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 $a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0 \in R$ se nazývá **hodnota polynomu f v prvku** c a označuje se symbolem $f(c)$. Je-li přitom splněno $f(c) = 0$, pak prvek c se nazývá **kořen** polynomu f.

Bezprostředně z této definice, z definic součtu a součinu polynomů a z předpokladu, že $(R, +, \cdot)$ je komutativní okruh, plyne následující fakt.

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

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

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 r je konstantní polynom. Takže máme $r = f - (x - c) \cdot q$, odkud podle předchozího tvrzení dostáváme, 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 $(R, +, \cdot)$ 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 pak přinejmenším $(x-c) \mid f$ a současně podle věty o dělení polynomů se zbytkem pro každé přirozené číslo $\ell > \mathrm{st}(f)$ máme $(x-c)^\ell \nmid f$. Skutečně $(x-c)^\ell$ 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 $n = \mathrm{st}(f) = k_1 + \cdots + k_\ell + \mathrm{st}(w) \geq k_1 + \cdots + k_\ell$, což odporuje předpokladu, že $k_1 + \cdots + k_\ell > n$. To dokazuje 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 $f(c) = g(c)$. To 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.

Na druhé straně těleso $(\mathbb{R}, +, \cdot)$ všech reálných čísel není algebraicky uzavřené. Snadno se ukáže, že ireducibilními polynomy v $\mathbb{R}[x]$ jsou právě lineární polynomy a kvadratické polynomy se záporným diskriminantem.