Rubikova teorie grup

Jakub „šnEk“ Opršal

Abstrakt. V tomto příspěvku se snažíme vysvětlit základní pojmy z teorie grup na příkladu klasického hlavolamu Rubikovy kostky. Definujeme pojem grupa a několik dalších elementárních pojmů. Popisujeme sktrukturu některých podgrup grupy permutací na čtyřech prvcích. Cvičení na konci obsahují velmi velkou nápovědu, jak všechnu tuto abstraktní teorii aplikovat na řešení Rubikovy kostky. Text přesahuje rozsah přednášky na soustředění v Domaslavi.

Teorie grup je rozsáhlá část moderní matematiky a jedna ze základních disciplín moderní abstraktní algebry. Pojem grupa byl v minolosti zkoumán Caylem, který zkoumal nejdříve grupy permutací, než byl zaveden pojem abstraktní grupy. Teorii dost rozšířil i Galois, jehož teorie dokazuje, že pro kořeny polynomu pátého a vyššího stupně neexistuje vzorec složený ze základních operací a odmocnin. V úvodních kapitolách zavádíme základní pojmy z teorie grup. K vyřešení Rubikovy kostky nemusíš znát nutně všechny tyto kapitoly, ale některé pojmy jsou nezbytné. Můžeš dokonce přeskočit rovnou na poslední kapitolu a pustit se do návodu a pokud narazíš na pojem, tak ho vyhledej v úvodních kapitolách. Podobně důkazy v úvodních kapitolách jsou spíše pro zajímavost a jako odpověď na otázku „Jak by se proboha tohle mohlo dokazovat?“ Často raději uvádíme teoretičtější důkazy, než ty elementární, pro příklad toho, jak důkazy v teorii grup běžně vypadají.

Grupy

Grupa pro nás bude množina, na které budeme mít dáno několik operací, které splňují podmínky napsané níže. Přesněji čtveřici $(G, \cdot, ^{-1}, 1)$, kde G je množina *prvků* grupy, $\cdot : G \times G \to G$ je binární operace (grupová operace), $^{-1}: G \to G$ je unární operace, která každému prvku přiřadí *inverzní prvek* a $1 \in G$ je vybraný prvek grupy, který budeme nazývat *jednotkou*.[1] Když je jasné, jaké jsou naše grupové operace mluvíme často o grupě $(G, \cdot, ^{-1}, 1)$ jen jako o grupě G.

Na tyto operace navíc klademe podmínky:

(1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativita)
(2) $a \cdot 1 = 1 \cdot a = a$ (jednotka)
(3) $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (inverse)

Nejdůležitější z těchto operací je $\cdot$, která definuje celou strukturu, dalšími dvěma operacemi vlastně říkáme, že existuje jednotka a pro každý prvek existuje inverzní.

Klíčová slova. teorie grup, algebra, abstraktní algebra, hlavolamy, Rubikova kostka

[1] Někdy se místo pojmu jednotka používá neutrální prvek a místo inverzní prvek opačný prvek.

Raději však budeme používat tuto notaci s více operacemi, protože tím se nám axiomy grupy zjednodušší o kvantifikátory.

Příklad. Klíčovým příkladem grupy pro nás bude Rubikova kostka. Jak tato grupa vypadá? Můžeme na ni nahlížet dvěma způsoby. Za prvé jako na grupu všech možných uspořádání kostiček na Rubikově kostce a za druhé jako na posloupnost tahů, kterými se k tomuto uspořádání můžeme dostat.

Jednotka pro nás bude základní uspořádání. Inverse nějakého uspořádání je posloupnost tahů, který toto uspořádání řeší (tj. vrátí do původního stavu). Grupová operaci definujme pro dvě uspořádání a, b (tedy i pro dvě posloupnosti tahů, neboť pro nás je to totéž), začneme v uspořádání a a pak provedeme posloupnost tahů, kterou bychom se dostali z uspořádání základního do uspořádání b, výsledné uspořádání je $a \cdot b$.

