Homomorfismus grup

Definice. Nechť $(G_1, \cdot)$ a $(G_2, *)$ jsou grupy, $f : G_1 \to G_2$ zobrazení.

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 $f(a \cdot b) = f(a) * f(b)$.

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**.

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*“.

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 $p : \mathbb{S}_m \to \{1, -1\}$ homomorfismus grupy permutací $(\mathbb{S}_m, \circ)$ do grupy $(\{1, -1\}, \cdot)$, neboť pro libovolné permutace $f, g \in \mathbb{S}_m$ platí $p(f \circ g) = p(f) \cdot p(g)$.

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

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 $p : \mathbb{S}_m \to \{1, -1\}$ homomorfismus grupy permutací $(\mathbb{S}_m, \circ)$ do grupy $(\{1, -1\}, \cdot)$, neboť pro libovolné permutace $f, g \in \mathbb{S}_m$ 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 $\log(a \cdot b) = (\log a) + (\log b)$.

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 $p : \mathbb{S}_m \to \{1, -1\}$ homomorfismus grupy permutací $(\mathbb{S}_m, \circ)$ do grupy $(\{1, -1\}, \cdot)$, neboť pro libovolné permutace $f, g \in \mathbb{S}_m$ 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.

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.

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 $\det : \mathbb{GL}_m(\mathbb{R}) \to \mathbb{R}^*$ homomorfismus grupy regulárních matic typu $m \times m$ s reálnými prvky $(\mathbb{GL}_m(\mathbb{R}), \cdot)$ do grupy nenulových reálných čísel $(\mathbb{R}^*, \cdot)$.

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

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

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 $\det : \mathbb{GL}_m(\mathbb{R}) \to \mathbb{R}^*$ homomorfismus grupy regulárních matic typu $m \times m$ s reálnými prvky $(\mathbb{GL}_m(\mathbb{R}), \cdot)$ do grupy nenulových reálných čísel $(\mathbb{R}^*, \cdot)$. Pro libovolné matice $A, B \in \mathbb{GL}_m(\mathbb{R})$ 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. [Věta 8.3, str. 41]

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 $\det : \mathbb{GL}_m(\mathbb{R}) \to \mathbb{R}^*$ homomorfismus grupy regulárních matic typu $m \times m$ s reálnými prvky $(\mathbb{GL}_m(\mathbb{R}), \cdot)$ do grupy nenulových reálných čísel $(\mathbb{R}^*, \cdot)$. Pro libovolné matice $A, B \in \mathbb{GL}_m(\mathbb{R})$ 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. [Věta 8.3, str. 41]

Věta. Nechť $f : G_1 \to G_2$ je homomorfismus grup. Pak $f(1) = 1$ a pro každé $a \in G_1$ platí $f(a^{-1}) = f(a)^{-1}$. [Věta 8.4, str. 41]

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 $\det : \mathbb{GL}_m(\mathbb{R}) \to \mathbb{R}^*$ homomorfismus grupy regulárních matic typu $m \times m$ s reálnými prvky $(\mathbb{GL}_m(\mathbb{R}), \cdot)$ do grupy nenulových reálných čísel $(\mathbb{R}^*, \cdot)$. Pro libovolné matice $A, B \in \mathbb{GL}_m(\mathbb{R})$ 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. [Věta 8.3, str. 41]

Věta. Nechť $f : G_1 \to G_2$ je homomorfismus grup. Pak $f(1) = 1$ a pro každé $a \in G_1$ platí $f(a^{-1}) = f(a)^{-1}$. [Věta 8.4, str. 41]

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. [Věta 6.3, str. 33]

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, pak pro každé $a \in G_1$ a každé celé číslo n platí $f(a^n) = f(a)^n$.*

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, pak pro každé $a \in G_1$ a každé celé číslo n platí $f(a^n) = f(a)^n$.*

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 $k \mid n$.*

[Jestliže $a^n = 1$, pak $(f(a))^n = f(a^n) = f(1) = 1$, a proto řád k prvku $f(a)$ je dělitelem čísla n.]

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, pak pro každé $a \in G_1$ a každé celé číslo n platí $f(a^n) = f(a)^n$.*

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 $k \mid n$.*

[Jestliže $a^n = 1$, pak $(f(a))^n = f(a^n) = f(1) = 1$, a proto řád k prvku $f(a)$ je dělitelem čísla n.]

