Exponent konečné grupy

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.* Důkaz.

Definice. Nechť G je konečná grupa. Nejmenší přirozené číslo e takové, že pro každé $a \in G$ platí $a^e = 1$, se nazývá **exponent** grupy G. Příklad.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů. Tento nejmenší společný násobek je roven exponentu grupy G.

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.* Důkaz.

Věta (zákony o krácení). *Nechť G je grupa, $a, b, c \in G$. Pak platí*

$$a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c,$$

$$b \cdot a = c \cdot a \quad \Longrightarrow \quad b = c.$$

Důkaz.

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,
- pro každé $a, b \in H$ platí $a \cdot b \in H$.

Poznámka. Největší podgrupou grupy G (vzhledem k $\subseteq$) je celá G, nejmenší podgrupou je $\{1\}$.

Věta. *Nechť H je podgrupa grupy $(G, \cdot)$. Pak $\cdot$ určuje operaci na množině H, přičemž H je grupa vzhledem k této operaci. Je-li grupa G komutativní, pak je i grupa H komutativní.*

Označení. Zmiňovanou operaci na podgrupě budeme označovat stejným symbolem jako původní operaci na celé grupě, přestože tyto operace nejsou stejné.

Věta. *Jestliže H je podgrupa grupy G a K je podgrupa grupy H, pak je K také podgrupou grupy G.*

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G.* Důkaz.

Definice. Nechť M je podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podgrupou grupy G obsahující množinu M; evidentně je nejmenší s touto vlastností. Podgrupu $\langle M \rangle$ nazýváme **podgrupa generovaná množinou** M, množinu M nazýváme **množina generátorů podgrupy** $\langle M \rangle$.

Označení. Je-li $M = \{a_1, \ldots, a_n\}$, lze psát stručně $\langle a_1, \ldots, a_n \rangle$ místo $\langle M \rangle$. Příklady.

Poznámka. Zřejmě $\langle G \rangle = G$, $\langle \emptyset \rangle = \{1\}$. Pro každou $M \subseteq G$ platí

$$\langle M \rangle = \langle M \cup \{a^{-1};\ a \in M\} \rangle.$$

Definice. Řádem konečné grupy $(G, \cdot)$ rozumíme počet prvků této grupy, značíme $|G|$.

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$ Důkaz.

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. Důkaz.

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

Definice. Grupa G se nazývá **cyklická**, existuje-li $a \in G$ tak, že $G = \langle a \rangle$.

Příklad. Grupy $(\mathbb{Z}, +)$ i $(\mathbb{Z}_m, +)$ pro libovolné $m \in \mathbb{N}$ jsou cyklické.

Důsledek. *Konečná n-prvková grupa je cyklická, právě když obsahuje prvek řádu n.*

Důsledek. *Nechť H, K jsou podgrupy komutativní grupy $(G, \cdot)$. Pak platí $\langle H \cup K \rangle = \{h \cdot k;\ h \in H,\ k \in K\}$.*

Homomorfismus grup

Definice. Nechť $(G_1, \cdot)$ a $(G_2, *)$ jsou grupy, $f : G_1 \to G_2$ zobrazení. Řekneme, že f je **homomorfismus** grupy $(G_1, \cdot)$ do grupy $(G_2, *)$, jestliže pro každé $a, b \in G_1$ platí $f(a \cdot b) = f(a) * f(b)$. Injektivní homomorfismus se nazývá **vnoření**, bijektivnímu homomorfismu říkáme **izomorfismus**.

Poznámka. Nepřesně řečeno: homomorfismus je zobrazení mezi grupami, u kterého dostaneme totéž, ať už „*napřed počítáme a pak zobrazujeme*“ anebo „*napřed zobrazujeme a pak počítáme*“.

Příklad. Pro libovolné $m \in \mathbb{N}$ je zobrazení parita $p : \mathcal{S}_m \to \{1, -1\}$ homomorfismus grupy permutací $(\mathcal{S}_m, \circ)$ do grupy $(\{1, -1\}, \cdot)$, neboť pro libovolné permutace $f, g \in \mathcal{S}_m$ platí $p(f \circ g) = p(f) \cdot p(g)$. V případě $m = 2$ jde o izomorfismus.

Příklad. Zobrazení logaritmus $\log : \mathbb{R}^+ \to \mathbb{R}$ je homomorfismus multiplikativní grupy všech kladných reálných čísel $(\mathbb{R}^+, \cdot)$ do aditivní grupy všech reálných čísel $(\mathbb{R}, +)$, neboť pro libovolná kladná reálná čísla a, b platí $\log(a \cdot b) = (\log a) + (\log b)$. Protože je toto zobrazení bijekce, jde o izomorfismus.