6. přednáška, 7. 11. 2023

4.3. Ireducibilní polynomy

Definice 4.3.1. Polynom je *reducibilní* nad polem P, jestliže je součinem dvou nekonstantních polynomů nad polem P. Polynom je *ireducibilní* nad polem P, jestliže není konstantní a není reducibilní nad polem P.

Pro polynom z $P[x]$ označením *reducibilní*, resp. *ireducibilní* se myslí *reducibilní nad* P, resp. *ireducibilní nad* P.

Je-li polynom f reducibilní a $f = g \cdot h$, kde g, h jsou nekonstantní polynomy, říká se také, že $g \cdot h$ je *rozklad* polynomu f na součin polynomů g, h nebo také, že $g \cdot h$ je *rozklad* polynomu f na činitele g, h.

Příklad. (1) Každý polynom stupně 1 je ireducibilní, neboť není konstantní a součin dvou nekonstantních polynomů je polynom stupně aspoň 2.

(2) Polynom $x^2 - 1 = (x - 1)(x + 1)$ je reducibilní nad $\mathbb{R}$. Polynomy $x - 1$ a $x + 1$ jsou ireducibilní nad $\mathbb{R}$. □

Cvičení. Normovaný reducibilní polynom je součinem normovaných nekonstantních polynomů. □

Tvrzení 4.3.1. *Nechť jsou $f, g \in P[x]$ normované polynomy, g je ireducibilní a $f \mid g$. Potom buď $f = 1$, anebo $f = g$. Je-li f také ireducibilní, pak $f = g$.*

Důkaz. Když $f \mid g$, existuje $h \in P[x]$ takové, že $fh = g$. Jelikož g je ireducibilní, právě jeden z polynomů f, h je konstantní. Je-li normovaný polynom f konstantní, pak $f = 1$. Je-li h konstantní a fh je normovaný polynom, pak $h = 1$, tedy $f = g$. Je-li f ireducibilní, pak není konstantní, a zbývá tedy jen $f = g$. □

Lemma 4.3.2. *Buďte $g, h_1, \ldots, h_n \in P[x]$ normované ireducibilní polynomy a nechť $g \mid h_1 \cdots h_n$. Pak existuje index j takový, že $g = h_j$.*

Důkaz. Označme $d = D(g, h_1)$. Jelikož $d \mid g$ a g je ireducibilní, podle Tvrzení 4.3.1 buď $d = g$ anebo $d = 1$. Jestliže $d = g$, pak $g \mid h_1$ a $g = h_1$. Jestliže $d = 1$, pak Tvrzení 4.2.3

$$1 = gu + h_1 v$$

pro vhodné $u, v \in P[x]$. Vynásobíme-li obě strany polynomem $h_2 \cdots h_n$, dostaneme

$$h_2 \cdots h_n = g h_2 \cdots h_n u + h_1 h_2 \cdots h_n v.$$

Podle předpokladu $g \mid h_1 \cdots h_n$, takže pravá strana je dělitelná g, proto i levá strana je dělitelná g, čili $g \mid h_2 \cdots h_n$. Stejným postupem ukážeme, že buď $g = h_2$ anebo $g \mid h_3 \cdots h_n$. Opakováním tohoto postupu najdeme j, $1 \leq j \leq n$, takové, že $g = h_j$. □

Tvrzení 4.3.3. *Každý nekonstantní polynom je součinem konstanty a normovaných ireducibilních polynomů, přičemž všechny činitele jsou určeny jednoznačně až na pořadí.*

Důkaz. Buď $f \in P[x]$ nekonstantní polynom a označme $\bar{f} = \frac{1}{\operatorname{lc} f} \cdot f$. Je-li $\bar{f}$ ireducibilní, pak $f = \operatorname{lc} f \cdot \bar{f}$. Je-li $\bar{f}$ reducibilní, pak je součinem normovaných nekonstantních polynomů nižšího stupně. Každý z těchto polynomů je také buď ireducibilní nebo reducibilní, ve druhém případě je opět součinem normovaných nekonstantních polynomů nižšího stupně. Opakováním tohoto postupu po konečně mnoha krocích dojdeme ke konečnému počtu normovaných ireducibilních polynomů. Jejich počet je shora omezen stupněm polynomu f a jejich součin je roven $\bar{f}$.

