6. Grupy

6.1. Binární operace

Definice 6.1.1. *Binární operace* na množině X je libovolné zobrazení $X \times X \to X$.

Jedná se tedy o zobrazení, které libovolné dvojici (x, y) prvků z X přiřazuje nějaký jednoznačně určený 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) Buď $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ množina všech celých nezáporných čísel. Zobrazení $+ \colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, 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

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

tedy například $1 + 2 = 0$.

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

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

(7) Množina $P[x]$ všech polynomů s operací sčítání nebo násobení polynomů.

(8) Množina X^X všech zobrazení $X \to X$ s operací $\circ$ skládání zobrazení.

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

Definice 6.1.2. 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 6.1.3. Binární operace $*$ na množině X je *komutativní*, jestliže pro každé $x, y \in X$ platí

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

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

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

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

(4) Násobení matic na množině $\mathcal{M}_n(P)$ je asociativní, ale není komutativní.

(5) Sčítání i násobení 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. ■

Definice 6.1.4. 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 6.1.1. *Každá binární operace má nejvýše jeden neutrální prvek.*

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

Příklad. (1) Neutrální prvek operace sčítání na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je 0.

(2) Neutrální prvek operace násobení na množinách $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je 1.

(3) Neutrální prvek operace sčítání na množině $\mathbb{R}^2$ je $(0, 0)$.

(4) Neutrální prvek operace sčítání matic na množině $\mathcal{M}_{m\times n}(P)$ je nulová matice příslušného typu, tedy $0_{m\times n}$.

(5) Neutrální prvek operace násobení matic na množině $\mathcal{M}_n(P)$ je jednotková matice příslušného typu, tedy E_n.

(6) Neutrální prvek operace sčítání polynomů na množině $P[x]$ je polynom 0.

(7) Neutrální prvek operace násobení 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 $\emptyset$. ■

Definice 6.1.5. 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 6.1.2. *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

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2.$$ □

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

Přímo z definice inverzního prvku vyplývá, že

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

Příklad. (1) Inverzní prvek k číslu x vzhledem k operaci sčítání 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 násobení 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 sčítání je $(-x, -y)$.

(4) Inverzní prvek k matici A vzhledem k operaci sčítání matic na množině $\mathcal{M}_{m\times n}(P)$ je opačná matice $-A$.

(5) Inverzní prvek k matici A vzhledem k operaci násobení matic na množině $\mathcal{M}_n(P)$ je inverzní matice A^{-1} (je-li A invertibilní).

(6) Inverzní prvek k zobrazení $f\colon X \to X$ 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. ■

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

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

Čili 1 a 2 jsou inverzní prvky k 2. Podle Tvrzení 6.1.2 to znamená, že operace $*$ není asociativní. A skutečně, například,

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

6.2. Grupy

Definice 6.2.1. Množina G s binární operací $*\colon G \times G \to G$ 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 sčítání je grupa. Stejně tak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(2) Množina $\mathbb{N}_0$ s operací sčítání není grupa.

(3) Množina $\mathbb{Q}^*$ s násobením je grupa. Stejně tak $\mathbb{R}^*, \mathbb{C}^*$, $\mathbb{R}_+$ (kladná reálná čísla).

(4) Množina $\mathbb{Z} \setminus \{0\}$ s operací násobení není grupa. Stejně tak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(5) Množina $\mathbb{R}^2$ s operací sčítání je grupa.

(6) Množina $\mathcal{M}_{m\times n}(P)$ s operací sčítání matic je grupa.

(7) Množina $\mathcal{M}_n(P)$ s operací násobení matic není grupa.

(8) Množina $\mathrm{GL}_n(P)$ invertibilních matic typu $n \times n$ s operací násobení matic je grupa (nazývá se *obecná lineární grupa*). ■

Tvrzení 6.2.1. *Buď $(G, *, e, ^{-1})$ 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 (1) a rovnosti $x * y * y^{-1} * x^{-1} = e$. □

6.3. Podgrupy

Definice 6.3.1. Buď $(X, *, e, ^{-1})$ grupa, buď $Y \subset X$ 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 inverzím*.

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 $\{z \in \mathbb{C} \,|\, |z| = 1\}$ je podgrupa multiplikativní grupy $\mathbb{C}^*$.

(6) Množina $\{(x, 2x) \in \mathbb{R}^2 \,|\, x \in \mathbb{R}\}$ je podgrupa grupy $\mathbb{R}^2$ s operací sčítání.

(7) Množiny $\{(x, 1) \in \mathbb{R}^2 \,|\, x \in \mathbb{R}\}$ a $\{(x, y) \in \mathbb{R}^2 \,|\, x, y \in \mathbb{R}, x^2 + y^2 \leq 1\}$ nejsou podgrupy grupy $\mathbb{R}^2$ s operací sčítání. ■

Tvrzení 6.3.1. *(1) Buďte X grupa, Y podgrupa X a Z podgrupa Y. Pak Z je podgrupa X.*

(2) Buďte X grupa a Y, Z její podgrupy. Pak $Y \cap Z$ je podgrupa X.

Důkaz. Cvičení. □

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

6.4. 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

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

Tvrzení 6.4.1. *Množiny $m\mathbb{Z}$, $m \in \mathbb{N}_0$, jsou podgrupy aditivní grupy $\mathbb{Z}$ a jiné podgrupy v $\mathbb{Z}$ nejsou.*

Důkaz. Buď $m \in \mathbb{N}_0$ 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 $m\mathbb{Z}$ na 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 $m\mathbb{Z}$ na inverzní (opačné) prvky.

Ukážeme, že každá podgrupa $B \subset \mathbb{Z}$ 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 $m\mathbb{Z} \subset B$. Již víme, že $0 \in B$ a $m \in B$. Matematickou indukcí se snadno dokáže, že $mk = m(k-1) + m \in B$ 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 $B \subset m\mathbb{Z}$. Buď $b \in B$ libovolné a předpokládejme, že $b \notin m\mathbb{Z}$. Pak existují $q, r \in \mathbb{Z}$ taková, že

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

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