Podgrupy a homomorfismy grup

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 $X = \{1, 2, \dots, n\}$, kde n je přirozené číslo. Pak stejně jako v kapitole o permutacích 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.

Nechť $(G, \cdot)$ a $(H, *)$ jsou dvě grupy a nechť $f : G \to H$ je zobrazení. Řekneme, že f je **homomorfismus** grupy $(G, \cdot)$ do grupy $(H, *)$, je-li splněna podmínka

$$(\forall a, b \in G)(f(a \cdot b) = f(a) * f(b)).$$

Tvrzení. Jsou-li $(G, \cdot)$, resp. $(H, *)$ grupy mající jednotkové prvky $\mathtt{1}$, resp. $\mathbb{1}$ a je-li $f : G \to H$ homomorfismus grupy $(G, \cdot)$ do grupy $(H, *)$, pak jsou rovněž splněny podmínky

$$f(\mathtt{1}) = \mathbb{1} \quad \text{a} \quad (\forall a \in G)(f(a^{-1}) = f(a)^{-1}).$$

Důkaz. Máme $f(\mathtt{1}) * f(\mathtt{1}) = f(\mathtt{1} \cdot \mathtt{1}) = f(\mathtt{1})$, odkud plyne $\mathbb{1} = f(\mathtt{1}) * f(\mathtt{1})^{-1} = f(\mathtt{1}) * f(\mathtt{1}) * f(\mathtt{1})^{-1} = f(\mathtt{1}) * \mathbb{1} = f(\mathtt{1})$. Dále pro každé $a \in G$ máme $f(a) * f(a^{-1}) = f(a \cdot a^{-1}) = f(\mathtt{1}) = \mathbb{1} = f(\mathtt{1}) = f(a^{-1} \cdot a) = f(a^{-1}) * f(a)$, takže $f(a^{-1})$ je inverzním prvkem k prvku $f(a)$, a tedy $f(a^{-1}) = f(a)^{-1}$.

Příklady. Vezměme libovolné $n \in \mathbb{N}$ a uvažme zobrazení $h : \mathbb{Z} \to \mathbb{Z}_n$ dané pro každé $a \in \mathbb{Z}$ předpisem $h(a) = [a]_n$. Pak zobrazení h je homomorfismus grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}_n, +)$, neboť pro libovolná $a, b \in \mathbb{Z}$ máme $[a + b]_n = [a]_n + [b]_n$.

Nechť opět $n \in \mathbb{N}$ je libovolné číslo. V kapitole o permutacích jsme pro každou permutaci $\sigma \in S_n$ definovali její paritu $\wp(\sigma)$ a v posledním důsledku této kapitoly jsme viděli, že pro kterékoliv dvě permutace $\sigma, \tau \in S_n$ platí $\wp(\sigma \circ \tau) = \wp(\sigma) \cdot \wp(\tau)$. To znamená, že zobrazení $\wp : S_n \to \mathbb{Q} - \{0\}$ přiřazující každé permutaci $\sigma \in S_n$ její paritu $\wp(\sigma)$ je homomorfismus grupy $(S_n, \circ)$ do grupy $(\mathbb{Q} - \{0\}, \cdot)$.

Tvrzení. Nechť $(G,\cdot)$, $(H,*)$ a $(K,\bullet)$ jsou grupy a nechť $f : G \to H$, resp. $g : H \to K$ jsou homomorfismy grupy $(G,\cdot)$ do grupy $(H,*)$, resp. grupy $(H,*)$ do grupy $(K,\bullet)$. Pak složené zobrazení $g \circ f : G \to K$ je homomorfismus grupy $(G,\cdot)$ do grupy $(K,\bullet)$.

Důkaz. Skutečně pak pro libovolná $a, b \in G$ máme

$$\begin{aligned}(g \circ f)(a \cdot b) &= g(f(a \cdot b)) = g(f(a) * f(b)) \\ &= g(f(a)) \bullet g(f(b)) = (g \circ f)(a) \bullet (g \circ f)(b).\end{aligned}$$

Tvrzení. Nechť $(G,\cdot)$ a $(H,*)$ jsou grupy a nechť $f : G \to H$ je homomorfismus grupy $(G,\cdot)$ do grupy $(H,*)$. Pak obraz $f(G)$ při tomto homomorfismu je podgrupa grupy $(H,*)$.

Důkaz. Nechť 1, resp. $\mathbb{1}$ jsou jednotkové prvky grup $(G,\cdot)$, resp. $(H,*)$. Nechť $c, d \in f(G)$ jsou libovolné prvky. Pak existují prvky $a, b \in G$ takové, že $f(a) = c$ a $f(b) = d$. Pak máme $c * d = f(a) * f(b) = f(a \cdot b)$, takže také $c * d \in f(G)$. Dále $\mathbb{1} = f(1)$, takže též $\mathbb{1} \in f(G)$. Konečně pro každý prvek $c \in f(G)$, $c = f(a)$, kde $a \in G$, máme $c^{-1} = f(a)^{-1} = f(a^{-1})$, takže rovněž $c^{-1} \in f(G)$. Je tedy $f(G)$ podgrupa grupy $(H,*)$.

Nechť $(G,\cdot)$ a $(H,*)$ jsou grupy a nechť $f : G \to H$ je zobrazení, které je současně bijekcí množiny G na množinu H a také homomorfismem grupy $(G,\cdot)$ do grupy $(H,*)$. Pak říkáme, že f je **izomorfismus** grupy $(G,\cdot)$ na grupu $(H,*)$. Názorně lze význam tohoto pojmu přiblížit sdělením, že v takovém případě jsou obě grupy $(G,\cdot)$ a $(H,*)$ vlastně jenom kopiemi jedné a téže grupy. O takových dvou grupách pak říkáme, že jsou **izomorfní**.

