7. přednáška, 8. 11. 2022

4.6. Nehomogenní soustavy lineárních rovnic

Definice 4.6.1. Soustava lineárních rovnic s nenulovou pravou stranou se nazývá *nehomogenní.* Je-li $Ax = b$ nehomogenní soustava, potom $Ax = 0$ se nazývá *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 4.6.1. *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 $\xi = \xi_p + \xi_0$ řešení soustavy $Ax = b$.

Důkaz. Buďte 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 $A\xi = A(\xi_p + \xi_0) = A\xi_p + A\xi_0 = b + 0 = b$. □

Důsledek. *Je-li ξ_p řešení soustavy $Ax = b$, potom množina všech řešení této soustavy je*

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

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

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

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

(2) Soustava

$$\begin{aligned} x^1 + 2x^2 &= 0 \\ 3x^1 + 4x^2 &= 2 \end{aligned}$$

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

$$\begin{aligned} x^1 + 2x^2 &= 0 \\ 3x^1 + 4x^2 &= 0 \end{aligned}$$

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

$$\begin{aligned} x^1 + 2x^2 &= 0 \\ 3x^1 + 4x^2 &= 2 \end{aligned}$$

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

5. Polynomy

5.1. Polynomy, algebraické vlastnosti, dělitelnost

Definice 5.1.1. Buď P pole, $n \in \mathbb{N}$, $a_0, \ldots, a_n \in P$, $x \notin P$. *Polynom* (*mnohočlen*) jedné neurčité x nad polem P je výraz tvaru

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

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 $a_0, \ldots, a_n \in P$ jsou *koeficienty*, a_i je *i-tý koeficient*. Koeficient a_0 je *absolutní člen*. 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. Polynom se všemi koeficienty nulovými je *nulový polynom* a označujeme ho 0.

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

Definice 5.1.2. Polynomy

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$
$$g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

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

$$f = g, \text{ jestliže } a_0 = b_0, a_1 = b_1, \ldots$$

Definice 5.1.3. *Stupeň* polynomu $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 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 $\operatorname{lc} f$.

Pro nulový polynom nemáme definován ani stupeň ani vedoucí koeficient.

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

Definice 5.1.4. 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 5.1.5. Mějme polynomy

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$
$$g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

Označme $p = \max\{n, m\}$. *Součet* polynomů f a g je polynom

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

Součin polynomů f a g je polynom

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

Tedy, pro $k \in \{0, 1, \ldots, n+m\}$ 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

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

je

$$f + g = 6x^4 + x^3 + x^2 - x + 6,$$
$$fg = 6x^7 - 12x^6 - 3x^5 - 6x^4 + 3x^3 - 12x^2 - 6x.$$ ■

Tvrzení 5.1.1. *Buďte $f, g \in P[x]$ nenulové. Potom fg je nenulový polynom a*

$$\deg(fg) = \deg f + \deg g,$$
$$\operatorname{lc}(fg) = \operatorname{lc} f \cdot \operatorname{lc} g.$$

Důkaz. Buďte f, g nenulové polynomy. Nechť $\deg f = n$, $\deg g = m$, $\operatorname{lc} f = a_n$ a $\operatorname{lc} g = b_m$. 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 $\operatorname{lc} fg = a_n b_m = \operatorname{lc} f \cdot \operatorname{lc} g$ a $\deg(fg) = n + m = \deg f + \deg g$. □

Cvičení. Součin polynomů je nulový právě tehdy, když aspoň jeden z nich je nulový. ▷

Tvrzení 5.1.2. *Buďte $f, g, h \in P[x]$. Potom*

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

Důkaz. Cvičení. □

Tvrzení 5.1.3. *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 5.1.6. Buďte $f, g \in P[x]$. 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 5.1.4. *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 5.1.7. Buďte $f, g \in P[x]$. 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 5.1.5. *Buďte $f, g, h \in P[x]$.*

(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 5.1.6. *Buďte $f, g \in P[x]$, $g \neq 0$. 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

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

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,

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

$$r_1 = 0 \text{ nebo } \deg r_1 < \deg g \tag{2}$$

$$r_2 = 0 \text{ nebo } \deg r_2 < \deg g. \tag{3}$$

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 5.1.8. V předchozím tvrzení q je *částečný podíl* (*podíl*, je-li $r = 0$) polynomů f a g a r je *zbytek*.

