

23. Симетрична и алтернативна група. Действие на група върху множество.

Теорема на Кейли и формула за класовете.

Симетрична група S_n – представяне на елементите като произведение на независими цикли. Спрягане на елементите на S_n . Транспозиции и представяне на елементите като произведение на транспозиции. Алтернативна група. Действие на група върху множество – орбити и стабилизатори, транзитивно действие. Формула за класовете. Теорема на Кейли.

Примерна задача: Представяне на елементите на S_n като произведение на независими цикли и действия в S_n .

Симетрична група.

Дефиниция: С S_n означаваме **симетричната група** от степен n , т.е. множеството от всички биекции на множеството $\Omega_n = \{1, 2, \dots, n\}$ в себе си с операцията композиция на изображения. Единицата на S_n е идентитетът на Ω_n , който ще бележим с (1) .

$\Psi \in S_n$; $\Psi = (1 \ 2 \ 3 \dots n)$ – къде отива всеки елемент.

$$i_1 \ i_2 \ i_3 \dots i_n$$

- Тъй като Ψ е биекция, то $i_1, i_2, i_3, \dots, i_n$ е пермутация на $1, 2, \dots, n \Rightarrow |S_n| = n!$
- Групата S_n не е комутативна!

Пример: $\Psi = (1 \ 2 \ 3)$: $\Psi = |3|$, защото $\Psi^3 = \text{id} < \Psi > = \{\text{id}, \Psi, \Psi^2\}$
 $2 \ 3 \ 1$

Дефиниция: Под **цикъл** разбираме пермутация Ψ , действаща по правилото: $\Psi(i_1)=i_2, \Psi(i_2)=i_3, \dots, \Psi(i_{k-1})=i_k, \Psi(i_k)=i_1$, а всички останали числа от Ω_n остават на място под действието на Ψ , където $i_1, i_2, \dots, i_k$ са различни числа от Ω_n . Числото k наричаме дължина на цикъла. Пишем $\Psi = (i_1, i_2, \dots, i_k)$. Цикъл с дължина 2 наричаме **транспозиция**. Два цикъла $(i_1, i_2, \dots, i_k)$ и $(j_1, j_2, \dots, j_n)$ се наричат **независими**, ако $\{i_1, i_2, \dots, i_k\}$ и $\{j_1, j_2, \dots, j_n\}$ нямат общи елементи. Всеки 2 независими цикъла τ и δ комутират, т.е. $\tau\delta = \delta\tau$.

Теорема1: Всеки неединичен елемент на S_n може да се представи като произведение на независими цикли $\tau_1 \tau_2 \dots \tau_t$ и това представяне е единствено с точност до реда на множителите.

Доказателство:

1. Съществуване: Нека i_1 е произволно число от Ω_n . Разглеждаме $i_1, i_2 = \Psi(i_1), i_3 = \Psi(i_2), \dots, i_k = \Psi(i_{k-1})$, където k е максимално естествено число, за което тези числа са

различни. Тогава $\Psi(i_k)$ е някое от тях. Твърдим, че $\Psi(i_k) = i_1$. Действително това е изпълнено при $k = 1$, а ако $k > 1$ и например $\Psi(i_k) = i_2$, то $\Psi(i_k) = \Psi(i_1)$, а $i_k \neq i_1 \Rightarrow$ противоречие! $\Rightarrow \Psi(i_k) = i_1$. Нека сега $\tau_1 = (i_1, i_2, \dots, i_k)$ и j_1 е число от Ω_n (ако има такова), което не участва в τ_1 . Аналогично получаваме цикъл $\tau_2 = (j_1, j_2, \dots, j_s)$, τ_1 и τ_2 са независими (в противен случай бихме получили две различни числа с еднакви образи)! Продължаваме така докато не изчерпаме всички числа. Очевидно Ψ е произведение на получените независими цикли.

