Matematický ústav Slezské univerzity v Opavě

Učební texty k přednášce ALGEBRA I, zimní semestr 2002/2003

Michal Marvan

1. Pologrupy, monoidy a grupy

Algebra dvacátého století je nauka o algebraických strukturách. Struktury se osvědčily jako prostředek ke sjednocení a utřídění dosaženého poznání v matematice.

Struktura obecně je vždy zadána na nějaké množině. Algebraická struktura je zpravidla zadána jako jedna či několik algebraických operací. Mezi užitečné algebraické struktury patří již struktury s jednou asociativní binární operací; nazývají se pologrupy. Bohatší jsou monoidy a grupy. Další často se vyskytující struktury poznáme později: okruhy, pole, vektorové prostory a svazy.

Obecně platí úměra: čím bohatší struktura, tím více výsledků pro ni můžeme odvodit, ale tím méně příkladů pro ni nalezneme.

1. Binární operace

1.1. Definice. *Binární operace* na množině A je libovolné zobrazení $A \times A \longrightarrow A$.

Tudíž, zadat binární operaci $*$ na množině A je totéž, co zadat předpis, který libovolné dvojici (x, y) prvků z A (nazývají se operandy) přiřadí nějaký jednoznačně určený prvek z A (výsledek operace), který zpravidla označujeme $x * y$ (symbolem binární operace umístěným mezi operandy). Další často používané symboly binárních operací jsou $\cdot$, $+$, $\circ$. Zápis $a \cdot b$ se často zkracuje na ab.

Příklad. Buď $\mathbf{N} = \{0, 1, 2, \ldots\} \subset \mathbf{Z}$ množina všech přirozených čísel. Zobrazení $\mathbf{N} \times \mathbf{N} \longrightarrow \mathbf{N}$, které dvojici přirozených čísel $(a, b) \in \mathbf{N} \times \mathbf{N}$ přiřazuje aritmetický součet $a + b \in \mathbf{N}$, je binární operace na množině $\mathbf{N}$.

Příklad. Na konečné množině, například $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ je možno zadat operaci „$\odot$“ tabulkou, například

$\odot$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$
$\spadesuit$	$\heartsuit$	$\spadesuit$	$\heartsuit$	$\spadesuit$
$\diamondsuit$	$\heartsuit$	$\heartsuit$	$\diamondsuit$	$\diamondsuit$
$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$

Podle této tabulky například $\spadesuit \odot \clubsuit = \spadesuit$.

1.2. Definice. Řekneme, že binární operace „$*$“ na množině A je *asociativní*, jestliže pro každé tři prvky $a, b, c \in A$ platí

$$a * (b * c) = (a * b) * c.$$

Závorky pak můžeme vynechat a psát prostě $a * b * c$. Podobně $a * b * c * d = a * (b * (c * d)) = ((a * b) * c) * d = (a * (b * c)) * d$ atd.

1.3. Definice. Řekneme, že binární operace „$*$“ na množině A je *komutativní*, jestliže pro každé dva prvky $a, b \in A$ platí

$$a * b = b * a.$$

Cvičení. Ukažte, že operace „$\odot$“ na množině $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ ze shora uvedeného příkladu je asociativní a komutativní.

Návod: S jakou symetrií tabulky je spojena komutativita operace „$\odot$“? Asociativitu prověřte pro každou ze $4^3 = 64$ trojic a, b, c sestavených z prvků $\heartsuit, \spadesuit, \diamondsuit, \clubsuit$ nebo počkejte na pozdější přednášku o svazech.

2. Pologrupy

Asociativní binární operace „$*$“ na množině A zadává *strukturu pologrupy*:

2.1. Definice. (1) Řekneme, že je dána *pologrupa* $(A, *)$, je-li dána
– množina A;
– binární operace „$*$“ na A, která je asociativní.
(2) Pologrupa $(A, *)$ se nazývá *komutativní*, je-li operace „$*$“ navíc komutativní.

