Seminar 12

16 Dec 2024

ex 1

$\boxed{P_1}$ Fie $(G, \cdot)$ un grup și $x \in G$ $ord(x) = n < \infty$

Atunci $ord(x^k) = \frac{n}{(n, k)}$

Calculați $ord(\overline{31})$ în $(\mathbb{Z}_{100}, +)$

$ord(\overline{96})$ în $(\mathbb{Z}_{100}, +)$

$ord(\overline{32})$ în $U(\mathbb{Z}_{101}, \cdot)$

$ord(\overline{81})$ în $U(\mathbb{Z}_{101}, \cdot)$

Sol:

$(\mathbb{Z}_{100}, +)$

$$\overline{31} = \underbrace{\hat{1} + \hat{1} + \dots + \hat{1}}_{31 \text{ ori}}$$

$ord(\hat{1})$ în $(\mathbb{Z}_n, +)$ este n

$$ord(\overline{31}) = \frac{ord(\hat{1})}{(ord(\hat{1}), 31)} = \frac{100}{(100, 31)} = 100$$

$$\overline{96} = \underbrace{\hat{1} + \hat{1} + \dots + \hat{1}}_{96 \text{ ori}}$$

$$ord(\overline{96}) = \frac{ord(\hat{1})}{(ord(\hat{1}), 96)} = \frac{100}{(100, 96)} = \frac{100}{4} = 25$$

$\widehat{32} = \hat{2}^5$

$(2, 101) = 1 \overset{\text{Euler}}{\Longrightarrow} 2^{\varphi(101)} \equiv 1 \pmod{101}$

$2^{100} \equiv 1 \pmod{101}$

$\Rightarrow$ ord $\hat{2}$ în $U(\mathbb{Z}_{101}, \cdot)$ este un divizor al lui 100

$ord(\widehat{32}) = ord(\hat{2}^5) \overset{\boxed{P_1}}{=} \dfrac{ord(\hat{2})}{(ord(\hat{2}), 5)}$

$101 \mid 2^{100} - 1 = (2^{50} - 1)(2^{50} + 1)$

$$\begin{aligned}
2^{50} &\equiv (2^{10})^5 \pmod{101} \\
&\equiv 1024^5 \pmod{101} \\
& \ 1010 \\
&\equiv 14^5 \pmod{101} \\
&\equiv (14^2)^2 \cdot 14 \pmod{101} \\
&\equiv (-6)^2 \cdot 14 \pmod{101} \\
&\equiv 6 \cdot (-17) \pmod{101} \\
&\equiv -102 \pmod{101} \\
&\equiv -1 \pmod{101}
\end{aligned}$$

$\Rightarrow 2^{50} \equiv -1 \pmod{101}$

$\hat{2}^{50} = -\hat{1}$ în $U(\mathbb{Z}_{101}, \cdot)$

$\Rightarrow ord(\hat{2}) = 100 \Rightarrow U(\mathbb{Z}_{101}, \cdot)$ e grup ciclic generat de $\hat{2}$

$$\operatorname{ord}(\widehat{52}) = \operatorname{ord}(\hat{2}^5) = \frac{\operatorname{ord}(\hat{2})}{(\operatorname{ord}(\hat{2}), 5)} = \frac{100}{(100, 5)} = 20$$

$$\operatorname{ord}(\widehat{81}) = \operatorname{ord}(\hat{3}^4)$$ (! Exc)

Calculați ord $(\hat{3})$ și aplici formula

ex 2

Calculați ord $(\bar{2}, \hat{3})$ în $(\mathbb{Z}_6 \times \mathbb{Z}_{12}, +)$;

î produsul direct al grupurilor $\mathbb{Z}_6$ și $\mathbb{Z}_8$

și elementele de ordin 8 din $(\mathbb{Z}_{32} \times \mathbb{Z}_{62}, +)$

$(\mathbb{Z}_{97} \times \mathbb{Z}_{42}, +)$

---

produsul direct

$\boxed{P_2}$ Fie $(\bar{h}, \hat{\ell}) \in (\mathbb{Z}_n \times \mathbb{Z}_m, +)$

cmmmc

Atunci $\operatorname{ord}(\bar{h}, \hat{\ell}) = [\operatorname{ord}(\bar{h}), \operatorname{ord}(\bar{\ell})]$

