

5. přednáška, 31. 10. 2024

Definice 3.5.2. *Fundamentální systém řešení* homogenní soustavy je taková množina řešení té soustavy, která je lineárně nezávislá a každé řešení lze vyjádřit jako lineární kombinaci řešení z této množiny.

Tvrzení 3.5.3. *Fundamentální systém řešení soustavy rovnic $Ax = 0$ o n neznámých má $n - \text{rank } A$ prvků.*

Důkaz. Obecné řešení ξ soustavy $Ax = 0$ o n neznámých je vyjádřeno pomocí $n - \text{rank } A$ parametrů $t^1, \dots, t^{n-\text{rank } A}$, tedy $\xi = \xi(t^1, \dots, t^{n-\text{rank } A})$. Provedeme-li $n - \text{rank } A$ voleb parametrů

$$\begin{aligned}(t^1, \dots, t^{n-\text{rank } A}) &= (1, 0, \dots, 0), \\(t^1, \dots, t^{n-\text{rank } A}) &= (0, 1, \dots, 0), \\&\dots \\(t^1, \dots, t^{n-\text{rank } A}) &= (0, \dots, 0, 1),\end{aligned}$$

dostaneme množinu partikulárních řešení

$$\{\xi(1, 0, \dots, 0), \xi(0, 1, \dots, 0), \dots, \xi(0, \dots, 0, 1)\},$$

která je lineárně nezávislá a

$$\xi(t^1, \dots, t^{n-\text{rank } A}) = t^1 \xi(1, 0, \dots, 0) + t^2 \xi(0, 1, \dots, 0) + \dots + t^{n-\text{rank } A} \xi(0, \dots, 0, 1),$$

takže obecné řešení, čili každé řešení, soustavy je lineární kombinací těchto partikulárních řešení. $\square$

Příklad. (1) Soustava

$$x^1 - x^2 = 0$$

má 2 neznámé, matice soustavy má hodnost 1, obecné řešení je

$$\xi(t) = (t, t), \quad t \in \mathbb{R},$$

množina všech řešení soustavy je

$$\{(t, t) \mid t \in \mathbb{R}\} = \{t(1, 1) \mid t \in \mathbb{R}\}$$

a fundamentální systém řešení soustavy je například

$$\{(1, 1)\}.$$

(2) Soustava

$$\begin{aligned}x^1 + x^2 + 2x^3 &= 0 \\-x^1 + x^2 + 2x^3 &= 0 \\x^1 + 3x^2 + 6x^3 &= 0\end{aligned}$$

má 3 neznámé, matice soustavy má hodnost 2, obecné řešení je

$$\xi(t) = (0, -2t, t), \quad t \in \mathbb{R},$$

množina všech řešení soustavy je

$$\{(0, -2t, t) \mid t \in \mathbb{R}\} = \{t(0, -2, 1) \mid t \in \mathbb{R}\}$$

a fundamentální systém řešení soustavy je například

$$\{(0, -2, 1)\}.$$

(3) Soustava

$$x^1 - x^2 + x^3 = 0$$

má 3 neznámé, matice soustavy má hodnost 1, obecné řešení je

$$\xi(t^1, t^2) = (t^1 - t^2, t^1, t^2), \quad t^1, t^2 \in \mathbb{R},$$

množina všech řešení soustavy je

$$\{(t^1 - t^2, t^1, t^2) \mid t^1, t^2 \in \mathbb{R}\} = \{t^1(1, 1, 0) - t^2(-1, 0, 1) \mid t^1, t^2 \in \mathbb{R}\}$$

a fundamentální systém řešení soustavy je například

$$\{(1, 1, 0), (-1, 0, 1)\}.$$

(4) Soustava

$$x^1 + 2x^2 = 0$$

$$3x^1 + 4x^2 = 0$$

má 2 neznámé, matice soustavy má hodnost 2 a soustava má jediné řešení, čili obecné řešení je

$$\xi = (0, 0),$$

množina všech řešení soustavy je

$$\{(0, 0)\}$$

a fundamentální systém řešení soustavy je $\emptyset$.

(5) Soustava

$$0x = 0$$

má 1 neznámou, matice soustavy má hodnost 0, obecné řešení je

$$\xi(t) = t, \quad t \in \mathbb{R},$$

množina všech řešení soustavy je

$$\{t \mid t \in \mathbb{R}\} = \mathbb{R}$$

a fundamentální systém řešení soustavy je například

$$\{1\}.$$

□

Poznámka. Je-li $\{\xi_1, \xi_2, \dots, \xi_r\}$ fundamentální systém řešení nějaké soustavy, potom

$$t^1 \xi_1 + t^2 \xi_2 + \dots + t^r \xi_r, \quad t^1, t^2, \dots, t^r \in P,$$

je obecné řešení soustavy a

$$\{t^1 \xi_1 + t^2 \xi_2 + \dots + t^r \xi_r \mid t^1, t^2, \dots, t^r \in P\}$$

je množina všech řešení soustavy.

Homogenní soustava rovnic k zadanému fundamentálnímu systému řešení.

Pro libovolnou lineárně nezávislou množinu $\{\xi_1, \xi_2, \dots, \xi_r\} \subset P^n$ existuje homogenní soustava lineárních rovnic taková, že $\{\xi_1, \xi_2, \dots, \xi_r\}$ je její fundamentální systém řešení. Takových soustav, vzájemně ekvivalentních, existuje více. Uvedeme postup nalezení jedné z nich.

