# Okruhy polynomů

Polynomy například s reálnými koeficienty si představujeme jako výrazy tvaru

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

kde $n \in \mathbb{N} \cup \{0\}$ a $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{R}$. Je ovšem možné si dále představovat, že takový polynom má rovněž koeficienty $a_{n+1}, a_{n+2}, \ldots$ u mocnin $x^{n+1}, x^{n+2}, \ldots$ a že všechny tyto další koeficienty jsou rovny nule. Můžeme tedy tento polynom vnímat jako směrem doleva nekonečný výraz, v němž je ale jen konečný počet nenulových koficientů. Poněvadž uvedený polynom je plně určen tím, jaké má koeficienty, můžeme místo něj uvažovat přímo jen posloupnost jeho koeficientů, tedy posloupnost

$$(a_0, a_1, \ldots, a_{n-1}, a_n, a_{n+1}, a_{n+2}, \ldots).$$

Tuto představu můžeme dále zobecnit tak, že místo reálných čísel budeme brát koeficienty z nějakého obecného pevně daného okruhu $(R, +, \cdot)$. To nás vede k následující definici toho, co je polynom.

Buď $(R, +, \cdot)$ okruh. **Polynom nad okruhem** $(R, +, \cdot)$ je libovolná nekonečná posloupnost

$$f = (f_0, f_1, f_2, \ldots),$$

kde $f_0, f_1, f_2, \ldots$ jsou prvky z $R$, taková, že pro všechny indexy $k \in \{0, 1, 2, \ldots\}$ s výjimkou jenom konečně mnoha indexů platí $f_k = 0$. Pak prvky $f_0, f_1, f_2 \ldots$ se nazývají **koeficienty** polynomu $f$. Množinu všech polynomů nad okruhem $(R, +, \cdot)$ označujeme symbolem $R[x]$.

Vrátíme-li se ještě jednou k počáteční představě polynomů jakožto výrazů a vzpomeneme-li si, jakým způsobem, jde-li o polynomy s reálnými koeficienty, se tyto výrazy sečítají a násobí, pak přímočarým zobecněním příslušných vzorců na případ polynomů s koeficienty z obecného okruhu $(R, +, \cdot)$ dostáváme následující definici sečítání a násobení v rámci množiny $R[x]$ všech polynomů nad $(R, +, \cdot)$. Tyto operace, aniž by hrozilo nebezpečí záměny, budeme rovněž značit symboly $+, \cdot$ .

Buď $(R, +, \cdot)$ libovolný okruh. Pak pro kterékoliv dva polynomy $f = (f_0, f_1, f_2, \dots)$ a $g = (g_0, g_1, g_2, \dots)$ z $R[x]$ definujeme součet $f + g$ těchto polynomů jakožto polynom

$$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \dots),$$

takže pro každý index $k \in \{0, 1, 2, \dots\}$ platí $(f + g)_k = f_k + g_k$, a dále definujeme součin $f \cdot g$ těchto polynomů jakožto polynom

$$f \cdot g = (h_0, h_1, h_2, \dots),$$

kde $h_0 = f_0 \cdot g_0$, $h_1 = f_0 \cdot g_1 + f_1 \cdot g_0$, $h_2 = f_0 \cdot g_2 + f_1 \cdot g_1 + f_2 \cdot g_0$, $\dots$ , takže pro každý index $k \in \{0, 1, 2, \dots\}$ platí

$$(f \cdot g)_k = h_k = f_0 \cdot g_k + f_1 \cdot g_{k-1} + \cdots + f_{k-1} \cdot g_1 + f_k \cdot g_0,$$

čili pro každé $k \in \{0, 1, 2, \dots\}$ je $(f \cdot g)_k = \sum_{i=0}^{k} f_i \cdot g_{k-i}$. Je jasné, že pak obě posloupnosti $f + g$ i $f \cdot g$ mají zase jen konečný počet nenulových prvků, čili jde opět o polynomy z $R[x]$.

**Tvrzení.** Buď $(R, +, \cdot)$ okruh. Potom také $(R[x], +, \cdot)$ je okruh. Je-li Je-li přitom okruh $(R, +, \cdot)$ komutativní, pak také okruh $(R[x], +, \cdot)$ je komutativní.

**Důkaz.** Ověření všech vlastností okruhu, případně komutativního okruhu pro $(R[x], +, \cdot)$ je rutinní záležitostí.

Je-li $(R, +, \cdot)$ okruh, pak okruh $(R[x], +, \cdot)$ se nazývá **okruh polynomů nad okruhem** $(R, +, \cdot)$.

Polynomy tvaru $(a, 0, 0, \dots, 0, \dots)$, kde $a \in R$, se nazývají **konstantní polynomy** okruhu $(R[x], +, \cdot)$. Přitom význačnou úlohu mezi nimi hrají **nulový polynom** $(0, 0, 0, \dots, 0, \dots)$, který je nulovým prvkem okruhu $(R[x], +, \cdot)$, a dále polynom $(1, 0, 0, \dots, 0, \dots)$, který je jednotkovým prvkem tohoto okruhu.

**Tvrzení.** Buď $(R, +, \cdot)$ okruh. Pak zobrazení $\mathsf{C} : R \to R[x]$ dané pro každé $a \in R$ předpisem

$$\mathsf{C}(a) = (a, 0, 0, \dots, 0, \dots)$$

je prostý homomorfismus okruhu $(R, +, \cdot)$ do okruhu $(R[x], +, \cdot)$.

