Cvičenie 9

Okruhy polynómov – korene polynómov

Prvok $c \in F$ sa nazýva koreňom polynómu $F[x]$, ak $f(c) = 0$ (po dosadení c do polynómu dostaneme 0.) Ak pracujeme s polynómami z $F[x]$, tak ako korene môžeme uvažovať aj prvky z nejakého nadpoľa $F_1 \supseteq F$. (Lebo $F[x] \subseteq F_1[x]$ – ak sú všetky koeficienty z F, tak súčasne patria aj do nadpoľa F_1.)

Prvok c je koreň polynómu $f(x)$ práve vtedy, keď $f(x) = g(x)(x-c)$ (t.j. keď $x-c \mid f(x)$). Ak platí $f(x) = g(x)(x-c)^k$ (t.j. $(x-c)^k \mid f(x)$), hovoríme, že c je k-násobný koreň $f(x)$.

1. Dokážte, že zvyšok polynómu $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$ po delení $x-b$ je práve $f(b)$ (=jeho hodnota v bode $b \in F[x]$).

2. Vydeľte dané polynómy so zvyškom v $\mathbb{C}[x]$.
   a) $f(x) = x^4 + 3x^3 - 4x + 2$, $g(x) = x^2 + x - 2$
   b) $f(x) = x^5 + 2x^3 + 3x + 4$, $g(x) = x^3 + x + 1$
   c) $f(x) = x^3 + (2+2i)x^2 + 3ix + 1$, $g(x) = x^2 + (2+i)x + i$

3. Použitím Hornerovej schémy[1] zistite, či c je koreň polynómu $f(x) \in \mathbb{C}[x]$ a vyjadrite tento polynóm v tvare $f(x) = g(x)(x-c) + f(c)$.
   a) $f(x) = x^4 + 3x^3 - 4x + 2$, $c = -2$
   b) $f(x) = x^5 + 2x^3 + 3x + 4$, $c = -1$
   c) $f(x) = x^3 + (2+2i)x^2 + 3ix + 1$, $c = -i$

4. Pomocou Hornerovej schémy vyjadriť:
   a) $f(x+3)$ pre $f(x) = x^4 - x^3 + 1$
   b) $(x-2)^4 + 4(x-2)^3 + 6(x-2)^2 + 10(x-2) + 20$

5. * Dokážte, že ak $c = \frac{p}{q} \in \mathbb{Q}$ je koreň polynómu $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ s celočíselnými koeficientami, tak $p \mid a_0$ a $q \mid a_n$.

6. Nájdite všetky racionálne korene daných polynómov a ich násobnosť (s pomocou Hornerovej schémy a tvrdenia dokázaného v predchádzajúcej úlohe)
   a) $f(x) = 4x^4 - 7x^2 - 5x - 1$
   b) $f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6$
   c) $f(x) = 6x^4 + 19x^3 - 7x^2 - 26x + 12$
   [a) $-\frac{1}{2}$ dvojnásobný; b) $\frac{1}{2}$, $-\frac{2}{3}$, $\frac{3}{4}$; c) -3, $\frac{1}{2}$]

7. Dokážte: Ak $a+bi$ je koreň polynómu $f(x) \in \mathbb{R}[x]$ a $b \neq 0$, tak $x^2 - 2ax + a^2 + b^2 \mid f(x)$.

8. * Nech $f(x) \in \mathbb{Z}[x]$ je polynóm s celočíselnými koeficientami. Dokážte, že ak $a + b\sqrt{3}$ je koreň $f(x)$, tak aj $a - b\sqrt{3}$ je koreň $f(x)$. Dokážte, že podobné tvrdenie platí, ak c nahradíme ľubovoľným prirodzeným číslom, ktoré nie je druhou mocninou prirodzeného čísla.

Najväčší spoločný deliteľ, deliteľnosť

1. Vypočítajte $d(x) = \gcd(f(x), g(x))$ a vyjadrite ho v tvare $d(x) = u(x)f(x) + v(x)g(x)$.
   a) $f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$, $g(x) = 3x^4 - 4x^3 - x^2 - x - 2$;
   b) $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$, $g(x) = 2x^3 - x^2 - 5x + 4$;

[1] Pozri text k prednáške.