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.* [Věta 8.5, str. 42]

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, pak pro každé $a \in G_1$ a každé celé číslo n platí $f(a^n) = f(a)^n$.*

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 $k \mid n$.*

[Jestliže $a^n = 1$, pak $(f(a))^n = f(a^n) = f(1) = 1$, a proto řád k prvku $f(a)$ je dělitelem čísla n.]

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.* [Věta 8.5, str. 42]

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.* [Věta 8.9, str. 42]

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, pak pro každé $a \in G_1$ a každé celé číslo n platí $f(a^n) = f(a)^n$.*

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 $k \mid n$.*

[Jestliže $a^n = 1$, pak $(f(a))^n = f(a^n) = f(1) = 1$, a proto řád k prvku $f(a)$ je dělitelem čísla n.]

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.* [Věta 8.5, str. 42]

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.* [Věta 8.9, str. 42]

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.

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, pak pro každé $a \in G_1$ a každé celé číslo n platí $f(a^n) = f(a)^n$.*

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 $k \mid n$.*

[Jestliže $a^n = 1$, pak $(f(a))^n = f(a^n) = f(1) = 1$, a proto řád k prvku $f(a)$ je dělitelem čísla n.]

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.* [Věta 8.5, str. 42]

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.* [Věta 8.9, str. 42]

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.*

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, pak pro každé $a \in G_1$ a každé celé číslo n platí $f(a^n) = f(a)^n$.*

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 $k \mid n$.*

[Jestliže $a^n = 1$, pak $(f(a))^n = f(a^n) = f(1) = 1$, a proto řád k prvku $f(a)$ je dělitelem čísla n.]

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.* [Věta 8.5, str. 42]

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.* [Věta 8.9, str. 42]

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* $\ker f = \{1\}$. [Věta 8.11, str. 43]

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3.

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3. V grupě $\mathbb{Z}_4$ má neutrální prvek $[0]_4$ řád 1, prvek $[2]_4$ řád 2, prvky $[1]_4$ a $[3]_4$ řád 4.

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3. V grupě $\mathbb{Z}_4$ má neutrální prvek $[0]_4$ řád 1, prvek $[2]_4$ řád 2, prvky $[1]_4$ a $[3]_4$ řád 4. Protože v $\mathbb{Z}_4$ není prvek řádu 3, v každém homomorfismu $f : \mathbb{S}_3 \to \mathbb{Z}_4$ se každá z permutací $(1,2,3)$ a $(1,3,2)$ zobrazí na $[0]_4$.

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3. V grupě $\mathbb{Z}_4$ má neutrální prvek $[0]_4$ řád 1, prvek $[2]_4$ řád 2, prvky $[1]_4$ a $[3]_4$ řád 4. Protože v $\mathbb{Z}_4$ není prvek řádu 3, v každém homomorfismu $f : \mathbb{S}_3 \to \mathbb{Z}_4$ se každá z permutací $(1,2,3)$ a $(1,3,2)$ zobrazí na $[0]_4$. Permutace $(1,2)$ se může zobrazit jen na prvek řádu 1 nebo 2, tj. na $[0]_4$ nebo $[2]_4$.

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3. V grupě $\mathbb{Z}_4$ má neutrální prvek $[0]_4$ řád 1, prvek $[2]_4$ řád 2, prvky $[1]_4$ a $[3]_4$ řád 4. Protože v $\mathbb{Z}_4$ není prvek řádu 3, v každém homomorfismu $f : \mathbb{S}_3 \to \mathbb{Z}_4$ se každá z permutací $(1,2,3)$ a $(1,3,2)$ zobrazí na $[0]_4$. Permutace $(1,2)$ se může zobrazit jen na prvek řádu 1 nebo 2, tj. na $[0]_4$ nebo $[2]_4$. Protože $(1,2) \circ (1,2,3) = (2,3)$ a $(1,2,3) \circ (1,2) = (1,3)$, platí

$$f((2,3)) = f((1,2)) + f((1,2,3)) = f((1,2)) + [0]_4 = f((1,2)),$$
$$f((1,3)) = f((1,2,3)) + f((1,2)) = [0]_4 + f((1,2)) = f((1,2)).$$

