Algebra V

Tomáš Mrkvička mrkvicka@pf.jcu.cz

15. prosince 2003

Literatura

J. Vysoká: Algebra III. Č.B. 1997

P. Tlustý: Algebra II. Č.B. 1995

V. Kořínek: Základy algebry, Academia Praha, 1956

Opakování základních definic algebry

$(M, \circ)$: Algebraická struktura s binární operací $a \circ b$.
Grupoid: $(M, \circ)$, M je uzavřená na $\circ$.
Pologrupa: grupoid, asociativní zákon.
Monoid: pologrupa, existence 1.
Grupa $(M, \circ, 1, x^{-1})$: monoid, existence inverzního prvku x^{-1}.
Abelova grupa: grupa, komutativní zákon.
Př: Grupa všech rotací v $\mathbf{R_2}$,...

Těleso $(M, \star, \circ)$: Abelova grupa $(M, \star, 0, x_\star^{-1})$, grupa $(M \setminus \{0\}, \circ, 1, x_\circ^{-1})$, $(\star, \circ)$ distributivní zákon.
Komutativní těleso: $(M \setminus \{0\}, \circ, 1, x_\circ^{-1})$ jest komutativní grupa.
Př: $\mathbf{Q}, \mathbf{R}, \mathbf{C}$

Vektorový prostor nad tělesem T $(V, +, \cdot)$: Pro každá $u, v \in V, r \in T$ je $u + v \in V$ a $r \cdot u \in V$.

Okruh $(M, \star, \circ)$: Abelova grupa $(M, \star, 0, x_\star^{-1})$, monoid $(M, \circ, 1)$, $(\star, \circ)$ zleva i zprava distributivní.
Komutativní okruh: $(M, \circ, 1)$ jest komutativní monoid.
Př: $\mathbf{Z}$, Okruhy polynomů nad okruhem.

Obor integrity: komutativní okruh bez dělitelů 0.
Př: $\mathbf{Z}$, Okruh polynomů nad oborem integrity.

Gaussův obor integrity: obor integrity, kde existuje jednoznačný rozklad na ireducibilní prvky.
Př: $\mathbf{Z}$, Okruh polynomů nad Gaussovým oborem integrity nebo nad tělesem.

Ireducibilní rozklady polynomů v T[x]

T - libovolné těleso pak platí: Je-li $f(x)$ reducibilní, pak existují $g(x), h(x)$ takové, že $st\ f(x) > st\ g(x), st\ h(x) \geq 1$ a $f(x) = g(x)h(x)$.

Věta 1 *Nechť $f(x)$ je ireducibilní polynom v $T[x]$, $g(x)$ je libovolný polynom v $T[x]$. Potom platí bud' $NSD\{f(x), g(x)\} = 1$ nebo $f(x)|g(x)$ v $T[x]$.*

Věta 2 *Polynom $f(x) \in T[x]$ je ireducibilní polynom v $T[x]$, právě když platí implikace:*
Jestliže pro $\forall g(x) \in T[x]$ a $\forall h(x) \in T[x]$ platí $f(x)|g(x)h(x)$, pak $f(x)|g(x)$ nebo $f(x)|h(x)$.

Důsledek 1 *Polynom $f(x)$ nad T je ireducibilní v $T[x]$, právě když platí implikace:*
Jestliže $f(x)|g_1(x)g_2(x)\ldots g_k(x)$, kde $k \geq 1$, pak existuje index $i \in \{1, \ldots, k\}$ tak, že $f(x)|g_i(x)$ v $T[x]$.

Věta 3 *Každý polynom z $T[x]$ stupně alespoň 1 má za dělitele alespoň jeden ireducibilní polynom z $T[x]$.*

Věta 4 *Je-li T těleso, pak $T[x]$ je Gaussův obor integrity.*

Poznámka 1 $\mathbf{C}[x]$, $\mathbf{R}[x]$, $\mathbf{Q}[x]$, *mají vlastnosti existence a jednoznačnosti ireducibilního rozkladu.*

Věta 5 *Platí následující dvě tvrzení:*

1. *Každý polynom z $\mathbf{C}[x]$ stupně $n \geq 2$ je reducibilní v $\mathbf{C}[x]$.*
2. *Libovolný polynom $f(x) \in \mathbf{C}[x]$ stupně alespoň 1 má v $\mathbf{C}[x]$ (kanonický) rozklad ve tvaru:*

$$f(x) = a(x - \alpha_1)^{k_1} \ldots (x - \alpha_s)^{k_s}$$

kde $\alpha_i \neq \alpha_j$ pro $\forall i \neq j$, $k_1 + k_2 + \ldots + k_s = n$, $a \in \mathbf{C}$.

