5. Симетрична група. Представяне на ел. на S_n като произведение на независими цикли, ред на ел. от S_n и спрягане. Алтернативна гр.

$M \neq \emptyset$ $S(M) = \{\varphi \mid \varphi: M \to M$ биекция$\}$
$\varphi \circ \psi(x) = \varphi(\psi(x))$ $|M| = n$ $M = \{1, \dots n\}$
$S(M) = S_n$ - симетрична група от степен n на мн. M.

Деф: $\varphi \in S_n$: $\varphi : \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ $i_1 \dots i_n$ - числата от $1 \to n$
$i_k = \varphi(k)$ $|S_n| = n!$
$\sigma = (i_1 \dots i_k)$ - цикъл с дължина k $|\sigma| = k$
$\{i_1 \dots i_k\} \subseteq \{1, \dots n\}$
$i_1 \xrightarrow{\sigma} i_2 \dots i_{k-1} \xrightarrow{\sigma} i_k$ Ако $j \notin \{i_1, \dots, i_k\}$: $\sigma(j) = j$

$S_8(2,4,6,8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 6 & 5 & 8 & 7 & 2 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1,3)(2,4)$ - не е цикъл

Опр: Независими цикли: Цикъла: $\sigma = (i_1, \dots i_k) \in S_n$ и $\tau = (j_1, \dots, j_s) \in S_n$ са независими ако $\{i_1 \dots i_k\} \cap \{j_1 \dots j_s\} = \emptyset$

Св: Ако $\sigma = (i_1 \dots i_k)$ и $\tau = (j_1 \dots j_s)$ са независими цикли тогава комутират $\sigma \circ \tau = \tau \circ \sigma$

Забележка: Ако циклите са зависими то (няма по св-то)
$(i_1, i_2 \dots i_k) = (i_2, i_3 \dots i_k, i_1)$ - всеки един цикъл с дължина k може да бъде записан по k начина.
Обратен на $(i_1 \dots i_k)^{-1} = (i_k, i_{k-1}, \dots, i_1)$ - обратен цикъл на цикъл с дължина k е същото с дължина k.

Т-ма: Всеки елемент $\sigma \in S_n$, $\sigma \neq id$ може да се представи като произведение на независими цикли и това представяне е единствено с точност до реда на множителите.

Д-во: Индукция по бр. на символите които се променят при действието на σ.

Нека $\mu(\sigma) = |\{k \mid \sigma(k) \neq k\}|$ - цяло число $n \geq \mu(\sigma) \geq 2$

база: 1) $\mu(\sigma)=2 \Rightarrow \exists i \neq j : \sigma(i) \neq i, \sigma(j) \neq j$ и $\Rightarrow$
$\sigma(i)=j \quad \sigma(j)=i$
$\forall k \in \{i,j\} : \sigma(k)=k \Rightarrow \sigma=(i,j)$

2) Нека $\mu(\sigma)>2$
Нека $i_1 : \sigma(i_1) \neq i_1$
Нека $i_2=\sigma(i_1)$; $i_3=\sigma(i_2) \dots i_s=\sigma(i_{s-1})$
безкрайна редица от числа $i_1 \dots i_{s-1}, i_s \dots$
Ако $i_s=i_t$ $s>1, t>1 \Rightarrow \sigma(i_{s-1})=\sigma(i_{t-1}) \Rightarrow i_{s-1}=i_{t-2}$
Изберем най-малкото число измежду всички, които се повтарят в редицата са $i_1, i_2 \dots i_k$ $i_{k+1}=i_1$
$\tilde{\tau}=(i_1 \dots i_k)$ - цикъл Нека $\sigma_1=\tilde{\tau}^{-1} \circ \sigma$
$\sigma_1(i_1)=\tilde{\tau}^{-1}(\sigma(i_1))=\tilde{\tau}^{-1}(i_2)=i_1$
Аналогично за $\forall i_s$ от тази вид $\sigma_1(i_s)=i_s$
$j \notin \{i_1 \dots i_k\}$ ~~$\sigma_1(j)=\tilde{\tau}^{-1}(i_s)$~~ $\Rightarrow \sigma(j) \notin \{i_1 \dots i_k\}$
$\sigma_1(j)=\tilde{\tau}^{-1}(\sigma(j))=\sigma(j)$
$\mu(\sigma_1)=\mu(\sigma)-k \Rightarrow$ за σ_1 приложим индукцията
$\tilde{\tau}^{-1} \circ \sigma=\sigma_1=\tilde{\tau}_1 \circ \tilde{\tau}_2 \circ \dots \circ \tilde{\tau}_t \Rightarrow \sigma=\tilde{\tau} \circ \tilde{\tau}_1 \circ \dots \circ \tilde{\tau}_t$