2. Единственост: Нека $\Psi = \tau_1 \tau_2 \dots \tau_t = \tau_1' \tau_2' \dots \tau_m'$. Всяко число от Ω_n участва и в двете разлагания. Нека например $i \in \Omega_n$ участва в τ_1 и τ_1' (например). Тогава $\tau_1 = \tau_1'$ (иначе има противоречие с това, че е биекция) $\Rightarrow \tau_2 \dots \tau_t = \tau_2' \dots \tau_m'$. След неколkokратно прилагане на аналогични разсъждения получаваме $t=m$ и $\tau_2 = \tau_2', \dots, \tau_t = \tau_t'$ (след евентуално преномериране на $\{\tau_i'\}$).

Свойства:

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

Твърдение:

Нека $\Psi = \tau_1 \tau_2 \dots \tau_s \in S_n$, τ_i - независими цикли. Тогава редът на Ψ е $|\Psi| = \text{НОК}(|\tau_1|, |\tau_2|, \dots, |\tau_s|)$.

Доказателство: Нека $\Psi = \tau_1 \tau_2$, $|\Psi| = r$, $|\tau_1| = k$, $|\tau_2| = t$ и $(\tau_1 \tau_2)^r = \tau_1^r \tau_2^r = \text{id} \Rightarrow \tau_1^r = \tau_2^{-r}$

Ако $\tau_1 = (i_1, i_2, \dots, i_k)$, то $(\tau_1(i_1))^r \in \{i_1, i_2, \dots, i_k\}$ и ако $\tau_2 = (j_1, j_2, \dots, j_t)$, то $(\tau_2(i_1))^r = i_1 \Rightarrow (\tau_1(i_1))^r = i_1 \Rightarrow$ аналогично $(\tau_1(i_p))^r = i_p$, за всяко $p=1, \dots, k$.

$\tau_1^r = \text{id}$ и $\tau_2^r = \text{id} \Rightarrow k/r$ и $t/r \Rightarrow \text{НОК}(k, t)/r$.

$(\tau_1 \tau_2)^{\text{НОК}(k,t)} = \tau_1^{\text{НОК}(k,t)} \tau_2^{\text{НОК}(k,t)} = (\tau_1^k)^{t1} (\tau_2^t)^{k1} = \text{id} \Rightarrow r/\text{НОК}(k, t) \Rightarrow r = \text{НОК}(k, t)$

Спрягане ' ~ ':

$\tau \Psi \tau^{-1} = \eta \Rightarrow \tau^{-1} \eta \tau = \Psi \quad (\Psi \sim \eta, \eta \sim \Psi)$

- $\Psi \sim \Psi \Rightarrow \Psi = \text{id} \Psi \text{id}^{-1}$

- $\Psi \sim \eta \Rightarrow \eta \sim \Psi$

- $\Psi \sim \eta$ и $\eta \sim \zeta \Rightarrow \Psi \sim \zeta$

$(\Psi = \tau_1 \eta \tau_1^{-1}, \zeta = \tau_2 \Psi \tau_2^{-1} = \tau_1 \tau_2 \eta \tau_1^{-1} \tau_2^{-1} = (\tau_1 \tau_2) \eta (\tau_1 \tau_2)^{-1}) \Rightarrow \text{' ~ ' е релация на еквивалентност!}$

Твърдение: Нека Ψ и $\tau \in S_n$ пермутациите са спрегнати точно когато имат еднакъв цикличен строеж, т.е. τ и Ψ са произведение на еднакъв брой независими цикли със (след евентуално размятане) съответно равни дължини.

Доказателство: Нека Ψ и τ са спрегнати $\tau = \eta \Psi \eta^{-1}$.

$$\Psi = (i_1 \dots i_{k_1})(j_1 \dots j_{k_2}) \dots (t_1 \dots t_{k_t})$$

$$\eta = (\quad i_1 \dots i_{k_1} \quad j_1 \dots j_{k_2} \dots t_1 \dots t_{k_t} \mid s_1 \dots s_l \quad)$$

$$p_1 \dots p_{k_1} \quad q_1 \dots q_{k_2} \dots r_1 \dots r_{k_t} \mid u_1 \dots u_l$$

$$\tau(p_1) = \eta(\Psi(\eta^{-1}(p_1))) = \eta\Psi(i_1) = \eta(i_2) = p_2$$

$$\tau(p_2) = p_3$$

.....

$$\tau(p_{k_1}) = p_1$$

$\Rightarrow (p_1, p_2, \dots, p_{k_1})$ е цикъл, които участва в записа на τ .