Tato definice funguje pro Rubikovy kostky všech různých rozměrů, včetně klasických $3 \times 3 \times 3$. Dále se v textu pro jednoduchost budeme odvolávat na Rubikovu kostku menší velikosti $2 \times 2 \times 2$. Většina úvah však skoro beze změny, nebo s menší úpravou funguje i pro libovolně velkou kostku.

Příklad. Uvedeme ještě některé grupy, které běžně potkáte v matematice. Grupa nenulových reálných čísel s násobením $(\mathbb{R} \setminus \{0\}, \cdot, ^{-1}, 1)$, multiplikativní grupa nenulových racionálních čísel $(\mathbb{Q}\setminus\{0\}, \cdot, ^{-1}, 1)$. Kromě toho ještě aditivní grupa celých čísel $(\mathbb{Z}, +, -, 0)$, nenech se zmást tím, že grupová operace je tady sčítání, správně bychom měli u definice grupy psát nějaký abstraktní symbol, za který pak můžeme dosadit cokoliv.

Naproti tomu, třeba přirozená čísla se sčítáním grupu neutvoří, protože tam nemáme ani nulu, ani inverzi (v našm případě $-n$) pro žádné přirozené číslo n. Dokonce ani přirozená čísla s násobením netvoří grupu, přestože tam máme jednotku 1.

Příklad. Zajímavá grupová operace je třeba skládání zobrazení, jak je tomu u permutačních grup $(S_n, \circ, ^{-1}, 1_n)$, kde S_n je množina všech zobrazení $\pi : n \to n$, z n-prvkové množiny do n-prvkové množiny, které jsou prosté[2] a na (tj. bijekce, nebo také permutace, uspořádání prvků $1, 2, \ldots, n$). Grupová operace $\circ$ je pak skládání zobrazení, tj. $(\pi \circ \sigma)(x) = \pi(\sigma(x))$. Inverse je opačná permutace, tj. $\pi^{-1}(x) = y$ takové, že $\pi(y) = x$ (jeho existenci a jednoznačnost máme z toho, že π je na a prosté). Jednotka v této grupě je identické zobrazení, tj. $1_n(x) = x$.

Příklad. (teorie čísel) Ještě uvedeme pár příkladů z teorie čísel. První z nich je additivní grupa zbytků modulo n, tj. $(\mathbb{Z}_n, +_n, -_n, 0)$, kde $\mathbb{Z}_n$ je množina zbytků po dělení číslem n a všechny operace jsou definovány modulo n, tj. $a +_n b$ je zbytek čísla $a + b$ po dělení n.

[2]Zobrazení $f\colon A \to B$ je *prosté* pokud pro každé $a, b \in A$, $a \neq b$ platí $f(a) \neq f(b)$. Dále f je *na* pokud pro každé $y \in B$ existuje $x \in A$, že $f(x) = y$.

Dalším příkladem je multiplikativní grupa nenulových zbytků modulo prvočíslo p, $(\mathbb{Z}_p^*, \cdot, {}^{-1}, 1)$. Kde násobení je modulo p a inverse prvku a je takové b, že $ab \equiv 1 \pmod{p}$. Jeho existenci nám zaručuje Bézoutova věta.[3] Dokonce pokud uvážíme grupu všech zbytků modulo n, které jsou s n nesoudělné, osnačme ji $(\mathbb{Z}_n^*, \cdot, {}^{-1}, 1)$, tak z naprosto stejnýc důvodů můžeme definovat inversi. Uvědomte si na tomto místě, že tato grupa má právě $\varphi(n)$ prvků, ještě se na to za chvíli odvoláme při jednom z budoucích příkladů.

Ještě než postoupíme dále. Upozorrním, že grupová operace $\cdot$, se zpravidla nepíše. Tedy výrazem abc myslíme $a \cdot b \cdot c$. Definujme si ještě pro n celé výraz a^n jako $a^n = aa \cdots a$, kde a je na pravé straně právě n-krát, je-li n kladné. Je-li záporné tak jako $a^n = (a^{-1})^{-n}$ a je-li nulové, pak $a^0 = 1$.

Řád prvku, grupy a Lagrangeova věta

Je-li a prvek grupy $(G, \cdot, {}^{-1}, 1)$, řekneme, že přirozené číslo n je *řád prvku* a, pokud $a^n = 1$ a navíc n je nejmenší takové přirozené číslo, tj. pro každé $k < n$ platí $a^n \neq 1$. Například otočení jedné stěny rubikovy kostky má řád 4.