Věta 6 *Nechť* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *je reálný polynom. Je-li* $\beta = b_1 + ib_2$, $b_2 \neq 0$, *k-násobným kořenem polynomu* $f(x)$, *je zároveň číslo* $\overline{\beta}$ *k-násobným kořenem polynomu* $f(x)$ *(*$k \geq 1$*).*

Věta 7 *Každý polynom* $f(x)$ *stupně* $n \geq 1$ *lze nad* $\mathbf{R}$ *zapsat v součin ireducibilních prvků následovně:*

$$f(x) = a(x - \alpha_1) \ldots (x - \alpha_r)(x^2 + a_1 x + b_1) \ldots (x^2 + a_s x + b_s)$$

kde $a, \alpha_1, \ldots, \alpha_r, a_i, b_i \in \mathbf{R}$ *pro* $\forall i \in 1, \ldots, s$. *Polynomy* $x^2 + a_i x + b_i$ *pro* $\forall i \in 1, \ldots, s$ *mají za kořeny dvě čísla komplexně sdružená,* $n = r + 2s$.

Důsledek 2 *Jedinými iredubicilními polynomy nad* $\mathbf{R}$ *jsou polynomy stupně 1 a ty polynomy stupně* 2, *které mají pár komplexně sdružených kořenů. Je-li stupeň* $f(x) \in \mathbf{R}$ *liché číslo, pak má polynom* $f(x)$ *vždy alespoň jeden reálný kořen. Obecně: Tento polynom má vždy lichý počet reálných kořenů, je-li každý počítán ve své násobnosti.*

Ireducibilní rozklady polynomů v $\mathbf{Z}[x]$

Definice 1 *Polynom* $f(x) \in \mathbf{Z}[x]$ *ve tvaru:*

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

kde $f(x) \neq 0$ *se nazývá primitivní polynom, právě když* $NSD\{a_0, \ldots, a_n\}$*=1. V opačném případě budeme hovořit o neprimitivním polynomu.*

Příkladem primitivních polynomů v $\mathbf{Z}[x]$ jsou polynomy: $3x^4 - 6x^3 + 10x^2 - 2x - 4$, $x^6 - x^5 + 1$, zatímco polynomy 3, $6x^2 - 4x + 4$ primitivní nejsou.

Lemma 1 *Součin dvou primitivních polynomů ze* $\mathbf{Z}[x]$ *je opět primitivní polynom.*

Lemma 2 *Každý nenulový polynom* $f(x) \in \mathbf{Q}[x]$ *lze vyjádřit ve tvaru:*

$$f(x) = q f_p(x) \tag{1}$$

kde $q \in \mathbf{Q}$ *a* $f_p(x)$ *je primitivní polynom v* $\mathbf{Z}[x]$.

Lemma 3 *Jsou-li $f(x), g(x) \in \mathbf{Z}[x]$ primitivní polynomy, $a, b \in \mathbf{Z}$ a $af(x) = bg(x)$, pak $a \parallel b$ a $f(x) \parallel g(x)$.*

Věta 8 *Primitivní polynom $f(x) \in \mathbf{Z}[x]$, stupně alesoň 1 je ireducibilní v $\mathbf{Z}[x]$, právě když je ireducibilní v $\mathbf{Q}[x]$.*

Poznámka 2 *Všechna prvočísla jsou ireducibilní polynomy stupně 0 v $\mathbf{Z}[x]$. Všechna racionální čísla jsou ireducibilní polynomy stupně 0 v $\mathbf{Q}[x]$. V nenulové třídě asociovaných polynomů z $\mathbf{Q}[x]$ jsou právě 2 asociované a primitivní polynomy z $\mathbf{Z}[x]$.*

Věta 9 *$\mathbf{Z}[x]$ je Gaussův obor integrity.*

Věta 10 (o existenci NSD konečné množiny polynomů ze $\mathbf{Z}[x]$) *Nechť je dáno r polynomů $f_1(x), f_2(x), \ldots, f_r(x)$, kde $f_i(x) = a_i g_i(x)$ a $a_i \in \mathbf{Z}$ a $g_i(x)$ jsou primitivní polynomy v $\mathbf{Z}[x]$ pro $\forall i \in 1, \ldots, r$. Nechť d je největší společný dělitel čísel a_i a $\mathrm{D}(x)$ je největší společný dělitel polynomů $g_i(x)$ jakožto polynomů z $\mathbf{Q}[x]$. Pak $\mathrm{D}(x)$ můžeme volit tak, že to je primitivní polynom ze $\mathbf{Z}[x]$ a $\mathrm{dD}(x)$ je největší společný dělitel polynomů $f_1(x), f_2(x), \ldots, f_r(x)$ v $\mathbf{Z}[x]$.*

Poznámka 3 *Větu o existenci nejmenšího společného násobku bychom mohli vyslovit ekvivaltně jako v případě NSD.*

Poznámka 4 *$\mathrm{D}(x)$ jakožto NSD v $\mathbf{Q}[x]$ je určen jednoznačně až na násobek $\Rightarrow \exists\, \mathrm{D}(x)$ NSD v $\mathbf{Q}[x]$ takový že $\mathrm{D}(x)$ je primitivní polynom v $\mathbf{Z}[x]$.*

