Vlastnosti polynomů

Buď $(R, +, \cdot)$ komutativní okruh. Pak $(R[x], +, \cdot)$ je také komutativní okruh. Řekneme, že polynom $f \in R[x]$ **dělí** polynom $g \in R[x]$, jestliže existuje polynom $w \in R[x]$ takový, že $g = f{\cdot}w$. Pak rovněž říkáme, že polynom f je **dělitel** polynomu g, a píšeme $f \mid g$. Následuje věta o dělení polynomů se zbytkem.

Věta. Nechť $(R, +, \cdot)$ je komutativní okruh, nechť $f, g \in R[x]$ jsou dva polynomy splňující $g \neq 0$ a nechť vedoucí koeficient polynomu g je jednotka okruhu $(R, +, \cdot)$. Pak existují polynomy $q, r \in R[x]$ takové, že platí

$$f = g{\cdot}q + r, \quad \mathrm{st}(r) < \mathrm{st}(g).$$

Přitom tyto polynomy q, r jsou určeny jednoznačně.

Poznámka. Polynom q se potom nazývá **podíl** a polynom r **zbytek** po dělení polynomu f polynomem g.

Důkaz. Dokážeme nejprve existenci potřebných polynomů q, r. Je-li $\mathrm{st}(f) < \mathrm{st}(g)$, pak můžeme vzít $q = 0$ a $r = f$. Předpokládejme tedy dále, že $\mathrm{st}(f) \geq \mathrm{st}(g)$. Položme $n = \mathrm{st}(f)$ a $k = \mathrm{st}(g)$. Pak tedy máme $n \geq k \geq 0$. Budeme postupovat indukcí vzhledem k n. Je-li $n = 0$, pak $k = 0$, čili g je nenulový konstantní polynom, který viděn jako prvek okruhu $(R, +, \cdot)$ je podle předpokladu v tomto okruhu jednotkou. Existuje zde tedy k němu prvek inverzní g^{-1}, který chápán zase jako konstantní polynom v $R[x]$ je inverzním prvkem ke g v okruhu $(R[x], +, \cdot)$. Pak můžeme položit $q = g^{-1}{\cdot}f$ a $r = 0$. Nechť tedy dále $n \geq 1$. Podle indukčního předpokladu pak požadované polynomy z tvrzení věty existují, bereme-li místo f libovolné polynomy stupně menšího než n. Nechť f_n, resp. g_k jsou vedoucí koeficienty polynomů f, resp g. Pak g_k je podle předpokladu jednotka okruhu $(R, +, \cdot)$, takže existuje k ní inverzní prvek g_k^{-1}. Uvažme polynom

$p = (f_n g_k^{-1}) x^{n-k} \cdot g$. Tento polynom p je stupně n a má vedoucí koeficient roven f_n. Vezměme nyní polynom $h = f - p$. Pak polynom h je stupně menšího než n. Podle zmíněného indukčního předpokladu tedy existují polynomy $q, r \in R[x]$ takové, že $h = g \cdot q + r$ a $\mathrm{st}(r) < \mathrm{st}(g)$. Čili $f - p = g \cdot q + r$, odkud plyne $f = p + g \cdot q + r$. Podle definice polynomu p odtud plyne $f = g \cdot (f_n g_k^{-1} x^{n-k} + q) + r$, což dokazuje existenci polynomů požadovaných v tvrzení věty také pro polynom f.

