$\boxed{1. \text{CV.}}$

- 12:00–14:00
- okruh
- polynomy nad okruhem R (R je v tomto případě defaultně komutativní)
- ireducibilní $\iff$ nejde napsat jako součin dvou nekonst. polynomů nad tím samým okruhem

- $f(x)$ je primitivní, pokud $f(x) \neq 0$ a $\gcd(a_m, a_{m-1}, \dots, a_0) = 1$.
- Gaussovo lemma (primitivita): Nechť $f(x), g(x) \in \mathbb{Z}[x]$ jsou primitivní. Pak $f(x) \cdot g(x)$ je primitivní
- důkaz: sporem: $f(x) \cdot g(x)$ není primitivní $\Rightarrow \exists$ prvočíslo p: p dělí všechny koeficienty $f(x) \cdot g(x)$

  $f(x) = a_m x^m + \dots + a_0$

  $g(x) = b_n x^n + \dots + a_0$

  Nechť r, s jsou nejmenší takové indexy, že $p \nmid a_r$, $p \nmid b_s$.

  Pak koeficient $f(x) \cdot g(x)$ u x^{r+s} ~~není dělitelný~~ je $\cancel{a_r + b_s}$ $a_r b_s + k$, kde k je dělitelný p, spor. $\square$

- Gaussovo lemma (ireducibilita): Nechť $f(x) \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$. Pak je ireducibilní nad $\mathbb{Q}$. (opačná implikace je zřejmá)
- důkaz: sporem, nechť existují $\overbrace{g(x), h(x)}^{\text{nekonst.}} \in \mathbb{Q}[x]$, $f(x) = g(x) \cdot h(x)$.

  $\exists\, a, b \in \mathbb{Q}$, $\neq 0$ a $\overbrace{g_1(x), h_1(x)}^{\text{nekonst.}} \in \mathbb{Z}[x]$ | $g(x) = a \cdot g_1(x)$, $h(x) = b \cdot h_1(x)$.

  $f(x) = ab \cdot g_1(x) \cdot h_1(x)$, tedy $a \cdot b \in \mathbb{Z}$, spor.
  (z předchozího lemmatu, sporem)

- rational root theorem
- Eisensteinovo kritérium: p je prvočíslo, $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ takový, že $p \mid a_0, \dots, p \mid a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$. Pak $f(x)$ je ireducibilní nad $\mathbb{Z}$
- důkaz: sporem $\underbrace{g(x) \cdot h(x)}_{\text{nekonst}} \in \mathbb{Z}[x]$, $f(x) = g(x) \cdot h(x)$

  $g(x) = b_k x^k + \dots + b_0$, $h(x) = c_l x^l + \dots + c_0$

  $a_0 = b_0 c_0 \Rightarrow$ BÚNO $p \mid b_0$, $p \nmid c_0$

  $a_n = b_k \cdot c_l \Rightarrow p \nmid b_k$.

  Nechť i je ~~největší index~~ nejmenší index takový, že $p \nmid b_i$.

Víme $a_j = \underbrace{b_j c_0 + b_{j-1} \cdot c_1 + \dots + b_0 c_j}_{\text{dělitelný } p}$ $\quad p \nmid b_j c_0 \Rightarrow p \nmid a_j$, $j < n \Rightarrow$ spor

– polynomy splňující toto kritérium se nazývají Eisensteinovské

* Nechť p je prvočíslo, dokažte, že $f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ je ireducibilní nad $\mathbb{Z}$

$$\frac{x^p-1}{x-1} \qquad x = y+1$$

$$(y+1)^{p-1} + (y+1)^{p-2} + \dots + y+1+1$$

$f(x)$ je ired. $\Leftrightarrow f(x+c)$ je ired.

$$f(x) = \frac{x^p-1}{x-1} = \frac{(y+1)^p-1}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + \dots + p$$

tento je Eisensteinovský a tedy ireducibilní.

– cyklotomický (kruhový) polynom: $\zeta_n = e^{\frac{2\pi i}{n}}$

$$\Phi_n(x) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} \qquad \text{př.)}\ \Phi_1(x) = x-1,\ \Phi_2 = x+1,\ \Phi_p = \frac{x^p-1}{x-1},\ \Phi_4(x) = x^2+1$$

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x) \Rightarrow \Phi_n(x) \in \mathbb{Z}[x] \qquad \deg \Phi_n(x) = \varphi(n) \Rightarrow \sum_{d \mid n} \varphi(d) = n.$$

* (IMO 1993/1). Nechť $n \in \mathbb{N}$, $n > 1$. Dokažte, že $f(x) = x^n + 5x^{n-1} + 3$ je ireducibilní nad $\mathbb{Z}$

důkaz Eisensteina zakončíme s tím, že $j = n-1$, tedy $f(x)$ má celočíselný kořen

$f(c) = 0 \Rightarrow c \in \{-1, 1, -3, 3\}$, spor

$\boxed{2.\text{ CV.}}$

pro složené $n = a \cdot b$, $a, b > 1$

$$x^{n-1} + x^{n-2} + \dots + x + 1 = \frac{x^a - 1}{x-1}\left(x^{a(b-1)} + x^{a(b-2)} + \dots + x^a + 1\right)$$

$$= \frac{x^n-1}{x-1} = \prod_{\substack{d \mid n \\ d > 1}} \Phi_d(x)$$

* Nechť $f(x) \in \mathbb{Z}[x]$ nekonst., dokažte, že $\exists$ nekonečně mnoho $k \in \mathbb{Z}$ takových, že $f(x)+k$ je ireducibilní

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$$

$\cancel{f(x+p)} = \cancel{a_0}\, a_0 + k$ je prvočíslo $\cancel{p}$

$$f(x) = g(x)h(x) = (b_{n-k}x^{n-k} + \dots + b_0)(c_k x^k + \dots + c_0)$$

BÚNO $\quad b_0 = p \quad \alpha_{k+1}, \dots, \quad \alpha_1, \dots, \alpha_k$

$c_0 = \pm 1$ $\quad$ α kořeny

$b_{n-k}c_k = a_n \qquad |\alpha_1| \cdot \dots \cdot |\alpha_k| = \frac{1}{|c_k|} \leq 1$

$a_{k} \Rightarrow$

- lemma: $|a_0| > |a_n| + \dots + |a_1|$, pak ~~∀~~ pro každý kořen $|\alpha| > 1$

sporem

$$|a_n| + \dots + |a_1| \geq |a_n||\alpha|^n + \dots + |a_1| \cdot |\alpha| \geq |a_n\alpha^n + \dots + a_1\alpha| = |-a_0| = |a_0| \qquad \square$$

z toho plyne předchozí $\qquad \square$

- Jordanova křivka – uzavřená, neprotíná se
- ~~Cauchyova~~ věta (z komplexní analýzy)
  Rouchéova
- lze jí dokázat základní věta algebry

* $f(x) \in \mathbb{Z}[x]$ normovaný, $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ $(a_0 \neq 0)$ takový, že $n-1$ jeho kořenů včetně násobnosti leží uvnitř $K(0,1)$. Dokažte, že $f(x)$ je ireducibilní

jednotková kružnice

$|\alpha_1| < 1, |\alpha_2| < 1, \dots, \cancel{|\alpha_{n-1}| < 1}, |\alpha_n| \cancel{< 1}$

nemohou všechny ležet uvnitř, tedy, kdyby byl šel rozložit, tak ~~všechny~~ kořeny budou ležet uvnitř, spor

- Perronovo kritérium: $f(x) \in \mathbb{Z}[x]$, $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ $(a_0 \neq 0)$ takový, že

buď $\quad$ 1) $|a_{n-1}| > 1 + |a_{n-2}| + \dots + |a_0|$

nebo $\quad$ 2) $|a_{n-1}| = 1 + |a_{n-2}| + \dots + |a_0|$ a $f(1) \neq 0 \neq f(-1)$

pak $f(x)$ je ireducibilní

- důkaz: $\quad g(a_{n-1}x^{n-1})$

$$|z| = 1: \quad |f(z) - g(z)| = |z^n + a_{n-2}z^{n-2} + \dots + a_0| \leq 1 + |a_{n-2}| + \dots + |a_0| \leq |a_{n-1}| = |a_{n-1}z^{n-1}|$$

$= |g(z)| \leq |f(z)| + |g(z)|$

Chceme ukázat, že to je ostrá nerovnost, v 1) případě je to jasný

2. případ $\quad f(z) \neq 0$, pak $|g(z)| < |f(z)| + |g(z)|$, pokud $\cancel{f(z) \neq 0}$ $f(z) = 0$

$$f(z)=0 \Rightarrow a_{n-1}z^{n-1} \in \mathbb{R}$$
$$\not\Downarrow$$
$$z^n \in \mathbb{R}$$

$$\frac{z}{a_{n-1}} = \frac{z^n}{a_{n-1}z^{n-1}} \in \mathbb{R} \Rightarrow z \in \mathbb{R}$$ $\square$