Dem

Fie $r = \operatorname{ord}(\bar{h}, \hat{\ell})$, $t = \operatorname{ord}(\hat{h})$ în $(\mathbb{Z}_n, +)$

$s = \operatorname{ord}(\hat{\ell})$ în $(\mathbb{Z}_m, +)$

$[t, s] = u$

$u = t \cdot t_1$

$u = s \cdot s_1$

$t \cdot s = [t, s] \cdot (t, s)$

$$s = s_1 \cdot (t, s)$$

$$t = t_1 \cdot (t, s)$$

$$\Rightarrow \quad (s_1, t_1) = 1$$

$$n \cdot (\bar{h}, \hat{l}) = \underbrace{(\bar{h}, \hat{l}) + \ldots + (\bar{h}, \hat{l})}_{n \text{ ori}} = (n \cdot \bar{h}, n \cdot \hat{l})$$

$$= (t_1 \cdot t \cdot \bar{h}, \; s_1 \cdot s \cdot \hat{l})$$

$$= (t_1 \cdot \overline{th}, \; s_1 \cdot \widehat{sl})$$

$$= (t_1 \cdot \bar{0}, \; s_1 \cdot \hat{0})$$

$$= (\bar{0}, \hat{0}) \qquad (1)$$

Fie $v \in \mathbb{N}^*$ a.î. $v \cdot (\bar{h}, \hat{l}) = (\bar{0}, \hat{0})$

$$\Rightarrow \quad (v \cdot \bar{h}, \; v \cdot \hat{l}) = (\bar{0}, \hat{0})$$

$$\Rightarrow \quad \begin{array}{l} v \cdot \bar{h} = 0 \\ v \cdot \hat{l} = 0 \end{array} \quad \overset{\text{vezi curs}}{\Rightarrow} \quad \begin{array}{l} \operatorname{ord}(\bar{h}) \mid v \\ \operatorname{ord}(\hat{l}) \mid v \end{array} \quad \Rightarrow$$

$$\underbrace{[\operatorname{ord}(\bar{h}), \operatorname{ord}(\hat{l})]}_{\parallel \; n} \mid v$$

$$\Rightarrow \quad n \mid v \qquad \Rightarrow \quad n \leq v \qquad (2)$$

Din (1) și (2) $\Rightarrow \quad r = \operatorname{ord}(\bar{h}, \hat{l}) = n$

$\text{ord}(\bar{2}, \hat{3})$ în $(\mathbb{Z}_6 \times \mathbb{Z}_{12}, +)$

$\|$

$[\text{ord}(\bar{2}), \text{ord}(\hat{3})] = [3, 4] = 12$

$\text{ord}(\bar{2})$ în $(\mathbb{Z}_6, +)$

$\|$

$\dfrac{\text{ord}(\bar{1})}{(\text{ord}(\bar{1}), 2)} = \dfrac{6}{(6, 2)} = \dfrac{6}{2} = 3$ $\swarrow$ sau

$\bar{2} \neq \hat{0}$

$\bar{2} + \bar{2} = \bar{4} \neq 0$

$\bar{2} + \bar{2} + \bar{2} = \bar{6} = 0$

$\text{ord}(\hat{3})$ în $(\mathbb{Z}_{12}, +)$

$\|$

$\dfrac{12}{(12, 3)} = 4$

b) deci $\exists\ \bar{k}, \hat{l}$ a.î. $\text{ord}(\bar{k}, \hat{l}) = 8$?