Věta 11 Eisensteinovo kritérium ireducibility. *Nechť $f(x)$ je primitivní polynom n-tého stupně ze $\mathbf{Z}[x]$ ve tvaru:*

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

a nechť existuje prvočíslo p tak, že současně platí:

1. *p nedělí a_n*

2. $p|a_i \, \forall i = 0, \ldots, n-1$

3. p^2 *nedělí* a_0

Potom je polynom $f(x)$ *ireducibilní v* $\mathbf{Z}[x]$ *(i v* $\mathbf{Q}[x]$*).*

Věta 12 *V* $\mathbf{Q}[x]$ *existují ireducibilní polynomy libovolných stupňů.*

Diskriminant

Definice 2 *Diskriminantem n neurčitých* $x_1, x_2 \ldots x_n$ *rozumíme polynom z* $I\,[x_1, x_2 \ldots x_n]$ *ve tvaru:*

$$D_n(x_1, x_2 \ldots x_n) = \prod_{1 \le i \le j \le n} (x_i - x_j)^2 \tag{2}$$

kde I je obor integrity popř. těleso.

Věta 13 *Označme:*

$$V_n(x_1, x_2 \ldots x_n) = \begin{vmatrix} 1 & 1 & \ldots & 1 & 1 \\ x_1 & x_2 & \ldots & x_{n-1} & x_n \\ x_1^2 & x_2^2 & \ldots & x_{n-1}^2 & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_{n-1}^{n-1} & x_n^{n-1} \end{vmatrix}$$

(tzv. Vandermondův determinant). Pak platí:

$$D_n(x_1, x_2 \ldots x_n) = V_n^2(x_1, x_2 \ldots x_n)$$

Důsledek 3 *Platí:*

$$D_n(x_1, x_2 \ldots x_n) = \begin{vmatrix} P_0 & P_1 & \ldots & P_{n-1} \\ P_1 & P_2 & \ldots & P_n \\ \vdots & \vdots & \vdots & \vdots \\ P_{n-1} & P_n & \ldots & P_{2n-2} \end{vmatrix}$$

kde $P_i = P_i(x_1, x_2 \ldots x_n) = x_1^i + x_2^i + \ldots + x_n^i, \;\; i = 1, \ldots, 2n-2, \;\; P_0 = n$

Příklad 1 *Spočtěte* $D_2(x_1, x_2)$.
Postup:

$$\begin{aligned} D_2(x_1,x_2) &= \begin{vmatrix} P_0 & P_1 \\ P_1 & P_2 \end{vmatrix} = P_0P_2 - P_1^2 \\ &= 2(\sigma_1^2 - 2\sigma_2) - \sigma_1^2 = \sigma_1^2 - 4\sigma_2 = (x_2 - x_1)^2 \end{aligned}$$

kde σ_1 *a* σ_2 *jsou elementární symetrické polynomy dvou neurčitých.*

Definice 3 *Nechť je dán polynom* $f(x) \in I[x]$ *ve tvaru*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,\ a_0 \neq 0,\ n \geq 1$$

Nechť $\alpha_1, \ldots, \alpha_n$ *jsou kořeny tohoto polynomu. Diskriminantem polynomu* $f(x)$ *resp. diskriminantem algebraické rovnice* $f(x) = 0$, *budeme rozumět výraz* $a_n^{2n-2} D_n(\alpha_1, \ldots, \alpha_n)$

$$a_2^2 D_2(\alpha_1, \alpha_2) = a_1^2 - 4a_0a_2$$

Diskriminanty polynomů v základním tvaru
$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$.

$$D_3(\alpha_1, \alpha_2, \alpha_3) = a_1^2a_2^2 + 18a_0a_1a_2 - 4a_0a_2^3 - 4a_1^3 - 27a_0^2$$

$$\begin{aligned} D_4(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \frac{1}{27}[4(12a_0 + a_2^2 - 3a_1a_3)^3 - \\ -(27a_1^2 - 72a_0a_2 + 2a_2^3 - 9a_1a_2a_3 + 27a_0a_3^2)^2] \end{aligned}$$

Lemma 4 $D_n(\alpha_1, \ldots, \alpha_n) \neq 0$, *právě když má příslušná algebraická rovnice vesměs jednoduché kořeny.*

Věta 14 *Nechť* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbf{R}[x], a_0 \neq 0, n \geq 1$, *má vesměs jednoduché kořeny. Pak její diskriminant je kladný (resp. záporný), právě když je počet párů komplexně sdružených kořenů polynomu* $f(x)$ *sudý (resp. lichý).*

Binomické rovnice

Definice 4 *Rovnice tvaru*

$$x^n - z = 0 \tag{3}$$

kde $z \in \mathbf{C}$, $z \neq 0$, $n > 0$, $n \in \mathbf{N}$, *se nazývá binomická rovnice. Kořeny rovnice* (3) *budeme nazývat n-té odmocniny z čísla z.*

$$z = r(\cos\varphi + i\sin\varphi),\ x = \rho(\cos\tau + i\sin\tau)$$

S využitím Moivreovy věty obdržíme

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

Pokud existuje n-tá odmocnina z čísla z, pak má tvar některého z čísel:

$$\sqrt[n]{r}(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}) \tag{4}$$

kde $k = 0, 1, \ldots, n-1$.

