8. přednáška, 15. 11. 2022

5.3. Ireducibilní polynomy

Definice 5.3.1. *Reducibilní* polynom je nekonstantní polynom, který je součinem dvou nekonstantních polynomů. *Ireducibilní* polynom je nekonstantní polynom, který není reducibilní.

Příklad. Polynom $x^2 - 1 = (x-1)(x+1)$ je reducibilní. Polynomy $x-1$ a $x+1$ jsou ireducibilní, máte tedy rozklad na normované ireducibilní polynomy. ■

Cvičení. Nechť jsou $f, g \in P[x]$ normované polynomy, nechť g je ireducibilní a $f \mid g$. Potom buď $f = 1$ nebo $f = g$. Je-li f také ireducibilní, pak $f = g$. ▷

Lemma 5.3.1. *Buďte $g, h_1, \ldots, h_n \in P[x]$ ireducibilní normované polynomy a nechť $g \mid h_1 \cdots h_n$. Pak existuje index j takový, že $g = h_j$.*

Důkaz. □

Tvrzení 5.3.2. *Buď $f \in P[x]$ normovaný polynom. Pak existují normované ireducibilní polynomy $g_1, \ldots, g_n$ takové, že $f = g_1 \cdots g_n$.*

Tento rozklad je jediný. Je-li $f = h_1 \cdots h_m$ jiný rozklad na normované ireducibilní činitele, pak $m = n$ a po vhodném přečíslování platí $h_i = g_i$ pro všechna $i \in \{1, \ldots, n\}$. (Přesněji, existuje bijekce $\varphi\colon \{1, \ldots, n\} \to \{1, \ldots, m\}$ taková, že $h_i = g_{\varphi(i)}$ pro všechna i.)

Důkaz. □

Příklad. Polynom $x^2 + 1$ je reducibilní nad polem $\mathbb{C}$, protože $x^2 + 1 = (x+i)(x-i)$. Tentýž polynom je ireducibilní nad polem $\mathbb{R}$, protože jakýkoliv jeho hypotetický rozklad $x^2 + 1 = (x+\xi)(x+\eta)$, $\xi, \eta \in \mathbb{R}$ je současně rozkladem nad $\mathbb{C}$ různým od $x^2 + 1 = (x+i)(x-i)$, ve sporu s jednoznačností rozkladu. ■

Jako důsledek obdržíme jisté zobecnění shora uvedeného lemmatu.

Důsledek. *Nechť $f \in P[x]$, buďte $g_1, \ldots, g_m \in P[x]$ ireducibilní, normované a po dvou různé, tj. $g_i \neq g_j$ pro $i \neq j$. Jestliže $g_1^{k_1} \mid f$, …, $g_m^{k_m} \mid f$, pak $g_1^{k_1} \cdots g_m^{k_m} \mid f$.*

5.4. Kořeny a jejich násobnost

Když $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in P[x]$ a $\xi \in P$, položme

$$f(\xi) = a_n \xi^n + a_{n-1}\xi^{n-1} + \cdots + a_1 \xi + a_0 \in P.$$

Tvrzení 5.4.1. *Pro libovolné polynomy $f, g \in P[x]$ a libovolný prvek $\xi \in P$ platí*

$$(f+g)(\xi) = f(\xi) + g(\xi), \quad (-f)(\xi) = -f(\xi), \quad (fg)(\xi) = f(\xi)g(\xi).$$

Důkaz. Cvičení. □

Definice 5.4.1. Prvek $\xi \in P$ je *kořen* polynomu $f \in P[x]$, jestliže $f(\xi) = 0$.

Tvrzení 5.4.2. *Nechť $f \in P[x]$ a $\xi \in P$. Potom ξ je kořen polynomu f právě tehdy, když polynom $x - \xi$ dělí f.*

Důkaz. Předpokládejme, že ξ je kořen polynomu f. Dělením $f : (x-\xi)$ dostaneme

$$f = (x-\xi)q + r, \quad \text{kde buď } r = 0 \text{ nebo } \deg r = 0 < 1 = \deg(x-\xi).$$

Takže r je konstantní polynom. Navíc $0 = f(\xi) = (\xi - \xi)q(\xi) + r = r$, čili $f = (x - \xi)q$ a $x - \xi$ dělí f.

