10.04.2013г.

среда

Упражнение

$\boxed{\text{За Контролно}}$: симетр. ~~полиноми~~ оператор
Числови сравнения от I степен
Ферма, Ойлер
зад. от групи

зад. G-група; $a, b \in G$, $ab = ba$
$|a| = r$
$|b| = s$

а) Док, че ако $(r,s) = 1 \Rightarrow |ab| = r.s$

$|ab| = t$

$\boxed{?\ t / rs \text{ и } rs / t \Rightarrow t = rs}$

$(ab)^{rs} = a^{rs} \cdot b^{rs} = (a^r)^s \cdot (b^s)^r = 1 \Rightarrow t / rs$

$1 = (ab)^t = a^t \cdot b^t = a^{ts} \cdot b^{ts}$
$\Rightarrow a^{ts} = 1$
r / ts, но $(r,s) = 1$
$\Rightarrow r / t$

Аналог., $\underset{\underset{1}{\|}}{a^{tr}} \cdot b^{tr} = 1$

$\Rightarrow b^{tr} = 1 \Rightarrow s / tr$, но $(r,s) = 1$
$\Rightarrow s / t$

s / t и $r / t \Rightarrow sr / t$

б) ? в G има елемент от ред
$[r,s] \to$ НОК на r и s

$[r,s] = \dfrac{r.s}{(r,s) = d}$ $\quad r = d.r_1$
$s = d.s_1$
$(r_1, s_1) = 1$

$(ab)^{rs} = 1$

$|ab| = t$, t / rs

$1 = (ab)^t = a^t b^t = a^{ts}$

r / ts
r_1 / ts_1 $\quad 1 = (ab)^t = a^t b^t = a^{tr}$

$s / tr \Rightarrow s_1 / tr_1 \Rightarrow r_1 s_1 / t$

$t / r_1 s_1 d^2$ $\quad (r_1, s_1) = 1$

$r = p_1^{\alpha_1} \dots p_n^{\alpha_n}$
$s = p_1^{\beta_1} \dots p_n^{\beta_n}$
$[r,s] = p_1^{\gamma_1} \dots p_n^{\gamma_n}$

$\gamma_i = \max(\alpha_i, \beta_i)$

$\exists k : |a^k| = p_i^{\gamma_i}$ или $|b^k| = p_i^{\gamma_i}$, т.е.

$\exists\ c_i \in G:$

$|c_i| = p_i^{\gamma_i}$

Но $(p_i, p_j) = 1,\ i \neq j$

$\Rightarrow$ от а) $\Rightarrow\ \exists\ c$ в G:

$$c = \prod_{i=1}^{n} c_i$$

$|c| = [r.s]$

$$\boxed{\begin{array}{l} |a| = r \\ |a^k| = \dfrac{r}{(k,r)} \end{array}}$$

<u>Зад.</u> G - крайна група и $|G| = 2k$, $k \in \mathbb{N}$

ДСД, че в G има елемент g: $|g| = 2$

$\{a, a^{-1}\} \in G$; $1 \in G$ - правят нечетен брой елементи от $G \Rightarrow$

$\Rightarrow \exists g^{\neq 1} \in G: g = g^{-1} \Rightarrow g^2 = 1$

<u>Зад</u> G - група $\exists!\ a \in G: |a| = 2$

Док., че a комутира с $\forall$ ел. на G

$\overset{?}{-}\ \forall g \in G\ \ ag = ga$

$$! \boxed{|a| = |g^{-1} \cdot a \cdot g|} \rightarrow \text{за произволна група (от предна задача)}$$

$2 = |a| = |g^{-1} \cdot a \cdot g|$

$a = g^{-1} \cdot a \cdot g$

$ga = ag$

<u>Зад.</u> G - група, $\forall g \neq 1\ \ g \in G: |g| = 2$

ДСД, че G е абелева

$a, b \neq 1 \in G$

$|a| = 2$ и $|b| = 2$ $\quad |ab| = 2$

$a = a^{-1} \quad b = b^{-1} \Rightarrow (ab) = (ab)^{-1} = \underset{\overset{\parallel}{b}}{b^{-1}}\ \underset{\overset{\parallel}{a}}{a^{-1}}$

<u>Зад.</u> Q_8, D_4 ? редовете на елементите на двете групи

$Q_8 = \{\pm 1; \pm i, \pm j, \pm k\}$

$i^2 = j^2 = k^2 = -1$

$i \cdot j = -j \cdot i = k$

$j \cdot k = -k \cdot j = i$

$ki = -i \cdot k = j$

1 - единичен ел.

