Polynomy

Saša Kazda

Polynomy (mnohočleny) můžeme uvažovat nad různými množinami: $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_n$ a dalšími. Pokaždé se chovají trochu jinak, ale některé vlastnosti mají společné. V tomto povídání se budeme zabývat především polynomy nad $\mathbb{Q}, \mathbb{R}$ a $\mathbb{C}$.

Definice. *Buď R množina s definovanými operacemi sčítání a násobení*[12]. *Potom* polynom stupně n nad R *je výraz* $r_n x^n + r_{n-1}x^{n-1} + \cdots + r_0$, *kde* $r_n \neq 0$ a $r_0, \ldots, r_n \in R$.

K polynomům přidáme ještě nulový polynom, jehož stupeň se obvykle klade roven divným číslům jako -1 nebo $-\infty$. Násobení a sčítání polynomů definujeme „člen po členu“.

Všimni si, že polynom je zároveň něco algebraického ($(n+1)$-tice koeficientů $r_0, r_1, \ldots, r_n$) a zároveň funkce. Tento rozdíl se stírá v případě polynomů nad reálnými čísly, kde každá polynomiální funkce odpovídá právě jedné sadě koeficientů. Ovšem třeba nad $\mathbb{Z}_2$ máme nenulové polynomy odpovídající nulovým funkcím, například $x^2 + x$.

Problém. Buď p polynom nad $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$. Je možné, aby $\forall x, p(x) = 0$, ale p nebyl nulový?

Definice. *Řekneme, že polynom p je* dělitelem *polynomu q, píšeme $p|q$, pokud existuje polynom r takový, že $p \cdot r = q$.*

Ze školy možná znáte algoritmus pro dělení polynomů. S trochou šikovnosti z něj lze odvodit, že pokud r je polynom nad $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$, který není dělitelný žádným polynomem stupně vyššího než 0, a $r|pq$, tak buď $r|p$, nebo $r|q$. Tedy takzvané ireducibilní polynomy se chovají podobně jako prvočísla. Po další úvaze zjistíme, že polynomy nad $\mathbb{Q}, \mathbb{Z}, \mathbb{R}$ můžeme „rozložit na prvočinitele“ jednoznačně (až na pořadí a násobení konstantou).

Opět nic takového nemusí platit nad jinými množinami čísel: Nad $\mathbb{Z}_4$ je $x+2|x^2$, ale $\neg(x+2|x)$.

Definice. *Kořen polynomu p nad R je takové číslo $\alpha \in R$, že $p(\alpha) = 0$.*

Pozorování. Pokud má polynom $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, a_i \in \mathbb{Z}$, racionální kořen $q = \frac{r}{s}$ (r, s nesoudělná), tak platí $r|a_0$ a $s|a_n$.

Tvrzení. Pokud α je kořen polynomu p, tak $(x - \alpha)|p$.

[12] Úplně přesně bychom řekli, že R má být komutativní okruh, tedy chceme, aby ono sčítání a násobení byly komutativní a asociativní operace, abychom měli jednotku a nulu a platil distributivní zákon $a(b+c) = ab + ac$.

Důsledek. Pokud p je polynom nad $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$ stupně nejvýš n, který má $n+1$ kořenů, tak p je nulový polynom.

Důsledek. Polynom stupně nejvýš n nad $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$ je jednoznačně určený hodnotami v $n+1$ bodech.

Příklad. Dokažte, že pokud P je polynom s celočíselnými koeficienty a a, b, c různá celá čísla, tak se nemůže stát, aby $P(a) = b, P(b) = c, P(c) = a$.

Příklad. Dokažte, že pro všechna po dvou různá čísla $a, b, c \in \mathbb{R}$ platí:

$$\frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-a)(x-c)}{(b-a)(b-c)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} = 1$$

Věta. (Základní věta algebry) *Každý polynom řádu aspoň 1 s komplexními koeficienty má v $\mathbb{C}$ aspoň jeden kořen.*

Důsledek. Každý polynom nad $\mathbb{C}$ lze psát ve tvaru $c \prod_{i=1}^{n} (x - \alpha_i)$, kde α_i jsou komplexní čísla (kořeny) a c je nenulové komplexní číslo.

Tvrzení. (Viètovy vztahy) Buďte $\alpha_1, \alpha_2, \ldots, \alpha_n$ kořeny polynomu $p(x) = x^n + + c_{n-1}x^{n-1} \cdots + c_0$ nad $\mathbb{C}$. Potom platí:

$$\begin{aligned} c_{n-1} &= -\sum_{i=1}^{n} \alpha_i \\ c_{n-2} &= \sum_{\substack{i,j=1 \\ i<j}}^{n} \alpha_i \alpha_j \\ &\vdots \\ c_0 &= (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n \end{aligned}$$

Příklad. Buďte a, b, c reálná čísla taková, že

$$\begin{aligned} a + b + c &> 0 \\ ab + ac + bc &> 0 \\ abc &> 0. \end{aligned}$$

Dokažte, že pak $a > 0, b > 0, c > 0$.

Příklad. Mějme P, Q reálné polynomy, $P \neq 0$. Dokažte, že existuje polynom R s reálnými koeficienty takový, že $P(x) | R(Q(x))$.

Příklad. $P(x)$ buď polynom stupně nejvýš 6 nad $\mathbb{Z}$ takový, že $7 | P(x)$ pro každé $x \in \mathbb{Z}$. Ukažte, že potom 7 dělí všechny koeficienty $P(x)$.