~ВА~ 10.04.2013 г.

симетр. полиноми
числови сравнения от I ст.
Ферма, Ойлер
зад. от групи

} за контролното

Зад.1 G – група; $a, b \in G$, $ab = ba$

$|a| = r$

$|b| = s$

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

$|a.b| = t$

$t \mid r.s$ и $\underbrace{r.s \mid t}_{\text{защото комутират}}$ } $\Rightarrow t = r.s$ → начин на р-ие

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

$1 = (ab)^t = a^t . b^t = a^{ts} . \underset{1}{b^{ts}} \Rightarrow a^{ts} = 1$ $\quad r \mid t.s$, но $(r, s) = 1$

$\Rightarrow r \mid t$

$\underset{1}{a^{t.r}} . b^{tr} = 1 \Rightarrow b^{tr} = 1 \Rightarrow s \mid tr$, но $(r, s) = 1$

$\Rightarrow s \mid t$

$s \mid t$ и $r \mid t \Rightarrow sr \mid t$ ✓

б) ? в G има елем. от ред $[r, s]$ → (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

$1 = (ab)^t = a^t b^t = a^{ts}$ $\quad r \mid ts$

$r \mid ts \qquad 1 = (ab)^t = a^t b^t = a^{t\sigma}$

$r_1 \mid ts_1 \qquad s \mid t\sigma \quad \Rightarrow s_1 \mid t\sigma_1 \Rightarrow r_1 s_1 \mid t$

$t \mid r_1 s_1 d^2 \qquad\qquad * \ (r_1, s_1) = 1$

б) $r = p_1^{\alpha_1} \dots p_n^{\alpha_n}$

$s = p_1^{\beta_1} \dots p_n^{\beta_n}$

$[r, s] = p_1^{\gamma_1} \dots p_n^{\gamma_n}, \quad \gamma_i = \max(\alpha_i, \beta_i)$

$\exists k: |a^k| = p_i^{\gamma_i}$ 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) $\Rightarrow \exists\ c \in G: c = \prod_{i=1}^{n} c_i$

$|c| = [r, s]$

$$\boxed{\begin{aligned} &* \ |a| = r \\ &|a^k| = \frac{r}{(k, r)} \end{aligned}}$$

$\boxed{\text{Зад.}}$ G – кр. група и $|G| = 2k$, $k \in \mathbb{N}$. Д.Д., че в G има елем. $g : |g| = 2$.

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

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

$\boxed{\text{Зад.}}$ G – гр.; $\exists!\ a \in G: |a| = 2$. Д.Д., че a комут. с $\forall$ ел. на

? $\forall\ g \in G: ag = g \cdot a$

$*$

! $|a| = |g^{-1} \cdot a \cdot g| \to$ за произв. група $\to$ (от предна задача)

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

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

$g \cdot a = a \cdot g$ ✓

$\boxed{\text{Зад.}}$ G - група ; $\forall g \neq 1, g \in G : |g| = 2$. Д-те, че G е абелева.

$a, b \neq 1 \in G$

$|a| = 2$ и $|b| = 2$, $|ab| = 2 \Rightarrow$

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

$\boxed{\text{Зад.}}$ Q_8 , D_4 . ? редовете на елем. на двете групи

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

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

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

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

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

$\Rightarrow \underline{1}$ - един. елем.

$\Rightarrow |-1| = 2$

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

$D_4 = \{A^i B^j \mid i = 1, \dots, 4 ; j = 1, 2\}$

$B^{-1} \cdot A \cdot B = A^{-1}$

E,

$|A| = n = 4$; $|AB| = 2$; $|A^2 B| = 2$; $|A^3 B| = 2$

$|B| = 2$; $|A^2| = 2$; $|A^3| = 4$

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

$A^3 B = A^{-1} \cdot B = B^{-1} \cdot A = B \cdot A$

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

$|A^2 B| = 2$

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

Циклични групи

$\forall \{x_1, x_2, \ldots, x_n\}$

$\langle g \rangle = \{ g^0, g^{\pm 1}, g^{\pm 2}, \ldots \}$ $\to$ Гр. е цикл., ако $\forall$ са g на някоя степен.