Předpokládejme, že $x - \xi$ dělí f, tedy $f = (x - \xi)q$ pro nějaké q. Potom $f(\xi) = (\xi - \xi)q(\xi) = 0$, čili ξ je kořen polynomu f. □

Definice 5.4.2. Nechť $f \in P[x]$ a $\xi \in P$. Pokud $(x - \xi) \mid f$, polynom $x - \xi$ je *kořenový činitel* polynomu f.

Definice 5.4.3. Prvek $\xi \in P$ je *k-násobný kořen* polynomu $f \in P[x]$, jestliže $(x - \xi)^k$ dělí f, ale $(x - \xi)^{k+1}$ nedělí f.

Tvrzení 5.4.3. *Buďte $\xi_1, \ldots, \xi_n \in P$ různé kořeny polynomu $f \in P[x]$ s násobnostmi po řadě $k_1, \ldots, k_n$. Potom*

(1) $(x - \xi_1)^{k_1} \cdots (x - \xi_n)^{k_n} \mid f$;

(2) $k_1 + \cdots + k_n \leq \deg f$.

Důkaz. Cvičení. □

Tvrzení 5.4.4 (Základní věta algebry)**.** *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má aspoň jeden kořen.*

Důsledek. *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má rozklad na lineární ireducibilní činitele. Kořenů má se započtením násobnosti právě tolik, kolik činí jeho stupeň.*

Tvrzení 5.4.5 (Vlastnosti kořenů (Viètovy vzorce))**.** *Buď $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{C}[x]$ normovaný polynom a $\xi_1, \xi_2, \ldots, \xi_n$ jeho kořeny (nemusí být všechny různé). Potom*

$$\begin{aligned}
a_{n-1} &= -(\xi_1 + \xi_2 + \cdots + \xi_n) = -\sum_{i=1}^{n} \xi_i \\
a_{n-2} &= \xi_1\xi_2 + \xi_1\xi_3 + \cdots + \xi_1\xi_n + \xi_2\xi_3 + \cdots + \xi_2\xi_n + \cdots + \xi_{n-1}\xi_n = \\
&= \sum_{\substack{i,j=1 \\ i<j}}^{n} \xi_i\xi_j \\
a_{n-3} &= -(\xi_1\xi_2\xi_3 + \xi_1\xi_2\xi_4 + \cdots + \xi_1\xi_{n-1}\xi_n + \cdots + \xi_{n-2}\xi_{n-1}\xi_n) = \\
&= -\sum_{\substack{i,j,k=1 \\ i<j<k}}^{n} \xi_i\xi_j\xi_k \\
&\vdots \\
a_1 &= (-1)^{n-1}(\xi_1 \cdots \xi_{n-2}\xi_{n-1} + \xi_1 \cdots \xi_{n-2}\xi_n + \cdots \\
&\qquad \cdots + \xi_1\xi_3 \cdots \xi_n + \xi_2 \cdots \xi_n) \\
a_0 &= (-1)^n \xi_1\xi_2 \cdots \xi_n
\end{aligned}$$

Důkaz.

$$x^n + \ldots + a_0 = (x - \xi_1) \ldots (x - \xi_n)$$

□

Příklad. $x^2 - 5x + 6$ ■

Pro polynomy, jejichž koeficienty jsou celá čísla, navíc platí následující tvrzení.

Tvrzení 5.4.6. *Buďte $f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ polynom s celočíselnými koeficienty a p, q nesoudělná celá čísla. Jestliže $\frac{p}{q}$ je kořenem polynomu f, potom a_0 je dělitelné p a a_n je dělitelné q.*

Důkaz. Cvičení. Dosazení $\frac{p}{q}$ do f … ☐

Důsledek. *Celočíselné kořeny polynomu s celočíselnými koeficienty jsou dělitelé absolutního členu.*

5.5. Derivace

Definice 5.5.1. Buď $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. Polynom $f' = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \in \mathbb{C}[x]$ je *derivace* polynomu f.

Tvrzení 5.5.1. *(1)* $(f+g)' = f' + g'$,
(2) $(fg)' = f'g + fg'$,
(3) $(f^k)' = kf^{k-1}f'$.

Důkaz. Cvičení. ☐

Tvrzení 5.5.2. *Buď* $k \geq 2$, $f \in \mathbb{C}[x]$ *polynom a* $\xi \in \mathbb{C}$ *je jeho* k*-násobný kořen. Potom*
(1) ξ *je* $(k-1)$*-násobný kořen* f',
(2) ξ *je* $(k-1)$*-násobný kořen největšího společného dělitele* $D(f, f')$.