Cvičení. Nalezněte v grupě $\mathbb{Z}_{11}^*$ alespoň jeden prvek každého řádu: $1, 2, 5$ a 10. Může existovat prvek jiného řádu?

Cvičení. Existuje v grupě $\mathbb{Z}_8^*$ prvek řádu 4?

Tvrzení. *Je-li G grupa a $a \in G$ má řád n, pak $a^k = 1$ právěž*[4] *$n \mid k$.*

Důkaz. Předpokládejme, že $a^k = 1$. Vydělme k číslem n se zbytkem: $k = qn + r$. Platí $a^q n = 1$, tedy i $a^r = a^{k-qn} = 1$. Tedy musí platit $r = 0$, jinak dostaneme spor s definicí řádu prvku.

Pro grupu G definujeme *řád grupy*, jako počet prvků nosné množiny G. Tj. řád grupy je $|G|$. Mezi řádem grupy a řádem prvku je velice úzký vztah. Řád prvku $g \in G$, není nic jiného než řád pogrupy $\{g^z : z \in \mathbb{Z}\} \leq G$.

O grupě G řekneme, že je *konečná* (konečného řádu), pokud je řád přirozené číslo, tj. $|G| < \infty$. Z příkladů, které jsme uvedli v předchozí kapitole jsou konečné grupy permutací, grupy z teorie čísel a také grupa Rubikovy kostky.

Potřebujeme ještě definovat podgrupu, podgrupa je podmnožina grupy, která je sama grupou. Řekneme, že $H \subseteq G$ je *podgrupa* grupy $(G, \cdot, {}^{-1}, 1)$, pokud množina H je uzavřená vůči operacím $\cdot, {}^{-1}$ a $1 \in H$. Uzavřenost znamená, že pro každé $h_1, h_2 \in H$ platí $h_1 h_2 \in H$ a $h_1^{-1} \in H$.

[3] Její znění a důkaz naleznete v [3].

[4] Právě tehdy, když.

Věta. (Lagrange) *Pro každou konečnou*[5] *grupu* $(G, \cdot, ^{-1}, 1)$ *a její podgrupu* $H \leq G$ *existuje přirozené číslo* $[G : H]$ *nazvané index podgrupy* H*, že platí:*

$$|H| \cdot [G : H] = |G|$$

Speciálně řád prvku dělí řád grupy, pro každou konečnou grupu G*.*

Důkaz. Nejdříve označme pro prvek $g \in G$, gH množinu všech součinů $\{gh : h \in H\}$. Uvědom si, že pro nekomutativní grupy nemusí platit $gH = Hg = \{hg : h \in H\}$.

Uvažme systém podmnožin G, který se zkládá ze všech množin tvaru gH, pro $g \in G$. První pozorování je, že $|gH| = |H|$ pro libovolný prvek g. Najdeme bijekci $b\colon H \to gH$ mezi těmito množinami. Definujme $b(h) = gh$ a $b^{-1}(k) = g^{-1}k$. Platí $b^{-1}b(h) = g^{-1}gh = h$ a naopak $bb^{-1}(k) = gg^{-1}k = k$, tedy b a b^{-1} jsou navzájem inverzní zobrazení a musejí tedy být bijekce.

Druhé pozorování je, že buď $g_1H = g_2H$, nebo g_1H a g_2H jsou disjunktní. Předpokládejme, že g_1H a g_2H mají neprázdný průnik, tedy existují $h_1, h_2 \in H$, že $g_1h_1 = g_2h_2$, tedy $g_1 = g_2h_2h_1^{-1}$. Následně pro každé $h \in H$ platí $g_1h = g_2h_2h_1^{-1}h \in g_2H$, neboť $h_2h_1^{-1}h \in H$. Tedy $g_1H \subseteq g_2H$. A obdoně i obráceně $g_2H \subseteq g_1H$, tedy nakonec $g_1H = g_2H$.

