Řešení Rubikovy kostky

Libor Barto — 11. dubna 2001

Tento text je soupisem pojmů z teorie grup, které se hodí při řešení různých hlavolamů typu Rubikova kostka, Patnáctka, ... Samotné řešení zde nenajdete.

Permutace

Permutace, skládání, identická a inverzní permutace.

- *Permutací* na množině X budeme rozumět zobrazení $\sigma : X \to X$, které je vzájemně jednoznačné (tedy různým prvkům přiřadí různé prvky a každý prvek je obrazem nějakého prvku). My se setkáme pouze s případy, kdy X je konečná množina.
- *Složení* dvou permutací σ, ϱ na X je permutace $\sigma \circ \varrho$ na X definovaná jako $\sigma \circ \varrho(x) = \varrho(\sigma(x))$ (je to tedy běžné složené zobrazení, ale v opačném pořadí).
- Permutaci i, která „nic nedělá“, tedy $(\forall x \in X)\ i(x) = x$, nazýváme *identická permutace*.
- *Inverzní permutaci* k permutaci ϱ značíme ϱ^{-1}, je to inverzní zobrazení k zobrazení ϱ, tedy $\varrho^{-1}(i) = j$ právě když $\varrho(j) = i$.

Zápis permutací.

- Permutaci můžeme zapsat tabulkou: do horního řádku napíšeme prvky množiny X (nejčastěji přirozená čísla) a do spodního řádku jejich obrazy.
- Další možností je znázornit permutaci grafem. Vrcholy grafu budou prvky množiny X. Z vrcholu x povede šipka do vrcholu y právě tehdy, když permutace zobrazí x do y. Z každého vrcholu a do každého vrcholu grafu povede právě jedna šipka.
- Poslední možností, o které se zmíníme, je zápis výčtem cyklů: např. $(1)(2,4,3)(5,6)$ je zápis permutace σ na $X = 1,2,3,4,5,6$, při které $\sigma(1) = 1, \sigma(2) = 4, \sigma(4) = 3, \sigma(3) = 2, \sigma(5) = 6, \sigma(6) = 5$. Cykly též pěkně vidíme na grafu permutace. Pokud známe množinu X, tak se většinou ze zápisu vynechávají cykly délky 1.

Je dobré si uvědomit, jak se udělá tabulka, graf a výčet cyklů složené permutace a permutace inverzní.

Sudé a liché permutace. Permutaci σ říkáme *sudá* (resp. *lichá*), je-li rozdíl mezi počtem prvků X a počtem cyklů v σ sudý (resp. lichý) (zde musíme počítat i cykly délky 1). Složením dvou sudých nebo dvou lichých permutací je sudá permutace, složení sudé s lichou nebo liché se sudou je permutace lichá.

Permutace je sudá, právě když má sudý počet cyklů sudé délky (a je lichá právě když má lichý počet cyklů sudé délky).

Lze ukázat, že každou permutaci lze vyjádřit jako složení transpozic (transpozice je permutace s jedním cyklem délky 2). Permutace je sudá, právě když ji lze složit ze sudého počtu transpozic.

Každou sudou permutaci lze vyjádřit jako složení trojcyklů (trojcyklus je permutace s jedním cyklem délky 3).

Konjugované permutace. Permutacím p a $q \circ p \circ q^{-1}$ budeme říkat *konjugované* permutace. Permutace $q \circ p \circ q^{-1}$ „dělá to samé, co permutace p ale na jiných prvcích“. Například pokud máme permutaci p zapsanou výčtem cyklů jako $p = (1,2,3)(4,5)$, výčet cyklů permutace $q \circ p \circ q^{-1}$ bude $(q^{-1}(1), q^{-1}(2), q^{-1}(3))(q^{-1}(4), q^{-1}(5))$.

Grupy

Definice grupy. Grupa $\mathcal{G}$ je čtveřice $(G, \circ, i, {}^{-1})$, kde G je množina, $\circ$ je binární operace na G (operace přiřadí každým dvěma prvkům G prvek G), $i \in G$, ${}^{-1}$ je unární operace na G (každému prvku G přiřadí nějaký prvek G) a pro libovolné tři prvky x, y, z množiny G platí tyto axiomy:

- $(x \circ y) \circ z = x \circ (y \circ z)$ (asociativita)
- $i \circ x = x \circ i = x$ (i je neutrální prvek)
- $x \circ x^{-1} = x^{-1} \circ x = i$ (x^{-1} je inverzní prvek)

Počet prvků (mohutnost) množiny G se nazývá *řád* grupy $\mathcal{G}$. Množina G se nazývá *nosná množina* grupy $\mathcal{G}$.

Splňuje-li operace $\circ$ navíc podmínku $\forall x, y \in G \quad x \circ y = y \circ x$, pak hovoříme o *komutativní* nebo *abelovské* grupě.

Mějme podmnožinu H množiny G takovou, že $\mathcal{H} = (H, \circ, i, {}^{-1})$ je grupa. Tato grupa se nazývá podgrupa grupy $\mathcal{G}$. Ke každá grupě najdeme alespoň dvě podgrupy — samotná grupa $\mathcal{G}$ a grupa s jediným prvkem v nosné množině — $(\{i\}, \circ, i, {}^{-1})$. Těmto podgrupám říkáme triviální.