* n je prvočíslo, dokažte $f(x) = x^{n-1} + 2x^{n-2} + \dots + (n-1)x + n$ je ireducibilní

IMO 1993/1

$\cancel{f(x) = x^{n-1} + 2x^{n-2}}$

$$(x-1)f(x) = \cancel{x^n + 2x^{n-1}}\; x^n + x^{n-1} + \dots + x - n$$

$\cancel{(x-1)^2 f(x) = x^{n+1} - (n+1)x + n}$

$g(z) = -(n+1)z$

$\Gamma = k(0, R)$

$z \in \Gamma: \quad |(z-1)^2 f(z) - g(z)| = |z^{n+1} + n| \overset{?}{<} |-(n+1)z| = (n+1)R$

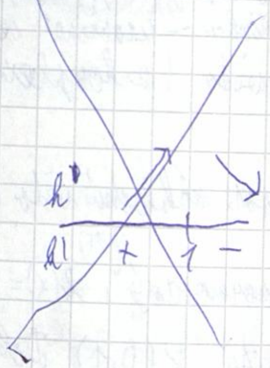
$R = 1-\varepsilon$

$|z^{n+1} + n| \le R^{n+1} + |n|$

dokažme $\quad R^{n+1} + n < (n+1)R$

$h(R) = (n+1)R - R^{n+1} - n$

$h'(R) = n+1 - (n+1)R^n = (n+1)(1-R^n)$



$$\left.\begin{array}{l} \alpha \in \mathbb{C},\ f(\alpha) = 0 \\ |\alpha| \le 1 \end{array}\right\} \quad \alpha^n + \dots + \alpha = n$$

$$n = |n| \le |\alpha^n + \dots + \alpha| \le |\alpha^n| + \dots + |\alpha| \le n$$

$$\exists\, u > 0: \quad \alpha^2 = u \cdot \alpha \Rightarrow \alpha = u \Rightarrow \alpha = 1$$

$$f(\alpha) = 0 \Rightarrow |\alpha| > 1$$

sporom: $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Z}[x]$ nekonšt, normované

$n = |n| = |f(0)| = |g(0)||h(0)|$

BÚNO $|g(0)| = 1$, ale $|\alpha| > 1$

* $n, a_1, \dots, a_n \in \mathbb{N}$, $a_1 \ge a_2 \ge \dots \ge a_n$, $f(x) = x^n - a_1 x^{n-1} - \dots - a_{n-1}x - a_n$. Dokažte, že $f(x)$ je ireducibilní.

$\cancel{f(x) = g(x)h(x)}$

$$f(x)(x-1) = x^{n+1} - (a_1+1)x^n + (a_1-a_2)x^{n-1} + (a_2-a_3)x^{n-2} + \dots + (a_{n-1}-a_n)x + a_n$$

$|1| + |a_1 - a_2| + \dots + |a_{n-1} - a_n| + |a_n| = 1 + (a_1 - a_2) + \dots + (a_{n-1} - a_n) + a_n = 1 + a_1 = |-(a_1+1)|$

$r = 1 + \varepsilon$, $\varepsilon > 0$, $\Gamma = k(0, r)$, Rouché pro $f(z)(z-1)$ a $g(z) = -(a_1+1)x^n$

$z \in \Gamma \Rightarrow |z| = r$ $|f(z)(z-1) - g(z)| = |z^{n+1} + (a_1 - a_2) z^{n-1} + \dots + (a_{n-1} - a_n) z + a_n| \leq$

$\leq r^{n+1} + (a_1 - a_2) r^{n-1} + \dots + (a_{n-1} - a_n) r + a_n$

$|g(z)| = (a+1) r^n$

$|f(z)(z-1)| + |g(z)| - |f(z)(z-1) - g(z)| \geq |g(z)| - |f(z)(z-1) - g(z)| \geq (a+1) r^n - r^{n+1} - (a_1 - a_2) r^{n-1} - \dots - a_n = h(r)$

$h(1) = 0$

$h'(1) = n(a_1+1) - (n+1) - (n-1)(a_1 - a_2) - (n-2)(a_2 - a_3) - \dots - 1 \cdot (a_{n-1} - a_n) \geq$

$\geq n(a_1+1) - (n+1) - n(a_1 - a_2) - n(a_2 - a_3) - \dots - n(a_{n-1} - a_n) =$

$= n \cdot a_n - 1 > 0$ pro $n \geq 2$, případ $n = 1$ je triviální

$\varepsilon \to 0^+$: $f(z)(z-1)$ má n z těch $n-1$ kořenů s abs. hodnotou ≤ 1.

$|\alpha| = 1$, $f(\alpha)(\alpha - 1) = 0$: $|\alpha^{n+1} + (a_1 - a_2)\alpha^{n-1} + \dots + (a_{n-1} - a_n)\alpha + a_n| = |(a_1+1)\alpha^n|$

$a_1 + 1 = 1 + (a_1 - a_2) + \dots + (a_{n-1} - a_n) + a_n \geq a_1 + 1$

$\alpha^{n+1}, (a_1 - a_2)\alpha^{n-1}, \dots, (a_{n-1} - a_n)\alpha \in \mathbb{R}_0^+ \Rightarrow (a_1+1)\alpha^n \in \mathbb{R}_0^+ \Rightarrow \alpha^n \in \mathbb{R}_0^+ \Rightarrow \alpha = \frac{\alpha^{n+1}}{\alpha^n} \in \mathbb{R}_0^+$

$\Rightarrow \alpha = 1$

$n \geq 2 \Rightarrow h(1) < 0 \Rightarrow n-1$ z n kořenů $f(x)$ má abs. hodnotu < 1, spor

* $n \in \mathbb{N}, n \geq 2, a \in \mathbb{Z}, a \neq 0$, $f(x) = x^n + ax^{n-1} + \dots + ax - 1$. Dokažte, že $f(x)$ je ired.

$P(x) = f(x)(x-1) = x^{n+1} + (a-1)x^n - (a+1)x + 1$

(i) $a < 0$: $g(x) = (a-1)x^n$

$|z| = r = 1 + \varepsilon$: $|P(z)| + |g(z)| - |P(z) - g(z)| \geq |g(z)| - |P(z) - g(z)| \geq$

$\geq (|a|+1) r^n - r^{n+1} - (|a| - 1) r - 1 = h(r)$

$h(1) = 0$, $h'(1) = (n-1) \cdot |a| > 0$

$|\alpha| = 1$, $P(\alpha) = 0 \Leftrightarrow |\alpha^{n+1} - (a+1)\alpha + 1| = |-(a-1)\alpha^n|$

$|a| + 1 = 1 + |a| - 1 + 1 \geq |a| + 1$

$\alpha^{n+1} \in \mathbb{R}^+, -(a-1)\alpha^n \in \mathbb{R}^+ \Rightarrow \alpha = \frac{\alpha^{n+1}}{\alpha^n} \in \mathbb{R}^+ \Rightarrow \alpha = 1$, $f(1) = (n-1)a \neq 0$

(ii) $a > 0$: $g(z) = -(a+1) z$

$r = 1 - \varepsilon$, $\varepsilon > 0$, $|z| = r$

$$|f(z)(z-1)| + |g(z)| - |f(z)(z-1) - g(z)| \geq |g(z)| - |f(z)(z-1) - g(z)| \geq$$

$$\geq (a+1)u - u^{n+1} - (a-1)u^{n} - 1 = h(u)$$

$$h(1) = 0, \quad h'(1) = a(1-n) < 0$$

$\varepsilon \to 0^{+} \Rightarrow f(z)(z-1)$ má 1 kořen s abs. hodnotou < 1.

$$|\alpha| = 1, \ \cancel{E(\alpha) +} f(\alpha)(\alpha - 1) = 0 \Rightarrow a+1 = |(a+1)\alpha| \leq |\alpha^{n+1}| + |(a-1)\alpha^{n}| + |1| = a+$$

$$(a+1)\alpha \in \mathbb{R}^{+} \Rightarrow \alpha \in \mathbb{R}^{+} \Rightarrow \alpha = 1$$

- značení $F(x) = a_n x^n + \dots + a_0, \ a_n \neq 0$

  $\tilde{F}(x) = a_0 x^n + \dots + a_n$

~~Týká se to další poznámka~~

- $a_0 = F(0) \neq 0 \Rightarrow \tilde{\tilde{F}}(x) = F(x)$

- $\tilde{F}(x) = F\left(\frac{1}{x}\right) \cdot x^n$

  $\widetilde{FG}(x) = \tilde{F}(x) \cdot \tilde{G}(x)$

- pokud $F(0) \neq 0$, tak F je ired $\iff \tilde{F}$ je ired

* př. $\forall n \in \mathbb{N}$ mají polynomy $(3x^2+7x+2)^n$ a $(6x^2+5x+1)^n$ stejné součty druhých mocnin koeficientů