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3. V grupě $\mathbb{Z}_4$ má neutrální prvek $[0]_4$ řád 1, prvek $[2]_4$ řád 2, prvky $[1]_4$ a $[3]_4$ řád 4. Protože v $\mathbb{Z}_4$ není prvek řádu 3, v každém homomorfismu $f : \mathbb{S}_3 \to \mathbb{Z}_4$ se každá z permutací $(1,2,3)$ a $(1,3,2)$ zobrazí na $[0]_4$. Permutace $(1,2)$ se může zobrazit jen na prvek řádu 1 nebo 2, tj. na $[0]_4$ nebo $[2]_4$. Protože $(1,2) \circ (1,2,3) = (2,3)$ a $(1,2,3) \circ (1,2) = (1,3)$, platí

$$f((2,3)) = f((1,2)) + f((1,2,3)) = f((1,2)) + [0]_4 = f((1,2)),$$
$$f((1,3)) = f((1,2,3)) + f((1,2)) = [0]_4 + f((1,2)) = f((1,2)).$$

Máme tedy dvě možnosti, jak definovat f: v prvním případě se každý prvek grupy $\mathbb{S}_3$ zobrazí na $[0]_4$, zřejmě to je homomorfismus a jeho jádro je $\mathbb{S}_3$.

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3. V grupě $\mathbb{Z}_4$ má neutrální prvek $[0]_4$ řád 1, prvek $[2]_4$ řád 2, prvky $[1]_4$ a $[3]_4$ řád 4. Protože v $\mathbb{Z}_4$ není prvek řádu 3, v každém homomorfismu $f : \mathbb{S}_3 \to \mathbb{Z}_4$ se každá z permutací $(1,2,3)$ a $(1,3,2)$ zobrazí na $[0]_4$. Permutace $(1,2)$ se může zobrazit jen na prvek řádu 1 nebo 2, tj. na $[0]_4$ nebo $[2]_4$. Protože $(1,2) \circ (1,2,3) = (2,3)$ a $(1,2,3) \circ (1,2) = (1,3)$, platí

$$f((2,3)) = f((1,2)) + f((1,2,3)) = f((1,2)) + [0]_4 = f((1,2)),$$
$$f((1,3)) = f((1,2,3)) + f((1,2)) = [0]_4 + f((1,2)) = f((1,2)).$$

Máme tedy dvě možnosti, jak definovat f: v prvním případě se každý prvek grupy $\mathbb{S}_3$ zobrazí na $[0]_4$, zřejmě to je homomorfismus a jeho jádro je $\mathbb{S}_3$. Ve druhém případě se každá transpozice zobrazí na $[2]_4$ a ostatní prvky na $[0]_4$.

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3. V grupě $\mathbb{Z}_4$ má neutrální prvek $[0]_4$ řád 1, prvek $[2]_4$ řád 2, prvky $[1]_4$ a $[3]_4$ řád 4. Protože v $\mathbb{Z}_4$ není prvek řádu 3, v každém homomorfismu $f : \mathbb{S}_3 \to \mathbb{Z}_4$ se každá z permutací $(1,2,3)$ a $(1,3,2)$ zobrazí na $[0]_4$. Permutace $(1,2)$ se může zobrazit jen na prvek řádu 1 nebo 2, tj. na $[0]_4$ nebo $[2]_4$. Protože $(1,2) \circ (1,2,3) = (2,3)$ a $(1,2,3) \circ (1,2) = (1,3)$, platí

$$f((2,3)) = f((1,2)) + f((1,2,3)) = f((1,2)) + [0]_4 = f((1,2)),$$
$$f((1,3)) = f((1,2,3)) + f((1,2)) = [0]_4 + f((1,2)) = f((1,2)).$$

Máme tedy dvě možnosti, jak definovat f: v prvním případě se každý prvek grupy $\mathbb{S}_3$ zobrazí na $[0]_4$, zřejmě to je homomorfismus a jeho jádro je $\mathbb{S}_3$. Ve druhém případě se každá transpozice zobrazí na $[2]_4$ a ostatní prvky na $[0]_4$. Protože liché permutace jsou zobrazeny na $[2]_4$ a sudé permutace na $[0]_4$, jde také o homomorfismus, jeho jádro je množina $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

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 $f : G_1 \to G_2$.

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.

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

- $G_1 \cong G_1$,

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

- $G_1 \cong G_1$,
- $G_1 \cong G_2 \quad \Longrightarrow \quad G_2 \cong G_1$,

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

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

[Identita na množině G_1 je izomorfismus. Inverzní zobrazení k izomorfismu je izomorfismus.

Složení dvou izomorfismů je izomorfismus.]

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

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

[Identita na množině G_1 je izomorfismus. Inverzní zobrazení k izomorfismu je izomorfismus.

Složení dvou izomorfismů je izomorfismus.]

