Симетрична и алтернативна група. Действие на група върху множество. Теорема на Кейли и формула за класовете.

///**20. 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 а класовете. Теорема на Кейли.

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

Симетрична група.

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

Ψ ∈ Sn ; Ψ = (1 2 3 .... n) – където отива всеки елемент.
i1 i2 i3........... in

- Тъй като Ψ е биекция, то i1, i2, i3,........... in е пермутация на 1,2,.... n => **|Sn|=n!** .
- Групата Sn не е комутативна, за n>2!

Пример: Ψ = (1 2 3): Ψ=|3| , защото Ψ^3 =id < Ψ >={id, Ψ , Ψ^2}
2 3 1

Дефиниция: Под **цикъл** разбираме пермутация Ψ, действаща по правилото : Ψ(i1)=i2Ψ(i2)=i3..... Ψ(ik-1) =ikΨ(ik)=i1, а всички останали числа от Ωn остават на място под действието на Ψ, където i1,i2…,ik са различни числа от Ωn. Числото k наричаме дължина на цикъла. Пишем Ψ=(i1,i2,…,ik) . Цикъл с дължина 2 наричаме **транспозиция.** Два цикъла (i1,i2,….,ik) и (j1,j2,…,jn) се наричат **назависими,** ако {i1,i2,…..,ik} ^{j1,j2,…….,jn} = 0. Всеки 2 независими цикъла комутират, т.е. τδ=δτ. Всеки цикъл с дължина 1 съвпада с единичния елемент на Sn -(1).

<u>Теорема. :</u>Всеки нееднинчен елемент на Sn може да се представи като произведение на независими цикли $\tau 1\ \tau 2\ldots\ \tau t$ и това представяна е единствено с точност до реда на множителите.

<u>Доказателство:</u>

1.Съществуване: Нека i1 е произволно число от Ωn. Разглеждаме $i1, i2= \Psi(i1)$, $i3= \Psi(i2),\ldots, ik= \Psi(ik-1)$, където k е максимално естествено число, за което тези числа са различни. Тогава $\Psi(ik)$ е някое от тях. Твърдим, че $\Psi(ik)=i1$. Действително това е изпълнено при k=1, а ако к>1 и например $\Psi(ik)=i2$, то $\Psi(ik)= \Psi(i1)$, а $ik!=i1$ => противоречие! => $\Psi(ik)=i1$. Нека $\tau 1=(i1,i2,\ldots,ik)$ и j1 е число от Ωn(ако има такова) , което не участва в $\tau 1$. Аналогично получаваме циктл $\tau 2=(j1,j2,\ldots,js)$, $\tau 1$ и $\tau 2$ са независими! Продължаваме така докато не изчерпаме всички числа. Очевидно Ψ е произведение на получените независими цикли.

2. Единственост: Нека $\Psi=\tau 1\tau 2\ldots\tau t=\tau 1'\tau 2'\ldots\tau m'$. Всяко число от Ωn участва и в двете разлагания. Наке например участва в $\tau 1$ и $\tau 1'$. Тогава $\tau 1= \tau 1'$(иначе има противоречие с това, че е биекция) => $\tau 2\ldots\tau t=\tau 2'\ldots\tau m'$. Аналогично $\tau 2=\tau 2'\ldots\ \tau t=\tau t'$.

<u>Свойства:</u>

1. $|(i1,i2,\ldots,ik)|=k$
2. $(i1,i2,\ldots ik)^{-1}=(ik,ik-1,\ldots,i1)$

<u>Твърдение:</u>

Нека $\Psi=\tau 1\tau 2\ldots\tau s \in Sn$, τi- независими цикли. Тогава редът на Ψ е $|\Psi|=НОК(|\tau 1|,|\tau 2|,\ldots,|\tau s|)$.

<u>Доказателство:</u> Нека $\Psi=\tau 1\tau 2$, $|\Psi| = r$ $|\tau 1| = k$ $|\tau 2| = t$ $(\tau 1\tau 2)^r= \tau 1^r\ \tau 2^r = id$ => $\tau 1^r=\tau 2^{-r}$

Ако $\tau 1=(i1,i2,\ldots,ik)$, то $(\tau 1(i1))^r \in \{i1,i2,\ldots,ik\}$ и Ако $\tau 2 = (j1,j2,\ldots,jt)$, то $(\tau 2(i1))^{-r} = i1$ =>

$(\tau 1(i1))^r =i1$ =>аналогично $(\tau 1(ip))^r= ip$ за всяко p=1, …k.

$\tau 1^r=id$ и $\tau 2^r=id$ => k/r и t/r => НОК(k,t)/r.

