Т G - циклична група и $H<G \Rightarrow H$ - циклична

Доказателство:

1) $|G|=\infty \Rightarrow G\cong\mathbb{Z}$

$H<G$. Нека $g^d\in H$ и d е $\min$ $\mathbb{N}$ число, за което $g^d\in H$.

$g^s\in H \Rightarrow s=qd+r,\ 0\le r<d$

$\Rightarrow g^s=g^{qd+r}=\underbrace{(g^d)^q}_{\in H}\cdot g^r\in H \Rightarrow g^r=g^{s-dq}\Rightarrow g^r\in H \Rightarrow$ т.к. d е $\min$ $\mathbb{N}$ число: $g^d\in H \Rightarrow r=0 \Rightarrow g^s=g^{dq}\Rightarrow <g^d> \Rightarrow H\le <g^d>,\ g^d\in H \Rightarrow$

$\Rightarrow (g^d)^k\in H \Rightarrow <g^d>\le H \Rightarrow H=<g^d> \Rightarrow H$ - циклична

2) $|G|=n \Rightarrow G=<g>$ и $<g>=n$

$H<G$ и $g^d\in H$, d е $\min$ $\mathbb{N}$, за което $g^d\in H$.

s - произволно, $g^s\in H$

... (аналогично на 1)) $\Rightarrow H\le <g^d>$ и $H=<g>$.

Ако приложим това за $e=g^n$, ще получим, че $n=qd+r_1,\ 0\le r_1<d \Rightarrow$

$\Rightarrow e=(g^d)^{q_1}\cdot r_1 \Rightarrow g^{r_1}\in H \Rightarrow r_1=0$. Така получаваме условие какви могат да бъдат подгрупите на крайна циклична група $\Rightarrow d/n$.

Симетрични групи

D $M\neq\emptyset$; $S(M)=\{\varphi \mid \varphi: M\to M$ - биекция$\}$

$\varphi\circ\psi(x)=\varphi(\psi(x))$

- некомутативна

$|M|=n \to M=\{1,2,3,\dots,n\}$

$S(M)=S_n$ - симетрична група от степен n

$\varphi\in S_n \Rightarrow \begin{pmatrix}1 & 2 & 3 & \dots & n\\ i_1 & i_2 & i_3 & \dots & i_n\end{pmatrix}$, $i_k=\varphi(k)$

↳ пермутация на $\overline{1,n}$ $\Rightarrow |S_n|=n!=P_n$

П Представяне на елементите чрез цикли

$\sigma=(i_1,i_2\dots i_k)$ - цикъл с дължина k

$\{i_1\dots i_k\}\subset\{1\dots n\}$

$i_1\xrightarrow{\sigma} i_2\xrightarrow{\sigma}\dots\to i_{k-1}\xrightarrow{\sigma} i_k\xrightarrow{\sigma} i_1$ ⟶ За всички останали елементи е изпълнено, че не се променят под действие на σ.

$S_8 \to (2,4,6,8) \to \begin{pmatrix}1&2&3&4&5&6&7&8\\1&4&3&6&5&8&7&2\end{pmatrix}$

D Циклите $(i_1\dots i_k)$ и $(j_1\dots j_s)$ са независими, ако подмножествата от точки, които преместват, нямат общ елемент.

Свойство: Ако σ и τ са независими цикли, то те комутират.

!Забележка: Това не важи за зависими цикли!

$(i_1, i_2 \dots i_k) = (i_2, i_3 \dots i_k, i_1) \dots \Rightarrow$ ВСЕКИ ЦИКЪЛ С ДЪЛЖИНА k МОЖЕ ДА БЪДЕ ЗАПИСАН ПО k НАЧИНА

τ //

ОБРАТЕН ЦИКЪЛ: $\tau^{-1} = (i_k \dots i_1)$ - ОЩЕ ЦИКЪЛ С ДЪЛЖИНА k.

