

Podgrupy

Př. $(\mathbb{Z}, +)$ je grupa. Uvažujme množinu $5\mathbb{Z} = \{5k \mid k \in \mathbb{Z}\}$, jejíž prvky budeme počítat stejně jako prvky množiny $\mathbb{Z}$. $\Rightarrow$

1.) $\forall 5k_1, 5k_2 \in 5\mathbb{Z} : 5k_1 + 5k_2 = 5(k_1 + k_2) = 5k \in 5\mathbb{Z}$
 $\in \mathbb{Z}$

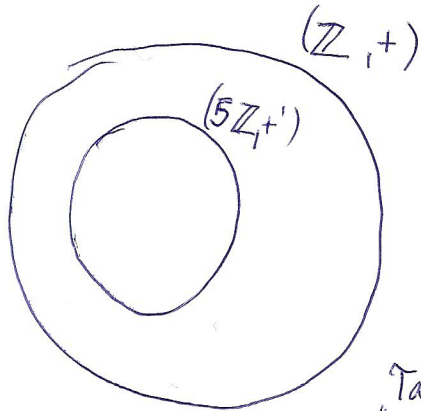
2.) $\forall 5a, 5b, 5c \in 5\mathbb{Z} : 5a + (5b + 5c) = (5a + 5b) + 5c$ protože sčítání celých čísel je asociativní

3.) $0 = 5 \cdot 0 \in 5\mathbb{Z}$ je neutrálním prvkem při sčítání v $5\mathbb{Z}$

4.) $\forall 5k \in 5\mathbb{Z} \exists 5(-k) \in 5\mathbb{Z} : 5k + 5(-k) = 5(-k) + 5k = 0$

Znamená to že inverzním prvkem k $5k \in 5\mathbb{Z}$ je prvek $5(-k) \in 5\mathbb{Z}$, tj. $-(5k) = 5(-k)$ (formální zápis)

$\Rightarrow$



$(5\mathbb{Z}, +')$ splňuje:

1.) $5\mathbb{Z} \subseteq \mathbb{Z}$

2.) $+$ je restrikce operace $+$ na $5\mathbb{Z}$

3.) $(5\mathbb{Z}, +')$ je grupa

"Takovéto" objekty budeme říkat "podgrupa."

Def. (Podgrupa): Necht' $(G, \cdot)$ je grupa. Uspořádanou dvojici $(H, \cdot')$ nazveme podgrupou grupy $(G, \cdot)$ právě když

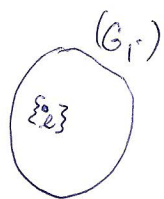
1.) $H \subseteq G$

2.) $\cdot' : H \times H \rightarrow G$, kde $\forall a, b \in H : a \cdot' b = a \cdot b$ ($\cdot'$ je restrikce $\cdot$ na H)

3.) $(H, \cdot')$ je grupa.

Vmluva: Nebudeme rozlišovat značení operací na grupe od operací na její podgrupě. Tam, budeme hovořit o podgrupě $(H, \cdot)$ grupy $(G, \cdot)$.

Pozorování:



1.) "Nejmenší" podgrupa v grupě $(G, \cdot)$ je podgrupa $(\{e\}, \cdot)$, kde e je neutrální prvek v $(G, \cdot)$.

oprávdu: $\{e\} \subseteq G$, "operace se nemění", $(\{e\}, \cdot)$ je grupa:

1.) $e \cdot e = e \in \{e\}$ (uzavřenost)

2.) $\underbrace{e \cdot (e \cdot e)}_e = \underbrace{(e \cdot e)}_e \cdot e$ (asociativita)

4.) $e \cdot e = e \Rightarrow e^{-1} = e$ (existují inverzní prvky)

3.) $e \cdot e = e$ (e je neutrální prvek v $(\{e\}, \cdot)$)

2.) "Největší" podgrupa v grupě $(G, \cdot)$ je grupa $(G, \cdot)$ samotná.

oprávdu:

