

5. GRUPY

5.1. Binární operace

Definice 5.1.1. *Binární operace* na množině X je libovolné zobrazení $X \times X \rightarrow X$.

Jedná se tedy o zobrazení, které každé uspořádané dvojici prvků z X přiřazuje nějaký prvek z X . Binární operace se často označují symboly $*$, $+$, $\cdot$, $\circ$ a hodnota takového zobrazení označeného například $*$ v bodě (x, y) se označuje $x * y$ (místo $*(x, y)$).

Příklad. (1) Bud' $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ množina všech celých nezáporných čísel. Zobrazení $+: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$, které uspořádané dvojici $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$ celých nezáporných čísel přiřadí jejich součet $x + y \in \mathbb{N}_0$, je binární operace na $\mathbb{N}_0$.

(2) Součet a součin na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(3) Na množině $\mathbb{R}^2$ všech uspořádaných dvojic reálných čísel binární operace sčítání:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2).$$

(4) Na konečné množině lze zadat binární operaci tabulkou. Například, nechť $X = \{0, 1, 2\}$ a binární operace $+$ na X je zadána takto

$$\begin{array}{c|ccc} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array} \quad \text{tedy například } 1 + 2 = 0.$$

(5) Množina $\mathcal{M}_{m \times n}(P)$ matic stejného typu s operací součet matic.

(6) Množina $\mathcal{M}_n(P)$ čtvercových matic stejného typu s operací součin matic.

(7) Množina $P[x]$ všech polynomů s operací součet nebo součin polynomů.

(8) Množina X^X všech zobrazení $X \rightarrow X$ s operací o skládání zobrazení.

(9) Bud' X množina. Označme $P(X)$ množinu všech podmnožin množiny X . Sjednocení, průnik a symetrický rozdíl množin jsou binární operace na množině $P(X)$. $\square$

Definice 5.1.2. Binární operace $*$ na množině X je *asociativní*, jestliže pro každé $x, y, z \in X$ platí

$$x * (y * z) = (x * y) * z.$$

Můžeme tedy psát bez závorek $x * y * z$.

Definice 5.1.3. Binární operace $*$ na množině X je *komutativní*, jestliže pro každé $x, y \in X$ platí

$$x * y = y * x.$$

Příklad. (1) Součet a součin na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ jsou asociativní i komutativní.

(2) Součet na množině $\mathbb{R}^2$ je asociativní i komutativní.

(3) Součet matic na množině $\mathcal{M}_{m \times n}(P)$ je asociativní i komutativní.

- (4) Součin matic na množině $\mathcal{M}_n(P)$ je asociativní, ale není komutativní.
 (5) Součet a součin polynomů na množině $P[x]$ jsou asociativní i komutativní.
 (6) Skládání zobrazení na množině X^X je asociativní. Komutativní je právě tehdy, když X je jednoprvková množina (cvičení).
 (7) Sjednocení, průnik a symetrický rozdíl množin na množině $P(X)$ jsou asociativní i komutativní. $\square$

Definice 5.1.4. Buď $*$ binární operace na množině X . Prvek $e \in X$ je *neutrální prvek* operace $*$, jestliže pro každý prvek $x \in X$ platí

$$x * e = x = e * x.$$

Tvrzení 5.1.1. Každá binární operace má nejvýše jeden neutrální prvek.

Důkaz. Jsou-li e_1, e_2 neutrální prvky operace $*$, pak $e_2 = e_1 * e_2 = e_1$. $\square$

- Příklad.** (1) Neutrální prvek operace součet na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je 0.
 (2) Neutrální prvek operace součin na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je 1.
 (3) Neutrální prvek operace součet na množině $\mathbb{R}^2$ je $(0, 0)$.
 (4) Neutrální prvek operace součet matic na množině $\mathcal{M}_{m \times n}(P)$ je nulová matice příslušného typu, tedy $0_{m \times n}$.
 (5) Neutrální prvek operace součin matic na množině $\mathcal{M}_n(P)$ je jednotková matice příslušného typu, tedy E_n .
 (6) Neutrální prvek operace součet polynomů na množině $P[x]$ je polynom 0.
 (7) Neutrální prvek operace součin polynomů na množině $P[x]$ je polynom 1.
 (8) Neutrální prvek operace skládání zobrazení na množině X^X je identita id_X .
 (9) Neutrální prvek operace sjednocení množin na množině $P(X)$ je $\emptyset$.
 (10) Neutrální prvek operace průnik množin na množině $P(X)$ je X .
 (11) Neutrální prvek operace symetrický rozdíl množin na množině $P(X)$ je $\emptyset$. $\square$

Definice 5.1.5. Buď $*$ binární operace na množině X , $e \in X$ její neutrální prvek. Prvek $x \in X$ je *invertibilní*, jestliže existuje prvek $y \in X$ takový, že

$$x * y = y * x = e.$$

Potom y je *inverzní prvek* nebo *inverze* k prvku x vzhledem k operaci $*$.