Ještě je potřeba dokázat jednoznačnost. Předpokládejme, že $\bar{f} = g_1 \cdots g_n = h_1 \cdots h_m$ a všechny činitele jsou normované ireducibilní polynomy. Jelikož $g_1 \mid h_1 \cdots h_m$, podle předchozího lemmatu existuje index $\varphi(1)$ takový, že $g_1 = h_{\varphi(1)}$. Takže rovnost $g_1 \cdots g_n = h_1 \cdots h_m$ můžeme zkrátit g_1 a na obou stranách rovnosti tedy bude o jednoho činitele méně. Obdobně dostaneme, že existuje index $\varphi(2)$ takový, že $g_2 = h_{\varphi(2)}$, a postupně až že existuje index $\varphi(n)$ takový, že $g_n = h_{\varphi(n)}$.

Navíc, $n \leq m$, protože jinak by $g_{m+1} \cdots g_n = 1$, což není možné, když všechny g_i jsou nekonstantní polynomy. A obdobně dostaneme, že $m \leq n$. Takže $n = m$. □

Příklad. Polynom $x^2 + 1$ je reducibilní nad polem $\mathbb{C}$, protože $x^2 + 1 = (x + i)(x - i)$. Tentýž polynom je ireducibilní nad polem $\mathbb{R}$, protože jakýkoliv jeho hypotetický rozklad $x^2 + 1 = (x + \xi)(x + \eta)$, $\xi, \eta \in \mathbb{R}$ je současně rozkladem nad $\mathbb{C}$ různým od $x^2 + 1 = (x + i)(x - i)$, ve sporu s jednoznačností rozkladu. □

Důsledek. *Buď $f \in P[x]$ a buďte $g_1, \ldots, g_m \in P[x]$ normované ireducibilní a po dvou různé, tj. $g_i \neq g_j$ pro $i \neq j$. Jestliže $g_1^{k_1} \mid f$, …, $g_m^{k_m} \mid f$, pak $g_1^{k_1} \cdots g_m^{k_m} \mid f$.*

4.4. Kořeny a jejich násobnost

Pro $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in P[x]$ a $\xi \in P$, označme

$$f(\xi) = a_n \xi^n + a_{n-1} \xi^{n-1} + \cdots + a_1 \xi + a_0 \in P.$$

Tvrzení 4.4.1. *Pro libovolné polynomy $f, g \in P[x]$ a libovolný prvek $\xi \in P$ platí*

$$(f + g)(\xi) = f(\xi) + g(\xi), \quad (-f)(\xi) = -f(\xi), \quad (fg)(\xi) = f(\xi) g(\xi).$$

Důkaz. Cvičení. □

Definice 4.4.1. Prvek $\xi \in P$ je *kořen* polynomu $f \in P[x]$, jestliže $f(\xi) = 0$.

Tvrzení 4.4.2. *Nechť $f \in P[x]$ a $\xi \in P$. Potom ξ je kořen polynomu f právě tehdy, když $x - \xi$ dělí f.*

Důkaz. Předpokládejme, že ξ je kořen polynomu f. Dělením $f : (x - \xi)$ dostaneme

$$f = (x - \xi)q + r, \quad \text{kde buď } r = 0 \text{ nebo } \deg r < \deg(x - \xi) = 1, \text{ čili } \deg r = 0.$$

Takže v obou případech r je konstantní polynom a $0 = f(\xi) = (\xi - \xi)q(\xi) + r = r$. Čili $r = 0$, $f = (x - \xi)q$ a $x - \xi$ dělí f.

Předpokládejme, že $x - \xi$ dělí f, tedy $f = (x - \xi)q$ pro nějaké q. Potom $f(\xi) = (\xi - \xi)q(\xi) = 0$, čili ξ je kořen polynomu f. □

Definice 4.4.2. Nechť $f \in P[x]$ a $\xi \in P$. Pokud ξ je kořen f, potom polynom $x - \xi$ je *kořenový činitel* polynomu f.

Definice 4.4.3. Prvek $\xi \in P$ je *k-násobný kořen* polynomu $f \in P[x]$, jestliže $(x-\xi)^k$ dělí f, ale $(x-\xi)^{k+1}$ nedělí f.

Tvrzení 4.4.3. *Buďte $\xi_1, \ldots, \xi_n \in P$ různé kořeny polynomu $f \in P[x]$ s násobnostmi po řadě $k_1, \ldots, k_n$. Potom*

(1) $(x-\xi_1)^{k_1} \cdots (x-\xi_n)^{k_n} \mid f$;

(2) $k_1 + \cdots + k_n \leq \deg f$.

