8 Permutace: Škatulata, hejbejte se – ale s rozmyslem

Řešení
verze ze dne 7. dubna 2025.

Cíle cvičení: Po připomenutí si základního počítání s permutacemi si rozmyslíme, jak se permutace konjugují a kolik permutací je potřeba na to, abychom už z nich mohli poskládat úplně všechny.

Úlohy, které bychom určitě měli umět řešit:

Úloha 8.1. Zapište následující permutace jako součin nezávislých cyklů a pro každou permutaci σ určete σ^{-1} a σ^{2020}:

(a) $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \in \mathbf{S}_5$,

(b) $\tau = (4\,6\,5\,1\,2) \in \mathbf{S}_6$,

(c) $\sigma = (1\,5\,6)(2\,3\,8\,4\,7) \in \mathbf{S}_8$,

(d) $\rho = (4\,3\,5) \circ (5\,1\,2) \in \mathbf{S}_5$.

Řešení. Nejprve si uvědomíme veledůležitou vlastnost, že nezávislé cykly spolu komutují, tj. $c_1c_2 = c_2c_1$ pro každé dva nezávislé cykly (což pro obecné dvojice cyklů, natož permutací, neplatí). Pak v cyklickém zápisu $c_1 \dots c_k$ každou permutaci snadno umocníme i invertujeme

$$[c_1c_2 \dots c_k]^n = c_1^n c_2^n \dots c_k^n, \quad [c_1c_2 \dots c_k]^{-1} = c_1^{-1}c_2^{-1} \dots c_k^{-1}.$$

Dále si všimneme, že $c^n = \mathrm{id}$ pro každé n dělitelné délkou cyklu c.

(a) Nejprve tedy zapíšeme permutaci π v cyklickém zápisu, tedy ve tvaru

$$\dots(\dots a\pi(a)\pi^2(a)\dots)\dots$$

Dostáváme $\pi = (1\,4)(2\,3\,5)$.

Abychom invertovali permutaci, stačí invertovat, tedy převrátit, každý z cyklů (samozřejmě si můžeme vybrat kterýkoli z n ekvivalentních zápisů jednoho cyklu délky n)

$$\pi^{-1} = (1\,4)^{-1}(2\,3\,5)^{-1} = (4\,1)(5\,3\,2) \quad (= (14)(2\,5\,3) = \dots)$$

a podobně umocníme

$$\pi^{2020} = (1\,4)^{2020}(2\,3\,5)^{2020} = ((1\,4)^2)^{1010}((2\,3\,5)^3)^{673}(2\,3\,5) = \mathrm{id}^{1010}\mathrm{id}^{673}(2\,3\,5) = (2\,3\,5).$$

(b) Permutaci $\tau = (4\,6\,5\,1\,2)$ tvoří jeden cyklus délky 5 a poté jeden cyklus délky 1, který nemusíme (a obvykle nebudeme) zapisovat (jde pak o tzv. redukovaný cyklický zápis).Nakonec si snadno rozmyslíme, že $\tau^{-1} = (2\,1\,5\,6\,4)$ a $\tau^{2020} = \mathrm{id}$, protože délka cyklu 5 dělí 2020.

(c) Obdobně jako v předchozích úlohách dostáváme

$$\sigma = (1\,5\,6)(2\,3\,8\,4\,7), \quad \sigma^{-1} = (6\,5\,1)(7\,4\,8\,3\,2), \quad \sigma^{2020} = (1\,5\,6).$$

(d) Složíme oba cykly a dostaneme $\rho = (1\,2\,4\,3\,5)$ a $\rho^{-1} = (5\,3\,4\,2\,1)$. Ze stejného důvodu jako v (b) máme $\rho^{2020} = \mathrm{id}$.

Úloha 8.2. Buďte $\pi, \tau \in \mathbf{S}_n$.