Věta. Libovolná nekonečná cyklická grupa je izomorfní s grupou $(\mathbb{Z}, +)$.

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*

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

[Identita na množině G_1 je izomorfismus. Inverzní zobrazení k izomorfismu je izomorfismus.

Složení dvou izomorfismů je izomorfismus.]

Věta. *Libovolná nekonečná cyklická grupa je izomorfní s grupou $(\mathbb{Z}, +)$. Libovolná konečná cyklická grupa řádu n je izomorfní s grupou $(\mathbb{Z}_n, +)$.* [Věta 6.6, str. 34]

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy.*

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy. Definujme na kartézském součinu* $G_1 \times G_2$ *novou operaci* $\cdot$ *po složkách, tj. definujeme* $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$ *pro libovolné* $g_1, h_1 \in G_1$ *a* $g_2, h_2 \in G_2$.

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy. Definujme na kartézském součinu* $G_1 \times G_2$ *novou operaci* $\cdot$ *po složkách, tj. definujeme* $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$ *pro libovolné* $g_1, h_1 \in G_1$ *a* $g_2, h_2 \in G_2$. *Pak* $(G_1 \times G_2, \cdot)$ *je grupa.*

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy. Definujme na kartézském součinu* $G_1 \times G_2$ *novou operaci* $\cdot$ *po složkách, tj. definujeme* $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$ *pro libovolné* $g_1, h_1 \in G_1$ *a* $g_2, h_2 \in G_2$. *Pak* $(G_1 \times G_2, \cdot)$ *je grupa.* [Věta 6.7, str. 35]

Definice. Výše popsaná grupa $(G_1 \times G_2, \cdot)$ se nazývá **součin grup** $(G_1, \cdot)$ a $(G_2, \cdot)$,

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy. Definujme na kartézském součinu* $G_1 \times G_2$ *novou operaci* $\cdot$ *po složkách, tj. definujeme* $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$ *pro libovolné* $g_1, h_1 \in G_1$ *a* $g_2, h_2 \in G_2$. *Pak* $(G_1 \times G_2, \cdot)$ *je grupa.* [Věta 6.7, str. 35]

Definice. Výše popsaná grupa $(G_1 \times G_2, \cdot)$ se nazývá **součin grup** $(G_1, \cdot)$ a $(G_2, \cdot)$, zapisujeme $(G_1 \times G_2, \cdot) = (G_1, \cdot) \times (G_2, \cdot)$

Příklad. Při důkazu druhé věty o Eulerově funkci jsme pro libovolná nesoudělná $a, b \in \mathbb{N}$ sestrojili zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$ a ukázali, že f je bijekce.

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy. Definujme na kartézském součinu* $G_1 \times G_2$ *novou operaci* $\cdot$ *po složkách, tj. definujeme* $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$ *pro libovolné* $g_1, h_1 \in G_1$ *a* $g_2, h_2 \in G_2$. *Pak* $(G_1 \times G_2, \cdot)$ *je grupa.* [Věta 6.7, str. 35]

Definice. Výše popsaná grupa $(G_1 \times G_2, \cdot)$ se nazývá **součin grup** $(G_1, \cdot)$ a $(G_2, \cdot)$, zapisujeme $(G_1 \times G_2, \cdot) = (G_1, \cdot) \times (G_2, \cdot)$

Příklad. Při důkazu druhé věty o Eulerově funkci jsme pro libovolná nesoudělná $a, b \in \mathbb{N}$ sestrojili zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$ a ukázali, že f je bijekce. Pro každá $c, d \in \mathbb{Z}$ platí

$$\begin{aligned} f([c]_{ab} + [d]_{ab}) &= f([c+d]_{ab}) = ([c+d]_a, [c+d]_b) = \\ &= ([c]_a + [d]_a, [c]_b + [d]_b) = ([c]_a, [c]_b) + ([d]_a, [d]_b) = \\ &= f([c]_{ab}) + f([d]_{ab}), \end{aligned}$$

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy. Definujme na kartézském součinu* $G_1 \times G_2$ *novou operaci* $\cdot$ *po složkách, tj. definujeme* $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$ *pro libovolné* $g_1, h_1 \in G_1$ *a* $g_2, h_2 \in G_2$. *Pak* $(G_1 \times G_2, \cdot)$ *je grupa.* [Věta 6.7, str. 35]

Definice. Výše popsaná grupa $(G_1 \times G_2, \cdot)$ se nazývá **součin grup** $(G_1, \cdot)$ a $(G_2, \cdot)$, zapisujeme $(G_1 \times G_2, \cdot) = (G_1, \cdot) \times (G_2, \cdot)$