Množina $\{\xi_1, \xi_2, \dots, \xi_r\}$ uspořádaných n -tic prvků pole P má být fundamentální systémem řešení soustavy, takže hledáme homogenní soustavu

$$\begin{aligned} a_1^1 x^1 + a_2^1 x^2 + \dots + a_n^1 x^n &= 0 \\ a_1^2 x^1 + a_2^2 x^2 + \dots + a_n^2 x^n &= 0 \\ &\vdots \\ a_1^{n-r} x^1 + a_2^{n-r} x^2 + \dots + a_n^{n-r} x^n &= 0 \end{aligned} \quad \text{resp. } Ax = 0$$

lineárních rovnic nad polem P o n neznámých $x^1, x^2, \dots, x^n$, jejíž matice $A = (a_j^i)$ má hodnost $n - r$. Je tedy potřeba najít vhodné koeficienty a_j^i .

Jednotlivé uspořádané n -tice $\xi_1, \xi_2, \dots, \xi_r$ mají být řešení soustavy $Ax = 0$, takže po jejich dosazení za x dostaneme $r \cdot (n - r)$ homogenních rovnic o celkem $n \cdot (n - r)$ neznámých a_j^i , $i \in \{1, \dots, n - r\}$, $j \in \{1, \dots, n\}$. Ovšem, pro každé $k \in \{1, \dots, r\}$ dosazením ξ_k za x dostaneme $A\xi_k = 0$, což představuje $n - r$ rovnic

$$\begin{aligned} \xi_k^1 a_1^1 + \xi_k^2 a_2^1 + \dots + \xi_k^n a_n^1 &= 0 \\ \xi_k^1 a_1^2 + \xi_k^2 a_2^2 + \dots + \xi_k^n a_n^2 &= 0 \\ &\vdots \\ \xi_k^1 a_1^{n-r} + \xi_k^2 a_2^{n-r} + \dots + \xi_k^n a_n^{n-r} &= 0, \end{aligned}$$

z nichž každá má jiných n neznámých $a_1^j, \dots, a_n^j$, $j \in \{1, \dots, n - r\}$, ale všechny mají stejné koeficienty $\xi_k^1, \dots, \xi_k^n$, takže všechny mají stejnou množinu všech řešení a stačí pro každé $k \in \{1, \dots, r\}$ uvažovat jen jednu rovnici

$$\xi_k^1 a^1 + \xi_k^2 a^2 + \dots + \xi_k^n a^n = 0$$

s neznámými $a^1, a^2, \dots, a^n$. Dosazením všech $\xi_1, \xi_2, \dots, \xi_r$ tak dostaneme homogenní soustavu

$$\begin{aligned} \xi_1^1 a^1 + \xi_1^2 a^2 + \dots + \xi_1^n a^n &= 0 \\ \xi_2^1 a^1 + \xi_2^2 a^2 + \dots + \xi_2^n a^n &= 0 \\ &\vdots \\ \xi_r^1 a^1 + \xi_r^2 a^2 + \dots + \xi_r^n a^n &= 0 \end{aligned}$$

r lineárních rovnic o n neznámých $a^1, a^2, \dots, a^n$ s maticí Ξ , jejíž řádky jsou tvořeny uspořádanými n -ticemi $\xi_1, \xi_2, \dots, \xi_r$. Hodnost matice Ξ je tedy rovna r , fundamentální systém řešení má $n - r$ prvků $(a_1^1, a_2^1, \dots, a_n^1), (a_1^2, a_2^2, \dots, a_n^2), \dots, (a_1^{n-r}, a_2^{n-r}, \dots, a_n^{n-r})$ a toto jsou řádky hledané matice A .

Příklad. Necht $\xi_1 = (1, 2, 3, 4), \xi_2 = (4, 3, 2, 1) \in \mathbb{R}^4$. Najdeme homogenní soustavu lineárních rovnic nad polem $\mathbb{R}$, jejímž fundamentálním systémem řešení je

$$\{\xi_1, \xi_2\}.$$

Hledáme tedy soustavu $Ax = 0$ dvou rovnic o čtyřech neznámých. Sestavíme soustavu $\Xi \cdot a = 0$, kde

$$\Xi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \text{a} \quad a = \begin{pmatrix} a^1 \\ a^2 \\ a^3 \\ a^4 \end{pmatrix}.$$

Tedy,

$$a^1 + 2a^2 + 3a^3 + 4a^4 = 0$$

$$4a^1 + 3a^2 + 2a^3 + a^4 = 0.$$

Fundamentální systém řešení této soustavy je, například,

$$\{(2, -3, 0, 1), (1, -2, 1, 0)\}.$$

Zvolíme-li

$$A = \begin{pmatrix} a_1^1 & a_2^1 & a_3^1 & a_4^1 \\ a_1^2 & a_2^2 & a_3^2 & a_4^2 \end{pmatrix} = \begin{pmatrix} 2 & -3 & 0 & 1 \\ 1 & -2 & 1 & 0 \end{pmatrix},$$

dostaneme soustavu

$$\begin{pmatrix} 2 & -3 & 0 & 1 \\ 1 & -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x^1 \\ x^2 \\ x^3 \\ x^4 \end{pmatrix} = 0$$

tedy

$$2x^1 - 3x^2 + x^4 = 0$$

$$x^1 - 2x^2 + x^3 = 0.$$

Potom $\{(1, 2, 3, 4), (4, 3, 2, 1)\}$ je fundamentální systém řešení této soustavy,

$$t^1(1, 2, 3, 4) + t^2(4, 3, 2, 1), \quad t^1, t^2 \in \mathbb{R},$$

je její obecné řešení a

$$\{t^1(1, 2, 3, 4) + t^2(4, 3, 2, 1) \mid t^1, t^2 \in \mathbb{R}\}$$

je množina všech řešení soustavy. □

3.6. Nehomogenní soustavy lineárních rovnic

Definice 3.6.1. Soustava lineárních rovnic s nenulovou pravou stranou je *nehomogenní*. Je-li $Ax = b$ nehomogenní soustava, potom $Ax = 0$ je *homogenizovaná soustava*.

