Euklidův algoritmus

$f, g \quad \dots \quad D(f,g)$

$f = g q_1 + r_1$

$g = r_1 q_2 + r_2$

$r_1 = r_2 q_3 + r_3$

$\vdots$

$\exists m \in \mathbb{N} : r_m \neq 0 \wedge r_{m+1} = 0.$

$r_m = D(f,g)$

Tvrzení $f, g \in P[x]$, potom existuje jejich $D(f,g)$ a polynomy $u, v \in P[x]$ takové, že

$$D(f,g) = fu + g \cdot v.$$

Rozšířený Euklidův algoritmus

DÚ, cvičení

Nekonstantní polynom $\in P[x]$ je REDUCIBILNÍ, jestliže je součinem dvou nekonstantních polynomů.
IREDUCIBILNÍ polynom je nekonstantní polynom, který není reducibilní.

Př.: $f = x+1$

$f = x^2 - 1 = (x+1)(x-1)$

$f = x^2 + 1 = (x+i)(x-i)$

$\in \mathbb{R}[x]$ ... ireducibilní

$\in \mathbb{C}[x]$ ... reducibilní.

Tvrzení $f \in P[x]$ normovaný. Pak existují normované polynomy $g_1, \dots, g_n \in P[x]$ ireducibilní a $f = g_1 \cdot \dots \cdot g_n$.

Kořeny polynomů

Prvek $\xi \in P$ je ASPOŇ k-NÁSOBNÝ KOŘEN polynomu $f \in P[x]$, jestliže $(x-\xi)^k \mid f$.

$\xi \in P$ je k-NÁSOBNÝ KOŘEN polynomu $f \in P[x]$, jestliže $(x-\xi)^k \mid f$ a neplatí $(x-\xi)^{k+1} \mid f$.

Základní věta algebry

Každý nekonstantní polynom z $\mathbb{C}[x]$ má aspoň jeden kořen.

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{C}[x]$$

$$f' = n \cdot a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$$

se nazývá DERIVACE polynomu f.

Tvrzení 1) $(f+g)' = f' + g'$

2) $(fg)' = f'g + f \cdot g'$.

3) $(f^k)' = k \cdot f^{k-1} \cdot f'$.

Důkaz DÚ.

Tvrzení $k \geq 2$, $f \in \mathbb{C}[x]$ a $\xi \in \mathbb{C}$ je k-násobný kořen f. Pak

1) ξ je $(k-1)$-násobný kořen f'.

2) ξ je $(k-1)$-násobný kořen $D(f, f')$.

Důkaz $(x-\xi)^k \mid f \Rightarrow \exists g \in \mathbb{C}[x]$:

$$f = (x-\xi)^k \cdot g$$

$$f' = ((x-\xi)^k)' \cdot g + (x-\xi)^k \cdot g'$$

$$= k \cdot (x-\xi)^{k-1} \cdot g + (x-\xi)^k \cdot g'$$

$$= (x-\xi)^{k-1} \cdot (k \cdot g + (x-\xi) \cdot g')$$

2) ✓ ✓

Tvrzení $f \in \mathbb{C}[x]$, $\xi \in \mathbb{C}$ kořen f. Pak ξ je 1-násobný kořen polynomu

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

Tvrzení (Viètovy vzorce)

$f = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{C}[x]$

$\xi_1, \dots, \xi_n$ jeho kořeny. Pak

$$a_{n-1} = -(\xi_1 + \xi_2 + \dots + \xi_n) = -\sum_{i=1}^{n} \xi_i$$

$$a_{n-2} = \sum_{\substack{i,j=1 \\ i<j}}^{n} \xi_i \xi_j$$

$$\vdots$$

$$a_0 = (-1)^n \xi_1 \xi_2 \dots \xi_n .$$

Př.: $x^2 - 5x + 6$, $n = 2$

$a_1 = -5$, $a_0 = 6$ $\qquad \xi_1 = 2, \xi_2 = 3$

$f \in \mathbb{C}[x]$, $\xi \in \mathbb{C}$ je kořen f.

ξ^* je také kořen f se stejnou násobností.

POLOGRUPY, MONOIDY, GRUPY

BINÁRNÍ OPERACE na množině X je zobrazení $X \times X \to X$.

Operace $*$ na mn. X je ASOCIATIVNÍ, jestliže $\forall x, y, z \in X$ platí
$(x * y) * z = x * (y * z)$.

Operace $*$ na X je KOMUTATIVNÍ, jestliže $\forall x, y \in X$ platí $x * y = y * x$.

Pologrupy

X ... množina, $*$ ... operace na X
Když $*$ je asociativní, pak
$(X, *)$ se nazývá POLOGRUPA.
Když $*$ je navíc komutativní, pak pologrupa se nazývá KOMUTATIVNÍ.

X ... množina, $*$ operace.
$e \in X$ se nazývá NEUTRÁLNÍ prvek operace $*$, jestliže $\forall y \in X$ platí $e * y = y * e = y$.

Tvrzení V množině X s operací $*$ existuje nejvýše jeden neutrální prvek.

Důkaz Předpokládejme, že e', e'' jsou neutrální prvky $*$. Pak

$$e' = e' * e'' = e''.$$

X ... množina, $*$ ... operace na X.
Když $*$ je asociativní a v X existuje neutrální prvek e operace $*$, pak
$(X, *, e)$ se nazývá MONOID.