Příklad. Při důkazu druhé věty o Eulerově funkci jsme pro libovolná nesoudělná $a, b \in \mathbb{N}$ sestrojili zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$ a ukázali, že f je bijekce. Pro každá $c, d \in \mathbb{Z}$ platí

$$\begin{aligned} f([c]_{ab} + [d]_{ab}) &= f([c+d]_{ab}) = ([c+d]_a, [c+d]_b) = \\ &= ([c]_a + [d]_a, [c]_b + [d]_b) = ([c]_a, [c]_b) + ([d]_a, [d]_b) = \\ &= f([c]_{ab}) + f([d]_{ab}), \end{aligned}$$

a tedy f je izomorfismus grup.

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy. Definujme na kartézském součinu* $G_1 \times G_2$ *novou operaci* $\cdot$ *po složkách, tj. definujeme* $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$ *pro libovolné* $g_1, h_1 \in G_1$ *a* $g_2, h_2 \in G_2$. *Pak* $(G_1 \times G_2, \cdot)$ *je grupa.* [Věta 6.7, str. 35]

Definice. Výše popsaná grupa $(G_1 \times G_2, \cdot)$ se nazývá **součin grup** $(G_1, \cdot)$ a $(G_2, \cdot)$, zapisujeme $(G_1 \times G_2, \cdot) = (G_1, \cdot) \times (G_2, \cdot)$

Příklad. Při důkazu druhé věty o Eulerově funkci jsme pro libovolná nesoudělná $a, b \in \mathbb{N}$ sestrojili zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$ a ukázali, že f je bijekce. Pro každá $c, d \in \mathbb{Z}$ platí

$$\begin{aligned} f([c]_{ab} + [d]_{ab}) &= f([c+d]_{ab}) = ([c+d]_a, [c+d]_b) = \\ &= ([c]_a + [d]_a, [c]_b + [d]_b) = ([c]_a, [c]_b) + ([d]_a, [d]_b) = \\ &= f([c]_{ab}) + f([d]_{ab}), \end{aligned}$$

a tedy f je izomorfismus grup. Platí tedy:

Věta. *Jsou-li* $a, b \in \mathbb{N}$ *nesoudělná přirozená čísla, pak* $(\mathbb{Z}_{ab}, +) \cong (\mathbb{Z}_a, +) \times (\mathbb{Z}_b, +)$.

Projekce ze součinu

Definice. Zobrazení

$$p_1 : G_1 \times G_2 \to G_1 \qquad \text{a} \qquad p_2 : G_1 \times G_2 \to G_2$$

určená předpisy

$$p_1((a, b)) = a, \qquad p_2((a, b)) = b$$

pro libovolné $(a, b) \in G_1 \times G_2$ se nazývají **projekce** (ze součinu).

Projekce ze součinu

Definice. Zobrazení

$$p_1 : G_1 \times G_2 \to G_1 \qquad \text{a} \qquad p_2 : G_1 \times G_2 \to G_2$$

určená předpisy

$$p_1((a,b)) = a, \qquad p_2((a,b)) = b$$

pro libovolné $(a,b) \in G_1 \times G_2$ se nazývají **projekce** (ze součinu).

Věta. *Nechť* $(G_1 \times G_2, \cdot)$ *je součin grup* $(G_1, \cdot)$ *a* $(G_2, \cdot)$.

Projekce ze součinu

Definice. Zobrazení

$$p_1 : G_1 \times G_2 \to G_1 \qquad \text{a} \qquad p_2 : G_1 \times G_2 \to G_2$$

určená předpisy

$$p_1((a,b)) = a, \qquad p_2((a,b)) = b$$

pro libovolné $(a,b) \in G_1 \times G_2$ se nazývají **projekce** (ze součinu).

Věta. *Nechť $(G_1 \times G_2, \cdot)$ je součin grup $(G_1, \cdot)$ a $(G_2, \cdot)$. Pak obě projekce p_1 a p_2 jsou surjektivní homomorfismy grup.* [Věta 8.12, str. 43]

Projekce ze součinu

Definice. Zobrazení

$$p_1 : G_1 \times G_2 \to G_1 \qquad \text{a} \qquad p_2 : G_1 \times G_2 \to G_2$$

určená předpisy

$$p_1((a,b)) = a, \qquad p_2((a,b)) = b$$

pro libovolné $(a,b) \in G_1 \times G_2$ se nazývají **projekce** (ze součinu).

