

V. Polynomy jedné neurčité.

1. Algebraická definice polynomu.

Definice 1.1:

Je-li $(M, +, \cdot)$ libovolný okruh, pak polynomem nad okruhem M (s koeficienty z M) rozumíme libovolnou nekonečnou posloupnost $f = (a_0, a_1, a_2, \dots)$ prvků z M , ve které je pouze konečný počet prvků nenulových. Množinu všech polynomů nad okruhem M budeme značit $P(M)$. Tedy

$$P(M) = \{ (a_0, a_1, a_2, \dots); (\forall i) a_i \in M \wedge (\exists n) (\forall j) (j > n \Rightarrow a_j = 0) \}.$$

Definice 1.2:

Celé nezáporné číslo n se nazývá stupeň polynomu

$f = (a_0, a_1, a_2, \dots) \in P(M)$ právě když platí:

$a_n \neq 0 \wedge (\forall i \in N) (i > n \Rightarrow a_i = 0)$. Což značíme st $f = n$. Polynom $(0, 0, 0, \dots) \in P(M)$ se nazývá nulový polynom a pro něj není stupeň definován.

Poznámka 1.1:

Stupeň polynomu f je tedy největší celé nezáporné číslo n , pro které platí $a_n \neq 0$.

Definice 1.3:

Nechť $f = (a_0, a_1, a_2, \dots)$, $g = (b_0, b_1, b_2, \dots)$ jsou dva polynomy z $P(M)$. Na $P(M)$ definujeme rovnost $f=g$, součet $f+g$ a součin $f \cdot g$ polynomů takto:

a) $(a_0, a_1, a_2, \dots) = (b_0, b_1, b_2, \dots) \Leftrightarrow (\forall i \in N_0) a_i = b_i, (N_0 = N \cup \{0\})$.

b) $f+g = (a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) =$
 $= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots),$

c) $f \cdot g = (a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$, kde pro
 $k = 0, 1, 2, \dots$ položíme

$$c_k = \sum_{i=0}^k a_i b_{k-i} \quad \text{resp.} \quad c_k = \sum_{\substack{i, j \geq 0 \\ i+j=k}} a_i b_j.$$

Věta 1.1:

Pro libovolný okruh $(M, +, \cdot)$ je struktura $(P(M), +, \cdot)$ také okruh.

Důkaz:

Označme $f = (a_0, a_1, a_2, \dots)$ a $g = (b_0, b_1, b_2, \dots)$, $a_i, b_j \in M$. Pro každé $f, g \in P(M)$ je také $f+g \in P(M)$ a $f \cdot g \in P(M)$. Neboť podle definice sčítání a násobení polynomů je každý člen polynomů $f+g$ a $f \cdot g$ z okruhu M . Jestliže st $f = n_1$ a st $g = n_2$, stačí u operace sčítání položit $n = \max(n_1, n_2)$ a pro všechna $i > n$ máme $a_i + b_i = 0$. Tedy polynom $f+g$ má pouze konečný počet nenulových prvků z M . U operace násobení pak pro každé $k > n_1 + n_2$ je $c_k = 0$. Jelikož st $f = n_1$ a st $g = n_2$, je $a_i = 0$ pro každé $i > n_1$ a $b_j = 0$ pro každé $j > n_2$. Nechť $k > n_1 + n_2$. Jelikož

$$c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{\substack{i, j \geq 0 \\ i+j=k}} a_i b_j \quad \text{a } i+j = k > n_1 + n_2, \text{ pak není}$$

současně $i \leq n_1$, $j \leq n_2$ a tudíž v tomto případě je vždy $a_i b_j = 0$. Tedy $c_k = 0$ pro všechna $k > n_1 + n_2$ a polynom $f \cdot g$ má pouze konečný počet nenulových členů.

Dokázali jsme zatím, že obě operace $+$ a \cdot jsou na $P(M)$ uzavřené. Snadno se ověří, že $(P(M), +)$ je komutativní grupa. Asociativnost a komutativnost sčítání plyne z toho, že M je asociativní a komutativní vzhledem k operaci sčítání. Nulový polynom $(0, 0, 0, \dots) \in P(M)$ je nulový prvek v $P(M)$ a ke každému polynomu $f = (a_0, a_1, a_2, \dots)$ existuje právě jeden opačný prvek $-f = -(a_0, a_1, a_2, \dots) = (-a_0, -a_1, -a_2, \dots) \in P(M)$.

Obdobně lze ověřit, že $(P(M), \cdot)$ je asociativní, a že v $(P(M), +, \cdot)$ platí distributivní zákony. Využívá se při tom vlastnosti okruhu $(M, +, \cdot)$. Čtenář si tuto část důkazu může provést samostatně jako cvičení.

Poznámka 1.2:

Okruh $(M, +, \cdot)$ lze vždy považovat za podokruh okruhu $(P(M), +, \cdot)$. Označme $P'(M)$ množinu všech polynomů z $P(M)$ tvaru $(a, 0, 0, \dots)$, $a \in M$ a uvažujme zobrazení $\varphi: M \rightarrow P'(M)$ definované takto: $\forall a \in M$, $\varphi(a) = (a, 0, 0, \dots)$. Snadno se ověří, že φ je izomorfní zobrazení okruhu M na $P'(M) \subseteq P(M)$. Neboť pro každé $a, b \in M$ platí: $a \neq b$ právě když $(a, 0, 0, \dots) \neq (b, 0, 0, \dots)$, $\varphi(a+b) = (a+b, 0, 0, \dots) = (a, 0, 0, \dots) + (b, 0, 0, \dots) = \varphi(a) + \varphi(b)$ a $\varphi(a \cdot b) = (a \cdot b, 0, 0, \dots) = (a, 0, 0, \dots) \cdot (b, 0, 0, \dots) = \varphi(a) \cdot \varphi(b)$.

Ztotožníme-li každý prvek $a \in M$ s jeho obrazem $(a, 0, 0, \dots) \in P'(M) \subseteq P(M)$, můžeme okruh M uvažovat jako podokruh okruhu $P(M)$. Že

$P'(M)$ je podokruh v $P(M)$ je zřejmé. Předcházející úvahou jsme vlastně provedli izomorfní vnoření okruhu $(M, +, \cdot)$ do okruhu $(P(M), +, \cdot)$.

Nadále, když nemůže dojít k nedorozumění, budeme místo okruhu $(M, +, \cdot)$ psát stručně okruh M a místo okruhu polynomů $(P(M), +, \cdot)$ psát stručně okruh polynomů $P(M)$ resp. pouze okruh $P(M)$.

Věta 1.2:

Nechť M je okruh a $P(M)$ je okruh polynomů nad M . Potom platí:

- Okruh $P(M)$ je komutativní, právě když M je komutativní.
- Okruh $P(M)$ má jednotkový prvek, právě když M má jednotkový prvek.
- Okruh $P(M)$ je bez dělitelů nuly, právě když M je bez dělitelů nuly.

Důkaz:

- Je-li M komutativní, je $P(M)$ komutativní podle definice násobení polynomů. Je-li $P(M)$ komutativní je M komutativní, protože M je podokruh v $P(M)$. (Dědičná vlastnost).
- Nechť M má jednotkový prvek e , pak jistě $(e, o, o, \dots) \in P(M)$ je jednotkový prvek v $P(M)$, což se snadno ověří.

Nechť obráceně $P(M)$ má jednotkový prvek (e_0, e_1, e_2, \dots) . Vezmeme-li polynom $(a, o, o, \dots) \in P(M)$, kde a je libovolný prvek z M , musí nutně platit:

$$(a, o, o, \dots) \cdot (e_0, e_1, e_2, \dots) = (a, o, o, \dots) \quad \text{a odtud obdržíme} \\ a \cdot e_0 = a. \quad \text{Dále musí platit: } (e_0, e_1, e_2, \dots) \cdot (a, o, o, \dots) = \\ = (a, o, o, \dots), \quad \text{z čehož plyne } e_0 \cdot a = a. \quad \text{Tedy } e_0 \text{ je jednotkový} \\ \text{prvek v } M.$$

- Jelikož okruh $P(M)$ je bez dělitelů nuly, pak také jeho podokruh M je bez dělitelů nuly. (Dědičná vlastnost).

Nyní nechť M je bez dělitelů nuly. Ověříme, že platí implikace:

$$f, g \in P(M), \quad f \neq (o, o, o, \dots), \quad g \neq (o, o, o, \dots), \quad \text{pak } f \cdot g \neq \\ \neq (o, o, o, \dots). \quad \text{Nechť tedy } f = (a_0, a_1, a_2, \dots), \quad \text{st } f = m \text{ a } g = \\ = (b_0, b_1, b_2, \dots), \quad \text{st } g = n. \quad \text{Pak } a_m \neq o, \quad b_n \neq o \quad \text{a } f \cdot g = \\ = (c_0, c_1, c_2, \dots), \quad \text{kde } c_{m+n} = \sum_{i+j=m+n} a_i b_j = a_m b_n \neq o, \quad \text{neboť} \\ i+j=m+n$$

okruh M je bez dělitelů nuly.

Důsledek 1.1:

Okruh polynomů $P(M)$ nad oborem integrity M je oborem integrity.

Věta 1.3:

Nechť M je okruh a f, g jsou nenulové polynomy z $P(M)$. Pak platí:

a) Součet $f+g$ je buď polynom nulový, nebo

$$st(f+g) \leq \max(st f, st g).$$

b) Součin $f \cdot g$ je buď polynom nulový, nebo

$st(f \cdot g) \leq st f + st g$. Přitom, je-li okruh M bez dělitelů nuly, pak platí $st(f \cdot g) = st f + st g$.

Důkaz:

Položme pro $f, g \in P(M)$, $f = (a_0, a_1, a_2, \dots)$, $g = (b_0, b_1, b_2, \dots)$,

$$st f = m, st g = n.$$

a) Jestliže $m = n$ a $a_i = -b_i$ pro $i = 0, 1, 2, \dots$, pak $f+g$ je

polynom nulový.

Jestliže $m = n$ a existuje $j \in \{0, 1, 2, \dots, n\}$ takové, že

$$a_j \neq -b_j, \text{ pak } st(f+g) \leq m = \max(st f, st g).$$

Jestliže $m \neq n$ a $k = \max(m, n)$, pak $st(f+g) = k = \max(st f, st g)$.

b) Je-li okruh M bez dělitelů nuly, pak $f \cdot g = (c_0, c_1, c_2, \dots)$,

$$c_k = \sum_{\substack{i, j \geq 0 \\ i+j=k}} a_i b_j \text{ a } p = m+n \text{ je největší celé číslo, pro které je}$$

$c_p \neq 0$. Neboť $c_p = c_{m+n} = a_m \cdot b_n \neq 0$ a pro všechna $k > p$ je $c_k = 0$.

Tedy $st(f \cdot g) = p = m+n = st f + st g$.

Jestliže jsou v okruhu M dělitelé nuly, může být polynom $f \cdot g$

polynom nulový, nebo platí $st(f \cdot g) \leq st f + st g$. Protože v

tomto případě může pro všechna $k = 0, 1, 2, \dots$ platit $c_k = 0$,

nebo alespoň $c_p = a_m \cdot b_n$ může být rovno nulovému prvku $o \in M$.

Poznámka 1.3:

Nadále budeme uvažovat obory integrity polynomů $P(I)$, které jsou definovány nad oborem integrity I . Tím máme v $P(I)$ zaručenu existenci jednotkového prvku e , komutativitu pro operaci násobení a to, že v $P(I)$ nejsou dělitelé nuly. Polynom $f = (a_0, a_1, a_2, \dots) \in P(I)$, jehož stupeň je n , budeme zapisovat také

$$f = (a_0, a_1, \dots, a_n, 0, \dots), a_n \neq 0.$$

Lemma 1.1:

Nechť I je obor integrity. Pak platí:

a) Pro polynom $(o, e, o, \dots) \in P(I)$ platí pro každé $n \in N$ vztah

$$(o, e, o, \dots)^n = (o, o, \dots, o, e, o, \dots) \text{ n-krát}$$

b) Pro polynom $(o, o, \dots, o, a_n, o, \dots) \in P(I)$, $a_n \neq o$, platí pro každé $n \in N$ vztah

$$\begin{aligned} (o, o, \dots, o, a_n, o, \dots) &= (a_n, o, o, \dots). (o, o, \dots, o, e, o, \dots) = \\ &= (a_n, o, o, \dots). (o, e, o, \dots)^n. \end{aligned}$$

Důkaz:

V obou případech úplnou matematickou indukcí.

a) Pro $n=1$ máme $(o, e, o, \dots)^1 = (o, e, o, \dots)$.

1-krát

Předpokládejme, že pro $k \geq 1$ platí:

$(o, e, o, \dots)^k = (o, o, \dots, o, e, o, \dots)$ a za tohoto předpokladu

dokažme, že $(o, e, o, \dots)^{k+1} = (o, o, \dots, o, e, o, \dots)$. Skutečně

podle definice násobení polynomů z $P(I)$ a za použití indukčního předpokladu obdržíme $(o, e, o, \dots)^{k+1} =$

$$= (o, e, o, \dots)^k. (o, e, o, \dots) = (o, o, \dots, o, e, o, \dots). (o, e, o, \dots) =$$

k-krát

$$= (c_0, c_1, c_2, \dots) = (o, o, \dots, o, e, o, \dots). \text{ Neboť pouze pro } n = k+2$$

(k+1)-krát

platí $c_n = c_{k+2} = e \cdot e = e$ a pro všechna ostatní $n \in N_0$, $n \neq k+2$

máme $c_n = o$. Protože v součtu sčítanců pro výpočet c_n , $n \neq k+2$

($c_n = \sum_{\substack{i+j \geq 0 \\ i+j=n}} a_i b_j$) jsou všichni sčítanci tvaru $o \cdot e$ nebo $e \cdot o$

nebo $o \cdot o$.

Tedy vztah $(o, e, o, \dots)^n = (o, o, \dots, o, e, o, \dots)$ platí pro všechna

$n \in N$.

b) Pro $n=1$ platí $(o, a_1, o, \dots) = (a_1, o, o, \dots). (o, e, o, \dots)^1$, neboť

$$(a_1, o, o, \dots). (o, e, o, \dots) = (c_0, c_1, c_2, \dots), \text{ kde } c_1 = a_1 \cdot e = a_1$$

a pro všechna $k \in N_0$, $k \neq 1$, platí $c_k = o$.