1.) $\{e\} \subseteq G$

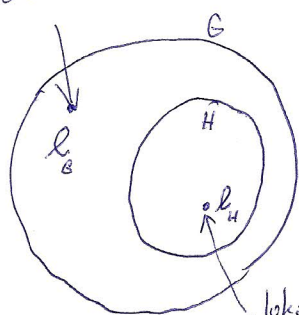
2.) operace se nemění

3.) $(G, \cdot)$ je grupa

Problém:

$(H, \cdot)$ je podgrupa $(G, \cdot)$. $(H, \cdot)$ je tedy sama o sobě grupa $\Rightarrow$ musí obsahovat nějaký neutrální prvek. Je možná situace, že neutrálním prvkem v $(H, \cdot)$ není neutrální prvek v G , ale nějaký jiný prvek $e_H \in H$? Ne, to nemůže nastat!

neutr. prvek
na G



"lokalní" neutr.
prvek
(který není neutr.
prvkem na G , ale na
 H ano)

Věta: Necht' $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$ a e_G je neutrální prvek v $(G, \cdot)$. Pak $e_G \in H$ a je neutrálním prvkem v $(H, \cdot)$

Důkaz: $(H, \cdot)$ je grupa $\Rightarrow H \neq \emptyset \Rightarrow (\exists h \in H \wedge \exists e_H \in H)$
takže, že $\forall h \in H: e_H h = h e_H = h$

$\Rightarrow \forall h \in H: e_H h = h$

$e_H h = e_G h$ (protože e_G je neutrální prvek v G)

$e_H = e_G$ (využijeme větu o zobrazení v grupě)

□

Problém: Jak poznáme, že $(H, \cdot)$ je podgrupou $(G, \cdot)$?
(a nechtěme ověřovat platnost všech axiomů grupy)

Věta 1: Necht' platí následující podmínky

1.) $H \subseteq G$

2.) a) $H \neq \emptyset$

b) $\forall a, b \in H : ab \in H$

c) $\forall a \in H : a^{-1} \in H$

Potom $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$

Důkaz: Ověříme platnost podmínek a definice podgrupy

1.) $H \subseteq G$

2.) na H „převládá“ restrikce operace na G

3.) Podmínky z bodu 2.) představují všechny podmínky kladené na to, aby $(H, \cdot)$ byla grupa s výjimkou asociativity operace. Ale $(G, \cdot)$ je grupa $\Rightarrow$

$\forall a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c \Rightarrow \forall a, b, c \in H \subseteq G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$
($\leftarrow$ protože do H patří neboť $H \neq \emptyset \Rightarrow \exists a \in H \Rightarrow \exists a^{-1} \in H \Rightarrow aa^{-1} = e \in H$)

Věta 2: Necht' $(G, \cdot)$ je grupa a platí:

1.) $H \subseteq G$

2.) a) $H \neq \emptyset$

b) $\forall a, b \in H : ab^{-1} \in H$

Potom $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$.

Důkaz: 1.) $H \subseteq G$ 2.) operace na H je restrikce operace na G .

3.) Dokažeme, že $(H, \cdot)$ je grupa: a) $H \neq \emptyset$ (zřejmě)

b) $H \neq \emptyset \Rightarrow \exists a \in H \Rightarrow a \cdot a^{-1} = e \in H$ (kvůli jmu $b=a$) $\Rightarrow \forall H$ je neut. prvek.

js) $\forall a \in H : \exists a^{-1} = \bar{a}^{-1} \in H \Rightarrow \forall H$ mají všechny prvky prvek inverzní

5) $\forall a, b \in H : b^{-1} \in H \Rightarrow a \cdot (b^{-1})^{-1} = a \cdot b \in H \Rightarrow \cdot$ je uzavřená na H

6) $(G, \cdot)$ je grupa $\Rightarrow \cdot$ je asociativní operace $\Rightarrow \cdot$ je restrikce na H je asociativní

Pr: Necht^{abelova} $(G, \cdot)$ je grupa a $H = \{h \in G \mid h^2 = e\}$. Potom $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$.