Аналогично получаваме същото за $(q_1 \dots q_{k_2}), \dots, (r_1 \dots r_{k_t})$. Тъй като може не всички елементи да участват в записа на τ , това са $s_1 \dots s_l$.

$$\tau(u_i) = \eta(\Psi(\eta^{-1}(u_i))) = \eta(\Psi(s_i)) = \eta(s_i) = u_i \Rightarrow \tau(u_i) = u_i \Rightarrow u_i \text{ са неподвижни за } \tau \Rightarrow$$

$\tau = (p_1, \dots, p_{k_1}) \dots (r_1, \dots, r_{k_t})$, т.е. τ има същия цикличен строеж като Ψ .

Свойства:

1. Всеки елемент от S_n може да се представи като произведение на транспозиции, като това представяне не е единствено. Следва от:
 $(i_1, i_2, \dots, i_{t-1}, i_t) = (i_{t-1}, i_t)(i_{t-2}, i_t) \dots (i_2, i_t)(i_1, i_t)$, което се проверява непосредствено.
2. Ако идентитетът $id = \tau_1 \tau_2 \dots \tau_r$, където τ_i са транспозиции, то тогава r е четно.
3. Ако един елемент (пермутация) се представя по два начина като произведение на транспозиции, то броят на множителите в тези представянията е с една и съща четност, т.е. ако $\Psi = \tau_1 \tau_2 \dots \tau_r = \eta_1 \eta_2 \dots \eta_s$ (τ_i, η_i са транспозиции), то $r \equiv s \pmod{2}$.
 - $(i_1 \dots i_r) = (i_1 i_r)(i_1 i_{r-1}) \dots (i_1 i_3)(i_1 i_2)$, т.е. $i_1 \rightarrow i_2 \rightarrow \dots \rightarrow i_r$
 - $(i, j)(i, k) = (i, k)(k, j)$
 - $(i, j)(j, i) = id$
 - $(i, j)(k, s) = (k, s)(i, j)$

Дефиниция: Елементът $\Psi \in S_n$ е **четен**, ако може да се представи като произведение на четен брой транспозиции.

Ψ - четен, η - нечетен $\Rightarrow \Psi \cdot \eta$ - нечетен, $\eta \cdot \Psi$ - нечетен

Ψ, η – еднаква четност $\Rightarrow \eta \cdot \Psi$ – четен, $\Psi \cdot \eta$ - четен.

Една пермутация се нарича четна, ако броя на двойките числа $(i_k > i_s, \text{ но } k < s)$, образуващи инверсия е четен.

(!) - Когато всички транспозиции са нечетни пермутации, цикълът $(i_1, i_2, \dots, i_k)$ е четна пермутация когато k е нечетно число.

Твърдение: Във всяко представяне на една пермутация като произведение на транспозиции броят на множителите е с една и съща четност. При това

пермутацията е четна точно когато броят на множителите във всяко такова представяне е четно число.

Дефиниция: Множеството от всички четни пермутации е подгрупа на S_n и се нарича

A_n - алтернативна група от степен n .

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

A_n е подгрупа на S_n защото, ако $\Psi, \eta \in A_n \Rightarrow \Psi \cdot \eta \in A_n$ и $\Psi^{-1} \in A_n$ (От горното тв.)

$|A_n| = |S_n|/2 = n!/2 \Rightarrow |S_n:A_n| = 2 \Rightarrow A_n \trianglelefteq S_n$.

Твърдение. Групата A_n ($n \geq 3$) се поражда от всички тройни цикли.

