

Permutace

Připomeňme, že pro libovolnou množinu X jsme symbolem X^X označili množinu všech zobrazení $f : X \rightarrow X$ a symbolem \circ jsme označili skládání zobrazení. Uvažujme dále pouze libovolné bijekce $f : X \rightarrow X$. Takovým bijekcím říkáme **permutace** množiny X . Množinu všech permutací množiny X značíme $S(X)$. Je to podmnožina v množině X^X a je uzavřená vzhledem ke skládání zobrazení, neboť složením kterýchkoliv dvou takových bijekcí vznikne opět bijekce.

Budeme dále vyšetřovat pouze permutace konečných množin a přitom budeme pracovat pouze s množinami tvaru $X = \{1, 2, \dots, n\}$, kde n je přirozené číslo. Pak místo $S(X)$ budeme psát S_n . Permutace $\sigma \in S_n$ budeme zapisovat ve tvaru

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

kde $i_r = \sigma(r)$ pro každé $r \in \{1, 2, \dots, n\}$. Poznamenejme, že pak (i_1, i_2, \dots, i_n) je obecně libovolná uspořádaná n -tice vzájemně různých prvků množiny $\{1, 2, \dots, n\}$, takže jde vlastně o prvky $1, 2, \dots, n$ zapsané v nějakém obecném pořadí. To znamená, že permutace $\sigma \in S_n$ tímto způsobem odpovídají permutacím (i_1, i_2, \dots, i_n) prvků $1, 2, \dots, n$ tak, jak byly zavedeny v kombinatorice. Odtud plyne, že existuje celkem $n!$ takových permutací. Kvůli odlišení ale budeme nyní uspořádaným n -ticím (i_1, i_2, \dots, i_n) vzájemně různých prvků množiny $\{1, 2, \dots, n\}$ říkat **pořadí** prvků $1, 2, \dots, n$.

Prvek $r \in \{1, 2, \dots, n\}$ se nazývá **samodružným prvkem** permutace $\sigma \in S_n$, jestliže $\sigma(r) = r$.

Nechť $\ell > 1$ je přirozené číslo a nechť $\sigma \in S_n$. Pak permutace σ se nazývá **cyklus** délky ℓ , existují-li vzájemně různé prvky $j_1, j_2, \dots, j_\ell \in \{1, 2, \dots, n\}$ takové, že platí $\sigma(j_1) = j_2$,

$\sigma(j_2) = j_3, \dots, \sigma(j_{\ell-1}) = j_\ell, \sigma(j_\ell) = j_1$ a $\sigma(r) = r$ pro všechna $r \in \{1, 2, \dots, n\} - \{j_1, j_2, \dots, j_\ell\}$. Takovou permutaci pak zapisujeme jednodušeji ve tvaru

$$\sigma = (j_1 \ j_2 \ \dots \ j_\ell).$$

Dva cykly $\sigma = (j_1 \ j_2 \ \dots \ j_\ell)$ a $\tau = (k_1 \ k_2 \ \dots \ k_m)$ z S_n se nazývají **nezávislé**, jestliže $\{j_1, j_2, \dots, j_\ell\} \cap \{k_1, k_2, \dots, k_m\} = \emptyset$. Řekneme, že cykly $\sigma_1, \sigma_2, \dots, \sigma_t$ jsou vzájemně nezávislé, jestliže jsou nezávislé cykly σ_p, σ_q pro všechna $p, q \in \{1, 2, \dots, t\}, p \neq q$. Je vidět, že nezávislé cykly spolu při skládání komutují.

Věta. Každou neidentickou permutaci $\sigma \in S_n$ lze vyjádřit ve tvaru součinu několika navzájem nezávislých cyklů. Toto vyjádření je jediné až na pořadí zmíněných cyklů.

Důkaz. Existenci uvedeného vyjádření dokážeme indukcí vzhledem k počtu samodružných prvků permutace σ . Poněvadž σ je neidentická permutace, existuje $i \in \{1, 2, \dots, n\}$ takové, že $\sigma(i) \neq i$. Uvažme prvky

