Rozklad grupy podle podgrupy

Př.: Uvažujme grupu $(\mathbb{Z}_6, +)$. Pak $(H, +)$, kde $H = \{0, 2, 4\}$ je její podgrupa, neboť H je neprázdná konečná podmnožina množiny $G = \mathbb{Z}_6$ je uzavřená vzhledem k násobení:

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Vytvoříme množiny $x + H = \{x + h \mid h \in H\}$ pro každé $x \in G$:

$0 + H = \{0+0, 0+2, 0+4\} = \{0, 2, 4\} = H$

$1 + H = \{1+0, 1+2, 1+4\} = \{1, 3, 5\}$

$2 + H = \{2+0, 2+2, 2+4\} = \{2, 4, 0\} = H$

$3 + H = \{3+0, 3+2, 3+4\} = \{3, 5, 1\}$

$4 + H = \{4+0, 4+2, 4+4\} = \{4, 0, 2\} = H$

$5 + H = \{5+0, 5+2, 5+4\} = \{5, 1, 3\}$

Pozorování:

1.) $x + H = H \iff x \in H$

2.) $\bigcup_{x \in G} (x + H) = \{0, 2, 4\} \cup \{1, 3, 5\} = G = \mathbb{Z}_6$

3.) $G/H = \{x + H \mid x \in G\} \Rightarrow G/H = \{\{0, 2, 4\}, \{1, 3, 5\}\}$

$\Rightarrow$ a) $|a + H| = |b + H| = |H|$

b) $|G| = \underbrace{|G/H|}_{\text{budeme označovat } (G:H)} \cdot |H|$

Věta: Nechť $(G,\cdot)$ je grupa a $(H,\cdot)$ její podgrupa. Potom

$$Hx = H \iff xH = H \iff x \in H$$

Důkaz: $xH = H \iff x \in H$

$\boxed{\Leftarrow}$ Předpokládejme $x \in H$.

1.) Dokážeme $xH \subseteq H$:

$$(\forall xh \in xH : \underbrace{(\text{uzavřenost!}\ x\in H, h\in H)}\ xh \in H) \Rightarrow xH \subseteq H$$

2.) Dokážeme $H \subseteq xH$

$$(\forall h \in H : h = x\cdot(\underbrace{x^{-1}\cdot h}_{h_1\in H}) = xh_1 \in xH) \Rightarrow H \subseteq xH$$

(inverze na H: $x\in H \Rightarrow x^{-1}\in H$)

$\boxed{\Rightarrow}$ Předpokládejme $xH = H$.

$(H,\cdot)$ je podgrupa $\Rightarrow e \in H \Rightarrow$ protože $xH = H$ musí platit:

$$xe \in xH \Rightarrow xe = x \in H$$

Ekvivalenci $Hx = H \iff x \in H$ bychom dokázali analogicky. □

Věta: Nechť $(G,\cdot)$ je grupa a $(H,\cdot)$ její podgrupa. Potom

$$\forall a,b \in G : (aH \cap bH \neq \emptyset \Rightarrow aH = bH)$$

Důkaz:

$$aH \cap bH \neq \emptyset \Rightarrow \exists x \in aH \cap bH \Rightarrow \exists h_1, h_2 \in H : x = ah_1 = bh_2$$

$$\Rightarrow a = b\underbrace{h_2 h_1^{-1}}_{\in H} \Rightarrow \exists h \in H : a = bh \Rightarrow aH = (bh)H = b(hH) = bH.$$

□

Důsledek: Věta obměněná: $\forall a,b \in G : aH \neq bH \Rightarrow aH \cap bH = \emptyset$

Tzn. navzájem různé třídy rozkladu jsou disjunktní.

Poznámka $(G,\cdot)$ je podgrupou grupy $(G,\cdot)$. Z výše uvedeného plyne, že $\forall g \in G : gG = G = Gg$

Věta: Nechť $(G,\cdot)$ je grupa a $H \subseteq G$, $H \neq \emptyset$. Potom

$$\bigcup_{a \in G} aH = G$$

Důkaz:

a) $G \supseteq \bigcup_{a \in G} aH$ (plyne z uzavřenosti násobení na G)

b) $H \neq \emptyset \Rightarrow \exists h \in H \Rightarrow \bigcup_{a \in g} aH \supseteq \bigcup_{a \in g} a\{h\} = \{ah \mid a \in G\} = G \cdot h_{\in g} = G$

$\Rightarrow$ $G \supseteq \bigcup_{g \in G} aH \supseteq G$ □

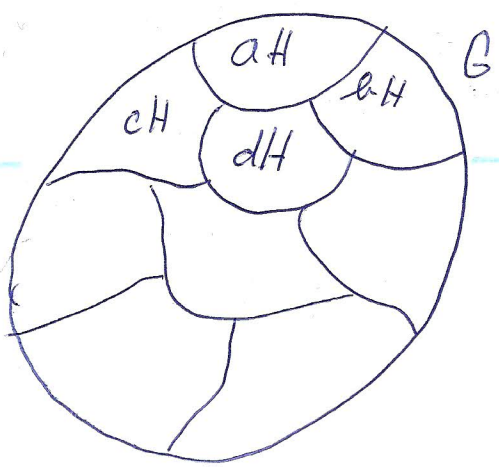
Jestliže $(H,\cdot)$ je podgrupa grupy $(G,\cdot)$, pak