Зад. ДД, че $\mathbb{Z}$ (безкр. цикл.) има точно два пор. елем. | C_n, $\mathbb{Z}_n$

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

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

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

$\omega_1^k = \omega_k$

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

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

$* \; \varphi(n)$ – бр. числа, $< n$ и вз. прости с n

$k < n$

пр.: C_4

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

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

Зад. 1 Да се опр. $\forall$ подгрупи на гр. G и да вкл.-та

а) $G = \mathbb{C}_8$

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

* подгр. на циклична е циклична.

$\{E\}$, G – тривиалните подгр.

g, g^5, g^7, g^{11} – вз. прости с 12 $\Rightarrow$ не могат да уч. в подгрупа (пораждат цялата)

$\rightarrow |g^2| = 6$

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

$\mathbb{C}_6$ 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: $\longrightarrow$

$$\begin{tikzcd}
 & G = \mathbb{C}_{12} \arrow[dl] \arrow[dr] & \\
\mathbb{C}_6 \arrow[d] \arrow[dr] & & \mathbb{C}_4 \arrow[dl] \\
\mathbb{C}_3 \arrow[dr] & \mathbb{C}_2 \arrow[d] & \\
 & \{E\} &
\end{tikzcd}$$

Формула на графита

!:>

в) $G = C_n$

$C_d \le C_n$, $d | n$

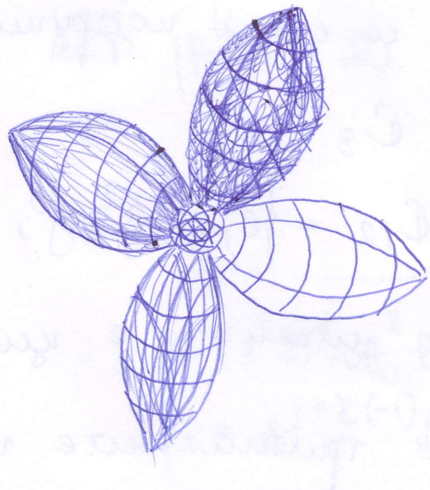
$\varphi(n)$ – нерандация

г) $G = \mathbb{Z}$

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

$n_1\mathbb{Z} \le n_2\mathbb{Z}$, $n_2 | n_1$

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



зад.1 ? бр. на р-ията на $x^d = 1$ • Бр. елем. от ред d в гр. C_n?

а) $n = 12$, $d = 6$ $\qquad |\omega_2| = |\omega_{10}| = 6$

$x^6 = 1$ за C_{12}

~~Ако $a \in G$ и $|a| = r$. $a^n = 1 \Leftrightarrow r | n$~~

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

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

C_6 – $\forall$ елем. са р-ия на $x^6 = 1$

б) $n = 100$; $d = 20$ $\qquad$ в) $n, d \in \mathbb{N}$, $d | n$

Симетрична група

$\Omega_n = \{1, 2, \dots, n\}$ – пермут. на числата от $1 \dots n$

$|S_n| = n!$

→ композиция – операцията в гр.

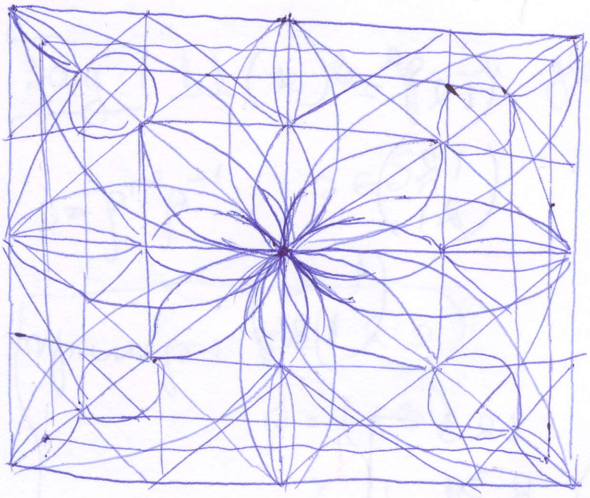
→ id – един. елемент

$\forall\ i_1, i_2, \dots, i_n$

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

$\sigma = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = (1\,2\,3)$ $\qquad\qquad$ $\sigma = (i_1, \dots i_k)$

