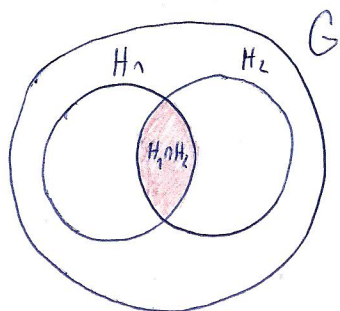


Pr. min Dokažte. Necht $(G, \cdot)$ je grupa a $(H_1, \cdot)$ i $(H_2, \cdot)$ její podgrupy. Pakom $(H_1 \cap H_2, \cdot)$ je podgrupa grupy $(G, \cdot)$.



Důkaz: I.) $H_1 \subseteq G, H_2 \subseteq G \Rightarrow H_1 \cap H_2 \subseteq G$

II.) α) $x \in H_1, x \in H_2 \Rightarrow x \in H_1 \cap H_2 \Rightarrow H_1 \cap H_2 \neq \emptyset$

β)

1.) $\forall a, b \in H_1 \cap H_2 : \begin{cases} a \cdot b \in H_1 \Rightarrow a \cdot b \in H_1 \\ a \cdot b \in H_2 \Rightarrow a \cdot b \in H_2 \end{cases} \Rightarrow a \cdot b \in H_1 \cap H_2$ (uzavřenost)

2) asociativita - Obecná vlastnost a asociativita násobení na G

3) neutrální prvek: $e \in H_1 \wedge e \in H_2 \Rightarrow e \in H_1 \cap H_2$

4) inverzní prvek: $\forall a \in H_1 \cap H_2 : \begin{cases} a \in H_1 \Rightarrow a^{-1} \in H_1 \\ a \in H_2 \Rightarrow a^{-1} \in H_2 \end{cases} \Rightarrow a^{-1} \in H_1 \cap H_2$

□

Rozklad grupy podle podgroupy

Značení: $(G, \cdot)$ je grupa a $(H, \cdot)$ její podgrupa, pak

$$G/H = \{ a \cdot H \mid a \in G \} \dots \text{rozklad grupy } (G, \cdot) \text{ podle podgroupy } (H, \cdot)$$

$$|G/H| \dots \text{počet prvků } G/H = \text{index podgroupy } (H, \cdot) \text{ v grupě } (G, \cdot)$$

Př. Proved'te rozklad grupy $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ podle podgrupy $(H, \cdot)$
 kde $\mathbb{Z}_7 \setminus \{0\} = \{1, 2, 3, 4, 5, 6\}$, $\cdot$ je "násobení modulo 7".

a) $H = \{1, 2, 4\}$

$$1 \cdot H = \{1 \cdot 1, 1 \cdot 2, 1 \cdot 4\} = \{1, 2, 4\} = H$$

$$2 \cdot H = \{2 \cdot 1, 2 \cdot 2, 2 \cdot 4\} = \{2, 4, 1\} = H$$

$$3 \cdot H = \{3 \cdot 1, 3 \cdot 2, 3 \cdot 4\} = \{3, 6, 5\}$$

$$4 \cdot H = \{4 \cdot 1, 4 \cdot 2, 4 \cdot 4\} = \{4, 1, 2\} = H$$

$$5 \cdot H = \{5 \cdot 1, 5 \cdot 2, 5 \cdot 4\} = \{5, 3, 6\}$$

$$6 \cdot H = \{6 \cdot 1, 6 \cdot 2, 6 \cdot 4\} = \{6, 5, 3\}$$

$$\Rightarrow \underline{\underline{G/H = \{ \{1, 2, 4\}, \{3, 6, 5\} \}}}$$

$$\Rightarrow |G| = |G/H| \cdot |H| = (G:H) |H|$$

$$(6 = 2 \cdot 3)$$

b) $H = \{1, 6\}$

$$1 \cdot H = \{1 \cdot 1, 1 \cdot 6\} = \{1, 6\} = H$$

$$2 \cdot H = \{2 \cdot 1, 2 \cdot 6\} = \{2, 5\}$$

$$3 \cdot H = \{3 \cdot 1, 3 \cdot 6\} = \{3, 4\}$$

$$4 \cdot H = \{4 \cdot 1, 4 \cdot 6\} = \{4, 3\}$$

$$5 \cdot H = \{5 \cdot 1, 5 \cdot 6\} = \{5, 2\}$$

$$6 \cdot H = \{6 \cdot 1, 6 \cdot 6\} = \{6, 1\} = H$$

$$\Rightarrow \underline{\underline{G/H = \{ \{1, 6\}, \{2, 5\}, \{3, 4\} \}}} \Rightarrow (G:H) = 3$$

