

6. přednáška, 7. 11. 2024

Definice 4.4.2. Necht $f \in P[x]$ 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. Budte $\xi_1, \dots, \xi_n \in P$ různé kořeny polynomu $f \in P[x]$ s násobnostmi po řadě $k_1, \dots, k_n$. Potom

- (1) $(x - \xi_1)^{k_1} \dots (x - \xi_n)^{k_n} \mid f$;
- (2) $k_1 + \dots + k_n \leq \deg f$.

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, a navzájem různých kořenů má nejvýše tolik.

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

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

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

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

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

Důkaz. Polynom f můžeme rozložit na součin jeho kořenových činitelů

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x - \xi_1) \cdots (x - \xi_n).$$

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

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

$$a_1 = -(2 + 3) = -5,$$

$$a_0 = (-1)^2 \cdot 2 \cdot 3 = 6. \quad \square$$

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. $\square$

Cvičení. Pro komplexní čísla z_1, z_2 platí

- (1) $(z_1 + z_2)^* = z_1^* + z_2^*$,
- (2) $(z_1 z_2)^* = z_1^* z_2^*$. $\square$

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. $\square$

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

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

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 . $\square$

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^* :

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

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

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:

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

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 $\mathbb{R}$. $\square$

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

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

Tvrzení 4.5.2. *Budte $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ 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. Předpokládejme, že $\frac{p}{q}$ je kořenem polynomu f , tedy

$$f\left(\frac{p}{q}\right) = a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \frac{p}{q} + a_0 = 0.$$

Vhodnými úpravami lze získat uvedené vlastnosti. Cvičení. $\square$

Důsledek. *Celočíselné kořeny polynomu s celočíselnými koeficienty jsou dělitele 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

$$f' = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1 \in \mathbb{C}[x]$$

je *derivace* polynomu f .

Tvrzení 4.6.1. (1) $(f + g)' = f' + g'$,

(2) $(fg)' = f'g + fg'$,

(3) $(f^k)' = k f^{k-1} f'$.

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) Předpokládejme, že ξ je k -násobný kořen polynomu f , čili $(x - \xi)^k$ dělí f a $(x - \xi)^{k+1}$ nedělí f . Pro nějaký polynom q tedy $f = (x - \xi)^k q$. 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' , potom $x - \xi$ by dělilo $kq + (x - \xi)q'$ a vzhledem k tomu, že $x - \xi$ dělí $(x - \xi)q'$, muselo by $x - \xi$ dělit také kq , tedy i q . V takovém případě $(x - \xi)^{k+1}$ by dělilo f , což je spor 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

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

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. □

4.7. Hornerovo schéma

Bud' $f \in P[x]$ a $\xi \in P$. Podle Tvzení 4.1.6 existuje právě jedna dvojice polynomů $q, r \in P[x]$ taková, že

- (i) $f = (x - \xi)q + r$;
- (ii) buď $r = 0$ nebo $\deg r < \deg(x - \xi) = 1$.

Takže r je konstantní polynom a $f(\xi) = r$.

Je-li f konstantní polynom, potom $q = 0$ a $r = f$. Je-li $\deg f \geq 1$, potom $\deg q = \deg f - 1$. Nechť $\deg f = n \geq 1$ a

$$\begin{aligned} f &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ q &= b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0. \end{aligned}$$

Potom,

$$\begin{aligned} a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 &= \\ &= (x - \xi)(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0) + r = \\ &= b_{n-1} x^n + (b_{n-2} - \xi b_{n-1}) x^{n-1} + \cdots + (b_1 - \xi b_2) x^2 + (b_0 - \xi b_1) x + (r - \xi b_0). \end{aligned}$$

Když se polynomy vzájemně rovnají, rovnají se jejich koeficienty u stejných mocnin neurčité x . Díky tomu dostaneme soustavu lineárních rovnic s neznámými $b_{n-1}, \dots, b_1, b_0, r$, jejíž řešení lze snadno vyjádřit pomocí $a_n, \dots, a_1, a_0$ a ξ .

$$\begin{array}{lll} a_n = b_{n-1} & \Rightarrow & b_{n-1} = a_n \\ a_{n-1} = b_{n-2} - \xi b_{n-1} & \Rightarrow & b_{n-2} = a_{n-1} + \xi b_{n-1} \\ a_{n-2} = b_{n-3} - \xi b_{n-2} & \Rightarrow & b_{n-3} = a_{n-2} + \xi b_{n-2} \\ \vdots & \vdots & \vdots \\ a_2 = b_1 - \xi b_2 & \Rightarrow & b_1 = a_2 + \xi b_2 \\ a_1 = b_0 - \xi b_1 & \Rightarrow & b_0 = a_1 + \xi b_1 \\ a_0 = r - \xi b_0 & \Rightarrow & r = a_0 + \xi b_0 \end{array}$$

Tedy,

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= a_{n-1} + \xi a_n \\ b_{n-3} &= a_{n-2} + \xi(a_{n-1} + \xi a_n) \\ &\vdots \\ b_1 &= a_2 + \xi(a_3 + \xi(a_4 + \cdots + \xi(a_{n-2} + \xi(a_{n-1} + \xi a_n)) \cdots)) \\ b_0 &= a_1 + \xi(a_2 + \xi(a_3 + \cdots + \xi(a_{n-2} + \xi(a_{n-1} + \xi a_n)) \cdots)) \\ r &= a_0 + \xi(a_1 + \xi(a_2 + \cdots + \xi(a_{n-2} + \xi(a_{n-1} + \xi a_n)) \cdots)). \end{aligned}$$

Pro výpočet je praktické uspořádat si koeficienty, jak známé $a_n, \dots, a_1, a_0, \xi$, tak hledané $b_{n-1}, \dots, b_1, b_0, r$, do tabulky (schématu) tak, že v prvním řádku jsou koeficienty polynomu f , do druhého řádku postupně píšeme ξ -násobky vypočítaných koeficientů polynomu q a do třetího řádku napíšeme ξ a potom postupně součty hodnot v příslušných sloupcích v prvních dvou řádcích, tedy koeficienty polynomu q a také hodnotu $r = f(\xi)$.

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_2	a_1	a_0
		ξb_{n-1}	ξb_{n-2}	$\dots$	ξb_2	ξb_1	ξb_0
ξ	a_n $= b_{n-1}$	$a_{n-1} + \xi b_{n-1}$ $= b_{n-2}$	$a_{n-2} + \xi b_{n-2}$ $= b_{n-3}$	$\dots$ $\dots$	$a_2 + \xi b_2$ $= b_1$	$a_0 + \xi b_0$ $= b_0$	$a_0 + \xi b_0$ $= r$

Takto lze tedy spočítat částečný podíl q a zbytek r při dělení polynomu f polynomem $x - \xi$, čili také $f(\xi) = r$, a ověřit tak, například, zda ξ je kořenem polynomu f .

Navíc, Hornerovo schéma lze použít pro nalezení hodnot derivací polynomu f v bodě ξ a k převodu čísla z nedesítkové do desítkové soustavy.

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 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 $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ 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

$+$	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 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 $\circ$ 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 $P(X)$. $\square$

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*.

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 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 . □

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

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