# Grupy, podgrupy, homomorfizmy

17. februára 2025

# Definícia grupy

## Definícia

Dvojicu $(G, *)$, kde $G$ je množina a $*$ je binárna operácia na $G$ nazývame *grupa*, ak

*(i)* operácia $*$ je asociatívna

$$(\forall g, h, k \in G) g * (h * k) = (g * h) * k,$$

*(ii)* operácia $*$ má neutrálny prvok

$$(\exists e \in G)(\forall g \in G) e * g = g * e = g,$$

*(iii)* pre každý prvok $g \in G$ existuje inverzný prvok vzhľadom na operáciu $*$

$$(\forall g \in G)(\exists g^{-1} \in G) g * g^{-1} = g^{-1} * g = e.$$

# Definícia grupy

$$(\forall g, h, k \in G) g * (h * k) = (g * h) * k$$
$$(\exists e \in G)(\forall g \in G) e * g = g * e = g$$
$$(\forall g \in G)(\exists g^{-1} \in G) g * g^{-1} = g^{-1} * g = e$$

Ak je binárna operácia $*$ komutatívna

$$(\forall g, h \in G) g * h = h * g,$$

hovoríme o *komutatívnej grupe.*

# Zákony o krátení

$$
\begin{aligned}
g * h_1 = g * h_2 \qquad &\Rightarrow h_1 = h_2 \\
h_1 * g = h_2 * g \qquad &\Rightarrow h_1 = h_2
\end{aligned}
$$

# Inverzný prvok

$$(g^{-1})^{-1} = g$$
$$(g * h)^{-1} = h^{-1} * g^{-1}$$

# Príklady grúp

- $(V, +)$ kde $V$ je ľubovoľný vektorový priestor,
- $(F, +)$ a $(F \setminus \{0\}, \cdot)$ pre ľubovoľné pole $(F, +, \cdot)$,
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$,
- $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$,
- $(\mathbb{Z}_n, \oplus)$ pre $n \in \mathbb{N}$, $n \geq 2$,
- $(\mathbb{Z}_p \setminus \{0\}, \odot)$ kde $p$ je prvočíslo.

Príkladom nekomutatívnej grupy je grupa $S_n$ všetkých permutácií $n$-prvkovej množiny s operáciou skladania zobrazení pre $n \geq 3$.

# Priamy súčin grúp

## Príklad

Ak $(G, *_G)$ a $(H, *_H)$ sú grupy, tak aj $G \times H$ s operáciou

$$(a, b) * (a', b') = (a *_G a', b *_H b')$$

je grupa.

## Definícia

Grupu $G \times H$ z predchádzajúceho príkladu nazývame *priamy súčin grúp $G$ a $H$* (alebo tiež *direktný súčin* grúp.)

# Podgrupy

## Definícia

Nech $(G, *)$ je grupa a $H \subseteq G$ je ľubovoľná podmnožina $G$.
Hovoríme, že $H$ je *podgrupa* grupy $G$, ak $H$ s binárnou operáciou $*$ zúženou na podmnožinu $H$ tvorí grupu.
Budeme používať označenie $H \leq G$, prípadne $(H, *) \leq (G, *)$.

Zúženie operácie:

$$h_1 *_H h_2 = h_1 *_G h_2$$

pre ľubovoľné $h_1, h_2 \in H$.

# Podgrupy

## Lema

*Nech $(G, *)$ je grupa a $H$ je jej podgrupa.*

*(i) Ak $e_H$ je neutrálny prvok grupy $H$ a $e_G$ je neutrálny prvok grupy $G$, tak $e_H = e_G$. (Z toho špeciálne vyplýva $e_G \in H$, teda každá podgrupa musí obsahovať neutrálny prvok.)*

*(ii) Ak $a \in H$, $b$ je inverzný prvok k $a$ v $G$ a $c$ je inverzný prvok k $a$ v $H$, tak $b = c$.*

# Kritérium podgrupy

## Veta (Kritérium podgrupy)

*Nech $(G, *)$ je grupa a $H \subseteq G$, $H \neq \emptyset$. Nasledujúce podmienky sú ekvivalentné*