Dokážeme dále jednoznačnost polynomů q, r požadovaných v tvrzení věty. Nechť tedy $q, q', r, r' \in R[x]$ jsou takové polynomy, že platí $f = g \cdot q + r$ a také $f = g \cdot q' + r'$, přičemž $\mathrm{st}(r) < \mathrm{st}(g)$ a také $\mathrm{st}(r') < \mathrm{st}(g)$. To znamená, že pak máme $g \cdot q + r = g \cdot q' + r'$, takže dostáváme $g \cdot (q - q') = r' - r$. Jestliže $q \neq q'$, takže $q - q' \neq 0$, položme $\ell = \mathrm{st}(q - q')$, a kromě toho opět také $k = \mathrm{st}(g)$. Nechť g_k, resp. $\overline{q}_\ell$ jsou vedoucí koeficienty polynomů g, resp. $q - q'$. Poněvadž $\overline{q}_\ell \neq 0$ a g_k je podle předpokladu jednotka okruhu $(R, +, \cdot)$, plyne odtud, že také $g_k \overline{q}_\ell \neq 0$. To ale znamená, že $g \cdot (q - q')$ je polynom stupně $k + \ell$ s vedoucím koeficientem $g_k \overline{q}_\ell$. Na druhé straně ovšem $\mathrm{st}(r' - r) \leq \max\{\mathrm{st}(r), \mathrm{st}(r')\} < \mathrm{st}(g)$, čili $\mathrm{st}(r' - r) < k$. Ovšem $k \leq k + \ell$, neboť $\ell \geq 0$, což znamená, že $\mathrm{st}(r' - r) < \mathrm{st}(g \cdot (q - q'))$. To je ale ve sporu s tím, že $g \cdot (q - q') = r' - r$. Nutně tedy musí být $q = q'$, takže $q - q' = 0$, odkud plyne, že také $r' - r = 0$, čili $r = r'$.

Buď $(R, +, \cdot)$ komutativní okruh. Polynom $h \in R[x]$ se nazývá **společný dělitel** polynomů $f, g \in R[x]$, jestliže $h \mid f$ a také $h \mid g$. Polynom $s \in R[x]$ se nazývá **největší společný dělitel** polynomů $f, g \in R[x]$, jestliže $s \mid f$ a $s \mid g$ a navíc je splněna podmínka, že pro každý polynom $w \in R[x]$ takový, že $w \mid f$ a $w \mid g$, platí, že $w \mid s$. Odnikud ale neplyne, že největší společný dělitel daných dvou polynomů $f, g \in R[x]$ musí vždy existovat, ani že je snad určen jednoznačně. Uvedeme, za jakých předpokladů se lze k těmto požadavkům přiblížit.

Tvrzení. Buď $(R,+,\cdot)$ obor integrity. Nechť $f,g \in R[x]$ jsou libovolné dva polynomy takové, že existuje jejich největší společný dělitel $s \in R[x]$. Pak největší společní dělitelé polynomů f,g jsou právě všechny polynomy tvaru $a\cdot s$, kde $a \in R[x]$ je konstantní polynom odpovídající jednotce okruhu $(R,+,\cdot)$.

Poznámka. To znamená, že je-li $(R,+,\cdot)$ obor integrity, pak největší společný dělitel dvou polynomů z $R[x]$, pokud existuje, je určen jednoznačně až na násobek jednotkou z okruhu $(R,+,\cdot)$.

Důkaz. Nechť $t \in R[x]$ je libovolný největší společný dělitel polynomů f,g. Pak z definice plyne, že $s \mid t$ i $t \mid s$. Existují tedy polynomy $a,b \in R[x]$ takové, že $t = a\cdot s$ a $s = b\cdot t$. To znamená, že například $t = a\cdot b\cdot t$. Odtud podle poznatků o stupních polynomů z minulé kapitoly plyne, že $\mathrm{st}(t) = \mathrm{st}(a\cdot b\cdot t) = \mathrm{st}(a\cdot b)+\mathrm{st}(t)$. Je-li $\mathrm{st}(t) = -\infty$, tedy je-li t nulový polynom, pak také s je nulový polynom, takže máme kupříkladu $t = 1\cdot s$. Je-li $\mathrm{st}(t) \geq 0$, pak z předchozí rovnosti se stupni polynomů plyne, že $\mathrm{st}(a\cdot b) = 0$, takže $\mathrm{st}(a) + \mathrm{st}(b) = 0$, a tedy $\mathrm{st}(a) = \mathrm{st}(b) = 0$. Jsou tedy a,b konstantní polynomy, a poněvadž $1\cdot t = t = a\cdot b\cdot t$ a také $(R[x],+,\cdot)$ je obor integrity, plyne odtud krácením, že $1 = a\cdot b$, takže a,b jsou jednotky okruhu $(R,+,\cdot)$.

