

## 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 v obou pořadích.

**Řešení:**

Permutace  $p$  zobrazuje  $1 \rightarrow 2$ , dále  $2 \rightarrow 3$ ,  $3 \rightarrow 4$  a  $4 \rightarrow 1$ . Tudíž jeden cyklus je  $(1, 2, 3, 4)$ , analogicky druhý cyklus je  $(5, 6)$ . Tudíž zápis permutace pomocí cyklů je  $p = (1, 2, 3, 4)(5, 6)$ .

Podobně pro permutaci  $q$  máme  $1 \rightarrow 1$  (první cyklus),  $2 \rightarrow 3$ ,  $3 \rightarrow 2$  (druhý cyklus) a  $4 \rightarrow 5$ ,  $5 \rightarrow 6$ ,  $6 \rightarrow 4$  (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  $\text{sgn}(p) = (-1)^{n-\text{počet cyklů}} = (-1)^{6-2} = 1$ . Podobně spočítáme  $\text{sgn}(q) = (-1)^{6-3} = -1$ .

Inverzní permutaci k permutaci  $p$  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 setřídít 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

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

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 permutace  $p^9$  a  $p^{-14}$ .

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

**Řešení:**

Naivní způsob spočítání  $p^9$  je složit postupně permutaci  $p^9 = p \circ p \circ p \circ p \circ p \circ p \circ p \circ p \circ p$ .

Efektivnější způsob počítání vysokých mocnin (čehokoli) je využití dvojkového zápisu exponentu a iterovaného mocnění na druhou. Konkrétně k permutaci  $p^9$  se 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  $p^9 = p^8 \circ p$ .

V našem případě, kdy mocníme permutace, můžeme využít ještě rozkladu na cykly. Cyklus  $p = (u_1, \dots, u_k)$  délky  $k$  se při mocnění chová tak, že  $p^k = id$  a  $p^{k+1} = p$ . To nás vede k metodě, kdy budeme mocnit každý cyklus zvlášť a mocninu daného cyklu spočítáme efektivně s využitím modula jeho délky. Konkrétně,  $(1, 3, 4)^9 = id$ ,  $(2, 5)^9 = (2, 5)^1 = (2, 5)$  a  $(6, 11, 10, 9, 8, 7)^9 = (6, 11, 10, 9, 8, 7)^3 = (6, 9)(7, 10)(8, 11)$  Tudíž

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

Permutaci  $p^{-14}$  určíme stejným způsobem s tím, že uvažujeme i záporné exponenty. Tudíž  $(1, 3, 4)^{-14} = (1, 3, 4)^1$ ,  $(2, 5)^{-14} = (2, 5)^0 = id$ ,  $(6, 11, 10, 9, 8, 7)^{-14} = (6, 11, 10, 9, 8, 7)^4 = (6, 8, 10)(7, 9, 11)$ . Nakonec dostáváme

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

Abychom určili nejmenší mocninu  $k \geq 1$  takovou, že  $p^k = id$ , podíváme se na jednotlivé cykly a zjistíme, jaké mocniny dají identitu. První cyklus má délku 3, tedy třetí mocnina a jakýkoli její celý násobek dají identitu. Podobně druhý cyklus má délku 2, čili identitu dostaneme pro sudé mocniny, a konečně třetí cyklus délky 6 vede na mocninu 6. Nejmenší společný násobek čísel 2, 3, 6 je 6, tedy hledané  $k = 6$ . Při šesté mocnině se první cyklus *protočí* 2-krát, druhý 3-krát a poslední 1-krát.

**Cv. 6.3** Rozložte permutaci  $(1, 2, 3, 4, 5)$  na složení transpozic, a to alespoň dvěma různými způsoby. Jaký je nejmenší možný počet transpozic, které k rozkladu potřebujeme?

**Řešení:**

Dvě možná řešení jsou:

$$(1, 2, 3, 4, 5) = (1, 2)(2, 3)(3, 4)(4, 5) = (1, 5)(1, 4)(1, 3)(1, 2).$$

Transpozic musí být alespoň 4. Každá nová transpozice snížší počet cyklů maximálně o 1, takže abychom z identity zkonstruovali cyklus délky 5, potřebujeme alespoň 4 transpozice.