$$i, \sigma(i), \sigma(\sigma(i)), \sigma(\sigma(\sigma(i))), \dots$$

Značme prvky této posloupnosti $\sigma^h(i)$ pro $h = 0, 1, 2, \dots$. Poněvadž množina $\{1, 2, \dots, n\}$ je konečná, existují κ, λ splňující $\kappa < \lambda$ taková, že $\sigma^\kappa(i) = \sigma^\lambda(i)$. Předpokládejme navíc, že λ je nejmenší možné číslo s takovou vlastností. Ukážeme, že pak platí $\kappa = 0$. V opačném případě bychom totiž měli $\sigma^\kappa(i) = \sigma(\sigma^{\kappa-1}(i))$ a zároveň $\sigma^\kappa(i) = \sigma(\sigma^{\lambda-1}(i))$, přičemž $\sigma^{\kappa-1}(i) \neq \sigma^{\lambda-1}(i)$, což není možné vzhledem k tomu, že σ je permutace. Takže $\kappa = 0$, a tedy máme $i = \sigma^\lambda(i)$. Přitom platí $\lambda > 1$, poněvadž $\sigma(i) \neq i$. Kromě toho z minimality λ plyne, že prvky $\sigma^h(i)$ pro $h = 0, 1, \dots, \lambda - 1$ jsou vzájemně různé. Takže permutace

$$\tau = (i \ \sigma(i) \ \dots \ \sigma^{\lambda-1}(i))$$

je cyklus délky λ . Uvažme nyní permutaci $\tau^{-1} \circ \sigma$. Všechny samodružné prvky permutace σ jsou také samodružnými prvky

permutace $\tau^{-1} \circ \sigma$ a navíc také prvky $\sigma^h(i)$ pro $h = 0, 1, \dots, \lambda - 1$ jsou samodružnými prvky permutace $\tau^{-1} \circ \sigma$. Má tedy permutace $\tau^{-1} \circ \sigma$ více samodružných prvků než permutace σ . Je-li $\tau^{-1} \circ \sigma$ identická permutace, pak $\sigma = \tau$. V opačném případě lze permutaci $\tau^{-1} \circ \sigma$ podle indukčního předpokladu rozložit na součin vzájemně nezávislých cyklů ve tvaru $\tau^{-1} \circ \sigma = \rho_1 \circ \dots \circ \rho_t$. Přitom prvky vystupující v cyklech ρ_1, \dots, ρ_t nejsou samodružnými prvky permutace $\tau^{-1} \circ \sigma$, takže jsou různé od prvků $\sigma^h(i)$ pro $h = 0, 1, \dots, \lambda - 1$ vystupujících v cyklu τ . Takže odtud dostáváme $\sigma = \tau \circ \rho_1 \circ \dots \circ \rho_t$, přičemž cykly τ a ρ_1, \dots, ρ_t jsou vzájemně nezávislé. Jednoznačnost takového rozkladu je zřejmá.

Cyklus délky 2, to znamená cyklus tvaru $\sigma = (i \ j)$, kde $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, se nazývá **transpozice**.

Věta. Nechť $n > 1$. Pak každou permutaci $\sigma \in S_n$ lze vyjádřit ve tvaru součinu několika transpozic.

Důkaz. Identickou permutaci lze vyjádřit například ve tvaru $(1 \ 2) \circ (1 \ 2)$. Pokud jde o neidentické permutace, z předchozí věty plyne, že tvrzení stačí dokázat pro cykly. Pro libovolný cyklus $\sigma = (j_1 \ j_2 \ \dots \ j_\ell)$ ovšem platí

$$(j_1 \ j_2 \ \dots \ j_\ell) = (j_1 \ j_\ell) \circ (j_1 \ j_{\ell-1}) \circ \dots \circ (j_1 \ j_3) \circ (j_1 \ j_2).$$

Nechť (i_1, i_2, \dots, i_n) je libovolné pořadí prvků $1, 2, \dots, n$. Jsou-li $s, t \in \{1, 2, \dots, n\}$ takové prvky, že $s < t$ a $i_s > i_t$, pak říkáme, že prvky i_s, i_t tvoří **inverzi** v pořadí (i_1, i_2, \dots, i_n) .

Pro libovolnou permutaci

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

z S_n definujeme její **paritu** $\wp(\sigma)$ předpisem

$$\wp(\sigma) = (-1)^{\mathfrak{S}(i_1, i_2, \dots, i_n)}, \quad \text{kde } \mathfrak{S}(i_1, i_2, \dots, i_n) \text{ je celkový počet všech inverzí v pořadí } (i_1, i_2, \dots, i_n).$$

Říkáme, že uvedená permutace σ je **sudá**, je-li $\wp(\sigma) = 1$, to znamemá obsahuje-li pořadí (i_1, i_2, \dots, i_n) sudý počet inverzí. Říkáme, že tato permutace σ je **lichá**, je-li $\wp(\sigma) = -1$, to znamemá obsahuje-li pořadí (i_1, i_2, \dots, i_n) lichý počet inverzí. V kontextu předchozí věty ovšem charakterizujeme sudé a liché permutace ještě jiným způsobem.