Poznámka 5 *Rovnice* (3) *má tedy pouze jednoduché kořeny, což plyne okamžitě z rovnice* $nx^{n-1} = 0$, *kterou získáme derivací levé strany rovnice* (3). *Symbolem* $\sqrt[n]{z}$ *tedy označujeme jedno z n řešení.*

Problém 1 *Platí*

$$\sqrt[n]{z_1}\sqrt[n]{z_2} = \sqrt[n]{z_1 z_2}\ ?$$

Příklad 2 *Vypočtěte všechny hodnoty symbolu* $\sqrt[n]{1}$.

Postup: $1 = \cos 0 + i\sin 0$, *pak hledané n-té odmocniny jsou tato čísla*

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

kde $k = 1, \ldots, n$. *Označíme-li*

$$\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

platí dle Moivreovy věty

$$\varepsilon^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

nebo-li n-té odmocniny z čísla 1 můžeme označit postupně

$$\varepsilon, \varepsilon^2, \ldots \varepsilon^n$$

kde $\varepsilon^n = 1$.

Příklad 3 *Vypočtěte všechny hodnoty symbolu* $\sqrt[3]{z}$,
kde $z = r(\cos\varphi + i\sin\varphi) \neq 0$.
Postup:
$z_1 = |\sqrt[3]{r}|(\cos\frac{\varphi}{3} + i\sin\frac{\varphi}{3})$,
$z_2 = |\sqrt[3]{r}|(\cos\frac{\varphi+2\pi}{3} + i\sin\frac{\varphi+2\pi}{3}) =$
$|\sqrt[3]{r}|(\cos\frac{\varphi}{3} + i\sin\frac{\varphi}{3})(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}) = z_1\varepsilon$,
$z_3 = |\sqrt[3]{r}|(\cos\frac{\varphi+4\pi}{3} + i\sin\frac{\varphi+4\pi}{3}) = z_1\varepsilon^2$.

Věta 15 *Nechť z je nenulové komplexní číslo. Nechť* $\sqrt[n]{z}$ *označuje libovolnou pevně zvolenou hodnotu tohoto symbolu. Potom všechny n-té odmocniny z čísla z jsou dány čísly*
$\sqrt[n]{z}, \varepsilon\sqrt[n]{z}, \varepsilon^2\sqrt[n]{z}, \ldots, \varepsilon^{n-1}\sqrt[n]{z}$, *kde* $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Definice 5 *Binomickou rovnici ve tvaru*

$$x^n - 1 = 0 \tag{5}$$

kde $n \geq 1$, *budeme nazývat rovnicí pro dělení kruhu.*

Problém 2 *Nalezněte 3.,4. a 5. odmocniny z jedné.*

Věta 16 *Druhá odmocnina z komplexního čísla* $a + ib$, $b \neq 0$, *má dvě hodnoty, lišící se pouze znaménkem a to*

a) pro $b > 0$

$$\pm\left[\sqrt{\frac{1}{2}\left(a + \sqrt{a^2+b^2}\right)} + i\sqrt{\frac{1}{2}\left(-a + \sqrt{a^2+b^2}\right)}\right]$$

b) pro $b < 0$

$$\pm\left[\sqrt{\frac{1}{2}\left(a+\sqrt{a^2+b^2}\right)}-i\sqrt{\frac{1}{2}\left(-a+\sqrt{a^2+b^2}\right)}\right]$$

Hodnoty symbolů odmocnin bereme vždy s kladným znaménkem.

Důkaz. Nechť je dáno koplexní číslo $a+bi$, $b \neq 0$. *Předpokládejme, že existují reálná čísla* c *a* d *tak, že platí:*

$$(c+id)^2 = a+bi.$$

Umocněním této rovnice a porovnáním reálných a imaginárních částí dostaneme

$$c^2 - d^2 = a,$$
$$2cd = b.$$

Úpravou těchto rovnic získáme

$$c^2 + (-d^2) = a,$$
$$c^2(-d^2) = -\frac{b^2}{4},$$

kde c^2 *a* $-d^2$ *jsou podle Vietových vztahů kořeny kvadratické rovnice ve tvaru*

$$x^2 - ax - \frac{b^2}{4} = 0.$$

Kořeny této rovnice jsou $x_{1,2} = \frac{1}{2}\left(a \pm \sqrt{a^2+b^2}\right)$. *Poněvadž* $x_1 = c^2 \geq 0$ *platí*

$$c^2 = \frac{1}{2}\left(a+\sqrt{a^2+b^2}\right),$$
$$-d^2 = \frac{1}{2}\left(a-\sqrt{a^2+b^2}\right).$$

