Симетрична група. Представяне на елементите като произведение на независими цикли, ред на елемент, спрягане, алтернативна група.

Носителят на пермутация $\sigma \in S_n$ е множеството $\mathrm{Supp}(\sigma) := \{i \,|\, \sigma(i) \neq i,\ 1 \leq i \leq n\}$ на числата от 1 до n, които не остават на място под действие на σ.

Определение 1. *Цикъл с дължина k е пермутация $\zeta \in S_n$, чийто носител $\mathrm{Supp}(\zeta) = \{i_1, \ldots, i_k\}$ се състои от k различни числа и която действа по правилото $\zeta(i_s) = i_{s+1}$ за всички $1 \leq s \leq k-1$ и $\zeta(i_k) = i_1$. Бележим $\zeta = (i_1, \ldots, i_k)$.*

Цикъл $\zeta = (i_1, \ldots, i_k) \in S_n$ с дължина k е елемент на S_n от ред . От една страна, $\zeta^k = \varepsilon$ е тъждествената пермутация. От друга страна, $\zeta^r \neq \varepsilon$ за всички естествени $r < k$, защото

$$\zeta^r(i_1) = \zeta^{r-1}(i_2) = \ldots = i_{1+r} \neq i_1 \quad \text{при} \quad 2 = 1+1 \leq r+1 \leq (k-1)+1 = k.$$

Определение 2. *Цикли $(i_1, \ldots, i_k)$ и $(j_1, \ldots, j_l)$ са независими, ако носителите им $\mathrm{Supp}(i_1, \ldots, i_k) = \{i_1, \ldots, i_k\}$ и $\mathrm{Supp}(j_1, \ldots, j_l) = \{j_1, \ldots, j_l\}$ не се пресичат, $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$.*

Независими цикли $(i_1, \ldots, i_k)$ и $(j_1, \ldots, j_l)$ комутират, защото действат върху непресичащите се подмножества $\{i_1, \ldots, i_k\}$ и $\{j_1, \ldots, j_l\}$ на $\{1, \ldots, n\}$.

Твърдение 3. *Всяка нетъждествена пермутация $\sigma \in S_n \setminus \{\varepsilon\}$ има единствено с точност до реда на множителите разлагане в произведение на независими цикли.*

Доказателство. Преди да докажем твърдението, да дадем един пример:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 2 & 1 & 8 & 9 & 10 & 7 & 6 \end{pmatrix} = (1,3,5)(2,4)(6,8,10)(7,9).$$

Съществуване: Ако $\sigma \in S_n \setminus \{\varepsilon\}$, то съществува $i_1 \in \mathrm{Supp}(\sigma)$, така че $\sigma(i_1) = i_2 \neq i_1$. Ако $\sigma(i_2) = i_1$, то отделяме цикъл (i_1, i_2) и продължаваме с разлагането на σ като пермутация на $\{1, \ldots, n\} \setminus \{i_1, i_2\}$. Ако $\sigma(i_2) = i_3 \notin \{i_1, i_2\}$, то при $\sigma(i_3) \in \{i_1, i_2, i_3\}$ имаме $\sigma(i_3) = i_1$ поради биективността на σ и това, че $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$ за различни i_1, i_2, i_3. Ако $\sigma(i_3) = i_4 \notin \{i_1, i_2, i_3\}$, продължаваме по същия начин. Множеството $\{1, \ldots, n\}$ е крайно, така че след краен брой стъпки имаме $\sigma(i_k) \in \{i_1, \ldots, i_k\}$. За $s < k$ е изпълнено $\sigma(i_s) = i_{s+1}$, така че $\sigma(i_k) = i_1$ поради биективността на σ. След отделяне на цикъла $(i_1, \ldots, i_k)$, който представя действието на σ върху $\{i_1, \ldots, i_k\}$, разглеждаме

σ като пермутация на $\{1,\dots,n\}\setminus\{i_1,\dots,i_k\}$ и отделяме следващия цикъл от разлагането на σ. След краен брой стъпки представяме σ като произведение на независими цикли.

