29. Симетрична и алтернативна група. Теорема на Кейли. Теорема за хомоморфизмите на групи

1. **Симетрична група S_n - представяне на елементите като произведение на независими цикли.**

Деф: Симетрична група на множество M:

$S(M) = \{\varphi \mid \varphi: M \to M - биекция\}$ *е симетрична група на множеството M.*

Деф: Симетрична група от степен n:

Нека $|M| = n, \quad M = \{1, 2, \dots, n\}, \quad \varphi \in S(M)$.

$\varphi \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, φ - биекция $\Rightarrow$ $i_1 \dots i_n$ е пермутация на числата $1 \dots n$

$S(M) = S_n$ - симетрична група от степен n. Елементите на симетричната група се наричат **пермутации**. $|S_n| = n!$

Деф: Цикъл

$\varphi \in S_n$, φ е цикъл с дължина k: $\varphi = (i_1, i_2, \dots, i_k)$, когато $\varphi(i_1) = i_2$, $\varphi(i_2) = i_3$, ... , $\varphi(i_{k-1}) = i_k, \varphi(i_k) = i_1$ и $\varphi(j) = j$ за $j \notin \{i_1, \dots, i_k\}$.

Деф: Независими цикли

$\varphi(\mathrm{i}_1, \dots, \mathrm{i}_k)$, $\psi(\mathrm{j}_1, \dots, \mathrm{j}_s)$, φ и ψ са независими цикли, когато $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_k\} \neq \emptyset$.

Теорема: $\forall$ ел. от S_n $(\varphi \neq id)$ може да се представи като произведение на независими цикли и това представяне е единствено с точност до реда на множителите.

Д-во:

$\varphi \in S_n, \varphi \neq id, \qquad M_\varphi = \{t \mid \varphi(t) \neq t\} \subset \{1, 2, \dots, n\}$

Индукция по $m_\varphi = |M_\varphi|$

- $m_\varphi = 1$ - невъзможно, защото $\varphi(t) \neq t \Rightarrow \varphi(t) = u \neq t \Rightarrow \varphi(u) \neq u$
- $m_\varphi = 2$ и $M_\varphi = \{t, u\}$

  $\varphi(t) = u$ и $\varphi(u) = t$ и $\varphi(s) = s$ за $s \neq t \Rightarrow \varphi = (u, t)$
- Нека $m_\varphi > 2$ и да допуснем, че е доказано твърдението за всички стойности, за които $2 \leq m_\psi < m_\varphi$.
- Стъпка:

  $i_1 \in M_\varphi$: $\varphi(i_1) \neq i_1$, $i_2 = \varphi(i_1)$, $i_3 = \varphi(i_2), \dots, i_t = \varphi(i_{t-1})$

  $i_1, i_2, \dots i_t, i_{t+1}, \dots$ - безкрайна редица с елементи от S_n

  От един момент нататък има повторения. Нека $i_t = i_s \Rightarrow \varphi(i_{t-1}) = \varphi(i_{s-1}) \Rightarrow$ $i_{t-1} = i_{s-1} \Rightarrow i_{t-2} = i_{s-2} \Rightarrow \cdots$

  Първото число, което се повтаря в редицата е $i_1 \Rightarrow \underbrace{i_1, \dots, i_k}_{\text{различни}}, i_1, \dots, i_k, i_1, \dots, i_k, \dots$

  Разглеждаме цикъла $\psi = (i_1, \dots, i_k)$ върху числата $i_1, \dots, i_k$ и φ и ψ действат по един и същи начин

$$\varphi_1 = \psi^{-1} \circ \varphi \qquad \begin{array}{l} \varphi_1(i_1) = i_1 \\ \varphi_1(i_2) = i_2 \\ \vdots \\ \varphi_1(i_k) = i_k \end{array}$$

  Ако $j \notin \{i_1, \dots, i_k\} \Rightarrow \varphi_1(j) = \psi^{-1}\left(\varphi(j)\right) = \varphi(j) \Rightarrow \varphi(j) \notin \{i_1, \dots, i_k\}$

  Щом $j \notin \{i_1, \dots, i_k\} \Rightarrow \varphi(j) \notin \{i_1, \dots, i_k\}$, защото иначе j щеше да $\in \{i_1, \dots, i_k\}$

  $\Rightarrow M_{\varphi_1} = M_\varphi \{i_1, \dots, i_k\}$ $m_{\varphi_1} = m_\varphi - k$

Прилагаме индукцията за $\varphi_1 = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_s$ - независими цикли.