$|-1| = 2$

$|\pm i|, |\pm j|, |\pm k| = 4$

$$\boxed{\begin{aligned} &D_4 = \{A^i B^j \mid i = 1, \dots 4; j = 1, 2\} \\ &B^{-1} \cdot A \cdot B = A^{-1} \end{aligned}}$$

$|A| = n = 4$

$|B| = 2$ $\quad |A^2 B| = 2 \quad |A^3 B| = 2$

$|AB| = 2 \quad |A^3| = 4$

$|A^2| = 2$

$\forall A$

$(AB)^2 = A\underbrace{BA}_{A^{-1}}B = E \quad , B = B^{-1}$

$\Rightarrow |AB| = 2$

$A^3 B = A^{-1} B = B^{-1} A = B . A$

$\Rightarrow |A^3 B| = 2$

$|A^2 B| = 2$

$$\boxed{* \; A^i B^j A^k B^l = A^{i + k(-1)^j} B^{j+l}}$$

Циклични групи

$\langle g \rangle = \{g^0, g^{\pm 1}, g^{\pm 2} \dots\}$ - Групата е цикл., ако $\forall$ са дна някоя степен

Зад. Дсд, че $\mathbb{Z}$ безкрайна циклична има точно 2 пораждащи елемента

$| C_n \; \mathbb{Z}_n$

$\mathbb{Z} = \langle 1, -1 \rangle$

$C_n = \{z \in \mathbb{C} \mid z^4 = 1\}$

$\omega_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \quad , k = 0, 1, \dots, n-1$

$\omega_1^k = \omega_k$

$\exists\; \varphi(n)$ - бр. числа, $< n$, взаимно прости с n

$|\omega_1| = n$, то от $\omega_k = \omega_1^k \Rightarrow$

ако $(k, n) = 1 \Rightarrow |\omega_k| = |\omega_1^k| = n$
$k < n$

Пример C_4

$\omega_2 = \cos \frac{4\pi}{4} + i \sin \frac{4\pi}{4} \Rightarrow \omega_2^2 = \cos 2\pi + i \sin 2\pi = 1$

$\Rightarrow$ пор. елем на C_n са $\varphi(n)$ на брой

Зад. Да се опр. $\forall$ подгрупи на гр. G

а) $G = \mathbb{C}_8$

б) $G = \mathbb{C}_{12} = \{e, g, g^2, g^3, \dots, g^{11}\}$

$\boxed{\text{* подгрупа на циклична е циклична}}$

$\{E\}$, G - тривиалните подгр.

g, g^5, g^7, g^{11} - взаимнопрости с $12 \Rightarrow$ не могат да участват в подгрупа (пораждат цялата)

$\rightarrow |g^2| = 6$

$\{e, g^2, g^4, g^6, g^{10}\}$ - поражд. се от $g^2 = \langle g^2, g^{10} \rangle$

$\searrow$ е група и $= \mathbb{C}_6$

$\rightarrow |g^3| = 4$

$\{e, g^3, g^6, g^9\} = \mathbb{C}_4 = \langle g^3, g^9 \rangle$

$\rightarrow |g^4| = 3$

$\{e, g^4, g^8\} = \mathbb{C}_3 = \langle g^4, g^8 \rangle$

$\rightarrow |g^6| = 2$

$\{e, g^6\} = \mathbb{C}_2 = \langle g^6 \rangle$

Включванията:

$$
\begin{tikzcd}
 & G = \mathbb{C}_{12} \arrow[dl] \arrow[dr] & \\
C_6 \arrow[d] \arrow[drr] & & C_4 \arrow[d] \\
C_3 \arrow[dr] & & C_2 \arrow[dl] \\
 & \{E\} &
\end{tikzcd}
$$

