Algebră #12

- criptosc Vigenere (altă temă)
  - engleză
  - franceză
  - germană
  - italiană
  - spaniolă

  - lungime cuv ≤ 4
  - cheia mode mesaj sens (ex. XYZ)

Grupul de permutări

$\sigma, \tau \in S_n \quad \exists x \in S_n$

Încă condiția există alte permutări a.î. $x \sigma x^{-1} = \tau$?

Există x, dacă și numai dacă σ și τ au același tip de descompunere:

Știm că orice permutare se descompune în produs de cicli disjuncți

$\sigma = (a_1, a_2, \dots, a_{k_1})(b_1, b_2, \dots, b_{k_2}) \dots (x_1, x_2, \dots, x_{k_s})$

Tipul de descompunere = lista lungimilor ciclilor =

$= k_1, k_2, \dots, k_s \quad \left(\sum_{i=1}^{s} k_i = n \right)$

Ex $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 7 & 6 & 8 \end{pmatrix} = (1,2,3)(4,5)(6,7)(8)$

$3 \quad 2 \quad 2 \quad 1$

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 1 & 2 & 6 & 4 & 8 \end{pmatrix} = (1,3,7,4)(2,5)(6)(8)$

$4 \quad 2 \quad 1 \quad 1$

Scanned by CamScanner

cele 2 liste au același, dacă au aceeași descompu

τ, σ sunt permutări conjugate

$\Rightarrow$ " $\chi \sigma \chi^{-1} = \tau \Rightarrow \tau$ și σ au aceeași descompu

$\sigma = (a_1, a_2, \dots a_{k_1})(b_1, b_2, \dots, b_{k_2}) \dots (x_1, x_2, \dots, x_{k_s})$

$\chi \sigma \chi^{-1} = \boxed{\chi (a_1, a_2, \dots, a_{k_1}) \chi^{-1}} \chi^{-1} (b_1, b_2, \dots b_{k_2}) \dots$

$\cdot \chi^{-1} \chi (x_1, x_2, \dots x_{k_s}) \chi^{-1}$

$\chi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ & & & & \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_{k_1} & \dots \\ m_1 & m_2 & \dots & m_{k_1} & \dots \end{pmatrix}$

// mulțea schimbărilor de ordine

Calculez $\chi (a_1, a_2, \dots, a_{k_1}) \chi^{-1} = (m_1, m_2, \dots, m_{k_1})$

$\left(\chi (a_1, a_2, \dots, a_{k_1}) \chi^{-1} \right) (m_1) = \left(\chi (a_1, a_2, \dots, a_{k_1}) \right) (a_1)$

$= (\chi)(a_2) = m_2$

$\left(\chi (a_1, a_2, \dots, a_{k_1}) \chi^{-1} \right) (j) = \left(\chi (a_1, a_2, \dots, a_{k_1}) \right) (\chi^{-1}($

dacă $j \notin \{m_1, m_2, \dots m_{k_1}\}$ $\chi^{-1}(j) \neq a_t, \forall t \in \overline{1, k_1}$ $\Rightarrow \chi \chi^{-1}(j) = j$

Scanned by CamScanner

Reciproca σ și τ au aceeași descompunere $\Rightarrow \exists X \in S_n$

a.î. $X \sigma X^{-1} = \tau$ " "

$\sigma = (\dots)$

$\tau = (a_1, a_2, \dots, a_{k_1})(d_1, d_2, \dots, d_{k_2}) \dots$

$\text{Alg } X = \begin{pmatrix} a_1, a_2, \dots a_{k_1} & b_1 b_2 \dots b_{k_2} \dots \\ c_1 c_2 \dots c_{k_1} & d_1 d_2 \dots d_{k_2} \dots \end{pmatrix}$

Calculez $(X \sigma X^{-1})(c_1) = X \sigma(a_1) = X(a_2) = c_2$

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = (12)(345)$

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (24)(135)$

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

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

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

3/

Scanned by CamScanner

Spunem că $x, y \in G$ sunt conjugate $(\sim) \exists g \in$

$gxg^{-1} = y$, $(G, \cdot)$ grup

Noțiunea e interesantă în cazul grupurilor necomutative

$$C_x = \{ \cancel{g \in G \mid gxg^{-1} \in} \quad gxg^{-1} \mid g \in G \}$$ orbita lui x

- mulțimea elementelor conjugate lui x

Obs. $C_x = C_y$ sau $C_x \cap C_y = \emptyset$

Pp că $C_x \cap C_y \neq \emptyset$

$g_1, g_2 \in G$ a.î. $g_1 x g_1^{-1} = g_2 y g_2^{-1}$ (2)

