6. Permutace

Cv. 6.1 Mějme permutace

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}, \quad q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 6 & 4 \end{pmatrix}.$$

Najděte jejich cykly, znaménka, inverze a složte permutace p, q mezi sebou.

Řešení:
Permutace p zobrazuje $1 \to 2$, dále $2 \to 3$,$3 \to 4$ a $4 \to 1$. Tudíž jeden cyklus je $(1, 2, 3, 4)$, analogicky druhý cyklus je $(5, 6) \implies p = (1, 2, 3, 4)(5, 6)$. Podobně pro permutaci q máme $1 \to 1$ (první cyklus), $2 \to 3$,$3 \to 2$ (druhý cyklus) a $4 \to 5$,$5 \to 6$,$6 \to 4$ (třetí cyklus). Permutaci q lze zapsat pomocí cyklů jako $q = (1)(2, 3)(4, 5, 6)$.

Permutace p je zadána na $n = 6$ prvcích a skládá se ze $c = 2$ cyklů, proto má znaménko $\operatorname{sgn}(p) = (-1)^{n-c} = (-1)^{6-2} = 1$. Podobně spočítáme $\operatorname{sgn}(q) = (-1)^{6-3} = -1$.

Inverzní permutaci k p můžeme najít několika způsoby. Pokud vyjdeme z tabulkového zadání p, tak stačí prohodit oba řádky, čímž se ze vzorů stanou obrazy a naopak, a pak jen setřídit sloupce od nejmenšího po největší. Dostaneme p^{-1} vyjádřené tabulkou

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}.$$

Pokud využijeme zápisu p pomocí cyklů, stačí pouze prohodit pořadí čísel v každém cyklu, tj. $p^{-1} = (4, 3, 2, 1)(6, 5)$. Zde si můžeme uvědomit, že cykly délek 1 a 2 nemusíme invertovat, protože jsou sami sobě inverzní.

Permutace skládáme jako každé jiné zobrazení, tedy $p \circ q$ zobrazí prvek i na $p(q(i))$. Tabulkově vyjádřeno

$$\begin{array}{ccccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ q & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 & 5 & 6 & 4 \\ p & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 4 & 3 & 6 & 5 & 1 \end{array}$$

čili

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix}.$$

Podobně můžeme postupovat pomocí popisu přes cykly a dospějeme k vyjádření $p \circ q = (1, 2, 4, 6)(3)(5)$. Pro srovnání, složení v opačném pořadí je $q \circ p = (1, 3, 5, 4)(2)(6)$. To ilustruje, že skládání permutací není komutativní.

Cv. 6.2 Mějme permutaci

$$p = (1, 3, 4)(2, 5)(6, 11, 10, 9, 8, 7).$$

Spočítejte p^9 a p^{-14}.

Pro jakou nejmenší mocninu $k \geq 1$ dostaneme $p^k = id$?

Řešení:
K permutaci p^9 se nejrychleji dostaneme tak, že spočítáme $p^2 = p \circ p$, následně $p^4 = p^2 \circ p^2$, $p^8 = p^4 \circ p^4$ a nakonec $p^9 = p^8 \circ p$.

Dostáváme

- $p^2 = (1,4,3)(2)(5)(6,10,8)(7,11,9)$,
- $p^4 = (1,3,4)(2)(5)(6,8,10)(7,9,11)$,
- $p^8 = (1,4,3)(2)(5)(6,10,8)(7,11,9)$,
- $p^9 = (1)(2,5)(3)(4)(6,9)(7,10)(8,11)$.

Pro p^{-14} nejprve určíme stejným způsobem $p^{14} = p^8 \circ p^4 \circ p^2$ a následně spočítáme inverzní zobrazení. Dostáváme

- $p^{14} = (1,4,3)(2)(5)(6,10,8)(7,11,9)$
- $p^{-14} = (1,3,4)(2)(5)(6,8,10)(7,9,11)$.

Abychom určili nejmenší mocninu $k \geq 1$ takovou, že $p^k = id$, podíváme se na mocniny, které se budou chovat jako id na jednotlivých cyklech. První cyklus má délku 3, tedy každý prvek v něm obsažený bude vždy po 3 iteracích zpátky na svém místě. Prvnímu cyklu tedy odpovídá mocnina $3k_1$, kde $k_1 \geq 1$. Podobně pro druhý cyklus délky 2 potřebujeme, aby byla mocnina násobek 2 a pro třetí cyklus délky 6 mocninu, která je násobkem 6. Nejmenší společný násobek čísel $2,3,6$ je 6, tedy $k = 6$. První cyklus se *protočí* 2-krát, druhý 3-krát a poslední 1-krát.

Cv. 6.3 Určete znaménko permutací r, s, kde

$$r = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}, \quad s = (1,3,\dots,2n-1,2,4,6,\dots,2n)$$

Řešení:
Permutaci r můžeme pomocí cyklů zapsat jako

$$r = \begin{cases} (1,n)(2,n-1)\dots(\frac{n}{2},\frac{n+2}{2}) & \text{pro } n \text{ sudé,} \\ (1,n)(2,n-1)\dots(\frac{n-1}{2},\frac{n+3}{2})(\frac{n+1}{2}) & \text{pro } n \text{ liché.} \end{cases}$$