формула на графита

в) $G = \mathbb{C}_n$

$C_d \leq \mathbb{C}_n \quad d/n$

$\varphi(n)$ - пораждащи

г) $G = \mathbb{Z}$

подгрупи: $n\mathbb{Z}$, $n \in \mathbb{N}$

$n_1\mathbb{Z} \leq n_2\mathbb{Z}$, n_2/n_1

$6\mathbb{Z} \leq 3\mathbb{Z}$

Зад. ? бр. на решенията на $x^d = 1$. бр. елем. от ред d в гр. $\mathbb{C}_n$?

а) $n = 12$, $d = 6$

$|\omega_2| = |\omega_{10}| = 6$

$x^6 = 1$ за $\mathbb{C}_{12}$ | $\mathbb{C}_6$ - $\forall$ елем. са реш. на $x^6 = 1$

$\omega_k^n = 1$

$(k, n) = 1 \Rightarrow |\omega_k| = n$

$(k, n) = d \neq 1 \Rightarrow |w_k| = \frac{n}{d}$

б) $n = 100;\ d = 20$

в) $n, d \in \mathbb{N},\ d | n$

$\boxed{\text{Симетрична група}}$

$\Omega_n = \{1, 2, \ldots, n\}$ - пермутация на числата от $1..n$

$|S_n| = n!$

→ композиция - операцията в групата

$i_1, i_2, \ldots i_n$

$$\left.\begin{aligned} \sigma \in S_n : \ & \sigma(i_1) = i_2 \\ & \sigma(i_2) = i_2 \\ & \vdots \\ & \sigma(i_{k-1}) = i_k \\ & \sigma(i_k) = i_1 \end{aligned}\right\} \text{цикъл}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$$

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

$\sigma = (i_1, \ldots, i_k)$

$g \in S_n$

$\sigma = (i_1, \ldots, i_k)$

$\beta = (j_1, \ldots j_s)$

$\sigma g = g\sigma$

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

?

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

зад. ДСД, че $\forall$ перм. в S_n

$\forall \sigma \in S_n,\ !\,\sigma = \sigma_1, \sigma_2, \ldots \sigma_k$

$\sigma_i \cap \sigma_j = \{\emptyset\}$

Нека k е най-голямото ест. число, за което

$\sigma_1, \sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \ldots \sigma(i_{k-1}) = i_k$

$\sigma(i_k) = i_j \quad j \neq 1$

$\Rightarrow \sigma(i_k) = \sigma(i_{j-1}) - \text{x} \Rightarrow \sigma(i_k) = i_1$

$\sigma = \sigma_1\sigma_2 \ldots \sigma_k = \sigma_1' \ldots \sigma_s'$

$i_1 \in \sigma_1$

$\in \sigma_i' \Rightarrow \sigma_1 = \sigma_i'$

Зад. ДСД, че в гр. S_n:

а) редът на цикъл = дължината му

$\sigma = (i_1, i_2, \dots, i_n)$

$$\left.\begin{array}{ll} & i_1, \dots, i_n \\ \sigma & i_2, i_3, \dots i_1 \\ \sigma^2 & i_3\ i_4 \dots i_2 \\ \vdots & \\ \sigma^n & i_1, i_2, \dots, i_n \end{array}\right] \quad (i_1)(i_2)\dots(i_n) = (1)$$

пр.: $(12)^2 = (1)$ $\quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

(123) 123

$(123$ 231

(123) 312

123

б) $\rho \in S_n \quad \rho = \sigma_1 \sigma_2 \dots \sigma_n$

$|\rho| = [r_1, r_2, \dots, r_n]$, ако $|\sigma_i| = r_i$

$|\rho| = t$

$(1) = \rho^t = \sigma_1^t \sigma_2^t \dots \sigma_n^t$

$\Rightarrow r_i \mid t \quad i = 1, \dots, n$

$\Rightarrow$:))