Je též možno říci, že *A je pologrupa vzhledem k operaci „$*$“*. Je-li binární operace určena kontextem, lze místo o pologrupě $(A, *)$ hovořit prostě o pologrupě A.

Příklad. Různé příklady komutativních pologrup poskytují známé číselné obory. Máme pologrupy $(\mathbf{N}, +)$, $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ resp. $(\mathbf{C}, +)$ přirozených, celých, racionálních, reálných resp. komplexních čísel, vzhledem k operaci obvyklého sčítání. Máme též pologrupy $(\mathbf{N}, \cdot)$, $(\mathbf{Z}, \cdot)$, $(\mathbf{Q}, \cdot)$, $(\mathbf{R}, \cdot)$ resp. $(\mathbf{C}, \cdot)$ vzhledem k operaci obvyklého násobení.

Pologrupa s binární operací označenou symbolem „$+$“ se nazývá *aditivní*. Dodržuje se zásada, že *aditivně se zapisují pouze komutativní pologrupy.* Pologrupa s binární operací označenou symbolem „$\cdot$“ se nazývá *multiplikativní*. (Jde o aditivní či multiplikativní *způsob zápisu*.)

2.2. Příklad. Prodejní automat rozeznává tři možné vstupy, které označíme po řadě ◯ (mince), □ (tlačítko) a ⊤ (zásah operátora). Nechť $A = \{\bigcirc, \square, \top\}$, označme S_A množinu všech konečných a neprázdných posloupností s sestavených ze symbolů ◯, □, ⊤. Zaveďme operaci „$\cdot$“ na množině S_A tak, že pro dvě posloupnosti $s, t \in S_A$ bude $s{\cdot}t$ posloupnost vzniklá napojením posloupnosti t za posloupnost s. Například: ◯⊤$\cdot$□⊤ = ◯⊤□⊤.

Operace „$\cdot$“ na množině S_A je zřejmě asociativní (prověřte), ale *není* komutativní. Dostáváme tak příklad nekomutativní pologrupy.

2.3. Příklad. Buď X libovolná neprázdná množina. Uvažujme o množině X^X všech zobrazení $X \longrightarrow X$. Pro skládání zobrazení „$\circ$“ platí asociativní zákon, tudíž $(X^X, \circ)$ je pologrupa.

Cvičení. Dokažte, že pologrupa $(X^X, \circ)$ je komutativni právě tehdy, když množina X má jeden prvek.

Návod: (a) Má-li množina X jediný prvek, $X = \{a\}$, pak X^X má též jediný prvek, a sice zobrazení $\mathrm{id}_X : a \longmapsto a$.

(b) Obsahuje-li X dva různé prvky, řekněme $c_1 \neq c_2$, zaveďte zobrazení f_1 jako $x \longmapsto c_1$ pro každé $x \in X$ (konstantní zobrazení s hodnotou c_1) a podobně f_2 jako $x \longmapsto c_2$ pro každé $x \in X$. Ukažte, že $f_1 \circ f_2 \neq f_2 \circ f_1$.

Cvičení. Buď A libovolná neprázdná množina, buď na A zadána operace „o_2“ („druhý operand“) předpisem $a\, o_2\, b = b$.

(1) Dokažte, že (A, o_2) je pologrupa.

(2) Dokažte, že pologrupa (A, o_2) je komutativní právě tehdy, když množina A má jeden prvek.

3. Monoidy

3.1. Definice. Buď „$*$“ binární operace na množině A. Prvek $e \in A$ se nazývá *neutrální prvek* vzhledem k operaci „$*$“, jestliže pro každý prvek $a \in A$ platí

$$a * e = a = e * a.$$

Cvičení. Ověřte, že v naší pologrupě $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ s operaci „$\odot$“ je prvek $\clubsuit$ neutrálnim prvkem.

3.2. Tvrzení. *V množině A se zadanou binární operací „$*$“ existuje nejvýše jeden neutrální prvek.*

3.3. Důkaz. Jsou-li e', e'' dva neutrální prvky, pak $e'' = e' * e'' = e'$. První rovnost platí, protože e' je neutrální prvek, druhá rovnost platí, protože e'' je neutrální prvek.

