Polynomy

Libor Barto

Definice. *$\mathbb{T}$-polynomem nazveme funkci*

$$p:\ p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,\ \text{kde } a_0 \neq 0,\quad a_0,\ a_1,\ \ldots,\ a_n \in \mathbb{T}.$$

Zde $\mathbb{T} = \mathbb{Z},\ \mathbb{Q}$ nebo $\mathbb{R}$. Číslu n budeme říkat stupeň polynomu p, značíme $\deg(p)$. Funkci $p : p(x) = 0$ nazveme polynomem stupně -1. Reálné číslo a nazveme kořenem p, je-li $p(a) = 0$. Číslo a nazveme n-násobným kořenem p, existuje-li $\mathbb{T}$-polynom q takový, že $p = (x - a)^n q$ a a není kořenem q.

Polynom bude v následujícím textu znamenat $\mathbb{R}$-polynom.

Dělení polynomů

Máme-li dva polynomy můžeme snadno vypočítat jejich součet, rozdíl a součin. Polynomy však také můžeme dělit se zbytkem:

Věta. *Nechť $p,\ q$ jsou nenulové polynomy. Pak existují polynomy $f,\ r$ takové, že $p = fq+r$ a $\deg(r) < \deg(q)$. Polynomy $f,\ r$ jsou těmito podmínkami určeny jednoznačně. Polynom f se nazývá částečný podíl, r se nazývá zbytek.*

Definice. *Nechť $p,\ q$ jsou polynomy*

(1) *Říkáme q dělí p a píšeme $q \mid p$, pokud existuje polynom f takový, že $qf = p$.*
(2) *Říkáme, že polynom f je společný dělitel $p,\ q$, pokud $f \mid p$ a $f \mid q$.*
(3) *Říkáme, že f ke největší společný dělitel $p,\ q$, pokud f je jejich společný dělitel a pro každý společný dělitel g polynomů $p,\ q$, platí $g \mid f$. Největší společný dělitel polynomů p, q budeme značit $\mathrm{NSD}(p, q)$.*

$\mathrm{NSD}(p, q)$ vždy existuje (a je „skoro jednoznačně“ určen — dva NSD jsou stejné pokud je vynásobíme vhodnými čísly), kromě případu, že $p,\ q = 0$. K výpočtu NSD lze použít Eukleidův algoritmus, založený na vztahu $\mathrm{NSD}(p, q) = \mathrm{NSD}(p - kq, q)$, který platí pro libovolné polynomy $k,\ p,\ q$.

Derivace

Definice. *Derivací polynomu $p : p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ nazveme polynom $p' : p'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1}$.*

Věta. *Pro polynomy p, q a přirozené číslo $n \in \mathbb{N}$ platí:*
(1) $(p+q)' = p' + q'$.
(2) $(pq)' = p'q + pq'$.
(3) $(p^n)' = np^{n-1}p'$.

Věta. *Má-li polynom p kořen x, pak x je vícenásobný právě tehdy, když p' má kořen x.*

Ireducibilní polynomy

Definice. *O polynomu p řekneme, že je $\mathbb{T}$-reducibilní, pokud existují nekonstantní $\mathbb{T}$-polynomy $p_1, \ldots, p_n$ $(n \geq 2)$ takové, že $p = p_1 p_2 \cdots p_n$. V opačném případě řekneme, že polynom je $\mathbb{T}$-ireducibilní.*

Věta. *Každý $\mathbb{T}$-polynom stupně alespoň 1 lze rozložit na součin $\mathbb{T}$-ireducibilních $\mathbb{T}$-polynomů stupňů alespoň 1. Tento rozklad je jednoznačný až na pořadí a vynásobení polynomů konstantami.*

Věta. (Gaussova) *Každý $\mathbb{Q}$-reducibilní $\mathbb{Z}$-polynom je $\mathbb{Z}$-reducibilní.*

Věta. (Eisensteinovo kritérium) *Nechť $p : p(x) = a_0x^n + \cdots + a_{n-1}x + a_n$ je $\mathbb{Z}$-polynom. Nechť p je prvočíslo, pro které $p \nmid a_0$, $p \mid a_i$, $i = 1, \ldots, n$, $p^2 \nmid a_n$. ($a \mid b$ je zde relace mezi celými čísly, ne polynomy) Potom p je $\mathbb{Q}$-ireducibilní.*

Kořeny

V následujících větách uvažujme polynom $p : p(x) = a_0x^n + \cdots + a_{n-1}x + a_n$.

Věta. *Polynom p má nejvýše n kořenů (počítáme-li každý kořen tolikrát, kolik je jeho násobnost).*

Věta. *Je-li p $\mathbb{Z}$-polynom a $z \in \mathbb{Q}$ jeho kořen, potom $z = \frac{p}{q}$, kde $p \mid a_n, q \mid a_0$.*

Věta. *Je-li z kořenem polynomu p, pak platí:*

$$|z| < 1 + \frac{\max(|a_1|, |a_2|, \ldots, |a_n|)}{|a_0|}.$$

Věta. (Rolleova) *Mezi dvěma různými bezprostředně za sebou jdoucími kořeny polynomu p leží lichý počet kořenů polynomu p' (počítáno i s jejich násobnostmi).*

Definice. *Počtem znaménkových změn v posloupnosti* $c_0,\ c_1,\ \ldots,\ c_m$ *nenulových čísel budeme rozumět počet těch indexů* $i,\ 0 \leq i < m$, *pro které* c_i *a* c_{i+1} *mají opačná znaménka. Počet změn v posloupnosti, v níž se nuly vyskutují spočítáme tak, že nuly vyškrtneme a spočteme počet změn ve vzniklé posloupnosti.*

Věta. (Descartesova) *Označme* V *počet znaménkových změn v posloupnosti čísel* $a_0,\ a_1,\ \ldots,\ a_n$ *a* N *počet kladných kořenů* p. *Potom číslo* $V - N$ *je nezáporné a sudé.*