Uvažme konečně systém $\{gH : g \in G\}$ a označme $[G : H]$ počet různých množin v tomto systému. Pak neboť pro každé $g \in G$ je $g = g1_H \in gH$, tak G je sjednocení všech těchto množin. Každá z nich má velikost $|H|$, tedy $|G| = |H| \cdot [G : H]$. □

Speciální případem této věty je Eulerova věta z teorie čísel. Přesněji Eulerova věta je přesně Lagrangeova věta pro grupu $\mathbb{Z}_n^*$.

Komutativní grupy a komutátor

Zvláštní a jednodušší podtřídou grup jsou *komutativní* neboli *Abelovské grupy*. Řekneme, že grupa je komutativní, pokud kromě axiomů grupy splňuje ještě čtvrtý axiom $gh = hg$ pro každé dva prvky g, h.

Je-li G grupa, její komutativnost budeme „měřit“ *komutátorem*, který pro dva prvky g, h definujeme jako $[g, h] = ghg^{-1}h^{-1}$.

Tvrzení. *Grupa* G *je komutativní právěž pro každé dva prvky* $g, h \in G$ *platí* $[g, h] = 1$*.*

Důkaz. Chceme dokázat, že pro každé dva prvky platí $gh = hg$ právěž $[g, h] = 1$. Stačí první vztah vynásobit zprava prvkem $g^{-1}h^{-1} = (hg)^{-1}$. Tato úprava je ekvivalentní tedy dokázali jsme zároveň obě implikace. □

[5] Věta platí i bez předpokladu konečnosti, pak ale musíme trochu změnit význam symbolů. Pokud jsi někdy slyšel o tom, jak se počítá s kardinály, pak $|A|$ označíme kardinalitu množiny A a index $[G : H]$ nemusí být konečný, ale nějaký kardinál κ.

Konečné komutativní grupy nejsou moc zajímavé. Všechny můžeme zkonstruovat z grup $\mathbb{Z}_n$. Těmto grupám se docela věnuje teorie čísel. Nás ovšem budou dále zajímat hlavně nekomutativní grupy. Z příkladů v úvodní kapitole jsou to grupy permutací a hlavně grupa Rubikovy kostky.

Něco málo z permutačních grup

Zopakujeme definici permutační grupy. *Permutační grupa* S_n na n prvcích je množina všech bijektivních zobrazení $\pi\colon\{1,2,\dots,n\}\to\{1,2,\dots,n\}$, spolu s operací skládání zobrazení, $(\pi\circ\sigma)(x)=\pi(\sigma(x))$. Jednotka v této grupě je identická permutace, kterou budeme značit 1_n. Inverse pak inverzní permutace π^{-1}. Pro zmatení často symbol $\circ$ vynecháváme, avšak k nedorozumnění dojít nemůže.

Cvičení. Kolik má každá grupa S_n řád? Najdi všechny prvky v S_3.

Jak se dají permutace zapisovat? Nejjednodušší je zapisovat je tabulkou, tedy například tabulka

$$\pi=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$$

znamená, že permutace π zobrazí třeba prvek 1 na 3. My však raději budeme používat úspornější zápis pomocí cyklů, který navíc ještě popisuje i strukturu permutace. Ta samá permutace má zápis pomocí cyklů $\pi=(1\ 3)(2)(4)$. Ještě uvedeme jeden příklad, permutace se zápisem pomocí cyklů $\sigma=(1\ 2)(3\ 4)$ je zapsána tabulkou jako

$$\sigma=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

Zápis pomocí cyklů se čte tak, že číslo, které je v některé závorce se zobrazí na další číslo v té závorce, pokud je poslední, tak na první. Všimni si, že v tabulce musí být každé číslo dvakrát, ale v zápise pomocí cyklů je jen jednou. Rozmysli, jak se permutace v tomto tvaru skládají a jak bys převáděl mezi tabulkou a cykly.

Pokud při zápise pomocí cyklů nemůže dojít k nedorozumnění, vynecháváme pevné body, tedy závorky obsahující jen jedno číslo. Pak opravdu bude platit $(1\ 2)\circ(3\ 4)=(1\ 2)(3\ 4)$, takže symbol $\circ$ můžeme klidně také vynechávat.

