Polynomy jedné proměnné

Následující neformální popis je určen pro čtenáře, kteří nejsou aspoň základně seznámeni s pojmem *polynom v jedné proměnné.* Uvažujme pevně zvolený okruh $\mathcal{M}$ – například těleso racionálních čísel $\mathbb{Q} = (Q, +, \cdot)$, dále uvažujme pevnou proměnnou x. *Polynomem nad okruhem $\mathcal{M}$ v proměnné x* nazveme libovolnou nekonečnou posloupnost $p_0, p_1, \ldots$, kde $p_i \in M$ pro $i \in \mathbb{N}_0$ a platí, že pouze konečně mnoho prvků je různých od nuly okruhu $\mathcal{M}$. Speciálním polynomem je *nulový polynom o*, jenž je tvořen posloupností nul $0, 0, \ldots$ okruhu $\mathcal{M}$.

Označme $M[x]$ množinu všech polynomů nad okruhem $\mathcal{M}$ v proměnné x. Každý nenulový polynom nad $\mathcal{M}$ lze formalisovat buďto uspořádanou n-ticí

$$p = (p_0, p_1, p_2, \ldots, p_n), \text{ tak, že } p_i = 0 \text{ pro libovolné } i > n, \tag{1}$$

nebo jako součet členů s nenulovými koeficienty

$$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n. \tag{2}$$

V druhém případě evidentně nezáleží na uspořádání jednotlivých sčítanců, jejich jednoznačnost je dána mocninou proměnné x. Mezi oběma representacemi přirozeně existuje bijektivní zobrazení. Nulový polynom je označován buďto o (v první representaci), nebo 0 v druhé representaci.

Z předchozího plyne, že ke každému nenulovému polynomu existuje číslo n takové, že všechny jeho koeficienty počínající jsou počínaje tímto číslem nulové. Toto číslo se nazývá *stupeň polynomu.* Stupeň polynomu je zobrazení $\mathrm{st}\colon M[x] - \{o\} \to \mathbb{N}_0$. Mezi speciální polynomy patří *konstantní polynomy,* to jest polynomy řádu 0 – to jsou právě všechny nenulové prvky okruhu $\mathcal{M}$. Pro nulový polynom není stupeň definován. *Lineární polynomy* mají tvar $ax + b$, kvadratické $ax^2 + bx + c$, kubické $ax^3 + bx^2 + cx + d$ a tak dále.

Na množině polynomů $M[x]$ lze přirozeným způsobem zavést operace sčítání a násobení polynomů. Uvažujme polynomy $p = (p_0, \ldots, p_m)$ a $q = (q_0, \ldots, q_n)$, kde $p_m = \mathrm{st}\,(p)$, $q_n = \mathrm{st}\,(q)$. *Součet polynomů $p \oplus q$* lze definovat jako posloupnost

$$p_0 + q_0, p_1 + q_1, p_2 + q_2, \ldots \tag{3}$$

Je zřejmé, že součtem polynomů p, q je opět polynom, jeho stupeň je $\max(m, n)$. Sčítání je komutativní i asociativní, to plyne z vlastností operace + okruhu $\mathcal{M}$. Navíc se je operace $\oplus$ chová neutrálně vůči nulovému polynomu, $p \oplus o = o \oplus p = p$. Ke každému polynomu p lze navíc najít polynom opačný $-p = (-p_0, -p_1, \ldots, -p_m)$. Odtud plyne, že struktura $(M[x], \oplus, o)$ je *komutativní grupa. Součin polynomů $p \odot q$* lze definovat jako posloupnost $r_0, r_1 \ldots$, kde

$$r_k = \sum_{i+j=k} p_i \cdot q_j. \tag{4}$$

Posloupnost $r_0, r_1 \ldots$ má pouze konečně mnoho členů, poslední nenulový člen může být nejvýš r_{m+n}, to plyne ze vztahu (4) a z vlastností stupně polynomu. Součin dvou polynomů je tedy rovněž polynom. Struktura $(M[x], \odot)$ je pologrupa. Pokud má okruh $\mathcal{M}$ jedničku 1, pak se konstantní polynom (1) chová vůči násobení neutrálně. Je-li operace $\cdot$ okruhu $\mathcal{M}$ komutativní, pak je i násobení polynomů komutativní. Mezi $\oplus$ a $\odot$ platí *distributivní zákony*, dohromady lze konstatovat, že struktura $\mathcal{M}[x] = (M[x], \oplus, \odot, o)$ je okruh a nazývá se *okruh polynomů nad $\mathcal{M}$*. V dalším textu již nebudou rozlišovány operace v okruzích $\mathcal{M}$ a $\mathcal{M}[x]$ a budou shodně značeny + a $\cdot$, nemůže totiž dojít k jejich záměně. Je ale nutné uvědomit si, že se jedná o různé operace.

Násobení polynomů $p(x)$, $q(x)$ si lze díky distributivním zákonům jednoduše představit jako součet součinů polynomu s jedním členem,

$$p(x)q(x) = p_0 q(x) + p_1 x q(x) + p_2 x^2 q(x) + \cdots + p_m x^m q(x), \tag{5}$$

násobení mocninou x lze v datové representaci pomocí seznamů vyřešit velmi snadno. Rovněž násobení konstantním polynomem je velmi jednoduché.