3.4. Definice. *Monoid* $(A, *, e)$ je pologrupa $(A, *)$ s neutrálním prvkem e. Monoid $(A, *, e)$ se nazývá *komutativní*, je-li pologrupa $(A, *)$ komutativní.

Připomeňme, že podle posledního tvrzení mají dva monoidy se stejnou binární operací na stejné množině i stejné neutrální prvky.

Příklad. Máme aditivní monoidy $(\mathbf{N}, +, 0)$, $(\mathbf{Z}, +, 0)$, $(\mathbf{Q}, +, 0)$, $(\mathbf{R}, +, 0)$, $(\mathbf{C}, +, 0)$ a multiplikativní monoidy $(\mathbf{N}, \cdot, 1)$, $(\mathbf{Z}, \cdot, 1)$, $(\mathbf{Q}, \cdot, 1)$, $(\mathbf{R}, \cdot, 1)$, $(\mathbf{C}, \cdot, 1)$. Všechny jsou komutativní.

Neutrální prvek v aditivním monoidu se obvykle označuje symbolem 0, neutrální prvek v multiplikativním monoidu se obvykle označuje symbolem 1.

Příklad. Buď X libovolná neprázdná množina. Pak $(X^X, \circ, \mathrm{id}_X)$ je monoid. Je nekomutativní, pokud X má více než jeden prvek (cvičení).

Příklad. Buď A konečná množina, kterou nazveme *abeceda*. Definujme *slovo* nad abecedou A jako konečnou posloupnost $\alpha = a_1 a_2 \cdots a_n$, $n \geq 0$, prvků $a_i \in A$. Číslo n se nazývá *délka* slova, značí se $\ell(\alpha)$. Pro $n = 0$ dostáváme *prázdné slovo*, značí se ω a máme $\ell(\omega) = 0$.

Množina všech neprázdných slov nad abecedou A se značí S_A^*, množina všech slov nad abecedou A včetně prázdného se značí S_A.

Na množině S_A^* zavedeme binární operaci. Jsou-li $\alpha = a_1 a_2 \cdots a_p$, $\beta = b_1 b_2 \cdots b_q$ dvě slova, pak se slovo $a_1 a_2 \cdots a_p b_1 b_2 \cdots b_q$ značí $\alpha \cdot \beta$. Nazývá se *složení* slov α a β.

Na množině S_A zavedeme binární operaci „$\cdot$“ stejně jako na množině S_A^* a navíc položíme $\alpha \cdot \omega = \omega \cdot \alpha = \alpha$ pro každé $\alpha \in S_A$.

Pro libovolná slova $\alpha, \beta, \gamma \in S_A$ pak platí asociativní zákon (ověřte) a navíc existuje neutrální prvek, a sice ω. Dostáváme monoid $(S_A, \cdot, \omega)$. Nazývá se *monoid slov* nad abecedou A.

Cvičení. Ukažte, že $(S_A^*, \cdot)$ je pologrupa ale není monoid.

Návod: Pro libovolná slova α, β platí $\ell(\alpha \cdot \beta) = \ell(\alpha) + \ell(\beta)$. Připusťte, že β je neutrální prvek.

Cvičení. Přidání neutrálního prvku k pologrupě. Buď $(A, *)$ pologrupa. Vyberme jakýkoliv prvek e, který neleží v A. Označme $A^\bullet = A \cup \{e\}$. Zaveďme zobrazení $A^\bullet \times A^\bullet \longrightarrow A^\bullet$ předpisem

$$(a, b) \longmapsto \begin{cases} a * b & \text{jestliže } a, b \in A, \\ a & \text{jestliže } a \in A,\ b = e, \\ b & \text{jestliže } b \in A,\ a = e, \\ e & \text{jestliže } a = b = e. \end{cases}$$

(1) Ukažte, že $A^\bullet$ s touto binární operací je monoid s neutrálním prvkem e.
(2) Pokud pologrupa $(A, *)$ již měla neutrální prvek, kolik neutrálních prvků bude mít $A^\bullet$?
(3) Ověřte, že ${S_A^*}^\bullet = S_A$.