Единственост: Да предположим, че

$$\zeta_k\dots\zeta_1=\sigma=\eta_m\dots\eta_1 \tag{1}$$

а две разлагания на σ произведение на независими цикли ζ_i,η_j. Без ограничение на общността можем да считаме, че $k\leq m$. Ако $\zeta_k=(i_1,\dots,i_r)$, то съществува η_j с $i_1\in\mathrm{Supp}(\eta_j)$. Поради независимостта на циклите $\eta_1,\dots,\eta_m$, η_j трансформира i_1 в i_2, после i_2 в i_3 и т.н., $\zeta_k=\eta_j$. След преномерация на $\eta_1,\dots,\eta_m$ можем да считаме, че $\zeta_k=\eta_m$. След ляво умножение на (1) с ζ_k^{-1} получаваме $\zeta_{k-1}\dots\zeta_1=\eta_{m-1}\dots\eta_1$. По индукционно предположение, оттук следва $k-1=m-1$ и $\zeta_i=\eta_i$ за всички $1\leq i\leq k-1$, след подходяща преномерация на $\eta_1,\dots,\eta_{k-1}$.

□

Твърдение 4. *Редът на пермутация $\sigma(r_1,\dots r_s)\dots(j_1,\dots,j_l)(i_1,\dots,i_k)=\in S_n\setminus\{\varepsilon\}$ е равен на най-малкото общо кратно на дължините $s,\dots,l,k$ на участващите в разлагането на σ независими цикли.*

Доказателство. Нека $\sigma=(r_1,\dots r_s)\dots(j_1,\dots,j_l)(i_1,\dots,i_k)$ е разлагането на σ в произведение на независими цикли, а $m:=\mathrm{LCM}(k,l,\dots,s)\in\mathbb{N}$ е най-малкото общо кратно на дължините на участващите в разлагането на σ цикли. Тогава

$$\sigma^m=(r_1,\dots,r_s)^m\dots(j_1,\dots,j_l)^m(i_1,\dots,i_k)^m,$$

съгласно комутирането на независимите цикли. Сега $(i_1,\dots,i_k)^m=\varepsilon$, защото редът k на $(i_1,\dots,i_k)$ дели m. Аналогично, $(j_1,\dots,j_l)^m=\varepsilon$, ..., $(r_1,\dots,r_s)^m=\varepsilon$, защото редовете $l,\dots,s$ на тези цикли делят m. Следователно $\sigma^m=\varepsilon$ и редът $t:=\mathrm{ord}(\sigma)$ на σ дели m.

Обратно, от

$$\varepsilon=\sigma^t=(r_1,\dots,r_s)^t\dots(j_1,\dots j_l)^t(i_1,\dots,i_k)^t$$

получаваме $(r_1,\dots,r_s)^t=\varepsilon$, ..., $(j_1,\dots j_l)^t=\varepsilon$, $(i_1,\dots,i_k)^t=\varepsilon$, защото от независимостта на циклите в разлагането на σ следва, че носителите на t-тите степени на тези цикли са два по два непресичащи се. В резултат, редът s на $(r_1,\dots,r_s)$ дели t и т.н. l дели t и k дели t. Оттук, t е общо кратно на дължините $k,l,\dots,s$ на циклите от разлагането на σ и най-малкото общо кратно m на тези дължини дели t. От t дели m и m дели t за $m,t\in\mathbb{N}$ следва $m=t$.

□

Например, пермутацията $\sigma=(1,2,3)(4,5)(6,7,8)$ е от ред $\mathrm{LCM}(3,2,3)=6$

Лема 5. *За произволен цикъл $(i_1,\dots,i_k)\in S_n$ с дължина k и произволна пермутация $\rho\in S_n$ е в сила равенството*

$$\rho(i_1,\dots,i_k)\rho^{-1}=(\rho(i_1),\dots\rho(i_k)).$$

Доказателство. За всяко $1 \leq s \leq k$, лявата страна на доказваното равенство трансформира $\rho(i_{s(\mathrm{mod}\, k)})$ в

$$[\rho(i_1, \ldots, i_k)\rho^{-1}](\rho(i_{s(\mathrm{mod}\, k)})) = \rho(i_1, \ldots, i_k)(i_{s(\mathrm{mod}\, k)}) = \rho(i_{s+1(\mathrm{mod}\, k)}),$$

