Homomorfismus grup

Definice. Nechť $(G_1, \cdot)$ a $(G_2, *)$ jsou grupy. Zobrazení $f : G_1 \to G_2$ se nazývá **homomorfismus**, jestliže pro každé $a, b \in G_1$ platí $f(a \cdot b) = f(a) * f(b)$. **Vnoření** je injektivní homomorfismus, **izomorfismus** je bijektivní homomorfismus.

Příklad. Pro libovolné $m \in \mathbb{N}$ je determinant $\det : \mathcal{GL}_m(\mathbb{R}) \to \mathbb{R}$ homomorfismus grupy regulárních matic typu $m \times m$ s reálnými prvky $(\mathcal{GL}_m(\mathbb{R}), \cdot)$ do grupy nenulových reálných čísel $(\mathbb{R}^*, \cdot)$. Pro libovolné matice $A, B \in \mathcal{GL}_m(\mathbb{R})$ totiž podle Cauchyovy věty platí $\det(A \cdot B) = \det(A) \cdot \det(B)$. V případě $m = 1$ jde o izomorfismus.

Věta. Jsou-li G_1, G_2, G_3 grupy, $f : G_1 \to G_2$ a $g : G_2 \to G_3$ homomorfismy, pak je $g \circ f : G_1 \to G_3$ homomorfismus. Důkaz.

Věta. Nechť $f : G_1 \to G_2$ je homomorfismus grup. Pak $f(1) = 1$ a pro každé $a \in G_1$ platí $f(a^{-1}) = f(a)^{-1}$. Důkaz.

Věta. Nechť $f : G_1 \to G_2$ je izomorfismus grup. Pak i inverzní zobrazení $f^{-1} : G_2 \to G_1$ je izomorfismus grup. Důkaz.

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, $a \in G_1$ prvek řádu $n \in \mathbb{N}$. Pak řád prvku $f(a)$ v grupě G_2 je $k \in \mathbb{N}$ a platí $k \mid n$.*

Důkaz. Příklad.

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup. Pak obraz $f(G_1) = \{f(a);\, a \in G_1\}$ grupy G_1 je podgrupou grupy G_2.* *Důkaz.*

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, H podgrupa grupy G_2. Pak úplný vzor $f^{-1}(H) = \{a \in G_1;\, f(a) \in H\}$ podgrupy H je podgrupou grupy G_1.* *Důkaz.*

Definice. Nechť $f : G_1 \to G_2$ je homomorfismus grup. Množina $\ker f = \{a \in G_1;\, f(a) = 1\}$ se nazývá **jádro homomorfismu** f.

Důsledek. *Je-li $f : G_1 \to G_2$ je homomorfismus grup, pak jeho jádro $\ker f$ je podgrupa grupy G_1.*

Věta. *Homomorfismus grup $f : G_1 \to G_2$ je injektivní, právě když $\ker f = \{1\}$.* *Důkaz.*

Izomorfní grupy

Definice. Řekneme, že grupy G_1 a G_2 jsou **izomorfní**, a píšeme $G_1 \cong G_2$, jestliže existuje alespoň jeden izomorfismus $f : G_1 \to G_2$.

Příklad. Grupy $(\mathbb{R}^+, \cdot)$ a $(\mathbb{R}, +)$ jsou izomorfní, neboť logaritmus $\log : \mathbb{R}^+ \to \mathbb{R}$ je izomorfismus.

Věta. *Jsou-li G_1, G_2, G_3 grupy. Pak platí*

- $G_1 \cong G_1$,
- $G_1 \cong G_2 \implies G_2 \cong G_1$,
- $G_1 \cong G_2,\ G_2 \cong G_3 \implies G_1 \cong G_3$.

Věta. *Libovolná nekonečná cyklická grupa je izomorfní s grupou $(\mathbb{Z}, +)$. Libovolná konečná cyklická grupa řádu n je izomorfní s grupou $(\mathbb{Z}_n, +)$.* *Důkaz.*

Levé třídy rozkladu grupy podle podgrupy

<u>*Definice.*</u> Nechť $(G, \cdot)$ je grupa, H její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou <u>**levou třídu**</u> $a \cdot H$ rozkladu grupy G podle podgrupy H předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

<u>*Poznámka.*</u> Podle definice je levá třída $a \cdot H$ podmnožinou grupy G, je to množina všech součinů pevně zvoleného prvku a postupně se všemi prvky $h \in H$.

<u>*Věta.*</u> *Nechť $(G, \cdot)$ je grupa, H její podgrupa, $a, b \in G$ libovolné. Následující podmínky jsou ekvivalentní:*

- $a \cdot H = b \cdot H$,
- $a \in b \cdot H$,
- $b^{-1} \cdot a \in H$. *Důkaz.*

<u>*Označení.*</u> Označme G/H množinu všech levých tříd grupy G podle podgrupy H, tj. $G/H = \{a \cdot H;\ a \in G\}$. Příklady.