Důsledek: $G/H = \{aH \mid a \in G\}$ tvoří rozklad množiny G. Tj platí:

1.) $\bigcup_{a \in G} aH = G$

2.) $aH \neq bH \Rightarrow aH \cap bH = \emptyset$

3.) $\forall a \in G: aH \neq \emptyset$



Def. (Řád grupy): Nechť $(G,\cdot)$ je grupa. Počet prvků množiny G nazýváme řádem grupy $(G,\cdot)$. Značíme

$$|G|.$$

Def. (Index podgrupy): Nechť $(G,\cdot)$ je grupa a $(H,\cdot)$ její podgrupa. Indexem podgrupy $(H,\cdot)$ v grupě $(G,\cdot)$ nazveme počet prvků množiny G/H. Značíme

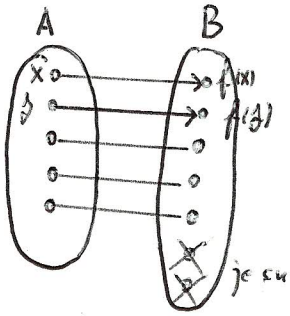
$$|G/H| = (G:H)$$

Pozorování: Množiny A a B mají stejný počet prvků (uvažujme konečné množiny A a B) právě když existuje bijektivní zobrazení $f: A \to B$

f je bijekce $\Leftrightarrow$

1.) je injektivní $\Leftrightarrow \forall x,y \in A: x \neq y \Rightarrow f(x) \neq f(y)$

2.) je surjektivní $\Leftrightarrow \forall b \in B\ \exists a \in A: f(a) = b$



Věta: Nechť $(G,\cdot)$ je grupa a $(H,\cdot)$ její konečná podgrupa. Pak $\forall aH \in G/H$:

$$\underbrace{|aH|}_{\text{počet prvků množiny } aH.} = |H|$$

Důkaz: Podle předchozího pozorování stačí nalézt bijektivní zobr. $f: H \to aH$.

Dokážeme, že $f: f(h) = ah$, $\forall h \in H$ je bijekce

1.) $\forall h_1, h_2 \in H$: $f(h_1) = f(h_2) \Leftrightarrow ah_1 = ah_2 \Leftrightarrow h_1 = h_2$ (věta o krácení) $\Rightarrow$ injektivní

2.) $\forall ah \in aH\ \exists h \in H$: $f(h) = ah \Rightarrow f$ je surjektivní

□

Def. (Řád prvku): Nechť $(G,\cdot)$ je grupa, $a \in G$. Nejmenší přirozené číslo n splňující

$$a^n = e,$$

kde e je neutrální prvek v $(G,\cdot)$ nazýváme řádem prvku a.
Pokud takové n neexistuje, říkáme, že a je nekonečného řádu.

Věta (Lagrangeova): Nechť $(G,\cdot)$ je konečná grupa a $(H,\cdot)$ její podgrupa. Potom platí:

1.) $|G| = |G/_H| \cdot |H| = (G:H)\,|H|$

2.) $|H| \mid |G|$ (Řád podgrupy dělí řád grupy)

3.) Nechť n je řád prvku $a \in G$. Potom $n \mid |G|$.

4.) Nechť $K \subseteq H \subseteq G$, $(K,\cdot), (H,\cdot)$ jsou podgrupy $(G,\cdot)$. Potom

$$|G/_K| = |G/_H| \cdot |H/_K|$$

tj. $$(G:K) = (G:H)(H:K)$$

Důkaz: 1.) $(G,\cdot)$ je konečná grupa $\Rightarrow$ $(H,\cdot)$ je konečná grupa $\Rightarrow$ $\forall a \in G: |H| = |aH| \Rightarrow$

$$|G/_H| = |\underbrace{\{aH \mid a \in G\}}_{\text{rozkladmi}\check{\text{z}}\ G}| \Rightarrow \qquad |G| = |G/_H| \cdot |H| = (G:H)\,|H|$$

2.) Plyne okamžitě z 1.).

3.) Nechť n je řád prvku a $\Rightarrow$ $e^n = e$ $\Rightarrow$ $(\underbrace{\{a, a^2, \dots, a^n = e\}}_{H}, \cdot)$ je podgrupa grupy $(G,\cdot)$ $\Rightarrow$ $\underbrace{|H|}_{=n} \mid |G|$ (podle 2.) $\Rightarrow$ $n \mid |G|$

4.) G je konečná $\Rightarrow$

$$\left.\begin{aligned} |G| &= (G:H)\,|H| \\ |G| &= (G:K)\,|K| \\ |H| &= (H:K)\,|K| \end{aligned}\right\} \longrightarrow \begin{aligned} |G| &= (G:H)\underbrace{(H:K)}_{|H|}|K| \\ |G| &= (G:K)\,|K| \end{aligned}$$

$$(G:K)\,|K| = (G:H)(H:K)\,|K| \quad /:|K| \neq 0 \text{ protože } K \neq \emptyset$$

$$(G:K) = (G:H)(H:K)$$

Pozn: Bod 4.) platí i pro nekonečnou grupu $(G,\cdot)$ stačí předpoklad $(G:H), (H:K) \in \mathbb{N}$.

□