(a) Ukažte, že je-li v cyklickém zápisu permutace π prvek b hned po prvku a, pak je v cyklickém zápisu permutace $\sigma = \tau\pi\tau^{-1}$ prvek $\tau(b)$ hned po prvku $\tau(a)$,

(b) určete $\pi\tau\pi^{-1}$ a $\tau\pi\tau^{-1}$ pro permutaci π z příkladu 8.1 a $\tau = (4\,3\,5\,1\,2)$.

Řešení. (a) Stačí pro $b = \pi(a)$ konjugovat $\tau\pi\tau^{-1}(\tau(a)) = \tau\pi(a) = \tau(b)$.

(b) Počítáme:

$$\pi\tau\pi^{-1} = (\pi(4)\,\pi(3)\,\pi(5)\,\pi(1)\,\pi(2)) = (1\,5\,2\,4\,3),$$
$$\tau\pi\tau^{-1} = (\tau(1)\,\tau(4))(\tau(2)\,\tau(3)\,\tau(5)) = (2\,3)(4\,5\,1).$$

Úloha 8.3. Ověřte, že je relace „být konjugovaný s“ ekvivalence na $\mathbf{S}_n$.

Řešení. Protože $\pi^{\mathrm{id}} = \mathrm{id} \circ \pi \circ \mathrm{id}^{-1} = \pi$, jedná se o reflexivní relaci. Jestliže $\pi^\sigma = \sigma\pi\sigma^{-1} = \rho$, pak

$$\rho^{\sigma^{-1}} = \sigma^{-1}\rho(\sigma^{-1})^{-1} = \sigma^{-1}\rho\sigma = \sigma^{-1}\sigma\pi\sigma^{-1}\sigma = \pi,$$

tedy je naše relace symetrická. Konečně, pokud $\pi^\sigma = \rho$ a $\rho^\tau = \theta$, pak

$$\pi^{\tau\sigma} = \tau\sigma\pi(\tau\sigma)^{-1} = \tau(\sigma\pi\sigma^{-1})\tau^{-1} = \tau\rho\tau^{-1} = \theta$$

a proto je naše relace tranzitivní, čímž jsme dokončili důkaz.

Úloha 8.4. Dokažte, že grupu $\mathbf{S}_n$ permutací na n prvcích je možné generovat

(a) $n-1$ transpozicemi $(1\,2), (1\,3), \ldots, (1\,n)$,

(b) $n-1$ transpozicemi $(1\,2), (2\,3), \ldots, (n{-}1\,n)$,

(c) jedním n-cyklem $(1\,2\,3\,\ldots\,n)$ a transpozicí $(1\,2)$.

Řešení. (a) Stačí nám nagenerovat všechny transpozice, jelikož ty už budou generovat celou grupu. Díky konjugování máme

$$(1\,a) \circ (1\,b) \circ (1\,a)^{-1} = (a\,b),$$

tedy kterákoliv transpozice je součinem předepsaných transpozic, jde tedy o množinu generátorů grupy $\mathbf{S}_n$.

(b) V podstatě jde o známý algoritmus *bubblesort*. Pro $i < j$ můžeme transpozici $(i\,j)$ vyjádřit přímo jako

$$(i\,j) = (i\,i{+}1)(i{+}1\,i{+}2)\ldots(j{-}2\,j{-}1)(j{-}1\,j)(j{-}2\,j{-}1)\ldots(i\,i{+}1),$$

tedy např.

$$(1\,4) = (1\,2)(2\,3)(3\,4)(2\,3)(1\,2).$$

Opět z toho, že umíme dostat libovolnou transpozici, vyvozujeme, že jde o generátory celé $\mathbf{S}_n$.

(c) Označme $\pi = (1\,2\,3\,\ldots\,n)$. Jelikož k-tá mocnina cyklu π pošle 1 na k a 2 na $k+1$ (modulo n), konjugováním $(1\,2)$ s π^k dostáváme transpozici $(k\,k+1)$. Jak jsme nahlédli v předchozím bodě, tyto transpozice generují celou grupu $\mathbf{S}_n$.