Док.: Всяка четна пермутация е произведение на четен брой транспозиции и $(ij)(kl) = (jkl)(ilj)$ и $(ij)(il) = (ilj)$.

Действие на група върху множество – орбити и стабилизатори. Теорема на Кейли.

Определение: Нека G -група и H е непразно подмножество на G . H е **подгрупа** на G , ако за всеки $x, y \in H \Rightarrow xy \in H$ и, ако от $x \in H \Rightarrow x^{-1} \in H$. Означения за подгрупа: $H \leq G$ и $H < G$.

Определение: Нека G и G' са групи и $\Phi: G \rightarrow G'$ е изображение. Тогава:

- 1) Φ е **хомоморфизъм**, ако $\Phi(ab) = \Phi(a)\Phi(b)$, за всяко $a, b \in G$.
- 2) Φ е **изоморфизъм**, ако Φ е хомоморфизъм и биекция ($G \cong G'$)

Определение: Нека Ω – множество, G -група. Ще казваме, че групата G **действа в/у** множеството Ω , ако на всеки елемент $g \in G$ и на всеки елемент $x \in \Omega$ е съпоставен елемент $gx \in \Omega$, като се изпълняват следните две условия:

- 1) $1x = x$, всяко $x \in \Omega$ (1 единичен елемент на G).
- 2) $(g_1g_2)x = g_1(g_2x)$, за всеки $g_1, g_2 \in G$, всяко $x \in \Omega$

Свойства:

- Ако G действа върху Ω , то всеки елемент $g \in G$ задава изображение $\Phi_g: \Omega \rightarrow \Omega$ чрез равенството $\Phi_g(x) = gx$ ($x \in \Omega$). Директно се проверява, че Φ_g е биекция $\Rightarrow \Phi_g$ е елемент на симетричната група S_Ω ($\Phi_g \in S_\Omega$).
- Всяко действие на G върху Ω задава изображение $\Psi: G \rightarrow S_\Omega$ чрез равенството $\Psi(g) = \Phi_g$, като Ψ е хомоморфизъм на G в S_Ω .
 $\Phi_g \cdot \Phi_h = \Phi_{gh}$, защото $(\Phi_g \cdot \Phi_h)(x) = \Phi_g(\Phi_h(x)) = \Phi_g(hx) = g(hx) = (gh)x = \Phi_{gh}(x)$
- **Извод :** Задаването на действие на група G върху множество Ω е еквивалентно на хомоморфизъм $\Psi: G \rightarrow S_\Omega$

$\text{Ker } \Psi = \{g \in G \mid gx=x, \text{ всяко } x \in \Omega\} = \{1\} = \{e\}$
 $G/\text{Ker } \Psi \approx \text{Im } \Psi$ е подмножество на S_Ω .

В следващата теорема ще разгледаме случая, когато $\Omega=G$.

Теорема на Кейли : Всяка група от ред n е изоморфна на подгрупа на симетричната група S_n .

Доказателство: Нека G е крайна група и $|G| = n$. Нека a е фиксиран елемент на G . Дефинираме изображение $L_a : G \rightarrow G$ като, ако $g \in G$, то $L_a(g) = ag$.

L_a е биекция:

Нека $g_1 \neq g_2$. Да допуснем, че $L_a(g_1) = L_a(g_2) \Rightarrow ag_1 = ag_2 \cdot a^{-1}$ отляво $\Rightarrow g_1 = g_2 \Rightarrow$ противоречие $\Rightarrow L_a(g_1) \neq L_a(g_2)$. Нека $g \in G$ е произволен елемент от G и $h = a^{-1}g$. Имаме $L_a(h) = ah = (aa^{-1})g = eg = g \Rightarrow$ съществува $h \in G$, такъв че за всяко $g \in G$, $L_a(h) = g \Rightarrow L_a$ – биекция. $\Rightarrow L_a \in S_G = S_n$.