Důkaz. (1) $(x-\xi)^k \mid f$, tedy $f = (x-\xi)^k q$ a $(x-\xi)^{k+1}$ nedělí f. Potom

$$f' = k(x-\xi)^{k-1}q + (x-\xi)^k q' = (x-\xi)^{k-1}(kq + (x-\xi)q').$$

Takže, $(x-\xi)^{k-1}$ dělí f'. Kdyby $(x-\xi)^k$ dělilo f', pak by $(x-\xi) \mid (kq + (x-\xi)q')$, načež $(x-\xi) \mid kq$, tedy $(x-\xi) \mid q$ a $(x-\xi)^{k+1} \mid f$ ve sporu s předpokladem.

(2) $(x-\xi)^{k-1}$ je dělitel f i f', takže $(x-\xi)^{k-1} \mid D(f, f')$. Kdyby $(x-\xi)^k$ dělilo $D(f, f')$, pak by $(x-\xi)^k \mid f'$ ve sporu s předchozím bodem. ☐

Tvrzení 5.5.3. *Buďte* $f \in \mathbb{C}[x]$ *a* $\xi \in \mathbb{C}$ *jeho kořen. Potom* ξ *je* 1*-násobný kořen polynomu*

$$\frac{f}{D(f, f')} \in \mathbb{C}[x].$$

Důkaz. Buď ξ je k-násobný kořen, tedy $f = (x-\xi)^k q$, ale $(x-\xi)^{k+1}$ nedělí f, čili $x - \xi$ nedělí q. Podle předchozího tvrzení $D(f, f') = (x-\xi)^{k-1} r$. Takže

$$\frac{f}{D(f, f')} = (x-\xi)\frac{q}{r} \quad \text{a jelikož } x-\xi \text{ nedělí } q, \text{ nedělí ani } \frac{q}{r}.$$ ☐

Důsledek. *Buď* $f \in \mathbb{C}[x]$.
(1) Množina všech kořenů polynomu $f/D(f, f')$ *je rovna množině všech kořenů polynomu* f.
(2) Všechny kořeny polynomu $f/D(f, f')$ *jsou* 1*-násobné.*

Důkaz. Cvičení. ☐

5.6. Polynomy s reálnými koeficienty

Mějme polynom $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. Přiřaďme mu polynom $f^* = a_n^* x^n + \cdots + a_1^* x + a_0^* \in \mathbb{C}[x]$.

Tvrzení 5.6.1. *(1)* $(f+g)^* = f^* + g^*$,
(2) $(fg)^* = f^* g^*$.

Důkaz. Cvičení. ☐

Tvrzení 5.6.2. *Buď $f \in \mathbb{R}[x]$ polynom a $\xi \in \mathbb{C}$ jeho kořen. Pak komplexně sdružené číslo ξ^* je též kořen stejné násobnosti.*

Důkaz. $f = (x-\xi)^k q$. Aplikujeme komplexní sdružení $f = f^* = (x-\xi^*)^k q^*$ (cvičení). Kdyby $f = (x-\xi^*)^{k+1} r$, pak $f = f^* = (x-\xi)^{k+1} r^*$. □

Rozklad polynomu $f \in \mathbb{R}[x]$ na ireducibilní činitele nad $\mathbb{C}$ pak obsahuje …
Vidíme, že $\deg f =$.

Tvrzení 5.6.3. *Každý polynom $f \in \mathbb{R}[x]$ lichého stupně má aspoň jeden reálný kořen.*

Důkaz. Cvičení. □

Tvrzení 5.6.4. *Nechť $\xi \in \mathbb{C} \setminus \mathbb{R}$. Ukažte, že $(x-\xi)(x-\xi^*) = x^2 - 2\operatorname{re}\xi + |\xi|^2$ je kvadratický polynom s reálnými koeficienty a záporným diskriminantem.*

Důkaz. Cvičení.
Návod: pište $\xi = \alpha + \beta\mathrm{i}$, kde $\alpha, \beta \in \mathbb{R}$. □

Cvičení. Ukažte, že reálné polynomy řádu > 2 jsou vždy reducibilní nad $\mathbb{R}$. ▷

Cvičení. Rozložte polynom $x^4 + 1$ na ireducibilní činitele nad polem $\mathbb{C}$ a nad polem $\mathbb{R}$. ▷