Učební texty k přednášce ALGEBRAICKÉ STRUKTURY
Michal Marvan, Matematický ústav
Slezská univerzita v Opavě

7. Grupy

Definice. Množina G, na níž existuje binární operace "$\cdot$": $G \times G \to G$, $(a, b) \mapsto a \cdot b$, nulární operace "1" $\in G$ a unární operace "$^{-1}$": $G \to G$, $a \mapsto a^{-1}$ takové, že pro všechny prvky $a, b, c \in G$ platí

1° $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
2° $a \cdot 1 = 1 \cdot a = a$,
3° $a \cdot a^{-1} = a^{-1} \cdot a = 1$

se nazývá *grupa*. Vztah (1) se nazývá *asociativní zákon*. Prvek 1 se nazývá *jednička* grupy. Prvek a^{-1} se nazývá prvek *inverzní* k prvku a.

Definice. Grupa G, která navíc pro všechna $a, b \in G$ splňuje

4° $a \cdot b = b \cdot a$

se nazývá *abelovská* čili *komutativní* grupa. Grupa, která podmínku (4) nesplňuje se nazývá *neabelovská* nebo též *nekomutativní*.

Vidíme, že grupa, tak jak je zde zavedena, je algebra se signaturou $(\cdot, 1, ^{-1})$, přičemž operace $\cdot, 1, ^{-1}$ mají po řadě aritu $2, 0, 1$. Na grupy se proto přirozeně vztahují všechny definice a konstrukce, se kterými jsme se seznámili v předchozích kapitolách.

Tvrzení. (1) *Každá podalgebra grupy je grupa.*
(2) *Každá faktorová algebra grupy je grupa.*
(3) *Součin grup je grupa.*

Důkaz. Je nutno ověřit, že v každé podalgebře a faktorové algebře grupy a v každém součinu grup platí vztahy 1° až 3° z definice grupy. Ověření je snadné a pro všechny tři podmínky podobné, proto se omezíme na ověření druhé z rovností 3°, tj. $a^{-1} \cdot a = 1$, ostatní ponecháme jako jednoduché cvičení. Pro určitost budeme rozlišovat operace na jednotlivých algebrách indexy.

(1) Buď $(H, \cdot_H, 1_H, {}^{-1_H})$ podalgebra v grupě $(G, \cdot_G, 1_G, {}^{-1_G})$. Podle definice podalgebry platí $a \cdot_H b = a \cdot_G b$, $1_H = 1_G$ a $a_H^{-1} = a_G^{-1}$ pro libovolné prvky $a, b \in H$. Proto

$$a_H^{-1} \cdot_H a = a_G^{-1} \cdot_G a = 1_G = 1_H.$$

(2) Buď $(H, \cdot_H, 1_H, {}^{-1_H})$ faktorová algebra grupy G, tj. $H = G/\kappa$ pro nějakou kongruenci κ na grupě G. Víme, že prvky algebry H jsou třídy $[a]_\kappa$ kongruence κ, kde $a \in G$, a že operace faktorové algebry jsou dány předpisem $[a]_\kappa \cdot_H [b]_\kappa = [a \cdot_G b]_\kappa$, $1_H = [1_G]_\kappa$ a $[a]_\kappa{}_H^{-1} = [a_G^{-1}]_\kappa$.

Potom

$$[a]_\kappa{}_H^{-1} \cdot_H [a]_\kappa = [a_G^{-1}]_\kappa \cdot_H [a]_\kappa = [a_G^{-1} \cdot_G a]_\kappa = [1_G]_\kappa = 1_H.$$

(3) Buď $H = G_1 \times G_2$ součin grup G_j, $j = 1, 2$. Prvky v H jsou (a_1, a_2), kde $a_j \in G_j$. Operace jsou dány předpisem $(a_1, a_2) \cdot_H (b_1, b_2) = (a_1 \cdot_{G_1} b_1, a_2 \cdot_{G_2} b_2)$, $1_H = (1_{G_1}, 1_{G_2})$. $(a_1, a_2)_H^{-1} = (a_1{}_{G_1}^{-1}, a_2{}_{G_2}^{-1})$.