$\psi^{-1} \circ \varphi = \tau_1 \circ \cdots \circ \tau_s \Rightarrow \varphi = \psi \circ \tau_1 \circ \cdots \circ \tau_s \Rightarrow \psi, \tau_1, \dots, \tau_s$ са независими цикли

Единственост:

$$\left.\begin{array}{l} \varphi = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_s \\ \varphi = \psi_1 \circ \psi_2 \circ \cdots \circ \psi_r \end{array}\right. - \text{независими цикли,} \qquad \begin{array}{l} M_\varphi = M_{\tau_1} \cup M_{\tau_2} \cup \cdots \cup M_{\tau_s} \\ M_\varphi = M_{\psi_1} \cup M_{\psi_2} \cup \cdots \cup M_{\psi_r} \end{array}$$

$M_\varphi \cup M_{\tau_2} \cup \dots \cup M_{\tau_s} = M_{\psi_1} \cup M_{\psi_2} \cup \dots \cup M_{\psi_r}$

Нека $i_1 \in M_\varphi$, преномерираме т.ч. $i_1 \in M_{\tau_1}$, $i_1 \in M_{\psi_1}$. $\tau_1(i_1) = \varphi(i_1) = \psi(i_1) = i_2$

$$\left.\begin{array}{l} \tau_1 = \left(i_1, i_2, \overbrace{\varphi(i_2)}^{=i_3}, \dots\right) \\ \psi_1 = \left(i_1, i_2, \underbrace{\varphi(i_2)}_{=i_3}, \dots\right) \end{array}\right\} \text{ двата цикъла са еднакви}$$

$\tau_1 = \psi_1 \Rightarrow \tau_2 \circ \dots \circ \tau_s = \psi_2 \circ \dots \circ \psi_r$ и след краен брой стъпки $\Rightarrow s = r \Rightarrow \tau_p = \psi_p,\ p = 1, \dots, r$

2. **Спрягане на елементите на S_n**

Деф: Спрегнат елемент

(G,·) - група, $\boldsymbol{a \sim b}$, казваме,че елементът а е **спрегнат** с елемента b, когато $\exists c$: $b = c^{-1}ac$.

Лема: $\varphi = (i_1, \dots, i_t), \tau \in S_n$

$$\psi = \tau^{-1} \cdot \varphi \cdot \tau \qquad \begin{array}{l} \tau^{-1}(i_1) \xrightarrow{\tau} i_1 \xrightarrow{\varphi} i_2 \xrightarrow{\tau^{-1}} \tau^{-1}(i_2) \\ \tau^{-1}(i_2) \xrightarrow{\tau} i_2 \xrightarrow{\varphi} i_3 \xrightarrow{\tau^{-1}} \tau^{-1}(i_3) \end{array}$$

$$\psi = \tau^{-1}\varphi\tau = (\tau^{-1}(i_1), \tau^{-1}(i_2), \dots, \tau^{-1}(i_t))$$
$$\psi = \mu\varphi\mu^{-1} = (\mu(i_1), \mu(i_2), \dots, \mu(i_t)) \qquad \tau^{-1} = \mu$$

Спрягане на произведение: $\mu\varphi_1\varphi_2 \dots \varphi_s\mu^{-1} = (\mu\varphi_1\mu^{-1})(\mu\varphi_2\mu^{-1}) \dots (\mu\varphi_s\mu^{-1})$