$f(x) \cdot \tilde{f}(x)$ ... koeficient u x^n je $\sum_{i=0}^{n} a_i^2$

$3x^2 + 7x + 2 = f(x)$

$6x^2 + 5x + 1 = g(x)$

$$\left.\begin{array}{l} f(x) = (3x+1)(x+2) \\ g(x) = (3x+1)(2x+1) \end{array}\right\} \quad f(x) \cdot \tilde{f}(x) = (3x+1)(x+2)(x+3)(2x+1) = g(x) \cdot \tilde{g}(x)$$

$$f^n \cdot \widetilde{f^n}(x) = f^n(x) \cdot \tilde{f}^n(x) = (f(x) \cdot \tilde{f}(x))^n = (g(x) \cdot \tilde{g}(x))^n$$

- $f(x) \mid g(x) \iff \tilde{f}(x) \mid \tilde{g}(x)$

  $f(0) \neq 0 \neq g(0)$

- $(\tilde{f}(x), \tilde{g}(x)) = c \cdot \widetilde{(f(x), g(x))}, \quad c \in \mathbb{C} \setminus \{0\}$

- $f(x) \in \mathbb{Z}[x], \ f(x) \neq 0$

  $f(x) = c \cdot q_1(x) \cdots q_k(x)$, $q(x)$ ired, primitivní, jednoznačný rozklad

  $c \in \mathbb{Z} \setminus \{0\}$

  tohle lze definovat gcd

– ~~reciproký~~ (kladně) reciproký polynom $\tilde{f}(x)=f(x)$

$$x^n\cdot f\left(\frac{1}{x}\right)=f(x)$$

$x=-1$: $(-1)^n f(-1)=f(-1) \xRightarrow{n \text{ liché}} f(-1)=0$

– záporně reciproký polynom: $\tilde{f}(x)=-f(x)$

$x^n\cdot f\left(\frac{1}{x}\right)=-f(x)$

$x=1$: $f(1)=-f(1) \Rightarrow f(1)=0$

$x=-1$: n sudé $\Rightarrow f(-1)=0$

$$\frac{1}{x^{n/2}}\cdot f(x)=h\left(x+\frac{1}{x}\right)$$

– $f(0)\neq 0$, $c\in\mathbb{C}\setminus\{0\}$ $\quad \tilde{f}(x)=c\cdot f(x)$

$a_0=c\cdot a_n$

$a_n=c\cdot a_0$

$a_0\cdot a_n=c^2\cdot a_n\cdot a_0$

$c^2=1$

$c=\pm 1$

– lemma: a) $f(x), g(x)\in\mathbb{Q}[x]$, $f(0)\neq 0\neq g(0)$, $\tilde{g}(x)=\pm g(x)$

Pak $g(x)\mid f(x) \iff g(x)\mid (f(x),\tilde{f}(x))$

b) $f(x)$ má nekonstantní ~~faktor~~ $\pm$ reciproký faktor $\iff (f(x),\tilde{f}(x))\neq 1$ (norm.)

– důkaz: a) "$\Rightarrow$" $g(x)\mid f(x) \Rightarrow \pm g(x)=\tilde{g}(x)\mid\tilde{f}(x) \Rightarrow g(x)\mid\tilde{f}(x)$

"$\Leftarrow$" zřejmý

b) "$\Rightarrow$" $h(x)$ nekonst. $\tilde{h}(x)=\pm h(x)$, $h(x)\mid f(x) \overset{a)}{\Rightarrow} h(x)\mid(f(x),\tilde{f}(x)) \Rightarrow (f(x),\tilde{f}(x))$ nekonst.

"$\Leftarrow$" ~~$(\widetilde{f(x),\tilde{f}(x)})=c\in\mathbb{Q}\setminus\{0\}$~~

$(\widetilde{f(x),\tilde{f}(x)})=\underset{\mathbb{Q}\setminus\{0\}}{c}\cdot(\tilde{f}(x),f(x))=c\cdot(f(x),\tilde{f}(x)) \Rightarrow (f(x),\tilde{f}(x))$ je reciproký faktor $f(x)$

– $f(x)\in\mathbb{Z}[x]$, $f(0)\neq 0$

$S_f=\{g(x)\in\mathbb{Z}[x] \mid f(x)\cdot\tilde{f}(x)=g(x)\cdot\tilde{g}(x)\}$

$\pm f(x), \pm\tilde{f}(x)\in S_f$

$f(x)=f_1(x)\cdot f_2(x) \Rightarrow f_1(x)\cdot\tilde{f}_2(x)\in S_f$

$f_1(x)\cdot\tilde{f}_2(x)=\pm f(x)=\pm f_1(x)\cdot f_2(x)$

$\tilde{f}_2(x)=\pm f_2(x)$

$f_1(x)\cdot\tilde{f}_2(x)=\pm\tilde{f}(x) \quad f_1(x)=\pm\tilde{f}_1(x)$

- důsledek 1: $f(x) \in \mathbb{Z}[x]$, $f(0) \neq 0$,

$$S_f = \{\pm f(x), \pm \tilde{f}(x)\} \qquad |S_f| \leq 4$$

Pokud $f(x) = f_1(x) \cdot f_2(x)$, pak $f_1(x)$ nebo $f_2(x)$ je reciproký

- důsledek 2: $f \in \mathbb{Z}[x]$, $f(x) \neq 0$, $S_f = \{\pm f(x), \pm \tilde{f}(x)\}$

$(f, \tilde{f}) = \text{konst.} \Rightarrow f$ je ired.

- důsledek 3: $f \in \mathbb{Z}[x]$, $f(0) \neq 0$, $S_f = \{\pm f(x), \pm \tilde{f}(x)\}$, $(f(x), \tilde{f}(x))$ je nekonst. ired nad $\mathbb{Z}$.

Pak $\dfrac{f(x)}{(f(x), \tilde{f}(x))}$ je ired. nad $\mathbb{Z} \Longrightarrow f(x) = (f(x), \tilde{f}(x)) \cdot \dfrac{f(x)}{(f(x), \tilde{f}(x))}$

- důkaz: $p(x)$ je nekonst. ired. $p(x) \mid \dfrac{f(x)}{(f(x), \tilde{f}(x))}$. Pak $p(x)$ není recip.

Kdyby $p(x)$ byl recip. $\Rightarrow p(x)(f(x), \tilde{f}(x))$ je recip $\Rightarrow p(x)(f(x), \tilde{f}(x)) \mid (f(x), \tilde{f}(x)) \Rightarrow p(x)$
$= \text{spor}$

$f(x) = p(x) \cdot \dfrac{f(x)}{p(x)} \Rightarrow \dfrac{f(x)}{p(x)}$ je recip. $\Rightarrow \dfrac{f(x)}{p(x)} \Big| (f(x), \tilde{f}(x)) \Rightarrow f(x) \mid p(x)(f(x), \tilde{f}(x))$

□

* $n \in \mathbb{N} \setminus \{1\}$, $f(x) = x^n - x - 1$ (Artin-Schreierův polynom) je ireducibilní

Nechť $g(x) \in \mathbb{Z}[x]$: $g(x) \cdot \tilde{g}(x) = f(x) \cdot \tilde{f}(x)$
$g(0) \neq 0$

tedy $g(x) = \pm x^n \pm x^k \pm 1$, $1 \leq k \leq n-1$

~~koef. u x^{n+k} v $g(x)\tilde{g}(x)$ bude~~ $\tilde{g}(x) = \pm x^n \pm x^{n-k} \pm 1$

$$g(x) \cdot \tilde{g}(x) = \pm x^{2n} \pm x^{n+k} \pm x^{2n-k} + 3x^n \pm x^{n-k} \pm x^k \pm 1$$

$$\tilde{f} = -x^n - x^{n-1} + 1$$

$$f(x)\tilde{f}(x) = -x^{2n} - x^{2n-1} + x^{n+1} + 3x^n$$

$n+k = 2n-1 \iff k = n-1$
$2n-k = 2n-1 \iff k = 1$

tedy $S_f = \{\pm f(x), \pm \tilde{f}(x)\}$

$h(x) \mid f(x) \wedge h(x) \mid \tilde{f}(x) \Rightarrow h(x) \mid (f(x) + \tilde{f}(x)) = -(x^{n-1} + x) \Rightarrow h(x) \mid x^n + x^2 =$
$\Rightarrow h(x) \mid x^2 + x + 1$

* $-||-$ $f(x) = x^n + x + 1$ $\qquad \omega = e^{\frac{2\pi i}{3}}$ $f(\omega) = 0 \Rightarrow \omega^n = \omega + 1$

