$*: A \times A \longrightarrow A$ binární operace

$(a * b) * c = a * (b * c)$ asociativita

$a * b = b * a$ komutativita

$e * a = a * e = a$ neutrální prvek

# GRUPY

$(A, *, e)$ monoid

$a \in A$

Když existuje $b \in A$ takové, že $a * b = b * a = e$, pak $a$ se nazývá INVERTIBILNÍ. $b$ je INVERZNÍ PRVEK k $a$.

Monoid, jehož každý prvek je invertibilní, se nazývá GRUPA.

$(\mathbb{R} \setminus \{0\}, \cdot, 1, ^{-1})$ je grupa.

$(\mathbb{R}, +, 0, -)$

**Tvrzení** $(A, *, e)$ monoid, $a \in A$ invertibilní prvek. Pak existuje k $a$ právě jeden prvek inverzní.

**Důkaz** $a$ je invertibilní $\Rightarrow$ existuje inverze.

Předp., že $b_1, b_2 \in A$ jsou inverzní k $a$.

$$a * b_1 = b_1 * a = e = a * b_2 = b_2 * a.$$

$$b_1 = b_1 * e = b_1 * (a * b_2) =$$

$$= (b_1 * a) * b_2 = e * b_2 = b_2.$$

**Tvrdení** $(G, *, e, ^{-1})$ grupa.
Pak pro lib. $a, b \in G$ platí:

1) Když $a * b = e$, pak $b = a^{-1}$, $a = b^{-1}$.
2) $e^{-1} = e$
3) $(a^{-1})^{-1} = a$
4) $(a*b)^{-1} = b^{-1} * a^{-1}$.

**Důkaz** 1) $b = e * b = (a^{-1} * a) * b =$

$= a^{-1} * (a * b) = a^{-1} * e = a^{-1}$.

$a = b^{-1}$ ... DÚ.

2) $e * e = e \Rightarrow e^{-1} = e$.

3) $a * a^{-1} = e \Rightarrow (a^{-1})^{-1} = a$.

4) $a * \underbrace{b * b^{-1}}_{e} * a^{-1} = e$

$(a*b) * (b^{-1} * a^{-1}) = e$

$\Rightarrow (a*b)^{-1} = b^{-1} * a^{-1}$

$(b^{-1} * a^{-1})^{-1} = a * b$.

## PODGRUPY

$(G, *, e, ^{-1})$ grupa. $H \subseteq G$.

1) $a, b \in H \Rightarrow a * b \in H$
2) $e \in H$.
3) $a \in H \Rightarrow a^{-1} \in H$.

Pak $H$ se nazývá PODGRUPA grupy $G$.

---

$(\mathbb{Z}, +, 0, -)$ grupa.

$2\mathbb{Z}$ mn. sudých celých čísel.

$2\mathbb{Z}$ je podgrupa.

---

$G$ je grupa. $G$ je podgrupa $G$.

$H = \{e\} \Rightarrow e * e = e \in H$

$e^{-1} = e \in H$

$\{e\}$ je podgrupa $G$.

---

## Podgrupy grupy $(\mathbb{Z}, +, 0, -)$

$$m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, 2m, \dots\}$$

**Tvrzení:** Podmnožiny $m\mathbb{Z} \subseteq \mathbb{Z}$ jsou podgrupy grupy $(\mathbb{Z}, +, 0, -)$ a jiné podgrupy v ní nejsou.

**Důkaz** $m \in \mathbb{N}$, $m\mathbb{Z}$.

$mk_1 + mk_2 = m(k_1 + k_2) \in m\mathbb{Z}$

$0 \in m\mathbb{Z}$

$mk \in m\mathbb{Z}$, $-mk = m \cdot (-k) \in m\mathbb{Z}$

$H \subseteq \mathbb{Z}$ je podgrupa.

$\Rightarrow 0 \in H$

1) $H = \{0\} = 0 \cdot \mathbb{Z}$ ✓

2) $H \neq \{0\}$

$0 \neq h \in H$, předp., že $h > 0$.

a navíc předp. že $h$ je nejmenší kladné číslo v $H$.

$h \in H$, $h + h = 2h \in H$

$k \cdot h = (k-1) \cdot h + h \in H$

$h \cdot \mathbb{Z} \subseteq H$

$a \in H$

$a = k \cdot h + r$, $0 \leq r < h$.

$a, k \cdot h \in H$

$r = a + (-k) \cdot h \in H$

$\Rightarrow r = 0$.

$\Rightarrow a = k \cdot h \Rightarrow a \in h \cdot \mathbb{Z}$.

$\Rightarrow H \subseteq h\mathbb{Z}$

$\Rightarrow H = h\mathbb{Z}$.

# HOMOMORFISMY

$(A,*), (B,+)$ pologrupy.

$f: A \to B$.

Když $\forall a_1, a_2 \in A$ platí

$$f(a_1 * a_2) = f(a_1) + f(a_2),$$

pak $f$ je HOMOMORFISMUS pologrup $(A,*), (B,+)$.

---

$(A,*,e_A), (B,+,e_B)$ monoidy.

$f: A \to B$ homomorfismus pologrup $(A,*), (B,+)$ takový, že $f(e_A) = e_B$,

pak $f$ je HOMOMORFISMUS monoidů $(A,*,e_A), (B,+,e_B)$.

---

$(A,*,e_A,^{-1}), (B,+,e_B,^{-1})$ grupy.

$f: A \to B$ je homomorfismus monoidů $(A,*,e_A), (B,+,e_B)$ takový, že

$\forall a \in A$ $$f(a^{-1}) = (f(a))^{-1}.$$

Pak $f$ je HOMOMORFISMUS grup $(A,*,e_A,^{-1}), (B,+,e_B,^{-1})$.

Příklad

$(2\mathbb{Z}, +, 0, -)$, $2\mathbb{Z}$

$f: k \mapsto 2k$

$f(k_1 + k_2) = 2(k_1 + k_2) = 2k_1 + 2k_2 =$

$= f(k_1) + f(k_2)$

$f(0) = 2 \cdot 0 = 0$

$f(-k) = 2 \cdot (-k) = -2 \cdot k = -f(k)$

---

Tvrzení Budže $f: A \to B$, $g: B \to C$ homomorfismy pologrup (monoidů, grup). Pak jejich složení $g \circ f: A \to C$ je homomorfismus pologrup (monoidů, grup)

---

Důkaz $(A, *), (B, +), (C, \times)$

$f: A \to B$, $g: B \to C$. $a_1, a_2 \in A$. $b_1, b_2 \in B$.

$f(a_1 * a_2) = f(a_1) + f(a_2)$

$g(b_1 + b_2) = g(b_1) \times g(b_2)$

$(g \circ f)(a_1 * a_2) = g(f(a_1 * a_2)) =$

$= g(f(a_1) + f(a_2)) = g(f(a_1)) \times g(f(a_2$

$= (g \circ f)(a_1) \times (g \circ f)(a_2)$ ✓

Zbytek DÚ.