

### 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

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

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) Vyplyvá z předchozího bodu a z Gaussovy eliminační metody.

(3) Vyplyvá z předchozího bodu a z Tvrzení 3.5.1.

(4) Zřejmé. □

Množina všech řešení nehomogenní soustavy nemá vlastnosti uvedené v Tvrzení 3.5.2, které má množina všech řešení homogenní 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  $\xi_p$  je nějaké řešení soustavy  $Ax = b$ . Potom pro každé řešení  $\xi$  této soustavy existuje jediné řešení  $\xi_0$  homogenizované soustavy takové, že  $\xi = \xi_p + \xi_0$ .

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

*Důkaz.* Buďte  $\xi_p$  a  $\xi$  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,  $\xi_0$  je řešením homogenizované soustavy a  $\xi = \xi_0 + \xi_p$ . Jednoznačnost  $\xi_0$  je zřejmá.

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

**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  $\xi_p$  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  $\{(2, -1) + (0, 0)\} = \{(2, -1)\}$ .  $\square$



## 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 *koeficienty*,  $a_i$  je  *$i$ -tý koeficient*. Koeficient  $a_0$  je *absolutní člen*.

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

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

**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 koeficienty. 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  $\deg f$ . Koeficient  $a_s$ , kde  $s$  je stupeň, je *vedoucí koeficient* polynomu  $f$ , označujeme ho  $\text{lc } f$ .

Pro nulový polynom nemáme definován ani stupeň ani vedoucí koeficient.

**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.** *Součín* 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  $a_n \neq 0$ ,  $b_m \neq 0$  a  $(n+m)$ -tý koeficient součinu  $fg$  je roven  $a_n b_m$ , je  $fg$  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.** Součín 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.** Budte  $f, g \in P[x]$ . 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.** Budte  $f, g \in P[x]$ . 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.** *Budte  $f, g, h \in P[x]$ .*

- (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,

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

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

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

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

$$\begin{array}{r} (x^5 + 2x^3 + 2x + 4) : (x^2 + x + 2) = \underbrace{x^3}_{q_1} - x^2 + x + 1 + \frac{-x+2}{x^2+x+2} \\ \underline{-(x^5 + x^4 + 2x^3)} \phantom{+ 2x + 4} \\ r_1 = -x^4 \phantom{+ 2x + 4} \\ \underline{-(-x^4 - x^3 - 2x^2)} \phantom{+ 2x + 4} \\ r_2 = x^3 + 2x^2 + 2x + 4 \\ \underline{-(x^3 + x^2 + 2x)} \\ r_3 = x^2 + 4 \\ \underline{-(x^2 + x + 2)} \\ r_4 = -x + 2 \end{array}$$

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  $\deg r_4 = 1 < 2 = \deg g$ ,

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

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.** Normovaný polynom je nenulový polynom, jehož vedoucí koeficient je 1.

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.** Buďte  $f, g$  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.** Buďte  $f, g \in P[x]$ . 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.** 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  $D(f, g) = 1$ ,  $N = 4$ ,

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

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

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