Příklady. Grupa $(\mathbb{Z}_2, +)$ má dva prvky, totiž třídy $[0]_2$ a $[1]_2$. Množina čísel $\{-1, 1\}$ je zřejmě podgrupou grupy $(\mathbb{Q} - \{0\}, \cdot)$. Takto dostáváme rovněž dvouprvkovou grupu $(\{-1, 1\}, \cdot)$. Lze se přímo přesvědčit, že zobrazení množiny $\mathbb{Z}_2$ na množinu $\{-1, 1\}$

přiřazující třídě $[0]_2$ číslo 1 a třídě $[1]_2$ číslo -1 je izomorfismus grupy $(\mathbb{Z}_2, +)$ na grupu $(\{-1, 1\}, \cdot)$.

Zobrazení $\log : \mathbb{R}^+ \to \mathbb{R}$ přiřazující každému kladnému reálnému číslu x jeho přirozený logaritmus $\log(x)$ je bijekcí množiny $\mathbb{R}^+$ všech kladných reálných čísel na množinu $\mathbb{R}$ všech reálných čísel a současně je to homomorfismus grupy $(\mathbb{R}^+, \cdot)$ na grupu $(\mathbb{R}, +)$, neboť, jak známo, pro libovolná kladná reálná čísla x, y platí $\log(x \cdot y) = \log(x) + \log(y)$. Jde tedy o izomorfismus těchto dvou grup.

Tvrzení. Jsou-li $(G, \cdot)$ a $(H, *)$ grupy a je-li $f : G \to H$ izomorfismus těchto grup, pak také inverzní zobrazení $f^{-1} : H \to G$ je izomorfismem těchto grup.

Důkaz. Skutečně pro libovolná $c, d \in H$ máme

$$f(f^{-1}(c*d)) = c*d = f(f^{-1}(c))*f(f^{-1}(d)) = f(f^{-1}(c)\cdot f^{-1}(d)),$$

neboť f je homomorfismus. Aplikací inverzního zobrazení f^{-1} na první a poslední prvek v této posloupnosti rovností pak obdržíme, že $f^{-1}(c * d) = f^{-1}(c) \cdot f^{-1}(d)$, což potvrzuje, že f^{-1} je rovněž homomorfismus.

Nechť znovu $(G, \cdot)$ a $(H, *)$ jsou grupy a nechť $f : G \to H$ je homomorfismus grupy $(G, \cdot)$ do grupy $(H, *)$. Podle předminulého tvrzení pak obraz $f(G)$ při tomto homomorfismu je podgrupa grupy $(H, *)$. Je tedy dvojice $(f(G), *)$ sama grupou. Je-li navíc zobrazení f prosté, pak lze toto zobrazení chápat jako bijekci množiny G na množinu $f(G)$, a tedy jde o izomorfismus grupy $(G, \cdot)$ na grupu $(f(G), *)$, jež je podgrupou grupy $(H, *)$.

Nyní jsme připraveni dokázat následující **Cayleyho větu**.

Věta. Každá grupa $(G, \cdot)$ je izomorfní některé podgrupě grupy permutací $(S(X), \circ)$ pro nějakou množinu X. Je-li uvedená grupa konečná, může být množina X také konečná.

Důkaz. Ke každému prvku $a \in G$ uvažujme zobrazení $\lambda_a : G \to G$ definované pro každé $g \in G$ předpisem $\lambda_a(g) = a \cdot g$. Toto zobrazení je bijekce, neboť zobrazení $\lambda_{a^{-1}}$ je k němu zobrazením inverzním, jelikož platí $\lambda_a \circ \lambda_{a^{-1}} = id_G = \lambda_{a^{-1}} \circ \lambda_a$, neboť $a \cdot a^{-1} = \mathtt{1} = a^{-1} \cdot a$. Je tedy zobrazení λ_a permutací množiny G. Nyní můžeme definovat zobrazení

$$\Lambda : G \to S(G)$$

tak, že pro každý prvek a položíme $\Lambda(a) = \lambda_a$. Abychom důkaz dokončili, podle komentáře předcházejícího této větě stačí, když ukážeme, že Λ je prostý homomorfismus grupy $(G, \cdot)$ do grupy $(S(G), \circ)$. Fakt, že zobrazení Λ je prosté, plyne z toho, že pro libovolná $a, b \in G$ rovnost $\lambda_a = \lambda_b$ má za důsledek, že $a = \lambda_a(\mathtt{1}) = \lambda_b(\mathtt{1}) = b$, tedy že $a = b$. Zbývá dokázat, že Λ je homomorfismus, čili že pro každá $a, b \in G$ máme $\Lambda(a \cdot b) = \Lambda(a) \circ \Lambda(b)$, tedy že platí

$$\lambda_{a \cdot b} = \lambda_a \circ \lambda_b.$$

Jde o rovnost zobrazení, kterou ověříme, když zkontrolujeme, že obě zobrazení přiřazují každému prvku z G tentýž prvek. Vezměme tedy libovolný prvek $g \in G$. Pak ovšem máme

$$\lambda_{a \cdot b}(g) = a \cdot b \cdot g = a \cdot \lambda_b(g) = \lambda_a(\lambda_b(g)) = (\lambda_a \circ \lambda_b)(g).$$

Je tedy Λ prostý homomorfismus, což znamená, že grupa $(G, \cdot)$ je izomorfní podgrupě $(\Lambda(G), \circ)$ grupy $(S(G), \circ)$.