

6. přednáška, 4. 11. 2025

Tvrzení 4.1.2. *Bud'te $f, g, h \in P[x]$. 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. Bud'te $f, g \in P[x]$. 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. Bud'te $f, g \in P[x]$. 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.** *Bud'te $f, g, h \in P[x]$.*

- (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. *Bud'te $f, g \in P[x]$, $g \neq 0$. 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 $f = 0$ nebo $\deg f < \deg g$, dvojice $q = 0$, $r = f$ splňuje podmínky (i) a (ii).

Předpokládejme, že $f \neq 0$ a $\deg f \geq \deg g$. Položme $q_0 = 0$ a $r_0 = f$ a pro $i \in \mathbb{N}$ taková, že $r_i \neq 0$ a $\deg r_i \geq \deg g$, definujme rekurzivně

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

Jelikož stupeň polynomu

$$\frac{\text{lc } r_i}{\text{lc } g} \cdot x^{\deg r_i - \deg g} \cdot g$$

je roven $\deg r_i$ a jeho vedoucí koeficient je roven $\text{lc } r_i$, tak buď $r_{i+1} = 0$ nebo $\deg r_{i+1} < \deg r_i$. Proto existuje i_0 takové, že buď $r_{i_0} = 0$ nebo $\deg r_{i_0} < \deg g$. Navíc, $f = gq_0 + r_0$ a je-li $f = gq_i + r_i$ pro nějaké i , potom také $f = gq_{i+1} + r_{i+1}$. Takže dvojice $q = q_{i_0}$, $r = r_{i_0}$ splňuje podmínky (i) a (ii).

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

$$f = gq_1 + r_1 \quad f = gq_2 + r_2 \quad (1)$$

$$\text{buď } r_1 = 0 \text{ nebo } \deg r_1 < \deg g \quad \text{buď } r_2 = 0 \text{ nebo } \deg r_2 < \deg g. \quad (2)$$

Předpokládejme, že $r_2 - r_1 \neq 0$. Podle (5)

$$gq_1 + r_1 = gq_2 + r_2 \quad \text{tedy } g(q_1 - q_2) = r_2 - r_1 \quad \text{a } \deg g \leq \deg(r_2 - r_1), \quad (3)$$

zatímco z (2) vyplývá, že

$$\deg(r_2 - r_1) < \deg g. \quad (4)$$

Na základě předpokladu $r_2 - r_1 \neq 0$ 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. Buďte $f, g \in \mathbb{R}[x]$,

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

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

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

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. 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. Bud' $f, g \in P[x]$. 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) Největší společný dělitel polynomů $f = g = 0$ neexistuje.

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

Tvrzení 4.2.1 (Eukleidův algoritmus). Bud' $f, g \in P[x]$ nenulové polynomy. Bud' $r_0, r_1, r_2, r_3, \dots$ 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} :

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

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

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

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

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

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. Bud'te $f, g \in P[x]$. Je-li $f \neq 0$ a $g = 0$, $D(f, 0) = \bar{f}$. Předpokládejme, že f, g jsou nenulové, a aplikujme Eukleidův algoritmus. Bud' $N \in \mathbb{N}$ 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 $d \mid r_0 = f$.

Bud' $h \in P[x]$ 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, $d = D(f, g)$.

Bud'te 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. Bud'te $f, g \in \mathbb{R}[x]$,

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

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

Tvrzení 4.2.3 (Bézoutova věta). *Bud'te $f, g \in P[x]$ 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 $d \mid g$.