Cvičení. Jaký má řád prvek $\sigma=(1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)(10)$?

Ještě uvedeme jednu definici, která je založená na tom, že existuje homomorfismus[6] z S_n na dvojprvkové grupy $(\{\pm1\},\cdot,^{-1},1)$. Označme ho $\operatorname{sgn}:S_n\to\{\pm1\}$ a nazvěme ho *znamínko permutace*. Tento homomorfismus zobrazuje libovolnou transpozici (tj. permutaci prohazující pouze dva prvky) na číslo -1. Ve skutečnosti

[6]Homomorfismus je zobrazení, které zachovává grupové operace. Přesněji $f\colon G\to H$ je *homomorfismus* pokud $f(g\cdot_G h)=f(g)\cdot_H f(h)$, $f(g^{-1_G})=f(g)^{-1_H}$ a $f(1_G)=1_H$.

každou permutaci umíme rozložit na složení transpozic (můžeš si zkusit nějaké rozložit) a ačkoliv tento rozklad není nikdy jednoznačný, tak parita počtu transpozic je vždy stejná a vyjadřuje ji znamínko permutace. Pokud je počet transpozic lichý, pak znamínko permutace je -1, jinak je znamínko 1.

Permutace $\pi \in S_n$, které mají znamínko $+1$ nazveme *sudé*, ty ostatní *liché*. Množina všech sudých permutací je podgrupou S_n a značí se A_n. Sudé permutace jsou právě ty permutace, které umíme napsat jako složení několika (ne nutně nezávislých) trojcyklů.

Cvičení. Jaké je znamínko cyklu délky n, tedy permutace $(1\ 2\ \cdots\ n)$.

Cvičení. Je-li $g \in S_4$ permutace, spočti $g \circ (1\ 3) \circ g^{-1}$. Jak to bude vypadat v obecném případě? Tedy, jak se liší rozklad na cykly permutace h a ghg^{-1}?

Řešení Rubikovy kostky

Konečně nastal správný čas vzít si zase do ruky Rubikovu kostku. Ještě upozorním, že všechna tato cvičení jsou primárně určena pro Rubikovu kostku rozměrů $2\times2\times2$, pro větší se budeš muset chvíli zamyslet a trochu je zobecnit.

Nejdříve si označme některé tahy na Rubikově kostce. Bude se nám hodit několik základních tahů. Otočení pravé stěny v kladném směru označme R, podobně otočení horní a přední stěny označme U a F.[7] Otáčení v opačném směru (tj. podle směru hodinových ručiček) budeme značit R^{-1}, U^{-1} a F^{-1}.

Cvičení 1. Chvíli si hraj s kostkou. Kolik z kostiček umíš dostat na správné místo? Zkus navrhnout nějaký postup, jak kostku vyřešit. Nemušíš přemýšlet, jestli všechny tahy umíš, spíš se jen zamysli, které tahy potřebuješ umět.

Cvičení 2. Ukaž, že Rubikova kostka není komutativní grupa. „Spočítej" komutátor $[R, U]$.

Narhněme tedy postup, jak kostku řešit. Prvně zapomeneme na orientaci kostiček a bude nás zajímat jen jejich poloha. Co se polohy týče zjednodušuje se nám tedy celá Rubikova kostka na grupu permutací S_8 na osmi prvcích.

Z předchozí kapitoly víme, že permutačí grupy jsou generovány transpozicemi, tedy budeme se chtít naučit prohodit dvě kostičky.

Cvičení 3. Pomůže nám v tom komutátor $[R, U]$, co vlastně dělá?

Cvičení 4. Zkus přesunout dvojice prohozených kostiček komutátorem $[R, U]$ a použij vztahu $(1\ 2)(3\ 4) \circ (1\ 2\ 3\ 4) = (2\ 4)$ k prohození dvou kostiček za zachování polohy všech ostatních.

Umíš už z prohození těchto dvou kostiček prohodit libovolné dvě? Zkus použít podobný trik jako předtím a prohodit dvě sousední kostičky.

[7] Z anglického „right", „upper" a „front".