S_f se ukáže úplně stejně

$\tilde{f}(x) = x^n + x^{n-1} + 1$

$h(x) \mid (f(x), \tilde{f}(x)) \Rightarrow h(x) \mid (\tilde{f}(x) - f(x)) = x^{n-1} - x \Rightarrow h(x) \mid (x^n - x^2 - f(x)) = -(x^2 \ldots$

$f(\omega) = 0$
$\omega^n = -\omega - 1$
$\omega^n = \omega^2$
$n \equiv 2 \pmod 3$

$$x^n + x + 1 = \begin{cases} (x^2+x+1) \cdot \dfrac{x^n+x+1}{x^2+x+1} & n \equiv 2 \pmod 3 \\ \text{je ired.} & n \not\equiv 2 \pmod 3 \end{cases}$$

* $x^n+x-1 = f(x)$

$$f(-x) = (-1)^n x^n - x - 1 = \begin{cases} x^n - x - 1 & 2\mid n \\ -(x^n+x+1) & 2\nmid n\end{cases}$$

$$x^n+x-1 \begin{cases} \text{ired. pro } n \not\equiv 5 \pmod 6 \\ (x^2-x+1)\cdot\frac{x^n+x-1}{x^2-x+1} \quad \text{pro } n\equiv 5 \pmod 6\end{cases}$$

* $x^n - x + 1$

analogicky lze rozložit právě pro $n \equiv 2 \pmod 6$

* Dokažte (jiným způsobem), že $f(x)=x^n\pm(x+1)$ jsou ireducibilní $n\geq 3$.

$f(\alpha)=0$

$\alpha = re^{i\varphi}$

$\alpha^n = r^n(\cos(n\varphi)+i\sin(n\varphi))$

$\alpha^n = \mp(\alpha+1)$

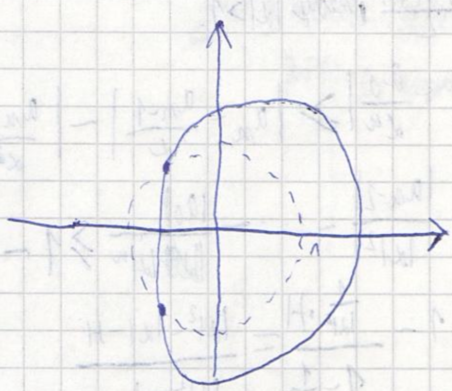
~~$|\alpha|^{n} = |\alpha+1|^2$~~

$|\alpha|^{2n} = |\alpha+1|^2$

$r^{2n} = (r\cos\varphi+1)^2 + (r\sin\varphi)^2 = r^2+2r\cos\varphi+1$

$\cos\varphi = \frac{r^{2n}-r^2-1}{2r} = \frac{r^{2n-1}}{2} - \frac{r}{2} - \frac{1}{2r} =: h(r)$

$h'(r) = \frac{2n-1}{2}\cdot r^{2n-2} - \frac{1}{2} + \frac{1}{2r^2} > 0$ pro $r>0$, tedy h je rostoucí



$\alpha_1,\dots,\alpha_k$ kořeny polynomu $p(x)$ stupně

$$S(p(x)) = \sum_{i=1}^{k} \left(\alpha_i - \frac{1}{\alpha_i}\right) = -\frac{a_{n-1}}{a_n} + \frac{a_1}{a_0}$$

$p(x)\in\mathbb{R}[x] \implies S(p(x))\in\mathbb{R}$

$S(p_1(x)\cdot p_2(x)) = S(p_1(x)) + S(p_2(x))$

$p(x)\in\mathbb{Z}[x] \wedge a_n, a_0\in\{-1,1\} \implies S(p(x))\in\mathbb{Z}$

$S(f(x)) = -\frac{0}{1} + \frac{\pm1}{\pm1} = 1$ $\quad f(x)=f_1(x)\cdot f_2(x)$

$$\underbrace{S(f_1(x))}_{\in\mathbb{Z}} + \underbrace{S(f_2(x))}_{\in\mathbb{Z}} = 1$$

$g(x) \mid f(x)$ $\quad g(x) \in \mathbb{Z}[x]$ $\quad \alpha_j = r_j e^{i\varphi_j}$

$$2S(g(x)) = S(g(x)) + \overline{S(g(x))} = \sum_{j=1}^{k}\left(\alpha_j + \bar{\alpha}_j - \frac{1}{\alpha_j} - \frac{1}{\bar{\alpha}_j}\right) = \sum_{j=1}^{k}\left(2r_j\cos\varphi_j - 2\cdot\frac{1}{r_j}\cos\varphi_j\right)$$

$$S(g(x)) = \sum_{j=1}^{k}\cos\varphi_j \cdot \frac{r_j^2-1}{r_j} = \sum_{j=1}^{k}\frac{r_j^{2n}-r_j^2-1}{2r_j}\cdot\frac{r_j^2-1}{r_j} = \sum_{j=1}^{k}\frac{r_j^{2n+2}-r_j^{2n}-r_j^4+1}{2r_j^2}$$

$$S(g(x)) = \frac{1}{2}\sum_{j=1}^{k}\left(r_j^{2n}-r_j^{2n-2}-r_j^2+\frac{1}{r_j^2}\right) \geq \frac{1}{2}\sum_{j=1}^{k}\left(-1+\frac{1}{r_j^2}\right) = \frac{1}{2}\left(\left(\sum_{j=1}^{k}\frac{1}{r_j^2}\right)-k\right) =$$

$$= \frac{k}{2}\left(\frac{\sum_{j=1}^{k}\frac{1}{r^2}}{k}-1\right) \geq \frac{k}{2}\left(\sqrt[k]{\prod \frac{1}{r_j^2}}-1\right) \geq 0 \quad \square$$

– $h(x) = f_1(x)\cdot f_2(x) \in \mathbb{Z}[x]$, c je prvočíslo, pak BÚNO $|f_1(c)| = 1$

$\alpha_1, \dots, \alpha_k$ kořeny $f_1(x)$

$$1 = |f_1(c)| = \left|\prod_{j=1}^{k}(c-\alpha_j)\right| = \prod_{j=1}^{k}|c-\alpha_j| \implies \text{nějaký kořen je „blízko" } c.$$

– Lemma 1: $f(x) \in \mathbb{Z}[x]$, $f(x) = a_n x^n + \dots + a_0$, $a_n \geq 1$, $a_{n-1} \geq 0$, $H > 0$, $|a_i| < H$ pro $i \in \{0, \dots, n-2\}$, $\alpha \in \mathbb{C}$, $f(\alpha) = 0$. Pak buď $\operatorname{Re}\alpha \leq 0$ nebo $|\alpha| < \frac{1+\sqrt{1+4H}}{2}$

– důkaz: sporem. Nechť $\operatorname{Re}\alpha > 0$ a $|\alpha| \geq \frac{1+\sqrt{1+4H}}{2}$, tedy $|\alpha| > 1$.

$$0 = \left|\frac{f(\alpha)}{\alpha^n}\right| = \left|a_n + \frac{a_{n-1}}{\alpha} + \frac{a_{n-2}}{\alpha^2} + \dots + \frac{a_0}{\alpha^n}\right| \geq \left|a_n + \frac{a_{n-1}}{\alpha}\right| - \left|\frac{a_{n-2}}{\alpha^2} + \dots + \frac{a_0}{\alpha^n}\right| \geq$$

$$\geq \operatorname{Re}\left(a_n + \frac{a_{n-1}}{\alpha}\right) - \frac{|a_{n-2}|}{|\alpha|^2} - \dots - \frac{|a_0|}{|\alpha|^n} \geq 1 - H\left(\frac{1}{|\alpha|^2} + \dots + \frac{1}{|\alpha|^n}\right) >$$

$$> 1 - H\cdot\sum_{j=2}^{\infty}\frac{1}{|\alpha|^j} = 1 - \frac{\frac{1}{|\alpha|^2}\cdot H}{1-\frac{1}{|\alpha|}} = \frac{|\alpha|^2-|\alpha|-H}{|\alpha|^2-\alpha}$$

tedy $|\alpha|^2 - |\alpha| - H < 0$, což ~~znamená~~ je spor. s $|\alpha| \geq \frac{1+\sqrt{1+4H}}{2}$

– Lemma 2: $f(x) = x^n + \dots + a_0$, $a_i \in \{0,1\}$, $i \in \{0, \dots, n-1\}$, $\alpha \in \mathbb{C}$, $f(\alpha) = 0$. Pak $\operatorname{Re}\alpha < \frac{3}{2}$.