(i) *$H$ je podgrupa grupy $G$;*

(ii) *množina $H$ je uzavretá vzhľadom na operáciu $*$ a na tvorenie inverzných prvkov v $G$, čiže platí (pre ľubovoľné $a, b \in H$)*

$$a, b \in H \ \Rightarrow a * b \in H$$
$$a \in H \Rightarrow a^{-1} \in H$$

(iii) *pre ľubovoľné $a, b \in H$ platí aj $a^{-1} * b \in H$*

# Kritérium podgrupy

## Poznámka

Ak $H$ je konečná množina, tak stačí podmienka

$$a, b \in H \ \Rightarrow a * b \in H.$$

# Príklady podgrúp

- Pre ľubovoľnú grupu $G$ máme $\{e\} \leq G$ a $G \leq G$.
- $S = \{x \in \mathbb{C}; |x| = 1\}$ je podgrupa grupy $(\mathbb{C} \setminus \{0\}, \cdot)$.
- Podmnožiny $\mathbb{R} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$ sú podgrupy grupy $(\mathbb{C} \setminus \{0\}, \cdot)$.
- Podmnožina $\mathbb{R}^+$ je podgrupa grupy $(\mathbb{R} \setminus \{0\}, \cdot)$.

# Podgrupa podgrupy

### Lema

*Nech $(G, *)$ je grupa. Potom*

(i) *Ak $K \subset H \subset G$ a $K$, $H$ sú podgrupy $G$, tak $K$ je podgrupa $H$.*

(ii) *Ak $H$ je podgrupa $G$ a $K$ je podgrupa $H$, tak $K$ je aj podgrupa $G$.*

# Prienik podgrúp

**Tvrdenie**

*Nech $(G, *)$ je grupa a $H_i$ je podgrupa grupy $G$ pre každé $i \in I$. Potom prienik týchto podgrúp*

$$H := \bigcap_{i \in I} H_i$$

*je opäť podgrupa grupy $G$.*

# Podgrupa generovaná danou množinou

## Dôsledok

*Ak $(G, *)$ je grupa a $A \subset G$ je ľubovoľná podmnožina $G$, tak prienik všetkých podgrúp obsahujúcich množinu $A$ je tiež podgrupa $G$. Túto podgrupu nazývame podgrupa generovaná podmnožinou $A$ a označujeme $[A]$. Ak $[A] = G$, hovoríme, že grupa $G$ je generovaná podmnožinou $A$ (alebo tiež, že $A$ generuje $G$). V prípade, že $A = \{a\}$ je jednoprvková množina, tak namiesto $[\{a\}]$ budeme používať označenie $[a]$ a hovoríme o podgrupe generovanej prvkom $a$.*

# Podgrupa generovaná danou množinou

Definíciu podgrupy generovanej množinou $A$ môžeme stručne zapísať ako

$$[A] = \bigcap \{H \subseteq G; H \supseteq A \ \wedge \ H \text{ je podgrupa } G\}.$$

Je to najmenšia (vzhľadom na inklúziu) podgrupa obsahujúca $A$.

# Podgrupa generovaná danou množinou

V grupe $(\mathbb{R}, +)$ platí:

- $[1] = \mathbb{Z}$
- $[-1] = \mathbb{Z}$
- $[2, 3] = \mathbb{Z}$

# Podgrupa generovaná danou množinou

V grupe $\mathbb{Z}_2 \times \mathbb{Z}_3$ platí:

- $[(1,0)] = \mathbb{Z}_2 \times \{0\}$
- $[(0,1)] = \{0\} \times \mathbb{Z}_3$
- $[(1,1)] = \mathbb{Z}_2 \times \mathbb{Z}_3$

# Homomorfizmus

## Definícia

Nech $(G, \circ)$, $(H, *)$ sú grupy. Potom zobrazenie $f\colon G \to H$ je *homomorfizmus*, ak

$$f(g_1 \circ g_2) = f(g_1) * f(g_2)$$

platí pre ľubovoľné $g_1, g_2 \in G$.