$(\tau 1\ \tau 2)^{НОК(k,t)}= \tau 1^{НОК(k,t)}\ \tau 2^{НОК(k,t)}=(\tau 1^k)^{t1}(\tau 2^t)^{k1}= id$ => r/ НОК(k,t)=> r= НОК(k,t)

<u>Спрягане ‘ ~ ‘ , Ψ~η :</u>

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

- $\Psi\sim\Psi=id\Psi id^{-1}$
- $\Psi\sim\eta$ => $\eta\sim\Psi$
- $\Psi\sim\eta$ и $\eta\sim\zeta$ =>$\Psi\sim\zeta$

$(\Psi=\tau 1\eta\tau 1^{-1}$, $\zeta= \tau 2\Psi\tau 2^{-1} = \tau 1\tau 2\eta\tau 1^{-1}\tau 2^{-1} = (\tau 1\tau 2)\eta(\tau 1\tau 2)^{-1}$) => ‘ ~ ’ е релация на еквивалентност!

Твърдение: Нека Ψ и $\eta \in S_n$ пермутациите са спрегнати $\Leftrightarrow$ имат еднакъв цикличен строеж, т.е. η и Ψ са произведение на еднакъв брой независими цикли със съответно еднакви редове.

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

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

$$\eta=\begin{pmatrix} i_1 \ldots i_{k_1} & j_1 \ldots j_{k_2} \ldots f_1 \ldots f_{k_t} & | & s_1 \ldots s_l \\ p_1 \ldots p_{k_1} & q_1 \ldots q_{k_2} \ldots r_1 \ldots r_{k_t} & | & u_1 \ldots u_l \end{pmatrix}$$

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

$\tau(p_2)=p_3$

$\ldots$

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

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

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

$\tau(u_i)=\eta(\Psi(\eta^{-1}(u_i)))=\eta\Psi(s_i)=\eta(s_i)=u_i \Rightarrow \tau(u_i)=u_i \Rightarrow u_i$ са неподвижни за $\tau \Rightarrow \tau=(p_1,\ldots p_{k_1})\ldots(r_1,\ldots r_{k_t})$, 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.
2. Ако идентитетът $id=\tau_1\tau_2\ldots\tau_r$, 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 представяния е с една и съща четност, т.е. ако $\Psi=\tau_1\tau_2\ldots\tau_r=\eta_1\eta_2\ldots\eta_s$($\tau_i,\eta_i$ са транспозиции), то $r \equiv s \pmod 2$.

- $(i_1 \ldots i_r)=(i_1 i_r)(i_1 i_{r-1})\ldots(i_1 i_3)(i_1 i_2)$, т.е. $i_1 \to i_2 \to \ldots \to i_r$
- $(i,j)(i,k)=(i,k)(k,j)$
- $(i,j)(j,i)=id$
- $(i,j)(k,s)=(k,s)(I,j)$

Дефиниция:

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

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

Ψ-четен, η-четен или Ψ- нечетен, η- нечетен $\Rightarrow \eta.\Psi$ – четен, $\Psi.\eta$-четен.

(!) - Когато всички транспозиции са нечетни пермутации, цикълът (i1,i2,……,ik) е четна пермутация когато k е нечетно число.

Дефиниция:

Множеството от всички четни пермуСтации е подгрупа на Sn и се нарича **алтернативна група от степен n.**

An = {Ψ|Ψ ℮ Sn, Ψ – четна пермутация}

|An|= |Sn|/2 = n!/2 => |Sn:An| = 2 => An ∆ Sn или защото ако Ψ,η ℮ An=> Ψ.η℮An и Ψ^-1 ℮ An

<u>Действие на група върху множество – орбити и стабилизатори. Теорема на Кейли.</u>

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

1) 1x=x, всяко x ℮ Ω (1 единичен елемент на G).
2) (g1g2)x = g1(g2x), за всеки g1,g2 ℮ G, всяко x ℮ Ω

<u>Свойства:</u>

- Ако G действа върху Ω, то всеки елемент g ℮ G задава изображение Φg : Ω -> Ω чрез равенството Φg(x)=gx (x ℮ Ω). Директно се проверява, че Φg е биекция => Φg е елемент на симетричната група SΩ (Φg ℮ SΩ).
- Всяко действие на G върху Ω задава изображение Ψ: G-> SΩ чрез равенството Ψ(g)=Φg, като Ψ е хомоморфизъм на групи.
  Φg.Φh(x) =Φg(hx)= g(hx)= gh(x) = gh = Φgh(x).
- **Извод :** Задаването на действие на група върху множество е еквивалентно на хомоморфизъм Ψ от групата G в симетричната група SΩ
  KerΨ={g ℮ G| g(x)=x, всяко x ℮ G} = {1} = {e}
  G/Ker Ψ≈ImΨ е подгрупа на SΩ.

<u>**Теорема на Кейли :**</u> Всяка група от ред n е изоморфна на подгрупа на симетричната група Sn.

<u>Доказателство:</u> Нека G е крайна група и |G| = n. Нека <u>а</u> е фиксиран елемент на G. Дефинираме изображение La : G -> G посредством умножение от ляво с а, т.е. ако g ℮ G,

то La(g) = ag.