Příklad. (1) Soustava

$$x^1 + 2x^2 - x^3 = 1$$

$$-x^1 + x^2 + 2x^3 = 0$$

$$2x^1 - x^2 + x^3 = 3$$

je nehomogenní.

(2) Soustava

$$x^1 - x^2 + x^3 = 1$$

je nehomogenní. □

Tvrzení 3.6.1. (1) Pokud nehomogenní soustava lineárních rovnic má právě jedno řešení, potom homogenizovaná soustava má jen nulové řešení.

(2) Nehomogenní soustava lineárních rovnic se čtvercovou maticí má právě jedno řešení právě tehdy, když homogenizovaná soustava má jen nulové řešení.

(3) Nehomogenní soustava lineárních rovnic se čtvercovou maticí má právě jedno řešení právě tehdy, když matice soustavy je regulární.

(4) *Nehomogenní soustava lineárních rovnic nemá nulové řešení.*

Důkaz. (1) Má-li soustava právě jedno řešení, potom žádná z neznámých není parametr a homogenizovaná soustava má jen nulové řešení.

(2) Vyplývá z předchozího bodu a z Gaussovy eliminační metody.

(3) Vyplývá z předchozího bodu a z Tvzení 3.5.1.

(4) Zřejmé. $\square$

Množina všech řešení nehomogenní soustavy nemá vlastnosti uvedené v Tvzení 3.5.2, které má množina všech řešení homogenizované soustavy. Totiž, součet řešení nehomogenní soustavy není její řešení, c -násobek řešení nehomogenní soustavy, kde $c \neq 1$, není její řešení a lineární kombinace řešení nehomogenní soustavy není její řešení.

Tvrzení 3.6.2. *Nechť ξ_p je nějaké řešení soustavy $Ax = b$. Potom pro každé řešení ξ této soustavy existuje jediné řešení ξ_0 homogenizované soustavy takové, že $\xi = \xi_p + \xi_0$.*

Na druhou stranu, pro libovolné řešení ξ_0 homogenizované soustavy je $\xi = \xi_p + \xi_0$ řešením soustavy $Ax = b$.

Důkaz. Budte ξ_p a ξ řešení soustavy. Položme $\xi_0 = \xi - \xi_p$. Potom $A\xi_0 = A(\xi - \xi_p) = A\xi - A\xi_p = b - b = 0$. Tedy, ξ_0 je řešení homogenizované soustavy a $\xi = \xi_0 + \xi_p$. Jednoznačnost ξ_0 je zřejmá.

Je-li $A\xi_0 = 0$, pak $A\xi = A(\xi_p + \xi_0) = A\xi_p + A\xi_0 = b + 0 = b$. $\square$

Důsledek. (1) *Má-li nehomogenní soustava řešení, potom její obecné řešení je součtem obecného řešení homogenizované soustavy a nějakého partikulárního řešení nehomogenní soustavy.*

(2) *Je-li ξ_p řešení soustavy $Ax = b$, potom množina všech řešení této soustavy je*

$$\{\xi_p + \xi_0 \mid \xi_0 \text{ je řešení homogenizované soustavy } Ax = 0\}.$$

Cvičení. Rozdíl libovolných dvou řešení nehomogenní soustavy je řešení homogenizované soustavy. $\square$

Příklad. (1) Jedno z řešení soustavy

$$x^1 - x^2 = 1$$

je $(1, 0)$. Množina všech řešení homogenizované soustavy

$$x^1 - x^2 = 0$$

je $\{(t, t) \mid t \in \mathbb{R}\}$. Množina všech řešení nehomogenní soustavy

$$x^1 - x^2 = 1$$

je $\{(1, 0) + (t, t) \mid t \in \mathbb{R}\} = \{(1 + t, t) \mid t \in \mathbb{R}\}$.

(2) Soustava

$$x^1 + 2x^2 = 0$$

$$3x^1 + 4x^2 = 2$$

má řešení $(2, -1)$. Množina všech řešení homogenizované soustavy

$$x^1 + 2x^2 = 0$$

$$3x^1 + 4x^2 = 0$$

je $\{(0, 0)\}$. Množina všech řešení nehomogenní soustavy

$$x^1 + 2x^2 = 0$$

$$3x^1 + 4x^2 = 2$$

je $\{(2, -1) + (0, 0)\} = \{(2, -1)\}$.

□

4. POLYNOMY

4.1. Polynomy, algebraické vlastnosti, dělitelnost

Definice 4.1.1. Buď P pole, $n \in \mathbb{N}$, $a_0, \dots, a_n \in P$, $x \notin P$. *Polynom (mnohočlen)* jedné neurčité x nad polem P je výraz tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0.$$

Zde x^i jsou mocniny, nejedná se o horní indexy. Mocninu x^0 klademe rovnu $1 \in P$, takže $a_0 = a_0 \cdot 1 = a_0 x^0$. Množinu všech polynomů neurčité x nad polem P označujeme $P[x]$.

Prvky $a_0, \dots, a_n \in P$ jsou *koefficienty*, a_i je *i -tý koefficient*. Koefficient a_0 je *absolutní člen*.

Polynom se všemi koefficienty nulovými je *nulový polynom* a označujeme ho 0.

Sčítance $a_i x^i$ s nulovými koefficienty a_i se v zápisu polynomu obvykle neuvádí, ty s nenulovými koefficienty se samozřejmě uvádí a neuvedené koefficienty a_i jsou tedy nulové.