A nakonec ještě trochu počítání pro radost a povzbuzení:

Úloha 8.5. Najděte všechny permutace α na množině $\{1, 2, 3, 4\}$, pro něž platí $\alpha \circ (1\,2\,3) \circ \alpha^{-1} = (1\,2\,4)$.

Řešení. Tentokrát si pro pořádek přidáme do cyklického zápisu i cykly délky 1 a hledáme všechna α, pro něž

$$\alpha \circ (1\,2\,3) \circ \alpha^{-1} = (\alpha(1)\,\alpha(2)\,\alpha(3))(\alpha(4)) = (1\,2\,4)(3).$$

Vzhledem k tomu, že máme 3 způsoby, jak zapsat cyklus $(124) = (241) = (412)$, odečteme permutaci α v maticovém zápisu:

$$\begin{matrix}(1&2&3)&(4)\\(1&2&4)&(3)\end{matrix}, \qquad \begin{matrix}(1&2&3)&(4)\\(2&4&1)&(3)\end{matrix}, \qquad \begin{matrix}(1&2&3)&(4)\\(4&1&2)&(3)\end{matrix}$$

Z prvního zápisu vidíme, že $\alpha = \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix} = (3\,4)$, z druhého $\alpha = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix} = (1\,2\,4\,3)$ a z posledního $\alpha = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = (1\,4\,3\,2)$. Našli jsme právě tři různé konjugující permutace $(3\,4)$, $(1\,2\,4\,3)$, $(1\,4\,3\,2)$.

Úloha 8.6. Je-li $\pi = \begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$, určete počet prvků množiny všech permutací $\alpha \in \mathbf{S}_5$,

(a) které jsou konjugované s permutací π,

(b) pro něž $\alpha\pi = \pi\alpha$.

Tvoří tyto množiny podgrupu $\mathbf{S}_5$?

Řešení. (a) Nejprve snadno spočítáme $\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix} = (1\,2\,3)(4\,5)$. V předchozí úloze jsme si uvědomili, že konjugované permutace jsou právě ty se stejným cyklickým zápisem, tedy v našem případě takové, které se skládají z jednoho trojcyklu a jednoho dvojcyklu. Výběrem tří prvků z pěti zvolíme rozdělení permutace na trojcyklus a dvojcyklus, oba možné zápisy představují týž dvojcyklus, zatímco u trojcyklů máme dvě možnosti, jak vytvořit různé (vzájemně inverzní) permutace. Tedy celkem dostáváme $2 \cdot \binom{5}{3}$ možností. Množina permutací se stejným cyklickým zápisem, s výjimkou té obsahující pouze identickou permutaci, netvoří podgrupu, například proto, že v ní neleží identická permutace.

(b) Všimněme si, že je podmínka $\alpha\pi = \pi\alpha$ ekvivalentní podmínce $\alpha\pi\alpha^{-1} = \pi$. Jak jsme nahlédli v minulé úloze, stačí si uvědomit, kolika způsoby můžeme permutaci zapsat ve stejném cyklickém zápisu. Protože $\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix} = (1\,2\,3)(4\,5)(6)$, mohu cyklus $(1\,2\,3) = (2\,3\,1) = (3\,1\,2)$ délky 3 napsat třemi způsoby a cyklus $(4\,5)$ délky 2 napsat dvěma způsoby, proto máme právě $2 \cdot 3 = 6$ permutací α splňujících podmínku.

Pokud $\alpha\pi = \pi\alpha$ a $\beta\pi = \pi\beta$, vidíme, že

$$(\alpha\beta)\pi = \alpha\beta\pi = \alpha\pi\beta = \pi\alpha\beta = \pi(\alpha\beta),$$

$$\pi\alpha^{-1} = \alpha^{-1}\alpha\pi\alpha^{-1} = \alpha^{-1}\pi, \qquad \mathrm{id}\pi = \pi = \pi\mathrm{id}$$

tedy uvažovaná množina tvoří podgrupu.