4. Grupy

4.1. Definice. Buď $(A, *, e)$ monoid. Prvek $a \in A$ se nazývá *invertibilní*, jestliže existuje prvek $b \in B$ takový, že

$$a * b = b * a = e.$$

Prvek b se nazývá *inverzní* k prvku a.

4.2. Tvrzení. *Buď $(A, *, e)$ monoid. Je-li prvek $a \in A$ invertibilní, pak k němu existuje právě jeden prvek inverzní.*

4.3. Důkaz. Existence: Alespoň jeden inverzní prvek k prvku a existuje, protože a je invertibilní.

Jednoznačnost: Připusťme, že dva prvky $b', b'' \in A$ jsou inverzní k prvku a. Pak máme

$$b' = b' * e = b' * (a * b'') = (b' * a) * b'' = e * b'' = b''.$$

Vidíme, že každé dva inverzní prvky k prvku a se rovnají.

Cvičení. Vysvětlete každou z rovností v předchozím důkazu.

4.4. Definice. Monoid, jehož každý prvek je invertibilní, se nazývá *grupa*.

Tudíž, v grupě ke každému prvku a existuje právě jeden prvek inverzní. Značí se obvykle a^{-1}, pouze v aditivním zápisu se užívá označení $-a$.

S grupou $(A, *, e)$ je pak spojeno zobrazení $A \longrightarrow A$, $a \longmapsto a^{-1}$ a taková grupa se označuje $(A, *, e, {}^{-1})$; v aditivním zápisu obvykle $(A, +, 0, -)$.

Příklady. (1) Aditivní grupy $(\mathbf{Z}, +, 0, -)$, $(\mathbf{Q}, +, 0, -)$, $(\mathbf{R}, +, 0, -)$, $(\mathbf{C}, +, 0, -)$ celých, racionálních, reálných a komplexních čísel.

(2) Multiplikativní grupy $(\mathbf{Q}^*, \cdot, 1, {}^{-1})$, $(\mathbf{R}^*, \cdot, 1, {}^{-1})$ a $(\mathbf{C}^*, \cdot, 1, {}^{-1})$ nenulových racionálních, nenulových reálných a nenulových komplexních čísel. Zde $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$ a podobně v ostatních případech.

(3) Je-li X neprázdná množina, pak *symetrická grupa* $S(X)$ je množina všech bijekcí $X \longrightarrow X$, spolu s operacemi „$\circ$“ skládání bijekccí, identickou bijekcí id_X jako neutrálním prvkem a inverzí „$^{-1}$“. Je nekomutativní, má-li X více než dva prvky.

(4) Na libovolné jednoprvkové množině existuje jediná struktura grupy. V multiplikativním zápisu: jediný prvek je nutně totožný s jedničkou grupy 1, operace jsou nutně zadány předpisem $1 \cdot 1 = 1$ a $1^{-1} = 1$.

4.5. Poznámka. Každé zobrazení $A \longrightarrow A$ se nazývá *unární operace* na A. Kromě toho se zavádí *nulární operace* na množině A jako libovolný vybraný prvek množiny A. Na grupě $(A, *, e)$ pak máme kromě binární operace „$*$“ i unární operaci „$^{-1}$“ a nulární operaci e.

Cvičení. (1) Dokažte, že monoid $(\mathbf{Z}, \cdot, 1)$ není grupa.
Návod: Dokažte, že rovnice $2x = 1$ nemá řešení v oboru celých čísel.

(2) Dokažte podrobně, že $(\mathbf{Q}^*, \cdot, 1, {}^{-1})$, $(\mathbf{R}^*, \cdot, 1, {}^{-1})$ a $(\mathbf{C}^*, \cdot, 1, {}^{-1})$ jsou grupy.
Návod: Považujte za dokázaný fakt, že ke každému nenulovému racionálnímu (reálnému, komplexnímu) číslu a existuje převrácené číslo a^{-1} splňující $a \cdot a^{-1} = 1$. Pro $a, b \in \mathbf{Q}^*$ dokažte (sporem), že $a \cdot b \in \mathbf{Q}^*$ a že $a^{-1} \in \mathbf{Q}^*$. Podobně pro $\mathbf{R}^*$ a $\mathbf{C}^*$.