– důkaz: sporem, nechť $\operatorname{Re}\alpha \geq 3/2$, tedy $|\alpha| \geq 3/2 > 1$

$$0 = \left|\frac{f(\alpha)}{\alpha^n}\right| = \left|1 + \frac{a_{n-1}}{\alpha^1} + \frac{a_{n-2}}{\alpha^2} + \dots + \frac{a_0}{\alpha^n}\right| \geq \left|1 + \frac{a_{n-1}}{\alpha} + \frac{a_{n-2}}{\alpha^2}\right| - \left|\frac{a_{n-3}}{\alpha^3} + \dots + \frac{a_0}{\alpha^n}\right| \geq$$

$$\geq \dots > \left|1 + \frac{a_{n-1}}{\alpha} + \frac{a_{n-2}}{\alpha^2}\right| - \frac{1}{|\alpha|^2(|\alpha|-1)}$$

Pokud $|\arg\alpha| \leq \frac{\pi}{4}$, tak $\operatorname{Re}\frac{1}{\alpha^2} \geq 0$, tedy

$$0 \geq \operatorname{Re}\left(1 + \frac{a_{n-1}}{\alpha} + \frac{a_{n-2}}{\alpha^2}\right) - \frac{1}{|\alpha|^2(|\alpha|-1)} \geq 1 - \frac{1}{|\alpha|^2(|\alpha|-1)} \geq 1 - \frac{1}{\left(\frac{3}{2}\right)^2\left(\frac{3}{2}-1\right)} = \frac{1}{9}$$

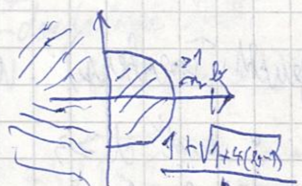
Pokud $|\arg \alpha| > \frac{\pi}{4}$, lemma 1 $\Longrightarrow |\alpha| < \frac{1+\sqrt{5}}{2}$

$$2(\mathrm{Re}\,\alpha)^2 < (\mathrm{Re}\,\alpha)^2 + (\mathrm{Im}\,\alpha)^2 < \left(\frac{1+\sqrt{5}}{2}\right)^2$$

$$|\mathrm{Re}\,\alpha| < \frac{1+\sqrt{5}}{2\sqrt{2}} < \frac{3}{2}, \text{ spor.}$$

- Cohnovo kritérium: $f \in \mathbb{N}$, $b \geq 2$, $\underset{\text{prvočíslo}}{p} = \overline{p_n p_{n-1} \cdots p_0}_b = p_n b^n + \dots + p_0$, $p_i \in \{0, \dots, b-1\}$, $p_n \neq 0$
  - Pak $f(x) = p_n x^n + \dots + p_0$ je ired nad $\mathbb{Z}$.
  - důkaz:

    Pokud $b \geq 3$, pak $H = b-1$



$$\frac{1+\sqrt{1+4(b-1)}}{2} \leq b-1$$

$$\sqrt{1+4(b-1)} \leq 2b-3 \qquad p = f(b)$$

$$4(b-3)(b-1) \geq 0$$

Pokud $b=2$: sporem $f(x) = g(x) \cdot h(x)$

$p = f(2) \Longrightarrow$ BÚNO $|g(2)| = 1$

$|1-\alpha_i| < |2-\alpha_i|$

$\mathbb{Z} \ni |g(1)| < |g(2)| = 1$

$g(1) = 0$, spor.

- $\alpha \in \mathbb{N}$, $\alpha > 0$

  $R_\alpha(s) =$

- $R[x_1, x_2] = (R[x_1])[x_2]$
- K těleso $\Longrightarrow K[x]$ je okruh hlavních ideálů
- homogenní polynom
- $f(x) \in K[x]$
- $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ je absolutně ireducibilní, pokud je ireducibilní nad $\overline{K}$ (algebraický uzávěr)

  $x^2 - y \in \mathbb{Q}[x,y]$ je abs. ired., $x^2 + y^2 \in \mathbb{R}[x,y]$ není abs. ired.
  $\qquad = (x+iy)(x-iy)$

  $f(x,y) = a_n x^n + a_{n-1} x^{n-1} y + \dots + a_1 x y^{n-1} + a_0 y^n = a_n (x - \alpha_1 y) \cdots (x - \alpha_n y)$

* $f(x_1,x_2) = x_1^{n_1} + x_2^{n_2} \in \mathbb{C}[x_1,x_2]$ $n_1, n_2 \in \mathbb{N}$ nemá v $\mathbb{C}[x_1,x_2]$ násobné faktory

sporem $g(x_1,x_2)^2 \mid f(x_1,x_2)$, $\deg_{x_1} g \neq 0$

$$\mathbb{C}[x_1,x_2] = (\mathbb{C}[x_2])[x_1] \subseteq \mathbb{C}(x_2)[x_1]$$

$$\frac{df}{dx_1} = n_1 x_1^{n-1} \implies f(x_1,x_2) \text{ a } \frac{df}{dx_1}(x_1,x_2) \text{ nemají spol. kořen}$$

* $d \geq 3$, $n_1, \dots, n_d \in \mathbb{N}$, pak $f(x_1, \dots, x_d) = x_1^{n_1} + \dots + x_d^{n_d} \in \mathbb{C}[x_1, \dots, x_d]$ je (abs.) ired.

indukcí: $d=3$: $f(x_1,x_2,x_3) = x_1^{n_1} + (x_2^{n_2} + x_3^{n_3}) \in (\mathbb{C}[x_1,x_3])[x_1]$

indukční krok: lehký

- Věta (Ehrenfeucht, Tverberg): $d \in \mathbb{N}$, $f_1(x), \dots, f_d(x) \in \mathbb{C}[x]$, $\deg f_i \geq 1$.

  Pokud:
  - buď $d \geq 3$
  - nebo $d = 2$ a $\gcd(\deg f_1, \deg f_2) = 1$,

  pak $f(x_1, \dots, x_d) = f_1(x_1) + \dots + f_d(x_d)$ je abs. ired.

- e_i elementární symetrické polynomy
- $f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} + \dots + (-1)^n e_n$ má kořeny $x_1, \dots, x_n$.
- fundamentální věta o symetrických polynomech

* $$f(x_1, \dots, x_n) = \prod_{\substack{i,j=1 \\ i<j}}^{n} (x_j - x_i) = \begin{vmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ \vdots & & & \\ 1 & x_n & \dots & x_n^{n-1} \end{vmatrix}$$

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \operatorname{sgn}\sigma \cdot f(x_1, \dots, x_n).$$

* $$f(x_1, \dots, x_n) = \prod_{\substack{i,j=1 \\ i<j}}^{n} (x_j - x_i)^2$$

- Def. $f(x) \in R[x]$ s kořeny $x_1, \dots, x_n$, $n = \deg f$

$$D_f = a_n^{2n-2} \prod_{i<j} (x_j - x_i)^2 \quad \text{(diskriminant)}$$

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

$D_f \in \mathbb{C}[a_0, \dots, a_{n-1}]$ je abs. ired.

$$D_f(a_0, \dots, a_{n-1}) = \prod_{i<j} (x_j - x_i)^2$$

$$a_i = (-1)^{n-i} e_{n-i}$$

$$D_f((-1)^n e_n, \dots, -e_1) = \prod_{i<j} (x_i - x_j)^2$$

sporem: $D_g = g \cdot h$

$\nexists (t-1)^n$

atd.

* $x^3 + ax^2 + bx + c$

$x = t + d$

$$(t+d)^3 + a(t+d)^2 = t^3 + t^2(3d+a) + O_{t\to\infty}(t)$$

vsuvka: velké (malé) O,

$\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty}, a_n, b_n \in \mathbb{C}$

$a_n = O(b_n) \iff \exists K > 0\ \forall n \in \mathbb{N}$ dostatečně velké $: |a_n| \le K |b_n|$

př. $\sqrt{n^2+1} = O(n)$, protože $\frac{\sqrt{n^2+1}}{n} = \sqrt{1+\frac{1}{n^2}} \xrightarrow{n\to\infty} 1$

$a_n = o(b_n) \iff \lim_{n\to\infty} \frac{|a_n|}{|b_n|} = 0$

př. $n^{10000000} = o(e^n)$ (10 000 000 L'Hospitalů)

$a_n \sim b_n$ (asymptoticky ekviv.) $\lim_{n\to\infty} \frac{|a_n|}{|b_n|} = 1$

př. $\sqrt{n^2+1} \sim n$

~~$\pi(x) \sim \ln(x)$~~

$\pi(n) \sim \frac{n}{\ln(n)}$ PNT

$f(x) = O_{x_0}(g(x))$

$$\pi(x) \underset{x\to\infty}{\sim} \frac{x}{\ln x}$$

$$\boxed{\frac{x}{\ln x} \underset{x\to\infty}{\sim} \int_2^x \frac{dt}{\ln t}} = \int_2^x 1 \cdot \frac{dt}{\ln t} \overset{*}{=} \left[\frac{t}{\ln t}\right]_2^x + \int_2^x \frac{dt}{(\ln t)^2} = \frac{x}{\ln x} - \frac{2}{\ln 2} + \int_2^x \frac{dt}{(\ln t)^2}$$

Chceme ukázat $\int_2^x \frac{dt}{(\ln t)^2} = o\left(\int_2^x \frac{dt}{\ln t}\right)$