както и дясната страна $(\rho(i_1), \ldots \rho(i_k))$, която действа по правилото

$$(\rho(i_1), \ldots \rho(i_k))(\rho(i_{s(\mathrm{mod}\, k)})) = \rho(i_{s+1(\mathrm{mod}\, k)}).$$

Ако $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_s\}$, то $\rho(j) \in \{1, \ldots, n\} \setminus \{\rho(i_1), \ldots, \rho(i_k)\}$ и

$$[\rho(i_1, \ldots, i_k)\rho^{-1}](\rho(j)) = \rho(i_1, \ldots, i_k)(j) = \rho(j) = (\rho(i_1), \ldots \rho(i_k))(\rho(j))$$

показват, че както лявата, така и дясната страна оставят на място $\rho(j)$. Това доказва равенството $\rho(i_1, \ldots, i_k)\rho^{-1} = (\rho(i_1), \ldots \rho(i_k))$.

□

Например, $(1,3)(1,2)(1,3)^{-1} = (3,2)$.

Определение 6. *Permutations $\sigma, \tau \in S_n$ имат еднакъв цикличен строеж, ако в разлаганията им в произведение на независими цикли има един и същи брой цикли с една и съща дължина.*

Ако $\sigma = (1,2,3)(4,5)(6,7,8)$, $\tau = (2,4,6)(7,9)(1,3,5)$ и $\rho = (1,5)(2,4)(6,7,8)$, то σ и τ имат еднакъв цикличен строеж, а σ и ρ нямат еднакъв цикличен строеж.

Твърдение 7. *Две permutations σ и τ от S_n са спрегнати в S_n тогава и само тогава, когато имат еднакъв цикличен строеж.*

Доказателство. Нека $\sigma = (r_1, \ldots, r_s)(t_1, \ldots, t_p) \ldots (j_1, \ldots, j_l)(i_1, \ldots, i_k)$ е разлагането на $\sigma \in S_n \setminus \{\varepsilon\}$ в произведение на независими цикли. Тогава за всяка permutation $\rho \in S_n$, спрегнатата на σ посредством ρ е

$$\begin{aligned}\rho\sigma\rho^{-1} = [\rho(r_1, \ldots, r_s)\rho^{-1}][\rho(t_1, \ldots, t_p)\rho^{-1}] \ldots [\rho(j_1, \ldots, j_l)\rho^{-1}][\rho(i_1, \ldots, i_k)\rho^{-1}] = \\ = (\rho(r_1), \ldots, \rho(r_s))(\rho(t_1), \ldots, \rho(t_p)) \ldots (\rho(j_1), \ldots, \rho(j_l))(\rho(i_1), \ldots, \rho(i_k))\end{aligned}$$

и има еднакъв цикличен строеж със σ.

Ако

$$\sigma = (r_1, \ldots, r_s)(t_1, \ldots, t_p) \ldots (j_1, \ldots, j_l)(i_1, \ldots, i_k) \quad \text{и}$$
$$\tau = (r'_1, \ldots, r'_s)(t'_1, \ldots, t'_p) \ldots (j'_1, \ldots, j'_l)(i'_1, \ldots, i'_k)$$

имат еднакъв цикличен строеж, то носителите на независимите цикли от разлагането на σ не се пресичат и

$$\rho = \begin{pmatrix} i_1 & \ldots & i_k & j_1 & \ldots & j_l & \ldots & t_1 & \ldots & t_p & r_1 & \ldots & r_s & \{1, \ldots, n\} \setminus \mathrm{Supp}(\sigma) \\ i'_1 & \ldots & i'_k & j'_1 & \ldots & j'_l & \ldots & t'_1 & \ldots & t'_p & r'_1 & \ldots & r'_s & \{1, \ldots, n\} \setminus \mathrm{Supp}(\tau) \end{pmatrix}$$

е коректно зададено изображение на множеството $\{1, \ldots, n\}$ в себе си. Биективността на ρ следва от независимостта на циклите от разлагането на τ, стига permutation