Твърдение: Ако φ е представен като независими цикли

$$\varphi = \psi_1 \circ \psi_2 \circ \dots \circ \psi_s = \left(i_1^{(1)}, \dots, i_{\tau_1}^{(1)}\right)\left(i_1^{(2)}, \dots, i_{\tau_2}^{(2)}\right) \dots \left(i_1^{(s)}, \dots, i_{\tau_s}^{(s)}\right)$$
$$\mu\varphi\mu^{-1} = (\mu\psi_1\mu^{-1}) \circ \dots \circ (\mu\psi_s\mu^{-1}) = \left(\mu(i_1^{(1)}), \dots, \mu(i_{\tau_1}^{(1)})\right) \dots \left(\mu(i_1^{(s)}), \dots, \mu(i_{\tau_s}^{(s)})\right)$$

3. **Транспозиции и представяне на елементите като произведение на транспозиции**

Деф: Цикъл с дължина 2 се нарича **транспозиция**: $\tau = (x, y)$, $\tau^2 = id$

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

$(i_1, \dots, i_k) = (i_1, i_k) \dots (i_1, i_5)(i_1, i_4)(i_1, i_3)(i_1, i_2)$

Има най-различни представяния:

$j \notin \{i_1, \dots, i_k\} \quad (j, i_1)(j, i_k) \dots (j, i_5)(j, i_4)(j, i_3)(j, i_2)(j, i_1)$

Св-ва:

1. $(b, c)(a, x) = (a, x)(b, c)$, когато (a, x) и (b, c) са независими (различни числа)
2. $(a, b)(a, x) = \varphi = (a, x, b) = (b, x)(a, b) \qquad \varphi(x) = b,\ \varphi(a) = x,\ \varphi(b) = a$
3. $\psi = (b, x)(a, x) = (a, b, x) = (a, x)(a, b) \qquad \psi(a) = b, \psi(x) = a, \psi(b) = x$
4. $\tau = (a, x)(a, x) = id \qquad \tau(a) = a, \tau(x) = x$

Теорема: S_n

a) Ако $\tau_1 \circ \dots \circ \tau_k = id$ и $\tau_1, \dots, \tau_k$ са транспозиции, тогава k е четно число

b) Ако $\varphi = \tau_1 \dots \tau_k = \mu_1 \dots \mu_s$ и τ_i, μ_j са транспозиции, тогава $k \equiv s \pmod 2$

Деф: Четен и нечетен елемент на S_n

Нека $\varphi = \tau_1 \dots \tau_k \quad (\tau_i - \text{транспозиции})$

φ е четен елемент на S_n, ако k е четно число

φ е нечетен елемент на S_n, ако k е нечетно число

id - четна пермутация (елемент от S_n)

$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$. φ е четна пермутация $\Leftrightarrow i_1, \dots, i_n$ е четна пермутация

(т.е. има четен брой инверсии)

$(i_1, \ldots, i_k)$ е четна пермутация $\Leftrightarrow k$ е нечетно число.

4. **Алтернативна група**

Деф: Алтернативна група

$A_n = \{\varphi \in S_n \mid \varphi\ -\text{четна пермутация}\}$

$B_n = \{\varphi \in S_n \mid \varphi\ -\text{нечетна пермутация}\}$

$A_n < S_n$ - алтернативна група

- четна $\cdot$ четна $=$ четна (пермутация)
- $\varphi = \tau_1 \ldots \tau_s$ - транспозиции, $\varphi^{-1} = \tau_s \tau_{s-1} \ldots \tau_1$, φ - четна $\Rightarrow \varphi^{-1}$ $-$ четна
- Id - четна

5. **Теорема на Кейли**

Деф: Теорема на Кейли

Всяка група G е изоморфна на подгрупа на симетричната група $S(G)$

$|G| = n \quad \Rightarrow \quad G \cong H < S_n$

Д-во:

Нека $(G,\cdot)$, $S(G) = \{\varphi: G \to G \mid \varphi\ -\text{биекция}\}$

$a \in G \quad \varphi_a: G \to G \quad \varphi_a(x) = ax \in G \quad (x \in G)$

$\varphi_a(x) = \varphi_a(y) \Leftrightarrow ax = ay \Leftrightarrow a^{-1}(ax) = a^{-1}(ay) \Leftrightarrow x = y$ (инекция)

$t \in G \quad \varphi_a(x) = t \Rightarrow ax = t \Rightarrow x = a^{-1}t \Rightarrow t = \varphi_a(a^{-1}t)$ (сюрекция)