Naopak je-li $t = a\cdot s$, kde a je jednotka okruhu $(R,+,\cdot)$, pak $s \mid t$, a dále máme $s = a^{-1}\cdot t$, takže rovněž $t \mid s$. To má za následek, že z toho, že $s \mid f$ a $s \mid g$, plyne také, že $t \mid f$ a $t \mid g$. Je-li dále $w \in R[x]$ polynom takový, že $w \mid f$ a $w \mid g$, pak $w \mid s$, a poněvadž $s \mid t$, plyne odtud, že $w \mid t$. Je tedy t rovněž největší společný dělitel polynomů f,g.

Věta. Buď $(R,+,\cdot)$ těleso. Pak pro libovolné dva polynomy $f,g \in R[x]$ existuje jejich největší společný dělitel v $R[x]$.

Důkaz. Jsou-li oba polynomy f,g nulové, je jejich největším společným dělitelem nulový polynom. Je-li právě jeden z polynomů f,g nulový, pak jejich největším společným dělitelem je druhý z těchto polynomů, tedy ten polynom, který je nenulový. Předpokládejme tedy dále, že oba polynomy f, g jsou nenulové. Pak mají tyto polynomy nenulové vedoucí koeficienty, a ty jsou přitom jednotkami v $(R, +, \cdot)$, neboť jde o těleso. Pak se k nalezení největšího společného dělitele polynomů f, g použije podobně jako v kapitole o celých číslech následující **Euklidův algoritmus**. Provádí se postupně dělení se zbytkem, tentokrát podle první věty této kapitoly. To znamená, že se hledají polynomy $q_0, q_1, \ldots, q_n, q_{n+1} \in R[x]$ a nenulové polynomy $r_0, r_1, \ldots, r_n \in R[x]$ takové, že platí:

$$\begin{aligned}
f &= g \cdot q_0 + r_0, \quad \mathrm{st}(r_0) < \mathrm{st}(g), \\
g &= r_0 \cdot q_1 + r_1, \quad \mathrm{st}(r_1) < \mathrm{st}(r_0), \\
r_0 &= r_1 \cdot q_2 + r_2, \quad \mathrm{st}(r_2) < \mathrm{st}(r_1), \\
r_1 &= r_2 \cdot q_3 + r_3, \quad \mathrm{st}(r_3) < \mathrm{st}(r_2), \\
&\ldots \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n, \quad \mathrm{st}(r_n) < \mathrm{st}(r_{n-1}), \\
r_{n-1} &= r_n \cdot q_{n+1}.
\end{aligned}$$

Poslední dělení je tedy vlastně tvaru $r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$, kde ale r_{n+1} je nulový polynom. Poněvadž $\mathrm{st}(g) > \mathrm{st}(r_0) > \mathrm{st}(r_1) > \mathrm{st}(r_2) > \ldots$, musí tato posloupnost dělení opravdu skončit uvedeným způsobem, což znamená, že buďto již r_0 je nulový polynom pokud $g \mid f$, anebo skutečně existuje $n \in \mathbb{N} \cup \{0\}$ takové, že r_{n+1} je nulový polynom. V situaci, kdy r_0 je nulový polynom, položme $n = -1$ a označme ještě $r_{-1} = g$. Pak stejnou argumentací jako v kapitole o celých číslech dospějeme ke zjištění, že je to polynom r_n, který je největším společným dělitelem polynomů f, g.

Buď $(R, +, \cdot)$ komutativní okruh. Je-li $f \in R[x]$ nenulový polynom, jehož vedoucí koeficient je jednotkovým prvkem okruhu $(R, +, \cdot)$, čili je roven 1, říkáme, že f je **normovaný polynom**.

Z předchozí věty a z tvrzení jemu předcházejícího plyne následující fakt.

Důsledek. Buď $(R, +, \cdot)$ těleso. Pak pro libovolné dva polynomy $f, g \in R[x]$, z nichž alespoň jeden je nenulový, existuje normovaný polynom v $R[x]$, který je jejich největším společným dělitelem, a tento polynom je jediný.