(!) Единственост:
$\sigma=\tilde{\tau}_0 \circ \tilde{\tau}_1 \circ \dots \circ \tilde{\tau}_t$; $\sigma=\varphi_0 \circ \varphi_1 \circ \dots \circ \varphi_s$ $j \in \{k \mid \sigma(k) \neq k\}$
Числото j участва в вайчка на 1 $\tilde{\tau}$ и само на 1 φ
$\tilde{\tau}, \varphi$ са независими и комутират можем да ги разместим така, че
умножителите $\Rightarrow$ крайните $\tilde{\tau}_t$ и φ_s - съдържат j.
$j \in \{j, \sigma(j), \sigma^2(j), \dots\} \Rightarrow \tilde{\tau}_t = \varphi_s \Rightarrow$
$j \in \{j, \sigma(j), \sigma^2(j) \dots\}$
махаме $\tilde{\tau}_t$ и $\varphi_s \Rightarrow \tilde{\tau}_0 \circ \dots \tilde{\tau}_{t-1}=\varphi_0 \circ \dots \circ \varphi_{s-1}$ - броят на цикълчетата е равен от двете страни

Св-во: $\tilde{\tau}_1 \dots \tilde{\tau}_k$ - независими цикли
$|\tilde{\tau}_1 \circ \dots \circ \tilde{\tau}_k| = НОК(|\tilde{\tau}_1|, |\tilde{\tau}_2|, \dots, |\tilde{\tau}_k|)$

Опр: Цикъл с дължина 2 се нарича транспозиция т.е размества на местата на 2 елемента.

Об: 1) Всеки елемент от S_n може да се представи като произведение на транспозиции: $(i_1, i_2 \dots i_k) = (i_1, i_k) \dots (i_1, i_4)(i_1, i_3)(i_1, i_2)$
- Цикъл с дължина k може да се запише като произведение на $k-1$ транспозиции.

Следствие: Всеки елемент от S_n може да се представи като произведение на транспозиции

Тв: 2) Ако произведението $\tau_1 \circ \tau_2 \circ \dots \circ \tau_k = id$ и τ_j са транспозиции тогава k е четно.

Доказ: $(i,j)(a,k) = (a,k)(i,j)$
$(i,j)(a,i) = (a,j)(j,i)$
$(a,i)(a,j) = (a,j)(i,j)$
$(a,i)(a,i) = id$

$\tau_1 \circ \tau_2 \circ \dots \circ \tau_k = \tau_1', \tau_2' \dots \tau_s' = id \Rightarrow \tau_1' \dots \tau_s'$ - празна числото q
Сл. като направим последователно преобразуване числото q може да е в τ_1' или никаре. т. като произвед. е равно на id не е възможно q да участва в 1 транспозиция (четвата) $\Rightarrow$ $\tau_1' \dots \tau_s'$ - празна числото q. По този начин изхвърляме всички числа по двойки, като чиято id не може да остане само една транспозиция, т.е не може да е id. Затова изхвърляме всички транспозиции.
$s = k - 2m \Rightarrow s \equiv k \pmod 2$ На всяка стъпка получаваме по-малък брой транспозиции по броя на транспозициите се запазва четността. На края получаваме 0 транспозиции $k \equiv s \equiv 0 (2)$

Тв: Ако $\sigma \in S_n$ и $\sigma = \tau_1 \circ \dots \circ \tau_s$, $\sigma = \mu_1 \circ \dots \circ \mu_l$ където τ_j и μ_j са транспозиции, тогава $l \equiv s (2)$ (l, s - с еднаква четност)