Vyjádření „polynom nad polem P “ tedy znamená, že se jedná o „polynom s koefficienty z pole P “.

Příklad. $6x^4 + 0x^3 + 3x^2 + 1x + 6 \in \mathbb{R}[x]$, $a_0 = 6$, $a_1 = 1$, $a_2 = 3$, $a_3 = 0$, $a_4 = 6$, pro $i > 4$ $a_i = 0$. □

Definice 4.1.2. Polynomy $f, g \in P[x]$,

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

$$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

se sobě *rovnají*, jestliže se rovnají jejich příslušné koefficienty. Tedy,

$$f = g, \text{ jestliže } a_i = b_i \text{ pro všechna nezáporná celá } i.$$

Definice 4.1.3. *Stupeň* polynomu $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ je největší číslo s takové, že $a_s \neq 0$, označujeme ho $\deg f$. Koefficient a_s , kde s je stupeň, je *vedoucí koefficient* polynomu f , označujeme ho $\text{lc } f$.

Pro nulový polynom nemáme definován ani stupeň ani vedoucí koefficient.

Příklad. Pro $f = 6x^4 + 3x^2 + x + 6$ je $\deg f = 4$ a $\text{lc } f = 6$. □

Definice 4.1.4. Nulový polynom a polynomy stupně 0 jsou *konstantní*, polynomy stupně 1 jsou *lineární*, polynomy stupně 2 jsou *kvadratické*, polynomy stupně 3 jsou *kubické*, polynomy stupně 4 jsou *bikvadratické*.

Definice 4.1.5. Pro polynomy $f, g \in P[x]$,

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

$$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0,$$

označme $p = \max\{n, m\}$. *Součet* polynomů f a g je polynom $f + g \in P[x]$,

$$f + g = (a_p + b_p)x^p + (a_{p-1} + b_{p-1})x^{p-1} + \dots + (a_1 + b_1)x + a_0 + b_0.$$

Definice 4.1.6. *Součin* polynomů $f, g \in P[x]$,

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

$$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0,$$

je polynom $fg \in P[x]$,

$$\begin{aligned} fg &= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k = \\ &= a_n b_m x^{n+m} + \\ &\quad + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \\ &\quad \vdots \\ &\quad + (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + \\ &\quad + (a_1 b_0 + a_0 b_1) x + \\ &\quad + a_0 b_0. \end{aligned}$$

Tedy, pro $k \in \{0, 1, \dots, n+m\}$ k -tý koeficient polynomu fg je

$$\sum_{i+j=k} a_i b_j = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k.$$

Je-li například f konstantní polynom, $f = a_0$, pak

$$fg = a_0 g = a_0 b_m x^m + a_0 b_{m-1} x^{m-1} + \cdots + a_0 b_1 x + a_0 b_0.$$

Speciálně, pokud $f = -1$, pak

$$fg = -g = -b_m x^m - b_{m-1} x^{m-1} - \cdots - b_1 x - b_0$$

je polynom *opačný* k polynomu g .

Příklad. Pro

$$f = 6x^4 + 3x^2 + 6, \quad g = x^3 - 2x^2 - x$$

je

$$f + g = 6x^4 + x^3 + x^2 - x + 6,$$

$$fg = 6x^7 - 12x^6 - 3x^5 - 6x^4 + 3x^3 - 12x^2 - 6x. \quad \square$$

Tvrzení 4.1.1. *Budte $f, g \in P[x]$ nenulové. Potom*

- (1) fg je nenulový polynom,
- (2) $\deg(fg) = \deg f + \deg g$,
- (3) $\text{lc}(fg) = \text{lc } f \cdot \text{lc } g$.

Důkaz. Budte f, g nenulové polynomy. Nechť $\deg f = n$, $\deg g = m$, $\text{lc } f = a_n$ a $\text{lc } g = b_m$. Jelikož $a_n \neq 0$ a $b_m \neq 0$, také $a_n b_m \neq 0$, viz kapitola 6. Ovšem, $a_n b_m$ je $(n+m)$ -tý koeficient součinu fg , takže fg je nenulový polynom. Pro $k > n+m$ je k -tý koeficient roven nule, takže $\text{lc } fg = a_n b_m = \text{lc } f \cdot \text{lc } g$ a $\deg(fg) = n+m = \deg f + \deg g$. $\square$

Cvičení. Součin polynomů je nulový právě tehdy, když aspoň jeden z nich je nulový. $\square$

Tvrzení 4.1.2. *Budte $f, g, h \in P[x]$. Potom*

- | | |
|----------------------------------|--|
| (1) $f + g = g + f,$ | (5) $f \cdot g = g \cdot f,$ |
| (2) $f + (g + h) = (f + g) + h,$ | (6) $f \cdot (g \cdot h) = (f \cdot g) \cdot h,$ |
| (3) $f + 0 = f,$ | (7) $f \cdot 1 = f,$ |
| (4) $f + (-f) = 0,$ | (8) $f \cdot (g + h) = f \cdot g + f \cdot h.$ |

Důkaz. Cvičení. □

Tvrzení 4.1.3. *Nechť $f, g, h \in P[x]$, $fg = fh$ a $f \neq 0$. Pak $g = h$.*

Důkaz. Jestliže $fg = fh$, pak $f(g - h) = 0$ a aspoň jeden z polynomů f a $g - h$ je nulový. Podle předpokladu $f \neq 0$, takže $g - h = 0$ a $g = h$. □

Podobně jako v případě matic nebo v případě prvků nějakého pole je možné definovat inverzní polynom.