Následující formule jsou užitečné při počítání v grupách:

4.6. Lemma. *Buď $(G, *, 1, {}^{-1})$ grupa. Pak pro libovolná $a, b \in G$ platí*:

(1) *Jestliže $a * b = 1$, pak $b = a^{-1}$, $a = b^{-1}$;*
(2) $1^{-1} = 1$;
(3) $(a^{-1})^{-1} = a$;
(4) $(a * b)^{-1} = b^{-1} * a^{-1}$.

4.7. Důkaz. (1) Nechť $a * b = 1$, pak $b = 1 * b = a^{-1} * a * b = a^{-1} * 1 = a^{-1}$. Podobně druhá rovnost (cvičení).

(2) Plyne z (1) a rovnosti $1 * 1 = 1$.
(3) Plyne z (1) a rovnosti $a^{-1} * a = 1$.
(4) Plyne z (1) a rovnosti $a * b * b^{-1} * a^{-1} = 1$.

5. Podpologrupy

Algebraické podstruktury jsou podmnožiny algebraických struktur, které jsou „uzavřené“ vzhledem ke *všem* algebraickým operacím, předepsaným pro danou strukturu. Samy se pak stávají algebraickými strukturami téhož typu.

5.1. Definice. Buď $(A, *)$ pologrupa, buď $B \subseteq A$ podmnožina. Nechť platí implikace:
1° jestliže $b_1, b_2 \in B$, pak $b_1 * b_2 \in B$.
Potom se B nazývá *podpologrupa* pologrupy A.

Předpisem $(b_1, b_2) \longmapsto b_1 * b_2$ je pak zadáno zobrazení $B \times B \longrightarrow B$, tj. binární operace na B. Označuje se zpravidla týmž symbolem $*$. Pro všechny prvky z B platí asociativní zákon (protože platí dokonce pro všechny prvky z A). Můžeme proto hovořit o podpologrupě $(B, *)$. Kratší označení podpologrupa B je ovšem postačující.

Každá pologrupa $(A, *)$ obsahuje jako podpologrupy sama sebe a prázdnou pologrupu $\emptyset$. Tyto podpologrupy se nazývají *triviální* podpologrupy.

Příklad. (1) Máme do sebe vložené aditivní pologrupy $(\mathbf{N}, +) \subset (\mathbf{Z}, +) \subset (\mathbf{Q}, +) \subset (\mathbf{R}, +) \subset (\mathbf{C}, +)$ i multiplikativní pologrupy $(\mathbf{N}, \cdot) \subset (\mathbf{Z}, \cdot) \subset (\mathbf{Q}, \cdot) \subset (\mathbf{R}, \cdot) \subset (\mathbf{C}, \cdot)$.

(2) Žádná z aditivních pologrup $(\mathbf{N}, +) \subset (\mathbf{Z}, +) \subset (\mathbf{Q}, +) \subset (\mathbf{R}, +) \subset (\mathbf{C}, +)$ není podpologrupou v žádné z multiplikativních pologrup $(\mathbf{N}, \cdot) \subset (\mathbf{Z}, \cdot) \subset (\mathbf{Q}, \cdot) \subset (\mathbf{R}, \cdot) \subset (\mathbf{C}, \cdot)$, ani naopak. Důvodem je odlišnost algebraických operací.