Odtud

$$c = \pm\sqrt{\frac{1}{2}\left(a+\sqrt{a^2+b^2}\right)}$$
$$d = \pm\sqrt{\frac{1}{2}\left(-a+\sqrt{a^2+b^2}\right)}$$

□

Problém 3 *Nechť* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$, $a_0 \neq 0$ *je rovnice n-tého stupně,* $n \geq 0$.

a) Určete substituci za x tak, aby daná rovnice po zavedení této substituce přešla v rovnici n-tého stupně bez členu s (n-1). mocninou.

b) Zaveďte do dané rovnice substituci $x = \frac{y}{k}$, *kde k je nenulová reálná konstanta, a popište, jakou vlastnost budou mít kořeny získané rovnice vzhledem ke kořenům původní rovnice.*

c) Popište totéž v případě, že $x = \frac{1}{y}$.

Algebraická řešitelnost algebraických rovnic

Definice 6 *Prvek x nazveme racionálně vyjádřitelný pomocí prvků* $x_1, x_2, \ldots, x_k$ *z tělesa* T, *právě když lze x vyjádřit pomocí operací* $+, -, ., :$ *prováděných na prvky* $x_1, x_2, \ldots, x_k$.

Příklad 4 *Prvek* $x = \frac{x_1 + x_2 x_3}{x_3^3 - x_1}$ *je racionálně vyjádřitelný pomocí prvků* x_1, x_2, x_3 *ale prvek* $y = \frac{x_1 + x_2}{\sqrt{x_3 - x_2^2}}$ *není racionálně vyjádřitelný pomocí prvků* x_1, x_2, x_3.

Definice 7 *Nechť* $f(x)$ *je nenulový polynom nad tělesem* T *stupně alespoň 1. řekneme, že rovnice* $f(x) = 0$ *je algebraicky řešitelná, právě když existuje konečná posloupnost binomických rovnic*

$$\begin{aligned} y^{n_1} - b_1 &= 0, \\ y^{n_2} - b_2 &= 0, \\ &\vdots \\ y^{n_k} - b_k &= 0, \end{aligned} \tag{6}$$

taková, že

1) koeficienty i-té rovnice $b_i (i = 1, \ldots, k)$ *lze racionálně vyjádřit pomocí koeficientů polynomu* $f(x)$ *a řešení předcházejících rovnic v* (6)

2) *každé řešení rovnice* $f(x) = 0$ *lze racionálně vyjádřit pomocí koeficientů polynomu* $f(x)$ *a řešení rovnic* (6)

Posloupnost binomických rovnic (6) *budeme nazývat řetězem algebraické řešitelnosti rovnice* $f(x) = 0$.

Věta 17 *Každá algebraická rovnice stupně 2 je algebraicky řešitelná.*

Věta 18 *Kvadratická rovnice s reálnými koeficienty má*

1) *dva různé reálné kořeny, je-li její diskriminant* $D_2 > 0$,

2) *jeden dvojnásobný reálný kořen, je-li* $D_2 = 0$,

3) *pár komplexně sdružených kořenů, je-li* $D_2 < 0$.

Důsledek 4 *Každá algebraická rovnice 2n-tého stupně,* $n > 0$ *je algebraicky řešitelná.*

Věta 19 *Každá algebraická rovnice 3. stupně (kubická rovnice) je algebraicky řešitelná*

Důkaz. Nechť tedy máme kubickou rovnici ve tvaru

$$x^3 + a_2x^2 + a_1x + a_0 = 0.$$

Zavedeme substituci $x = y - \frac{a_2}{3}$, *pak zřejmě platí:*

$$y^3 + py + q = 0, \tag{7}$$

kde

$$p = a_1 - \frac{a_2^2}{3}, \qquad q = a_0 - \frac{a_1a_2}{3} + \frac{2a_2^3}{27}.$$

Zavedeme další substituci a to: $y = u + v$. *Dosazením do* (7) *dostaneme:*

$$(u+v)^3 + p(u+v) + q = \underbrace{u^3 + v^3 + q}_{=0} + \underbrace{(3uv + p)}_{=0 \Rightarrow uv = -\frac{p}{3}}(u+v) = 0$$

tedy

$$u^3v^3 = -\frac{p^3}{27}, \qquad u^3 + v^3 = -q.$$

To ale znamená, že u^3 a v^3 jsou kořeny, kvadratické rovnice, která má tvar:

$$z^2 + qz - \frac{p^3}{27} = 0.$$

Pro její kořeny platí

$$z_1 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \qquad z_2 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \tag{8}$$

z toho plyne:

$$\begin{array}{ll} u_1 = \sqrt[3]{z_1} & v_1 = \sqrt[3]{z_2}, \\ u_2 = \varepsilon\sqrt[3]{z_1} & v_2 = \varepsilon^2\sqrt[3]{z_2}, \\ u_3 = \varepsilon^2\sqrt[3]{z_1} & v_3 = \varepsilon\sqrt[3]{z_2} \end{array}$$

a zpětným dosazením do substituce dostáváme:

$$\begin{array}{ll} y_1 = u_1 + v_1 & \\ y_2 = \varepsilon u_1 + \varepsilon^2 v_1 & x_i = y_i - \frac{a_2}{3}, \quad \text{kde } i = 1, 2, 3. \\ y_3 = \varepsilon^2 u_1 + \varepsilon v_1 & \end{array}$$