Potom

$$\begin{aligned}(a_1, a_2)_H^{-1} \cdot_H (a_1, a_2) &= (a_1{}_{G_1}^{-1}, a_2{}_{G_2}^{-1}) \cdot_H (a_1, a_2) \\ &= (a_1{}_{G_1}^{-1} \cdot_{G_1} a_1, a_2{}_{G_2}^{-1} \cdot_{G_2} a_2) = (1_{G_1}, 1_{G_2}) = 1_H\end{aligned}$$

Analogický důkaz je možno provést pro obecné součiny $\prod_{j\in J} G^{(j)}$ grup.

Definice. Podalgebra grupy se nazývá *podgrupa*. Faktorová algebra grupy se nazývá *faktorová grupa*.

Tvrzení. *Podgrupy, faktorové grupy a součiny komutativních grup jsou komutativní.*

Důkaz. Cvičení.

Příklady. (1) *Číselné grupy* jsou grupa $(\mathbf{C}, +, 0, -)$ a její podgrupy, jako např. $\mathbf{R}, \mathbf{Q}, \mathbf{Z}$. Jsou komutativní.

(2) *Multiplikativní číselné grupy* jsou $\mathbf{C}^* = (\mathbf{C} \setminus \{0\}, \cdot, 1, ^{-1})$ a její podgrupy, jako např. $\mathbf{R}^* = (\mathbf{R} \setminus \{0\}, \cdot, 1, ^{-1})$, $\mathbf{Q}^* = (\mathbf{Q} \setminus \{0\}, \cdot, 1, ^{-1})$.

(3) *Grupy zbytkových tříd* $(\mathbf{Z}_m, +, 0, -)$. Jde o faktorové grupy grupy $(\mathbf{Z}, +, 0, -)$ (viz výše). Jsou komutativní.

(4) *Maticové grupy* jsou podgrupy v $GL(n, P)$, grupě všech regulárních matic typu $n \times n$ nad polem P, vzhledem k obvyklému maticovému násobení a inverzi. Jedničkou je jednotková matice. Například $SL(n, P)$ je podgrupa matic A splňujících $\det A = 1$. Maticové grupy jsou obecně nekomutativní.

(5) *Grupy permutací*: S_n je grupa všech bijekcí $\{1, \ldots, n\} \to \{1, \ldots, n\}$. Pro $n > 1$ je nekomutativní.

(6) *Grupy symetrií* (např. geometrických útvarů).

Dále součiny uvedených grup, jejich podgrupy a faktorové grupy.

Pro prvky grup platí řada jednoduchých, avšak užitečných tvrzení. Uveďme si prozatím několik nejjednodušších. V následujícím tvrzení označují a, b, c, x prvky nějaké grupy G.

Tvrzení. (i) *Nechť $a \cdot b = 1$. Pak $b = a^{-1}$ a současně $a = b^{-1}$.*
(ii) *Zákon o krácení zleva: Jestliže $a \cdot b = a \cdot c$, pak $b = c$.*
(iii) *Zákon o krácení zprava: Jestliže $a \cdot c = b \cdot c$, pak $a = b$.*
(iv) *Rovnice $a \cdot x = b$ s neznámou x má jediné řešení: $x = a^{-1} \cdot b$.*
(v) *Rovnice $x \cdot a = b$ s neznámou x má jediné řešení: $x = b \cdot a^{-1}$.*

Důkaz. Ad (i): Nechť $a \cdot b = 1$. Vynásobme obě strany této rovnosti *zleva* prvkem a^{-1}:

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 1.$$

Výraz na pravé straně je a^{-1}, na levé straně dostaneme postupně $(a^{-1} \cdot a) \cdot b = 1 \cdot b = b$. To jest, $b = a^{-1}$. Druhá rovnost: Cvičení.