Důkaz. Cvičení. □

Tvrzení 4.4.4 (Základní věta algebry)**.** *Každý nekonstantní polynom nad polem $\mathbb{C}$ má aspoň jeden kořen.*

Všechny známé důkazy využívají výsledky matematické analýzy, proto zde důkaz neuvádíme.

Důsledek. *Každý nekonstantní polynom nad polem $\mathbb{C}$ má rozklad na lineární činitele. Kořenů se započtením násobnosti má právě tolik, kolik činí jeho stupeň.*

Předchozí důsledek znamená, že pro každý nekonstantní polynom $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ stupně n s komplexními koeficienty existují čísla $\xi_1, \xi_2, \ldots, \xi_n$ (nemusí být po dvou různá), pro která platí

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = a_n(x-\xi_1)(x-\xi_2)\ldots(x-\xi_n).$$

Každé z čísel $\xi_1, \xi_2, \ldots, \xi_n$ je kořenem polynomu f.

Důsledek. *Každý nekonstantní polynom stupně n s komplexními koeficienty má nejvýše n navzájem různých kořenů.*

Tvrzení 4.4.5 (Vlastnosti kořenů (Viètovy vzorce))**.** *Buďte $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ a $\xi_1, \xi_2, \ldots, \xi_n$ jeho kořeny (nemusí být všechny různé). Potom*

$$\begin{aligned}
a_{n-1} &= -(\xi_1 + \xi_2 + \cdots + \xi_n) = -\sum_{i=1}^{n} \xi_i \\
a_{n-2} &= \xi_1\xi_2 + \xi_1\xi_3 + \cdots + \xi_1\xi_n + \xi_2\xi_3 + \cdots + \xi_2\xi_n + \cdots + \xi_{n-1}\xi_n = \\
&= \sum_{\substack{i,j=1 \\ i<j}}^{n} \xi_i\xi_j \\
a_{n-3} &= -(\xi_1\xi_2\xi_3 + \xi_1\xi_2\xi_4 + \cdots + \xi_1\xi_{n-1}\xi_n + \cdots + \xi_{n-2}\xi_{n-1}\xi_n) = \\
&= -\sum_{\substack{i,j,k=1 \\ i<j<k}}^{n} \xi_i\xi_j\xi_k \\
&\vdots \\
a_1 &= (-1)^{n-1}(\xi_1\cdots\xi_{n-2}\xi_{n-1} + \xi_1\cdots\xi_{n-2}\xi_n + \cdots \\
&\qquad \cdots + \xi_1\xi_3\cdots\xi_n + \xi_2\cdots\xi_n) \\
a_0 &= (-1)^n\xi_1\xi_2\cdots\xi_n
\end{aligned}$$

Důkaz. Polynom f můžeme rozložit na součin jeho kořenových činitelů

$$x^n + \ldots + a_0 = (x - \xi_1) \ldots (x - \xi_n).$$

Po roznásobení pravé strany porovnáním koeficientů s příslušnými koeficienty na levé straně získáme uvedené vztahy. □

Příklad. Kořeny polynomu $x^2 - 5x + 6$ jsou 2 a 3 a

$$a_1 = -(2 + 3) = -5,$$
$$a_0 = (-1)^2 \cdot 2 \cdot 3 = 6.$$ □

4.5. Polynomy s reálnými koeficienty

Komplexní čísla

Komplexní číslo je číslo $a + bi$, kde a, b jsou reálná čísla a i je *imaginární jednotka*, čili $i^2 = -1$.

Komplexní čísla $z_1 = a + bi$, $z_2 = c + di$ se rovnají právě tehdy, když $a = c$ a $b = d$.

Pro $z_1 = a + bi$, $z_2 = c + di$

$$z_1 + z_2 = (a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$z_1 - z_2 = (a + bi) - (c + di) = (a - c) + (b - d)i,$$
$$z_1 \cdot z_2 = (a + bi) \cdot (c + di) = (ac + bdi^2) + adi + bci = (ac - bd) + (ad + bc)i.$$

Číslo komplexně sdružené k číslu $z = a + bi$ je číslo $a - bi$ a označujeme jej z^*.