**Důkaz** plyne ihned z definice operací v okruhu $(R[x], +, \cdot)$.

Z uvedeného tvrzení podle poznatků z předchozí kapitoly dále plyne, že množina všech konstantních polynomů okruhu $(R[x], +, \cdot)$ tvoří v tomto okruhu podokruh, který jakožto okruh je izomorfní okruhu $(R, +, \cdot)$. Z tohoto důvodu často přímo ztotožnujeme prvek $a \in R$ a jemu příslušný konstantní polynom $(a, 0, 0, \dots, 0, \dots)$, takže píšeme $a = (a, 0, 0, \dots, 0, \dots)$.

Buď $f = (f_0, f_1, f_2, \dots)$ nenulový polynom nad okruhem $(R, +, \cdot)$. Pak největší číslo $n \in \mathbb{N} \cup \{0\}$ takové, že $f_n \neq 0$, se nazývá **stupeň** polynomu $f$ a označuje se symbolem $\mathrm{st}(f)$. Prvek $f_n$ sám se pak nazývá **vedoucí koeficient** polynomu $f$. Zmíněné číslo $n$ vždy existuje, neboť polynom $f$ má podle definice pouze konečný počet nenulových koeficientů. Navíc pro nulový polynom $(0, 0, 0, \dots, 0, \dots)$ klademe jeho stupeň rovný $-\infty$, přičemž $-\infty < m$ pro všechna $m \in \mathbb{Z}$ a dále $k + \ell = -\infty$ kdykoliv $k, \ell \in \mathbb{Z} \cup \{-\infty\}$ jsou taková, že alespoň jedno z nich je rovno $-\infty$.

Chápeme-li symbol $x$ jako značku pro polynom stupně 1 tvaru $(0, 1, 0, 0, \dots, 0, \dots)$, pak zjišťujeme následující skutečnost.

**Tvrzení.** Buď $(R, +, \cdot)$ okruh. Pak pro každé $n \in \mathbb{N} \cup \{0\}$ a každý polynom $f = (f_0, f_1, \dots, f_{n-1}, f_n, 0, 0, \dots, 0, \dots)$ stupně $n$ z $R[x]$ platí rovnost

$$f = f_n \cdot x^n + f_{n-1} \cdot x^{n-1} + \dots + f_1 \cdot x + f_0,$$

kde koeficienty $f_0, f_1, \dots, f_{n-1}, f_n$ chápeme jako konstantní polynomy v $R[x]$ a operace $+, \cdot$ jsou operacemi okruhu $(R[x], +, \cdot)$.

**Důkaz.** Stačí si jenom uvědomit, že je-li $x$ polynom shora uvedeného tvaru, pak pro každé $k \in \mathbb{N}$ je $x^k$ polynom stupně $k$ tvaru $(0, 0, \dots, 0, 1, 0, 0, \dots)$, kde 1 leží na pozici s indexem $k$.

Vzhledem ke skutečnosti obsažené v tomto tvrzení budeme nadále polynom $f = (f_0, f_1, \dots, f_{n-1}, f_n, 0, 0, \dots, 0, \dots)$ zapisovat zpravidla ve tvaru $f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0$, tedy nikoliv jako posloupnost, ale jako jí odpovídající výraz ve smyslu uvedeném na začátku této kapitoly.

**Tvrzení.** Buď $(R, +, \cdot)$ okruh. Pak pro libovolné dva polynomy $f, g$ z $R[x]$ platí

$$\mathrm{st}(f + g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\} \quad \text{a} \quad \mathrm{st}(f \cdot g) \leq \mathrm{st}(f) + \mathrm{st}(g).$$

Je-li navíc $(R, +, \cdot)$ obor integrity, pak ve druhé nerovnosti platí vždy rovnost.

**Důkaz.** Uvedené nerovnosti ihned plynou z definic operací v okruhu $(R[x], +, \cdot)$. Je-li některý z polynomů $f, g$ nulový, pak součin $f \cdot g$ je nulový polynom a ve druhé nerovnosti platí rovnost podle výše uvedených pravidel počítání se symbolem $-\infty$. Je-li $(R, +, \cdot)$ obor integrity a jsou-li $f = f_m x^m + f_{m-1} x^{m-1} + \cdots + f_1 x + f_0$, resp. $g = g_n x^n + g_{n-1} x^{n-1} + \cdots + g_1 x + g_0$ nenulové polynomy stupňů $m$, resp. $n$, takže $f_m \neq 0 \neq g_n$, pak součin $f \cdot g$ je polynom stupně $m + n$, poněvadž jeho poslední nenulový koeficient je u mocniny $x^{m+n}$ a je roven $f_m \, g_n \neq 0$. Takže ve druhé nerovnosti platí zase rovnost.

**Důsledek.** Je-li $(R, +, \cdot)$ obor integrity, pak také $(R[x], +, \cdot)$ je obor integrity.

**Důsledek.** Je-li $(R, +, \cdot)$ obor integrity, potom jednotkami okruhu $(R[x], +, \cdot)$ jsou právě ty konstantní polynomy, které odpovídají jednotkám okruhu $(R, +, \cdot)$.