Pr. Označme $V = \{V_1, V_2, V_3, V_4, V_5, V_6\}$ množinu vrcholů šestiúhelníku
a σ zobrazení definované předpisem:

$$\sigma(V_1) = V_2$$

$$\sigma(V_2) = V_3$$

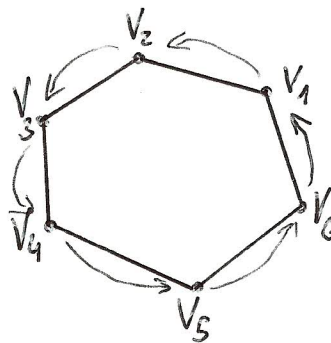
$$\sigma(V_3) = V_4$$

$$\sigma(V_4) = V_5$$

$$\sigma(V_5) = V_6$$

$$\sigma(V_6) = V_1$$

$\Rightarrow$



Dále označme $\sigma^2 = \sigma \circ \sigma$, $\sigma^3 = \sigma \circ \sigma \circ \sigma$, ... a

$$G = \{ \sigma^k \mid k \in \mathbb{N} \} = \{ \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6 = \text{id} \}$$

$$\sigma^7 = \sigma^6 \circ \sigma = \text{id} \circ \sigma = \sigma$$

$$\sigma^8 = \sigma^6 \circ \sigma^2 = \text{id} \circ \sigma^2 = \sigma^2$$

a) Dokažte, že $(G, \circ)$, kde $\circ$ je složením zobrazení, je grupa:

$$1) \forall \sigma^{k_1}, \sigma^{k_2} \in G : \sigma^{k_1} \circ \sigma^{k_2} = \sigma^{k_1+k_2} \in G$$

$$2) \forall \sigma^{k_1}, \sigma^{k_2}, \sigma^{k_3} \in G : \sigma^{k_1} \circ (\sigma^{k_2} \circ \sigma^{k_3}) = \sigma^{k_1+k_2+k_3} = (\sigma^{k_1} \circ \sigma^{k_2}) \circ \sigma^{k_3}$$

$$3) \forall \sigma^k \in G : \sigma^6 \circ \sigma^k = \text{id} \circ \sigma^k = \sigma^k$$

$$\sigma^k \circ \sigma^6 = \sigma^k \circ \text{id} = \sigma^k \quad \Rightarrow \quad \text{id} = \sigma^6 = \text{id}$$

$$4) \forall \sigma^k \in G : \sigma^k \in \{ \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \text{id} \}$$

$$\sigma^1 \circ \sigma^5 = \sigma^5 \circ \sigma^1 = \text{id} \quad \Rightarrow \quad \sigma^{-1} = \sigma^5 ; (\sigma^5)^{-1} = \sigma$$

$$\sigma^2 \circ \sigma^4 = \sigma^4 \circ \sigma^2 = \text{id} \quad \Rightarrow \quad (\sigma^2)^{-1} = \sigma^4$$

$$(\sigma^4)^{-1} = \sigma^2$$

$$\sigma^3 \circ \sigma^3 = \sigma^3 \circ \sigma^3 = \text{id} \quad \Rightarrow \quad (\sigma^3)^{-1} = \sigma^3$$

$$\sigma^6 \circ \sigma^6 = \text{id} \circ \text{id} = \text{id} \quad \Rightarrow \quad (\sigma^6)^{-1} = \sigma^6$$

b) DokaŹte, Źe $H_1 = \{\sigma^2, \sigma^4, \sigma^6 = id\}$ je podgrupou grupy G

H_1 je konečná neprázdná podmnoŹina G a je uzavřena vzhledem ke skłádáním a obrácení:

$\circ$	σ^2	σ^4	σ^6	
σ^2	σ^4	σ^6	$\sigma^8 = \sigma^2$	
σ^4	σ^6	σ^2	σ^4	
σ^6	σ^2	σ^4	σ^6	

$\Rightarrow (H_1, \circ)$ je podgrupa
grupy $(G, \circ)$

c) Proveďte rozklad grupy $(G, \circ)$ podle podgrupy $(H_1, \circ)$.

