Podgrupy

Nechť $(G,\cdot)$ je grupa s jednotkovým prvkem $\mathtt{1}$ a nechť $H \subseteq G$ je podmnožina splňující následující tři podmínky:

$$\begin{aligned}
&(\forall a, b \in H)(a \cdot b \in H),\\
&\mathtt{1} \in H,\\
&(\forall a \in H)(a^{-1} \in H).
\end{aligned}$$

Pak říkáme, že H je **podgrupa** grupy $(G,\cdot)$. Důvodem pro tuto terminologii je fakt plynoucí přímo z uvedených podmínek, že potom totiž množina H je uzavřená vzhledem k operaci $\cdot$, čili $\cdot$ zůstává operací, i když ji zúžíme jenom na množinu H, a přitom dvojice $(H,\cdot)$ je opět grupa.

Pro každou grupu $(G,\cdot)$ jsou podmnožiny $\{\mathtt{1}\}$ a G množiny G podgrupami grupy $(G,\cdot)$. Kromě nich ovšem může mít grupa $(G,\cdot)$ množství dalších podgrup. Příklady budou následovat. Podgrupy $H \subseteq G$ grupy $(G,\cdot)$ splňující $H \neq G$ se nazývají **vlastní** podgrupy grupy $(G,\cdot)$.

Příklady. Množina $\mathbb{Z}$ všech celých čísel je podgrupou v grupě $(\mathbb{Q},+)$. Podobně množina $\mathbb{Q}-\{0\}$ všech nenulových racionálních čísel je podgrupou v grupě $(\mathbb{R}-\{0\},\cdot)$. Rovněž množina $\mathbb{R}^+$ všech kladných reálných čísel je podgrupou v grupě $(\mathbb{R}-\{0\},\cdot)$.

V kapitole o permutacích jsme zavedli množinu $S(X)$ všech permutací dané množiny X a v kapitole o grupách jsme viděli, že spolu se skládáním zobrazení $\circ$ tak vzniká grupa $(S(X),\circ)$, nazývaná grupa permutací množiny X. Budeme dále opět pracovat pouze s konečnými množinami tvaru $X = \{1, 2, \ldots, n\}$, kde n je přirozené číslo. Pak místo $S(X)$ budeme psát S_n. Vziká tak grupa $(S_n,\circ)$, která se nazývá **symetrická grupa** stupně n.

Dále jsme v kapitole o permutacích označili A_n množinu všech sudých permutací množiny $X = \{1, 2, \dots, n\}$. Potom z posledního důsledku v citované kapitole plyne, že A_n je podgrupa v grupě $(S_n, \circ)$. To znamená, že pak také $(A_n, \circ)$ je grupa. Tato grupa se nazývá **alternující grupa** stupně n.

Tvrzení. Nechť $(G, \cdot)$ je grupa. Pak pro libovolnou indexovou množinu $I \neq \emptyset$ a pro libovolný soubor podgrup H_i grupy $(G, \cdot)$, kde $i \in I$, platí, že průnik tohoto souboru podgrup $\bigcap_{i \in I} H_i$ je také podgrupa grupy $(G, \cdot)$.

Důkaz. Nechť $a, b \in \bigcap_{i \in I} H_i$ jsou libovolné prvky. Pak ovšem máme $a, b \in H_i$ pro všechna $i \in I$. Poněvadž jde o podgrupy, plyne odtud, že pak $a \cdot b \in H_i$ platí pro všechna $i \in I$. To ale znamená, že $a \cdot b \in \bigcap_{i \in I} H_i$. Podobně se zjistí, že také $1 \in \bigcap_{i \in I} H_i$ a že z toho, že $a \in \bigcap_{i \in I} H_i$, plyne rovněž, že $a^{-1} \in \bigcap_{i \in I} H_i$. Je tedy $\bigcap_{i \in I} H_i$ podgrupa grupy $(G, \cdot)$.

Důsledek. Nechť $(G, \cdot)$ je grupa. Označme $\boldsymbol{\mathcal{S}}(G)$ množinu všech podgrup grupy $(G, \cdot)$. Podgrupy grupy $(G, \cdot)$ lze navzájem porovnávat množinovou inkluzí $\subseteq$. Vzniká tak uspořádaná množina $(\boldsymbol{\mathcal{S}}(G), \subseteq)$, a tato uspořádaná množina je úplný svaz.

Důkaz. Z kapitoly o svazech víme, že stačí pro libovolnou podmnožinu $\mathcal{Q} \subseteq \boldsymbol{\mathcal{S}}(G)$ ukázat, že existuje $\inf \mathcal{Q}$ v $(\boldsymbol{\mathcal{S}}(G), \subseteq)$. Je-li $\mathcal{Q} \neq \emptyset$, pak z předchozího tvrzení víme, že průnik $\bigcap \mathcal{Q}$ všech podgrup z $\mathcal{Q}$ je zase podgrupou grupy $(G, \cdot)$, a je jasné, že pak $\inf \mathcal{Q} = \bigcap \mathcal{Q}$. Pro $\mathcal{Q} = \emptyset$ pak evidentně je $\inf \emptyset = G$, což je největší podgrupa grupy $(G, \cdot)$. Je tedy $(\boldsymbol{\mathcal{S}}(G), \subseteq)$ úplný svaz.