Iné označenie: $f\colon (G, \circ) \to (H, *)$

# Homomorfizmus

### Veta

*Nech* $(G, \circ)$, $(H, *)$ *sú grupy a* $f\colon G \to H$ *je homomorfizmus. Označme ďalej* $e_G$ *neutrálny prvok grupy* $G$ *a* $e_H$ *neutrálny prvok grupy* $H$. *(Inverzné prvky budeme v oboch prípadoch označovať pomocou horného indexu* $-1$ *ako obvykle.) Potom platí:*

(i) $f(e_G) = e_H$ *(teda homomorfizmus musí zobraziť neutrálny prvok na neutrálny prvok);*

(ii) $f(a^{-1}) = (f(a))^{-1}$ *(teda homomorfizmy zachovávajú aj inverzné prvky).*

# Príklady homomorfizmov

## Príklad

Ak $(G, *)$ a $(H, \circ)$ sú ľubovoľné grupy, tak $f\colon G \to H$ určené predpisom $f(g) = e_H$ pre všetky $g \in G$ je homomorfizmus.

Zobrazenie $id_G\colon G \to G$ je homomorfizmus pre každú grupu $(G, *)$.

# Príklady homomorfizmov

## Príklad

Uvažujme zobrazenie

$$f\colon (\mathbb{R},+) \to (\mathbb{R}^+,\cdot), \qquad f\colon x \mapsto e^x.$$

Priamo z vlastností exponenciálnej funkcie vyplýva, že $f$ je homomorfizmus

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x)\cdot f(y)$$

# Príklady homomorfizmov

$$g\colon (\mathbb{R}, +) \to (S, \cdot)$$
$$g\colon \varphi \mapsto e^{i\varphi} = \cos\varphi + i\sin\varphi$$

$$g(\varphi_1 + \varphi_2) = (\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)) =$$
$$= (\cos\varphi_1 + i\sin\varphi_1)\cdot(\cos\varphi_2 + i\sin\varphi_2) = g(\varphi_1)\cdot g(\varphi_2)$$

# Príklady homomorfizmov

## Príklad

Nech $n \in \mathbb{N}$, $n \geq 2$. Zobrazenie $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}_n, \oplus)$ dané predpisom

$$f(k) = k \bmod n$$

je homomorfizmus.

# Obraz a vzor podgrupy

$$f[A] = \{f(a); a \in A\}$$
$$f^{-1}[B] = \{a \in A; f(a) \in B\}$$

## Tvrdenie

*Nech $(G, \circ)$, $(H, *)$ sú grupy a $f\colon G \to H$ je homomorfizmus.*

*(i) Ak $G'$ je podgrupa grupy $G$, tak aj jej obraz $f[G']$ je podgrupa grupy $H$.*

*(ii) Ak $H'$ je podgrupa grupy $H$, tak aj jej vzor $f^{-1}[H']$ je podgrupa grupy $G$.*

# Izomorfizmus

## Definícia

Nech $(G, \circ)$, $(H, *)$ sú grupy. Ak $f\colon G \to H$ je bijektívny homomorfizmus, hovoríme, že $f$ je *izomorfizmus* alebo tiež, že grupy $G$ a $H$ sú izomorfné (označujeme $G \cong H$).

$G \cong H$ znamená, že grupy $G$ a $H$ sú „v podstate rovnaké“.

# Zloženie homomorfizmov

**Lema**

*Nech* $(G, *)$, $(H, \circ)$, $(K, \odot)$ *sú grupy.*

(i) *Ak* $f\colon G \to H$ *je izomorfizmus, tak aj* $f^{-1}\colon H \to G$ *je izomorfizmus.*

(ii) *Ak* $f\colon G \to H$ *a* $g\colon H \to K$ *sú homomorfizmy, tak aj* $g \circ f\colon G \to K$ *je homomorfizmus.*

(iii) *Ak* $f\colon G \to H$ *a* $g\colon H \to K$ *sú izomorfizmy, tak aj* $g \circ f\colon G \to K$ *je izomorfizmus.*