7. Permutace a vektorové prostory

Permutace

Dcv. 7.1 Mějme permutaci

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

Spočítejte permutaci p^{-14}.

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

Řešení:
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. 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.

Dcv. 7.2 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 $(\ldots, 1, a, 3, \ldots)$. Podobně aby se 3 zobrazilo na 1, musí být $(\ldots, 3, b, 1, \ldots)$. Spojením obou úseků dostáváme $(\ldots, 1, a, 3, b, 1, \ldots)$, 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 $p(7), \ldots, p(10)$. Podobně jako v případě prvků $1, 3$ odvodíme, že musí existovat úsek $(\ldots, 7, e, 8, f, 9, g, 10, h, 7, \ldots)$, resp. cyklus $(7, e, 8, f, 9, q, 10, h, 7)$, který ale nejsme schopni pouze s pomocí prvků $7, \ldots, 10$ zkonstruovat. Z toho důvodu žádná permutace p nesplňuje zadání.

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

Dcv. 7.3 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 $x, y \in \{1, \ldots, n\}$ 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 $x \in \{1, \ldots n\}$ existovat prvek $y \in \{1, \ldots, n\}$ takový, že $(p \circ q)(y) = p(q(y)) = x$. Protože zobrazení p je „na“, tak existuje $z \in \{1, \ldots, n\}$ takové, že $p(z) = x$. Zároveň z vlastnosti na permutace q existuje y, že $q(y) = z$. Toto y splňuje tedy vztah $q(p(y)) = x$.

Dcv. 7.4 Najděte všechny symetrie čtverce, popište je permutacemi a ověřte, že tvoří podgrupu grupy $(S_4, \circ)$.

Řešení:
Analogické předchozímu cvičení **??**. Kromě tamějších symetrií zde máme navíc:

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

Vektorové prostory

Dcv. 7.5 Rozhodněte, zda tvoří vektorový prostor:

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

(b) $U \times V$ nad $\mathbb{T}$, kde U, V jsou vektorové prostory nad $\mathbb{T}$, sčítání a násobení je definováno standardně po složkách.

(c) množina všech zobrazení $f\colon M \to V$ nad tělesem $\mathbb{T}$, kde M je daná množina a V vektorový prostor nad $\mathbb{T}$.

Řešení:

(a) Není vektorový prostor, protože neplatí distributivita. Pro jakékoli $\beta = -\alpha \neq 0$ dostáváme

$$(\alpha+\beta)\odot v \ = |0|v \ = 0 \neq 2|\alpha|v \ = |\alpha|v \ + |-\alpha|v \ = \alpha \odot v \ + \beta \odot v.$$

Konkrétně například stačí vzít $\alpha = 1$, $\beta = -1$, $v = (1,1)^T$.

(b) Prvky množiny $U \times V$ jsou uspořádané dvojice (u, v), kde $u \in U$, $v \in V$. Pro $(u,v),(u',v') \in U \times V$ je součet definován takto: $(u,v)+(u',v') = (u+u', v+v')$. Násobek je definován analogicky $\alpha(u,v) = (\alpha u', \alpha v)$, kde $\alpha \in \mathbb{T}$ a $(u,v) \in U \times V$.

Vlastnosti operací $U \times V$ nad $\mathbb{T}$ plynou z vlastností operací pro jednotlivé prostory U a V, takže se jedná vektorový prostor.

(c) Pokud není uvedeno jinak, uvažujeme přirozené definice operací sčítání a násobení funkcí, tedy

$$(f+g)(x) = f(x) + g(x), \quad (\alpha f)(x) = f(x).$$

Následně o dvou funkcích řekneme, že se rovnají, pokud se rovnají jejich funkční hodnoty na všech $x \in M$. Daná struktura je vektorový prostor, protože platí

i. asociativita sčítání

$$((f+g)+h)(x) = (f+g)(x) + h(x) = f(x) + g(x) + h(x),$$

$$(f+(g+h))(x) = f(x) + (g+h)(x) = f(x) + g(x) + h(x),$$

ii. neutrální prvek pro sčítání je funkce $e(x) = o$, kde o je nulový vektor prostoru V,

iii. inverzní prvek f^{-1} k funkci f je $f^{-1}(x) = -1 \cdot f(x)$,

iv. komutativita sčítání

$$(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x),$$

v. asociativita násobení skalárem

$$(\alpha(\beta f))(x) = \alpha(\beta f)(x) = \alpha\beta f(x) = (\alpha\beta)f(x) = ((\alpha\beta)f)(x),$$

vi. neutrální prvek pro násobení skalárem je $1 \in \mathbb{T}$,

vii. distributivita

$$((\alpha+\beta)f)(x) = (\alpha+\beta)f(x) = \alpha f(x) + \beta f(x) = (\alpha f)(x) + (\beta f)(x),$$

viii. distributivita

$$\begin{aligned}(\alpha(f+g))(x) &= \alpha(f+g)(x) = \alpha(f(x)+g(x)) = \\ &= \alpha f(x) + \alpha g(x) = (\alpha f)(x) + (\alpha g)(x).\end{aligned}$$