$\|$

$[\text{ord}(\bar{k}), \text{ord}(\hat{l})] = 8$

$\Rightarrow$ $\text{ord}(\bar{k}) = 8$ sau $\text{ord}(\hat{l}) = 8$

$\bar{k} \in (\mathbb{Z}_n, +)$ $\Bigg|\Rightarrow$ $8 \mid n$

În $(\mathbb{Z}_{97} \times \mathbb{Z}_{42}, +)$ nu avem elemente de ordin 8 deoarece $8 \nmid 97$ și $8 \nmid 42$

În $(\mathbb{Z}_{32} \times \mathbb{Z}_{62}, +)$ avem $\underline{8 \mid 32}$ și $\underline{8 \nmid 62}$

$\Rightarrow$ elementele de ordin 8 vor fi $(\bar{k}, \hat{l})$ cu $\text{ord}(\bar{k}) = 8$ și $\text{ord}(\hat{l}) < 8$

$[\,ord(\bar{h}),\ ord(\hat{\ell})\,] = 8$

$ord(\bar{h}) = 8$

$ord(\hat{\ell}) < 8$

$\Rightarrow \begin{cases} ord(\bar{h}) = 8 \\ ord(\hat{\ell}) = 1 \end{cases}$

sau

$\begin{cases} ord(\bar{h}) = 8 \\ ord(\hat{\ell}) = 2 \end{cases}$

$\cancel{\begin{cases} ord(\bar{h}) = 8 \\ ord(\hat{\ell}) = 4 \end{cases}}$

deoarece $4 \nmid 62$

Elementul de ordin 1 din $(\mathbb{Z}_{62}, +)$ este $\hat{0}$

Elementele de ordin 2 din $(\mathbb{Z}_{62}, +)$ este $\widehat{31}$

$$ord(\hat{\ell}) = \frac{62}{(62, \ell)} = 2 \Rightarrow (62, \ell) = 31$$

$$\Rightarrow \hat{\ell} = \widehat{31}$$

Elementele de ordin 8 din $(\mathbb{Z}_{32}, +)$ sunt $\{\bar{4}, \overline{12}, \overline{20}, \overline{28}\}$

$$\frac{32}{(32, h)} = ord(\bar{h}) = 8 \quad \Rightarrow \quad (32, h) = 4$$

$$\Rightarrow h \in \{4\cdot 1, 4\cdot 3, 4\cdot 5, 4\cdot 7\}$$

$\Rightarrow$ Avem 8 elemente de ordin 8 în $(\mathbb{Z}_{32} \times \mathbb{Z}_{62}, +)$

$(\hat{4}, \hat{0})$, $(\hat{4}, \widehat{31})$ $(\hat{8}, \hat{0})$, $(\hat{8}, \widehat{31})$

etc

La EXAMEN !

Grupul $(S_n, \cdot)$

- grup neabelian dacă $n \geq 3$

$\sigma \in S_n$

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

$|S_n| = n!$

$$S_3 = \left\{ \underset{= e}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}, \underset{= (1\,2\,3)}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}, \underset{= (1\,3\,2)}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}, \underset{= (1\,2)}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}, \underset{= (1\,3)}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}, \underset{= (2\,3)}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}} \right\}$$

î transpoziție

Ciclu de lungime m $(\leq n)$ din S_n se notează

$(i_1 \; i_2 \; i_m) = \sigma$ a.î.

are ordinul $= m$ (lungimea sa)

$\sigma(j) = j \quad \forall j \notin \{i_1, i_2, \dots, i_m\}$

$\sigma(i_1) = i_2$

$\sigma(i_2) = i_3$

...

$\sigma(i_{m-1}) = i_m$

$\sigma(i_m) = i_1$

$\boxed{\text{Th}}$ Orice permutare se descompune în mod unic în produs de cicluri disjuncte

Două cicluri $(i_1, i_2, \dots, i_m)$ $(j_1, j_2, \dots, j_l)$ sunt disjuncte $\Leftrightarrow$ $\{i_1, i_2, \dots, i_m\} \cap \{j_1, j_2, \dots, j_l\} = \emptyset$

$$\text{ord}(\sigma) = [\,\text{ord}(\sigma_{i_1}), \dots, \text{ord}(\sigma_{i_r})\,]$$

$$\sigma = \sigma_{i_1} \cdots \sigma_{i_r}$$

descompunerea în produs de cicluri disjuncte

ex 2

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 7 & 3 & 4 & 8 & 14 & 13 & 6 & 10 & 5 & 12 & 1 & 2 & 5 & 9 & 11 & 16 \end{pmatrix} \in S_{16}$$