Definice 4.1.7. Budťe $f, g \in P[x]$. Polynom g je *inverzní* k polynomu f , jestliže $fg = gf = 1$. Inverzní polynom k polynomu f značíme f^{-1} . Polynom, ke kterému existuje polynom inverzní, je *invertibilní*. Množina všech invertibilních prvků $P[x]$ nebo P se značí $P[x]^*$, resp. P^* .

Tvrzení 4.1.4. *Invertibilní polynomy jsou právě nenulové konstantní polynomy (tedy polynomy stupně 0).*

Důkaz. Existuje-li k polynomu f inverze f^{-1} , potom $ff^{-1} = 1$ a oba polynomy f, f^{-1} jsou nenulové. Dále $\deg f \leq \deg f + \deg f^{-1} = \deg(ff^{-1}) = \deg 1 = 0$. Takže $\deg f = 0$ a f je tedy nenulový konstantní polynom.

Na druhou stranu, pokud f je nenulový konstantní polynom, můžeme ho ztotožnit s příslušným prvkem pole, ke kterému díky vlastnostem pole existuje prvek inverzní a ten zase můžeme ztotožnit s příslušným polynomem, který je tedy inverzní k f . □

Nyní se budeme věnovat dělitelnosti polynomů. Teorie dělitelnosti polynomů a teorie dělitelnosti celých čísel si jsou dosti podobné.

Definice 4.1.8. Budťe $f, g \in P[x]$. Polynom g *dělí* polynom f , jestliže existuje polynom $h \in P[x]$ takový, že $f = gh$. Pak také polynom g je *dělitel* polynomu f a polynom f je *dělitelný* polynomem g . Zapisujeme $g \mid f$.

Cvičení. Jestliže $g \mid f$ a $f \neq 0$, pak $\deg g \leq \deg f$. □

Příklad. (1) $x \mid x^2 - x$, protože $x^2 - x = x(x - 1)$.

(2) x nedělí $x^2 + 1$. Aby $x \cdot h$ byl polynom stupně 2, h musí být stupně 1, ale pro jakýkoliv polynom $h = a_1x + a_0$ stupně 1 platí $x \cdot h = a_1x^2 + a_0x$. □

Cvičení. (1) Ukažte, že $x - 1 \mid x^n - 1$ pro každé celé $n > 1$.

(2) Ukažte, že relace $\mid$ je reflexivní a tranzitivní. □

Tvrzení 4.1.5. *Budťe $f, g, h \in P[x]$.*

- (1) $f \mid f$ a $f \mid 0$.
- (2) Jestliže $f \mid g$ a $g \mid h$, pak $f \mid h$.
- (3) Jestliže $f \mid g$ a $f \mid h$, pak $f \mid (g + h)$.
- (4) Jestliže $f \mid g$, pak $f \mid (gh)$.
- (5) Jestliže $fg \mid fh$ a $f \neq 0$, pak $g \mid h$.

Důkaz. Cvičení. □

Podobně jako v případě celých čísel i v případě polynomů existuje dělení se zbytkem (nebo neúplné dělení).

Tvrzení 4.1.6. *Budte $f, g \in P[x]$, $g \neq 0$. Pak existuje právě jedna dvojice $q, r \in P[x]$ taková, že*

- (i) $f = gq + r$;
- (ii) *buď $r = 0$ nebo $\deg r < \deg g$.*

Důkaz. Jestliže $f = 0$, tak pro dvojici $q = 0, r = 0$ jsou splněny podmínky (i) a (ii).

Předpokládejme, že $f \neq 0$. Položme $q_0 = 0$ a $r_0 = f$ a definujme rekurzivně

$$q_{i+1} = q_i + \frac{\text{lc } r_i}{\text{lc } g} \cdot x^{\deg r_i - \deg g}, \quad r_{i+1} = r_i - \frac{\text{lc } r_i}{\text{lc } g} \cdot x^{\deg r_i - \deg g} \cdot g.$$

Potom pro každé i platí $f = gq_i + r_i$ a buď $r_{i+1} = 0$ nebo $\deg r_{i+1} < \deg r_i$. Proto pro nějaké i buď $r_i = 0$ nebo $\deg r_i < \deg g$. V takovém případě v rekurzi nepokračujeme a poslední dvojice q_i, r_i je hledaná dvojice q, r .

Ještě je třeba dokázat jednoznačnost. Předpokládejme, že pro dvojice q_1, r_1 a q_2, r_2 jsou splněny podmínky (i) a (ii). Tedy,

$$f = gq_1 + r_1 = gq_2 + r_2, \text{ čili } g(q_1 - q_2) = r_2 - r_1 \text{ a } g \mid r_2 - r_1 \quad (1)$$

$$r_1 = 0 \text{ nebo } \deg r_1 < \deg g \quad (2)$$

$$r_2 = 0 \text{ nebo } \deg r_2 < \deg g. \quad (3)$$

Kdyby $r_2 - r_1 \neq 0$, tak z (1) vyplývá, že $\deg g \leq \deg(r_2 - r_1)$, zatímco z (2) a (3) vyplývá, že $\deg(r_2 - r_1) < \deg g$. Dostáváme spor, takže $r_2 - r_1 = 0$, čili $r_1 = r_2$. Vzhledem k tomu, že $g \neq 0$, z $g(q_1 - q_2) = 0$ vyplývá, že $q_1 - q_2 = 0$, čili $q_1 = q_2$. □

Definice 4.1.9. V předchozím tvrzení q je *částečný podíl* (*podíl*, je-li $r = 0$) polynomů f a g (v tomto pořadí) a r je příslušný *zbytek*.

Je zřejmé, že $g \mid f$ právě tehdy, když zbytek při (částečném) podílu polynomů f a g je roven nule.