$\varepsilon > 0$: $K > 0$: $\frac{1}{\ln K} < \frac{\varepsilon}{2}$

$x > K$: $$\frac{\int_2^x \frac{dt}{(\ln t)^2}}{\int_2^x \frac{dt}{\ln t}} = \frac{\int_2^K \frac{dt}{(\ln t)^2} + \int_K^x \frac{dt}{(\ln t)^2}}{\int_2^K \frac{dt}{\ln t} + \int_K^x \frac{dt}{\ln t}} < \frac{\int_2^K \frac{dt}{(\ln t)^2} + \frac{\varepsilon}{2}\int_K^x \frac{dt}{\ln t}}{\int_2^K \frac{dt}{\ln t} + \int_K^x \frac{dt}{\ln t}} \to \frac{\varepsilon}{2}$$

$$\pi(x) - \frac{x}{\ln x} = O\left(\frac{x}{(\ln x)^2}\right)$$

$$\pi(x) - \int_2^x \frac{dt}{t} = O\left(\sqrt{x} \cdot \ln x\right) \quad \text{(hypotéza, ekviv. RH)}$$

$$3d + a = 0 \Rightarrow d = -\frac{a}{3}$$

$$t^3 + pt + q = 0$$

$$\alpha_1 + \alpha_2 + \alpha_3 = 0 \quad \text{(kořeny)} \qquad \alpha_3 = -\alpha_1 - \alpha_2$$

$$\Delta_f = (\alpha_2 - \alpha_1)^2 (\alpha_3 - \alpha_1)^2 (\alpha_3 - \alpha_2)^2 = (\alpha_2 - \alpha_1)^2 (-2\alpha_1 - \alpha_2)^2 (-\alpha_1 - 2\alpha_2)^2$$

$$p = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 =$$
$$= \alpha_1\alpha_2 + \cancel{0} - (\alpha_1 + \alpha_2)^2$$
$$q = \alpha_1\alpha_2\alpha_3 = \alpha_1\alpha_2(\alpha_1 + \alpha_2)$$

$$\Delta_f = \cancel{((\alpha_2 - \alpha_1)(2\alpha_1^2 + 5\alpha_1\alpha_2}$$
$$= (\alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2)(2\alpha_1^2 + 5\alpha_1\alpha_2 + 2\alpha_2^2)^2$$
$$= ((\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2)(2(\alpha_1 + \alpha_2)^2 + \alpha_1\alpha_2)^2$$
$$= (-3\alpha_1\alpha_2 - p)(3\alpha_1\alpha_2 - 2p)^2$$
$$= -(3\alpha_1\alpha_2 + p)(9(\alpha_1\alpha_2)^2 - 12\alpha_1\alpha_2 p + 4p^2)$$
$$= -(27(\alpha_1\alpha_2)^3 - 36(\alpha_1\alpha_2)^2 p + 12(\alpha_1\alpha_2)p^2 + 9(\alpha_1\alpha_2)^2 p - 12\alpha_1\alpha_2 p^2 + 4p^3)$$
$$= \cancel{0} - 27((\alpha_1\alpha_2)^3 - (\alpha_1\alpha_2)^2 p) - 4p^3 = -27q^2 - 4p^3$$
$$= -4p^3 - 27q^2$$

$$(\alpha_1 + \alpha_2)^2 = \cancel{p}\,(-\alpha_1\alpha_2\ \alpha_1\alpha_2 - p$$
$$q^2 = (\alpha_1 + \alpha_2)^2 (\alpha_1\alpha_2)^2 = (\alpha_1\alpha_2)^3 - p$$

- casus irreducibilis

$$* \quad \sqrt{a + ib} = \pm(c + id)$$
$$a + ib = c^2 - d^2 + 2icd$$
$$a = c^2 - d^2$$
$$b = 2cd$$
$$(c^2 + d^2)^2 = (c^2 - d^2)^2 + 4(cd)^2 = a^2 + b^2$$
$$c^2 + d^2 = \sqrt{a^2 + b^2}$$
$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2} \qquad \operatorname{sgn}(c) \cdot \operatorname{sgn}(d) = \operatorname{sgn}(b)$$
$$d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}$$

$$c+id = \pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} \pm i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$$

$$a+ib = r(\cos\varphi + i\sin\varphi)$$

$$c+id = \pm\sqrt{r}\left(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}\right)$$

$$\cos\frac{\varphi}{2} = \pm\sqrt{\frac{1+\cos\varphi}{2}}$$

$$\sin\frac{\varphi}{2} = \pm\sqrt{\frac{1-\sin\varphi}{2}}$$

$$r = \sqrt{a^2+b^2}$$

$$\cos\varphi = \frac{a}{\sqrt{a^2+b^2}}$$

$$\sin\varphi = \frac{b}{\sqrt{a^2+b^2}}$$

*př. $f(x) = 2x^3+6x^2+7x+c,\quad c\in\mathbb{C}$

Pro která c má $f(x)$ násobný kořen?

1. způsob: $f'(x) = 6x^2+12x+7 \longrightarrow$ kořeny $x_1, x_2 \Rightarrow f(x_i)=0$

2. způsob: $x = t-1$

$$\cancel{f(x)=}\ f(t) = 2t^3+t-3+c = 2\left(t^3+\frac{t}{2}-\frac{3}{2}+\frac{c}{2}\right)$$

$$D_f = -4\left(\frac{1}{2}\right)^3 - 27\left(\frac{c-3}{2}\right)^2 = 0$$

* $f(x) = x^3-x-1,\ p$ prvočíslo $\quad f(x)\in\mathbb{Z}/p[X]$

pro která p má $f(x)$ násobný kořen jako polynom nad $\mathbb{Z}/p$.

1. způsob: $f'(x) = 3x^2-1$

$p=3 \Rightarrow f'(x) = -1 = 2$ nemá kořen

$p\neq 3 \Rightarrow f'(x)=0 \Rightarrow 3x^3 = x$

$f(x)=0 \Rightarrow 3x^3 = 3x+3$

$\cancel{x=3x+3}\ x = 3x+3$

$\cancel{-x=3}\ 2x = -3 \quad \rightarrow p=2 \quad 1=0$

$p\neq 2$

$x = -3\cdot\frac{p+1}{2}$

$3(2x)^3 = 4(2x)$

$3\cdot(-3)^3 = 4(-3)$

$-81 = -12$

$69 = 0 \qquad p\mid 69 \Rightarrow p = 23$

2. způsob: $D_f = -23 \Rightarrow n = 23$

plastic number = reálný kořen tohoto polynomu

* $d \geq 3$, $A_1, \dots, A_{d+1}$ je simplex v $\mathbb{R}^d$

$\forall i \in \{1, \dots, d+1\}$, O_i je střed sféry opsané $A_1 \dots A_{i-1} A_{i+1} \dots A_{d+1}$

$\forall i$ p_i je přímka kolmá k $O_1 \dots O_{i-1} O_{i+1} \dots O_{d+1}$, $A_i \in p_i$

Dokažte, že všechny přímky mají společný bod nebo jsou rovnoběžné.

- důkaz: Nechť $O_1, \dots, O_{d+1}$ neleží v obecné poloze, pak p_i jsou rovnoběžné

Nechť $O_1, \dots, O_{d+1}$ leží v obecné poloze, Q je střed sféry opsané $O_1 \dots O_{d+1}$

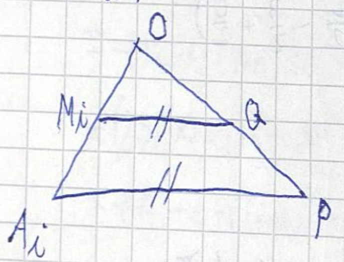
O ——— " ——— $A_1 \dots A_{d+1}$

~~Příklad~~ P je bod středově souměrný s O podle středu Q.

Nechť $i, j, k \in \{1, \dots, d-1\}$ po dvou různé.

Chceme dokázat, že $PA_i \perp O_j O_k$

M_i je střed OA_i.