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



- $\rho \in S_n$

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

$\rho = (j_1, \dots j_s)$

$\sigma\rho = \rho\sigma$

пример:

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

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

Зад 1

ДД, че $\forall$ перм. в S_n

$\forall \sigma \in S_n \; ; \; ! \, \sigma = \sigma_1, \sigma_2, \dots \sigma_k \qquad \sigma_i \cap \sigma_j = \{\emptyset\}$

Нека k е нг $\mathbb{N}$ число, за което

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

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

$\Rightarrow \sigma(i_k) = \sigma(i_{j-1})$ – противор. $\Rightarrow \sigma(i_k) = i_1$

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

$i_1 \in \sigma_1$

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

Зад. ДД, че в гр. S_n:

а) редът на цикъл = дължината му

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

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

пр.:

$(1\,2)^2 = (1)$

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

$$\begin{array}{ll} (1\,2\,3) & 1\,2\,3 \\ & 2\,3\,1 \\ (1\,2\,3) & 3\,1\,2 \\ (1\,2\,3) & 1\,2\,3 \end{array}$$

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

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

$|\rho| = t$

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

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

$\Rightarrow$ усл. ✓

Зад.

$\sigma, \rho \in S_n$. ДД:

а). $\sigma = (i_1, i_2, \dots, i_k)$

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

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

$$\left.\begin{array}{l|l} \rho^{-1} & i_1 \quad i_2 \dots i_k \\ \sigma & i_2 \quad i_3 \dots i_1 \\ \rho & \rho(i_2)\; \rho(i_3) \dots \rho(i_1) \end{array}\right]$$

б). $\sigma = (i_1 \dots i_k) \dots (j_1 \dots j_s)$

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

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

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

Зад.) ДД, че в гр. S_n две перм. ρ и τ са спрегнати $\Leftrightarrow$

$i = \rho\tau\rho^{-1}$, $\rho \in S_n$

пример: $\sigma = (1\,2\,3)$

$\rho = (1\,3)$

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

II н.)

		1 2 3
ρ^{-1}	$= (1\,3)$	3 2 1
σ	$= (1\,2\,3)$	1 3 2
ρ	$= (1\,3)$	3 1 2

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

Зад.) ДД, че в гр. S_n: ц-л с дълж. 2

а). $\forall$ перм. се разлага в произв. на непрем. незав. транспозиции

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

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

	$i_1, \dots, i_k$
(i_1, i_2)	$i_2, i_1, i_3, \dots, i_k$
(i_1, i_3)	$i_2\, i_3\, i_1 \dots i_k$
$\vdots$	
(i_1, i_k)	$i_2, i_3 \dots i_1$

$(i_1, i_2 \dots i_k) = (i_1, i_k)(i_1, i_{k-1}) \dots (i_1, i_2)$

б). ?. бр. на множ. в едно разлаг.на транспоз. е с четност = на четността на пермутацията

Пр.:

$$\left.\begin{matrix} 1 & 2 & \ldots & i & \ldots & j & \ldots & n \\ 1 & 2 & \ldots & j & \ldots & i & \ldots & n \end{matrix}\right\} \to$$ бр. на инв. е $2(i-j-1)+1$ - нечетно

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

A_n - множ. от четни пермут. (алтернативна група)

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

$\sigma, \rho \in A_n$

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

$\rho =$ — — — $= 2r$ - транспозиции

$\Rightarrow \sigma . \rho = 2(\ldots) \Rightarrow$ четна пермут.

$\Rightarrow (id)$ - четна пермут.

$\Rightarrow$ обратна на четна транспоз. е също четна $\Rightarrow$ A_n е група

$A_n \leq S_n$