Проверка дали La е биекция :

Нека $g1 \neq g2$.   Да допуснем, че $La(g1) = La(g2) \Rightarrow ag1=ag2 /\ .a^{-1}$ отляво $\Rightarrow g1=g2 \Rightarrow$ противоречие $\Rightarrow La(g1) \neq La(g2)$. Нека $g \in G$ е произволен елемент от G и $h=a^{-1}g$. Имаме $La(h) = ah=(aa^{-1})g=eg=g \Rightarrow$ съществува $h \in G$:, че за всяко $g \in G$ $La(h)=g \Rightarrow La$ – биекция. $\Rightarrow La \in SG = Sn$.

$G'=\{La | a \in G\}$ е подмножество на Sn.Ще докажем, че $G' \leq Sn$:

Нека $La, Lb \in G'$ и g – произволен елемент от G. Имаме $(LaLb)(g) = La(Lb(g)) = La(bg) = a(bg) = (ab)g = Lab(g) \Rightarrow LaLb = Lab \in G'$ (1)

Също така $LaLa^{-1} = Laa^{-1} = Le = e$

Аналогично $La^{-1}La=La^{-1}a = Le = e$ $\} \Rightarrow (La)^{-1} = La^{-1} \in G'$ (2)

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

Разглеждаме изображението $\Psi: G \to G'$, дефинирано чрез равенството $\Psi(a) = La$. Ще докажем, че Ψ е изоморфизъм.

- От $Lab = LaLb \Rightarrow \Psi(ab)= \Psi(a)\Psi(b) \Rightarrow \Psi$ - 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. $La=Lb \Rightarrow La(e)=Lb(e) \Rightarrow a=b \Rightarrow$ противоречие $\Rightarrow \Psi(a) \neq \Psi(b)$
- ⇨ Ψ е изоморфизъм $\Rightarrow G \approx G' \leq Sn$.

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

Определение: Нека $x \in \Omega$. Под **стабилизатор на x** в групата G ще разбираме множеството

$StG(x)=\{g \in G | gx=x\}$.

Свойство1: Стабилизаторът в G на всеки елемент $x \in \Omega$ е подгрупа на G, т.е. $x \in \Omega \Rightarrow StG(x) < G$.

Д-во: Нека $S = StG(x)$ и $g1,g2 \in S$, т.е. $g1x=x$ и $g2x=x$. Искаме $S \leq G$, като имаме $g1,g2 \in S$ и S е подмножество на G и $(g1g2)x = g1(g2x) = g1x = x \Rightarrow g1g2 \in S$.

Ako $g \in S$(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 $X,Y \in \Omega$. $X \sim Y$(x е еквивалентно на y) ако съществува $g \in G$:, че $Y=gX$.

$\sim$ е релация на еквивалентност. Тогава множеството Ω се разбива на непресичащи се класове на еквивалнтност, които се наричат G – орбити. Орбитата съдържаща даден елемент x бележим с O(x). Очевидно $O(x) = \{gx | g \in G\}$ – 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: $x \in \Omega$, $g1,g2 \in G$: $g1x=g2x \Leftrightarrow g2^{-1}g1 \in StG(x)$

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

<u>Свойство4:</u>Съществува биективно съответствие между $\{g\, StG(x) \mid g \in G\}$ и $O(x)$

<u>Твърдение:</u> Нека $x \in \Omega$. Тогава $|O(x)| =|G: StG(x)|$ в частност $|O(x)|/|G|$.

<u>Д-во:</u> Нека $S= StG(x)$ 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 дествието 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 => $|G|=|S|.|G:S|$ => $|G|=|S|.|O(x)|$ => $|O(x)| / |G|$.

<u>Твърдение:</u> Нека $\Omega_1,\Omega_2,......\Omega_s$ са всичките G – орбити в Ω и нека $x_i \in \Omega_i$ т.е. $\Omega_i=O(x_i)$, $i=1,....,s$. Тогава

$|\Omega| = \sum|\Omega_i| = \sum|G: StG(x_i)|$ /i=1.....S за сумите/.

<u>Определение:</u> Ще казваме, че групата **G действа транзитивно** върху множеството Ω, ако за всеки два елемента $X,Y \in \Omega$, съществува елемент $g \in G$:, че $Y=gX$.

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

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

<u>Формула за класовете:</u>

<u>Определение:</u> 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 $StG(x) = \{ g \in G \mid gxg^{-1} \}$ се нарича централизатор на G и се бележи $C_G(x)$ или $C(x)$. Тогава $|\Omega| = \sum|\Omega_i| = \sum|G: StG(x_i)|$ приема вида :

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

Нека $Z(G)$ е центъра на G, т.е. $Z(G) = \{x \in G \mid xg=gx$ 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 $Z(G) = \{ x_1, ……….x_t\}$ $1\le t\le s$ и сега равенството (1) може да се запише така:

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

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

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