Předpokládejme, že pro $k \geq 1$ platí $(o, o, \dots, o, a_k, o, \dots) =$

$$= (a_k, o, o, \dots). (o, e, o, \dots)^k \text{ a za tohoto předpokladu dokážeme,}$$

$$\text{že platí } (o, o, \dots, o, a_{k+1}, o, \dots) = (a_{k+1}, o, o, \dots).$$

$$\cdot (o, o, \dots, o, e, o, \dots) = (a_{k+1}, o, o, \dots). (o, e, o, \dots)^{k+1}.$$

(k+1)-krát

Skutečně podle definice násobení v $P(I)$ a za použití

indukčního předpokladu obdržíme

$$\begin{aligned} & (a_{k+1}, o, o, \dots) \cdot (o, e, o, \dots)^{k+1} = (a_{k+1}, o, o, \dots) \cdot [(o, e, o, \dots)^k \cdot \\ & \cdot (o, e, o, \dots)] = [(a_{k+1}, o, o, \dots) \cdot (o, e, o, \dots)^k] \cdot (o, e, o, \dots) = \\ & = (o, o, \dots, o, a_{k+1}, o, \dots) \cdot (o, e, o, \dots) = (o, o, \dots, o, a_{k+1}, o, \dots). \\ & \quad \text{k-krát} \qquad \qquad \qquad \text{(k+1)-krát} \\ & \text{Neboť } c_{k+2} = a_{k+1} \cdot e = a_{k+1} \text{ a obdobně jako v a) se ukáže, že} \\ & \text{pro všechna ostatní } n \in N_0, n \neq k+2, \text{ platí } c_n = o. \text{ Tedy vztah} \\ & (o, o, \dots, o, a_n, o, \dots) = (a_n, o, o, \dots) \cdot (o, e, o, \dots)^n \text{ platí pro} \\ & \quad \text{n-krát} \\ & \text{všechna } n \in N. \end{aligned}$$

Věta 1.4:

Nechť I je obor integrity, e jednotkový prvek z I. Pak existuje v $P(I)$ prvek $(o, e, o, \dots) = x$ tak, že platí:

Každý polynom $f = (a_0, a_1, \dots, a_n, o, \dots) \in P(I), a_n \neq 0$ se dá vyjádřit právě jedním způsobem ve tvaru:

$$f = (a_0, a_1, \dots, a_n, o, \dots) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n.$$

Důkaz:

$$\begin{aligned} & \text{Polynom } (o, e, o, \dots) \in P(I) \text{ označíme symbolem } x \text{ a za použití} \\ & \text{lemmatu 1.1 získáme pro každý polynom } f = (a_0, a_1, \dots, a_n, o, \dots) \in \\ & \in P(I), a_n \neq 0 \text{ jednoznačné vyjádření ve tvaru: } f = (a_0, a_1, \dots, a_n, o, \dots) = \\ & = (a_0, o, o, \dots) + (o, a_1, o, \dots) + (o, o, a_2, o, \dots) + \dots + \\ & + (o, o, \dots, o, a_n, o, \dots) = (a_0, o, o, \dots) + (a_1, o, o, \dots) \cdot (o, e, o, \dots) + \\ & \quad \text{n-krát} \\ & + (a_2, o, o, \dots) \cdot (o, e, o, \dots)^2 + \dots + (a_n, o, o, \dots) \cdot (o, e, o, \dots)^n = \\ & = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n. \end{aligned}$$

Zde jsme ztotožnili pro $i = 0, 1, 2, \dots, n$ prvky $a_i \in I$ s prvky $(a_i, o, o, \dots) \in P(I)$ podle poznámky 1.2.

Poznámka 1.4:

Před vyslovením následující definice si uvědomme, že průnik libovolného neprázdného systému podokruhů okruhu M je opět podokruh okruhu M.

Definice 1.4:

Nechť M je podokruhem okruhu M' a nechť A je libovolná množina prvků z M'. Potom symbolem $M[A]$ budeme rozumět průnik všech podokruhů okruhu M', které obsahují současně M i A. O okruhu $M[A]$ budeme říkat, že vznikl adjunkcí množiny A k okruhu M.

Poznámka 1.5:

Je zřejmé, že $M[A]$ je podokruh okruhu M' a to nejmenší takový, že obsahuje M i A a platí tedy $M \cdot A \subseteq M[A] \subseteq M'$.

Množina A může obsahovat pouze jediný prvek a , pak píšeme $M[a]$ místo $M[\{a\}]$.

Věta 1.5:

Je-li I obor integrity, e jeho jednotkový prvek, $x = (o, e, o, \dots) \in P(I)$, pak platí $P(I) = I[x]$.

Důkaz:

Podle poznámky 1.2 je $I \subseteq P(I)$. Rovněž $x \in P(I)$. Pak platí $I[x] \subseteq P(I)$, neboť $I[x]$ je průnik všech podokruhů okruhu $P(I)$, které obsahují I i x a $P(I)$ je jeden z nich.

Obráceně: Každý polynom $f \in P(I)$ můžeme zapsat ve tvaru

$f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$. Jelikož $a_0, a_1, a_2, \dots, a_n \in I[x]$, $x \in I[x]$ a protože $I[x]$ je okruh, platí $a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in I[x]$ a odtud $P(I) \subseteq I[x]$.

Celkem tedy $P(I) = I[x]$.

Definice 1.5:

Nechť I je obor integrity.

- a) Obor integrity $I[x]$ se nazývá obor integrity polynomů jedné neurčité x nad I , polynomy z $I[x]$ značíme $f(x), g(x)$, atd.
- b) Nechť $f(x) \in I[x]$ a $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, pak celé nezáporné číslo k takové, že v polynomu $f(x)$ je $a_k \neq 0$ a pro každé $i > k$ je $a_i = 0$, se nazývá stupeň polynomu $f(x)$, což značíme st $f(x) = k$. Nulovému polynomu $f(x) = 0$ stupeň nepřiřazujeme.
- c) prvek $a_i x^i \in f(x)$ se nazývá člen i -tého stupně a prvky $a_0, a_1, a_2, \dots, a_n \in I$ koeficienty polynomu $f(x)$.
- d) Říkáme, že polynom $f(x) \in I[x]$ stupně n je v normálním tvaru, jestliže pro libovolnou mocninu x^i ($i = 0, 1, \dots, n$) obsahuje $f(x)$ nejvýše jeden člen $a_i x^i$ (člen a_0 chápeme jako $a_0 x^0$), tj. $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $a_n \neq 0$.

Definice 1.6:

Nechť I je obor integrity, $I' \supseteq I$ libovolný jeho nadobor integrity, $f(x)$ polynom jedné neurčité x nad I . Prvek $a \in I'$ se nazývá kořen polynomu $f(x)$, právě když jeho dosazením za neurčitou x do polynomu $f(x)$ obdržíme prvek ($v I'$), rovný nulovému prvku o , což zapisujeme $f(a) = o$.

Definice 1.7:

Nechť I je obor integrity, $I' \supseteq I$ jeho libovolný nadobor integrity. Říkáme, že prvek $a \in I'$ je algebraický prvek stupně $n > 0$ nad I , právě když existuje nenulový polynom $f(x) \in I[x]$, st $f(x) = n$, jehož je prvek a kořenem a $n \in \mathbb{N}$ je nejmenší takové číslo. Není-li prvek $a \in I'$ algebraický prvek nad I , pak říkáme, že a je transcendentní prvek nad I .

Poznámka 1.6:

Jinými slovy: Prvek $u \in I' \supseteq I$ je algebraický nad I stupně $n > 0$, jestliže existuje alespoň jeden polynom $f(x) \in I[x]$, $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, $a_n \neq 0$ takový, že platí rovnost $a_0 + a_1 u + a_2 u^2 + \dots + a_n u^n = o$. Přitom $n \in \mathbb{N}$ je nejmenší takové číslo.

Je zřejmé, že platí:

- a) Každý prvek a z tělesa T je algebraický prvek nad T , neboť je kořenem nenulového polynomu $x-a \in T[x]$. Jeho stupeň je 1.
- b) Každé komplexní číslo $\alpha = a_1 + a_2 i$, $a_2 \neq 0$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$ je algebraický prvek stupně 2 nad tělesem reálných čísel R . Neboť komplexní číslo $\alpha = a_1 + a_2 i$ je kořenem nenulového polynomu $f(x) \in R[x]$, $f(x) = [x - (a_1 + a_2 i)][x - (a_1 - a_2 i)] = 1 \cdot x^2 - 2a_1 x + (a_1^2 + a_2^2)$, $a_1 \in R$, $a_1^2 + a_2^2 \in R$. Číslo $\alpha \in \mathbb{C} \setminus R$ přitom nemůže být algebraický prvek stupně 1, neboť $\alpha \notin R$.
- c) Dá se dokázat, že číslo π je transcendentní prvek nad Q , ale je algebraický prvek nad R . (Např. $x-\pi = 0$).
- d) Číslo $a = \sqrt[3]{3} \in R$ je algebraický prvek stupně 2 nad tělesem Q a stupně 1 nad tělesem R . Číslo $\sqrt[3]{3}$ je zřejmě kořenem polynomu $x^2 - 3 = 0$ z $Q[x]$ a není kořenem žádného polynomu prvního stupně z $Q[x]$, neboť $\sqrt[3]{3} \notin Q$. Číslo $a = \sqrt[3]{3}$ je zřejmě kořenem polynomu $x - \sqrt[3]{3} = 0$ z $R[x]$.

Věta 1.6:

Nechť I je obor integrity. Pak prvek $x = (o, e, o, \dots) \in P(I)$ je transcendentní prvek nad I .

Důkaz:

Sporem. Předpokládejme, že x je algebraický prvek nad I . Pak existuje nenulový polynom $f(x) \in I[x]$, $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, $a_n \neq 0$, jehož je prvek $x \in I$ kořenem.

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = (a_0, o, o, \dots) + (a_1, o, o, \dots) \cdot \\ &\quad \cdot (o, e, o, \dots) + (a_2, o, o, \dots) \cdot (o, e, o, \dots)^2 + \dots + (a_n, o, o, \dots) \cdot \\ &\quad \cdot (o, e, o, \dots)^n = (a_0, o, o, \dots) + (a_1, o, o, \dots) \cdot (o, e, o, \dots) + \\ &\quad + (a_2, o, o, \dots) \cdot (o, o, e, o, \dots) + \dots + (a_n, o, o, \dots) \cdot \\ &\quad \cdot (o, o, \dots, o, e, o, \dots) = (a_0, o, o, \dots) + (o, a_1, o, \dots) + \\ &\quad + (o, o, a_2, o, \dots) + \dots + (o, o, \dots, o, a_n, o, \dots) = \\ &= (a_0, a_1, a_2, \dots, a_n, o, \dots) \stackrel{n\text{-krát}}{\neq} (o, o, o, \dots) = o, \text{ protože } a_n \neq 0. \end{aligned}$$

Obdrželi jsme spor s předpokladem, že x je algebraický prvek nad I .

Poznámka 1.7:

Jiný důkaz věty 1.6 můžeme udělat takto: Z definice rovnosti polynomů v $I[x]$ plyne, že pro každý polynom $f(x) \in I[x]$, pro který $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = o$, musí platit $a_0 = a_1 = a_2 = \dots = a_n = o$.

Věta 1.7:

Nechť I je obor integrity. Každý polynom $f(x) \in I[x]$ stupně alespoň prvního je transcendentní prvek nad I .

Důkaz:

Provedeme ho v kapitole, která bude pojednávat o polynomech n neurčitých nad oborem integrity I .

Věta 1.8: (Dosazovací pravidlo).

Nechť I je obor integrity, $f(x), g(x) \in I[x]$, pro které platí $f(x) = g(x)$. Pak pro každé $a \in I$ platí $f(a) = g(a)$.

Důkaz:

Polynomy $f(x), g(x) \in I[x]$, $f(x) = g(x)$ převedeme na normální tvar
 $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$. Podle definice rovnosti polynomů platí $f(x) = g(x)$ právě tehdy, když $a_i = b_i$ pro každé $i = 0, 1, 2, \dots, n$. Po dosazení libovolného $a \in I$ zůstane rovnost zachována a tedy $f(a) = g(a)$.

Věta 1.9:

Obor integrity $I[x]$ není těleso.

Důkaz:

Kdyby $I[x]$ bylo těleso, musel by pro každé $f(x), g(x) \in I[x]$, st $f(x) = m$, st $g(x) = n$ existovat polynom $h(x) \in I[x]$, st $h(x) = p$ takový, že $f(x) \cdot h(x) = g(x)$ a tedy $m+p = n$. Poslední rovnost však pro $m > n$ neplatí a tudíž $I[x]$ není těleso.

Cvičení 1:

Příklad 1:

Najděte všechny polynomy jedné neurčité x v $Z_2[x]$ stupně nultého, prvního, druhého, třetího a čtvrtého.

Příklad 2:

Najděte všechny polynomy jedné neurčité x v $Z_3[x]$ stupně prvního a druhého. Kolik je polynomů v $Z_3[x]$ stupně třetího?

Příklad 3:

Určete počet všech polynomů jedné neurčité x v $Z_5[x]$, které jsou stupně nultého, prvního, druhého a n -tého.

Příklad 4:

Ukažte, že v oboru integrity $Z_2[x]$ platí:

- a) $(x + \bar{1})^2 = x^2 + \bar{1}$,
- b) $(x + \bar{1})^4 = x^4 + \bar{1}$.

Příklad 5:

Ukažte, že v $Z_3[x]$ pro všechna $a \in \{\bar{0}, \bar{1}, \bar{2}\}$ nabývají polynomy $f(x) = \bar{2} + x + x^2$ a $g(x) = \bar{2} + x^2 + x^3$ stejných hodnot.

Příklad 6:

Nechť I je obor integrity, jehož nulový prvek je 0 a jednotkový prvek je 1 . Pro libovolné $a \in I$ a libovolné $k \in N_0$ označme symbolem $(a)_k$ polynom $(a_0, a_1, a_2, \dots) \in P(I)$, pro nějž je $a_i = 0$ pro všechny indexy různé od k a $a_k = a$. Podobně jako v poznámce 1.2 a větě 1.4 nečiňme rozdíl mezi prvkem $a \in I$ a polynomem $(a)_0 = (a, 0, 0, \dots) \in P(I)$. Dále položme $(1)_1 = x$.

Za těchto předpokladů dokažte, že pro libovolné $a \in I$ a libovolné $k \in N_0$ platí:

a) $((1)_1)^k = (1)_k$,

b) $(a)_0 ((1)_1)^k = (a)_k$,

c) každý polynom $f = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) \in P(I)$ se dá vyjádřit právě jedním způsobem ve tvaru $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$.

Tímto způsobem vlastně provedeme jinými formálními zápisu důkaz věty 1.4.

Příklad 7:

Přeformulujte definici rovnosti polynomů a stupně polynomu pro polynomy $f(x) \in I[x]$ zapsané ve tvaru $f(x) = a_0 + a_1 x + \dots + a_n x^n$.

Příklad 8:

a) Pro polynomy ze $Z_3[x]$: $f(x) = x^3 + x^2 + x + \bar{1}$,

$$g(x) = x^3 + x^2 - x + \bar{1},$$

$$h(x) = x^3 + x^2 + \bar{1}$$

určete $f(x)+g(x)+h(x)$ a také $f(x).g(x)-h^2(x)$,

b) určete počet všech nenulových polynomů v $Z_3[x]$ stupně nejvyšše pátého,

c) nechť $A = \{0, 1, -1\}$ a nechť v A jsou definovány tyto operace:

+	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

.	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

Ukažte, že $(A, +, .)$ je izomorfní s tělesem $(Z_3, +, .)$.

Příklad 9:

Ukažte, že čísla a) $a_1 = 1 + \sqrt{5}$,

b) $a_2 = 2 - 3i$,

c) $a_3 = \sqrt{2} - \sqrt{3}$

jsou algebraické prvky nad tělesem \mathbb{Q} .

Příklad 10:

Sestavte polynom nad \mathbb{Q} nejnižšího stupně, který má za kořen číslo $\sqrt[3]{i}$.