Tvrzení 5.1.2. Každý prvek množiny s asociativní binární operací má vzhledem k této operaci nejvýše jeden inverzní prvek.

Důkaz. Je-li e neutrální prvek operace $*$ a jsou-li y_1, y_2 inverzní prvky k prvku x , pak

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2. \quad \square$$

Inverzní prvek k prvku x se obvykle značí x^{-1} . Pouze u operace $+$ se značí $-x$ a říká se mu *opačný*.

Cvičení. Přímou z definice inverzního prvku vyplývá, že

$$e^{-1} = e \quad \text{a} \quad (x^{-1})^{-1} = x. \quad \square$$

- Příklad.** (1) Inverzní prvek k číslu x vzhledem k operaci součet na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je číslo opačné $-x$ (pokud v příslušné množině existuje).
- (2) Inverzní prvek k číslu x vzhledem k operaci součin na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je převrácená hodnota x^{-1} (pokud v příslušné množině existuje).
- (3) Inverzní prvek k dvojici $(x, y) \in \mathbb{R}^2$ vzhledem k operaci součet je $(-x, -y)$.
- (4) Inverzní prvek k matici A vzhledem k operaci součet matic na množině $\mathcal{M}_{m \times n}(P)$ je opačná matice $-A$.
- (5) Inverzní prvek k matici A vzhledem k operaci součin matic na množině $\mathcal{M}_n(P)$ je inverzní matice A^{-1} (je-li A invertibilní).
- (6) Inverzní prvek k zobrazení $f: X \rightarrow X$ vzhledem k operaci skládání zobrazení na množině X^X je inverzní zobrazení f^{-1} , pokud toto inverzní zobrazení existuje.
- (7) Inverzní prvek k množině $Y \in P(X)$ vzhledem k operaci symetrický rozdíl množin na množině $P(X)$ je Y . $\square$

Příklad. Na množině $\{0, 1, 2\}$ mějme binární operaci $*$ zadanou tabulkou

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	0

Neutrální prvek operace $*$ je 0 a

$$1 * 2 = 2 * 1 = 0 \quad \text{a} \quad 2 * 2 = 0.$$

Čísla 1 a 2 jsou inverzní prvky k 2. Podle Tvzení 5.1.2 to znamená, že operace $*$ není asociativní. A skutečně, například,

$$(1 * 1) * 2 = 2 * 2 = 0 \quad \text{zatímco} \quad 1 * (1 * 2) = 1 * 0 = 1. \quad \square$$

5.2. Grupy

Definice 5.2.1. Množina G s binární operací $*$: $G \times G \rightarrow G$ je *grupa*, jestliže

- (1) operace $*$ je asociativní,
- (2) v množině G je neutrální prvek operace $*$,
- (3) množina G s každým prvkem obsahuje také prvek k němu inverzní vzhledem k operaci $*$.

Je-li navíc operace $*$ komutativní, grupa G je také *komutativní*.

Grupa G s binární operací $*$, neutrálním prvkem e a označením inverzního prvku $^{-1}$ se někdy zapisuje $(G, *, e, ^{-1})$, někdy jen $(G, *)$ a je-li z kontextu zřejmé, o jakou operaci se jedná, někdy se hovoří jen o grupě G .

Grupa s binární operací označenou $+$ se nazývá *aditivní* (používá se pouze u komutativních grup). Grupa s binární operací označenou $\cdot$ se nazývá *multiplikativní*.

Označme $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ a obdobně v případech $\mathbb{R}^*, \mathbb{C}^*$.

- Příklad.** (1) Množina $\mathbb{Z}$ s operací součet je grupa. Stejně tak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- (2) Množina $\mathbb{N}_0$ s operací součet není grupa.
- (3) Množina $\mathbb{Q}^*$ s operací součin je grupa. Stejně tak $\mathbb{R}^*, \mathbb{C}^*, \mathbb{R}_+$ (kladná reálná čísla).
- (4) Množina $\mathbb{Z} \setminus \{0\}$ s operací součin není grupa. Stejně tak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- (5) Množina $\mathbb{R}^2$ s operací součet je grupa.