(2) $x = g_1^{-1} g_2 y g_2^{-1} g_1 = h y h^{-1}$

$(ab)^{-1} = b^{-1} a^{-1}$ / $(g_1^{-1} g_2)^{-1} = g_2^{-1} g_1$

$x \in C_x \Leftrightarrow x = gxg^{-1}$ (2) $y = g h y h^{-1} g^{-1}$ (2)

(2) $y = (gh)\, y\, (h^{-1} g^{-1}) \in C_y$ 2) $C_x = C_y$

$t \in C_y$ $t = gyg^{-1} = g(h^{-1} x h) g^{-1} = (gh^{-1}) x (hg^{-1})$

$\in C_x$

2) $C_x = C_y$

4/

Scanned by CamScanner

Ecuația claselor de conjugare

$\exists\ x_1, x_2, \dots, x_n \in G$ a.i. $G = \bigcup_{i=1}^{n} Cx_i$

Întrebare

$x \in Gx$ (întotdeauna)

când $|Cx| = 1$ ($\Leftrightarrow$) $Cx = \{x\}$

$gxg^{-1} = x$ ($\Leftrightarrow$) $gx = xg, \forall g \in G$

Def $Z(G)$ - centrul grupului

$Z(G) = \{x \mid xy = yx \ \forall y \in G\}$

- toate elementele grupului care comută cu toate

Ex $Z(G) \trianglelefteq G$

Fie $y \in Z(G)$ $\Leftrightarrow$ $y \in xZ(G)x^{-1}$ ($\Leftrightarrow$)

$\Leftrightarrow$ $y = xzx^{-1}$ ($\Leftrightarrow$) z

$$|G| = |Z(G)| + \sum_{|Cx_i|>1} |Cx_i|$$

$Gx = \{g \in G \mid gxg^{-1} = x\}$

Ex: $Gx \leq G$

$$|Cx| = \frac{|G|}{|Gx|}$$

5/

Scanned by CamScanner

$(G,\cdot) = (S_n, \circ)$

(4)
(3,1)
(2,2)
(2,1,1)
(1,1,1,1)

$|S_4| = 4! = 24$

$Z(S_4) = ? = \{e\}$

1 _ _ _

3!

Câți cicli de lungime 4 = 3!

$|S_4| = 6 + 8 + 3 + 6 + 1$

Câți cicli de lungime 3 = 8

Câți de lungime 2

p nr prim $(G,\cdot)$ grup $|G| = p^2 \Rightarrow$ G comutativ și

$(G,\cdot) \simeq (\mathbb{Z}_{p^2}, +)$

$G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$

$|G| = |Z(G)| + \sum \frac{|G|}{|G_x|} = p^2$

G comutativ $\Rightarrow Z(G) = G$

$Z(G) \trianglelefteq G \Rightarrow |Z(G)| \mid p^2 \Rightarrow Z(G) \in \{1, p, p^2\}$

6/

Scanned by CamScanner

$\frac{|G|}{|C_G(x_i)|} = \frac{p^2}{|C_G(x_i)|} \in \{p, p^2\} \Rightarrow |C_G(x_i)| \in \{p, p^2\}$

Orice grup cu p elemente e ciclic
$H \leq (\mathbb{Z}_p, +)$

$|Z(G)| \geq p \Leftrightarrow Z(G) = \{h^i \mid i \in \overline{0, p-1}\}$ ord $h = p$

$Z(G) \trianglelefteq G$

$\left|\frac{G}{Z(G)}\right| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p \Rightarrow \frac{G}{Z(G)} \simeq (\mathbb{Z}_p, +)$

$\Rightarrow \exists b \in G$ a.i. $\frac{G}{Z(G)} = \{\hat{b}^i \mid i \in \overline{0, p-1}\}$

$x, y \in G \quad \hat{x} \in \frac{G}{Z(G)} \Rightarrow \hat{x} = \hat{b}^i \Rightarrow x = b^i u$

$\hat{y} \in \frac{G}{Z(G)} \Rightarrow \hat{y} = \hat{b}^j \Rightarrow y = b^j v$

$xy = b^i u b^j v = b^{i+j} uv$

Teorema lui Cauchy $(G, \cdot)$ grup finit, p prim $p \mid |G| \Rightarrow \exists g \in G$, a.i. ord $g = p$

$\square\!\!\!\!\!\!\square$

Scanned by CamScanner