2. Dělitelnost polynomů jedné neurčité .

Jelikož v praxi se převážně setkáváme s číselnými tělesy, která jsou komutativní, budeme se v této kapitole zabývat dělitelností polynomů, které jsou definovány nad komutativním tělesem $(T, +, \cdot)$. Přitom budeme využívat poznatků z kapitoly IV a tudíž řadu vět o dělitelnosti polynomů nemusíme znova dokazovat. Stačí si při tom uvědomit, že každé komutativní těleso je zároveň oborem integrity. Nadále tedy T bude značit libovolné komutativní těleso a $T[x]$ obor integrity polynomů jedné neurčité nad T , který je rovněž komutativní. Nulový prvek z T budeme značit o , jednotkový prvek z T pak e .

Definice 2.1:

Jsou-li $f(x), g(x)$ dva polynomy z $T[x]$, pak říkáme, že $f(x)$ dělí $g(x)$ (resp. $g(x)$ je dělitelné $f(x)$, $g(x)$ je násobek $f(x)$, $f(x)$ je dělitel $g(x)$), existuje-li polynom $h(x) \in T[x]$ tak, že $g(x) = f(x) \cdot h(x)$.

Skutečnost, že $f(x)$ dělí $g(x)$ značíme $f(x) | g(x)$. Jestliže $f(x)$ nedělí $g(x)$, zapisujeme $f(x) \nmid g(x)$.

Věta 2.1:

Nechť $f(x), g(x) \in T[x]$, $g(x) \neq o$ a platí $f(x) | g(x)$. Pak st $f(x) \leq$ st $g(x)$.

Důkaz:

Podle definice platí $f(x) | g(x)$ právě když existuje $h(x) \in T[x]$ tak, že $g(x) = f(x) \cdot h(x)$. Podle věty 1.3 musí platit st $g(x) =$ st $f(x) +$ st $h(x)$ a jelikož $g(x) \neq o$ je také $h(x) \neq o$ a st $h(x) \geq 0$. Odtud dostáváme st $f(x) \leq$ st $g(x)$.

Věta 2.2:

Nechť $T[x]$ je obor integrity polynomů jedné neurčité nad T . Pak platí:

- 1) $(\forall f(x) \in T[x]) \quad f(x) | f(x)$ (reflexivita)
- 2) $(\forall f(x) \in T[x]) \quad f(x) | o$
- 3) $(\forall f(x) \in T[x]) \quad e | f(x)$
- 4) $(\forall f(x), g(x), h(x) \in T[x]) \quad [(f(x) | g(x) \wedge g(x) | h(x)) \Rightarrow f(x) | h(x)]$ (tranzitivita)
- 5) $(\exists f(x), g(x) \in T[x]) \quad (f(x) | g(x) \wedge g(x) \nmid f(x))$
- 6) $(\forall f_1(x), f_2(x), g_1(x), g_2(x) \in T[x]) \quad [(f_1(x) | g_1(x) \wedge f_2(x) | g_2(x)) \Rightarrow f_1(x).f_2(x) | g_1(x).g_2(x)]$
- 7) $(\forall f_1(x), f_2(x), g(x) \in T[x]) \quad [f_1(x).f_2(x) | g(x) \Rightarrow f_1(x) | g(x) \wedge f_2(x) | g(x)]$
- 8) $(\forall f_1(x), f_2(x), g(x) \in T[x]) \quad [(f_1(x).g(x) | f_2(x).g(x) \wedge g(x) \neq o) \Rightarrow f_1(x) | f_2(x)]$
- 9) $(\forall f_1(x), f_2(x), \dots, f_n(x) \in T[x], \quad g_1(x), g_2(x), \dots, g_n(x), h(x) \in T[x]) \quad [(h(x) | f_1(x), h(x) | f_2(x), \dots, h(x) | f_n(x)) \Rightarrow h(x) | \sum_{i=1}^n f_i(x).g_i(x)]$

Důkaz:

Jelikož $T[x]$ je obor integrity, viz lemma 1.1 z kap. IV.

Poznámka 2.1:

Jako speciální případ tvrzení 9) z věty 2.2 obdržíme následující tvrzení, které budeme často používat: $(\forall f(x), g_1(x), g_2(x) \in T[x]) \quad [f(x) | g_1(x) \wedge f(x) | g_2(x) \Rightarrow f(x) | (g_1(x) + g_2(x)) \wedge f(x) | (g_1(x) - g_2(x))]$.

Věta 2.3:

- a) Jednotkami v $T[x]$ jsou právě všechny polynomy stupně nula (tj. všechny nenulové prvky komutativního tělesa T).
- b) S polynomem $f(x) \in T[x]$ jsou asociovány právě všechny polynomy $c.f(x)$, kde $c \in T$, $c \neq o$.

Důkaz:

- a) Nechť $f(x) \in T[x]$ je jednotka, pak $f(x) | e$. Jelikož $e \in T[x]$ je polynom stupně nula, platí podle věty 2.1, že $\text{st } f(x) \leq 0$ a jelikož $f(x) \neq o$, dostáváme $\text{st } f(x) = 0$.
Obráceně: Každý prvek $c \in T$, $c \neq o$ je jednotka v $T[x]$, neboť T je těleso a existuje tudíž $c^{-1} \in T$ tak, že $c.c^{-1} = e$.
- b) Zřejmě podle definice asociovaných prvků v oboru integrity.
Viz definice 1.3 v kap. IV.

Věta 2.4:

Pro každé $f(x), g(x) \in T[x]$ platí: $f(x)$ je asociováno s $g(x)$, právě když současně $f(x)|g(x)$ a $g(x)|f(x)$.

Důkaz:

Viz lemma 1.4 v kap. IV.

Věta 2.5:

- a) Pro každý polynom $f(x) \in T[x]$ a pro každé $c \in T$, $c \neq 0$ platí $c|f(x)$.
- b) Nechť $f(x), g(x) \in T[x]$ a $f_1(x) = c.f(x)$, $g_1(x) = d.g(x)$, kde $c, d \in T$, $c \neq 0$, $d \neq 0$. Pak $f(x)|g(x)$ právě když $f_1(x)|g_1(x)$.

Důkaz:

a) Zřejmě, neboť $f(x) = c.(c^{-1}f(x))$.

b) Viz lemma 1.5 v kap. IV.

Definice 2.2:

Polynom $f(x) \in T[x]$, st $f(x) \geq 1$ se nazývá reducibilní (rozložitelný) v $T[x]$, jestliže se dá psát jako součin dvou polynomů z $T[x]$, jež jsou oba stupně alespoň prvního. V opačném případě se nazývá polynom $f(x) \in T[x]$ ireducibilní (nerozložitelný) v $T[x]$.

Poznámka 2.2:

Reducibilita je relativní vlastnost. Např. polynom $f(x) = x^2 - 2$ ze $Z[x]$ je ireducibilní v $Q[x]$, ale je reducibilní v $R[x]$, neboť $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ a víme, že $\sqrt{2} \in R$ a $\sqrt{2} \notin Q$.

Lineární polynom $f(x) \in T[x]$ je vždy irreducibilní polynom v $T[x]$.

Definice 2.3:

- a) Jsou-li $f_1(x), f_2(x), \dots, f_n(x) \in T[x]$, pak polynom $D(x) \in T[x]$ se nazývá největší společný dělitel polynomů $f_i(x)$, $i = 1, 2, \dots, n$ právě když platí:
 - 1) $D(x)|f_1(x) \wedge D(x)|f_2(x) \wedge \dots \wedge D(x)|f_n(x)$,
 - 2) $(\forall d(x) \in T[x]) [(d(x)|f_1(x) \wedge d(x)|f_2(x) \wedge \dots \wedge d(x)|f_n(x)) \Rightarrow d(x)|D(x)]$.
- b) Polynomy $f_1(x), f_2(x), \dots, f_n(x) \in T[x]$ jsou soudělné, když jejich největší společný dělitel $D(x)$ je stupně alespoň

prvního. V opačném případě říkáme, že jsou nesoudělné.

Nyní bude následovat velice důležitá věta, že každý obor integrity $T[x]$ polynomů jedné neurčité nad T je eukleidovský obor integrity. Tudíž všechny věty, které jsme si v kap. IV dokázali pro libovolný eukleidovský obor integrity platí i v oboru integrity $T[x]$. Připomeňme si definici eukleidovského oboru integrity, tj. definici 4.1 z kap. IV:

Obor integrity I se nazývá eukleidovský obor integrity, právě když ke každému prvku $a \in I$, $a \neq 0$ lze přiřadit celé nezáporné číslo $n(a)$ takové, že pro libovolná $a, b \in I$, $b \neq 0$ platí současně:

- 1) $a|b \Rightarrow n(a) \leq n(b)$,
- 2) $(\exists q, r \in I) [a = b \cdot q + r \wedge (r=0 \vee n(r) < n(b))]$.

Věta 2.6:

Nechť $f(x)$ a $g(x) \neq 0$ jsou dva polynomy z $T[x]$. Pak existují v $T[x]$ právě dva polynomy $q(x)$ a $r(x)$ s vlastností:

$$(2.1) \quad f(x) = g(x) \cdot q(x) + r(x), \text{ přičemž } r(x) = 0 \vee \text{st } r(x) < \text{st } g(x).$$

Důkaz:

- a) Jestliže $f(x) = 0$, stačí zvolit $q(x) = r(x) = 0$ a věta platí.
- b) Jestliže $f(x) \neq 0$ a $\text{st } f(x) < \text{st } g(x)$, stačí zvolit $q(x) = 0$ a $r(x) = f(x)$ a věta rovněž platí.
- c) Předpokládejme tedy dále, že $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ ($a_n \neq 0$) a $g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m$ ($b_m \neq 0$) a $\text{st } f(x) \geq \text{st } g(x)$, tedy $n \geq m$.

Důkaz provedeme úplnou matematickou indukcí podle stupně n polynomu $f(x)$.

Nechť nejprve $n=0$, pak i $m=0$ a platí $f(x) = a_0$, $g(x) = b_0$, kde $a_0, b_0 \in T$, $a_0 \neq 0$, $b_0 \neq 0$. Jelikož T je komutativní těleso, existuje prvek $c_0 \in T$ tak, že $a_0 = b_0 \cdot c_0$. V tomto případě stačí položit $q(x) = c_0$ a $r(x) = 0$ a platnost (2.1) pro $n=0$ je ověřena.

Předpokládejme, že (2.1) platí pro všechny polynomy z $T[x]$ stupně menšího než $n>0$ a za tohoto předpokladu dokážeme, že (2.1) platí i pro polynom $f(x)$ stupně n .

Jelikož platí $a_n x^n - a_{n-m} b_{n-m}^{-1} x^{n-m} b_m x^m = 0$, má polynom

$$(2.2) \quad f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

stupeň menší než n. Tedy podle indukčního předpokladu existují polynomy $q_1(x), r_1(x) \in T[x]$ tak, že platí

$$(2.3) \quad f_1(x) = g(x) \cdot q_1(x) + r_1(x) \wedge (r_1(x) = 0 \vee \text{st } r_1(x) < \text{st } g(x)).$$

Dosadíme-li do (2.2) za $f_1(x)$ podle (2.3), obdržíme

$$g(x) \cdot q_1(x) + r_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x) \text{ a po úpravě}$$

$$(2.4) \quad f(x) = g(x)(q_1(x) + a_n b_m^{-1} x^{n-m}) + r_1(x).$$

Označíme-li $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$, $r(x) = r_1(x)$, máme

$$(2.5) \quad f(x) = g(x) \cdot q(x) + r(x), \text{ přičemž podle (2.3)} \quad r(x) = 0 \vee \text{st } r(x) < \text{st } g(x).$$

Dokázali jsme existenci takových polynomů $q(x), r(x) \in T[x]$, pro které platí vztah (2.1), zbývá dokázat jednoznačnost.

Předpokládejme dvě taková vyjádření tvaru (2.1):

$$(2.6) \quad f(x) = g(x) \cdot q_1(x) + r_1(x) \wedge (r_1(x) = 0 \vee \text{st } r_1(x) < \text{st } g(x)),$$

$$f(x) = g(x) \cdot q_2(x) + r_2(x) \wedge (r_2(x) = 0 \vee \text{st } r_2(x) < \text{st } g(x)).$$

Po úpravě obdržíme

$$(2.7) \quad g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$

a) Pro $r_1(x) = r_2(x)$ máme $g(x)[q_1(x) - q_2(x)] = 0$ a jelikož je $g(x) \neq 0$ a $T[x]$ je obor integrity, platí též $q_1(x) = q_2(x)$.

b) Pro $r_1(x) \neq r_2(x)$ platí $\text{st}(r_2(x) - r_1(x)) < \text{st } g(x)$ podle (2.6). Jelikož platí $g(x) \cdot (q_1(x) - q_2(x)) = r_2(x) - r_1(x) \neq 0$, musí být $\text{st}(q_1(x) - q_2(x)) \geq 0$ a jelikož $\text{st } g(x) > \text{st}(r_2(x) - r_1(x)) = \text{st } g(x) + \text{st}(q_1(x) - q_2(x))$, dostáváme spor.

Věta 2.7:

Nechť $T[x]$ je obor integrity polynomů jedné neurčité x nad komutativním tělesem T . Pak $T[x]$ je eukleidovský obor integrity.

Důkaz:

Každému nenulovému polynomu $f(x) \in T[x]$ definujeme jeho normu takto: $n(f(x)) = \text{st } f(x)$. Pak naše tvrzení plyne z věty 2.1 a z věty 2.6.

Důsledek 2.1:

Struktury $Q[x]$, $R[x]$, $C[x]$ jsou eukleidovské obory integrity.

Vzhledem k platnosti věty 2.7 a některých tvrzení, dokázaných v kap. IV, obdržíme odpovídající věty pro polynomy z $T[x]$:

Věta 2.8:

Nechť $T[x]$ je obor integrity polynomů jedné neurčité x nad komutativním tělesem T , $f_1(x)$ a $f_2(x)$ libovolné polynomy z $T[x]$. Pak platí:

- a) V $T[x]$ existuje právě jeden (ve smyslu dělitelnosti) největší společný dělitel $D(x)$ polynomů $f_1(x)$ a $f_2(x)$. $D(x)$ lze určit Eukleidovým algoritmem.
- b) V $T[x]$ existují polynomy $v_1(x)$ a $v_2(x)$ takové, že platí
$$(2.8) \quad f_1(x) \cdot v_1(x) + f_2(x) \cdot v_2(x) = D(x).$$
- c) Jsou-li $f_1(x)$ a $f_2(x)$ nesoudělné polynomy, tj. je-li $D(x) = e$, pak existují $v_1(x)$, $v_2(x) \in T[x]$ takové, že
$$f_1(x) \cdot v_1(x) + f_2(x) \cdot v_2(x) = e.$$

Důkaz:

Viz věta 2.7 a věty 3.1, 4.1 a 4.2 z kap. IV.

Věta 2.9:

Nechť $f_1(x), f_2(x), g(x) \in T[x]$ a nechť $f_1(x)$ a $g(x)$ jsou nesoudělné. Jestliže $g(x) | f_1(x) \cdot f_2(x)$, pak $g(x) | f_2(x)$.

Důkaz:

Viz věta 2.7 a lemma 3.4 z kap. IV.

Věta 2.10:

V $T[x]$ je každý irreducibilní prvek prvočinitel. (V $T[x]$ platí podmínka prvočinitelová).

Důkaz:

Viz věta 2.8 a věta 3.3 z kap. IV.