- (6) Množina $\mathcal{M}_{m \times n}(P)$ s operací součet je grupa.
 (7) Množina $\mathcal{M}_n(P)$ s operací součin není grupa.
 (8) Množina $\text{GL}_n(P)$ invertibilních matic typu $n \times n$ s operací součin je grupa (nazývá se *obecná lineární grupa*).
 (9) Množina X^X s operací skládání zobrazení není grupa.
 (10) Množina všech bijektivních zobrazení $X \rightarrow X$ s operací skládání je grupa. $\square$

Tvrzení 5.2.1. *Bud' $(G, *, e, {}^{-1})$ grupa. Pak pro libovolná $x, y \in G$ platí:*

- (1) *Jestliže $x * y = e$, pak $y = x^{-1}$, $x = y^{-1}$.*
 (2) *$(x * y)^{-1} = y^{-1} * x^{-1}$.*

Důkaz. (1) Jestliže $x * y = e$, pak $y = e * y = x^{-1} * x * y = x^{-1} * e = x^{-1}$. Podobně druhá rovnost (cvičení).

- (2) Plyne z rovnosti $x * y * y^{-1} * x^{-1} = e$ a (1). $\square$

Poznámka. Bez předpokladu existence inverze ke každému prvku nejde o grupu a implikace v bodě (1) v Tvrzení 5.2.1 nemusí platit, viz následující příklad (1), ale v některých případech i přesto platí, viz následující příklad (2).

Příklad. (1) Označme $I = [0, 1]$ a mějme množinu I^I všech zobrazení $I \rightarrow I$ s operací skládání a neutrálním prvkem id_I . Necht' $f, g \in I^I$ jsou taková, že

$$f(x) = \begin{cases} 2x & \text{pro } x \in [0, \frac{1}{2}], \\ 1 & \text{pro } x \in [\frac{1}{2}, 1], \end{cases} \quad g(x) = \frac{1}{2}x \quad \text{pro } x \in I.$$

Potom sice $f \circ g = \text{id}_I$, ale

$$(g \circ f)(x) = \begin{cases} x & \text{pro } x \in [0, \frac{1}{2}], \\ \frac{1}{2} & \text{pro } x \in [\frac{1}{2}, 1], \end{cases} \quad \text{a } f^{-1}, g^{-1} \text{ neexistují.}$$

- (2) Množina $\mathcal{M}_n(P)$ s operací součin sice není grupa, přesto pro libovolné dvě matice z $\mathcal{M}_n(P)$ bod (1) v Tvrzení 5.2.1 platí, viz Tvrzení 1.4.3. $\square$

5.3. Podgrupy

Definice 5.3.1. Bud' $(X, *, e, {}^{-1})$ grupa, bud' $Y \subseteq X$ podmnožina taková, že

- (1) jestliže $y_1, y_2 \in Y$, pak $y_1 * y_2 \in Y$;
 (2) $e \in Y$;
 (3) jestliže $y \in Y$, pak $y^{-1} \in Y$.

Potom Y je *podgrupa* grupy X .

Vlastnosti (1) se někdy říká *uzavřenost množiny vzhledem k operaci*, vlastnosti (3) *uzavřenost množiny vzhledem k inverzi*.

Je-li Y podgrupa grupy $(X, *, e, {}^{-1})$ a je-li $*_Y$ zúžení operace $*$ na podmnožinu $Y \times Y$, pak $(Y, *_Y, e, {}^{-1})$ je grupa. Zúžení operace na podmnožinu se obvykle značí stejně jako původní operace.

Příklad. (1) Každá grupa $(X, *, e, {}^{-1})$ má podgrupy X a $\{e\}$. Tyto podgrupy se nazývají *triviální podgrupy*.

- (2) Aditivní podgrupy $(\mathbb{Z}, +, 0, -) \subset (\mathbb{Q}, +, 0, -) \subset (\mathbb{R}, +, 0, -) \subset (\mathbb{C}, +, 0, -)$.