Cvičení. Uvažujme o pologrupě $(S_A, \cdot)$ všech konečných a neprázdných posloupností sestavených z prvků množiny $A = \{ \bigcirc, \square, \top \}$. Ukažte, že následující podmnožiny jsou podpologrupy:
(1) Podmnožina všech posloupností, zakončených symbolem $\top$.
(2) Podmnožina všech posloupností, v nichž po každém $\bigcirc$ následuje $\top$.
(3) Podmnožina všech posloupností, obsahujících alespoň jeden symbol $\bigcirc$.
(4) Podmnožina všech posloupností, obsahujících sudý počet symbolů $\bigcirc$.
(5) Podmnožina všech posloupností, neobsahujících žádný symbol $\bigcirc$.
Ukažte, že následující podmnožiny nejsou podpologrupy:
(6) Podmnožina všech posloupností, jejichž první symbol je shodný s posledním.
(7) Podmnožina všech posloupností, v nichž po $\top$ nenásleduje $\square$.
(8) Podmnožina všech posloupností, kde na sudých místech jsou $\top$.

Cvičení. Uvažujme o pologrupě $(X^X, \circ)$ všech zobrazení $X \longrightarrow X$. Ukažte, že následující podmnožiny jsou podpologrupy:
(1) Podmnožina všech injektivních zobrazení $X \longrightarrow X$.
(2) Podmnožina všech surjektivních zobrazení $X \longrightarrow X$.
(3) Podmnožina všech bijektivních zobrazení $X \longrightarrow X$.
$(1')$ Podmnožina všech neinjektivních zobrazení $X \longrightarrow X$.
$(2')$ Podmnožina všech nesurjektivních zobrazení $X \longrightarrow X$.
Nechť X má alespoň tři prvky. Ukažte, že následující podmnožiny nejsou podpologrupy:
(4) Podmnožina všech zobrazení $f : X \longrightarrow X$, která splňují $f \circ f = \mathrm{id}_X$.
$(4')$ Podmnožina všech zobrazení $f : X \longrightarrow X$, která nesplňují $f \circ f = \mathrm{id}_X$.
Jak je tomu v případě, že X má právě dva prvky?

Problém k řešení. Pro které množiny X je množina všech nebijektivních zobrazení $X \longrightarrow X$ podpologrupa v X^X?

Cvičení. Uvažujme o pologrupě (A, o_2)“ („druhý operand“). Dokažte, že každá podmnožina $B \subseteq A$ je podpologrupa.

6. Podmonoidy

Podmonoidy jsou podpologrupy, které navíc obsahují i neutrální prvek.

6.1. Definice. Buď $(A, *, e)$ monoid, buď B podmnožina v A. Nechť platí
1° jestliže $b_1, b_2 \in B$, pak $b_1 * b_2 \in B$
2° $e \in B$.
Potom se B nazývá *podmonoid* monoidu A.

Prvek $e \in B$ je potom neutrálním prvkem v pologrupě $(B, *)$, načež $(B, *, e)$ je rovněž monoid.

Každý monoid $(A, *, e)$ obsahuje jako podmonoidy sama sebe a monoid $(\{e\}, *, e)$. Tyto podmonoidy se nazývají *triviální* podmonoidy.

Příklad. Máme do sebe vložené aditivní monoidy $(\mathbf{N}, +, 0) \subset (\mathbf{Z}, +, 0) \subset (\mathbf{Q}, +, 0) \subset (\mathbf{R}, +, 0) \subset (\mathbf{C}, +, 0)$ resp. multiplikativní pologrupy $(\mathbf{N}, \cdot, 1) \subset (\mathbf{Z}, \cdot, 1) \subset (\mathbf{Q}, \cdot, 1) \subset (\mathbf{R}, \cdot, 1) \subset (\mathbf{C}, \cdot, 1)$.

Cvičení. Uvažujme o monoidu $(S_A^*, \cdot, \omega)$ všech konečných posloupností sestavených z prvků množiny $A = \{\bigcirc, \square, \sqcap\}$ včetně prázdné posloupnosti ω. Ukažte, že následující podmnožiny jsou podmonoidy:
(2*) Podmnožina všech posloupností, v nichž po $\bigcirc$ vždy následuje $\sqcap$.
(4*) Podmnožina všech posloupností, obsahujících sudý počet symbolů $\bigcirc$.
(5*) Podmnožina všech posloupností, neobsahujících žádný $\bigcirc$.
Ukažte, že následující podmnožina *není* podmonoid:
(1*′) Podmnožina všech posloupností, zakončených symbolem $\sqcap$.