Věta 2.11:

Nechť $g(x)$ je irreducibilní polynom z $T[x]$ a $f_i(x) \in T[x]$ pro $i = 1, 2, \dots, n$. Pak $g(x) | \prod_{i=1}^n f_i(x)$ právě tehdy, když existuje alespoň jedno $j \in \{1, 2, \dots, n\}$ tak, $g(x) | f_j(x)$.

Důkaz:

Viz věta 2.10 a lemma 2.4 z kap. IV.

Věta 2.12:

Obor integrity $T[x]$ polynomů jedné neurčité x nad komutativním tělesem T je Gaussův obor integrity.

Důkaz:

Viz věta 2.7 a věta 4.4 z kap. IV.

Věta 2.13:

Nechť $f(x) \in T[x]$ a $c \in T$. Pak existuje polynom $q(x) \in T[x]$ tak, že platí:

$$(2.9) \quad f(x) = (x-c) \cdot q(x) + f(c).$$

Důkaz:

Protože $x-c \in T[x]$, $x-c \neq 0$, existují podle věty 2.6 jednoznačně určené polynomy $q(x)$ a $r(x) \in T[x]$ tak, že platí

$$(2.10) \quad f(x) = (x-c) \cdot q(x) + r(x) \quad \wedge \quad (r(x) = 0 \vee st(r(x) < st(x-c))).$$

Přitom $st(x-c) = 1$.

To značí, že $r(x) = 0$ nebo $st(r(x)) = 0$ a tedy mohu psát $r(x) = r \in T$. Použitím dosazovacího pravidla obdržíme z (2.10) $f(c) = (c-c)q(c) + r = r$. Tedy platí $f(x) = (x-c) \cdot q(x) + f(c)$.

Věta 2.14: (Bezoutova věta).

Nechť $f(x)$ je nenulový polynom z $T[x]$ a nechť $c \in T$. Prvek c je kořenem polynomu $f(x)$ právě tehdy, když $(x-c) | f(x)$.

Důkaz:

Podle věty 2.13 existuje polynom $q(x) \in T[x]$ tak, že $f(x) = (x-c) \cdot q(x) + f(c)$.

Jestliže $c \in T$ je kořenem polynomu $f(x)$, je $f(c) = 0$ a odtud $f(x) = (x-c)q(x)$ a tedy $(x-c) | f(x)$.

Jestliže $(x-c) | f(x)$, existuje polynom $q(x) \in T[x]$ tak, že $f(x) = (x-c) \cdot q(x)$ a podle dosazovacího pravidla $f(c) = (c-c) \cdot q(c) = 0$.

Tedy c je kořenem polynomu $f(x)$.

Věta 2.15:

Je-li $f(x) \in T[x]$ a $st(f(x)) = n \geq 1$, pak polynom $f(x)$ má v T nejvýše n různých kořenů.

Důkaz:

Matematickou indukcí podle stupně polynomu n . Pro $n=1$ tvrzení platí, neboť $f(x) = a_0 + a_1 x$ a $f(x)$ má v T jediný kořen $c_1 = -\frac{a_0}{a_1}$.

Nechť $st(f(x)) = n > 1$ a předpokládejme, že tvrzení platí pro

všechny polynomy stupně menšího než n.

Polynom $f(x)$ buďto nemá žádný kořen a tvrzení tudíž platí. Nebo $f(x)$ má kořen $c \in T$. Pak podle Bezoutovy věty existuje $q(x) \in T[x]$ tak, že $f(x) = (x-c) \cdot q(x)$ a st $q(x) = n-1$. Podle indukčního předpokladu má polynom $q(x)$ nejvýše $(n-1)$ různých kořenů v T a tudíž polynom $f(x)$ má v T nejvýše n různých kořenů.

Věta 2.16:

Nechť $f_1(x), f_2(x) \in T[x]$. Existuje-li nekonečně mnoho hodnot různých prvků $c \in T$, pro které je $f_1(c) = f_2(c)$, pak $f_1(x) = f_2(x)$.

Důkaz:

Položme $f(x) = f_1(x) - f_2(x)$. Podle předpokladu existuje nekonečně mnoho různých prvků $c \in T$, pro které je $f(c) = f_1(c) - f_2(c) = 0$. Pak polynom $f(x)$ je nutně nulový polynom v $T[x]$ a tudíž $f_1(x) = f_2(x)$. Neboť v případě, že st $f(x) \geq 0$ bychom obdrželi spor s předchozí větou.

Poznámka 2.3:

Poslední věta nám umožňuje tvrdit, že když jsou polynomy definovány nad komutativním tělesem T , které má nekonečně mnoho prvků (např. Q, R, C), splývá v podstatě algebraická definice polynomů s definicí funkční, tak jak jsou polynomy definovány v matematické analýze. Jestliže však komutativní těleso obsahuje pouze konečný počet prvků, jsou tyto definice různé.

Nechť např. $T = \{a_1, a_2, \dots, a_n\}$, pak polynomy $g(x)$ a $f(x) = g(x) + (x-a_1)(x-a_2)\dots(x-a_n)$, st $f(x) < n$, st $g(x) < n$, jsou z hlediska algebry různé polynomy, neboť mají různé koeficienty u odpovídajících mocnin x^i (dokonce mají různý stupeň). Kdežto z hlediska matematické analýzy jsou si rovny, protože mají stejný definiční obor T a pro všechna $x \in T$ nabývají stejných funkčních hodnot. Tedy $f(x) = g(x)$.

Hornerovo schéma.

V praxi se velice často vyskytuje dělení polynomu $f(x) \in T[x]$ lineárním činitelem $(x-c)$, respektive je potřeba vypočítat

hodnotu polynomu $f(x) \in T[x]$ v nějakém $c \in T$. S výhodou přitom můžeme využívat schématu, které si nyní odvodíme a které se nazývá podle svého objevitele Hornerovo schema.

Věta 2.17:

Nechť T je komutativní těleso a $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in T[x]$, st $f(x) = n \geq 1$ a nechť $q(x) = b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1}$ je podíl a r je zbytek při dělení polynomu $f(x)$ polynomem $(x-c)$, kde $c \in T$. Pak platí:

$$b_{n-1} = a_n, b_{n-2} = a_{n-1} + cb_{n-1}, \dots, b_0 = a_1 + cb_1, r = a_0 + cb_0.$$

Důkaz:

Podle předpokladu platí $f(x) = (x-c) \cdot q(x) + r$. Polynomy $q(x)$ a r jsou jednoznačně určeny, protože $T[x]$ je eukleidovský obor integrity. Po dosazení za $f(x)$ a $q(x)$ a po roznásobení polynomu $(x-c) \cdot q(x)$ obdržíme $a_0 + a_1x + a_2x^2 + \dots + a_nx^n = r + b_0x + b_1x^2 + \dots + b_{n-1}x^{n-1} - (cb_0 + cb_1x + cb_{n-1}x^{n-1}) = (r - cb_0) + (b_0 - cb_1)x + \dots + (b_{n-2} - cb_{n-1})x^{n-1} + b_{n-1}x^n$.

Podle definice rovnosti polynomů obdržíme následující rovnosti

$$a_n = b_{n-1}, a_{n-1} = b_{n-2} - cb_{n-1}, \dots, a_1 = b_0 - cb_1, a_0 = r - cb_0$$

a odtud po snadné úpravě obdržíme požadované rovnosti.

Tento výpočet můžeme výhodně uspořádat do tzv. Hornerova schematu:

	a_n	a_{n-1}	a_{n-2}	a_2	a_1	a_0
c		cb_{n-1}	cb_{n-2}	cb_2	cb_1	cb_0
	b_{n-1}	b_{n-2}	b_{n-3}		b_1	b_0	$ r=f(c) $

koeficienty polynomu $q(x)$

Příklad 2.1:

Pomocí Hornerova schematu vydělte polynom $f(x) \in Q[x]$,
 $f(x) = x^4 - 2x^3 + 4x^2 - 6x - 80$ polynomem $(x+3)$.

Řešení:

	1	-2	4	-6	-80
-3	-	-3	15	-57	189
	1	-5	19	-63	<u>109</u>

Podíl $q(x) = x^3 - 5x^2 + 19x - 63$ a zbytek $r = f(-3) = 109$.
Můžeme tedy psát $f(x) = (x+3)(x^3 - 5x^2 + 19x - 63) + 109$.

Poznámka 2.4:

Věta 2.17 platí pro libovolné komutativní těleso T , tedy můžeme Hornerovo schema používat nejenom v tělesech Q a R , ale i v C , resp. v tělesech, která mají konečný počet prvků (tělesa nenulové charakteristiky).

Příklad 2.2:

a) Určete hodnotu polynomu $f(x) = \bar{2}x^5 + \bar{3}x^3 + \bar{4}x^2 + \bar{2}x + \bar{1} \in Z_5[x]$,
 $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ pro $c_1 = \bar{2} \in Z_5$.

b) Zjistěte, zda $c_2 = \bar{3} \in Z_5$ je kořenem uvažovaného polynomu $f(x) \in Z_5[x]$.

Řešení:

Použijeme Hornerova schematu. Příslušné operace provádíme v tělese $(Z_5, +, \cdot)$, které je charakteristiky 5.

a)

$c_1 = \bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{3}$	$\bar{4}$	$\bar{2}$	$\bar{1}$
$c_1 = \bar{2}$	-	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{2}$	$\bar{3}$
	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{1}$	$\bar{4}$	<u>$\bar{4} = f(\bar{2})$</u>

b)

$c_2 = \bar{3}$	$\bar{2}$	$\bar{0}$	$\bar{3}$	$\bar{4}$	$\bar{2}$	$\bar{1}$
$c_2 = \bar{3}$	-	$\bar{1}$	$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$
	$\bar{2}$	$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	<u>$\bar{0} = f(\bar{3})$</u>

Prvek $c_2 = \bar{3}$ je kořenem daného polynomu $f(x)$.

Příklad 2.3:

Určete hodnotu polynomu $f(x) = x^4 - 3ix^3 - 4x^2 + 5ix - 1 \in C[x]$
pro $c = 1 + 2i \in C$.

Řešení:

Pomocí Hornerova schematu. Příslušné operace provádíme v tělese C .

$c = 1 + 2i$	1	$-3i$	-4	$5i$	-1
$c = 1 + 2i$	-	$1+2i$	$3+i$	$-3-i$	$-11-2i$
	1	$1-i$	$-1+i$	$-3+4i$	<u>$-12-2i = f(1+2i)$</u>

Jak se provádí praktický výpočet největšího společného dělitele a určují polynomy $v_1(x)$ a $v_2(x)$ podle věty 2.8 si ukážeme na následujícím příkladě:

Příklad 2.4:

Nechť jsou dány polynomy $f_1(x) = x^3 - 6x^2 + 11x - 6$, $f_2(x) = x^3 - 1$ v $R[x]$.

a) Určete jejich největšího společného dělitele $D(x)$.

b) Určete polynomy $v_1(x)$ a $v_2(x)$ z $R[x]$ tak, aby platilo

$$D(x) = f_1(x) \cdot v_1(x) + f_2(x) \cdot v_2(x).$$

Řešení:

Budeme používat Eukleidův algoritmus. Během výpočtu s výhodou používáme toho, že polynomy můžeme dělit nebo násobit prvkem z R , který je různý od nuly.

$$\begin{array}{r} (x^3 - 6x^2 + 11x - 6):(x^3 - 1) = 1 \\ \hline -x^3 & + 1 \\ \hline -6x^2 + 11x - 5 = r_1(x), & q_1(x) = 1 \end{array}$$

$$\begin{array}{r} (36x^3 - 36):(6x^2 - 11x + 5) = 6x + 11 \\ \hline -36x^3 + 66x^2 - 30x \\ \hline 66x^2 - 30x - 36 \\ \hline -66x^2 + 121x - 55 \\ \hline 91x - 91 = r_2(x), & q_2(x) = 6x + 11 \end{array}$$

$$\begin{array}{r} (6x^2 - 11x + 5):(x - 1) = 6x - 5 \\ \hline -6x^2 + 6x \\ \hline -5x + 5 \\ \hline 5x - 5 \\ \hline 0 = r_3(x), & q_3(x) = 6x - 5. \end{array}$$

Největší společný dělitel daných polynomů $f_1(x)$ a $f_2(x)$ je tedy $D(x) = x - 1$.

b) Vidíme, že $D(x) = \frac{1}{91} r_2(x)$. Zapišme si odpovídající eukleidovský algoritmus, který jsme spočítali v a) a vypočítejme z něj $r_2(x)$. Obdržíme

$$f_1(x) = f_2(x) \cdot 1 + r_1(x) \quad / \cdot (6x + 11)$$

$$36f_2(x) = (-r_1(x)) \cdot (6x + 11) + r_2(x) .$$

První rovnost vynásobíme výrazem $(6x + 11)$ a přičteme ji ke druhé rovnosti. Po snadných úpravách obdržíme

$$r_2(x) = f_1(x) \cdot (6x + 11) + f_2(x) \cdot (25 - 6x) \quad \text{a odtud}$$

$$D(x) = f_1(x) \cdot \frac{1}{91} (6x + 11) + f_2(x) \cdot \frac{1}{91} (25 - 6x) .$$

$$\text{Tedy } v_1(x) = \frac{1}{91} (6x + 11) \quad \text{a} \quad v_2(x) = \frac{1}{91} (25 - 6x) .$$

Cvičení 2:

Příklad 1:

Vypočítejte podíl a zbytek po vydelení polynomu $f(x) = 2x^4 - 3x^3 + 4x^2 + 5x + 5$ polynomem $g(x) = x^2 - 3x + 2$ v $\mathbb{Q}[x]$ a totéž proved'te v $\mathbb{Z}_7[x]$ pro polynomy $f(x) = \bar{2}x^4 - \bar{3}x^3 + \bar{4}x^2 + \bar{5}x + \bar{5}$ a $g(x) = x^2 - \bar{3}x + \bar{2}$.

Příklad 2:

- Nechť jsou dány polynomy $f(x) = a_0 + a_1x + x^3$, $g(x) = 1 + b_1x + x^2 \in T[x]$, kde $T = \mathbb{Q}$ resp. $T = \mathbb{Z}_2$. Zjistěte, kdy $g(x) | f(x)$.
- Obdobně zjistěte, za jakých podmínek polynom $f(x) = x^3 + px + q$ je dělitelný polynomem $g(x) = x^2 + mx - 1$ v $\mathbb{R}[x]$.

Příklad 3:

Dělte se zbytkem:

- $(x^5 + 2x^3 - 3x^2 + 5x - 7):(x + 2)$ nad \mathbb{Q} ,
- $(\bar{2}x^5 - \bar{3}x^3 + x):(x + \bar{3})$ nad \mathbb{Z}_5 ,
- $(4x^3 + 2x^2 + (2 - i)x + i):(x + (1 + i))$ nad \mathbb{C} .

Příklad 4:

Zjistěte, zda $(x - 7)|(2x^5 - 17x^4 + 23x^3 - 18x^2 + 29x - 7)$ a také, zda $(x - 2)|(x^5 - x^4 - 13x^3 + 13x^2 + 36x + 36)$.