Т ВСЕКИ ЕЛЕМЕНТ σ ОТ S_n, $\sigma \neq id$ МОЖЕ ДА СЕ ПРЕДСТАВИ КАТО ПРОИЗВЕДЕНИЕ НА НЕЗАВИСИМИ ЦИКЛИ И ТОВА ПРЕДСТАВЯНЕ Е ЕДИНСТВЕНО С ТОЧНОСТ ДО РЕДА НА МНОЖИТЕЛИТЕ.

Доказателство: // ИНДУКЦИЯ ПО $\mu(\sigma)$ = БРОЯТ НА ЕЛЕМЕНТИТЕ, КОИТО СЕ // ПРОМЕНЯТ ПОД ДЕЙСТВИЕТО НА σ.

$\mu \in \mathbb{Z}$, $\mu \geq 2$, $\mu \leq n$

1. $\mu = 2 \Rightarrow \exists\, i \neq j : \sigma(i) \neq i$ и $\sigma(j) \neq j$; $\forall\, k \neq i, j \Rightarrow \sigma(k) = k \Rightarrow \sigma(i) = j$, $\sigma(j) = i$

$\Rightarrow \sigma = (i, j)$.

2. $\mu > 2$

НЕКА $i_1 : \sigma(i_1) \neq i_1$

$i_2 = \sigma(i_1)$

$i_3 = \sigma(i_2)$

$\dots$

$i_s = \sigma(i_{s-1})$

$\Rightarrow$ ПОЛУЧАВАМЕ БЕЗКРАЙНА РЕДИЦА

$s, t > 1 \Rightarrow i_s = i_t \Rightarrow \sigma(i_{s-1}) = \sigma(i_{t-1}) \Rightarrow i_{s-1} = i_{t-1} \Rightarrow$ ПЪРВОТО ЧИСЛО, КОЕТО ЗА ПЪРВИ ПЪТ СЕ ПОВТАРЯ В РЕДИЦАТА Е $i_1 \Rightarrow i_1 \dots i_k, i_{k+1} = i_1 \dots$

$\Rightarrow \tau = (i_1 \dots i_k)$

$\sigma_1 = \tau^{-1} \circ \sigma \Rightarrow \sigma_1(i_1) = \tau^{-1}(\sigma(i_1)) = \tau^{-1}(i_2) = i_1 \Rightarrow \sigma_1(i_s) = i_s$ ЗА $\forall\, i_s$.

$j \neq i_1 \dots i_k \Rightarrow \sigma_1 = \sigma_j \Rightarrow \mu(\sigma_1) = \mu(\sigma) - k \Rightarrow \mu(\sigma_1) < \mu(\sigma)$.

$\Rightarrow$ ЗА σ_1 ПРИЛ. ИНДУКЦИЯТА И $\sigma_1 = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k \Rightarrow$

$\Rightarrow \sigma = \tau_0 \circ \tau_1 \circ \dots \circ \tau_k$

ЕДИНСТВЕНОСТ

$\sigma = \tau_0 \circ \tau_1 \circ \dots \circ \tau_k$

$\sigma = \varphi_0 \circ \varphi_1 \circ \dots \circ \varphi_s$

$j \in \{k \mid \sigma(k) \neq k\} \Rightarrow j$ УЧАСТВА В ЗАПИСА НА ЕДНО τ И ЕДНО φ И Т.К.

τ И φ КОМУТИРАТ $\Rightarrow$ МОЖЕМ ДА МИСЛИМ, ЧЕ Е ПОСЛЕДНОТО $\Rightarrow$

$\Rightarrow j \in \tau_k$ и $j \in \varphi_s \Rightarrow \left.\begin{array}{l} \tau_k = (j, \sigma(j), \sigma^2(j) \dots) \\ \varphi_s = (j, \sigma(j), \sigma^2(j) \dots) \end{array}\right\} \Rightarrow \varphi_s = \tau_k \Rightarrow$

$\Rightarrow$ МОЖЕМ ДА НАХНЕМ ПОСЛЕДНИЯ МНОЖИТЕЛ

$\Rightarrow \tau_0 \dots \tau_{k-1} = \varphi_0 \dots \varphi_{s-1} \Rightarrow s = r$ И МНОЖИТЕЛИТЕ СА СЪОТВЕТНО # ЕДНАКВИ

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

$\downarrow$

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

Редът на цикъл с дължина k и k.