$$= (1\ 7\ 6\ 13\ 5\ 14\ 9\ 15\ 11)\ (2\ 3\ 4\ 8\ 10\ 12)\ (16)$$

$$\text{ord}(\sigma) = [9, 6] = 18$$

ex 3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 9 & 5 & 7 & 10 & 3 & 4 & 6 & 1 & 8 \end{pmatrix} \in S_{10}$$

$$= (1\,2\,9)\,(3\,5\,10\,8\,6)\,(4\,7)$$

$$\text{ord}(\sigma) = [3, 5, 2] = \underline{30}$$

ex 4

Det el de ordin 8 din S_7

Tony Cris?

$$\underbrace{(i_1, i_2, \dots, i_m)}_{\varepsilon} = (i_1\,i_2)\,(i_2\,i_3)\cdot\ldots\cdot(i_{m-1}, i_m)$$

ε signatura unui ciclu

$$\varepsilon((i_1, i_2, \dots, i_m)) = \varepsilon((i_1, i_2))\cdot\ldots\cdot\varepsilon((i_{m-1}, i_m)) = (-1)^{m-1}$$

$$\varepsilon((i, j)) = -1$$

---

ex 5

Se consideră permutarea

1) Descomp. σ în produs de cicluri disjuncte și în produs de transpoziții

2) Aflați $\varepsilon(\sigma)$ și calculați σ^{-2024}, ordin (σ), σ^{-1}

3) Det toate permutările $\tau \in S_n$ a.î. $\tau^2 = \sigma$

4) Fie $\rho \in S_{10}$ cu $ord(\rho) = 10$. Poate fi ρ permutare pară?

5) Există permutări de ordin 35 în S_{10}? Dar de 30?

Sol:

1) b) $\underbrace{(1\ 2\ 9)}_{\sigma_1}\ \underbrace{(3\ 5\ 10\ 8\ 6)}_{\sigma_2}\ \underbrace{(4\ 7)}_{\sigma_3}$

$\sigma = (1\ 2)(2\ 9)(3\ 5)(5\ 10)(10\ 8)(8\ 6)(4\ 7)$

2) $\varepsilon(\sigma) = (-1)^{\text{nr. transpoziții din-o descomp. a lui } \sigma} = (-1)^7 = -1$

$ord(\sigma) = [3, 5, 2] = 30$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 1 & 6 & 7 & 3 & 8 & 4 & 10 & 2 & 5 \end{pmatrix}$$

$\sigma^{-2024} = (\sigma^{-1})^{2024}$

sau

$= (\sigma^{2024})^{-1}$

$$\sigma^{2024} = (\sigma_1\ \sigma_2\ \sigma_3)^{2024} \underset{\substack{\text{ciclurile}\\ \text{disjuncte}\\ \text{comută}}}{=} \sigma_1^{2024} \cdot \sigma_2^{2024} \cdot \sigma_3^{2024}$$

$\operatorname{ord}(\sigma_1) = 3$

$\operatorname{ord}(\sigma_2) = 5$

$\operatorname{ord}(\sigma_3) = 2$

$$= \sigma_1^{3\cdot\smile+2} \cdot \sigma_2^{5\cdot\smile+4} \cdot (\sigma_3^{2})^{1012}$$

$$= \sigma_1^{2} \cdot \sigma_2^{4} \cdot e$$

$$\Rightarrow \sigma^{2024} = \sigma_1^{2} \cdot \sigma_2^{4} = \sigma_1^{-1} \cdot \sigma_2^{-1}$$

$$= \begin{pmatrix} 1 & 2 & 5 \\ 5 & 1 & 2 \end{pmatrix} \left(\;\ldots\; \right)$$

Etc

$$\| $$

$$(1\ 5\ 2)$$

e compunerea a 2 permutări

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 2 & 6 & 5 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 1 & 4 & 3 & 2 & 6 \end{pmatrix}$$

$$\sigma \circ \tau$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$

$$(\sigma \circ \tau)(1) = \sigma(\tau(1))$$