$G' = \{L_a \mid a \in G\}$ е подмножество на S_n . Ще докажем, че $G' \leq S_n$:

Нека $L_a, L_b \in G'$ и g – произволен елемент от G . Имаме:

$$(L_a L_b)(g) = L_a(L_b(g)) = L_a(bg) = a(bg) = (ab)g = L_{ab}(g) \Rightarrow L_a L_b = L_{ab} \in G' \quad (1)$$

Също така да намерим обратния елемент на L_a : $L_a L_{a^{-1}} = L_{aa^{-1}} = L_e = e$ (от (1)).

Аналогично $L_{a^{-1}} L_a = L_{a^{-1}a} = L_e = e \Rightarrow$

$$(L_a)^{-1} = L_{a^{-1}} \in G' \quad (2)$$

От (1) и (2) $\Rightarrow G' \leq S_n$.

Разглеждаме изображението $\Psi : G \rightarrow G'$, т. че $\Psi(a) = L_a$. Ще докажем, че Ψ е изоморфизъм:

- От $L_{ab} = L_a L_b \Rightarrow \Psi(ab) = \Psi(a)\Psi(b) \Rightarrow \Psi$ – хомоморфизъм.
 - Ψ очевидно е изображение на G върху G' .
 - Нека $a, b \in G$, $a \neq b$. Допускаме, че $\Psi(a) = \Psi(b)$, т.е. $L_a = L_b \Rightarrow L_a(e) = L_b(e) \Rightarrow a = b \Rightarrow$ противоречие $\Rightarrow \Psi(a) \neq \Psi(b)$ т.е. Ψ е биекция.
- $\Rightarrow \Psi$ е изоморфизъм $\Rightarrow G \approx G' \leq S_n$.

*Нека до края Ω е крайно множество, а G крайна група, действаща върху Ω .

Определение: Нека $x \in \Omega$. Под **стабилизатор на x** в групата G ще разбираме множеството $\text{St}_G(x) = \{g \in G \mid gx=x\}$.

Свойство1: Стабилизаторът в G на всеки елемент $x \in \Omega$ е подгрупа на G , т.е. $x \in \Omega \Rightarrow \text{St}_G(x) < G$.

Д-во: Нека $S = \text{St}_G(x)$ и $g_1, g_2 \in S$, т.е. $g_1 x = x$ и $g_2 x = x$. Искаме $S \leq G$, като имаме $g_1, g_2 \in S$ и S е подмножество на G и $(g_1 g_2)x = g_1(g_2 x) = g_1 x = x \Rightarrow g_1 g_2 \in S$.

Ако $g \in S$ (т.е. $gx=x$), то $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = x \Rightarrow g^{-1} \in S \Rightarrow S \leq G$.

Дефиниция: Нека $x, y \in \Omega$. $y \sim x$ (е еквивалентно на y) ако съществува $g \in G$, такова че $y=gx$.

$\sim$ е релация на еквивалентност. Тогава множеството Ω се разбива на непреципащи се класове на еквивалентност, които се наричат **G – орбити**. Орбитата съдържаща даден елемент x бележим с $O(x)$. Очевидно $O(x) = \{gx \mid g \in G\}$ – орбита на x .

Свойство2: $x \in \Omega$; $x \sim y$, т.е. $y \in O(x) \Leftrightarrow O(x) = O(y)$.

Д-во: $y \in O(x) \Rightarrow y=gx \Rightarrow x = g^{-1}y$

$a \in O(x) \Rightarrow a=hx = (hg^{-1})y \Rightarrow a \in O(y) \Rightarrow O(x)$ е подмножество на $O(y)$ *

$b \in O(y) \Rightarrow b=ty = (tg)x \Rightarrow b \in O(x) \Rightarrow O(y)$ е подмножество на $O(x)$ **

От * и ** $\Rightarrow O(x) = O(y)$.

