Rozklad grupy podle podgrupy

Příklad. Pro libovolné $m \in \mathbb{N}$ tvoří množina H všech celých čísel dělitelných číslem m podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$. Výpočet.

Příklad. Pro $G = \mathcal{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = H$, $(1,3) \circ H = \{(1,3) \circ \mathrm{id}, (1,3) \circ (1,2)\} = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = \{(2,3) \circ \mathrm{id}, (2,3) \circ (1,2)\} = \{(2,3), (1,3,2)\}$, a tedy $G/H = \big\{H, \{(1,3), (1,2,3)\}, \{(2,3), (1,3,2)\}\big\}$.

Poznámka. Připomeňme, že rozkladem na množině M rozumíme systém neprázdných podmnožin množiny M, jejichž sjednocení je rovno celé množině M a které jsou po dvou disjunktní.

Věta. *Množina G/H všech levých tříd grupy G podle podgrupy H tvoří rozklad na množině G.* Důkaz.

Definice. Počet $|G/H|$ všech levých tříd grupy G podle podgrupy H se nazývá **index** podgrupy H v grupě G.

Věta. *Nechť $(G, \cdot)$ je konečná grupa, H její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.* Důkaz.

Lagrangeova věta a její důsledky

Věta. *Nechť $(G, \cdot)$ je konečná grupa, H její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.*

Důsledek (Lagrangeova věta). *Řád libovolné podgrupy konečné grupy G je dělitelem řádu grupy G.*

Důsledek. *Řád libovolného prvku konečné grupy G je dělitelem řádu grupy G.* Důkaz.

Důsledek. *Libovolná podgrupa prvočíselného řádu je cyklická.*

Důsledek. *Nechť G je konečná grupa konečného řádu $n = |G|$. Pak pro libovolný prvek $a \in G$ platí $a^n = 1$. Jinými slovy: exponent konečné grupy G je dělitelem řádu grupy G.*

Speciálním případem předchozího důsledku je následující věta z teorie čísel:

Věta (Eulerova). *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná nesoudělná čísla. Pak platí $a^{\varphi(m)} \equiv 1 \pmod{m}$.* Důkaz.

Naivní pokus o zavedení operace na rozkladu G/H

Inspirace. Zvolme pevně libovolné $m \in \mathbb{N}$ a jako dříve označme $H = [0]_m = \{mk;\ k \in \mathbb{Z}\}$. Pak H je podgrupa grupy $(\mathbb{Z}, +)$ a odpovídajícím rozkladem je $\mathbb{Z}/H = \mathbb{Z}_m$. Na $\mathbb{Z}_m$ jsme definovali operaci $+$ pomocí reprezentantů: pro libovolné $a \in \mathbb{Z}$ je totiž $a + H = [a]_m$ a použitou definici sčítání zbytkových tříd $[a]_m + [b]_m = [a + b]_m$ pro libovolná $a, b \in \mathbb{Z}$ lze psát ve tvaru $(a + H) + (b + H) = (a + b) + H$.

Pokus o zobecnění. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pak bychom na rozkladu G/H rádi zavedli operaci $\cdot$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$. Je to ale vždy možné?

Příklad. Pro $G = \mathcal{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = (1,2) \circ H = H$, $(1,3) \circ H = (1,2,3) \circ H = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = (1,3,2) \circ H = \{(2,3), (1,3,2)\}$, a tedy předchozí definice pomocí reprezentantů by dala $(1,3,2) \circ H = \big((1,2) \circ H\big) \circ \big((1,3) \circ H\big) = \big(\mathrm{id} \circ H\big) \circ \big((1,3) \circ H\big) = (1,3) \circ H$, což však není pravda.

Normální podgrupy

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Definice. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Řekneme, že H je **normální podgrupou** grupy G, jestliže pro každé $h \in H$ a každé $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$.

Příklad. V každé grupě G jsou $\{1\}$ i G normální podgrupy. Podgrupa $H = \{\mathrm{id}, (1,2)\}$ není normální podgrupou grupy $\mathcal{S}_3$.

Věta. V komutativní grupě G je každá podgrupa normální.

Věta. Je-li $f : G \to K$ homomorfismus grup, pak jeho jádro $\ker f$ je normální podgrupa grupy G. Důkaz.

Faktorgrupa

Věta. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak je možné na rozkladu G/H zavést operaci $\cdot$ následujícím způsobem: pro libovolné $a, b \in G$ definujeme součin levých tříd $a \cdot H$ a $b \cdot H$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$. Důkaz. Navíc platí: $(G/H, \cdot)$ je grupa. Důkaz.

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa G/H z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**. Příklady.

Věta. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je homomorfismus grup, jehož jádro $\ker \pi = H$. Důkaz.

Důsledek. Normální podgrupy grupy G jsou právě jádra homomorfismů $G \to K$ grupy G do vhodných grup K.

Věta. Nechť $(G, \cdot)$ je komutativní grupa, pak je každá podgrupa H grupy G normální a faktorgrupa G/H je komutativní.