Kořeny polynomů

Nechť $(R,+,\cdot)$ je komutativní okruh. Nechť $f \in R[x]$ je polynom, přičemž

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

kde $n \in \mathbb{N} \cup \{0\}$ a $a_0, a_1, \ldots, a_{n-1}, a_n \in R$, a nechť $c \in R$ je libovolný prvek. Pak prvek

$$f(c) = a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0$$

ležící množině R se nazývá **hodnota polynomu f v prvku** c. Je-li přitom splněno $f(c) = 0$, pak prvek c se nazývá **kořen** polynomu f.

Tvrzení. Je-li $(R,+,\cdot)$ komutativní okruh, pak pro libovolné dva polynomy $f, g \in R[x]$ a pro libovolný prvek $c \in R$ platí

$$(f+g)(c) = f(c) + g(c) \quad \text{a} \quad (f\cdot g)(c) = f(c)\cdot g(c).$$

Důkaz. První rovnost je zřejmá. Ověříme druhou rovnost. Nechť tedy $f = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ a nechť $g = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$. Potom ovšem máme $f\cdot g = h_{m+n}x^{m+n} + h_{m+n-1}x^{m+n-1} + \cdots + h_1 x + h_0$, kde pro každé $k \in \{0, 1, \ldots, m+n-1, m+n\}$ je $h_k = \sum_{i=0}^{k} a_i b_{k-i}$. Takže

$$(f\cdot g)(c) = h_{m+n}c^{m+n} + h_{m+n-1}c^{m+n-1} + \cdots + h_1 c + h_0,$$

kde $h_0, h_1, \ldots, h_{m+n-1}, h_{m+n}$ jsou prvky z R uvedeného tvaru. Na druhé straně

$$\begin{aligned} f(c)\cdot g(c) &= (a_m c^m + a_{m-1}c^{m-1} + \cdots + a_1 c + a_0)\cdot \\ &\qquad\qquad (b_n c^n + b_{n-1}c^{n-1} + \cdots + b_1 c + b_0) \\ &= \sum_{k=0}^{m+n}\sum_{i=0}^{k} a_i c^i \cdot b_{k-i}c^{k-i} = \sum_{k=0}^{m+n}\Big(\sum_{i=0}^{k} a_i b_{k-i}\Big)c^k \\ &= h_{m+n}c^{m+n} + h_{m+n-1}c^{m+n-1} + \cdots + h_1 c + h_0, \end{aligned}$$

kde $h_0, h_1, \ldots, h_{m+n-1}, h_{m+n}$ jsou tytéž prvky z R jako výše.

Důsledek. Nechť $(R, +, \cdot)$ je komutativní okruh a nechť $f \in R[x]$ je polynom. Pak prvek $c \in R$ je kořenem polynomu f právě tehdy, když $(x - c) \mid f$.

Důkaz. Nechť nejprve $c \in R$ je kořenem polynomu f, takže $f(c) = 0$. Podle věty o dělení polynomů se zbytkem existují polynomy $q, r \in R[x]$ takové, že $f = (x - c)\cdot q + r$, přičemž $\mathrm{st}(r) < 1$, takže r je konstantní polynom. Úpravou dostáváme, že $r = f - (x - c)\cdot q$, odkud s využitím předchozího tvrzení vyplývá, že $r = r(c) = f(c) - (c - c)\cdot q(c) = 0$. To ale znamená, že $f = (x - c)\cdot q$, čili $(x - c) \mid f$.

Nechť naopak $(x - c) \mid f$. Pak ovšem $f = (x - c)\cdot h$ pro jistý polynom $h \in R[x]$, odkud podle předchozího tvrzení plyne, že $f(c) = (c - c)\cdot h(c) = 0$. Je tedy c kořenem polynomu f.

Nechť znovu $(R, +, \cdot)$ je komutativní okruh, nechť $f \in R[x]$ je nenulový polynom a nechť $c \in R$ je kořen polynomu f. Nechť dále k je přirozené číslo. Pak řekneme, že c je kořen polynomu f **násobnosti** k, jestliže $(x - c)^k \mid f$, avšak $(x - c)^{k+1} \nmid f$.

Poznamenejme, že pro každý kořen $c \in R$ nenulového polynomu f takové přirozené číslo k existuje, neboť podle předchozího důsledku v takovém případě přinejmenším $(x - c) \mid f$, přičemž současně podle věty o dělení polynomů se zbytkem pro každé přirozené číslo $\ell > \mathrm{st}(f)$ máme $(x - c)^\ell \nmid f$. Skutečně tomu tak je, neboť $(x - c)^\ell$ je pak polynom stupně ℓ s vedoucím koeficientem 1, takže pokud $\ell > \mathrm{st}(f)$, je při dělení polynomu f polynomem $(x - c)^\ell$ polynom f sám zbytkem po tomto dělení. Je tedy touto definicí opravdu pro každý kořen $c \in R$ nenulového polynomu $f \in R[x]$ stanovena jeho násobnost k, což je konečné přirozené číslo.