Cvičení. Pro komplexní číslo $z = a + bi$ platí

(1) $(z^*)^* = z$,
(2) $z = z^*$ právě tehdy, když z je reálné číslo,
(3) $z + z^* = 2a$, tedy reálné číslo,
(4) $zz^* = a^2 + b^2$, tedy reálné číslo. □

Cvičení. Pro komplexní čísla z_1, z_2 platí

(1) $(z_1 + z_2)^* = z_1^* + z_2^*$,
(2) $(z_1 z_2)^* = z_1^* z_2^*$. □

Cvičení. Pro komplexní číslo $z = a + bi$

$$(x - z)(x - z^*) = x^2 - 2ax + a^2 + b^2$$

je polynom s reálnými koeficienty a pokud $z \notin \mathbb{R}$, čili $b \neq 0$, potom diskriminant tohoto polynomu je záporný. □

Polynomy s reálnými koeficienty

Tvrzení 4.5.1. *Je-li $\xi \in \mathbb{C}$ kořenem polynomu s reálnými koeficienty, potom $\xi^* \in \mathbb{C}$ je také kořenem tohoto polynomu, a to stejné násobnosti.*

Důkaz. Nechť $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ je polynom s reálnými koeficienty a $\xi \in \mathbb{C}$ je jeho kořen, čili $f(\xi) = 0$. Potom

$$\begin{aligned} f(\xi^*) &= a_n(\xi^*)^n + a_{n-1}(\xi^*)^{n-1} + \cdots + a_1\xi^* + a_0 = && (a = a^* \text{ pro } a \in \mathbb{R}) \\ &= a_n^*(\xi^*)^n + a_{n-1}^*(\xi^*)^{n-1} + \cdots + a_1^*\xi^* + a_0^* = && (a^*b^* = (ab)^*) \\ &= (a_n\xi^n)^* + (a_{n-1}\xi^{n-1})^* + \cdots + (a_1\xi)^* + a_0^* = && (a^* + b^* = (a+b)^*) \\ &= (a_n\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0)^* = \\ &= f(\xi)^* = 0^* = 0. \end{aligned}$$

Na druhou stranu, pokud ξ^* je kořen polynomu f, potom z právě dokázaného vyplývá, že $\xi = (\xi^*)^*$ je také kořen.

Takže, je-li $\xi = a + bi$ kořen f, potom $\xi^* = a - bi$ je také kořen f a

$$f = (x - \xi)(x - \xi^*)h.$$

Díky tomu, že $\xi + \xi^* = 2a$ a $\xi\xi^* = a^2 + b^2$ jsou reálná čísla,

$$(x - \xi)(x - \xi^*) = x^2 - (\xi + \xi^*)x + \xi\xi^*$$

je polynom s reálnými koeficienty, a proto h je také polynom s reálnými koeficienty. Proto, je-li ξ k-násobný kořen f,

$$f = (x - \xi)^k(x - \xi^*)^k g,$$

kde g je polynom s reálnými koeficienty, jehož kořenem nejsou ani ξ ani ξ^*, takže ξ^* je také k-násobný kořen f. □

Rozklad normovaného polynomu f s reálnými koeficienty na ireducibilní činitele nad $\mathbb{C}$ tedy obsahuje lineární činitele $x - \alpha_i$ s reálnými kořeny α_i a dvojice lineárních činitelů $x - \xi_j$, $x - \xi_j^*$ s dvojicemi komplexně sdružených kořenů ξ_j, ξ_j^*:

$$f = (x - \alpha_1)^{l_1} \cdots (x - \alpha_r)^{l_r}(x - \xi_1)^{k_1}(x - \xi_1^*)^{k_1} \cdots (x - \xi_s)^{k_s}(x - \xi_s^*)^{k_s}.$$

Takže $\deg f = l_1 + \cdots + l_r + 2(k_1 + \cdots + k_s)$.

Pokud roznásobíme všechny dvojice $(x - \xi_j), (x - \xi_j^*)$, dostaneme rozklad polynomu f na ireducibilní činitele nad $\mathbb{R}$, který obsahuje lineární činitele $x - \alpha_i$ a kvadratické činitele $x^2 - (\xi_j + \xi_j^*)x + \xi_j\xi_j^*$ se zápornými diskriminanty:

$$f = (x-\alpha_1)^{l_1} \cdots (x-\alpha_r)^{l_r}(x^2 - (\xi_1+\xi_1^*)x + \xi_1\xi_1^*)^{k_1} \cdots (x^2 - (\xi_s+\xi_s^*)x + \xi_s\xi_s^*)^{k_s}.$$

Cvičení. (1) Každý polynom s reálnými koeficienty lichého stupně má aspoň jeden reálný kořen.