**Cv. 6.4** Dokažte, že každou permutaci  $p \in S_n$  lze složit pomocí nanejvýš  $n - 1$  transpozic. Obecně, permutace  $p \in S_n$  se skládá z  $k$  cyklů. Pomocí kolika transpozic se dá složit? Najděte všechny možnosti.

**Řešení:**

V předchozím cvičení 6.3 jsme viděli, že každý cyklus délky  $c$  lze složit pomocí  $c - 1$  transpozic. Pokud se tedy permutace  $p$  skládá z právě  $k$  cyklů, tak ji umíme složit z právě  $n - k$  transpozic. Tím pádem každou permutaci lze složit z maximálně  $n - 1$  transpozic.

Vždycky lze přidat dodatečné (a v zásadě zbytečné) páry transpozic  $(i, j)(i, j)$  a počet transpozic tím navýšit. Není ale možné změnit paritu počtu transpozic (tím by se změnilo znaménko permutace). Možné počty transpozit, ze kterých můžeme  $p$  složit, jsou tedy  $n - k, n - k + 2, n - k + 4, \dots$

**Cv. 6.5** Určete znaménko permutace  $r$  zadané tabulkou:

$$r = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}$$

**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

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

Souhrnně můžeme též psát  $\text{sgn}(r) = (-1)^{\lfloor \frac{n}{2} \rfloor}$ .

**Cv. 6.6** 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  $p$  nespĺňuje zadání.

*Poznámka.* Znaménko permutace  $p^2$  je vždy sudé (pro libovolnou permutaci  $p$ ), neboť platí  $\text{sgn}(p^2) = \text{sgn}(p)\text{sgn}(p) = \text{sgn}(p)^2 = 1$ . Ale zadaná permutace  $(1, 3)(2, 4)(7, 8, 9, 10)$  má znaménko  $(-1)^{10-5} = -1$ , tudíž nemůže být druhou mocninou žádné permutace.

**Cv. 6.7** Dokažte, že složením permutací dostaneme permutaci.

**Řešení:**

Abychom dokázali toto tvrzení, stačí ukázat, že složení dvou 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.

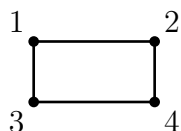
**Prosté:** Mějme  $x, y \in \{1, \dots, n\}$  a necht' platí

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

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  $y \in \{1, \dots, n\}$  takový, 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. 6.8** Najděte všechny symetrie obdélníku, popište je permutacemi a ověřte, že tvoří podgrupu grupy  $(S_4, \circ)$ .



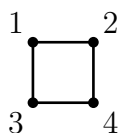
**Řešení:**

Obdélník má čtyři symetrie:

- identita, která odpovídá permutaci  $id = (1)(2)(3)(4)$ ,
- překlopení podle svislé osy odpovídá permutaci  $(1, 2)(3, 4)$ ,
- překlopení podle vodorovné osy odpovídá permutaci  $(1, 3)(2, 4)$ ,
- otočení o  $180^\circ$  odpovídá permutaci  $(1, 4)(2, 3)$ .

Snadno ověříme, že tato množina permutací je uzavřená na inverze a skládání, čili tvoří podgrupu.

**Cv. 6.9** Najděte všechny symetrie čtverce, popište je permutacemi a ověřte, že tvoří podgrupu grupy  $(S_4, \circ)$ .



**Řešení:**

Analogické předchozímu cvičení 6.8. Kromě tamějších symetrií zde máme navíc:

- překlopení podle diagonály, což odpovídá permutaci  $(1, 4)(2)(3)$ ,
- překlopení podle šikmé diagonály, což odpovídá permutaci  $(1)(4)(2, 3)$ ,
- otočení o  $90^\circ$  ve směru hodinových ručiček, což odpovídá  $(1, 2, 4, 3)$ ,
- otočení o  $90^\circ$  proti směru hodinových ručiček, což odpovídá  $(1, 3, 4, 2)$ .

Opět ověříme, že tato množina osmi permutací je uzavřená na inverze a skládání, takže tvoří podgrupu.