Příklad. Budte $f, g \in \mathbb{R}[x]$,

$$f = x^5 + 2x^3 + 2x + 4 \quad \text{a} \quad g = x^2 + x + 2.$$

Tedy $q_0 = 0, r_0 = f$ a polynomy $q_1, \dots, q_4$ a $r_1, \dots, r_4$ je možné získat pomocí schématu

$$\begin{array}{rcl}
 (x^5 + 2x^3 + 2x + 4) : (x^2 + x + 2) & = & \underbrace{x^3}_{q_1} - x^2 + x + 1 + \frac{-x+2}{x^2+x+2} \\
 -(x^5 + x^4 + 2x^3) & & \underbrace{-x^2}_{q_2} + x + 1 + \frac{-x+2}{x^2+x+2} \\
 \hline
 r_1 = -x^4 + 2x + 4 & & \underbrace{x + 1}_{q_3} + \frac{-x+2}{x^2+x+2} \\
 -(-x^4 - x^3 - 2x^2) & & \underbrace{-x^2}_{q_4} + x + 1 + \frac{-x+2}{x^2+x+2} \\
 \hline
 r_2 = x^3 + 2x^2 + 2x + 4 & & \\
 -(x^3 + x^2 + 2x) & & \\
 \hline
 r_3 = x^2 + 4 & & \\
 -(x^2 + x + 2) & & \\
 \hline
 r_4 = -x + 2 & &
 \end{array}$$

Čili

$$\begin{array}{ll} q_0 = 0 & r_0 = x^5 + 2x^3 + 2x + 4 \\ q_1 = x^3 & r_1 = -x^4 + 2x + 4 \\ q_2 = x^3 - x^2 & r_2 = x^3 + 2x^2 + 2x + 4 \\ q_3 = x^3 - x^2 + x & r_3 = x^2 + 4 \\ q_4 = x^3 - x^2 + x + 1 & r_4 = -x + 2 \end{array}$$

a je snadné ověřit, že $f = gq_i + r_i$ pro každé $i \in \{0, 1, 2, 3, 4\}$.

Jelikož $\deg r_4 = 1 < 2 = \deg g$,

$$\text{částečný podíl } q = q_4 = x^3 - x^2 + x + 1 \quad \text{a} \quad \text{zbytek } r = r_4 = -x + 2.$$

Tedy

$$f = x^5 + 2x^3 + 2x + 4 = gq + r = (x^2 + x + 2) \cdot (x^3 - x^2 + x + 1) + (-x + 2). \quad \square$$

Definice 4.1.10. Nenulový polynom, jehož vedoucí koeficient je 1, je *normovaný*.

Je-li $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ nenulový polynom s $\text{lc } f = a_n \neq 0$, pak

$$\bar{f} = \frac{1}{\text{lc } f} f = x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \dots + \frac{a_1}{a_n} x + \frac{a_0}{a_n}$$

je normovaný polynom. Polynomy $f, \bar{f}$ jsou z hlediska dělitelnosti rovnocenné ($f \mid \bar{f}$ a $\bar{f} \mid f$).

Lemma 4.1.7. *Budte f, g normované polynomy takové, že $f \mid g$ a $g \mid f$. Potom $f = g$.*

Důkaz. Předpokládejme, že $f \mid g$ a zároveň $g \mid f$. Potom existují polynomy $p, q \in P[x]$ tak, že $g = fp$ a $f = gq$. Máme $f = fpq$ a tedy $1 = pq$. Polynomy p, q jsou tedy nenulové konstantní polynomy a $1 = \text{lc } g = \text{lc}(fp) = \text{lc } f \cdot \text{lc } p = 1 \cdot p = p$. Takže $g = fp = f$. $\square$

Relace dělitelnosti mezi normovanými polynomy je tedy navíc antisymetrická, čili je to uspořádání a máme uspořádanou množinu všech normovaných polynomů.

4.2. Největší společný dělitel

Definice 4.2.1. Budte $f, g \in P[x]$. Polynom $d \in P[x]$ je *největší společný dělitel* polynomů f, g , jestliže

- (1) $d \mid f$ a $d \mid g$;
- (2) když $h \in P[x]$, $h \mid f$ a $h \mid g$, pak $h \mid d$;
- (3) d je normovaný.

Zapisujeme $d = D(f, g)$.

Definice 4.2.2. Polynomy, jejichž největší společný dělitel je 1, jsou *nesoudělné*.

Příklad. (1) $D(2x, x^2) = x$.

(2) Polynomy x a $x + 1$ jsou nesoudělné. Oba polynomy jsou stupně 1, proto jejich dělitele jsou stupně buď 1 nebo 0. Lineární dělitele polynomu x jsou cx , kde $c \in P$, ale žádný z nich není dělitelem $x + 1$. Společné dělitele polynomů x a $x + 1$ jsou tedy jen nenulové konstantní polynomy a jelikož největší společný dělitel je navíc normovaný, $D(x, x + 1) = 1$.

(3) Pokud $f = g = 0$, pak neexistuje jejich největší společný dělitel.

(4) Pro $f \neq 0$ $D(f, 0) = \bar{f}$. □

Tvrzení 4.2.1 (Eukleidův algoritmus). *Buďte $f, g \in P[x]$ nenulové polynomy. Buď $r_0, r_1, r_2, r_3, \dots$ posloupnost polynomů taková, že $r_0 = f$, $r_1 = g$ a jsou-li známy r_i, r_{i+1} , pak r_{i+2} získáme neúplným dělením polynomu r_i polynomem r_{i+1} :*

$$r_i = r_{i+1}q_i + r_{i+2}, \quad \text{buď } r_{i+2} = 0 \text{ nebo } \deg r_{i+2} < \deg r_{i+1}.$$

Potom existuje index N takový, že $r_{N-1} \neq 0$ a $r_N = 0$.