Věta. Nechť $(R, +, \cdot)$ je obor integrity a nechť $f \in R[x]$ je nenulový polynom stupně $n = \mathrm{st}(f)$, $n \geq 0$. Pak polynom f má jen konečný počet kořenů, a počítáme-li přitom každý kořen tolikrát, kolik je jeho násobnost, platí, že polynom f má nejvýše n kořenů.

Důkaz. Počítejme každý kořen polynomu f tolikrát, kolik je jeho násobnost. Připusťme, že by při tomto pohledu měl polynom f více než n kořenů. Pak bychom mohli vybrat ℓ vzájemně různých kořenů $c_1, \ldots, c_\ell$ polynomu f s násobnostmi $k_1, \ldots, k_\ell$ tak, aby bylo $k_1 + \cdots + k_\ell > n$. Pak bychom podle definice násobnosti kořenů měli $(x - c_1)^{k_1} \mid f, \ldots, (x - c_\ell)^{k_\ell} \mid f$. Lze ukázat, že odtud plyne $(x - c_1)^{k_1} \cdot \ldots \cdot (x - c_\ell)^{k_\ell} \mid f$. Je-li $(R, +, \cdot)$ těleso, pak tato skutečnost plyne přímo z faktu, že potom okruh polynomů $(R[x], +, \cdot)$ je okruhem s jednoznačným rozkladem. Je-li $(R, +, \cdot)$ pouze obor integrity, potom lze důkaz této skutečnosti provést indukcí vzhledem k číslu $k_1 + \cdots + k_\ell$. To ale znamená, že pak $f = (x - c_1)^{k_1} \cdot \ldots \cdot (x - c_\ell)^{k_\ell} \cdot w$ pro jistý nenulový polynom $w \in R[x]$. To ale není možné, neboť $(x - c_1)^{k_1} \cdot \ldots \cdot (x - c_\ell)^{k_\ell}$ je polynom stupně $k_1 + \cdots + k_\ell$ s vedoucím koeficientem 1, takže bychom pak měli $n = \mathrm{st}(f) = k_1 + \cdots + k_\ell + \mathrm{st}(w) \geq k_1 + \cdots + k_\ell$, neboť $\mathrm{st}(w) \geq 0$. To odporuje předpokladu, že $k_1 + \cdots + k_\ell > n$. Tím je dokázáno tvrzení věty.

Nechť $(R, +, \cdot)$ je komutativní okruh a nechť $f \in R[x]$ je polynom. Definujeme zobrazení

$$\wp_f : R \to R \quad \text{vztahem} \quad (\forall c \in R)(\wp_f(c) = f(c)).$$

Zobrazení $\wp_f$ se nazývá **polynomická funkce** určená polynomem f.

Důsledek. Nechť $(R, +, \cdot)$ je nekonečný obor integrity. Pak pro libovolné dva polynomy $f, g \in R[x]$ platí

$$f = g \iff \wp_f = \wp_g.$$

Důkaz. Je-li $f = g$, pak ovšem $\wp_f = \wp_g$. Předpokládejme naopak, že $\wp_f = \wp_g$, takže pro každé $c \in R$ platí $f(c) = g(c)$. Uvažme polynom $f - g$. Uvedený předpoklad pak znamená, že pro každé $c \in R$ máme $(f - g)(c) = f(c) - g(c) = 0$, takže polynom $f - g$ má nekonečně mnoho kořenů, neboť jsou jimi všechny prvky z R. Podle předchozí věty pak ale $f - g$ musí být nulový polynom, takže $f = g$.

Bez předpokladu nekonečnosti oboru integrity $(R, +, \cdot)$ předchozí důsledek neplatí. Například pro konečné těleso $(\mathbb{Z}_2, +, \cdot)$, píšeme-li $\mathbb{Z}_2 = \{0, 1\}$, nulový polynom a polynom $x^2 + x$ určují tutéž polynomickou funkci.

Buď dále $(R, +, \cdot)$ těleso. Pak $(R, +, \cdot)$ se nazývá **algebraicky uzavřené** těleso, jestliže každý nekonstantní polynom z $R[x]$ má alespoň jeden kořen v R.

Věta. Pro libovolné těleso $(R, +, \cdot)$ jsou následující podmínky ekvivalentní:

- $(R, +, \cdot)$ je algebraicky uzavřené těleso.
- Ireducibilní polynomy v $R[x]$ jsou právě polynomy stupně 1.
- Každý nekonstantní polynom z $R[x]$ lze vyjádřit ve tvaru součinu polynomů stupně 1.
- Každý nenulový polynom z $R[x]$ stupně n má právě n kořenů v R, počítáme-li každý kořen tolikrát, kolik je jeho násobnost.