c) $f(x) = x^4 + 6x^3 + 9x^2 - 2x - 9$, $g(x) = x^3 + 4x^2 + 2x - 7$;
d) $f(x) = x^8 - 1$, $g(x) = x^5 - 1$
(Výsledky: a) $u(x) = -\frac{1}{3}x^2 + \frac{1}{3}x + \frac{1}{3}$, $v(x) = \frac{1}{3}x^3 + \frac{2}{3}x^2 - \frac{5}{3}x - \frac{4}{3}$, $d(x) = x + \frac{2}{3}$
b) $u(x) = -\frac{x-1}{3}$, $v(x) = \frac{2x^2-2x-3}{3}$, $d(x) = x - 1$
c) $d(x) = 1$, $u(x) = 1/30(2x^2 + 5x - 1)$, $v(x) = -1/30(2x^3 + 9x^2 + 7x + 3)$)

2. Dokážte, že $x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3p+2}$ (v $F[x]$ pre ľubovoľné pole F).

3. Dokážte, že $x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3p+2}$ v $\mathbb{C}[x]$. (Využite to, čo viete o koreňoch týchto polynómov.)

Okruhy polynómov – rozklad na ireducibilné polynómy

Ireducibilné prvky okruhu $F[x]$ sa nazývajú *ireducibilné polynómy.* Každý polynóm $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ sa dá jednoznačne rozložiť ako $f(x) = a_n p_1(x) \dots p_n(x)$, kde $p_1 \dots p_n$ sú ireducibilné normované (=vedúci koeficient je 1) polynómy. (Rozklad na ireducibilné polynómy nám môže pomôcť pri zisťovaní, či je jeden polynóm deliteľný druhým, ako aj pri hľadaní najväčšieho spoločného deliteľa.)

Každý polynóm stupňa 1 je ireducibilný. V prípade, že $f(x)$ má rozklad na polynómy stupňa 1, hovoríme o rozklade na *koreňové činitele*

$$f(x) = a_n(x - x_1)(x - x_2)\dots(x - x_n)$$

(prvky $x_1 \dots x_n$ sú práve korene polynómu f.)

V $\mathbb{C}[x]$ sú jediné ireducibilné polynómy polynómy stupňa 1 – každý polynóm sa dá nad $\mathbb{C}$ rozložiť na koreňové činitele.

V $\mathbb{R}[x]$ môžu existovať ireducibilné polynómu stupňa 2, každý polynóm $f(x) \in \mathbb{R}[x]$ stupňa 3 má však reálny koreň.

1. Rozložiť na koreňové činitele (nad $\mathbb{C}$):
a) $x^3 - 6x^2 + 11x - 6$
b) $x^4 + 4$,
c) $x^4 + 4x^3 + 4x^2 + 1$,
d) $x^4 - 10x^2 + 1$,
e) $x^4 - 4x^3 + 4x - 1$.

2. Rozložiť na súčin ireducibilných polynómov nad $\mathbb{R}$:
a) $x^4 + 4$
b) $x^6 + 27$
c) $x^4 + 4x^3 + 4x^2 + 1$
d*) $x^{2n} - 2x^n + 2$
e*) $x^4 - ax^2 + 1$ pre $a \in (-2, 2)$
f*) $x^{2n} + x^n + 1$.

3. Nájdite všetky ireducibilné polynómy nad $\mathbb{Z}_2$ stupňov 2,3,4.

4. Nájdite rozklad $f(x)$ na ireducibilné polynómy v $F[x]$.
a) $f(x) = 4x^4 + 3x^3 + 4x^2 + 4x + 6$, $F = \mathbb{Z}_7$
b) $f(x) = x^4 - 1$, $F = \mathbb{Z}_{11}$
c) $f(x) = x^4 - 1$, $F = \mathbb{Z}_{13}$

5. Ukážte, že polynóm stupňa 3 v $F[x]$ je ireducibilný práve vtedy, keď nemá koreň v F.

Taylorov rozvoj polynómu

Formálna derivácia polynómu $f(x) = \sum_{k=0}^{n} a_k x^k$ je polynóm $Df(x) = \sum_{k=1}^{n} k a_k x^{k-1}$. Polynóm f nemá násobné korene práve vtedy, keď $(f(x), Df(x)) = 1$.

Ľubovoľný polynóm $f(x) \in F[x]$ sa pre dané $c \in F$ dá vyjadriť v tvare $b_n(x-c)^n + \cdots + b_1(x-c) + b_0$, koeficienty b_i sú polynómom f prvkom c jednoznačne určené. V prípade, že F je pole nekonečnej charakteristiky (vysvetlíme si na cvičení – zatiaľ Vám stačí vedieť, že polia $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ túto vlastnosť majú), tak $b_k = \frac{D^k f(c)}{k!}$. (Taylorov rozvoj polynómu – rovnaký tvar ako Taylorov rozvoj, ktorý poznáte z analýzy.)

1. Dokážte, že polynóm $f(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!}$ nemá viacnásobný koreň.