Věta. Permutace $\sigma \in S_n$ je sudá, resp. lichá, právě když každé vyjádření σ ve tvaru součinu transpozic obsahuje sudý, resp. lichý počet transpozic.

Důkaz. Tvrzení bude dokázáno, ověříme-li, že pro libovolné transpozice $(i_1 \ j_1), (i_2 \ j_2), \dots, (i_t \ j_t)$ z S_n platí

$$\wp((i_1 \ j_1) \circ (i_2 \ j_2) \circ \dots \circ (i_t \ j_t)) = (-1)^t,$$

tedy že složením sudého, resp. lichého počtu transpozic vznikne sudá, resp. lichá permutace. Poněvadž identická permutace je sudá, bude k tomu účelu stačit následující úvaha.

Nechť $\sigma \in S_n$ je libovolná permutace a necht' $i, j \in \{1, 2, \dots, n\}$ jsou libovolné prvky splňující $i \neq j$, takže $(i \ j)$ je libovolná transpozice. Pak stačí ověřit, že $\wp(\sigma \circ (i \ j)) = -\wp(\sigma)$, tedy že složení permutace s transpozicí mění paritu permutace.

Ověříme tuto rovnost nejprve v případě, že uvedená transpozice je tvaru $(k \ k+1)$ pro nějaké $k \in \{1, 2, \dots, n-1\}$. Je-li ovšem (i_1, i_2, \dots, i_n) pořadí příslušné permutaci σ , je jasné, že pak $(i_1, \dots, i_{k-1}, i_{k+1}, i_k, i_{k+2}, \dots, i_n)$ je pořadí příslušné permutaci $\sigma \circ (k \ k+1)$. V tomto pořadí se změnila pouze poloha dvou sousedních prvků, což znamená, že počet inverzí se zvýšil nebo snížil o 1. Změnila se tudíž parita permutace.

Uvažujme nyní obecnou transpozici, tedy transpozici tvaru $(i \ j)$, kde $i, j \in \{1, 2, \dots, n\}$ splňují například $i < j$. Stačí si ale uvědomit, že takovou transpozici lze vyjádřit ve tvaru

$$(i \ j) = (i \ i+1) \circ (i+1 \ i+2) \circ \dots \circ (j-2 \ j-1) \circ (j-1 \ j) \\ \circ (j-2 \ j-1) \circ \dots \circ (i+1 \ i+2) \circ (i \ i+1),$$

kde na pravé straně se vyskytuje lichý počet transpozic výše uvedeného speciálního tvaru. Pak už jen stačí použít toho, co bylo ukázáno v předchozím odstavci.

Důsledek. Pro libovolné permutace $\sigma, \tau, \rho \in S_n$ platí

$$\wp(\sigma \circ \tau) = \wp(\sigma) \cdot \wp(\tau), \quad \wp(\rho^{-1}) = \wp(\rho).$$

Důkaz. První rovnost ihned plyne z předchozích dvou vět. Druhá rovnost plyne z první a z faktu, že $\rho \circ \rho^{-1}$ je identická, a tedy sudá permutace.

Bud' n přirozené číslo. Označme A_n množinu všech sudých permutací množiny $\{1, 2, \dots, n\}$. Vezměme dále libovolnou lichou permutaci $\vartheta \in S_n - A_n$. Pak podle předchozího důsledku je možno uvažovat zobrazení

$$\gamma : A_n \rightarrow S_n - A_n$$

definované pro každou sudou permutaci $\sigma \in A_n$ předpisem

$$\gamma(\sigma) = \sigma \circ \vartheta.$$

Toto zobrazení podle již zmíněného důsledku převádí vzájemně jednoznačně všechny sudé permutace na liché permutace. Skutečně inverzním zobrazením by bylo zobrazení

$$\delta : S_n - A_n \rightarrow A_n$$

definované pro každou lichou permutaci $\tau \in S_n - A_n$ předpisem

$$\delta(\tau) = \tau \circ \vartheta^{-1},$$

neboť pak $\delta \circ \gamma$ je identita na A_n a $\gamma \circ \delta$ je identita na $S_n - A_n$. To ukazuje, že sudých i lichých permutací množiny $\{1, 2, \dots, n\}$ je stejný počet a že tento počet je roven číslu $\frac{n!}{2}$.