Cvičení. Uvažujme o monoidu $(X^X, \circ, \mathrm{id}_X)$ všech zobrazení $X \longrightarrow X$. Ukažte, že následující podmnožiny jsou podmonoidy:
(1) Podmnožina všech injektivních zobrazení $X \longrightarrow X$.
(2) Podmnožina všech surjektivních zobrazení $X \longrightarrow X$.
(3) Podmnožina všech bijektivních zobrazení $X \longrightarrow X$.
Ukažte, že následující podmnožiny *nejsou* podmonoidy:
$(1', 2')$ Podmnožina všech neinjektivních resp. nesurjektivních zobrazení $X \longrightarrow X$.

6.2. Upozornění. Podpologrupa B v monoidu A může být sama o sobě monoidem a přitom nebýt podmonoidem v A.

Příklad. Nechť $A = \{\spadesuit, \heartsuit\}$ s operací „$\odot$“ zadanou tabulkou

$\odot$	$\heartsuit$	$\spadesuit$
$\heartsuit$	$\heartsuit$	$\heartsuit$
$\spadesuit$	$\heartsuit$	$\spadesuit$

Pak je $\spadesuit$ neutrální prvek a $(A, \odot, \spadesuit)$ je monoid. Podmnožina $B = \{\heartsuit\}$ je uzavřená na operaci $\odot$, takže $(B, \odot)$ je podpologrupa. Navíc má pologrupa $(B, \odot)$ neutrální prvek $\heartsuit$, takže $(B, \odot, \heartsuit)$ je monoid. Současně však $(B, \odot, \heartsuit)$ není podmonoid v monoidu $(A, \odot, \spadesuit)$, protože mají odlišné neutrální prvky.

7. Podgrupy

Podgrupa B je podmonoid, který s každým svým prvkem b obsahuje i prvek b^{-1} k němu inverzní. Opět je jasné, že podgrupa je sama grupou.

7.1. Definice. Buď $(A, *, e, {}^{-1})$ grupa, buď $B \subseteq A$ podmnožina. Nechť platí
1° jestliže $b_1, b_2 \in B$, pak $b_1 * b_2 \in B$;
2° $e \in B$
3° jestliže $b \in B$, pak $b^{-1} \in B$.

Potom se B nazývá *podgrupa* grupy A.

Každá grupa $(A, *, e, {}^{-1})$ obsahuje jako podgrupy sama sebe a grupu $(\{e\}, *, e, {}^{-1})$. Tyto podgrupy se nazývají *triviální* podgrupy.

Příklad. Máme do sebe vložené aditivní podgrupy $(\mathbf{Z}, +, 0, -) \subset (\mathbf{Q}, +, 0, -) \subset (\mathbf{R}, +, 0, -) \subset (\mathbf{C}, +, 0, -)$ resp. multiplikativní podgrupy $(\mathbf{Q}^*, \cdot, 1, {}^{-1}) \subset (\mathbf{R}^*, \cdot, 1, {}^{-1}) \subset (\mathbf{C}^*, \cdot, 1, {}^{-1})$.

Cvičení. (1) Ukažte, že dvouprvková množina $\{-1, 1\}$ je podgrupa multiplikativní grupy $\mathbf{R}^*$.
(2) Ukažte, že množina $S = \{z \in \mathbf{C} \mid |z| = 1\}$ je podgrupa multiplikativní grupy $\mathbf{C}^*$.

Podstruktury, které jsme zatím poznali, i ty, které ještě poznáme, vykazují určité shodné vlastnosti. Důkazy následujících tvrzení jsou snadná cvičení.

7.2. Tvrzení. 1. *Buď $(A, *)$ pologrupa, buď $(B, *)$ podpologrupa v $(A, *)$ a buď $(C, *)$ podpologrupa v $(B, *)$. Pak $(C, *)$ je podpologrupa v $(A, *)$.*
2. *Buď $(A, *)$ pologrupa, buďte $(B, *)$ a $(C, *)$ podpologrupy v $(A, *)$. Pak je $(B \cap C, *)$ podpologrupa v $(A, *)$.*
Analogická tvrzení platí též pro podmonoidy a podgrupy.