Věta. *Nechť $(G_1 \times G_2, \cdot)$ je součin grup $(G_1, \cdot)$ a $(G_2, \cdot)$. Pak obě projekce p_1 a p_2 jsou surjektivní homomorfismy grup.* [Věta 8.12, str. 43]

Věta. *Jestliže $(G_1, \cdot)$ a $(G_2, \cdot)$ jsou komutativní grupy, pak jejich součin $(G_1 \times G_2, \cdot)$ je komutativní grupa.*

Projekce ze součinu

Definice. Zobrazení

$$p_1 : G_1 \times G_2 \to G_1 \qquad \text{a} \qquad p_2 : G_1 \times G_2 \to G_2$$

určená předpisy

$$p_1((a,b)) = a, \qquad p_2((a,b)) = b$$

pro libovolné $(a,b) \in G_1 \times G_2$ se nazývají **projekce** (ze součinu).

Věta. *Nechť $(G_1 \times G_2, \cdot)$ je součin grup $(G_1, \cdot)$ a $(G_2, \cdot)$. Pak obě projekce p_1 a p_2 jsou surjektivní homomorfismy grup.* [Věta 8.12, str. 43]

Věta. *Jestliže $(G_1, \cdot)$ a $(G_2, \cdot)$ jsou komutativní grupy, pak jejich součin $(G_1 \times G_2, \cdot)$ je komutativní grupa.*

Poznámka. Podobně jako součin dvou grup můžeme definovat součin více grup.

Projekce ze součinu

Definice. Zobrazení

$$p_1 : G_1 \times G_2 \to G_1 \qquad \text{a} \qquad p_2 : G_1 \times G_2 \to G_2$$

určená předpisy

$$p_1((a,b)) = a, \qquad p_2((a,b)) = b$$

pro libovolné $(a,b) \in G_1 \times G_2$ se nazývají **projekce** (ze součinu).

Věta. *Nechť $(G_1 \times G_2, \cdot)$ je součin grup $(G_1, \cdot)$ a $(G_2, \cdot)$. Pak obě projekce p_1 a p_2 jsou surjektivní homomorfismy grup.* [Věta 8.12, str. 43]

Věta. *Jestliže $(G_1, \cdot)$ a $(G_2, \cdot)$ jsou komutativní grupy, pak jejich součin $(G_1 \times G_2, \cdot)$ je komutativní grupa.*

Poznámka. Podobně jako součin dvou grup můžeme definovat součin více grup. Opět na kartézském součinu nosných množin definujeme operaci po složkách.

První věta o struktuře konečných komutativních grup

Následující užitečnou větu uvedeme bez důkazu:

Věta. *Nechť* $(G, \cdot)$ *je konečná komutativní grupa,* $|G| > 1$. *Pak existuje* $s \in \mathbb{N}$ *a přirozená čísla* $d_1 \geq d_2 \geq \cdots \geq d_s > 1$ *splňující*

$$d_2 | d_1, \quad d_3 | d_2, \quad \ldots, \quad d_s | d_{s-1}$$

tak, že

$$(G, \cdot) \cong (\mathbb{Z}_{d_1}, +) \times \cdots \times (\mathbb{Z}_{d_s}, +).$$

První věta o struktuře konečných komutativních grup

Následující užitečnou větu uvedeme bez důkazu:

Věta. Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existuje $s \in \mathbb{N}$ a přirozená čísla $d_1 \geq d_2 \geq \cdots \geq d_s > 1$ splňující

$$d_2 | d_1, \quad d_3 | d_2, \quad \ldots, \quad d_s | d_{s-1}$$

tak, že

$$(G, \cdot) \cong (\mathbb{Z}_{d_1}, +) \times \cdots \times (\mathbb{Z}_{d_s}, +).$$

Tento rozklad grupy G na součin cyklických grup splňujících uvedené podmínky je určen jednoznačně.

První věta o struktuře konečných komutativních grup

Následující užitečnou větu uvedeme bez důkazu:

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existuje $s \in \mathbb{N}$ a přirozená čísla $d_1 \geq d_2 \geq \cdots \geq d_s > 1$ splňující*

$$d_2 | d_1, \quad d_3 | d_2, \quad \ldots, \quad d_s | d_{s-1}$$

tak, že

$$(G, \cdot) \cong (\mathbb{Z}_{d_1}, +) \times \cdots \times (\mathbb{Z}_{d_s}, +).$$

Tento rozklad grupy G na součin cyklických grup splňujících uvedené podmínky je určen jednoznačně. Navíc platí, že d_1 je exponent grupy G a že $|G| = d_1 \cdots d_s$.