V tuto chvíli bychom měli být schopni dostat všechny kostičky na svá místa. Zaměřme se na jejich natočení. Každá kostička má celkem tři možná natočení, správné, na jednu stranu a na druhou stranu. Tedy natočení jedné kostičky vlastně formuje grupu $Z_3 = \{-1, 0, 1\}$. Všimni si, že řád všech nenulových (nejednotkových) prvků v Z_3 je právě 3.

Cvičení 5. Jaký je řád komutátoru $[R, U]$? Proč je to právě tolik, jak to souvisí s permutací, kterou komutátor dělá na kostičkách, a jak to souvisí s natočením kostiček. Najdi $n \in \mathbb{N}$, že $[R, U]^n$ zachová polohu všech kostiček, ale ne jejich natočení.

Cvičení 6. Umíme už těmito tahy otočit kostičky všemi možnými způsoby? Najdi tah, který zachová otočení všech kostiček na jedné stěně, ale nezachová otočení kostiček na protilehlé stěně. Využij k tomu otočení přední stěny a toho, že otočíš kostičku na zadní stěně opačně, než předtím, kdežto na ostatních kostičkách už to bude bůh ví co.

Teď už by jsi měl znát všechny tahy, které potřebuješ k vyřešení kostky, přestože ještě neumíme otáčet jen jedinou kostičku. Finta je v tom, že ne všech natočení jde dosáhnout, narozdíl od permutací kostiček. Ty, kterých jde se dají popsat tak, že natočení kostek splňují vztah, který vypadá jako $a_1 + a_2 + \cdots + a_8 \equiv 0 \pmod 3$, kde $a_i \in \mathbb{Z}_3$ jsou natočení jednotlivých kostiček při správně zvolené orientaci.

Cvičení 7. Spočítej kolik je všech možných konfigurací Rubikovy kostky $2\times2\times2$, tj. řád grupy této kostky.

Ještě na závěr uvedeme pár problémů pro zamyšlení nad Rubikovými kostkami trochu obecněji. Většina těchto problému není určena pro žádný specifický rozměr kostky a některá ti můžou ti pomoci při řešení velkých až monstrózních kostek. Některé ze zajímavých teoretických otázek ještě nikdo nevyřešil, takže máš šanci být první.

Problém. Popiš všechny možné uspořádání Rubikovy kostky v závislosti na rozměrech kostky. Kolik jich je? Začni u malých rozměrů.

Problém. Uvaž, že máš tah t takový, že přeskládává kostky na přední stěně a na zbytku kostky, ale tyto dvě množiny kostiček mezi sebe nemíchá. Co dělá komutátor $[t, F]$? Dá se toho použít pro vyřešení kostky větších rozměrů?

Problém. Představ si, že znáš tah, který prohodí dvě kostky, ale neotočí je. Umíš ho využít k tomu, aby jsi některé kostky otočil?

Problém. Zkus tyto postupy aplikovat na nepravidelné Rubikovy kostky.

Problém. Najdi co nejkratší řešení Rubikovy kostky. Začni s rozměrem $2\times2\times2$. Je tvoje řešení opravdu nejkratší možné?

Problém. Jaký je nejmenší počet tahů, které si musíš pomatovat pro vyřešení Rubikovy kostky v závislosti na rozměrech?

Tak se do toho pusť a vyzkoušej si to. Dávej si pozor a neztrať se v Rubikově kostce. A nezapomeň zkusit použít vše, co znáš o permutacích a z teorie grup, bude se ti to hodit!

Literatura

[1] J. Chen, *Group Theory and the Rubik's Cube*, *http://www.math.harvard.edu/~jjchen/docs/Group Theory and the Rubik's Cube.pdf*.

[2] A. Drápal, *Teorie grup: základní aspekty*, Karolinum, Praha, 2000.

[3] J. Herman, R. Kučera, J. Šimša, *Metody řešení matematických úloh I*, Masarykova Universita, Brno, 2001.

[4] J. Trlifaj, *Algebra I*, Praha, 2009, *http://www.karlin.mff.cuni.cz/~trlifaj/en/NALG026.pdf*.

[5] Wikipedia, *Rubik's cube group*, *http://en.wikipedia.org/wiki/Rubik's cube group*.