O podmnožině M množiny G říkáme, že je *množinou generátorů*, pokud lze všechny prvky G získat operací $\circ$ a inverzemi z prvků množiny M. Naopak, pokud máme podmnožinu M množiny G, pak všechny prvky, které lze získat z prvků M operací $\circ$ a inverzemi tvoří podgrupu $\mathcal{G}$, které říkáme podgrupa *generovaná* množinou M.

Lagrangeova věta. Je-li $\mathcal{H}$ podgrupa konečné grupy $\mathcal{G}$, pak řád grupy $\mathcal{H}$ dělí řád grupy $\mathcal{G}$.

Důležité příklady grup.

- Množina celých (racionálních, reálných, komplexních) čísel tvoří s operací sčítání komutativní grupu. Neutrální prvkem je 0, inverzní prvek k x je $-x$.
- Množina racionálních (reálných, komplexních) čísel bez nuly tvoří s operací násobení komutativní grupu. Neutrální prvkem je 1, inverzní prvek k x je $\frac{1}{x}$.
- Množina všech permutací na dané konečné množině X spolu s operací skládání tvoří grupu, kterou značíme S_X a říkáme jí *symetrická* grupa. Neutrálním prvkem je identická permutace, inverzním prvkem je inverzní permutace. Symetrickou grupu na množině $X = \{1, 2, \ldots, n\}$ označujeme S_n. Její množinou generátorů je např. množina všech transpozic.
- Množina všech sudých permutací na dané konečné množině X spolu s operací skládání je podgrupu S_X, značíme A_X a říkáme jí *alternující* grupa. Její množinou generátorů je např. množina všech trojcyklů.

- Množina čísel $\{0, 1, \ldots, n-1\}$ tvoří s operací sčítání modulo n komutativní grupu. Tato grupa se nazývá *cyklická* a značí se $\mathbb{Z}_n$. Její množinou generátorů je např. množina $\{1\}$.

Konjugované prvky, normální podgrupy. Prvky p a $q \circ p \circ q^{-1}$ libovolné grupy se nazývají *konjugované*.

Mějme podgrupu $\mathcal{H}$ grupy $\mathcal{G}$ (nosné množiny jsou H, G). Řekneme, že $\mathcal{H}$ je *normální podgrupa* $\mathcal{G}$, pokud s každým prvkem H obsahuje množina H i všechny prvky konjugované (v grupě $\mathcal{G}$) — tedy platí $(\forall x \in H, y \in G) \quad y \circ x \circ y^{-1} \in H$.

Grupy permutací. Uvažujeme nějakou podgrupu $\mathcal{A}$ (s nosnou množinou A) grupy S_X. Řekneme, že prvky $a, b \in X$ jsou ekvivalentní, pokud existuje permutace $\varrho \in A$ taková, že $\varrho(a) = b$. Lze ukázat, že množinu X lze rozložit na navzájem disjunktní podmožiny (tzv. *orbity tranzitivity*) tak, že v každé orbitě jsou všechny dvojice prvků ekvivalentní.

Grupa $\mathcal{A}$ se nazývá *k-tranzitivní*, pokud pro každé dvě posloupnosti $i_1, \ldots, i_k$ a $j_1, \ldots, j_k$ různých prvků X existuje permutace $\varrho \in A$ taková, že $\varrho(i_1) = j_1, \ldots, \varrho(i_k) = j_k$.

Příklady

1. příklad Vyřešte všechny hlavolamy, které máte doma (tj. popište podmínky, kdy je pozice řešitelná a najděte postupy, kterými hlavolam uvedete z libovolné pozice do pozice základní).

2. příklad Uvažujme podgrupu S_{12} generovanou prvky

$$a = (12)(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11),$$
$$b = (1)(2)(9)(12)(3, 7, 11, 8)(4, 10, 5, 6),$$
$$c = (1, 12)(2, 11)(3, 6)(4, 8)(5, 9)(7, 10).$$

Dokažte, že je tato grupa 1-tranzitivní, 2-tranzitivní, ..., 5-tranzitivní. Pokud se dostanete až k 5-tranzitivitě, pokuste se dokázat, že není 6-tranzitivní.

3. příklad Zadání stejné jako u předchozího příkladu s tím rozdílem, že uvažujeme podgrupu S_{24} generovanou prvky

$$a = (24)(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23),$$
$$b = (1)(2)(6)(24)(3, 17, 10, 7, 9)(4, 13, 14, 19, 5)(8, 18, 11, 12, 23)(15, 20, 22, 21, 16),$$
$$c = (1, 24)(2, 23)(3, 12)(4, 16)(5, 18)(6, 10)(7, 20)(8, 14)(9, 21)(11, 17)(13, 22)(15, 19).$$

4. příklad Dokažte, že A_n, neobsahuje (pro žádné $n \geq 5$) žádnou netriviální normální podgrupu.