Příklad 5:

Vypočítejte hodnotu polynomu $f(x)$ pro hodnotu c , jestliže

$$\text{a)} \quad f(x) = x^4 + 3x^3 + 6x^2 + 10x + 16 \in \mathbb{Q}[x] \quad \text{pro } c = 2 \text{ resp.}$$

$$c = -1,82,$$

$$\text{b)} \quad f(x) = x^4 + 2ix^3 - (1 + i)x^2 - 3x + (7 + i) \in \mathbb{C}[x] \quad \text{pro } c = i,$$

$$\text{c)} \quad f(x) = \bar{2}x^5 - \bar{3}x^4 + \bar{2}x^3 - x^2 + \bar{4}x + \bar{1} \in \mathbb{Z}_5[x] \quad \text{pro } c = \bar{2}.$$

Příklad 6:

Určete největší společný dělitel polynomů

a) $f(x) = x^6 + 2x^4 - 4x^3 + 2$, $g(x) = x^5 - x^4 - x + 1$ v $Z[x]$ a

$Q[x]$. Také v $R[x]$ a $C[x]$.

b) $f(x) = x^4 + x^3 - 3x^2 - 4x - 1$, $g(x) = x^3 + x^2 - x - 1$ v

$Z_5[x]$.

c) $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$, $g(x) = 2x^3 - x^2 - 5x + 4$,

$h(x) = x^5 - 2x^2 + 1$ v $Q[x]$.

Příklad 7:

Napište největší společný dělitel $D(x)$ polynomů $f(x)$ a $g(x) \in Q[x]$ a určete polynomy $v_1(x)$ a $v_2(x) \in Q[x]$ tak, aby platilo

$D(x) = f(x).v_1(x) + g(x).v_2(x)$, jestliže

a) $f(x) = x^2 + 2x + 1$, $g(x) = x^2 - 1$,

b) $f(x) = x^5 - 8x^3 - x^2 + 7x + 1$, $g(x) = x^4 - 2x^3 - 4x^2 + 2x + 3$

c) $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$, $g(x) = x^2 - x - 1$,

d) $f(x) = x^3 - x^2 + 2x - 2$, $g(x) = x^3 - 4x^2 + 5x - 2$.

Příklad 8:

Určete nejmenší společný násobek polynomů:

a) $f(x) = x^6 - 7x^4 + 8x^3 - 7x + 7$,

$g(x) = 3x^5 - 7x^3 + 3x^2 - 7$ v $Q[x]$.

b) $f(x) = x^4 + 2x^3 - x^2 - 4x - 2$,

$g(x) = x^4 + 3x^3 - x^2 - 2x - 2$,

$h(x) = x^2 + 3x - 1$ v $Q[x]$.

Příklad 9:

Nechť jsou dány polynomy $f_1(x), f_2(x), f_3(x) \in T[x]$, kde T je komutativní těleso. Dokažte, že platí pro největší společný dělitel následující vztah

$$D(D(f_1(x), f_2(x)), f_3(x)) = D(f_1(x), D(f_2(x), f_3(x))).$$

Příklad 10:

Ukažte, že pro každé $f(x), g(x), u(x), v(x) \in T[x]$ platí

$$D(f(x), g(x))|f(x).u(x) + g(x).v(x).$$

Příklad 11:

Nechť T je podtěleso komutativního tělesa T_1 . Nechť $f(x) \in T_1[x]$ má koeficienty z tělesa T , st $f(x) \geq 1$. Dokažte, že platí:

- Jestliže $f(x)$ je irreducibilní polynom nad tělesem T_1 , pak je také irreducibilní nad T .
- Jestliže je $f(x)$ reducibilní polynom nad T , pak je také reducibilní nad T_1 .

Příklad 12:

Ukažte na příkladech, že obrácená tvrzení k předcházejícímu tvrzení neplatí.

Příklad 13:

Nechť jsou dány polynomy $p(x), f(x) \in T[x]$ a $p(x)$ je irreducibilní polynom nad tělesem T . Dokažte, že $p(x) \nmid f(x)$ právě tehdy, když $D(p(x), f(x)) = e$, kde e je jednotkový prvek z T .

Příklad 14:

Zkuste některá lemmata nebo věty dokázat přímo pro polynomy, bez znalosti vět o dělitelnosti v oboru integrity, na kteréž jsme se odvolávali z kap. IV.

Příklad 15:

Rozložte na součin irreducibilních faktorů nad R následující polynomy z $R[x]$:

- $f(x) = x^4 + 4$,
- $f(x) = x^6 + 27$,
- $f(x) = x^4 + 1$.

3. Vlastnosti kořenů polynomů.

Vzhledem k tomu, že v praxi (např. v matematické analýze) se nejčastěji zabýváme polynomy nad číselnými tělesy (tělesy charakteristiky nula), budeme v této kapitole pojednávat o polynomech, které jsou definovány nad tělesem T charakteristiky nula. Pro názornost si čtenář může pod tělesem T představovat těleso komplexních čísel C . Nulový prvek z T budeme nyní značit 0

a jednotkový prvek z T jako 1.

Tvrzení Bezoutovy věty nás přivádí k zavedení pojmu vícenásobného kořene polynomu.

Definice 3.1:

Nechť $f(x)$ je polynom nad tělesem T , $k \in \mathbb{N}$. Prvek c z nadtelesa $T' \supseteq T$ se nazývá k-násobný kořen polynomu $f(x)$, jestliže $(x-c)^k | f(x)$ a $(x-c)^{k+1} \nmid f(x)$.

Jestliže $k=1$, mluvíme o jednoduchém kořenu polynomu $f(x)$.

Poznámka 3.1:

Je zřejmé, že prvek $c \in T' \supseteq T$ je k-násobným kořenem polynomu $f(x)$, právě když

$$(3.1) \quad f(x) = (x-c)^k \cdot g(x), \quad g(c) \neq 0.$$

K dalšímu výkladu budeme potřebovat pojem derivace polynomu $f(x) \in T[x]$. Definici derivace polynomu zavedeme čistě formálně, ale tak, aby její vlastnosti byly ve shodě s tvrzeními, které jsme o derivacích polynomů získali v matematické analýze.

Definice 3.2:

Derivaci polynomu $f(x)$ n-tého stupně ($n \geq 1$) nad T , $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_n \neq 0$ rozumíme polynom

$$(3.2) \quad f'(x) = n \cdot a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1.$$

Derivaci polynomu $f(x) \in T[x]$, st $f(x) \leq 0$ rozumíme nulový polynom.

Poznámka 3.2:

Vytvoříme-li derivaci k polynomu $f'(x) \in T[x]$, získáme druhou derivaci polynomu $f(x)$ ve tvaru

$$f''(x) = n(n-1)a_n x^{n-2} + (n-1)(n-2)a_{n-1} x^{n-3} + \dots + 3 \cdot 2 a_3 x + 2 a_2.$$

Postupujeme-li takto dále a pro $k > 1$ použijeme rekurentní předpis $f^{(k)}(x) = (f^{(k-1)}(x))'$, obdržíme k polynomu $f(x) \in T[x]$ k-tou derivaci ve tvaru:

$$(3.3) \quad f^{(k)}(x) = k! \left[\binom{n}{k} a_n x^{n-k} + \binom{n-1}{k} a_{n-1} x^{n-k-1} + \dots + \binom{k+1}{k} a_{k+1} x + \binom{k}{k} a_k \right].$$

Odvození vztahu (3.3) si může čtenář provést jako cvičení, symboly $k!$, $\binom{n}{k}$ zná ze střední školy.

Poznámka 3.3:

Pro úplnost uvádíme, že pojem derivace polynomu můžeme formálně zavést i v případě, že těleso T je nenulové charakteristiky.

Nechť I je obor integrity a $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in I[x]$. Pak derivací polynomu $f(x)$ rozumíme polynom v $I[x]$ tvaru $f'(x) = (1 \cdot a_1) + (2 \cdot a_2)x + \dots + (n \cdot a_n)x^{n-1}$. Zde výrazy tvaru $(k \cdot a_k)$ jsou přirozené násobky prvku a_k pro $k = 1, 2, \dots, n$. Tedy $k \cdot a_k = \underbrace{a_k + a_k + \dots + a_k}_{k\text{-krát}}$.

Pro počítání s derivacemi je důležitá následující věta. Přitom obdržíme stejné výsledky, jaké známe z matematické analýzy.

Věta 3.1:

Nechť $f(x), g(x) \in T[x]$. Pak platí:

- a) $(f(x) + g(x))' = f'(x) + g'(x)$,
- b) $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.

Důkaz:

Nechť $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m \in T[x]$ a např. $n \geq m$. Potom $g(x)$ můžeme přepsat na tvar $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$, kde $b_j = 0$ pro $m < j \leq n$. Pak platí:

- a) Jelikož $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n$, platí $(f(x) + g(x))' = (a_1 + b_1) + 2(a_2 + b_2)x + \dots + n(a_n + b_n)x^{n-1} = a_1 + 2a_2x + \dots + na_nx^{n-1} + b_1 + 2b_2x + \dots + mb_mx^{m-1} + \dots + nb_nx^{n-1} = f'(x) + g'(x)$.
- b) Předpokládejme, $f(x) \cdot g(x) = c_0 + c_1x + \dots + c_{n+m}x^{n+m}$, kde $c_k = \sum_{i+j=k} a_i b_j$ pro každé $0 \leq k \leq n+m$. Víme, že $f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1}$ a $g'(x) = b_1 + 2b_2x + \dots + mb_mx^{m-1}$. Podle pravidel o násobení polynomů obdržíme $f'(x) \cdot g(x) = d_0 + d_1x + \dots + d_{n+m-1}x^{n+m-1}$, kde $d_{k-1} = \sum_{r+s=k} r a_r b_s$ pro každé $1 \leq k \leq n+m$ a podobně dostáváme $f(x) \cdot g'(x) = e_0 + e_1x + \dots + e_{n+m-1}x^{n+m-1}$,

$$\begin{aligned} \text{kde } e_{k-1} &= \sum_{r+s=k} a_r b_s \text{ pro každé } 1 \leq k \leq n+m. \text{ Z čehož plyne } d_{k-1} + \\ &+ e_{k-1} = \sum_{r+s=k} r a_r b_s + \sum_{r+s=k} a_r b_s = \sum_{r+s=k} (r+s) a_r b_s = \\ &= k \left(\sum_{r+s=k} a_r b_s \right) = k c_k \text{ pro každé } 1 \leq k \leq n+m. \end{aligned}$$

Důsledek 3.1:

Nechť $f_1(x), f_2(x), \dots, f_k(x) \in T[x]$, pak platí

$$(3.4) \quad (f_1(x) \cdot f_2(x) \cdots f_k(x))' = f'_1(x) \cdot f_2(x) \cdots f_k(x) + \\ + f_1(x) \cdot f'_2(x) \cdots f_k(x) + \dots + f_1(x) \cdot f_2(x) \cdots f_{k-1}(x) \cdot f'_k(x).$$

Důkaz:

Matematickou indukcí. Pro $k=2$ máme již tvrzení dokázáno. Viz věta 3.1 b).

Předpokládejme, že tvrzení platí pro $s \geq 2$ a za tohoto předpokladu dokážeme platnost tvrzení pro $(s+1)$.

$$\begin{aligned} (f_1(x) \cdots f_s(x) \cdot f_{s+1}(x))' &= [(f_1(x) \cdots f_s(x)) \cdot f_{s+1}(x)]' = \\ &= (f_1(x) \cdots f_s(x))' \cdot f_{s+1}(x) + (f_1(x) \cdots f_s(x)) \cdot f'_{s+1}(x) = \\ &= (f'_1(x) \cdot f_2(x) \cdots f_s(x) + f_1(x) \cdot f'_2(x) \cdots f_s(x) + \dots + f_1(x) \cdot f_2(x) \cdots \\ &\quad \cdot f'_s(x)) \cdot f_{s+1}(x) + f_1(x) \cdots f_s(x) \cdot f'_{s+1}(x) = f'_1(x) \cdots f_s(x) \cdot f'_{s+1}(x) + \\ &+ f_1(x) \cdot f'_2(x) \cdots f_s(x) \cdot f_{s+1}(x) + \dots + f_1(x) \cdot f_2(x) \cdots f_s(x) \cdot f'_{s+1}(x). \end{aligned}$$

Tedy vztah (3.4) platí pro všechna $k \in \mathbb{N}$.

Definice 3.3:

Nechť $f(x) \in T[x]$, st $f(x) = n \geq 1$, $d_0, d_1, \dots, d_n \in T$, c libovolný prvek z T . Polynom

$$(3.5) \quad d_0 + d_1(x-c) + d_2(x-c)^2 + \dots + d_n(x-c)^n$$

se nazývá Taylorův rozvoj o středu c (v bodě c) polynomu $f(x)$, jestliže polynom (3.5) je roven polynomu $f(x)$.

Věta 3.2:

Ke každému polynomu $f(x) \in T[x]$ n -tého stupně ($n \geq 1$) a k libovolnému prvku $c \in T$ existuje právě jeden Taylorův rozvoj o středu c , který je tvaru

$$(3.6) \quad f(x) = f(c) + \frac{f'(c)}{1!} (x-c) + \frac{f''(c)}{2!} (x-c)^2 + \dots + \\ + \frac{f^{(n)}(c)}{n!} (x-c)^n.$$

Důkaz:

Protože $T[x]$ je eukleidovský okruh, můžeme postupně dělit polynomem $(x-c)$ takto:

$$f(x) = (x-c)g_1(x) + d_0 \quad / \cdot 1$$

$$(3.7) \quad \begin{aligned} g_1(x) &= (x-c)g_2(x) + d_1 && /.(x-c) \\ g_2(x) &= (x-c)g_3(x) + d_2 && /.(x-c)^2 \\ \dots & & & \\ g_{n-2}(x) &= (x-c)g_{n-1}(x) + d_{n-2} && /.(x-c)^{n-2} \\ g_{n-1}(x) &= (x-c)g_n(x) + d_{n-1} && /.(x-c)^{n-1} \end{aligned}$$

Podle věty 2.13 jsou prvky $d_0, d_1, \dots, d_{n-1} \in T$ a st $g_1(x) = n-1$, st $g_2(x) = n-2, \dots$, st $g_{n-2} = 2$, st $g_{n-1} = 1$, st $g_n(x) = 0$.

Polynom nultého stupně $g_n(x)$ si označíme jako $d_n \in T$. Rovnosti (3.7) vynásobíme postupně výrazy $1, (x-c), (x-c)^2, \dots, (x-c)^{n-2}, (x-c)^{n-1}$ a po vynásobení všechny rovnosti sečteme. Obdržíme hledaný Taylorův rozvoj polynomu $f(x)$ v bodě c

$$f(x) = d_0 + d_1(x-c) + d_2(x-c)^2 + \dots + d_n(x-c)^n.$$

Máme tedy dokázánu existenci Taylorova rozvoje a nyní jeho jednoznačnost.