Správné kombinace řešení u_i, v_j musí splňovat podmínku $u_iv_j = -p/3$.

řetězec algebraické řešitelnosti je tedy tvořen následující posloupností binomických rovnic:

$$\begin{array}{ll} u^2 - b_1 = 0 & \text{kde } b_1 = \frac{q^2}{4} + \frac{p^3}{27} \\ u^3 - z_1 = 0 & \\ u^3 - z_2 = 0 & \text{kde } z_1 \text{ a } z_2 \text{ jsou dány vztahem (8)} \end{array}$$

□

Definice 8 *Nechť je dána kubická rovnice $y^3 + py + q = 0$, pak její řešení lze nalézt pomocí tzv. Cardanových vzorců:*

$$\begin{array}{l} D_3 = -4p^3 - 27q^2 = (-108)\left(\frac{q^2}{4} + \frac{p^3}{27}\right) \\ y_1 = \sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}} \\ y_2 = \varepsilon\sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \varepsilon^2\sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}} \\ y_3 = \varepsilon^2\sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \varepsilon\sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}, \end{array}$$

Věta 20 *Kubická rovnice s reálnými koeficienty ve tvaru* $x^3 + px + q = 0$ *má:*
1) dvojnásobný kořen, je-li $D_3 = 0$
2) všechny kořeny reálné, je-li $D_3 > 0$
3) jeden kořen reálný a dva komplexně sdružené, je-li $D_3 < 0$.

Věta 21 *Nechť diskriminant rovnice* $x^3 + px + q = 0$ *s reálnými koeficienty je kladný. Pak kořeny této rovnice vypočteme následujícím způsobem. Nalezneme řešení goniometrické rovnice*

$$\cos t = -\frac{q}{2}\sqrt{\frac{27}{-p^3}}$$

ležící v intervalu $(0, \pi)$. *Hledané řešení je pak dáno vztahy:*

$$\begin{aligned} x_1 &= 2\sqrt{-\tfrac{p}{3}}\cos\tfrac{t}{3} \\ x_2 &= 2\sqrt{-\tfrac{p}{3}}\cos\tfrac{t+2\pi}{3} \\ x_3 &= 2\sqrt{-\tfrac{p}{3}}\cos\tfrac{t+4\pi}{3} \end{aligned}$$

kde druhá odmocnina z kladného čísla $-\frac{p}{3}$ *je kladné číslo.*

Věta 22 *Každá algebraická rovnice 4. stupně je algebraicky řešitelná.*

Důkaz. Nechť tedy máme algebraickou rovnici 4. stupně ve tvaru

$$z^4 + a_3 z^3 + a_2 z^2 + a_1 z + a_0 = 0. \tag{9}$$

Zavedeme substituci $z = x - \frac{a_3}{4}$, *pak zřejmě platí:*

$$x^4 + px^2 + qx + r = 0, \tag{10}$$

kde

$$p = a_2 - \frac{3}{8}a_3^2, \qquad q = a_1 - \frac{a_2 a_3}{2} + \frac{a_3^3}{8},$$
$$r = a_0 - \frac{1}{4}a_1 a_3 + \frac{1}{16}a_2 a_3^2 - \frac{3}{256}a_3^4.$$

Provedeme substituci $x = \frac{1}{2}(u+v+w)$ *a dostaneme, že* u^2, v^2, w^2 *jsou kořeny rovnice (kubické resolventy)*

$$t^3 + 2pt^2 + (p^2 - 4r)t - q^2 = 0$$

s podmínkou $uvw = -q$. *Označíme-li kořeny kubické resolventy* t_1, t_2, t_3 *dostaneme:*

$$\begin{array}{ll} x_1 = \frac{1}{2}(\sqrt{t_1} + \sqrt{t_2} + \sqrt{t_3}) & \\ x_2 = \frac{1}{2}(\sqrt{t_1} - \sqrt{t_2} - \sqrt{t_3}) & z_i = x_i - \frac{a_1}{4} \\ x_3 = \frac{1}{2}(-\sqrt{t_1} + \sqrt{t_2} - \sqrt{t_3}) & \\ x_4 = \frac{1}{2}(-\sqrt{t_1} - \sqrt{t_2} + \sqrt{t_3}) & \end{array} \tag{11}$$

□

Věta 23 *Diskriminant rovnice (10) je roven diskriminantu její kubické rezolventy.*

Věta 24 *Rovnice* (9) *má vícenásobný kořen, právě když má vícenásobný kořen kubická rezolventa příslušná k rovnici* (10).