První věta o struktuře konečných komutativních grup

Následující užitečnou větu uvedeme bez důkazu:

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existuje $s \in \mathbb{N}$ a přirozená čísla $d_1 \geq d_2 \geq \cdots \geq d_s > 1$ splňující*

$$d_2 | d_1, \quad d_3 | d_2, \quad \ldots, \quad d_s | d_{s-1}$$

tak, že

$$(G, \cdot) \cong (\mathbb{Z}_{d_1}, +) \times \cdots \times (\mathbb{Z}_{d_s}, +).$$

Tento rozklad grupy G na součin cyklických grup splňujících uvedené podmínky je určen jednoznačně. Navíc platí, že d_1 je exponent grupy G a že $|G| = d_1 \cdots d_s$.

Důsledek. *Má-li konečná komutativní grupa řád, který není dělitelný druhou mocninou žádného prvočísla, pak je cyklická.*

První věta o struktuře konečných komutativních grup

Následující užitečnou větu uvedeme bez důkazu:

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existuje $s \in \mathbb{N}$ a přirozená čísla $d_1 \geq d_2 \geq \cdots \geq d_s > 1$ splňující*

$$d_2 | d_1, \quad d_3 | d_2, \quad \ldots, \quad d_s | d_{s-1}$$

tak, že

$$(G, \cdot) \cong (\mathbb{Z}_{d_1}, +) \times \cdots \times (\mathbb{Z}_{d_s}, +).$$

Tento rozklad grupy G na součin cyklických grup splňujících uvedené podmínky je určen jednoznačně. Navíc platí, že d_1 je exponent grupy G a že $|G| = d_1 \cdots d_s$.

Důsledek. *Má-li konečná komutativní grupa řád, který není dělitelný druhou mocninou žádného prvočísla, pak je cyklická.*

Příklad. Komutativní grupy $(\mathbb{Z}_9^\times, \cdot)$ i $(\mathbb{Z}_7^\times, \cdot)$ mají obě $\varphi(9) = \varphi(7) = 6$ prvků, a tedy jsou cyklické.

První věta o struktuře konečných komutativních grup

Následující užitečnou větu uvedeme bez důkazu:

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existuje $s \in \mathbb{N}$ a přirozená čísla $d_1 \geq d_2 \geq \cdots \geq d_s > 1$ splňující*

$$d_2 | d_1, \quad d_3 | d_2, \quad \ldots, \quad d_s | d_{s-1}$$

tak, že

$$(G, \cdot) \cong (\mathbb{Z}_{d_1}, +) \times \cdots \times (\mathbb{Z}_{d_s}, +).$$

Tento rozklad grupy G na součin cyklických grup splňujících uvedené podmínky je určen jednoznačně. Navíc platí, že d_1 je exponent grupy G a že $|G| = d_1 \cdots d_s$.

Důsledek. *Má-li konečná komutativní grupa řád, který není dělitelný druhou mocninou žádného prvočísla, pak je cyklická.*

Příklad. Komutativní grupy $(\mathbb{Z}_9^\times, \cdot)$ i $(\mathbb{Z}_7^\times, \cdot)$ mají obě $\varphi(9) = \varphi(7) = 6$ prvků, a tedy jsou cyklické. To lze snadno ověřit nalezením generátoru: $\mathbb{Z}_9^\times = \langle [2]_9 \rangle$, $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$.

První věta o struktuře konečných komutativních grup

Následující užitečnou větu uvedeme bez důkazu:

Věta. *Nechť $(G,\cdot)$ je konečná komutativní grupa, $|G|>1$. Pak existuje $s\in\mathbb{N}$ a přirozená čísla $d_1\geq d_2\geq\cdots\geq d_s>1$ splňující*

$$d_2|d_1,\quad d_3|d_2,\quad \ldots,\quad d_s|d_{s-1}$$

tak, že

$$(G,\cdot)\cong(\mathbb{Z}_{d_1},+)\times\cdots\times(\mathbb{Z}_{d_s},+).$$

Tento rozklad grupy G na součin cyklických grup splňujících uvedené podmínky je určen jednoznačně. Navíc platí, že d_1 je exponent grupy G a že $|G|=d_1\cdots d_s$.