Předpokládejme, že Taylorův rozvoj polynomu $f(x)$ o středu c má tvar

$$\begin{aligned} f(x) &= d_0 + d_1(x-c) + d_2(x-c)^2 + \dots + d_n(x-c)^n, \text{ pak platí } f(c) = d_0, \\ f'(x) &= d_1 + 2d_2(x-c) + \dots + nd_n(x-c)^{n-1}, \\ \text{odtud } f'(c) &= d_1 \text{ a } d_1 = \frac{f'(c)}{1!}, \\ f''(x) &= 2d_2 + 3.2.d_3(x-c) + \dots + n(n-1)d_n(x-c)^{n-2}, \\ \text{odtud } f''(c) &= 2d_2 \text{ a tedy } d_2 = \frac{f''(c)}{2!}, \end{aligned}$$

$$\begin{aligned} f^{(k)}(x) &= k!d_k + (k+1)k!d_{k+1}(x-c) + \dots + n(n-1)\dots(n-k+1)d_n(x-c)^{n-k} \\ \text{a odtud } f^{(k)}(c) &= k!d_k \text{ a } d_k = \frac{f^{(k)}(c)}{k!}, \end{aligned}$$

$$f^{(n)}(x) = n!d_n \text{ a odtud } d_n = \frac{f^{(n)}(c)}{n!}.$$

$$\begin{aligned} \text{Tedy } f(x) &= f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \dots + \\ &+ \frac{f^{(n)}(c)}{n!}(x-c)^n. \end{aligned}$$

Podle postupu v důkazu věty 3.2 je vidět, že pro praktický výpočet koeficientů Taylorova rozvoje polynomu $f(x) \in T[x]$ o středu $c \in T$ lze s výhodou použít Hornerova schématu tak, že postupně počítáme pro prvek c hodnoty polynomů $f(x), g_1(x), g_2(x), \dots, g_n(x)$. Celý výpočet přitom můžeme usporádat do jediné tabulky.

Příklad 3.1:

Určete Taylorův rozvoj o středu $c = -2$ polynomu $f(x) = 2x^5 - 3x^3 + x^2 - 4x + 8$.

Řešení:

Postupně počítáme podle Hornerova schematu pro $c = -2$.

	2	0	-3	1	-4	8	
-2	-	-4	8	-10	18	-28	
	2	-4	5	-9	14	<u>-20</u>	$= f(-2)$
-2	-	-4	16	-42	102		
	2	-8	21	-51	<u>116</u>	$\frac{f'(-2)}{1!}$	
-2	-	-4	24	-90			
	2	-12	45	<u>-141</u>	$\frac{f''(-2)}{2!}$		
-2	-	-4	32				
	2	-16	<u>77</u>	$\frac{f'''(-2)}{3!}$			
-2	-	-4					
	2	<u>-20</u>	$\frac{f^{IV}(-2)}{4!}$				
	2	$\frac{f^V(c)}{5!}$					

Hledaný Taylorův rozvoj má tedy tvar

$$f(x) = -20 + 116(x+2) - 141(x+2)^2 + 77(x+2)^3 - 20(x+2)^4 + 2(x+2)^5.$$

Taylorův rozvoj můžeme také využít pro výpočet hodnot všech derivací daného polynomu $f(x) \in T[x]$ v daném bodě $c \in T$, resp. pro zjištění, zda prvek $c \in T$ je kořenem daného polynomu a jaká je jeho násobnost.

Příklad 3.2:

Určete hodnotu polynomu a všech jeho derivací v bodě $c = -2$ pro polynom $f(x) = 2x^5 - 3x^3 + x^2 - 4x + 8$.

Řešení:

Použijeme výpočtu z příkladu 3.1 a odtud zjistíme, že $f(-2) = -20$, $f'(-2) = 116$, $f''(-2) = 2 \cdot (-141) = -282$, $f'''(-2) = 3! \cdot 77 = 462$, $f^{IV}(-2) = 4! \cdot (-20) = -480$, $f^V(-2) = 5! \cdot 2 = 240$.

Příklad 3.3:

Dokažte, že polynom $f(x) = x^4 - 5x^3 + 6x^2 + 4x - 8$ má trojnásobný kořen $c=2$. Určete zbývající kořen a daný polynom rozložte na součin lineárních faktorů.

Řešení:

Opět použijeme Hornerova schematu a vzhledem k tomu, že se jedná o snadné výpočty, rádky, odpovídající součinům $c \cdot b_k$ můžeme vynechat a psát přímo výsledné součty.

	1	-5	6	4	-8	
2	1	-3	0	4	<u>0</u>	$= f(2)$
2	1	-1	-2		<u>0</u>	
2	1	1		<u>0</u>		
2	1		<u>3 ≠ 0</u>			
2		<u>1</u>				

Můžeme tedy psát podle provedených výpočtů v Hornerově schematu $f(x) = (x-2)(x^3 - 3x^2 + 4) = (x-2)^2(x^2 - x - 2) = (x-2)^3 \cdot (x+1)$ a odtud vidíme, že $c=2$ je trojnásobný kořen polynomu $f(x)$ a zbývající čtvrtý kořen je roven -1 .

Další použití Hornerova schematu si ukážeme ve cvičeních, chci jenom připomenout, že jeho použití je zejména výhodné v takovýchto případech:

Příklad 3.4:

Určete hodnotu polynomu $f(x) = 0,0324x^4 - 256x^3 + 12,335x^2 + 284,45x + 3,854$ a všech jeho derivací v bodě $c = 2,138$ s přesností 10^{-3} .

Řešení:

|

	0,0324	-256	12,335	284,45	3,854
2,138	-	0,0693	-547,1798	-1143,4982	-1836,6451
	0,0324	-255,9307	-534,8448	-859,0482	<u>-1832,7911</u>
2,138	-	0,0693	-547,0317	-2313,0519	
	0,0324	-255,8614	-1081,8765	<u>-3172,1001</u>	
2,138	-	0,0693	-546,8835		
	0,0324	-255,7921	<u>-1628,7600</u>		
2,138	-	0,0693			
	0,0324	<u>-255,7228</u>			
	<u>0,0324</u>				

$$f(2,138) = -1832,792$$

$$f'(2,138) = -3172,101$$

$$f''(2,138) = -3257,520$$

$$f'''(2,138) = -1534,334$$

$$f^{IV}(2,138) = 0,778 .$$

Poznámka 3.4:

Vzorec (3.6) pro Taylorův rozvoj polynomu $f(x)$ se někdy používá ve tvaru: $f(y+c) = f(c) + \frac{f'(c)}{1!}y + \frac{f''(c)}{2!}y^2 + \dots + \frac{f^{(n)}(c)}{n!}y^n$. Který používáme v případě, že máme provést substituci tvaru $x = y+c$. Takto se řeší úlohy následujícího typu:

Příklad 3.5:

Nechť polynom $f(x) = x^2 + a_1x + a_0 \in T[x]$ má kořeny x_1 a x_2 . Sestrojte polynom $g(y)$, který má kořeny $y_1 = x_1 - \beta$, $y_2 = x_2 - \beta$, kde $\beta \in T$, $\beta \neq 0$.

Řešení:

	1	a_1	a_0
β	-	β	$a_1\beta + \beta^2$
	1	$a_1 + \beta$	<u>$a_0 + a_1\beta + \beta^2 = f(\beta)$</u>
β	-	β	
	1	<u>$a_1 + 2\beta$</u>	$= \frac{f'(\beta)}{1!}$
	<u>1</u>	<u>$\frac{f''(\beta)}{2!}$</u>	

Hledaný polynom má tvar

$$g(y) = f(y+\beta) = y^2 + (a_1 + \beta)y + (a_0 + a_1\beta + \beta^2).$$

Věta 3.3:

Je-li prvek $c \in T$ k-násobným kořenem nenulového polynomu $f(x) \in T[x]$, st $f(x) \geq 1$ pak při $k > 1$ je také $(k-1)$ -násobným kořenem první derivace $f'(x)$ tohoto polynomu. Při $k=1$ prvek c není kořenem první derivace $f'(x)$.

Důkaz:

Podle předpokladu platí pro $k=1$

$$(3.9) \quad f(x) = (x-c)g(x) \wedge (x-c) \nmid g(x).$$

Nechť $k > 1$. Vypočteme první derivaci a upravíme

$$(3.10) \quad f'(x) = k(x-c)^{k-1}g(x) + (x-c)^kg'(x) = (x-c)^{k-1}h(x), \text{ kde}$$

$$(3.11) \quad h(x) = kg(x) + (x-c)g'(x) \text{ a } h(c) = kg(c) \neq 0.$$

Ze vztahů (3.10) a (3.11) bezprostředně plyne naše tvrzení.

Poznámka 3.5:

Ukažme si na příkladu, že ve větě 3.3 je podmínka, aby těleso T bylo charakteristiky nula podstatná. Věta 3.3 pro tělesa nenulové charakteristiky neplatí.

Snadno se ověří, že polynom $f(x) = x^7 + x^5 = x^5(x^2 + 1) \in Z_5[x]$, $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ má pětinásobný kořen $c = \bar{0}$, kdežto $f'(x) = (7 \times 1)x^6 + (5 \times 1)x^4 = \bar{2}x^6$ má tento kořen šestinásobný.

Důsledek 3.2:

Každý k-násobný ($k > 1$) kořen polynomu $f(x) \in T[x]$, st $f(x) \geq 1$ je také $(k-s)$ -násobný kořen s-té derivace polynomu $f(x)$ pro $s = 1, 2, \dots, k-1$ a není kořen k-té derivace polynomu $f(x)$.

Věta 3.4:

Prvek $c \in T$ je k-násobným kořenem polynomu $f(x) \in T[x]$, st $f(x) \geq 1$, právě tehdy, když je kořenem polynomů $f(x), f'(x), \dots, f^{(k-1)}(x)$ a není kořenem k-té derivace polynomu $f(x)$.

Důkaz:

Nechť $c \in T$ je k-násobným kořenem polynomu $f(x)$, pak podle důsledku 3.2 je kořenem polynomů $f(x), f'(x), \dots, f^{(k-1)}(x)$ a není kořenem polynomu $f^{(k)}(x)$.

Obráceně, je-li $c \in T$ kořenem polynomů $f(x), f'(x), \dots, f^{(k-1)}(x)$ a není kořenem polynomu $f^{(k)}(x)$, má Taylorův rozvoj polynomu $f(x)$ o

středu c podle (3.6) tvar

$$(3.12) \quad f(x) = \frac{f^{(k)}(c)}{k!} (x-c)^k + \frac{f^{(k+1)}(c)}{(k+1)!} (x-c)^{k+1} + \dots + \\ + \frac{f^{(n)}(c)}{n!} (x-c)^n = (x-c)^k h(x), \text{ kde} \\ h(x) = \frac{f^{(k)}(c)}{k!} + \frac{f^{(k+1)}(c)}{(k+1)!} (x-c) + \dots + \frac{f^{(n)}(c)}{n!} (x-c)^{n-k} \\ \text{a } h(c) = \frac{f^{(k)}(c)}{k!} \neq 0.$$

Tedy $c \in T$ je k-násobný kořen polynomu $f(x)$.

Věta 3.5:

Má-li nenulový polynom $f(x) \in T[x]$ alespoň jeden vícenásobný kořen, pak jsou polynomy $f(x)$ a $f'(x)$ soudělné.

Důkaz:

Nechť $c \in T$ je k-násobný kořen polynomu $f(x)$, kde $k > 1$. Podle věty 3.3 platí $f(x) = (x-c)^k g_1(x)$ a $f'(x) = (x-c)^{k-1} g_2(x)$ a jelikož je $k-1 \geq 1$, jsou polynomy $f(x)$ a $f'(x)$ soudělné.

Poznámka 3.6:

Nad některými tělesy platí k větě 3.5 i věta obrácená. Jsou to tzv. algebraicky uzavřená tělesa, mezi něž patří např. těleso komplexních čísel C. V tělese komplexních čísel platí tzv. Základní věta algebry, jejíž první správný důkaz podal r. 1799 K.F. Gauss.

Vzhledem k tomu, že její důkaz je značně rozsáhlý a komplikovaný, nebudeme jej v našem základním kursu algebry uvádět. Navíc se při jejím důkazu používají i prostředky matematické analýzy, protože čistě algebraickými prostředky se důkaz provést nedá. Důkaz Základní věty algebry je uveden např. v [7].

Přitom však v další části skript budeme platnost Základní věty algebry předpokládat.

Základní věta algebry má několik ekvivalentních formulací, které si uvedeme. My budeme v dalším textu používat tu, která je uvedena na prvním místě. Ke čtvrté formulaci potřebujeme následující pojem.

Definice 3.4:

Těleso T se nazývá algebraicky uzavřené, jestliže každý polynom $f(x) \in T[x]$ stupně $n \geq 1$ má v tomto tělese alespoň jeden kořen.

Věta 3.6: (Základní věta algebry).

- I. Každý polynom s komplexními koeficienty stupně alespoň prvního má alespoň jeden kořen, který je komplexním číslem.
- II. Každý polynom $f(x) \in C[x]$ stupně $n \geq 1$ má v C rozklad tvaru $f(x) = a(x-c_1)(x-c_2)\dots(x-c_n)$, kde $a \neq 0$ a c_1, c_2, \dots, c_n jsou kořeny polynomu $f(x)$.
- III. Množina všech irreducibilních polynomů v $C[x]$ je totožná s množinou všech polynomů z $C[x]$ stupně 1.
- IV. Těleso komplexních čísel je algebraicky uzavřené.

Věta 3.7:

Nechť $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, $a_n \neq 0$ je polynom stupně $n \geq 1$ nad tělesem komplexních čísel C . Pak platí:

- 1) Polynom $f(x)$ se dá vyjádřit jako součin lineárních polynomů a nenulové konstanty ve tvaru

$$(3.13) \quad f(x) = a_n (x-c_1)(x-c_2)\dots(x-c_n), \text{ kde } a_n \neq 0 \text{ a}$$
 c_1, c_2, \dots, c_n jsou kořeny polynomu $f(x)$.
(Rozklad polynomu $f(x)$ na kořenové činitele).
- 2) Vyjádření polynomu $f(x)$ ve tvaru (3.13) je až na pořadí činitelů určeno jednoznačně.
- 3) Polynom $f(x)$ má právě n kořenů, počítáme-li každý kořen tolikrát, kolik činí jeho násobnost. Všechny kořeny jsou komplexní čísla.

Důkaz:

- 1) Podle ZVA existuje alespoň jedno $c_1 \in C$ takové, že $f(x) = (x-c_1).f_1(x)$, kde $f_1(x) \in C[x]$ a st $f_1(x) = n-1$. (Prvek c_1 je kořenem polynomu $f(x)$). Je-li $n-1 \geq 1$, existuje opět alespoň jedno $c_2 \in C$ takové, že $f_1(x) = (x-c_2).f_2(x)$, kde $f_2(x) \in C[x]$ a st $f_2(x) = n-2$.

Opakováním tohoto postupu získáme komplexní čísla c_1, c_2, \dots, c_n taková, že platí

$$(3.14) \quad f(x) = (x-c_1)(x-c_2)\dots(x-c_n).f_n(x),$$

kde st $f_n(x) = 0$. Porovnáním koeficientů na levé a pravé straně rovnosti (3.14) u x^n dostaneme, že $f_n(x) = a_n$. Máme

tedy $f(x) = (x-c_1)(x-c_2)\dots(x-c_n).a_n$.

2) Jestliže kromě rozkladu (3.13) polynomu $f(x)$ je možný ještě rozklad

$$(3.15) \quad f(x) = b_m(x-d_1)(x-d_2)\dots(x-d_m),$$

musí platit

$$(3.16) \quad a_n(x-c_1)(x-c_2)\dots(x-c_n) = b_m(x-d_1)(x-d_2)\dots(x-d_m).$$

Pak porovnáním stupňů obou polynomů a koeficientů u nejvyšších mocnin dostaneme $n = m$ a $a_n = b_m$. Kdyby některé c_k ($1 \leq k \leq n$) bylo různé od všech d_i ($1 \leq i \leq n$), pak levá strana rovnosti (3.16) pro $x=c_k$ by byla rovna nulovému prvku z C , kdežto pravá strana by byla různá od nuly, což odporuje dosazovacímu pravidlu. Obdobně se dokáže, že každý prvek d_i ($1 \leq i \leq n$) musí být roven některému c_k ($1 \leq k \leq n$).