Věta 25 *Nechť rovnice* (10), *kde* $q \neq 0$, *je rovnice s reálnými koeficienty s* $D_4 \neq 0$. *Pak platí:*

a) Je-li $D_4 < 0$,*pak rovnice* (10) *má dva reálné kořeny a jeden pár komplexně sdružených kořenů.*

b) Je-li $D_4 > 0$, $p < 0$, $p^2 - 4r > 0$, *pak má rovnice* (10) *čtyři různé reálné kořeny.*

c) Je-li $D_4 > 0$ *a podmínky v b) nejsou splněny, pak má rovnice dva páry komplexně sdružených kořenů.*

Poznámka 6 *Rovnice 5. a vyššího stupně nelze obecně algebraicky řešit.*

Definice 9 *Nechť je dán polynom* $f(x)$ *n-tého stupně,* $n > 0$, *ve tvaru*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \text{ kde } a_n \neq 0.$$

Jestliže pro koeficienty polynomu $f(x)$ platí následující vztahy:

$$\begin{aligned} a_0 &= a_n \\ a_1 &= a_{n-1} \\ a_2 &= a_{n-2} \\ &\vdots \\ a_k &= a_{n-k}, \end{aligned}$$

kde $k \leq \frac{n}{2}$, pak $f(x)$ nazveme reciprokým polynomem 1. druhu. Rovnici $f(x) = 0$ budeme analogicky nazývat reciprokou rovnicí 1. druhu.

Lemma 5 *Jestliže reciproká rovnice 1. druhu má kořen α, pak má rovněž kořen $\frac{1}{\alpha}$.*

Věta 26 *Každý reciproký polynom $f(x)$ 1. druhu lichého stupně n lze psát ve tvaru*

$$f(x) = (x+1)\, g(x)$$

kde polynom $g(x)$ je reciproký polynom 1. druhu sudého stupně $(n-1)$.

Tudíž se omezíme na polynomy sudého stupně.

$$f(x) = a_0 x^{2m} + a_1 x^{2m-1} + \ldots + a_1 x + a_0 = 0$$

$$f(x) = (a_0 x^{2m} + a_0) + (a_1 x^{2m-1} + a_1 x) + \ldots = 0$$

$$a_0(x^m + \frac{1}{x^m}) + a_1(x^{m-1} + \frac{1}{x^{m-1}}) + \ldots + a_{m-1}(x + \frac{1}{x}) + a_m = 0$$

$$y = x + \frac{1}{x}, \quad \text{pak} \quad y^2 - 2 = x^2 + \frac{1}{x^2},\ y^3 - 3y = x^3 + \frac{1}{x^3}, \ldots$$

$$b_0 y^m + b_1 y^{m-1} + \ldots + b_m = 0 \ \Rightarrow\ y_1, \ldots, y_m$$

$$x^2 - y_i x + 1 = 0, \text{ kde } i = 1, \ldots, m \ \Rightarrow\ x_1, \ldots, x_{2m}$$

Definice 10 *Polynom $f(x)$ nazveme reciprokým polynomem 2. druhu, jestliže pro jeho koeficienty platí:*

$$\begin{aligned} a_0 &= -a_n \\ a_1 &= -a_{n-1} \\ a_2 &= -a_{n-2} \\ &\vdots \\ a_k &= -a_{n-k}. \end{aligned}$$

Rovnici $f(x) = 0$ *pak nazveme reciprokou rovnicí 2. druhu.*

Poznámka 7 Lemma 5 *platí i pro reciproké polynomy 2. druhu.*

Věta 27 *Každý reciproký polynom* $f(x)$ *2. druhu lze psát ve tvaru*

$$f(x) = (x-1)\, g(x)$$

kde polynom $g(x)$ *je reciproký polynom 1. druhu.*

Problém 4 *Ukažte v jakém případě je algebraicky řešitelná rovnice ve tvaru:*

$$a_0 x^{mn} + a_1 x^{m(n-1)} + \ldots + a_{n-1} x^m + a_n = 0,$$

kde $m \geq 0$, $n \geq 1$ *a* $a_0 \neq 0$.

Interpolační polynomy

$x_0, x_1, \ldots, x_n$ jsou komplexní čísla
$y_0, y_1, \ldots, y_n$ jsou komplexní čísla
Hledejme polynom f tak, aby $f(x_0) = y_0, f(x_1) = y_1, \ldots, f(x_n) = y_n$.