8. Podgrupy aditivní grupy Z

Jednou z algebraických úloh je popsat všechny podstruktury dané struktury. Vyřešíme ji pro aditivní grupu $\mathbf{Z} = (\mathbf{Z}, +, 0, -)$. Pro přirozené číslo $m \in \mathbf{N}$ označme

$$m\mathbf{Z} = \{mk \mid k \in \mathbf{Z}\} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}.$$

Ukážeme, že podmnožinami $m\mathbf{Z}$ jsou vyčerpány všechny podgrupy grupy $\mathbf{Z}$.

8.1. Tvrzení. *Podmnožiny $m\mathbf{Z} \subseteq \mathbf{Z}$ jsou podgrupy v grupě $\mathbf{Z}$ a jiné podgrupy v grupě $\mathbf{Z}$ nejsou.*

8.2. Důkaz. Ukažme, že podmnožiny $m\mathbf{Z}$ jsou podgrupy. Jsou-li km, lm libovolné dva prvky množiny $m\mathbf{Z}$, pak $km + lm = (k + l)m$ je rovněž prvek množiny $m\mathbf{Z}$, čímž je dokázána uzavřenost na binární operaci sčítání. Neutrální prvek 0 grupy $\mathbf{Z}$ také leží v každé z množin $m\mathbf{Z}$. Nakonec, je-li km libovolný prvek množiny $m\mathbf{Z}$, pak $-(km) = (-k)m$ je rovněž prvek množiny $m\mathbf{Z}$, čímž je dokázána uzavřenost na inverzní (opačné) prvky.

Nyní dokažme, že každá podgrupa $B \subseteq \mathbf{Z}$ je shodná s některou podgrupou $m\mathbf{Z}$. Jistě $0 \in B$ (podle definice B obsahuje neutrální prvek). Rozeznávejme dva případy:

a) $B = \{0\}$. Pak $B = 0\mathbf{Z}$ (případ $m = 0$) a jsme hotovi.

b) $B \neq \{0\}$. Pak tedy existuje číslo $b \in B$, různé od nuly. Navíc existuje *kladné* číslo $b_+ \in B$. Skutečně, je-li výše zmíněné číslo $b \in B$ kladné, položíme $b_+ = b$, je-li naopak záporné, položíme $b_+ = -b$ (inverzní prvek $-b$ je číslo kladné a rovněž leží v B, protože B je podgrupa). A nakonec, existuje *nejmenší kladné číslo* $m \in B$, protože v neprázdné množině kladných celých čísel vždy existuje nejmenší číslo.

Dokažme, že takto určené číslo m je hledané číslo, pro něž $m\mathbf{Z} = B$. Ukažme nejdříve, že $m\mathbf{Z} \subseteq B$. Již víme, že $0 \in B$ a $m \in B$. Matematickou indukcí se snadno dokáže, že $km = (k-1)m + m$ leží v B pro každé kladné $k \in \mathbf{N}$. Pak ovšem i inverzní prvky $-km$ leží v B, a tím je ukázáno, že všechny prvky množiny $m\mathbf{Z}$ leží v B.

Zbývá dokázat inkluzi $B \subseteq m\mathbf{Z}$. O libovolně zvoleném prvku $b \in B$ ukažme, že $b \in m\mathbf{Z}$. Proveďme celočíselné dělení číslem $m \neq 0$ s částečným podílem q a zbytkem r:

$$b = mq + r, \qquad 0 \leq r < m.$$

Pak $r = b - mq = b + (-q)m$ je rovněž prvek podgrupy B. Kdyby $r \neq 0$, pak by r bylo kladným prvkem množiny B, menším než prvek m, což je v rozporu s definicí prvku m. Proto $r = 0$, načež $b = mq$, a tedy $b \in m\mathbf{Z}$, což se mělo ukázat.