на числата $\{1,\ldots,n\}\setminus \mathrm{Supp}(\sigma)$ да се трансформира биективно върху пермутация на числата $\{1,\ldots,n\}\setminus \mathrm{Supp}(\tau)$. Сега

$$\rho\sigma\rho^{-1} = (\rho(r_1),\ldots,\rho(r_s))(\rho(t_1),\ldots,\rho(t_p))\ldots(\rho(j_1),\ldots,\rho(j_l))(\rho(i_1),\ldots,\rho(i_k)) = \\ = (r'_1,\ldots,r'_s)(t'_1,\ldots,t'_p)\ldots(j'_1,\ldots,j'_l)(i'_1,\ldots,i'_k) = \tau$$

доказва спрегнатостта на произволни пермутации $\sigma,\tau\in S_n$ с еднакъв цикличен строеж. □

Пример 8. *Подмножеството*

$$K_4 = \{\varepsilon, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

на симетричната група S_4 е нормална подгрупа на S_4.

Доказателство. Преди всичко, K_4 е затворено относно композицията на пермутации, защото $\varepsilon\sigma = \sigma = \sigma\varepsilon$ за всяко $\sigma\in K_4$. Произволен елемент $\sigma\in K_4\setminus\{\varepsilon\}$ е от вида $\sigma = (i,j)(k,l)$ за някаква пермутация i,j,k,l на $1,2,3,4$ и $\sigma^2 = (i,j)^2(k,l)^2 = \varepsilon\in K_4$. Ако $\sigma\in K_4\setminus\{\varepsilon\}$ и $\tau\in K_4\setminus\{\varepsilon\}$ са различни елементи и $\sigma = (i,j)(k,l)$, то $\tau(i)\in\{k,l\}$. След евентуална размяна на k и l можем да считаме, че $\tau(i) = k$, откъдето $\tau = (i,k)(j,l)$ и $\tau\sigma = (i,l)(j,k)\in K_4$. Това доказва затвореността на K_4 относно композицията на пермутации.

Ясно е, че $\varepsilon^{-1} = \varepsilon\in K_4$. За всяко $\sigma\in K_4\setminus\{\varepsilon\}$ пресметнахме,че $\sigma^2 = \varepsilon$, откъдето $\sigma^{-1} = \sigma\in K_4$ и K_4 е подгрупа на S_4.

Понеже K_4 се състои от тъждествената пермутация ε и всички произведения на два независими цикъла с дължина 2, K_4 е нормална подгрупа на S_4.

□

Определение 9. *Циклите (i,j) с дължина 2 се наричат транспозиции.*

Задача 10. *За произволни естествени числа $1\le i<j\le n$ пермутациите $\sigma\in S_n$ и $(i,j)\sigma\in S_n$ са с различна четност.*

Доказателство. Първо ще разгледаме случая на транспозиция $(\sigma(p),\sigma(p+1))$ на съседни числа от редицата $\sigma(1),\ldots,\sigma(p),\sigma(p+1),\ldots,\sigma(n)$ от образите на σ. За произволни $q,r\in\{1,\ldots,n\}\setminus\{p,p+1\}$, транспозицията $(\sigma(p),\sigma(p+1))$ не променя взаимното положение на двойките числа $\sigma(q),\sigma(r)$, както и $\sigma(q),\sigma(p)$ или $\sigma(q),\sigma(p+1)$. При разместването на $\sigma(p)$ със $\sigma(p+1)$ се създава инверсия, ако $\sigma(p+1)>\sigma(p)$ или се унищожава инверсия, ако $\sigma(p+1)<\sigma(p)$.

В общия случай, транспозицията $(\sigma(p),\sigma(q))$ за $1\le p<q\le n$ се разлага в произведение

$$(\sigma(p),\sigma(q)) = \underbrace{(\sigma(q),\sigma(p+1))\ldots(\sigma(q),\sigma(q-1))}_{q-1-p}\underbrace{(\sigma(p),\sigma(q))\ldots(\sigma(p),\sigma(p+1))}_{q-p}$$

на нечетен брой, т.е. $2(q-p)-1$ транспозиции на съседни числа от съответните редици от образи, четени отдясно наляво. Умножението с всяка от тези $2(q-p)-1$ транспозиции променя четността на съответната редица от образи, така че умножението на σ с $(\sigma(p),\sigma(q))$ променя четността на редицата от образите.