Mezi kořeny c_k ($1 \leq k \leq n$) však mohou být některé stejné. Při vhodném očíslování kořenů lze rovnost (3.16) přepsat na tvar

$$(3.17) \quad a_n(x-c_1)^{i_1}(x-c_2)^{i_2}\dots(x-c_j)^{i_j} = a_n(x-c_1)^{k_1}(x-c_2)^{k_2}\dots(x-c_j)^{k_j},$$

kde c_1, c_2, \dots, c_j jsou navzájem různé kořeny polynomu $f(x)$ a

$$i_1 + i_2 + \dots + i_j = n = k_1 + k_2 + \dots + k_j.$$

Je-li např. $i_1 < k_1$, pak krácením v (3.17) polynomem

$a_n(x-c_1)^{i_1}$ obdržíme rovnost

$$(3.18) \quad (x-c_2)^{i_2}(x-c_3)^{i_3}\dots(x-c_j)^{i_j} = (x-c_1)^{k_1 - i_1} \cdot$$

$$\cdot (x-c_2)^{k_2} \dots (x-c_j)^{k_j}.$$

To však znamená, že pro $x = c_1$ je levá strana rovnosti (3.18) různá od nuly, kdežto pravá strana rovnosti se rovná nule, protože $k_1 - i_1 > 0$. Což je spor.

Podobně bychom došli ke sporu i v případě $i_1 > k_1$ nebo v kterémkoli z případů $i_2 \neq k_2, \dots, i_j \neq k_j$.

3) Z tvrzení 2) plyne, že polynom $f(x)$ se dá psát ve tvaru

$$(3.19) \quad f(x) = a_n(x-c_1)^{i_1}(x-c_2)^{i_2}\dots(x-c_j)^{i_j}$$

kde c_1, c_2, \dots, c_j jsou navzájem různé komplexní kořeny polynomu $f(x)$ a $i_1 + i_2 + \dots + i_j = n$.

Přitom číslo i_k ($1 \leq k \leq n$) udává násobnost kořene c_k polynomu $f(x)$.

Např. pro $k=1$ máme $f(x) = (x-c_1)^{i_1} \cdot g(x)$.

Přitom polynom $g(x)$ je nesoudělný s $(x-c_1)$, neboť kterýkoliv z činitelů $(x-c_2)\dots(x-c_j)$ je nesoudělný s $(x-c_1)$ a tudíž je nesoudělný s $(x-c_1)$ také jejich součin $g(x)$.

Pokud nemá $f(x)$ žádný další kořen, různý od c_1, c_2, \dots, c_j , je věta dokázána. Ale to není možné, neboť by to bylo ve sporu s tvrzením ve 2).

Definice 3.5:

Rozkladu polynomu $f(x) \in C[x]$ ve tvaru (3.19) se říká kanonický rozklad polynomu $f(x)$ na součin irreducibilních polynomů.

Jestliže připouštíme v rozkladu (3.19) také exponenty rovné 0, pak mluvíme o takzvaném zobecněném kanonickém rozkladu.

Poznámka 3.7:

Vztahy mezi koeficienty polynomu $f(x)$ a mezi jeho kořeny udává tzv. Newton-Vietova věta. Příslušným vzorcům se pak říká Newtonovy vzorce nebo také Vietovy vzorce.

Věta 3.8:

Nechť $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, $a_n \neq 0$, $n \geq 1$ je polynom nad tělesem C a $c_1, c_2, \dots, c_n \in C$ jsou jeho kořeny. Pak platí:

$$(3.20) \quad \begin{aligned} -\frac{a_{n-1}}{a_n} &= c_1 + c_2 + \dots + c_n \\ \frac{a_{n-2}}{a_n} &= c_1 c_2 + c_1 c_3 + \dots + c_{n-1} c_n \\ -\frac{a_{n-3}}{a_n} &= c_1 c_2 c_3 + c_1 c_2 c_4 + \dots + c_{n-2} c_{n-1} c_n \\ \dots & \\ (-1)^n \frac{a_0}{a_n} &= c_1 c_2 c_3 \dots c_n. \end{aligned}$$

Důkaz:

Podle věty 3.7 lze polynom $f(x)$ vyjádřit právě jedním způsobem ve tvaru $f(x) = a_n (x-c_1)(x-c_2)\dots(x-c_n)$.

Nejprve obě strany této rovnosti vydělíme prvkem $a_n \neq 0$. Provedeme-li roznásobení na pravé straně rovnosti a porovnáme-li koeficienty na obou stranách uvažované rovnosti u stejných mocnin x , obdržíme požadované vzorce (3.20).

Věta 3.9:

Je-li polynom $f(x) \in C[x]$ soudělný se svou první derivací, pak má alespoň jeden vícenásobný kořen.

Důkaz:

Nechť $D(x)$ je největší společný dělitel polynomů $f(x)$ a $f'(x)$. Podle věty 3.7 se dá polynom $D(x)$ rozložit na lineární faktory. V tomto rozkladu se bude vyskytovat alespoň jeden činitel tvaru $(x-c)^m$, $m > 0$. Pak musí být v rozkladu polynomu $f(x)$ činitel $(x-c)^{m+r}$, $r \geq 0$. Tj. prvek $c \in C$ je alespoň $(m+r)$ -násobným kořenem polynomu $f(x)$. Podle věty 3.3 je však $c \in C$ $(m+r-1)$ -násobným kořenem polynomu $f'(x)$ a v rozkladu polynomu $f'(x)$ se vyskytuje faktor $(x-c)^{m+r-1}$. Jelikož je $D(x)$ největší společný dělitel polynomů $f(x)$ a $f'(x)$, musí být $m+r-1 = m$ a odtud $r=1$. Jelikož je $m > 0$, je prvek $c \in C$ alespoň dvojnásobným kořenem polynomu $f(x)$.

Věta 3.10:

Nechť $f(x)$ je polynom stupně $n \geq 1$ nad tělesem C . Pak lze najít polynom $g(x) \in C[x]$ takový, že má tytéž kořeny jako polynom $f(x)$, ale samé jednoduché.

Důkaz:

Pro $n=1$ položíme $g(x) = f(x)$. Nechť tedy dále $n > 1$.

Podle věty 3.7 uděláme kanonický rozklad polynomu $f(x)$ ve tvaru

$$f(x) = a_n (x-c_1)^{i_1} (x-c_2)^{i_2} \dots (x-c_j)^{i_j}$$

kde c_1, c_2, \dots, c_j jsou navzájem různé kořeny polynomu $f(x)$ a

$i_1 + i_2 + \dots + i_j = n$. Podle věty 3.3 má derivace $f'(x)$ tvar

$$f'(x) = b (x-c_1)^{i_1-1} (x-c_2)^{i_2-1} \dots (x-c_j)^{i_j-1} (x-d_1)^{k_1-1} \cdot \\ \cdot (x-d_2)^{k_2-1} \dots (x-d_p)^{k_p-1}, \quad b \in C,$$

kde $c_1, c_2, \dots, c_j, d_1, d_2, \dots, d_p$ jsou navzájem různé prvky, takže žádný z prvků d_1, d_2, \dots, d_p není roven žádnému z prvků c_1, c_2, \dots, c_j . Polynom $D(x)$, který je největší společný dělitel polynomů $f(x)$ a $f'(x)$ má tedy až na číselný faktor tvar

$$D(x) = (x-c_1)^{i_1-1} (x-c_2)^{i_2-1} \dots (x-c_j)^{i_j-1}.$$

Podíl $\frac{f(x)}{D(x)}$ je rovněž polynom z $C[x]$ a označíme jej $g(x)$. Přitom má $g(x)$ tvar

$$g(x) = a_n (x-c_1) (x-c_2) \dots (x-c_j)$$

a splňuje naše požadavky.

Poznámka 3.8:

Předchozí věta nám současně dává návod, jak k danému polynomu $f(x)$ určit polynom $g(x)$ požadovaných vlastností, což si ukážeme na příkladě. Tomuto postupu budeme říkat odstranění vícenásobných kořenů polynomu.

Příklad 3.5:

Odstraňte vícenásobné kořeny polynomu $f(x) = x^3 - x^2 - 8x + 12$.
Řešení:

Postupovat budeme takto:

- 1) Pomocí Eukleidova algoritmu určíme největšího společného dělitele $D(x)$ polynomů $f(x)$ a $f'(x)$.
- 2) Polynom $f(x)$ vydělíme polynomem $D(x)$ a obdržíme hledaný polynom $g(x)$, který má tytéž kořeny jako polynom $f(x)$, ale samé jednoduché.

Jelikož $f'(x) = 3x^2 - 2x - 8$, vezmeme místo polynomu $f(x)$ polynom $9f(x)$ a počítáme

$$(9x^3 - 9x^2 - 72x + 108):(3x^2 - 2x - 8) = 3x - 1$$

$$\begin{array}{r} -9x^3 + 6x^2 - 24x \\ \hline -3x^2 - 48x + 108 \\ \hline 3x^2 - 2x - 8 \\ \hline -50x + 100 = -50(x-2) \end{array}$$

$$(3x^2 - 2x - 8):(x-2) = 3x + 4$$

$$\begin{array}{r} -3x^2 + 6x \\ \hline 4x - 8 \\ -4x + 8 \\ \hline 0 \end{array}$$

Tedy $D(x) = x-2$.

$$(x^3 - x^2 - 8x + 12):(x-2) = x^2 + x - 6$$

$$\begin{array}{r} -x^3 + 2x^2 \\ \hline x^2 - 8x + 12 \\ -x^2 + 2x \\ \hline -6x + 12 \\ 6x - 12 \\ \hline 0 \end{array}$$

Hledaný polynom $g(x) = x^2 + x - 6 = (x-2)(x+3)$.

(Daný polynom $f(x)$ má kanonický rozklad $f(x) = (x-2)^2(x+3)$).

Na závěr této kapitoly si uvedeme několik vět o polynomech s reálnými koeficienty a s celočíselnými koeficienty, které jsou potřebné pro některé partie z matematické analýzy.

K tomuto účelu si zopakujme některé vlastnosti komplexních čísel. Komplexní čísla, která nejsou reálná se nazývají imaginární čísla.

Je-li $z \in \mathbb{C}$, $z = a + bi$, pak $\bar{z} = a - bi$ se nazývá číslo komplexně sdružené k číslu z a platí: $z + \bar{z} = 2a \in \mathbb{R}$, $z \cdot \bar{z} = a^2 + b^2 \in \mathbb{R}$.

Jsou-li $y_1, y_2 \in \mathbb{C}$, $y_1 = a_1 + b_1 i$, $y_2 = a_2 + b_2 i$, pak platí:

Jestliže $y_1 + y_2 = u$, $y_1 \cdot y_2 = v$, pak $\bar{y}_1 + \bar{y}_2 = \bar{u}$, $\bar{y}_1 \cdot \bar{y}_2 = \bar{v}$. Toto se dá zobecnit na konečný počet sčítanců a činitelů. Jestliže

$y_1, y_2, \dots, y_n \in \mathbb{C}$ a $y_1 + y_2 + \dots + y_n = u$, $y_1 \cdot y_2 \cdots y_n = v$, pak

$\bar{y}_1 + \bar{y}_2 + \dots + \bar{y}_n = \bar{u}$ a $\bar{y}_1 \cdot \bar{y}_2 \cdots \bar{y}_n = \bar{v}$. Speciálně pro $y_1 = y_2 = \dots = y_n = y$ dostáváme $(\bar{y})^n = (\bar{y}^n)$.

Věta 3.11:

Nechť imaginární číslo c je kořenem polynomu $f(x)$ stupně alespoň jedna nad tělesem reálných čísel. Pak také číslo komplexně sdružené \bar{c} je kořenem polynomu $f(x)$.

Důkaz:

Nechť $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, $n \geq 1$, $a_n \neq 0$, $a_i \in \mathbb{R}$ pro $i = 1, 2, \dots, n$. Jelikož c je kořenem $f(x)$, platí

$$f(c) = a_0 + a_1 c + a_2 c^2 + \dots + a_n c^n = 0.$$

Podle pravidel pro počítání s komplexními čísly dostáváme

$$\begin{aligned} \bar{f}(\bar{c}) &= \overline{(a_0 + a_1 c + a_2 c^2 + \dots + a_n c^n)} = \bar{a}_0 + \bar{a}_1 \bar{c} + \bar{a}_2 \bar{c}^2 + \dots + \\ &+ \bar{a}_n \bar{c}^n = \bar{a}_0 + \bar{a}_1 \bar{c} + \bar{a}_2 (\bar{c})^2 + \dots + \bar{a}_n (\bar{c})^n = \bar{0}. \end{aligned}$$

Protože však $0 \in \mathbb{R}$ a $a_i \in \mathbb{R}$ pro $i = 1, 2, \dots, n$, dostáváme z poslední rovnosti následující rovnost $a_0 + a_1 \bar{c} + a_2 (\bar{c})^2 + \dots + a_n (\bar{c})^n = 0$ a tedy $f(\bar{c}) = 0$, což značí, že \bar{c} je kořenem polynomu $f(x)$.

Věta 3.12:

Ireducibilními polynomy v $R[x]$ jsou právě všechny polynomy stupně 1 a polynomy stupně 2, které mají imaginární kořeny.

Důkaz:

- Je-li polynom $f(x) \in R[x]$ lineární, je ireducibilní. Rovněž tak, je-li st $f(x) = 2$ a nemá-li přitom $f(x)$ žádný reálný kořen. Protože v tom případě nemůže v $R[x]$ existovat jeho dělitel stupně 1.
- Nechť $f(x) \in R[x]$, st $f(x) = n$ a $f(x)$ je ireducibilní v $R[x]$. Zřejmě musí být $n \geq 1$. Případ $n=1$ je triviální. Nechť tedy $n > 1$. Má-li $f(x)$ alespoň jeden reálný kořen c , je $f(x)$ dělitelný činitelem $(x-c)$ a tedy je reducibilní. Polynom $f(x)$ tedy nemůže mít žádný reálný kořen. Podle věty 3.11 má polynom $f(x) \in R[x]$ s každým imaginárním kořenem c také kořen \bar{c} . Tedy $f(x)$ je dělitelný polynomem $(x-c)(x-\bar{c}) = x^2 + (c + \bar{c})x + c\bar{c} \in R[x]$. Kdyby platilo $n > 2$, byl by polynom $f(x)$ nutně reducibilní v $R[x]$, takže $f(x)$ je stupně 2 s dvojicí imaginárních kořenů c a \bar{c} .

Na základě vět 3.7 a 3.12 dostáváme jako důsledek následující věty:

Věta 3.13:

Nechť $f(x) \in R[x]$, st $f(x) = n \geq 1$. Pak $f(x)$ má v $R[x]$ rozklad na součin ireducibilních polynomů tvaru

$$(3.21) \quad f(x) = a_n (x-c_1)^{i_1} \dots (x-c_j)^{i_j} (x^2 + p_1 x + q_1)^{k_1} \dots \dots (x^2 + p_r x + q_r)^{k_r},$$

$n = i_1 + \dots + i_j + 2(k_1 + \dots + k_r)$ a žádný z kvadratických činitelů v (3.21) nemá reálný kořen.