(2) Každý polynom s reálnými koeficienty stupně většího než 2 je reducibilní nad $\mathbb{R}$. □

Cvičení. Rozložte polynom $x^4 + 1$ na ireducibilní činitele nad $\mathbb{C}$ a nad $\mathbb{R}$. □

Pro polynomy, jejichž koeficienty jsou celá čísla, navíc platí následující tvrzení.

Tvrzení 4.5.2. *Buďte $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ polynom s celočíselnými koeficienty a p, q nesoudělná celá čísla. Jestliže $\frac{p}{q}$ je kořenem polynomu f, potom a_0 je dělitelné p a a_n je dělitelné q.*

Důkaz. Položíme $f(\frac{p}{q})$ rovno nule a po vhodných úpravách získáme uvedené vlastnosti. Cvičení. □

Důsledek. *Celočíselné kořeny polynomu s celočíselnými koeficienty jsou dělitelé absolutního členu.*

4.6. Derivace

Definice 4.6.1. Buď $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. Polynom $f' = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \in \mathbb{C}[x]$ je *derivace* polynomu f.

Tvrzení 4.6.1. *(1)* $(f+g)' = f' + g'$,
(2) $(fg)' = f'g + fg'$,
(3) $(f^k)' = kf^{k-1}f'$.

Důkaz. Cvičení. □

Tvrzení 4.6.2. *Nechť $k \geq 2$, $f \in \mathbb{C}[x]$ je polynom a $\xi \in \mathbb{C}$ je jeho k-násobný kořen. Potom*

(1) ξ je $(k-1)$-násobný kořen f',
(2) ξ je $(k-1)$-násobný kořen největšího společného dělitele $D(f, f')$.

Důkaz. (1) $(x-\xi)^k \mid f$, tedy $f = (x-\xi)^k q$ a $(x-\xi)^{k+1}$ nedělí f. Potom

$$f' = k(x-\xi)^{k-1}q + (x-\xi)^k q' = (x-\xi)^{k-1}(kq + (x-\xi)q').$$

Takže, $(x-\xi)^{k-1}$ dělí f'. Kdyby $(x-\xi)^k$ dělilo f', pak by $(x-\xi) \mid (kq + (x-\xi)q')$, načež $(x-\xi) \mid kq$, tedy $(x-\xi) \mid q$ a $(x-\xi)^{k+1} \mid f$ ve sporu s předpokladem.

(2) $(x-\xi)^{k-1}$ je dělitel f i f', takže $(x-\xi)^{k-1} \mid D(f, f')$. Kdyby $(x-\xi)^k$ dělilo $D(f, f')$, pak by $(x-\xi)^k \mid f'$ ve sporu s předchozím bodem. □

Tvrzení 4.6.3. *Buďte $f \in \mathbb{C}[x]$ a $\xi \in \mathbb{C}$ jeho kořen. Potom ξ je 1-násobný kořen polynomu*

$$\frac{f}{D(f, f')} \in \mathbb{C}[x].$$

Důkaz. Nechť ξ je k-násobný kořen polynomu f, tedy $f = (x-\xi)^k q$, ale $(x-\xi)^{k+1}$ nedělí f, čili $x - \xi$ nedělí q. Podle předchozího tvrzení $D(f, f') = (x-\xi)^{k-1}r$. Takže

$$\frac{f}{D(f, f')} = (x-\xi)\frac{q}{r} \quad \text{a jelikož } x-\xi \text{ nedělí } q, \text{ nedělí ani } \frac{q}{r}.$$ □

Důsledek. *Buď $f \in \mathbb{C}[x]$.*

(1) Množina všech kořenů polynomu $f/D(f, f')$ je rovna množině všech kořenů polynomu f.
(2) Všechny kořeny polynomu $f/D(f, f')$ jsou 1-násobné.

Důkaz. Cvičení. □

5. Grupy

5.1. Binární operace

Definice 5.1.1. *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 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) 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 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 $e_2 = e_1 * e_2 = e_1$. □

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 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

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

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 5.1.2 to znamená, že operace $*$ není asociativní. A skutečně, například,

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

5.2. Grupy

Definice 5.2.1. 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 5.2.1. *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 $x * y * y^{-1} * x^{-1} = e$. □

5.3. Podgrupy

Definice 5.3.1. Buď $(X, *, e, ^{-1})$ grupa, buď $Y \subseteq X$ 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 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 5.3.1. *(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. □