Je zřejmé, že $g \mid f$ právě tehdy, když zbytek je roven nule.

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

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

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

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

Čili

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

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

Jelikož $\deg r_4 = 1 < 2 = \deg g$,

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

Tedy

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

Definice 5.1.9. Polynom je *normovaný*, je-li nenulový a jeho vedoucí koeficient je 1.

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

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

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

Lemma 5.1.7. *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 $1 = \operatorname{lc} g = \operatorname{lc}(fp) = \operatorname{lc} f \cdot \operatorname{lc} p = 1 \cdot p = p$. 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.

5.2. Největší společný dělitel

Definice 5.2.1. Buďte $f, g \in P[x]$ nenulové. 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 5.2.2. 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) Pro $f \neq 0$ $D(f, 0) = \bar{f}$. ■

Tvrzení 5.2.1 (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}:*

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

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

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

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

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

Dělením polynomu r_1 polynomem r_2

$$\begin{array}{l} (x^2 + \ \ x + 2) : (-x + 2) = -x - 3 + \frac{8}{-x+2} \\ -\underline{(x^2 - 2x)} \\ \qquad\quad 3x + 2 \\ \quad\ -\underline{(-3x - 6)} \\ \qquad\qquad\quad 8 \end{array}$$

dostaneme

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

Dělením polynomu r_2 polynomem r_3

$$\begin{array}{l} (-x + 2) : (8) = -\frac{x}{8} + \frac{2}{8} \\ -\underline{(-x)} \\ \qquad\quad 2 \\ \qquad -\underline{2} \\ \qquad\quad 0 \end{array}$$

dostaneme

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

V tomto případě tedy $N = 4$. ■

Tvrzení 5.2.2. *Pro libovolné dva polynomy, z nichž aspoň jeden je nenulový, existuje 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 $i \in \{0, \ldots, N\}$, 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 $r_{i+2} = r_i - r_{i+1}q_i$. Postupně tedy dostaneme, že $h \mid r_i$ pro všechna $i \in \{0, \ldots, N\}$, včetně $h \mid r_{N-1} = d$. Tedy, $d = D(f, g)$. □

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

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

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

Tvrzení 5.2.3. *Libovolné dva polynomy mají nejvýše jeden největší společný dělitel.*

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

Tvrzení 5.2.4 (Bézoutova věta). *Buďte $f, g \in P[x]$ 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 5.2.5 (Rozšířený Eukleidův algoritmus.). *Buďte $f, g \in P[x]$ nenulové polynomy. Buďte $r_0, r_1, r_2, \ldots, r_{N-1}$ a $q_0, q_1, q_2, \ldots, q_{N-3}$ posloupnosti polynomů z Eukleidova algoritmu. Buďte*

$$u_0 = 1, u_1 = 0, u_2, \ldots, u_{N-1},$$
$$v_0 = 0, v_1 = 1, v_2, \ldots, v_{N-1},$$

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 $i \in \{0, \ldots, N - 3\}$. Potom $r_{N-1} = fu_{N-1} + gv_{N-1}$ a označíme-li

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

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

Důkaz. □

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

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

Už víme, že $D(f,g)=1,\ N=4$,

$$
\begin{aligned}
r_0 &= x^5+2x^3+2x+4 & q_0 &= x^3-x^2+x+1\\
r_1 &= x^2+x+2 & q_1 &= -x-3\\
r_2 &= -x+2 & &\\
r_3 &= 8 & &\\
\\
u_0 &= 1 & v_0 &= 0\\
u_1 &= 0 & v_1 &= 1.
\end{aligned}
$$

Dále

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

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 $D(f,g)=1=fu+gv$. ■