Ad (ii)–(v): Cvičení. V tvrzeních (iv) a (v) je nutno dokázat jak existenci, tak jednoznačnost řešení.

Tvrzení. (vi) *Pro všechna $u \in G$ platí $(u^{-1})^{-1} = u$.*
(vii) *Pro všechna $u, v \in G$ platí $(u \cdot v)^{-1} = v^{-1} \cdot u^{-1}$.*

Důkaz. Plyne z (i), položíme-li $a = u$, $b = u^{-1}$, resp. $a = u \cdot v$, $b = v^{-1} \cdot u^{-1}$.

Jak víme, *homomorfismus* grup $(G, \cdot_G, 1_G, \overline{}^{-1_G}) \to (H, \cdot_H, 1_H, \overline{}^{-1_H})$ je zobrazení $f : G \to H$ takové, že platí

(a) $f(a \cdot_G b) = f(a) \cdot_H f(b)$,
(b) $f(1_G) = 1_H$,

(c) $f(a_G^{-1}) = (f(a))_H^{-1}$.
Dokažme si podrobně následující kriterium.

Tvrzení. *K tomu, aby zobrazení $f : G \to H$ bylo homomorfismem stačí, aby byla splněna podmínka* (a), *to jest, aby f byl pologrupový homomorfismus.*

Důkaz. Nechť zobrazení $f : G \to H$ splňuje podmínku (a). Zřejmě v grupě G platí $1_G = 1_G \cdot 1_G$, a proto

$$f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot_H f(1_G)$$

(druhá z rovností platí podle (a)). Po zkrácení zleva prvkem $f(1_G)$ (v grupě H) obdržíme $1_H = f(1_G)$, což je hledaný vztah (b).

Nakonec ze vztahu

$$1_H = f(1_G) = f(a \cdot_G a_G^{-1}) = f(a) \cdot_H f(a_G^{-1})$$

(první z rovností jsme právě dokázali, ostatní jsou jasné) odvodíme, že $f(a_G^{-1}) = (f(a))_H^{-1}$ pro libovolné $a \in G$ (např. podle (i) nahoře), což je hledaný vztah (c).

Pro úplnou jasnost bylo vyznačeno, ke které grupě se ta či ona operace vztahuje. Takový zápis je však méně přehledný, a proto od něj nadále upustíme.

Příklady. (1) Determinant. Zobrazení det : $GL(n, \mathbf{R}) \to \mathbf{R}^*$, které matici přiřazuje její determinant, je homomorfismus grup. Podobně det : $GL(n, \mathbf{C}) \to \mathbf{C}^*$.

(2) Komplexní sdružení $z \mapsto \bar{z}$ je homomorfismus aditivních grup $\mathbf{C} \to \mathbf{C}$ i multiplikativních grup $\mathbf{C}^* \to \mathbf{C}^*$.

(3) Absolutní hodnota $\mathbf{C}^* \to \mathbf{R}^*$ je homomorfismus multiplikativních grup.

(4) Parita jako zobrazení $(S_n, \circ, \mathrm{id}, ^{-1}) \to (\mathbf{Z}_2, +, 0, -)$ je homomorfismus grup.

Tvrzení. *Buď G grupa. Podmnožina $H \subseteq G$ je podgrupa právě tehdy, když je neprázdná a pro každé $a, b \in H$ platí $a \cdot b^{-1} \in H$.*

Důkaz. "⇒": Cvičení.

"⇐": Buď $a \in H$ libovolné (existuje, protože $H \neq \emptyset$). Pak $1 = a \cdot a^{-1} \in H$. Dále pro každé $a \in H$ máme $a^{-1} = 1 \cdot a^{-1} \in H$. Nakonec pro libovolná $a, b \in H$ je $b^{-1} \in H$ a tedy též $a \cdot b = a \cdot (b^{-1})^{-1} \in H$.