$|M_i O_j| = |M_i O_k| = \frac{|OA_i|}{2}$ Thaletova věta

$M_i Q$ leží na ose úsečky $O_j O_k \Rightarrow M_i Q \perp O_j O_k$

$|\angle A_i O_j O| = 90^\circ$

$\Rightarrow A_i P \perp O_j O_k$

- Nechť $f(x_1, \dots, x_m, y_1, \dots, y_n) \in R[x_1, \dots, x_m, y_1, \dots, y_n]$ splňuje $\forall \sigma \in S_m, \forall \tau \in S_n$

$f(x_{\sigma(1)}, \dots, x_{\sigma(m)}, y_{\tau(1)}, \dots, y_{\tau(n)}) = f(x_1, \dots, x_m, y_1, \dots, y_n)$

pak $\exists g(z_1, \dots, z_m, w_1, \dots, w_n) \in R[z_1, \dots, z_m, w_1, \dots, w_n]: f(x_1, \dots, x_m, y_1, \dots, y_n) = g(e_{1,x}, \dots, e_{m,x}, e_{1,y}, \dots, e_{n,y})$

$a_m \neq 0 \neq b_n$

- $f(x) = a_m x^m + \dots + a_0$, $g(x) = b_n x^n + \dots + b_0 \in \mathbb{C}[x]$ s kořeny $\alpha_1, \dots, \alpha_m$, resp. $\beta_1, \dots, \beta_n$.
- Resultant polynomů f a g je: $\mathrm{Res}(f,g) = a_m^n \cdot b_n^m \cdot \prod_{i=1}^{m} \cdot \prod_{j=1}^{n} (\alpha_i - \beta_j)$
- $e_{i,\alpha} = (-1)^i \frac{a_{m-i}}{a_m}$, $e_{i,\beta} = (-1) \frac{b_{n-i}}{b_n}$
- př. $m=2, n=1$: $\mathrm{Res}(f,g) = a_2 \cdot b_1^2 (\alpha_1 - \beta_1)(\alpha_2 - \beta_1)$

$$= \alpha_1 \alpha_2 - (\alpha_1 + \alpha_2)\beta_1 + \beta_1^2$$

$$= a_2 b_1^2 \left(\frac{a_0}{a_2} \cancel{+} - \frac{a_1}{a_2} \cdot \frac{b_0}{b_1} + \left(\frac{b_0}{b_1}\right)^2 \right) = a_0 b_1^2 - a_1 b_1 b_0 + a_2 b_0^2$$

- $\mathrm{Res}(g,f) = (-1)^{mn} \mathrm{Res}(f,g)$
- $\mathrm{Res}(f,g) = a_m^n \cdot \prod_{i=1}^{m} g(\alpha_i)$ (protože $g(\alpha_i) = b_n(\alpha_i - \beta_1) \cdots (\alpha_i - \beta_n)$)
- př. $\mathrm{Res}(f, f') = ?$

$$\mathrm{Res}(f,f') = a_m^{m-1} \cdot \prod_{i=1}^{m} f'(\alpha_i) = a_m^{m-1} \cdot \prod_{i=1}^{m} \left(a_m \cdot \prod_{\substack{j=1 \\ j \neq i}}^{m} (\alpha_i - \alpha_j) \right) = a_m^{2m-1} \cdot \prod_{i \neq j} (\alpha_i - \alpha_j) =$$

$f(x) = a_m(x - \alpha_1) \cdots (x - \alpha_m)$

$f'(x) = a_m(x - \alpha_2) \cdots (x - \alpha_m) + \dots + a_m(x - \alpha_1) \cdots (x - \alpha_{m-1})$

$f'(x) = a_m(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_m)$

$$= (-1)^{\binom{m}{2}} \cdot a_m^{2m-1} \cdot \prod_{i<j} (\alpha_i - \alpha_j) = (-1)^{\binom{m}{2}} \cdot a_m \cdot D(f)$$

- Sylvestrova matice je $(m+n) \times (m+n)$ matice

$$\mathrm{Syl}(f,g) = \begin{array}{c} \\ \left(\begin{array}{cccccccc} a_m & a_{m-1} & \cdots & a_0 & \overbrace{0 & \cdots & 0}^{n-1} \\ 0 & a_m & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots \\ 0 & \cdots & 0 & a_m & \cdots & \cdots & a_0 \\ b_n & \cdots & b_1 & b_0 & \cdots & \cdots & 0 \\ \vdots \\ 0 & 0 & \cdots & 0 & b_n & \cdots & b_0 \end{array} \right) \end{array} \begin{array}{l} \left.\right\} n \\ \left.\right\} m \text{ řádků} \end{array}$$

- Věta: $\det \mathrm{Syl}(f,g) = \mathrm{Res}(f,g)$

- $Res(f,g) \in \mathbb{C}[a_0, \dots, a_m, b_0, \dots, b_n]$
- $Res(f,g) = 0 \iff f, g$ mají společný kořen
- Tvrzení: $|Syl(f,g)| = Res(f,g)$

$|Syl(f,g)| = \sum \pm a_{i_1} \cdots a_{i_n} b_{i_1} \cdots b_{i_m}$

tedy deg $Syl(f,g) = Res(f,g)$.

Nechť třeba $\alpha_1 = \beta_1$.

$$\cancel{f(x)(x-\beta_2)\cdots(x-\beta_n) - g(x)(x-\alpha_2)\cdots(x-\alpha_m) = 0}$$

$$f(x)\, \underbrace{b_n(x-\beta_2)\cdots(x-\beta_n)}_{c_{n-1}x^{n-1}+\dots+c_0} + g(x)\,\underbrace{(-a_m)(x-\alpha_2)\cdots(x-\alpha_m)}_{d_{m-1}x^{m-1}+\dots+d_0} = 0$$

$a_m c_{n-1} + b_n d_{m-1} = 0$

$a_{m-1} c_{n-1} + a_m c_{n-2} + b_{n-1} d_{m-1} + b_n d_{m-2} = 0$

$\vdots$

$(a_m\ 0 \dots b_n\ 0 \dots 0) \cdot (c_{n-1} \dots c_0\, d_{m-1} \dots d_0)$

$$Syl(f,g)^T \cdot \begin{pmatrix} c_{n-1} \\ \vdots \\ c_0 \\ d_{m-1} \\ \vdots \\ d_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\det(Syl(f,g)) = \det(Syl(f,g)^T) = 0$

$$Res(f,g) = a_m^n \cdot b_n^m \cdot \underbrace{h\left(\frac{a_0}{a_m}, \dots, \frac{a_{m-1}}{a_m}, \frac{b_0}{b_n}, \dots, \frac{b_{n-1}}{b_n}\right)}_{\parallel}$$

$$\prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$$

jeden člen, který nás zajímá:

$$\left(\prod_{j=1}^{n} (-\beta_j)\right)^m = \left(\frac{b_0}{b_n}\right)^m$$

- $f(x,y), g(x,y) \in \mathbb{C}[x,y] = (\mathbb{C}[y])[x] = (\mathbb{C}[x])[y]$

$\cap$

$\mathbb{C}(y)[x]$ ... rac. lomené fce

$Res_x(f(x,y), g(x,y))$,

$Res_y(f(x,y), g(x,y))$

$Res_x(f,g)=0 \iff$ f a g mají společný faktor nekonstantní v x v $\mathbb{C}[x,y]$

$Res_y(f,g)=0 \iff$ ——— " ——— y —— " ——

- řešení soustavy $f(x,y)=0$, $g(x,y)=0$

nechť (x_0,y_0) je řešení $\Rightarrow$ $f(x,y_0)$ a $g(x,y_0)$ mají spol. kořen x_0 $\Rightarrow$ y_0 je kořen $Res_x(f,g)$

analogicky x_0 je kořen $Res_y(f,g)$

- př. $f(x,y)=xy-2$

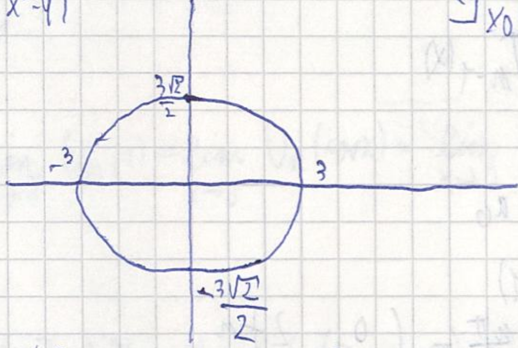
$g(x,y)=x^2+2y^2-9$

$$Res_x(f,g)=\begin{vmatrix} y & -2 & 0 \\ 0 & y & -2 \\ 1 & 0 & 2y^2-9 \end{vmatrix} = y^2(2y^2-9)+4 = 2y^4-9y^2+4 = (y^2-4)(2y^2-1) \neq 0$$

$\Rightarrow y_0 \in \{-2, 2, -\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\}$

$$Res_y(f,g) = \begin{vmatrix} x & -2 & 0 \\ 0 & x & -2 \\ 2 & 0 & x^2-9 \end{vmatrix} = x^4-9x^2+8 = (x^2-1)(x^2-8) \neq 0$$

$\Rightarrow x_0 \in \{-1, 1, 2\sqrt{2}, -2\sqrt{2}\}$



- $f(x), g(x) \in \mathbb{Z}[x]$. Pro která prvočísla p existuje $n \in \mathbb{Z}$: $f(n) \equiv g(n) \equiv 0 \pmod p$

nutná podmínka: $p \mid Res(f,g)$

protože víme $Res(f \bmod p, g \bmod p) = Res(f,g) \bmod p$

- př. $n=5$, $f(x)=5x$, $g(x)=5x+1 \Rightarrow Res(f,g) = \begin{vmatrix} 5 & 0 \\ 5 & 1 \end{vmatrix} = 5$, tedy to není postačující podmínka