Důkaz: Podle věty 2 :

1.) $H \subseteq G$

2.) a) $H \neq \emptyset$ protože $e^2 = e \cdot e = e \Rightarrow e \in H$.

b) $\forall a, b \in H$: (chceme dokázat $ab^{-1} \in H$, tedy $(ab^{-1})^2 = e$)

$$\begin{aligned}(a \cdot b^{-1})^2 &= (ab^{-1})(ab^{-1}) = a(b^{-1}a)b^{-1} = a(ab^{-1})b^{-1} = a^2(b^{-1})^2 = a^2(b^{-1})^{-1} \\ &= e(e)^{-1} = e\end{aligned}$$

Tan

$\forall a, b \in H : ab^{-1} \in H$

□

Věta 3: Necht^{abelova} $(G, \cdot)$ je grupa a platí:

1.) $H \subseteq G$

2.) H je konečná množina

3.) a) $H \neq \emptyset$

b) $\forall a, b \in H : a \cdot b \in H$

Potom $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$.

Důkaz: Podle věty 1 stačí dokázat, že $\forall a \in H : a^{-1} \in H$.

$H \neq \emptyset \Rightarrow \exists a \in H$. α) $a = e \Rightarrow a^{-1} = a$ β) $a \neq e$

Podle bodu 3.b): $a \in H \Rightarrow a^2 \in H \Rightarrow a^3 \in H \Rightarrow \dots \Rightarrow a^m \in H \Rightarrow \dots (\forall m \in \mathbb{N})$

H je konečná množina $\Rightarrow \exists m_1, m_2 \in \mathbb{N} :$

$a^{m_1} = a^{m_2}$, $m_1 > m_2$

$a^{m_2+d} = a^{m_2}$ (věta o krácení) $m_1 = m_2 + d$

$a^d = e$ ($a \neq e \Rightarrow d > 1$)

$\Rightarrow a \cdot \underbrace{a^{d-1}}_{\in H} = e$

$a^{d-1} \cdot a = e$

$\Rightarrow a^{d-1} = a^{-1} \in H$

□

Př: $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ tvoří grupu (· je násobení modulo 5):

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1.) uzavřenost $\checkmark$

2.) asociativita (plyne z asociativity nás. v $\mathbb{Z}$)

3.) $1 = e$

4.) $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$

$(H, \cdot)$ kde $H = \{1, 4\}$ tvoří podgrupu grupy $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ neboť:

·	1	4
1	1	4
4	4	1

$\Rightarrow$ množina $H = \{1, 4\}$ splňuje:

1.) $H \subseteq G = \mathbb{Z}_5 \setminus \{0\} = \{1, 2, 3, 4\}$

2.) H je konečná množina

3.) a) $H \neq \emptyset$

b) $\forall a, b \in H : ab \in H$

$\Rightarrow \underline{\underline{(H, \cdot) \text{ je podgrupa grupy } (\mathbb{Z}_5 \setminus \{0\}, \cdot)}}$

Def (Násobení komplexů): Komplexem v grupě $(G, \cdot)$ nazveme každou podmnožinu množiny G . Necht' $S_1, S_2 \subseteq G$.
Potom definujeme:

$$S_1 \cdot S_2 = \{ s_1 \cdot s_2 \mid s_1 \in S_1, s_2 \in S_2 \}$$

V případě, že $S_1 = \{a\} \in G$, $S_2 = H \subseteq G$ budeme psát:

$$S_1 S_2 = \{a\} H = aH = \{ah \mid h \in H\}.$$

Pr: $(G, \cdot) = (\mathbb{Z}_5, +)$, $a=3$, $H = \{2, 4\}$

$$\Rightarrow a+H = \{3+2, 3+4\} = \{0, 2\}$$

Věta: Necht' $(G, \cdot)$ je grupa a $A, B, H \subseteq G$. Potom

$$A(B \cdot H) = (AB)H$$

Trn. násobení komplexů je asociativní.

Důkaz:

$$\begin{aligned} A(BH) &= A \{ bh \mid b \in B, h \in H \} = \{ a(bh) \mid a \in A, b \in B, h \in H \} = \\ &= (\text{asoc. n. s. } G) = \{ (ab)h \mid a \in A, b \in B, h \in H \} = (AB)H \end{aligned}$$

□

Důsledek: Necht' $(G, \cdot)$ je grupa, $a \in G$, $b \in G$, $H \subseteq G$. Potom platí

$$a(bH) = (ab)H$$