$$\sigma \circ H_1 = \{\sigma \circ \sigma^2, \sigma \circ \sigma^4, \sigma \circ \sigma^6\} = \{\sigma^3, \sigma^5, \sigma\}$$

$$\sigma^2 \circ H_1 = \{\sigma^2 \circ \sigma^2, \sigma^2 \circ \sigma^4, \sigma^2 \circ \sigma^6\} = \{\sigma^4, \sigma^6, \sigma^2\} = H_1$$

$$\sigma^3 \circ H_1 = \{\sigma^3 \circ \sigma^2, \sigma^3 \circ \sigma^4, \sigma^3 \circ \sigma^6\} = \{\sigma^5, \sigma, \sigma^3\}$$

$$\sigma^4 \circ H_1 = \{\sigma^4 \circ \sigma^2, \sigma^4 \circ \sigma^4, \sigma^4 \circ \sigma^6\} = \{\sigma^6, \sigma^2, \sigma^4\} = H_1$$

$$\sigma^5 \circ H_1 = \{\sigma^5 \circ \sigma^2, \sigma^5 \circ \sigma^4, \sigma^5 \circ \sigma^6\} = \{\sigma, \sigma^3, \sigma^5\}$$

$$\sigma^6 \circ H_1 = \{\sigma^6 \circ \sigma^2, \sigma^6 \circ \sigma^4, \sigma^6 \circ \sigma^6\} = \{\sigma^2, \sigma^4, \sigma^6\} = H_1$$

$$\underline{\underline{G/H_1 = \{\{\sigma^3, \sigma^5, \sigma\}, \{\sigma^4, \sigma^6, \sigma^2\}\} \Rightarrow (G:H) = |G/H| = 2}}$$

d) Proveďte rozklad grupy $(G, \circ)$ podle podgrupy $(H_2, \circ)$, kde $H_2 = \{\sigma^6, \sigma^3\}$
IŹe to podgrupa, protože $\sigma^6 = id = e$, $\sigma^3 \circ \sigma^3 = id$

$$\sigma \circ H_2 = \{\sigma \circ \sigma^6, \sigma \circ \sigma^3\} = \{\sigma, \sigma^4\}$$

$$\sigma^2 \circ H_2 = \{\sigma^2 \circ \sigma^6, \sigma^2 \circ \sigma^3\} = \{\sigma^2, \sigma^5\}$$

$$\sigma^3 \circ H_2 = \{\sigma^3 \circ \sigma^6, \sigma^3 \circ \sigma^3\} = \{\sigma^3, \sigma^6\}$$

$$\Rightarrow \underline{\underline{G/H_2 = \{\{\sigma, \sigma^4\}, \{\sigma^2, \sigma^5\}, \{\sigma^3, \sigma^6\}\}}}$$

$\vdots$

$$\Rightarrow (G:H) = 3$$

Př. Proveďte rozklad grupy $(\mathbb{Z}, +)$ podle její pod grupy $(3\mathbb{Z}, +)$, kde $3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$.

$$\mathbb{Z}/3\mathbb{Z} = \{a+3\mathbb{Z} \mid a \in \mathbb{Z}\}$$

$$0+3\mathbb{Z} = \{0+3k \mid k \in \mathbb{Z}\} = 3\mathbb{Z} = \text{ násobky čísla 3 } = \bar{0}_3 \text{ (zbytek 0 při dělení číslem 3)}$$

$$1+3\mathbb{Z} = \{1+3k \mid k \in \mathbb{Z}\} = \bar{1}_3 \text{ (zbytek 1 při dělení číslem 3)}$$

$$2+3\mathbb{Z} = \{2+3k \mid k \in \mathbb{Z}\} = \bar{2}_3$$

$$3+3\mathbb{Z} = \{3+3k \mid k \in \mathbb{Z}\} = \{3(k+1) \mid k \in \mathbb{Z}\} = \{3k^* \mid k^* \in \mathbb{Z}\} = \bar{0}_3$$

$$4+3\mathbb{Z} = \{4+3k \mid k \in \mathbb{Z}\} = \{1+3(k+1) \mid k \in \mathbb{Z}\} = \{1+3k^* \mid k^* \in \mathbb{Z}\} = \bar{1}_3$$

$\vdots$

$\Downarrow$

$$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}_3, \bar{1}_3, \bar{2}_3\} = \text{Množina zbytkových tříd modulo 3} = \mathbb{Z}_3$$

Obecně:

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \dots \text{Množina zbytkových tříd modulo } m$$