V prvním případě máme $\frac{n}{2}$ cyklů, v druhém $\frac{n-1}{2}$ cyklů. Celkově tedy dostáváme, že

$$\operatorname{sgn}(r) = (-1)^{n - \text{počet cyklů}} = \begin{cases} (-1)^{n-\frac{n}{2}} = (-1)^{\frac{n}{2}} & \text{pro } n \text{ sudé,} \\ (-1)^{n-\frac{n-1}{2}} = (-1)^{\frac{n-1}{2}} & \text{pro } n \text{ liché.} \end{cases}$$

Znaménko permutace s můžeme spočítat pomocí počtu *inverzí*. Inverze je dvojice prvků (i,j), taková, že $i > j$ a i se v cyklu nachází před j. Určíme:

- $2n-1$: $(2n-1,2),(2n-1,4),\dots,(2n-1,2n-2)$ - dohromady $n-1$ inverzí,
- $2n-3$: $(2n-3,2),(2n-3,4),\dots,(2n-3,2n-4)$ - dohromady $n-2$ inverzí,
- $\vdots$

- $3 : (3,2)$ - dohromady 1 inverze.

Celkově tedy máme $\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}$ inverzí, proto $\operatorname{sgn}(s) = (-1)^{\text{počet inverzí}} = \operatorname{sgn}(s) = (-1)^{\frac{n(n-1)}{2}}$.

Cv. 6.4 Najděte všechny permutace komutující s $p = (1,2)(3)$.

Řešení:
Pro p máme celkem $3! = 6$ možných permutací, otestováním všech permutací dostaneme, že jediné 2 možnosti jsou p a id.

Cv. 6.5 Najděte všechny permutace splňující $p \in S_{10}$ a $p^2 = (1,3)(2,4)(7,8,9,10)$.

Řešení:
Podívejme se nejprve, jak může vzniknout cyklus $(1,3)$. Aby se 1 zobrazilo na 3 v p^2, musí v p být součástí nějaké cyklu $(\dots,1,a,3,\dots)$. Podobně aby se 3 zobrazilo na 1, musí být $(\dots,3,b,1,\dots)$. Spojením obou úseků dostáváme $(\dots,1,a,3,b,1,\dots)$, tedy nutně cyklus $(1,a,3,b)$. V permutaci p^2 se tento cyklus rozpadne na 2 podcykly $(1,3)(a,b)$. Ze struktury p^2 je jediná možnost, že $a = 2, b = 4$ nebo symetricky $a = 4, b = 2$.

Aby se dále prvky 5 a 6 zobrazily v p^2 sami na sebe, musí se buď oba zobrazit sami na sebe už v p, nebo tvořit cyklus o dvou prvcích $(5,c),(6,d)$. Pokud by libovolné z čísel byl součástí delšího cyklu, složením permutace sama se sebou bychom už nedostali (5), resp. (6). Ze struktury p^2 dále nutně vyplývá, že $c = 6$ a $d = 5$, jinak by (d) a (c) nebyly cykly z p^2.

Zbývá určit $p(7),\dots,p(10)$. Podobně jako v případě prvků 1, 3 odvodíme, že musí existovat úsek $(\dots,7,e,8,f,9,g,10,h,7,\dots)$, resp. cyklus $(7,e,8,f,9,q,10,h,7)$, který ale nejsme schopni pouze s pomocí prvků $7,\dots,10$ zkonstruovat. Z toho důvodu žádná permutace p nesplňuje zadání.

Cv. 6.6 Dokažte, že složením permutací dostaneme permutaci.

Řešení:
Abychom dokázali toto tvrzení, stačí ukázat, že složení dvojice permutací $p, q \in S_n$ je *prosté* a *na*. Poté se bude jednat o bijekci na konečné množině, což odpovídá definici permutace. Toto půjde jednoduše dokázat z faktu, že obě permutace tyto vlastnosti splňují.

Prosté: Mějme $x, y \in \{1,\dots,n\}$ a nechť platí

$$(p \circ q)(x) = p(q(x)) = p(q(y)) = (p \circ q)(y).$$

Protože zobrazení p je prosté, platí, že nutně $q(x) = q(y)$. Nyní využijeme toho, že je prosté q a tedy platí, že $x = y$. Tedy i zobrazení $(p \circ q)$ je prosté.

Na: Aby platila tato vlastnost, musí pro každé $x \in \{1,\dots n\}$ existovat prvek $y \in \{1,\dots,n\}$ takové, že $(p \circ q)(y) = p(q(y)) = x$. Protože zobrazení p je „na“, tak existuje $z \in \{1,\dots,n\}$ takové, že $p(z) = x$. Zároveň z vlastnosti na permutace q existuje y, že $q(y) = z$. Toto y splňuje tedy vztah $q(p(y)) = x$.

Cv. 6.7 Dokažte, že znaménko permutace p lze ekvivalentně definovat jako $\mathrm{sgn}(p) = (-1)^s$, kde s je počet cyklů p sudé délky.

Řešení:
Každý cyklus můžeme zapsat pomocí transpozic jako

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

Cyklus délky k tedy můžeme zapsat pomocí $k-1$ transpozic, tedy znaménko sudého cyklu je $(-1)^{k-1} = (-1)$, zatímco znaménko lichého cyklu $(-1)^{k-1} = 1$. Znaménko permutace o ℓ cyklech můžeme zapsat jako součin znamének jednotlivých cyklů. Vidíme, že cykly liché délky přispějí do celkového součinu hodnotou 1, zatímco cykly sudé délky hodnotou (-1). Stačí proto uvažovat pouze sudé cykly a skutečně platí, že $\mathrm{sgn}(p) = (-1)^s$, kde s je počet cyklů sudé délky.