□

Твърдение 11. *(i) Всяка пермутация $\sigma \in S_n \setminus \{\varepsilon\}$ се разлага в произведение на транспозиции;*

(ii) Всеки две разлагания на $\sigma \in S_n \setminus \{\varepsilon\}$ в произведение на транспозиции имат една и съща четност на броя на множителите.

Доказателство. (i) Всяка пермутация $\sigma \in S_n \setminus \{\varepsilon\}$ се разлага в произведение на независими цикли. Затова е достатъчно да забележим, че произволен цикъл

$$(i_1, \ldots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \ldots (i_1, i_3)(i_1, i_2)$$

се разлага в произведение на транспозиции, четени отдясно наляво.

(ii) Ако $\zeta_k \ldots \zeta_1 = \sigma = \eta_m \ldots \eta_1$ са две разлагания на $\sigma \in S_n \setminus \{\varepsilon\}$ в произведение на транспозиции ζ_i, η_j, то четността на броя k на множителите на първото разлагане съвпада с четността на броя на инверсиите в редицата $\sigma(1), \ldots, \sigma(n)$ от образите на σ. Аналогично, броят m на множителите във второто разлагане има същата четност като броя на инверсиите в редицата $\sigma(1), \ldots, \sigma(n)$. Оттук, k и m имат една и съща четност. □

Например, $(1,3)(1,2)(1,3)^{-1} = (3,2) = (1,3)(1,2)(1,3)$ са две разлагания на една и съща пермутация в произведение на транспозиции. Да забележим, че не само разлаганията са различни, но и броят на множителите в тези разлагания е различен - съответно, 1 и 3. И двете разлагания имат нечетен брой множители.

Твърдение 12. *За всяко естествено число $n \geq 2$ множеството A_n на четните пермутации от S_n е нормална подгрупа на S_n с индекс 2. В частност, редът на A_n е*

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Доказателство. Ако $\sigma = (i_{2k}, j_{2k}) \ldots (i_1, j_1), \tau = (i'_{2m}, j'_{2m}) \ldots (i'_1, j'_1) \in A_n$ са четни пермутации, то

$$\begin{aligned} \sigma\tau^{-1} &= [(i_{2k}, j_{2k}) \ldots (i_1, j_1)][(i'_{2m}, j'_{2m}) \ldots (i'_1, j'_1)]^{-1} = \\ &= [(i_{2k}, j_{2k}) \ldots (i_1, j_1)][(i'_1, j'_1)^{-1} \ldots (i'_{2m}, j'_{2m})^{-1}] = \\ &= [(i_{2k}, j_{2k}) \ldots (i_1, j_1)](i'_1, j'_1) \ldots (i'_{2m}, j'_{2m})] \in A_n \end{aligned}$$

е четна пермутация, вземайки предвид $(i'_s, j'_s)^{-1} = (i'_s, j'_s)$ за произволна транспозиция (i'_s, j'_s). Това доказва, че A_n е подгрупа на S_n.

За произволни фиксирани $1 \leq i < j \leq n$, лявото умножение

$$\mu_{(i,j)} : A_n \longrightarrow S_n \setminus A_n$$

с (i,j) е взаимно еднозначно изображение на множеството A_n на четните пермутации върху множеството $S_n \setminus A_n$ на нечетните пермутации. Аналогично, лявото умножение

$$\mu_{(i,j)} : S_n \setminus A_n \longrightarrow A_n,$$

с (i,j) е биективно изображение на множеството $S_n \setminus A_n$ на нечетните пермутации върху множеството A_n на четните пермутации. Следователно $S_n \setminus A_n = (i,j)A_n$ и

$$S_n = A_n \cup (i,j)A_n$$

е разлагането на S_n в леви съседни класове относно A_n. В резултат, A_n е подгрупа на S_n с индекс $[S_n : A_n] = 2$. В частност, подгрупата A_n на S_n е нормална и по Теоремата на Лагранж, редът на A_n е

$$|A_n| = \frac{|S_n|}{[S_n : A_n]} = \frac{n!}{2} \quad \text{за всяко } n \geq 2.$$

□