Důkaz. Jelikož $\deg g = \deg r_1 > \deg r_2 > \deg r_3 > \dots$ je klesající posloupnost nezáporných celých čísel, existuje $N \in \mathbb{N}$ takové, že $r_{N-1} \neq 0$ a $r_N = 0$. □

Příklad. Buďte $f, g \in \mathbb{R}[x]$,

$$f = x^5 + 2x^3 + 2x + 4 \quad \text{a} \quad g = x^2 + x + 2.$$

Tedy $r_0 = f$, $r_1 = g$ a už víme, že $f = g \cdot (x^3 - x^2 + x + 1) + (-x + 2)$, takže

$$r_2 = -x + 2 \quad \text{a} \quad q_0 = x^3 - x^2 + x + 1.$$

Dělením polynomu r_1 polynomem r_2

$$\begin{array}{r} (x^2 + x + 2) : (-x + 2) = -x - 3 + \frac{8}{-x+2} \\ -(x^2 - 2x) \\ \hline 3x + 2 \\ -(-3x - 6) \\ \hline 8 \end{array}$$

dostaneme

$$r_3 = 8 \quad \text{a} \quad q_1 = -x - 3.$$

Dělením polynomu r_2 polynomem r_3

$$\begin{array}{r} (-x + 2) : (8) = -\frac{x}{8} + \frac{2}{8} \\ -(-x) \\ \hline 2 \\ -2 \\ \hline 0 \end{array}$$

dostaneme

$$r_4 = 0 \quad \text{a} \quad q_2 = -\frac{x}{8} + \frac{2}{8}.$$

V tomto případě tedy $N = 4$. □

Tvrzení 4.2.2. *Pro libovolné dva polynomy, z nichž aspoň jeden je nenulový, existuje právě jeden jejich největší společný dělitel.*

Důkaz. Buďte $f, g \in P[x]$. Je-li $f \neq 0$ a $g = 0$, $D(f, 0) = \bar{f}$. Předpokládejme, že f, g jsou nenulové, a aplikujme Eukleidův algoritmus. Buď $N \in \mathbb{N}$ takové, že $r_{N-1} \neq 0$ a $r_N = 0$.

Označme $d = \bar{r}_{N-1}$ (normovaný polynom). Zřejmě $d \mid r_{N-1}$ a $d \mid r_N$. Je-li d dělitel polynomů r_{i+1} a r_{i+2} , pak je dělitel i polynomu $r_i = r_{i+1}q_i + r_{i+2}$. Postupně tedy dostaneme, že $d \mid r_i$ pro všechna $i \in \{0, \dots, N\}$, včetně $d \mid r_1 = g$ a $d \mid r_0 = f$.

Buď $h \in P[x]$ takové, že $h \mid f = r_0$ a $h \mid g = r_1$. Je-li h dělitel polynomů r_i a r_{i+1} , pak je dělitel i polynomu $r_{i+2} = r_i - r_{i+1}q_i$. Takto postupně dostaneme, že $h \mid r_i$ pro všechna $i \in \{0, \dots, N\}$, včetně $h \mid r_{N-1} = d$. Tedy, $d = D(f, g)$.

Buďte d_1, d_2 největší společné dělitele polynomů. Podle definice největšího společného dělitele $d_1 \mid d_2$ a $d_2 \mid d_1$ a jelikož d_1, d_2 jsou normované, $d_1 = d_2$. □

Příklad. Budte $f, g \in \mathbb{R}[x]$,

$$f = x^5 + 2x^3 + 2x + 4 \quad \text{a} \quad g = x^2 + x + 2.$$

Už víme, že $N = 4$ a $r_3 = 8$, čili $D(f, g) = \bar{r}_3 = 1$. □

Tvrzení 4.2.3 (Bézoutova věta). *Budte $f, g \in P[x]$ polynomy, z nichž aspoň jeden je nenulový. Pak existují polynomy $u, v \in P[x]$ takové, že $D(f, g) = fu + gv$.*

Důkaz. Označme $I = \{fu + gv \mid u, v \in P[x]\}$. V množině I existuje normovaný prvek minimálního stupně, označme jej d . Tedy, $d = fu + gv$ pro nějaká $u, v \in P[x]$.

Po dělení se zbytkem dostaneme $f = dq + r$, kde buď $r = 0$ nebo $\deg r < \deg d$. Zároveň $r = f - dq = f - (fu + gv)q = f(1 - uq) + g(-vq) \in I$. Kdyby $r \neq 0$, byl by to nenulový prvek I stupně nižšího než $\deg d$. Takže $r = 0$ a tedy $d \mid f$. Analogicky $d \mid g$.

Buď $h \in P[x]$ společný dělitel f a g . Pak h je dělitel i polynomu $fu + gv = d$. Tedy, $d = D(f, g)$. □

Pomocí Rozšířeného Eukleidova algoritmu lze získat nejen $D(f, g)$, ale i polynomy u, v z předchozího tvrzení.

Tvrzení 4.2.4 (Rozšířený Eukleidův algoritmus). *Budte $f, g \in P[x]$ nenulové polynomy. Budte $r_0, r_1, r_2, \dots, r_{N-1}$ a $q_0, q_1, q_2, \dots, q_{N-3}$ posloupnosti polynomů z Eukleidova algoritmu. Budte*

$$u_0 = 1, u_1 = 0, u_2, \dots, u_{N-1},$$

$$v_0 = 0, v_1 = 1, v_2, \dots, v_{N-1},$$

posloupnosti polynomů takové, že $u_i = u_{i+1}q_i + u_{i+2}$ a $v_i = v_{i+1}q_i + v_{i+2}$ pro všechna $i \in \{0, \dots, N-3\}$. Potom $r_{N-1} = fu_{N-1} + gv_{N-1}$ a označíme-li

$$u = \frac{1}{\text{lc } r_{N-1}} u_{N-1} \quad \text{a} \quad v = \frac{1}{\text{lc } r_{N-1}} v_{N-1},$$

pak $D(f, g) = fu + gv$.