$\Rightarrow \varphi_a$ - биекция т.е. $\varphi_a \in S(G)$

$H = \{\varphi_a \mid a \in G\} \subset S(G)$

$(\varphi_a \circ \varphi_b)(x) = \varphi_a(\varphi_b(x)) = \varphi_a(bx) = abx = (ab)x = \varphi_{ab}x$

$\Rightarrow (\varphi_a \circ \varphi_b) = \varphi_{ab} \in H$

$(\varphi_a)^{-1} = \varphi_{a^{-1}}$ от $\varphi_{a^{-1}} \circ \varphi_a(x) = a^{-1}(ax) = x = id$

$\Rightarrow H < S(G)$

Ще докажем, че $G \cong H$. $\Phi: G \to H < S(G)$

$\Phi(a) = \varphi_a$

$\Phi(a) \circ \Phi(b) = \Phi(ab) \quad \varphi_a \circ \varphi_b = \varphi_{ab}$

$$\begin{matrix} a \to \Phi(a) = \varphi_a \\ b \to \Phi(b) = \varphi_b \end{matrix} \quad \varphi_a = \varphi_b \Leftrightarrow \begin{matrix} \varphi_a(x) = \varphi_b(x), \forall x \in G \\ ax = bx,\ \exists (x^{-1}) \end{matrix} \Leftrightarrow a = b \Rightarrow \Phi \text{ е инекция}$$

$H = \{\varphi_a = \Phi(a) \mid a \in G\} \Rightarrow \Phi$ е сюрекция

$\Rightarrow \Phi$ е изоморфизъм $\Rightarrow G \cong H < S(G)$

6. **Хомоморфизъм при групи, ядро и образ**

Деф: $(G_1,\cdot)$ $(G_2,*)$ $\varphi(a.b) = \varphi(a) * \varphi(b)$, φ е хомоморфизъм

Св-ва: на хомоморфизмите $\varphi: G_1 \to G_2$

1. $\varphi(e_1) = e_2 \quad e_1 \in G_1, \quad e_2 \in G_2$

   $\varphi(e_1.e_1) = \varphi(e_1) * \varphi(e_1)$

   $\varphi(e_1) = \varphi(e_1) * \varphi(e_1) \ /\ \varphi(e_1)^{-1}$

   $e_2 = (\varphi(a))^{-1}$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$

   $\varphi(e_1) = e_2$

   $\varphi(e_1) = \varphi(a.a^{-1}) = \varphi(a) * \varphi(a^{-1}) = e_2 \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1}$

Деф: Ядро и образ

$\varphi -$ хомоморфизъм, $\quad G_1 \to G_2, \quad (G_1,\cdot), \quad (G_2,*)$

$\boldsymbol{Ker\ \varphi} = \{a \in G_1 \mid \varphi(a) = e_2\} \subset G_1$ - **ядро**

$\boldsymbol{Im\ \varphi} = \{\varphi(a) \mid a \in G_1\} \subset G_2$ - **образ**

Твърдение: $\varphi: G_1 \to G_2$ хомоморфизъм, тогава $Ker\ \varphi < G_1,\ Im\ \varphi < G_2$

Деф: Съседни класове

$(G,\cdot)\quad H < G,\ a \in G$

$aH = \{\, ax \mid x \in H\}$ – ляв съседен клас

$Ha = \{xa \mid x \in H\}$ – десен съседен клас

$aH \subset G, Ha \subset G$

$(L,+),\ T < L,\ a \in L$

$a + T = \{a + x \mid x \in T\}$ – ляв съседен клас

$T + a = \{x + a \mid x \in T\}$ – десен съседен клас

Деф: $H < G$. Броят на левите съседни класове на H в G се нарича **индекс** на H в G, пишем $|G{:}H|$

Следствие:

1. $H < G \quad |H| \mid |G|$ (дели), $|G{:}H| \mid |G|$
2. $a \in G,\ |G| < \infty \Rightarrow |a| \mid |G|,\ |a|$ - реда на ел. а
3. Ако $|G| = p$ - просто число $\Rightarrow$ G е циклична група