Úloha 8.7. Kolik ekvivalenčních tříd má ekvivalence „být konjugovaný“ na grupě $\mathbf{S}_6$?

Řešení. Díky úvahám předchozích dvou úloh si můžeme uvědomit, že se ptáme na to, kolik různých cyklických zápisů permutace na šesti prvcích existuje. Protože záleží jen na délkách jednotlivých cyklů, můžeme ekvivalentně spočítat počet neklesajících posloupností délek jednotlivých cyklů

$$\left\{(a_1,\ldots,a_2) \;\middle|\; k, a_1\ldots,a_k \in \mathbb{N},\ a_1 \le \cdots \le a_k,\ \sum_{i=1}^{k} a_i = 6\right\} =$$

$$= \{(6),(1,5),(2,4),(3,3),(1,1,4),(1,2,3),(2,2,2),(1,1,1,3),(1,1,2,2),$$
$$(1,1,1,1,2),(1,1,1,1,1,1)\},$$

kterých jsme hrubou silou našli právě jedenáct.

Úloha 8.8. Dokažte, že každou sudou permutaci lze zapsat jako složení trojcyklů.

Úloha 8.9. Ukažte, že na vygenerování všech sudých permutací stačí dokonce jen $n-2$ trojcyklů $(1\,2\,k)$, kde $k \in \{3, \ldots, n\}$.

Úloha 8.10. Je pravda, že permutace je sudá právě tehdy, když je druhou mocninou nějaké jiné permutace?

⋆ **Úloha 8.11.** Dokažte, že grupa $\mathbf{S}_n$ je generována libovolným n-cyklem a libovolnou transpozicí právě tehdy, když n je prvočíslo.

⋆ **Úloha 8.12.** Dokažte, že znaménko permutace $\pi \in \mathbf{S}_n$ je možné spočítat jako paritu počtu *inverzů* (fakt hloupá terminologie!), tj. takových dvojic $(i, j) \in \{1, \ldots, n\}^2$, že $i < j$ a $\pi(i) > \pi(j)$.

⋆ **Úloha 8.13.** Uvažme nějakou permutaci π množiny $1, 2, \ldots, n$. Postupně za sebe napišme všechny prvky $\pi(1), \pi(2), \ldots, \pi(n)$. Jejich čtením zleva doprava získáme postupně $f(\pi)$ rostoucích úseků (včetně těch délky 1, takže např. pro transpozici $\pi = (2\,1) \in \mathbf{S}_2$ je $f(\pi) = 2$). Jaká je průměrná hodnota $f(\pi)$ přes všechny permutace zadané množiny? (Nápověda: Párujte.)

⋆ **Úloha 8.14** (MEMO 2013)**.** Kolik různých permutací můžeme dostat, začneme-li s uspořádanými čísly $1, 2, \ldots, n$ ($n \geq 2$) a v nějakém pořadí provedeme všech $n-1$ prohození sousedních čísel? (Nápověda: Indukce.)

⋆ **Úloha 8.15.** Uvažme strom na n vrcholech označených čísly $1, 2, \ldots, n$. Postupně zvolíme všechny hrany (každou právě jednou), přičemž vždy prohodíme čísla na koncích zvolené hrany. Tím dostaneme nějakou permutaci čísel ve vrcholech. Kolik cyklů může tato permutace obsahovat? (Nápověda: Indukce.)

⋆⋆ **Úloha 8.16** (Zolotarevovo lemma)**.** Nechť p je liché prvočíslo. Násobení prvkem $a \in \mathbb{Z}_p^*$ indukuje jistou permutaci prvků $\mathbb{Z}_p^*$. Dokažte, že tato permutace je sudá právě tehdy, když je a kvadratickým zbytkem modulo p.