7. Permutace a vektorové prostory

Permutace

Cv. 7.1 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 $1 \to 2$, dále $2 \to 3$, $3 \to 4$ a $4 \to 1$. Tudíž jeden cyklus je $(1, 2, 3, 4)$, analogicky druhý cyklus je $(5, 6)$. Tudíž zápis permutace pomoci cyklů je $p = (1, 2, 3, 4)(5, 6)$.

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 $\mathrm{sgn}(p) = (-1)^{n-\text{počet cyklů}} = (-1)^{6-2} = 1$. Podobně spočítáme $\mathrm{sgn}(q) = (-1)^{6-3} = -1$.

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 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. 7.2 Mějme permutaci

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

Spočítejte permutaci p^9.

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 $p = (u_1, \ldots, u_k)$ 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

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

Cv. 7.3 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° odpovídá permutaci $(1,4)(2,3)$.

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

Vektorové prostory

Cv. 7.4 Rozhodněte, zda tvoří vektorový prostor:

(a) $\mathbb{R}^n$ nad $\mathbb{Q}$,

(b) $\mathbb{Q}^n$ nad $\mathbb{R}$,

(c) $\mathbb{R}^n$ nad $\mathbb{R}$ s operacemi $x \oplus y = x + y$, $\alpha \odot x = -\alpha \cdot x$,

(d) $\mathbb{R}^n$ nad $\mathbb{R}$ s operacemi $x \oplus y = x + y$, $\alpha \odot x = -\alpha \cdot x$, $\forall x, y \in \mathbb{R}^n, \alpha \in \mathbb{R}$, kde však tentokrát $\alpha \odot \beta = -\alpha \cdot \beta, \forall \alpha, \beta \in \mathbb{R}$.

Řešení:

(a) Jedná se o vektorový prostor, protože $\mathbb{R}^n$ nad $\mathbb{Q}$ má pro operace sčítání a násobení skalárem stejná vlastnosti jako vektorový prostor $\mathbb{R}^n$ nad $\mathbb{R}$. Potenciálně jediný problém by mohl být použití jiného tělesa, protože bychom mohli při násobení skalárem dostat vektory mimo $\mathbb{R}^n$. Protože $\mathbb{Q} \subseteq \mathbb{R}$, tento problém nenastane.

(b) Narozdíl od předchozího případu zde už problém nastane. Nejedná se o vektorový prostor, protože při násobení vektoru skalárem se nejedná o operaci $\mathbb{R} \times \mathbb{Q}^n \to \mathbb{Q}^n$; můžeme dostat ve vektoru reálné složky. Není splněna uzavřenost množiny na danou operaci.

(c) Není vektorový prostor, protože neplatí asociativita násobení:

$$\alpha \odot (\beta \odot v) = \alpha \odot (-\beta v) = \alpha\beta v \;\neq -\alpha\beta v \; = (\alpha\beta) \odot v.$$

Jako konkrétní protipříklad stačí vzít $\alpha = \beta = 1$ a $v = (1, 1)^T$.

(d) Jako první ověříme, že $(\mathbb{R}, +, \odot)$ je těleso. Zjistíme, že neutrálním prvkem vzhledem k násobení $\odot$ je -1. Dále postupujeme jako u předešlých příkladů, tedy ověřujeme definiční vlastnosti vektorového prostoru. Jedná se o vektorový prostor.