Теорема: на Лагранж

Ако $(G,\cdot)$ е крайна група $|G| < \infty$ и $H < G$, тогава $|G| = |H|\,.\,|G{:}H|$

Твърдение: $\varphi: G_1 \to G_2$ хомомоморфизъм, $a \in G_1,\ H = Ker\ \varphi < G_1$

$$\left.\begin{array}{l}\varphi(b) = \varphi(a) \Leftrightarrow b \in aH \\ \varphi(b) = \varphi(a) \Leftrightarrow b \in Ha\end{array}\right\} \Rightarrow aH = Ha$$

Деф: G - група, $H < G$, H е нормална подгрупа на G, когато $aH = Ha,\ \forall a \in G$, пишем $H \lhd G$

Деф: (G,·), $H \lhd G, G/H = \{\, aH \mid a \in G\}$ G/H е група и се нарича **факторгрупа**

- Факторгрупата не е подгрупа на G

Теорема: за хомоморфизмите при групи

Нека $\varphi: G_1 \to G_2$ е хомоморфизъм, тогава:

- $Ker\ \varphi \lhd G_1$
- $Im\ \varphi \cong G_1/Ker\ \varphi$

Д-во:

$H = Ker\ \varphi.$

$\varphi(a) = \varphi(b) \Leftrightarrow b \in aH \Leftrightarrow b \in Ha$ и $aH = Ha\quad \forall a \quad \Rightarrow Ker\ \varphi \lhd G$

$\varphi(a) = \varphi(b) \Leftrightarrow aH = bH$

$\psi: G_1/Ker\ \varphi \to Im\ \varphi \qquad \psi(aH) = \varphi(a)$

$aH = bH \Rightarrow \varphi(a) = \varphi(b)$

$\psi(aH) = \psi(bH) \Leftrightarrow \varphi(a) = \varphi(b)$

$\psi(aH\,.\,cH) = \psi(acH) = \varphi(ac) = \varphi(a).\varphi(c) = \psi(aH).\psi(cH)$

$x \in Im\ \varphi \Rightarrow \exists d \in G_1 : \varphi(d) = x = \psi(dH)$ - сюрекция

$\psi(mH) = \psi(tH) \Leftrightarrow \varphi(m) = \varphi(t) \Leftrightarrow t \in mH \Leftrightarrow t\ Ker\ \varphi = m\ Ker\ \varphi$ - инекция

$\Rightarrow \psi$ е биекция

$\Rightarrow$ ψ е изоморфизъм $\Rightarrow G_1/Ker\ \varphi \cong Im\varphi$

Допълнително инфо

Св-ва: на съседните класове

1. $aH < G \Leftrightarrow a \in H \Leftrightarrow aH = H \quad Ha < G \Leftrightarrow a \in H \Leftrightarrow Ha = H$
2. $b \in aH \Leftrightarrow bH \equiv aH \qquad c \in Ha \Leftrightarrow Ha \equiv Hc$
3. $aH \cap bH = \begin{cases} \emptyset, & \text{ако } b \notin aH \\ aH = bH, & \text{ако } b \in aH \end{cases} \qquad Ha \cap Hb = \begin{cases} \emptyset, & \text{ако } b \notin Ha \\ Ha = Hb, & \text{ако } b \in Ha \end{cases}$
4. $G = \bigcup_{a \in G} aH = a_1H \cup a_2H \cup \cdots \cup a_sH$
5. $aH = bH \Leftrightarrow b \in aH \Leftrightarrow a^{-1}b \in H$
6. Ако $|H| < \infty \Rightarrow |aH| = |H| = |Ha|$: $\quad ah_1 = ah_2 \Leftrightarrow h_1 = h_2 \Leftrightarrow h_1a = h_2a$
7. Нека $H < G$ $\mathrm{L_H} = \{aH \mid a \in G\}$ $\quad R\_H = \{ Ha \mid a \in G\}$,
   тогава L_H и R_H са равномощни, т.е. ∃ биекция от L в R
8. Броят на левите съседни класове = броят на десните съседни класове