Bud' $h \in P[x]$ 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). *Bud'te $f, g \in P[x]$ nenulové polynomy. Bud'te $r_0, r_1, r_2, \dots, r_{N-1}$ a $q_0, q_1, q_2, \dots, q_{N-3}$ posloupnosti polynomů z Eukleidova algoritmu. Bud'te*

$$\begin{aligned} u_0 &= 1, u_1 = 0, u_2, \dots, u_{N-1}, \\ v_0 &= 0, v_1 = 1, v_2, \dots, v_{N-1}, \end{aligned}$$

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

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

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

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

$$u_i = u_{i+1}q_i + u_{i+2}, \quad \text{tedy} \quad u_{i+2} = u_i - u_{i+1}q_i, \quad (6)$$

$$v_i = v_{i+1}q_i + v_{i+2}, \quad \text{tedy} \quad v_{i+2} = v_i - v_{i+1}q_i. \quad (7)$$

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

$$r_k = fu_k + gv_k, \quad (8)$$

$$r_{k+1} = fu_{k+1} + gv_{k+1}. \quad (9)$$

Potom

$$\begin{aligned} r_{k+2} &= && \text{(podle (8))} \\ &= r_k - r_{k+1}q_k = && \text{(podle (11), (12))} \\ &= fu_k + gv_k - (fu_{k+1} + gv_{k+1})q_k = \\ &= f(u_k - u_{k+1}q_k) + g(v_k - v_{k+1}q_k) = && \text{(podle (9), (10))} \\ &= fu_{k+2} + gv_{k+2}. \end{aligned}$$

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. Buďte $f, g \in \mathbb{R}[x]$,

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

Už víme, že $D(f, g) = 1$, $N = 4$,

$$r_0 = x^5 + 2x^3 + 2x + 4 \quad q_0 = x^3 - x^2 + x + 1$$

$$r_1 = x^2 + x + 2 \quad q_1 = -x - 3$$

$$r_2 = -x + 2$$

$$r_3 = 8$$

$$u_0 = 1 \quad v_0 = 0$$

$$u_1 = 0 \quad v_1 = 1.$$

Dále

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

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 $D(f, g) = 1 = fu + gv$. □

4.3. Ireducibilní polynomy

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

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

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

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

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

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

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

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

Lemma 4.3.2. Bud'te $g, h_1, \dots, h_n \in P[x]$ normované ireducibilní polynomy a necht' $g \mid h_1 \cdots h_n$. 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 Tvzení 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 Tvzení 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 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 $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in P[x]$ a $\xi \in P$, označme

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

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

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

Důkaz. Cvičení. $\square$

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

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

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

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

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

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

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

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

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

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

Důkaz. Cvičení. $\square$

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

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

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

Tvrzení 4.4.5 (Vlastnosti kořenů (Viètovy vzorce)). *Bud'ťe $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x]$ 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

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

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 v algebraickém tvaru 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 $z_1 = a + bi$, $z_2 = c + di$

$$z_1 + z_2 = (a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$z_1 - z_2 = (a + bi) - (c + di) = (a - c) + (b - d)i,$$

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

pro $z_2 \neq 0$

$$\frac{z_1}{z_2} = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2}.$$

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

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

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

Cvičení. Pro komplexní čísla z_1, z_2

$$(z_1 + z_2)^* = z_1^* + z_2^*, \quad (z_1 z_2)^* = z_1^* z_2^*, \quad \left(\frac{z_1}{z_2}\right)^* = \frac{z_1^*}{z_2^*}. \quad \square$$

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. □

Absolutní hodnota komplexního čísla $z = a + bi$ je

$$|z| = \sqrt{a^2 + b^2} = \sqrt{zz^*}$$

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 . □

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:

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

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

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

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

Důkaz. Předpokládejme, že $\frac{p}{q}$ je kořenem polynomu f , tedy

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

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. Bud'

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x].$$

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. $\square$

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. $\square$

Tvrzení 4.6.3. *Bud' $f \in \mathbb{C}[x]$ 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. *Bud' $f \in \mathbb{C}[x]$.*

- (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. $\square$

4.7. Hornerovo schéma

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

- (i) $f = (x - \xi)q + r$;
- (ii) bud' $r = 0$ 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,

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

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 $= b_{n-1}$	$a_{n-1} + \xi b_{n-1}$ $= b_{n-2}$	$a_{n-2} + \xi b_{n-2}$ $= b_{n-3}$	$\dots$ $\dots$	$a_2 + \xi b_2$ $= b_1$	$a_1 + \xi b_1$ $= b_0$	$a_0 + \xi b_0$ $= r$

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.