Buď dále $(G, \cdot)$ grupa. Buď $M \subseteq G$ libovolná podmnožina. Uvažme soubor $\mathcal{R}$ všech těch podgrup grupy $(G, \cdot)$, které v sobě obsahují množinu M. Tento soubor $\mathcal{R}$ je neprázdný, neboť jednou z podgrup s uvedenou vlastností je také celá množina G. Podle předchozího tvrzení je pak průnik $\bigcap \mathcal{R}$ tohoto souboru podgrup také podgrupou grupy $(G, \cdot)$, přičemž tato podgrupa v sobě rovněž obsahuje množinu M. Tuto poslední podgrupu $\bigcap \mathcal{R}$ pak značíme symbolem $\langle M \rangle$. Je to nejmenší podgrupa grupy $(G, \cdot)$ v uspořádané množině $(\boldsymbol{\mathcal{S}}(G), \subseteq)$ všech podgrup této grupy mezi všemi těmi podgrupami, které v sobě obsahují množinu M. O této podgrupě $\langle M \rangle$ říkáme, že je to podgrupa **generovaná** množinou M, a o samotné množině M pak říkáme, že je to množina **generátorů** podgrupy $\langle M \rangle$. Tato terminologie je odůvodněna následujícím faktem. Předem poznamenejme, že pro $M = \emptyset$ zřejmě máme $\langle \emptyset \rangle = \{1\}$.

Tvrzení. Nechť $(G, \cdot)$ je grupa a nechť $M \subseteq G$, $M \neq \emptyset$ je libovolná podmnožina. Pak platí následující rovnost:

$$\langle M \rangle = \{a_1^{i_1} \cdot a_2^{i_2} \cdot \ \ldots \ \cdot a_n^{i_n} \mid n \in \mathbb{N},\ a_1, a_2, \ldots, a_n \in M, \\ i_1, i_2, \ldots, i_n \in \{-1, 1\}\},$$

kde pro každý prvek $a \in M$ interpretujeme a^1 jako a a a^{-1} je inverzní prvek k prvku a.

Důkaz. Označme množinu uvedenou napravo v této rovnosti jako T. Máme ukázat, že pak platí $\langle M \rangle = T$. Podle definice je $\langle M \rangle$ nejmenší podgrupa grupy $(G, \cdot)$ vzhledem k inkluzi obsahující množinu M. Stačí, když ukážeme, že tyto podmínky, které jednoznačně vymezují množinu $\langle M \rangle$, platí také pro množinu T. Pak budeme vědět, že opravdu $\langle M \rangle = T$.

Nejprve se přesvědčíme, že T je podgrupa grupy $(G, \cdot)$. Jsou-li ovšem $a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_n^{i_n}$, $b_1^{j_1} \cdot b_2^{j_2} \cdot \ldots \cdot b_k^{j_k} \in T$ libovolné prvky, kde $n, k \in \mathbb{N}$, $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_k \in M$ a $i_1, i_2, \ldots, i_n, j_1, j_2, \ldots, j_k \in \{-1, 1\}$, pak je vidět, že také $a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_n^{i_n} \cdot b_1^{j_1} \cdot b_2^{j_2} \cdot \ldots \cdot b_k^{j_k} \in T$. Dále $M \neq \emptyset$ a pro libovolný prvek $a \in M$ máme $a \cdot a^{-1} \in T$, přičemž $a \cdot a^{-1} = \mathtt{1}$, takže $\mathtt{1} \in T$. Je také vidět, že pokud $a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_n^{i_n} \in T$, pak také $a_n^{-i_n} \cdot a_{n-1}^{-i_{n-1}} \cdot \ldots \cdot a_1^{-i_1} \in T$, a to je inverzní prvek k uvedenému prvku. Je tedy T podgrupa grupy $(G, \cdot)$.

Dále si všimneme, že očividně $M \subseteq T$, tedy že množina T v sobě obsahuje množinu M.

Nakonec ukážeme, že T je nejmenší podmnožina množiny G s předchozími dvěma vlastnostmi vzhledem k inkluzi, tedy že je to nejmenší podgrupa grupy $(G, \cdot)$ obsahující množinu M. Buď tedy W libovolná podgrupa grupy $(G, \cdot)$ obsahující množinu M. Pak je třeba ukázat, že platí $T \subseteq W$. Tedy pro libovolný prvek $a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_n^{i_n} \in T$, kde $n \in \mathbb{N}$, $a_1, a_2, \ldots, a_n \in M$ a $i_1, i_2, \ldots, i_n \in \{-1, 1\}$, máme ukázat, že $a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_n^{i_n} \in W$. To ale ovšem ihned plyne z toho, že $M \subseteq W$ a že W je podgrupa grupy $(G, \cdot)$. Je tedy vskutku pravda, že $T \subseteq W$.

Příklad. Podle poznatků o rozkladech permutací konečných množin na součiny transpozic víme, že pro každé číslo $n \in \mathbb{N}$ množina $\{(i \;\; j) \mid i, j \in \{1, 2, \ldots, n\}, i \neq j\}$ všech transpozic dvojic vzájemně různých čísel z $\{1, 2, \ldots, n\}$ vygeneruje v symetrické grupě $(S_n, \circ)$ stupně n jako podgrupu celou množinu S_n. Jinak řečeno, množina všech transpozic vzájemně různých čísel z $\{1, 2, \ldots, n\}$ vygeneruje celou symetrickou grupu $(S_n, \circ)$.