Свойство3: $x \in \Omega$, $g_1, g_2 \in G$: $g_1x=g_2x \Leftrightarrow g_2^{-1}g_1 \in St_G(x)$

$g_1x = g_2x \Leftrightarrow g_2^{-1}g_1x = g_2^{-1}g_2x \Leftrightarrow g_2^{-1}g_1x = x \Leftrightarrow g_2^{-1}g_1 \in St_G(x) \Leftrightarrow g_2 St_G(x) = g_1 St_G(x)$

Свойство4: Съществува биективно съответствие между $\{gSt_G(x) \mid g \in G\}$ и $O(x)$

Твърдение: Нека $x \in \Omega$. Тогава $|O(x)| = |G:St_G(x)|$ в частност $|O(x)|/|G|$.

Д-во: Нека $S = St_G(x)$ и $g_1, g_2 \in G$.

$g_1x = g_2x \Leftrightarrow (g_2^{-1}g_1)x = x \Leftrightarrow g_2^{-1}g_1 \in S \Leftrightarrow g_1S = g_2S$. Това означава, че броят на различните образи на x под действието на всевъзможните елементи на групата G е равен на броя на различните съседни класове на G по подгрупата S . С други думи $|O(x)| = |G:S|$.

По Теоремата на Лагранж $\Rightarrow |G|=|S| \cdot |G:S| \Rightarrow |G|=|S| \cdot |O(x)| \Rightarrow |O(x)| / |G|$.

Твърдение: Нека $\Omega_1, \Omega_2, \dots, \Omega_s$ са всичките G – орбити в Ω и нека $x_i \in \Omega_i$ т.е. $\Omega_i=O(x_i)$, $i=1, \dots, s$. Тогава $|\Omega| = \sum |\Omega_i| = \sum |G:St_G(x_i)| \quad /i=1, \dots, s \text{ за сумите}/$.

Определение: Ще казваме, че групата **G действа транзитивно** върху множеството Ω , ако за всеки два елемента $x, y \in \Omega$, съществува елемент $g \in G$, т. че $y = gx$.

От определението за транзитивно действие $\Rightarrow$ че за всяко $x \in \Omega$ орбитата $O(x)$ съвпада с Ω , т.е. Ω е единствената G – орбита.

Твърдение: Ако G действа транзитивно върху Ω , то числото $|\Omega|$ дели числото $|G|$.

Формула за класовете:

Определение: Нека групата G действа върху себе си чрез спрягане. Тогава орбитата $O(x)$ на елемент $x \in G$ се нарича клас спрегнати с x елементи и се бележи с C_x , $C_x = \{gxg^{-1} \mid g \in G\}$. Стабилизаторът $St_G(x) = \{g \in G \mid gxg^{-1} = x\}$ се нарича централизатор на G и се бележи $C_G(x)$ или $C(x)$. Тогава $|\Omega| = \sum |\Omega_i| = \sum |G:St_G(x_i)|$ приема вида:

$$|G| = \sum |C_{x_i}| = \sum |G:C_G(x_i)| \quad i = 1 \dots s \quad (1)$$

Нека $Z(G)$ е центъра на G , т.е. $Z(G) = \{x \in G \mid xg = gx \text{ за всяко } g \in G\}$. Тъй като $xg = gx \Leftrightarrow gxg^{-1} = x$, то $Z(G)$ се състои от тези елементи x на G , за които $C_x = \{x\}$. Тогава всеки елемент $x \in Z(G)$ участва като някое x_i в равенството (1) и съответно събираемо $|C_{x_i}|$ има стойност равна на 1.

Нека $Z(G) = \{x_1, \dots, x_t\}$, $1 \leq t \leq s$ и сега равенството (1) може да се запише така:

$$|G| = \sum |C_{x_i}| + \sum |C_{x_j}| = |Z(G)| + \sum |C_{x_j}| = |Z(G)| + \sum |G:C_G(x_j)| \quad i=1, \dots, t; \quad j = t+1, \dots, s$$

$$\Rightarrow |G| = |Z(G)| + \sum |G:C_G(x_i)|$$

Където $x_{t+1}, \dots, x_s$ са представители на класовете спрегнати елементи на G , нележащи в $Z(G)$, се нарича формула за класовете.