- (3) Multiplikativní podgrupy $(\mathbb{Q}^*, \cdot, 1, -^1) \subset (\mathbb{R}^*, \cdot, 1, -^1) \subset (\mathbb{C}^*, \cdot, 1, -^1)$.
- (4) Množina $\{-1, 1\}$ je podgrupa multiplikativní grupy $\mathbb{R}^*$.
- (5) Množina $\{z \in \mathbb{C} \mid |z| = 1\}$ je podgrupa multiplikativní grupy $\mathbb{C}^*$.
- (6) Množina $\{(x, 2x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$ je podgrupa grupy $\mathbb{R}^2$ s operací součet.
- (7) Množiny $\{(x, 1) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$ a $\{(x, y) \in \mathbb{R}^2 \mid x, y \in \mathbb{R}, x^2 + y^2 \leq 1\}$ nejsou podgrupy grupy $\mathbb{R}^2$ s operací součet. $\square$

Tvrzení 5.3.1. (1) *Bud' te X grupa, Y podgrupa X a Z podgrupa Y . Pak Z je podgrupa X .*

(2) *Bud' te X grupa a Y, Z její podgrupy. Pak $Y \cap Z$ je podgrupa X .*

Důkaz. Cvičení. $\square$

Cvičení. Pokud průnik prázdného systému podmnožin množiny X je množina X , potom průnik libovolného systému podgrup grupy X je podgrupa grupy X . $\square$

5.4. Podgrupy aditivní grupy $\mathbb{Z}$

Najdeme všechny podgrupy aditivní grupy $\mathbb{Z} = (\mathbb{Z}, +, 0, -)$. Pro celé nezáporné číslo $m \in \mathbb{N}_0$ označme

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

Tvrzení 5.4.1. *Množiny $m\mathbb{Z}$, $m \in \mathbb{N}_0$, jsou podgrupy aditivní grupy $\mathbb{Z}$ a jiné podgrupy v $\mathbb{Z}$ nejsou.*

Důkaz. Bud' $m \in \mathbb{N}_0$ libovolné. Ukážeme, že $m\mathbb{Z}$ je podgrupa. Pro libovolné $mk, ml \in m\mathbb{Z}$ platí $mk + ml = m(k + l) \in m\mathbb{Z}$, čímž je dokázána uzavřenost množiny $m\mathbb{Z}$ vzhledem ke sčítání. Množina $m\mathbb{Z}$ obsahuje neutrální prvek 0 grupy $\mathbb{Z}$. Nakonec, pro libovolné $mk \in m\mathbb{Z}$ platí $-(mk) = m(-k) \in m\mathbb{Z}$, čímž je dokázána uzavřenost množiny $m\mathbb{Z}$ vzhledem k inverzi (opačným prvkům).

Bud' $B \subseteq \mathbb{Z}$ libovolná podgrupa grupy $\mathbb{Z}$. Ukážeme, že B je rovna některé podgrupě $m\mathbb{Z}$. Jelikož B je podgrupa, obsahuje neutrální prvek 0. Pokud $B = \{0\}$, pak $B = 0\mathbb{Z}$ ($m = 0$). Předpokládejme, že $B \neq \{0\}$, tedy existuje nenulové číslo $b \in B$. Navíc existuje kladné číslo $b_+ \in B$, buď $b_+ = b$, nebo $b_+ = -b$ ($-b \in B$, protože B je podgrupa). Označme m nejmenší kladné číslo v B (v každé neprázdné množině kladných celých čísel existuje nejmenší číslo).

Dokážeme, že toto číslo m je hledané číslo, pro něž $B = m\mathbb{Z}$. Nejdříve ukážeme, že $m\mathbb{Z} \subseteq B$. Již víme, že $0 \in B$ a $m \in B$. Předpokládejme, že $mk \in B$. Potom i $m(k + 1) = mk + m \in B$ a díky matematické indukci dostáváme, že $mk \in B$ pro každé $k \in \mathbb{N}$. A potom i inverzní prvky $-mk$ leží v B , a tím je ukázáno, že všechny prvky množiny $m\mathbb{Z}$ leží v B .

Zbývá dokázat, že $B \subseteq m\mathbb{Z}$. Bud' $b \in B$ libovolné a předpokládejme, že $b \notin m\mathbb{Z}$. Pak existují $q, r \in \mathbb{Z}$ taková, že

$$b = mq + r \quad \text{a} \quad 0 < r < m.$$

Tedy, $r = b - mq = b + m(-q)$ je kladný prvek B , menší než m , což je v rozporu s definicí prvku m . Proto $b \in m\mathbb{Z}$. $\square$

5.5. Faktorové grupy

Definice 5.5.1. *Relace* na množině X je podmnožina kartézského součinu $X \times X$.

Je-li ρ relace, místo „ (x, y) je v relaci ρ “ se obvykle říká „ x je v relaci ρ s y “ a místo $(x, y) \in \rho$ se obvykle píše $x \rho y$.

