto$ ca mai sus (c)

Ex. 4: Fie $(S_4, \circ)$, $H = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ subgrup în S_4.

a. Arătați că $H \trianglelefteq S_4$ (subgrup normal)

b. Arătați că $S_4/_H \simeq S_3$.

Rez.: a. $H \trianglelefteq S_4 \iff \sigma H = H \sigma, \ \forall \sigma \in S_4$.

$\sigma H \sigma^{-1} = H, \ \forall \sigma \in S_4$.

$|S_4| = 4! = 24$.

Este suficient să verificăm cond. pt. $\forall \tau \in S_4$, unde τ transpoziție?

$\sigma \in S_4$, $\sigma = \tau_1 \tau_2 \dots \tau_t$, τ_i transpoziții.

„$\circ$" este asoc.

Dacă $\sigma = \tau_1 \tau_2$, τ_1, τ_2 transp. și $\tau_i H \tau_i^{-1} = H$, $i \in \{1,2\}$

$\sigma H \sigma^{-1} = \tau_1 \tau_2 H (\tau_1 \tau_2)^{-1} = \tau_1 \overbrace{\tau_2 H \tau_2^{-1}}^{H} \tau_1^{-1} = \tau_1 H \tau_1^{-1} = H$

Var. 2: Fie $\sigma \in S_4$, $\sigma H \sigma^{-1}$

$\sigma (1\ 2)(3\ 4)\ \sigma^{-1} =$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}^{-1} =$$

$\sigma(1) \to 1 \to 2 \to \sigma(2)$ $\qquad$ $\sigma(3) \to 3 \to 4 \to \sigma(4)$

$\sigma(2) \to 2 \to 1 \to \sigma(1)$ $\qquad$ $\sigma(4) \to 4 \to 3 \to \sigma(3)$

$= (\sigma(1)\ \sigma(2))(\sigma(3)\ \sigma(4)) \in H$, $\forall \sigma \in S_4$

Analog se arată că $\sigma(1\ 3)(2\ 4)\sigma^{-1}$, $\sigma(1\ 4)(2\ 3)\sigma^{-1} \in H$,

$\forall \sigma \in S_4$ $\Rightarrow$ $\sigma H \sigma^{-1} \subseteq H$. $\Rightarrow$ $\sigma H \sigma^{-1} = H$

(au același nr. de elem distincte)

b. S_4/H, $|S_4| = 24$, $|H| = 4$

$\Rightarrow |S_4/H| = 6$.

Th. Lagrange: G grup finit, $H \leq G$

$\Rightarrow |G| = |H| \cdot |G : H|$

" indicele lui H în G $\left(= \left|G/H\right|\right)$

! În particular, $|H| \mid |G|$.

$x \in G$, $\langle x \rangle = H \leq G$

$\left|S_4/H\right| = 6$

grup ciclic, com, are elem. de ord. 6

Obs: $|G| = 6$, G grup $\Rightarrow G \simeq (\mathbb{Z}_6, +)$, $G \simeq (S_3, \circ)$

$\sigma \in S_4$

- $\sigma = e \rightarrow$ ord. 1
- $\sigma = \tau$ transp. $\rightarrow 2$
- σ = ciclu de lungime $3 \rightarrow 3$
- σ = ciclu de lung. $4 \rightarrow 4$
- σ = produs de transp. disjuncte $\rightarrow 2$

$\forall \sigma \in S_4$, $\mathrm{ord}(\sigma) \in \{1, 2, 3, 4\}$.

S_4/H, $\hat{\sigma} \in S_4/H$.

$ord(\hat{\sigma}) = k \iff \hat{\sigma}^k = \hat{e}$, k minim cu această propr.

$\Updownarrow$

$\sigma^k \in H$

Nu există elem. de ord. 6 în S_4.

Nu există elem. de ordin 6 în S_4/H.

Obs: G, H grupuri, $x \in G$ de ordin finit, $ord(x) = n$.

$f : G \to H$ morfism de grupuri

$\Rightarrow (f(x))^n = e_H$ $\quad (ord(f(x)) \mid n)$

(izo $\Rightarrow$ $=$)

$f : S_4 \to S_4/H$, $f(\sigma) = \hat{\sigma}$ morfism de grupuri

$ord(\hat{\sigma}) \mid ord(\sigma)$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \in S_5.$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$$

$$\sigma^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e$$

$$\left.\begin{array}{l} \sigma^6 = e \Rightarrow \operatorname{ord}(\sigma) \mid 6 \\ \sigma, \sigma^2, \sigma^3 \neq e \end{array}\right\} \Rightarrow \operatorname{ord}(\sigma) = 6$$