Permutační grupy

Tomáš „Šavlík“ Pavlík

Permutace

Permutací rozumíme prosté zobrazení $\pi: M \to M$ na konečné množině M. Permutace můžeme skládat stejně jako zobrazení, tedy $\pi \circ \rho\,(x) = \pi\,(\rho\,(x))$. Dále si zavedeme několik základních pojmů a budeme zjišťovat, jaká je souvislost permutací s algebraickou strukturou nazývanou grupa.

Definice 1. *Pevným bodem* permutace π rozumíme prvek $x \in M$ takový, že $\pi(x) = x$.

Definice 2. *Identickou permutací* (také *identitou*) rozumíme permutaci, ve které jsou všechny prvky pevné body. Značíme ji *id*. *Transpozicí* rozumíme permutaci, kde se dva prvky prohodí a ostatní jsou pevné body.

Definice 3. Permutaci nazveme *lichou*, pokud ji lze zapsat jako složení lichého počtu transpozic. Permutace je *sudá*, pokud není lichá.

Poznámka 4. Sudost nebo lichost můžeme zjistit také pomocí počtu inverzí nebo počtu sudých cyklů v permutaci.

Definice 5. *Řád* permutace π je nejmenší přirozené číslo n takové, že

$$\underbrace{\pi \circ \cdots \circ \pi}_{n} = id.$$

Příklad 6. Najděte všechny permutace na 3 prvcích a rozhodněte, které jsou sudé a které liché.

Příklad 7. Dokažte, že pro každé n je stejně sudých a lichých permutací na n prvcích.

Grupy

Definice 8. *Grupa* je čtveřice $(G, \circ, {}^{-1}, e)$, kde G je množina prvků grupy, $\circ: G \times G \to G$ je binární operace, ${}^{-1}: G \to G$ je unární operace, která každému

prvku přiřadí prvek inverzní a $e \in G$ je neutrální prvek (též jednotka). Navíc musí platit:

(i) $a \circ (b \circ c) = (a \circ b) \circ c$,
(ii) $a \circ e = e \circ a = a$,
(iii) $a \circ a^{-1} = a^{-1} \circ a = e$.

Příklady grup:

(a) Množina čísel $\{0, 1, 2, \ldots, n-1\}$ s operací sčítání modulo n. Značíme $\mathbb{Z}_n$.
(b) Množina čísel $\{1, 2, \ldots, p-1\}$ s operací násobení modulo p, kde p je prvočíslo.
(c) Všechny symetrie čtverce s operaci skládání zobrazení, značíme D_8.

Definice 9. *Permutační grupou* nazveme grupu, kde G jsou některé permutace na konečné množině M, e je identická permutace, $(\pi \circ \rho)(x) := \pi(\rho(x))$ a π^{-1} je opačná permutace k π.

Poznámka 10. Pozor, permutace v permutační grupě G musí být uzavřené na skládání. Pokud G obsahuje všechny permutace na M, pak jí říkáme *symetrická* a značíme ji S_n, kde $n = |M|$. Pokud G obsahuje jen všechny sudé permutace, pak jí říkáme *alternující* a značíme ji A_n.

Tvrzení 11. *Každá grupa lze zapsat jako permutační grupa.*

Definice 12. Permutační grupa je *k-tranzitivní*, pokud pro každné dvě posloupnosti prvků $\{a_i\}_{i=1}^k \in M$, $\{b_i\}_{i=1}^k \in M$ existuje $\pi \in G$ takové, že $\pi(a_i) = b_i$ pro všechna $i = 1, 2, \ldots, k$.

Příklad 13. Pro každé $n \in \mathbb{N}$ určete, kolik má grupa S_6 prvků řádu n.

Příklad 14. Dokažte, že pokud má grupa sudý počet prvků, pak má alespoň jeden prvek řádu 2.

Příklad 15. Mějme 2-tranzitivní permutační grupu G, která obsahuje transpozici. Dokažte, že G je symetrická.

Příklad 16. Dokažte, že pokud je permutační grupa k-tranzitivní a obsahuje cyklus délky k, pak je už nutně symetrická nebo alternující.

Návod.

(i) G je k-tranzitivní a má k-cyklus $\Rightarrow$ G obsahuje všechny k-cykly.
(ii) G obsahuje všechny k-cykly $\Rightarrow$ G obsahuje všechny 3-cykly.
(iii) G obsahuje všechny 3-cykly $\Rightarrow$ G obsahuje všechny sudé permutace.
(iv) G obsahuje všechny sudé permutace a jednu lichou $\Rightarrow$ G je symetrická.

Tvrzení 17. *Pokud je permutační grupa n-tranzitivní, kde $n \geq 5$, pak je nutně symetrická nebo alternující.*

Literatura a zdroje

[1] Jakub Opršal: *Rubikova teorie grup* (Sborník MKS Domaslav 2010)
[2] Libor Barto: Hlavolamy a grupy (knihovna MKS, *mks.mff.cuni.cz*)