Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathcal{S}(G)$.*

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathcal{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.* Důkaz.

Důsledek (Cayleyho věta). *Každá grupa G je izomorfní s vhodnou podgrupou grupy permutací $\mathcal{S}(G)$. Každá konečná grupa řádu n je izomorfní s vhodnou podgrupou grupy $\mathcal{S}_n$.*

Poznámka. V předchozí větě jsme každý prvek a grupy $(G, \cdot)$ reprezentovali permutací r_a nosné množiny G. Tuto situaci lze zobecnit, můžeme prvky grupy $(G, \cdot)$ reprezentovat permutacemi nějaké jiné množiny X, kterou můžeme libovolně zvolit. Budeme tedy studovat homomorfismy $G \to \mathcal{S}(X)$. Této situaci říkáme reprezentace grupy G permutacemi na množině X anebo stručně **akce grupy G na množině X**.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathcal{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathcal{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathcal{S}(X) = \mathcal{S}_n$. Zvolme dále libovolně $f \in \mathcal{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathcal{S}_n$ generovaná permutací f. Potom φ lze zvolit jako inkluzi, tj. každý prvek grupy G je zobrazen na sebe. Pokud zapíšeme permutaci f jako složení nezávislých cyklů, ihned vidíme, jak vypadá orbita O_y pro libovolný $y \in X$: platí-li $f(y) = y$, je $O_y = \{y\}$, v opačném případě je O_y množina všech prvků z cyklu, v němž vystupuje y. Stabilizátorem S_y prvku y je množina všech mocnin f^k permutace f, které ponechávají y na místě, tj. splňují $f^k(y) = y$. Jde o podgrupu grupy G generovanou permutací $f^{|O_y|}$, tj. $S_y = \langle f^{|O_y|} \rangle$. Platí proto $|G/S_y| = |O_y|$. Konkrétní příklad.

Akce grupy G na množině X

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathcal{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta. *Množina všech orbit $\{O_y;\ y \in X\}$ je rozklad na množině X.* Důkaz.

Věta. *Pro libovolné $y \in X$ tvoří stabilizátor S_y podgrupu grupy G.* Důkaz.

Věta. *Předpokládejme navíc, že X je konečná množina. Pak pro každé $y \in X$ je počet prvků v orbitě O_y roven indexu stabilizátoru S_y, tj. $|O_y| = |G/S_y|$.* Důkaz.

Důsledek. *Nechť je navíc X konečná množina a $y_1, \ldots, y_m \in X$ jsou takové, že v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$ (a tedy m je počet orbit). Pak platí $|X| = \sum_{i=1}^{m} |G/S_{y_i}|$.*

Věta (Burnsidovo lemma). *Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.*

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathcal{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y| = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|G/S_y|} = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_y|} =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |O_{y_i}| \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |G| = m|G|.$$

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Proč? Ale pro $n > 1$ už naivní metodou nakreslení všech možností neuspějeme. Užijme Burnsidovo lemma, kde X je množina všech obarvení vrcholů pravidelného 7úhelníka n barvami. Pak $|X| = n^7$, každé obarvení určí náramek, ale různá obarvení mohou dát týž náramek. Abychom zjistili, která obarvení dávají stejný náramek, užijme grupu $\mathbb{D}_7$ všech symetrií pravidelného 7úhelníka a definujme $\varphi : \mathbb{D}_7 \to \mathcal{S}(X)$ takto: pro symetrii $a \in \mathbb{D}_7$ a obarvení $y \in X$ je $\varphi(a)(y)$ to obarvení, které z y vznikne, aplikujeme-li na 7úhelník symetrii a. Pak dvě obarvení z množiny X odpovídají témuž náramku, právě když patří do stejné orbity. Pro identitu id je $|F_{\mathrm{id}}| = |X| = n^7$, pro libovolnou ze 6 zbylých rotací $r \in \mathbb{D}_7$ je $|F_r| = n$ a pro každou ze 7 osových souměrností s je $|F_s| = n^4$. Proč? Podle Burnsidova lemmatu je hledaný počet $\frac{1}{14}(n^7 + 7n^4 + 6n)$.

Další akce libovolné grupy G na její nosné množině

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $\rho_a : G \to G$, určené předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro každé $g \in G$, je bijekce, tedy $\rho_a \in \mathcal{S}(G)$.* Důkaz.

Definice. Nechť $(G, \cdot)$ je grupa. Jejím centrem $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G; \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathcal{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy. Přitom jádro $\ker \rho = Z(G)$. Pro libovolný prvek $g \in G$ platí, že g má jednoprvkovou orbitu v této akci, právě když g je v centru grupy G, tj.*

$$O_g = \{g\} \qquad \Longleftrightarrow \qquad g \in Z(G).$$ Důkaz.

Důsledek. *$Z(G)$ je normální podgrupa grupy G.*

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathcal{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Víme: počet prvků libovolné orbity je index stabilizátoru, tento index je dělitelem řádu grupy G, tj. čísla $|G| = p^k$. Dále platí

$$\begin{aligned} a \in Z(G) \quad &\iff \quad |O_a| = 1, \\ a \notin Z(G) \quad &\implies \quad p \mid |O_a|. \end{aligned}$$

Každý prvek z G patří do právě jedné orbity, počet prvků grupy $|G|$ je dělitelný číslem p. Odtud $p \mid |Z(G)|$.