Důkaz. Fakt, že první z uvedených podmínek má za následek druhou, plyne z prvního důsledku této kapitoly. Skutečnosti, že ze druhé podmínky plyne třetí, ze třetí podmínky plyne čtvrtá, a ze čtvrté podmínky plyne zase první, jsou zřejmé.

Následující fakt, který zformulujeme bez důkazu, bývá tradičně označován jako **základní věta algebry**.

Věta. Těleso $(\mathbb{C}, +, \cdot)$ všech komplexních čísel je algebraicky uzavřené.

Základní věta algebry jinými slovy říká, že ireducibilními polynomy v $\mathbb{C}[x]$ jsou právě polynomy stupně 1.

Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 jsou **kvadratické** a polynomy stupně 3 se nazývají **kubické**.

Těleso $(\mathbb{R}, +, \cdot)$ všech reálných čísel není algebraicky uzavřené, jak plyne z dále uvedené věty. K jejímu důkazu potřebujeme následující poznatek:

Tvrzení. Je-li $f \in \mathbb{R}[x]$ libovolný polynom a je-li $c \in \mathbb{C}$ kořen polynomu f, potom také číslo $\overline{c}$ komplexně sdružené k c je kořenem polynomu f.

Důkaz. Je-li f konstantní polynom nebo je-li $c \in \mathbb{R}$, pak není co dokazovat. Předpokládejme tedy dále, že polynom f je nekonstantní a že $c \in \mathbb{C} - \mathbb{R}$. Nechť

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

kde $n \in \mathbb{N}$ a $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{R}$. Poněvadž c je kořen polynomu f, takže $f(c) = 0$, máme $a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0 = 0$. Přechodem ke komplexně sdruženým číslům odtud plyne, že $\overline{a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0} = 0$. Poněvadž přitom zobrazení $\overline{} : \mathbb{C} \to \mathbb{C}$ přiřazující každému komplexnímu číslu z číslo $\overline{z}$ k němu komplexně sdružené je homomorfismem tělesa $(\mathbb{C}, +, \cdot)$ na ně samotné a poněvadž $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{R}$, vychází odtud, že $a_n \overline{c}^{\,n} + a_{n-1} \overline{c}^{\,n-1} + \cdots + a_1 \overline{c} + a_0 = 0$. To ale znamená, že také $f(\overline{c}) = 0$, takže rovněž $\overline{c}$ je kořenem polynomu f.

Věta. Ireducibilními polynomy v $\mathbb{R}[x]$ jsou právě lineární polynomy a kvadratické polynomy nemající reálné kořeny.

Důkaz. Každý lineární polynom nad tělesem je ireducibilní. Rovněž každý kvadratický polynom nad tělesem všech reálných čísel nemající reálné kořeny je ireducibilní, neboť takový polynom nelze získat jako součin dvou lineárních polynomů s reálnými koeficienty.

Nechť naopak $f \in \mathbb{R}[x]$ je ireducibilní polynom nad $\mathbb{R}$. Pak f je nekonstantní polynom a podle základní věty algebry tedy má kořen $c \in \mathbb{C}$, takže $f(c) = 0$. Jestliže $c \in \mathbb{R}$, pak podle prvního důsledku v této kapitole máme $(x-c) \mid f$, takže $f = (x-c)\cdot h$ pro jistý nenulový polynom $h \in \mathbb{R}[x]$. Poněvadž ale f je ireducibilní polynom nad $\mathbb{R}$, musí h být konstantní polynom, takže potom polynom f sám je lineární. Jestliže ovšem $c \in \mathbb{C}-\mathbb{R}$, pak uvažme číslo $\overline{c}$ komplexně sdružené k c. Potom jistě $c \neq \overline{c}$. Z předchozího tvrzení víme, že pak také $\overline{c}$ je kořenem polynomu f, takže $f(\overline{c}) = 0$. Protože $f \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$, opět podle prvního důsledku v této kapitole máme $(x-c) \mid f$ a také $(x-\overline{c}) \mid f$. Poněvadž $c \neq \overline{c}$, podobně jako v důkazu první věty této kapitoly odtud plyne, že $(x-c)\cdot(x-\overline{c}) \mid f$. Ovšem $(x-c)\cdot(x-\overline{c}) = x^2 - (c+\overline{c})x + c\overline{c}$, kde $c+\overline{c}, c\overline{c} \in \mathbb{R}$, takže $(x-c)\cdot(x-\overline{c})$ je kvadratický polynom z $\mathbb{R}[x]$ nemající reálné kořeny. Protože přitom $(x-c)\cdot(x-\overline{c}) \mid f$, existuje nenulový polynom $t \in \mathbb{R}[x]$ takový, že $f = (x-c)\cdot(x-\overline{c})\cdot t$. Poněvadž ale f je ireducibilní polynom nad $\mathbb{R}$, musí t být konstantní polynom. To ukazuje, že tentokrát je f kvadratický polynom bez reálných kořenů.