Důsledek. *Má-li konečná komutativní grupa řád, který není dělitelný druhou mocninou žádného prvočísla, pak je cyklická.*

Příklad. Komutativní grupy $(\mathbb{Z}_9^\times,\cdot)$ i $(\mathbb{Z}_7^\times,\cdot)$ mají obě $\varphi(9)=\varphi(7)=6$ prvků, a tedy jsou cyklické. To lze snadno ověřit nalezením generátoru: $\mathbb{Z}_9^\times=\langle[2]_9\rangle$, $\mathbb{Z}_7^\times=\langle[3]_7\rangle$.

Poznámka. Předchozí věta i její důsledek platí jen pro komutativní grupy, například grupa $\mathbb{S}_3$ má také 6 prvků, ale není cyklická.

Druhá věta o struktuře konečných komutativních grup

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že*

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Druhá věta o struktuře konečných komutativních grup

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že*

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických grup, jejichž řád je mocnina prvočísla, je určen jednoznačně až na pořadí činitelů.

Druhá věta o struktuře konečných komutativních grup

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že*

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických grup, jejichž řád je mocnina prvočísla, je určen jednoznačně až na pořadí činitelů. Zřejmě platí $|G| = p_1^{k_1} \cdots p_s^{k_s}$.

Druhá věta o struktuře konečných komutativních grup

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že*

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických grup, jejichž řád je mocnina prvočísla, je určen jednoznačně až na pořadí činitelů. Zřejmě platí $|G| = p_1^{k_1} \cdots p_s^{k_s}$. [Věta 10.13, str. 52]

Příklad. Užijme tuto druhou větu k tomu, abychom zjistili, jak mohou vypadat komutativní grupy řádu 8.

Druhá věta o struktuře konečných komutativních grup

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že*

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických grup, jejichž řád je mocnina prvočísla, je určen jednoznačně až na pořadí činitelů. Zřejmě platí $|G| = p_1^{k_1} \cdots p_s^{k_s}$. *[Věta 10.13, str. 52]*

Příklad. Užijme tuto druhou větu k tomu, abychom zjistili, jak mohou vypadat komutativní grupy řádu 8. Podle ní jde o to, jakými způsoby je možné napsat 8 jako součin mocnin prvočísel: $8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2$,

Druhá věta o struktuře konečných komutativních grup

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že*

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických grup, jejichž řád je mocnina prvočísla, je určen jednoznačně až na pořadí činitelů. Zřejmě platí $|G| = p_1^{k_1} \cdots p_s^{k_s}$. *[Věta 10.13, str. 52]*

Příklad. Užijme tuto druhou větu k tomu, abychom zjistili, jak mohou vypadat komutativní grupy řádu 8. Podle ní jde o to, jakými způsoby je možné napsat 8 jako součin mocnin prvočísel: $8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2$, proto každá komutativní grupa řádu 8 je izomorfní s právě jednou z grup $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Druhá věta o struktuře konečných komutativních grup

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že*

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických grup, jejichž řád je mocnina prvočísla, je určen jednoznačně až na pořadí činitelů. Zřejmě platí $|G| = p_1^{k_1} \cdots p_s^{k_s}$. [Věta 10.13, str. 52]

Příklad. Užijme tuto druhou větu k tomu, abychom zjistili, jak mohou vypadat komutativní grupy řádu 8. Podle ní jde o to, jakými způsoby je možné napsat 8 jako součin mocnin prvočísel: $8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2$, proto každá komutativní grupa řádu 8 je izomorfní s právě jednou z grup $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Ke stejnému výsledku bychom se snadno dostali i pomocí první věty.

Druhá věta o struktuře konečných komutativních grup

Věta. *Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že*

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických grup, jejichž řád je mocnina prvočísla, je určen jednoznačně až na pořadí činitelů. Zřejmě platí $|G| = p_1^{k_1} \cdots p_s^{k_s}$. [Věta 10.13, str. 52]

Příklad. Užijme tuto druhou větu k tomu, abychom zjistili, jak mohou vypadat komutativní grupy řádu 8. Podle ní jde o to, jakými způsoby je možné napsat 8 jako součin mocnin prvočísel: $8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2$, proto každá komutativní grupa řádu 8 je izomorfní s právě jednou z grup $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Ke stejnému výsledku bychom se snadno dostali i pomocí první věty. Zdůrazněme, že tento výčet se týká jen komutativních grup, existují i nekomutativní grupy řádu 8, například grupa symetrií čtverce $\mathbb{D}_4$.