D Цикъл с дължина 2 се нарича транспозиция.

Св-во Всеки елемент от S_n може да се представи като произведение на транспозиции.

$(i_1, i_2 \dots i_k) = (i_1, i_k) \circ \dots \circ (i_1, i_3) \circ (i_1, i_2)$; $id = (1,2) \circ (1,2)$

Тв Ако $\tau_1 \circ \tau_2 \dots \circ \tau_k$ дава id и τ_j са транспозиции, то k е четно

Доказателство:

$(i,j)(a,k) = (a,k)(i,j)$

$(i,j)(a,i) = (a,j)(j,i)$

$(a,i)(a,j) = (a,j)(i,j)$

$(a,i)(a,i) = id$

$\tau_1 \circ \dots \tau_k \longrightarrow$ фиксирано число a. $\longrightarrow$ „Избутваме" a все по-напред $\Rightarrow \tau_1' \circ \dots \tau_s' = id$ (a е или в τ_1', или никъде → не възможно $\Rightarrow a$ го няма в новия запис

На следващата стъпка изхвърляме друго число и т.н.

По този начин изхвърляме всички числа и т.к. имаме id, не може да остане една транспозиция $\Rightarrow$ Оставаме без транспозиции. Само в последното равенството имаме от две транспозиции към $O \Rightarrow s = k - 2m \Rightarrow k \equiv s(2)$. На всяка стъпка получаваме по-малък брой транспозиции, но четността се запазва $\Rightarrow$ След няколко стъпки получаваме $O \Rightarrow k$ е четно.

Тв Ако $\sigma \in S_n$ и $\sigma = \tau_1 \circ \dots \circ \tau_n$ и $\sigma = \mu_1 \circ \dots \circ \mu_\ell$, където τ_i и μ_j са транспозиции $\Rightarrow s \equiv \ell(2)$. $\overset{?}{\circ}\ (i,j) = (i,j) \overset{?}{\circ}$

Доказателство

$\mu_1 \circ \dots \circ \mu_\ell = \tau_1 \circ \dots \circ \tau_s \mid \circ \tau_s^{-1}$

$\mu_1 \dots \mu_\ell \circ \tau_s = \tau_1 \circ \dots \circ \tau_{s-1}$

$\mu_1 \dots \mu_\ell \circ \tau_s \dots \circ \tau_1 = id \Rightarrow \ell + s \equiv 0(2) \Rightarrow \ell \equiv s(2)$

Четна пермутация – представя се като произведение на четен брой транспозиции.

$S_n \to A_n = \{\varphi \in S_n \mid \varphi$ – четна пермутация$\}$

$\to B_n = \{\varphi \in S_n \mid \varphi$ – нечетна пермутация$\}$

$B_n \not\subset S_n$ $(\varphi_1, \varphi_2 \in B_n \Rightarrow \varphi_1 \circ \varphi_n \in A_n)$

$\xi : S_n \to S_n : \varphi \in S_n \to \xi(\varphi) = (1,2) \circ \varphi$

$\Rightarrow \xi(A_n) \subset B_n$ $\quad \xi^2(A_n) = A_n$

$\xi(B_n) \subset A_n$

$\Rightarrow A_n \xrightarrow{\xi} B_n \xrightarrow{\xi} A_n \Rightarrow |A_n| = |B_n|$

ξ – биекция

Алтернативна група от степен n

$n \geq 2$