Зад. $\sigma, \rho \in S_n$ ДСД:

а) $\sigma = (i_1, i_2, \dots, i_k)$

$\rho\sigma\rho^{-1} = (\rho(i_1)\ \rho(i_2) \dots \rho(i_k))$

$\rho(i_1)\rho(i_2) \dots \rho(i_k)$ ||

$$\begin{array}{l|l} \rho^{-1} & i_1\ i_2 \dots i_k \\ \sigma & i_2\ i_3 \dots i_1 \\ \rho & \rho(i_2) \dots \rho(i_1) \end{array}$$

б) $\sigma\ (i_1, \dots, i_k) \dots (j_1 \dots j_s)$

$\rho\sigma\rho^{-1} = (\rho(i_1) \dots \rho(i_k) \dots \rho(j_1) \dots \rho(j_s))$

$\rho\sigma\rho^{-1} = \rho(i_1, \dots, i_k) \dots (j_1 \dots j_s)\rho^{-1} =$

$= \rho(i_1, \dots, i_k)\rho^{-1}\rho(\dots)\rho^{-1}\rho(\dots)\dots$

$\rho(j_1 \dots j_s)\rho^{-1}$

Зад. ДСД, че в гр. S_n 2 пермут. ρ и $\tilde{\tau}$ са спрегнати $\Leftrightarrow$ $\boxed{\tau = \rho\tilde{\tau}\rho^{-1}}$, $\rho \in S_n$

Пример: $\sigma = (123)$

$\rho = (13)$

$\rho\sigma\rho^{-1} = ? \quad (\rho(1)\rho(2)\rho(3)) = (321)$

II н. (123) 123

$$\left.\begin{array}{ll} \rho^{-1} = (13) & 321 \\ \sigma = (123) & 132 \\ \rho = (13) & 312 \end{array}\right] = (132)$$

~~(32)(123) = (~~

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

Зад. ДСД, че в гр. S_4:

а) $\forall$ перм. се разлага в произв. на непрш. незав. транспозиции (цикъл с дължина 2)

$\sigma = (i_1, i_2, \dots, i_k)$

$\sigma(i_1) = i_2, \dots \sigma(i_k) = i_1$

$$\left.\begin{array}{ll} & i_1, \dots i_k \\ (i_1, i_2) & i_2 i_1 \dots i_k \\ (i_1, i_3) & i_2 i_3 i_1 \dots i_k \\ \vdots & \\ (i_1, i_k) & i_2 i_3 \dots i_1 \end{array}\right] \quad \begin{array}{l}(i_1, i_2, \dots i_k) = \\ = (i_1, i_k)(i_1, i_{k-1}) \dots (i_1, i_2)\end{array}$$

б) ? бр. множ. $\sqrt{}$ в едно разлаг. на транспоз. е четност = четността на пермутацията

Пример: $\left.\begin{array}{l} 1\ 2 \dots i \dots j \dots n \\ 1\ 2 \dots j \dots i \dots n \end{array}\right\} \longrightarrow$

бр. на инв. е $2(i-j-1)+1$ - нечетно

в) цикъл е четна (нечетна) пермут., точно когато дълж. му е нечетно (четно) число

$\boxed{\text{An - множ. от четни пермут. (алтернативна група)}}$

Зад. ДСД, че $A_n \leq S_n$ и $|A_n| = \frac{1}{2} n!$, $n \geq 2$

$\sigma, \rho \in A_n$

$\sigma = (i_1, i_2, \dots, i_k) \dots (j_1 \dots j_s) =$

$= \underbrace{(i_1, i_k) \dots (i_1, i_2) \dots (j_1 j_s) \dots (j_1 j_2)}_{2t}$

$\rho = \dots = 2r$ - транспозиции

$\rightarrow \Theta\ \sigma.\rho = 2(\dots) \Rightarrow$ четна пермут.

$\rightarrow (id) \rightarrow$ четна пермут.

$\rightarrow$ обратна на четна трансп. е също четна $\Rightarrow A_n$ е група

$A_n \leq S_n$