Dělení se zbytkem

Speciální obory integrity, v nichž lze provádět *dělení se zbytkem* se nazývají *euklidovské okruhy.* V těchto strukturách lze nalézt největšího společného dělitele pomocí Euklidova algoritmu. Obor integrity $\mathcal{M} = (M, +, \cdot, 0, 1)$ se nazývá *euklidovský okruh*, pokud existuje *norma dělení* $\nu\colon M - \{0\} \to \mathbb{N}_0$ takové, že pro libovolné $a, b \in M$ existují $c, r \in M$ a platí

$$a = b \cdot c + r, \text{ přitom } r = 0, \text{ nebo } \nu(r) < \nu(b). \tag{6}$$

Například okruh celých čísel $\mathbb{Z}$ je euklidovský okruh. Normu dělení lze v tomto případě zvolit jako *absolutní hodnotu* celého čísla. Pokud je $\mathcal{M}$ těleso, pak je rovněž $\mathcal{M}[x]$ euklidovský okruh – norma dělení je v tomto případě *stupeň polynomu,* $\nu(p) = \mathrm{st}\,(p)$. V dalším textu budeme uvažovat okruh polynomů $\mathbb{Q}[x]$, jenž je podle předchozího euklidovským okruhem.

Dělení dvou polynomů se zbytkem lze v okruhu $\mathbb{Q}[x]$ vypočítat jednoduše. Mějme například polynomy $p(x) = x^3 + 5x^2 + 6$, $q(x) = x^2 + 3$. Chceme-li získat podíl $p(x)/q(x)$ a adekvátní zbytek po dělení, provedeme dělení následujícím způsobem.

$$\begin{aligned} (x^3{+}5x^2 + 6) \,:\, (x^2 + 3) &= x + 5 \\ 5x^2 - 3x + 6 & \\ -\,3x - 9 & \end{aligned} \tag{7}$$

Podíl je roven $x + 5$, zbytek po dělení je $-3x - 9$. Zvláštní význam má u polynomů dělení lineárním polynomem, nebo jeho libovolnou mocninou. Zbytek po dělení lineárním polynomem je konstantní. Dělení tímto polynomem má důležitý vztah k existenci kořenu daného polynomu.

Pro polynom $p(x) \in M[x]$ a číslo $m \in M$ definujeme *hodnotu polynomu* $p(x)$ *v bodě* m jako číslo $p(m) \in M$ přepisem

$$p(m) = p_0 + p_1 m + p_2 m^2 + \cdots + p_n m^n, \tag{8}$$

to jest proměnná x je ohodnocena číslem m a hodnota $p(m)$ je vyjádřena jako interpretace polynomu $p(x)$ při ohodnocení proměnné $\|x\| = m$. Číslo $m \in M$ pro které je hodnota polynomu nulová, to jest $p(m) = 0$, se nazývá *kořen polynomu* $p(x)$. Každý lineární polynom tvaru $(x - m)$ má kořen m neboť $p(m) = m - m = 0$.

Tvrzení. Je-li $\mathcal{M}$ těleso, pak je $m \in \mathcal{M}$ kořenem $p(x) \in \mathcal{M}[x]$, právě když $(x - m) \mid p(x)$.

Důkaz. Nejprve dokážeme „⇐“. Předpokládejme, že $(x - m) \mid p(x)$. To jest existuje polynom $q(x)$ stupně $\mathrm{st}\,(p(x)) - 1$ tak, že $p(x) = (x - m)q(x)$. Potom je ale $p(m) = 0 \cdot q(m) = 0$.

Obráceně, předpokládejme $p(m) = 0$ a $p(x) = q(x)(x - m) + r(x)$. Chceme ukázat, že $r(x) = 0$. Jelikož $p(m) = 0$, platí $0 = q(m)(m - m) + r(m)$, odtud $r(m) = 0$. Ale zbytek po dělení musí být buďto nulový, nebo musí $\mathrm{st}\, r(x) < \mathrm{st}\,(x - m) = 1$. Odtud $r(x) = 0$. □

Předchozí tvrzení se nazývá Bezoutova věta a dává jednoduché kritérium zda-li je daný prvek kořenem polynomu. Pokud platí $p(m) = 0$ a zároveň $q(m) = 0$ pro $q(x) = p(x)/(x - m)$, pak se m nazývá dvojnásobný kořen polynomu $p(x)$. Obecně, pokud pro $m \in \mathcal{M}$, $k \in \mathbb{N}$ a pro polynom $p(x) \in \mathcal{M}[x]$ platí

$$(x - m)^k \mid p(x) \,\wedge\, (x - m)^{k+1} \nmid p(x), \tag{9}$$

pak se m nazývá *k-násobný kořen polynomu* $p(x)$.

Předchozí vlastnosti lze využít ke stanovení polynomu s libovolnými kořeny. Stačí si uvědomit, že $(x - m)$ má kořen m. Chceme-li stanovit polynom $p(x)$ s kořeny $m_1, m_2, \ldots, m_k$, stačí vynásobit $(x - m_1)q(x)$, kde $q(x)$ je polynom s kořeny $m_2, \ldots, m_k$. Tento předpis přímo vede k rekursivnímu algoritmu stanovení hledaného polynomu $p(x)$.