Jinými slovy: Každý nenulový polynom s reálnými koeficienty lze psát jako součin konečného počtu ireducibilních polynomů nad R .

Věta 3.14:

Každý polynom z $R[x]$ lichého stupně má alespoň jeden reálný kořen.

Věta 3.15:

Má-li polynom $f(x) \in R[x]$ imaginární kořeny, pak jich má sudý počet.

Definice 3.5:

Rozklad (3.21) polynomu $f(x) \in R[x]$ se nazývá rozklad polynomu $f(x)$ nad tělesem reálných čísel.

Věta 3.16:

Nechť $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, $a_n \neq 0$, $n \geq 1$ je polynom s celočíselnými koeficienty. Pak je-li racionální číslo $r = \frac{p}{q}$ (kde $p \neq 0$, $q \neq 0$ jsou nesoudělná celá čísla) kořenem polynomu $f(x)$, pak platí $p|a_0$ a $q|a_n$.

Důkaz:

Podle předpokladu platí

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

Odtud po vynásobení prvkem q^n dostáváme

$$(3.22) \quad a_0 q^n + a_1 p q^{n-1} + \dots + a_n p^n = 0.$$

Úpravou vztahu (3.21) dostáváme rovnosti

$$p(a_1 q^{n-1} + \dots + a_n p^{n-1}) = -a_0 q^n,$$

$$q(a_0 q^{n-1} + \dots + a_{n-1} p^{n-1}) = -a_n p^n.$$

Z první rovnosti dostáváme $p|a_0$ a z druhé rovnosti $q|a_n$.

Jako důsledek věty 3.16 dostáváme následující větu:

Věta 3.17:

Jestliže $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1} + x^n$ je libovolný polynom s celočíselnými koeficienty, pak každé racionální číslo r , které je kořenem tohoto polynomu je číslo celé a platí $r|a_0$.

Věta 3.18:

Nechť $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, $a_n \neq 0$, $n \geq 1$ je polynom s celočíselnými koeficienty a pro prvek $c \in Z$ nechť $f(c) \neq 0$. Pak je-li racionální číslo $r = \frac{p}{q}$ (kde $p \neq 0, q \neq 0$ jsou nesoudělná celá čísla) kořenem polynomu $f(x)$, platí $(p-q)|f(c)$.

Speciálně $(p-q)|f(1)$, jestliže $f(1) \neq 0$ a $(p+q)|f(-1)$, jestliže $f(-1) \neq 0$.

Důkaz:

Vezměme libovolné $c \in \mathbb{Z}$, pro které $f(c) \neq 0$, pak podle věty 2.13 máme $f(x) = (x-c)g(x) + f(c)$. Jestliže $r = \frac{p}{q}$ je kořen polynomu $f(x)$, dostáváme $f\left(\frac{p}{q}\right) = 0$ a $\left(\frac{p}{q} - c\right) \cdot g\left(\frac{p}{q}\right) = -f(c)$. Po vynásobení poslední rovnosti číslem $q \neq 0$ obdržíme $(p - cq)g\left(\frac{p}{q}\right) = -q \cdot f(c)$. Jelikož p, q jsou nesoudělná, jsou také $(p - cq)$ a q nesoudělná a tudíž platí $(p - cq) | f(c)$.

Výpočet racionálních kořenů polynomu s celočíselnými koeficienty si ukážeme na následujících příkladech:

Příklad 3.6:

Najděte racionální kořeny polynomu $f(x) = x^3 + 3x^2 - 8x + 10 \in \mathbb{Z}[x]$.

Řešení:

Jestliže polynom $f(x)$ má nějaký racionální kořen r , musí to být podle věty 3.17 číslo celé a musí dělit $a_0 = 10$. Připadají tedy do úvahy pouze čísla $1, -1, 2, -2, 5, -5, 10, -10$. Postupným prováděním Hornerova schematu pro tato čísla zjistíme, že polynom $f(x)$ má jediný racionální kořen $c = -5$. Zbývající kořeny jsou $1+i$ a $1-i$. Neboť

	1	3	-8	10
-5	-	-5	10	-10
	1	-2	2	0 = f(-5)

Příklad 3.7:

Určete racionální kořeny polynomu $f(x) = 4x^3 - 4x^2 - 11x + 6$.

Řešení:

Jestliže daný polynom má racionální kořen r , bude $r = \frac{p}{q}$, kde $p, q \in \mathbb{Z}$, navzájem nesoudělná a $p|6$, $q|4$. V úvahu přicházejí tedy čísla $p \in \{1, -1, 2, -2, 3, -3, 6, -6\}$, $q \in \{1, -1, 2, -2, 4, -4\}$. Pomocí Hornerova schématu zjistíme, že $f(1) = -5$, $f(-1) = 9$. Budeme tedy hledat zlomky $r = \frac{p}{q}$, pro něž platí podmínky $(p - q)|(-5)$ a $(p + q)|9$. Snadným výpočtem ověříme, že připadají do úvahy pouze čísla $\frac{1}{2}, (-\frac{1}{4}), 2, (-\frac{3}{2})$. Opět pomocí Hornerova schematu zjistíme, že daný polynom má racionální kořeny a jsou to čísla $\frac{1}{2}, 2$ a $(-\frac{3}{2})$.

Cvičení 3:

Příklad 1:

Zjistěte násobnost kořenů $c_1 = -2$, $c_2 = 1$ polynomu $f(x) = x^6 + 3x^5 + 4x^4 + 3x^3 - 15x^2 - 16x + 20$. Polynom poté rozložte na součin irreducibilních polynomů nad $\mathbb{R}[x]$.

Příklad 2:

- a) Najděte zbývající kořeny polynomu $f(x) = x^4 - 4x^2 + 8x - 4 \in \mathbb{R}[x]$, jestliže jeden kořen je $c = 1+i$.
- b) Najděte všechny kořeny polynomu $f(x) = 6x^6 - 5x^5 - 14x^4 - 25x^3 - 146x^2 - 20x + 24$, víte-li, že $c_1 = 2i$, $c_2 = 3$, $c_3 = -2$.

Příklad 3:

Napište polynom $f(x)$ čtvrtého stupně s reálnými koeficienty, kde $a_4 = 1$, jestliže číslo $c = 2+i$ je dvojnásobným kořenem polynomu $f(x)$.

Příklad 4:

Dokažte, že polynom $f(x) = x^5 + ax + b$ má vícenásobný kořen právě když $(\frac{b}{4})^4 + (\frac{a}{5})^5 = 0$.

Příklad 5:

Najděte kořeny polynomu $f(x) = 4x^3 - 8x^2 + x + 3$, jestliže jeden z nich je roven součtu ostatních.

Příklad 6:

Najděte kořeny polynomu $f(x) = x^4 - 7x^3 + 17x^2 - 17x + 6$, jestliže součet dvou kořenů je roven 4.

Příklad 7:

Najděte taková čísla $a, b, c \in \mathbb{Z}$, aby byla kořeny polynomu $f(x) = x^3 + ax^2 + bx + c$.

Příklad 8:

Najděte rozklad polynomu $f(x) = x^4 - 8x^2 + 15$ v $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, \mathbb{R} , kde $\mathbb{Q}[\sqrt{3}]$ resp. $\mathbb{Q}[\sqrt{5}]$ jsou obory integrity, sestávající ze všech prvků tvaru $a + b\sqrt{3}$, resp. $a + b\sqrt{5}$, $a, b \in \mathbb{Q}$.

Příklad 9:

Nechť $f(x) = x^3 - 3x + 1$ má kořeny c_1, c_2, c_3 . Najděte polynom třetího stupně, který má kořeny $c_1 - 1, c_2 - 1, c_3 - 1$.

Příklad 10:

Jestliže víte, že polynom $f(x) = x^5 - 5x^3 + 4x$ má kořeny $c_1 = 0, c_2 = 1, c_3 = 2$, vypočítejte zbývající kořeny a napište kanonický rozklad polynomu $f(x)$.

Příklad 11:

Určete všechny kořeny polynomu $f(x) = x^4 - 3x^3 + 6x^2 - 3x + 5$, jestliže víte, že jeden kořen je roven i. Napište rozklad $f(x)$ na součin ireducibilních polynomů nad \mathbb{R} .

Příklad 12:

- Určete polynom čtvrtého stupně, jsou-li dány jeho kořeny $c_1 = 5, c_2 = -4, c_3 = 2, c_4 = -3$.
- Určete polynom pátého stupně, který má trojnásobný kořen 2 a dvojnásobný kořen 3.
- Určete polynom pátého stupně, znáte-li jeho čtyři kořeny $c_1 = -1, c_2 = 0, c_3 = \frac{1}{2}, c_4 = 3$.

Příklad 13:

Ověřte, že polynom $f(x) = x^4 - 5x^3 + 6x^2 + 4x - 8$ má trojnásobný kořen $c=2$. Napište kanonický rozklad tohoto polynomu.

Příklad 14:

Zjistěte, zda polynom $f(x) = x^3 - 2x + 4$ má vícenásobný kořen.

Příklad 15:

Jestliže víte, že polynom $f(x) = 16x^4 - 8x + 3$ má dvojnásobný kořen, vypočtěte tento kořen i ostatní kořeny.

Příklad 16:

Přesvěťte se, že polynom $f(x) = x^4 + 5x^3 + 6x^2 - 4x - 8$ splňuje podmínky pro to, aby měl trojnásobný kořen.

Příklad 17:

V polynomu $f(x) = x^3 - 5x^2 + 3x + a_0$ určete člen a_0 tak, aby měl polynom dvojnásobný kořen. Vypočítejte zbývající kořen.

Příklad 18:

Dokažte, že polynom $f(x) = x^n + a$, $a \neq 0$ nemá vícenásobný kořen.

Příklad 19:

Určete Taylorův rozvoj polynomu $f(x)$ o středu c , je-li dáno

- a) $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$, $c = -1$,
- b) $f(x) = x^5$, $c = 1$,
- c) $f(x) = x^4 + 2ix^3 - (1+i)x^2 - 3x + (7+i)$, $c = -i$,
- d) $f(x) = x^4 - ax^3 + a^2x^2 + a^3x + a^4$, $c = a$.
- e) $f(x) = 3x^5 + 4x^3 + 5x^2 + x - 1$, $c = -1$

Příklad 20:

Určete hodnotu polynomu a všech jeho derivací v daném bodě c , je-li dáno

- a) $f(x) = x^5 - 4x^3 + 6x^2 - 8x + 10$, $c = 2$,
- b) $f(x) = x^4 - 3ix^3 - 4x^2 + 5ix - 1$, $c = 1+2i$.
- c) $f(x) = 3x^5 + 4x^3 + 5x^2 + x - 1$, $c = -1$

Příklad 21:

Pomocí Hornerova schematu dané zlomky

$$a) \frac{x^3 - x + 1}{(x - 2)^5} \quad a \quad b) \frac{x^4 - 2x^2 + 3}{(x + 1)^5}$$

vyjádřete jako součty tvaru $\frac{c_k}{(x - c)^k}$, kde $k \in \mathbb{N}_0$, c je číslo (v našem případě buď 2 nebo -1) a c_k je vhodný koeficient, který se má vypočítat.

Příklad 22:

V polynomu $f(x) \in \mathbb{Q}[x]$ určete absolutní člen b tak, aby polynom $f(x)$ měl k -násobný kořen a určete zbývající kořen je-li

- a) $f(x) = x^3 - 3x + b$, $k=2$,
- b) $f(x) = x^4 - 10x^3 + 36x^2 - 54x + b$, $k=3$.

Příklad 23:

Určete polynom třetího stupně, jehož kořeny jsou o 5 menší než kořeny polynomu $f(x) = x^3 - 15x^2 + 71x - 105$. Určete kořeny nového i původního polynomu.

Příklad 24:

Určete polynom třetího stupně, který má kořeny $c_1 = 2$, $c_2 = 2+i$, přičemž je tento polynom z $\mathbb{R}[x]$.

Příklad 25:

Nechť je dán polynom $f(x) = x^6 + 12x^5 + 60x^4 + 160x^3 + 240x^2 + 192x + 63$. Rozviňte ho podle klesajících mocnin $(x+2)$. Dovedete potom určit alespoň dva kořeny polynomu $f(x)$?

Příklad 26:

Najděte racionální kořeny polynomů

- a) $f(x) = x^3 - 6x^2 + 11x - 6$,
- b) $f(x) = 6x^4 + 19x^3 - 7x^2 - 26x + 12$,
- c) $f(x) = 2x^3 + 3x^2 + 6x - 6$,
- d) $f(x) = 10x^4 - 13x^3 + 15x^2 - 18x - 24$,
- e) $f(x) = x^3 + 3x^2 - 4x - 12$.

Příklad 27:

Určete v substituci $x = y+k$ pro polynom $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{R}[x]$ číslo $k \in \mathbb{R}$ tak, aby polynom $f(y+k)$ měl koeficient u y^{n-1} roven nule.

Příklad 28:

Odstraňte vícenásobné kořeny daného polynomu $f(x) \in \mathbb{Q}[x]$ a výsledek využijte k nalezení rozkladu polynomu $f(x)$ v součin ireducibilních polynomů, jestliže

- a) $f(x) = x^5 + 2x^4 - 8x^3 - 16x^2 + 16x + 32$,
- b) $f(x) = x^7 + 3x^6 - 6x^5 - 14x^4 + 21x^3 + 15x^2 - 32x + 12$,
- c) $f(x) = 4x^5 + 20x^4 + 25x^3 - 10x^2 - 20x + 8$,
- d) $f(x) = x^5 - 6x^4 + 16x^3 - 24x^2 + 20x - 8$.

Příklad 29:

Zjistěte, zda polynomy $f(x) = x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4 \in \mathbb{Q}[x]$ a $g(x) = x^7 + x^4 + x^3 + \bar{2} \in \mathbb{Z}_3[x]$ mají vícenásobné kořeny.

Příklad 30:

Co lze říci o počtu reálných kořenů polynomu $f(x) \in R[x]$ stupně n, víme-li, že

- a) $n = 9$ a $f(x)$ má trojnásobný kořen $c = 2 + i\sqrt{3}$,
- b) $n = 10$ a $f(x)$ má jednoduché kořeny $c_1 = 2+i$, $c_2 = 1-i$ a dvojnásobný kořen $c_3 = \bar{\sqrt{2}} + 4i$.

Příklad 31:

Dokažte následující zobecnění věty 3.11:

Nechť imaginární číslo c je k-násobným kořenem polynomu $f(x) \in R[x]$. Pak i komplexně sdružené číslo \bar{c} je k-násobným kořenem polynomu $f(x)$.

Příklad 32:

Určete koeficienty polynomu $f(y)$, kde $y = x+3$, $f(x) = x^4 + x^3 + 1$.

Příklad 33:

Určete a tak, aby polynom $f(x) = x^5 - ax^2 - ax + 1$ měl číslo (-1) za kořen násobnosti alespoň 2.

Příklad 34:

Dokažte, že polynom $f(x) = x^n + ax^{n-m} + b$, ($n \geq m > 0$) nemůže mít kořen různý od nuly větší násobnosti než 2.

Příklad 35:

Najděte polynom, který má tytéž kořeny jako polynom $f(x) = x^4 - 6x^2 - 8x - 3$, ale samé jednoduché.

Příklad 36:

Tvoří kořeny polynomu $f(x) = 125x^3 - 350x^2 + 280x - 64$ geometrickou posloupnost?