- $f(x) = a_m x^m + \dots + a_0$

homogenizace: $f(x,y) = a_m x^m + a_{m-1}x^{m-1}y + \dots + a_1 x y^{m-1} + a_0 y^m$

$f([x,1]) = f(x)$

$f([1,0]) = a_m$

- Čebyševovy polynomy

$n \in \mathbb{N}$: jak vyjádřit $\cos(nx)$ pomocí $\cos x$?

$$\cos nx = \frac{(\cos nx + i \sin nx) + (\cos nx - i \sin x)}{2} = \frac{(\cos x + i \sin x)^n + (\cos x - i \sin x)^n}{2} =$$

$$= \frac{1}{2}\left(\sum_{j=0}^{n} i^{j}\binom{n}{j}\cos^{n-j}x \sin^{j}x + \sum_{j=0}^{n}(-i)^{j}\binom{n}{j}\cos^{n-j}x\sin^{j}x\right) =$$

$$= \sum_{j=0}^{[n/2]} i^{2j}\binom{n}{2j}\cos^{n-2j}x\sin^{2j}x = \sum_{j=0}^{[n/2]}(-1)^{j}\binom{n}{2j}\cos^{n-2j}x\,(1-\cos^2 x)^{j} = T_n(\cos x) \ldots$$ n-tý Čebyševův p. 1. druhu

$$T_n(x) = \sum_{k=0}^{[n/2]}(-1)^k\binom{n}{2k}x^{n-2k}(1-x^2)^k$$

$\forall_0 \; \forall$

$T_0(x)=1$

$T_1(x)=x$

$$T_{n+1}(\cos x)+T_{n-1}(\cos x) = \cos((n+1)x)+\cos((n-1)x) = 2\cdot\cos nx\cdot\cos x = 2\cdot T_n(\cos x)\cdot\cos x$$

$$T_{n+1}(x)+T_{n-1}(x) = 2x\cdot T_n(x)$$

$$T_{n+1}(x) = 2x\,T_n(x) - T_{n-1}(x)$$

$\deg T_n(x) = n$

$T_n(x) = a_n x^n + \ldots + a_0$

$a_n = 2^{n-1} \quad (n\geq 1)$

$$T_n(0) = a_0 = \cos\frac{n\pi}{2} = \begin{cases} 0 & 2\nmid n \\ (-1)^{n/2} & 2\mid n\end{cases}$$

$T_n(1) = 1$

$- n\in\mathbb{N}_0, \; U_n(x)\in\mathbb{R}[x]$.

$\sin((n+1)x) = \sin x\cdot U_n(\cos x)$

$U_n \ldots n$-tý Čeb. polynom 2. druhu

$$\sin((n+1)x) = \frac{(\cos x + i\sin x)^{n+1} - (\cos x - i\sin x)^{n+1}}{2i} = \frac{1}{i}\cdot\sum_{k=0}^{[\frac{n+1}{2}]}\binom{n+1}{2k+1}(i\sin x)^{2k+1}\cos^{n-2k}x$$

$$= \sum_{k=0}^{[\frac{n}{2}]}(-1)^k\cdot\binom{n+1}{2k+1}\sin^{2k+1}x\cdot\cos^{n-2k}x = \sin x\cdot\sum_{k=0}^{[\frac{n}{2}]}(-1)^k\cdot\binom{n+1}{2k+1}(1-\cos^2 x)^k(\cos^{n-2k}x)$$

$$U_n(x)=\sum_{k=0}^{[\frac{n}{2}]}(-1)^k\binom{n+1}{2k+1}x^{n-2k}(1-x^2)^k$$

$U_0(x)=1,\quad U_1(x)=2x$

$$\sin((n+2)x)+\sin(nx)=2\cdot\sin((n+1)x)\cdot\cos x$$

$$\sin x\cdot U_{n+1}(\cos x)+\sin x\, U_{n-1}(\cos x)=2\cdot\sin x\cdot U_n(\cos x)\cdot\cos x$$

$$U_{n+1}(x)+U_{n-1}(x)=2x\cdot U_n(x)$$

$$U_{n+1}(x)=2x\,U_n(x)-U_{n-1}(x)$$

$\deg U_n(x)=n$

$a_n=2^n$

$$U_n(0)=a_0=\sin\frac{(n+1)\pi}{2}=\begin{cases}0 & 2\nmid n\\ (-1)^{\frac{n}{2}}& 2\mid n\end{cases}$$

$U_n(1)=n+1$

$$U_n(1)=\lim_{x\to1}U_n(x)=\lim_{x\to0}U_n(\cos x)=\lim_{x\to0}\frac{\sin((n+1)x)}{\sin x}\overset{L'H}{=}n+1$$

- $C([0,2\pi])$ – spoj. fce $[0,2\pi]\to\mathbb{R}$. $f,g\in C([0,2\pi])$.

$$(f,g)=\int_0^{2\pi}f(x)\cdot g(x)\,dx\quad\ldots\text{ skal. součin}$$

$$(f,g)=(g,f)$$

$$(af_1+bf_2,g)=a(f_1,g)+b(f_2,g)$$

$$(f,f)=\int_0^{2\pi}f^2(x)\,dx\geq0$$

$$(f,f)=0\iff f(x)=0$$

- Tvrzení: Systém fcí $\cos nx,\sin nx$, $n\in\mathbb{N}_0$ je ortogonální vzhledem k $(\ ,\ )$.

- důkaz: 1) $m\neq n\in\mathbb{N}_0$

$$(\cos mx,\cos nx)=\int_0^{2\pi}\cos mx\cos nx\,dx=\frac12\left(\int_0^{2\pi}\cos((m+n)x)\,dx+\int_0^{2\pi}\cos((m-n)x)\,dx\right)=$$
$$=\frac12\left(\left[\frac{1}{m+n}\sin((m+n)x)\right]_0^{2\pi}+\left[\frac{1}{m-n}\cdot\sin((m-n)x)\right]_0^{2\pi}\right)=0$$

$$f(x)=\sum_{n=0}^{\infty}(a_n \cos nx + b_n \sin nx)$$

$$(f(x),\cos kx)=\sum_{n=0}^{\infty}\left(a_n(\cos nx,\cos kx)+b_n(\sin nx,\cos kx)\right)=a_k(\cos kx,\cos kx)=\begin{cases}\pi a_k & k\ldots\\ 2\pi a_k & k=\ldots\end{cases}$$

$m\neq n\in\mathbb{N}_0$

$$0=\int_0^{2\pi}T_m(\cos x)\cdot T_n(\cos x)\,dx=\int_0^{\pi}T_m(\cos x)\cdot T_n(\cos x)\,dx+\cancel{\int_0^{\pi}T_m(\cos(x+\pi))\cdot T_n(\cos(x+\pi))\,dx}=$$

$$=\int_0^{\pi}T_m(\cos x)\cdot T_n(\cos x)\,dx+\cancel{\int_0^{\pi}T_m(-\cos x)\cdot T_n(-\cos x)\,dx}=\left|\begin{matrix}x=\arccos s\\ dx=\frac{-1}{\sqrt{1-s^2}}ds\end{matrix}\right|=$$

$$=-\int_1^{-1}T_m(s)\cdot T_n(s)\cdot\frac{1}{\sqrt{1-s^2}}\,ds+\cancel{\int_1^{-1}T_m(-s)\cdot T_n(s)\cdot\frac{1}{\sqrt{1-s^2}}\,ds}=$$

$$=\int_{-1}^{1}T_m(s)\cdot T_n(s)\cdot\frac{ds}{\sqrt{1-s^2}}$$

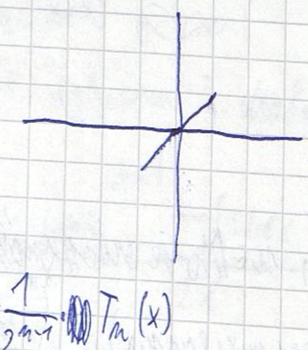
$f,g\in C[-1,1]$

$$(f,g)=\int_{-1}^{1}f(x)\cdot g(x)\cdot\frac{1}{\sqrt{1-x^2}}\,dx \quad \ldots \text{ skal. součin}$$

$(T_m,T_n)=0$. $T_m\perp T_n$, tj. $(T_m(x),T_n(x))$

* $\forall n\in\mathbb{N}$. Jaké je nejmenší možné $C>0$ takové, že $\exists$ normovaný polynom $f(x)\in\mathbb{R}[x]$, $\deg f=n$, takový, že $\forall x\in[-1,1]$ platí $|f(x)|\leq C$

$n=1$: $f(x)=x$, $C=1$



odpověď: $C=\frac{1}{2^{n-1}}$, $f(x)=\frac{1}{2^{n-1}}\cdot T_n(x)$