$\mu_1 \circ \dots \circ \mu_l = \tau_1 \circ \dots \circ \tau_s \quad / \circ \tau_s$ $\quad (i,j)^{-1} = (i,j)$
$\mu_1 \dots \mu_l \circ \tau_s = \tau_1 \dots \tau_{s-1}$
$\mu_1 \dots \mu_l \tau_s \tau_{s-1} \dots \tau_1 = id \Rightarrow s + l \equiv 0 \pmod 2 \Rightarrow s \equiv l \pmod 2$

Опр: Четна пермутация която е произведение на четен бр. транспозиции. Нечетна пермутация която е произведение на нечетен бр. транспозиции. (Н.Н. = четна, $2 \cdot 4 = 4$, $2 \cdot 2 = 2$)

$A_n = \{ \varphi \in S_n \mid \varphi$ - четна пермут. $\}$
$B_n = \{ \varphi \in S_n \mid \varphi$ - нечетна пермут. $\}$ } разбиване S_n на A_n и B_n

$\varphi_1, \varphi_2 \in A_n \Rightarrow \varphi_1 \circ \varphi_2 \in A_n$

$\varphi^{-1} \in A_n \Rightarrow A_n < S_n$ - (подгрупа)

$\Rightarrow B_n$ - не е подгрупа на S_n (защото 2 е. от B_n дават е. от A_n)

$\zeta : S_n \to S_n$

$\zeta(\varphi) = (12) \circ \varphi$

$\zeta(A_n) \subset B_n$

$\zeta^2 = id$ т.е. $A_n \overset{\zeta}{\underset{\zeta}{\rightleftarrows}} B_n \Rightarrow |A_n| = |B_n| = \frac{|S_n|}{2} = \frac{n!}{2}$, $n \geq 2$

A_n - алтернативна група от степен n и съдържа половината е. от S_n.

6. Съседни класове. Теорема на Лагранж, следствия

Опр: G - абстрактна група $(G, \circ)$, $H < G$ - подгрупа

$a \in G$ $aH = \{ah \mid h \in H\}$ - ляв съседен клас

$Ha = \{ha \mid h \in H\}$ - десен съседен клас

Пр: а) $\mathbb{R}^n$ $H: \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ a_{k1}x_1 + \dots + a_{kn}x_n = 0 \end{cases}$ $H < \mathbb{R}^n$ $L: \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ a_{k1}x_1 + \dots + a_{kn}x_n = b_k \end{cases}$

$L = \{\alpha + \gamma \mid \gamma \in H\} = \alpha + H$ α - частно решение на нехомог.

2) $\mathbb{Z}$ $5\mathbb{Z} < \mathbb{Z}$

$1 + 5\mathbb{Z} = \{1 + 5k \mid k \in \mathbb{Z}\}$ - цялата част от 1 при делене с 5

$2 + 5\mathbb{Z}$, $3 + 5\mathbb{Z}$, $4 + 5\mathbb{Z}$, $5 + 5\mathbb{Z} = 5\mathbb{Z}$, $6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$

$\mathbb{Z} = 5\mathbb{Z} \cup \{1 + 5\mathbb{Z}\} \cup \{2 + 5\mathbb{Z}\} \cup \{3 + 5\mathbb{Z}\} \cup \{4 + 5\mathbb{Z}\}$ - числата от $\mathbb{Z}$ с 2, 3 или 4.

Тв 1: $H < G$ $\rho H = H \iff \rho \in H$

Док: // $\rho H = H \Rightarrow \rho = \rho \cdot e \in \rho H \Rightarrow \rho \in H$

$\rho \in H \Rightarrow \rho h \in H \Rightarrow \rho H \subset H$ $h = \rho(\rho^{-1}h) \in \rho H$

Тв 2: $\ell \in \rho H \iff \rho \in \ell H$

Док: // $\ell \in \rho H \Rightarrow \ell = \rho h_1$, $h_1 \in H \Rightarrow \rho = \ell \cdot h_1^{-1} \in \ell H$

Тв 3: $\ell \in \rho H \iff \rho H = \ell H$

Док: // $\ell \in \rho H \Rightarrow \ell = \rho h_1$, $h_1 \in H$, $\ell h_2 \in \ell H \Rightarrow \ell h_2 = \rho(h_1 h_2) \in \rho H$

$\ell H \subset \rho H$

аналог: $\ell \in \rho H \Rightarrow \rho \in \ell H \Rightarrow \rho H \subset \ell H \Rightarrow \ell H = \rho H$