V situaci z právě uvedeného důsledku značíme normovaný největší společný dělitel polynomů f, g symbolem (f, g). Navíc pro nulový polynom 0 klademe $(0, 0) = 0$.

Z předchozí věty o existenci největšího společného dělitele pro libovolné dva polynomy nad daným tělesem a z jejího důkazu prostřednictvím Euklidova algoritmu plyne podobně jako v kapitole o celých číslech následující **Bezoutova rovnost**:

Věta. Buď $(R, +, \cdot)$ těleso. Pak pro libovolné dva polynomy $f, g \in R[x]$ existují takové dva polynomy $u, v \in R[x]$, že platí rovnost $(f, g) = f \cdot u + g \cdot v$.

Poznámka. Jsou-li oba polynomy f, g nekonstantní, pak lze zvolit polynomy u, v tak, že $\mathrm{st}(u) < \mathrm{st}(g)$ a $\mathrm{st}(v) < \mathrm{st}(f)$.

Důkaz. Tvrzení věty samo se odvodí z Euklidova algoritmu obdobnou argumentací jako v kapitole o celých číslech. Podrobnou analýzou stupňů polynomů vystupujících v těchto argumentech je možné obdržet také tvrzení uvedené v poznámce.

Buď $(R, +, \cdot)$ těleso. Pak polynomy $f, g \in R[x]$ se nazývají **nesoudělné**, jestliže $(f, g) = 1$.

Důsledek. Buď $(R, +, \cdot)$ těleso. Jestliže pro nějaké polynomy $f, g, h \in R[x]$ platí $f \mid g \cdot h$ a současně $(f, g) = 1$, pak odtud plyne, že $f \mid h$.

Důkaz. Postupujeme analogicky jako v kapitole o celých číslech. Jestliže tedy $(f, g) = 1$, pak podle předchozí věty existují polynomy $u, v \in R[x]$ takové, že $1 = f{\cdot}u + g{\cdot}v$. Vynásobením polynomem h odtud dostáváme $h = f{\cdot}h{\cdot}u + g{\cdot}h{\cdot}v$. Jestliže nyní $f \mid g{\cdot}h$, plyne odtud, že $f \mid h$.

Nechť $(R, +, \cdot)$ je komutativní okruh. Říkáme, že polynom $f \in R[x]$ je **ireducibilní nad** R, jestliže f není konstantní polynom a jestliže neexistují polynomy $g, h \in R[x]$, oba nikoliv konstantní polynomy, pro něž by platilo $f = g{\cdot}h$.

Poznamenejme, že je-li $(R, +, \cdot)$ těleso a jsou-li $f, g \in R[x]$ dva normované polynomy, které jsou ireducibilní nad R, pak buďto $f = g$, anebo $(f, g) = 1$.

Věta. Buď $(R, +, \cdot)$ těleso. Pak pro každý nenulový polynom $f \in R[x]$ existují číslo $k \in \mathbb{N} \cup \{0\}$, konstantní polynom $a \in R[x]$ a normované polynomy $p_1, p_2, \ldots, p_k \in R[x]$ ireducibilní nad R takové, že platí

$$f = a{\cdot}p_1{\cdot}p_2{\cdot} \ldots {\cdot}p_k.$$

Tento rozklad polynomu f je přitom jediný až na pořadí činitelů $p_1, p_2, \ldots, p_k$.

Poznámka. Tuto skutečnost označujeme slovy, že v případě, když $(R, +, \cdot)$ je těleso, okruh $(R[x], +, \cdot)$ je **okruhem s jednoznačným rozkladem**.

Důkaz. Existenci uvedeného rozkladu lze dokázat indukcí vzhledem ke stupni polynomu f podobně, jak byla dokázána- existence rozkladů přirozených čísel na součin prvočísel.

Jednoznačnost zmíněného rozkladu lze dokázat s využitím předchozího důsledku argumenty podobnými těm, jimiž byla dokázána jednoznačnost rozkladů přirozených čísel na součin prvočísel.