Definice 5.5.2. Relace ρ na množině X je *relace ekvivalence*, jestliže je

- (1) reflexivní, tj. $x \rho x$ pro každé $x \in X$,
- (2) symetrická, tj. $x \rho y$ implikuje $y \rho x$,
- (3) tranzitivní, tj. $x \rho y, y \rho z$ implikuje $x \rho z$.

Definice 5.5.3. Buďte $\equiv$ relace ekvivalence na množině X a $x, y \in X$. Jestliže $x \equiv y$, potom x je *ekvivalentní* y vzhledem k $\equiv$. Množina

$$\{y \in X \mid x \equiv y\}$$

všech prvků ekvivalentních prvku x je *třída ekvivalence* příslušná x vzhledem k $\equiv$, označujeme ji $[x]_{\equiv}$ nebo jen $[x]$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

$$[x]_{\equiv} = \{y \in X \mid x \equiv y\}.$$

Definice 5.5.4. Buď $\equiv$ relace ekvivalence na množině X . Množina

$$\{[x]_{\equiv} \mid x \in X\}$$

všech příslušných tříd ekvivalence je *faktorová množina* vzhledem k $\equiv$, označujeme ji $\tilde{X}_{\equiv}$ nebo jen $\tilde{X}$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

$$\tilde{X}_{\equiv} = \{[x]_{\equiv} \mid x \in X\}.$$

Poznamenejme, že $\tilde{X}$ je *rozklad množiny* X , to znamená, že množiny $[x]$ jsou neprázdné, po dvou disjunktní a jejich sjednocení je X .

Definice 5.5.5. Buďte X množina s binární operací $*$ a $\equiv$ relace ekvivalence na množině X . Relace $\equiv$ je *kongruence* na X s $*$, jestliže platí *podmínka kompatibility*, čili implikace

$$\text{jestliže } x_1 \equiv x_2 \text{ a } y_1 \equiv y_2, \text{ pak } x_1 * y_1 \equiv x_2 * y_2,$$

nebo ekvivalentně

$$\text{jestliže } [x_1] = [x_2] \text{ a } [y_1] = [y_2], \text{ pak } [x_1 * y_1] = [x_2 * y_2].$$

Tvrzení 5.5.1. Buďte $\equiv$ kongruence na množině s asociativní binární operací a x, y invertibilní prvky. Pak platí implikace

$$\text{jestliže } x \equiv y, \text{ pak } x^{-1} \equiv y^{-1}$$

nebo ekvivalentně zapsáno

$$\text{jestliže } [x] = [y], \text{ pak } [x^{-1}] = [y^{-1}].$$

Důkaz. Nechť $x \equiv y$. Jelikož $x^{-1} \equiv x^{-1}$ a $y^{-1} \equiv y^{-1}$, z podmínky kompatibility dostaneme $x * x^{-1} \equiv y * x^{-1}$, tedy $e \equiv y * x^{-1}$, a $y^{-1} * e \equiv y^{-1} * y * x^{-1}$, tedy $y^{-1} \equiv x^{-1}$. $\square$

Příklad. (1) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$. Potom $\equiv$ je kongruence na $\mathbb{Z}$ s $+$, protože součet jakýchkoliv sudých čísel je sudé číslo, součet jakýchkoliv dvou lichých čísel je sudé číslo a součet jakéhokoliv sudého čísla a jakéhokoliv lichého čísla je liché číslo.

(2) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě záporná nebo obě kladná nebo obě nulová, tedy $\tilde{\mathbb{Z}} = \{[-1], [0], [1]\}$. Potom $\equiv$ je relace ekvivalence, platí implikace

$$\text{jestliže } x \equiv y, \text{ pak } -x \equiv -y,$$

ale existují $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ taková, že $x_1 \equiv x_2$ a $y_1 \equiv y_2$, ale $x_1 + y_1 \not\equiv x_2 + y_2$. Čili $\equiv$ nesplňuje podmínku kompatibility a není to tedy kongruence na $\mathbb{Z}$ s $+$.

(3) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě záporná nebo obě nezáporná, tedy $\tilde{\mathbb{Z}} = \{[-1], [0]\}$. Potom $\equiv$ je relace ekvivalence, ale existují $x, y \in \mathbb{Z}$ taková, že $x \equiv y$, ale $-x \not\equiv -y$. Podle Tvrzení 5.5.1 $\equiv$ není kongruence na $\mathbb{Z}$ s $+$, a nesplňuje tedy podmínku kompatibility. $\square$