Důkaz. Podle Eukleidova algoritmu a podle předpokladů

$$r_0 = f, \quad r_1 = g, \quad u_0 = 1, \quad u_1 = 0, \quad v_0 = 0, \quad v_1 = 1$$

a pro $i \in \{0, \dots, N-3\}$

$$r_i = r_{i+1}q_i + r_{i+2}, \quad \text{tedy} \quad r_{i+2} = r_i - r_{i+1}q_i, \quad (4)$$

$$u_i = u_{i+1}q_i + u_{i+2}, \quad \text{tedy} \quad u_{i+2} = u_i - u_{i+1}q_i, \quad (5)$$

$$v_i = v_{i+1}q_i + v_{i+2}, \quad \text{tedy} \quad v_{i+2} = v_i - v_{i+1}q_i. \quad (6)$$

Matematickou indukcí ukážeme, že $r_i = fu_i + gv_i$ pro všechna $i \in \{0, \dots, N-1\}$. Platí

$$r_0 = f = f \cdot 1 + g \cdot 0 = f \cdot u_0 + g \cdot v_0,$$

$$r_1 = g = f \cdot 0 + g \cdot 1 = f \cdot u_1 + g \cdot v_1.$$

Předpokládejme, že pro nějaké k platí

$$r_k = fu_k + gv_k, \quad (7)$$

$$r_{k+1} = fu_{k+1} + gv_{k+1}. \quad (8)$$

Potom

$$\begin{aligned}
 r_{k+2} &= && \text{(podle (4))} \\
 &= r_k - r_{k+1}q_k = && \text{(podle (7), (8))} \\
 &= fu_k + gv_k - (fu_{k+1} + gv_{k+1})q_k = \\
 &= f(u_k - u_{k+1}q_k) + g(v_k - v_{k+1}q_k) = && \text{(podle (5), (6))} \\
 &= fu_{k+2} + gv_{k+2}.
 \end{aligned}$$

Takže, vztah $r_i = fu_i + gv_i$ platí pro $i = 0, i = 1$ a když platí pro $i = k$ a $i = k + 1$, pak platí pro $i = k + 2$. Z toho vyplývá, že platí pro každé $i \in \{0, \dots, N - 1\}$. Zbytek tvrzení je zřejmý. $\square$

Příklad. Budťe $f, g \in \mathbb{R}[x]$,

$$f = x^5 + 2x^3 + 2x + 4 \quad \text{a} \quad g = x^2 + x + 2.$$

Už víme, že $D(f, g) = 1$, $N = 4$,

$$\begin{aligned}
 r_0 &= x^5 + 2x^3 + 2x + 4 & q_0 &= x^3 - x^2 + x + 1 \\
 r_1 &= x^2 + x + 2 & q_1 &= -x - 3 \\
 r_2 &= -x + 2 \\
 r_3 &= 8
 \end{aligned}$$

$$\begin{aligned}
 u_0 &= 1 & v_0 &= 0 \\
 u_1 &= 0 & v_1 &= 1.
 \end{aligned}$$

Dále

$$\begin{aligned}
 u_0 &= u_1q_0 + u_2 \\
 1 &= 0 \cdot q_0 + u_2 && \text{implikuje} \quad u_2 = 1, \\
 v_0 &= v_1q_0 + v_2 \\
 0 &= 1 \cdot q_0 + v_2 && \text{implikuje} \quad v_2 = -q_0 = -x^3 + x^2 - x - 1, \\
 u_1 &= u_2q_1 + u_3 \\
 0 &= 1 \cdot q_1 + u_3 && \text{implikuje} \quad u_3 = -q_1 = x + 3, \\
 v_1 &= v_2q_1 + v_3 \\
 1 &= -q_0 \cdot q_1 + v_3 && \text{implikuje} \quad v_3 = 1 + q_0q_1 = -x^4 - 2x^3 + 2x^2 - 4x - 2.
 \end{aligned}$$

Lze snadno ověřit, že $r_3 = fu_3 + gv_3$, a když

$$\begin{aligned}
 u &= \frac{x}{8} + \frac{3}{8} \\
 v &= -\frac{x^4}{8} - \frac{x^3}{4} + \frac{x^2}{4} - \frac{x}{2} - \frac{1}{4}
 \end{aligned}$$

pak $D(f, g) = 1 = fu + gv$. $\square$

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

Cvičení. Normovaný reducibilní polynom je součinem normovaných nekonstantních polynomů. $\square$

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 $f = g$. $\square$

Lemma 4.3.2. *Budte $g, h_1, \dots, h_n \in P[x]$ 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

$$1 = gu + h_1v$$

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

$$h_2 \cdots h_n = gh_2 \cdots h_nu + h_1h_2 \cdots h_nv.$$

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 $g = h_j$. $\square$

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 $\bar{f} = \frac{1}{\text{lc } f} \cdot f$. Je-li $\bar{f}$ ireducibilní, pak $f = \text{lc } f \cdot \bar{f}$. 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 $n = m$. $\square$

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. $\square$

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

4.4. Kořeny a jejich násobnost

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

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

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. $\square$

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

Tvrzení 4.4.2. Necht' $f \in P[x]$ 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 . $\square$