Lagrangeův interpolační polynom:

$$\begin{aligned} f(x) &= y_0 \frac{(x-x_1)(x-x_2)\ldots(x-x_n)}{(x_0-x_1)(x_0-x_2)\ldots(x_0-x_n)} + \\ &+ y_1 \frac{(x-x_0)(x-x_2)\ldots(x-x_n)}{(x_1-x_0)(x_1-x_2)\ldots(x_1-x_n)} + \ldots + \\ &+ y_n \frac{(x-x_0)(x-x_1)\ldots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)\ldots(x_n-x_{n-1})} \end{aligned}$$

Newtonův interpolační polynom:

$$\begin{aligned} f(x) &= a_0 + a_1(x-x_0) + a_2(x-x_0)(x-x_1) + \ldots + \\ &+ a_n(x-x_0)(x-x_1)\ldots(x-x_{n-1}) \end{aligned}$$

Postupným dosazováním $x_0, x_1, \ldots, x_n$ vypočteme $a_0, a_1, \ldots, a_n$.

Faktorizace polynomů - Kroneckerův algoritmus

Algoritmus na určení reducibility či ireducibility polynomu $f(x)$ ze $Z[x]$.
1. Při hledání event. dělitele $g(x) \in Z[x]$ polynomu $f(x)$ se můžeme omezit na ty polynomy, jejichž stupeň je menší nebo roven celé části čísla $n/2$.
2. Vypočteme $s+1$ funkčních hodnot polynomu $f(x)$. V ilustračních příkladech budeme volit $x = 0, 1, ..., s$. Získáme celočíselné funkční hodnoty $f(0), f(1), \ldots, f(s)$.
3. Má-li dělit $g(x)$ polynom $f(x)$, musí funkční hodnota $g(0)$ dělit $f(0), g(1)$ dělit $f(1), ..., g(s)$ dělit $f(s)$. Utvořme tedy množiny $D_{f(0)}, ..., D_{f(s)}$ všech celočíselných dělitelů čísel $f(0), f(1), .., f(s)$. (Kdyby $f(k) = 0$ pro některé $k = 0, 1, ..., s$ bylo by číslo k kořenem polynomu $f(x)$ a $f(x) = x - k$ by byl kořenový činitel, čímž by byla naše úloha vyřešena.) Můžeme proto předpokládat, že $f(k) \neq 0$ pro všechna $k = 0, 1, ..., s$ a množiny $D_{f(k)}$ jsou tudíž konečné a neprázdné.
4. Pro každou $s+1$ -tici čísel $g(0) \in D_{f(0)}, g(1) \in D_{f(1)}, ..., g(s) \in D_{f(s)}$ nalezneme takový polynom $g(x)$, který nabývá v bodech $x = 0, 1, ..., s$ předepsaných hodnot $g(0), g(1), ..., g(s)$. (Pomocí např. Newtonova nebo Lagrangeova polynomu.)
5. Je=li $g(x)$ vskutku polynom s celočíselnými koeficienty,$1 \leq st\ g(x) \leq s$, pak otestujeme, zda v oboru integrity $Z[x]$ polynom $g(x)$ dělí $f(x)$. V kladném případě jsme úlohu vyřešili a získali jsme rozklad tvaru $f(x) = g(x).h(x), g(x) \in Z[x], h(x) \in Z[x], st\ g(x) > 0, st\ h(x) > 0$;,jinak se vrátíme k bodu 4 a celý postup opakujeme pro další $s+1$ -tici až do té doby, kdy jsou všechny tyto $s+1$ -tice vyčerpány. Poté můžeme konstatovat, že polynom f(x) je ireducibilní v $Z[x]$.

Numerické řešení rovnic

Některé vlastnosti reálných kořenů

Věta 28 *Všechny reálné kořeny algebraické rovnice stupně alespoň 1*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

s reálnými koeficienty leží v intervalu $(-A-1, A+1)$*, kde* $A = \max |a_0|, |a_1|, \ldots, |a_{n-1}|$.

Věta 29 *Mezi dvěma různými kořeny algebraické rovnice* $f(x) = 0$ *s reálnými koeficienty leží nejméně jeden kořen rovnice* $f'(x) = 0$.

Věta 30 *Je-li* $a < b$ *a platí-li pro funkční hodnoty* $f(a), f(b)$ *polynomu s reálnými koeficienty* $f(x)$ *vztah* $f(a)f(b) > 0$*, pak má rovnice* $f(x) = 0$ *v intervale* (a, b) *sudý počet kořenů (nebo žádný kořen). Platí-li* $f(a)f(b) < 0$*, pak má rovnice* $f(x) = 0$ *v intervale* (a, b) *lichý počet kořenů.*

Separace reálných kořenů

Věta 31 *Nechť* $a < b$ *a pro funkční hodnoty* $f(a), f(b)$ *polynomu s reálnými koeficienty* $f(x)$ *platí vztah* $f(a)f(b) < 0$*. Jestliže derivace* $f'(x)$ *nemění v intervale* (a, b) *znaménko, pak má rovnice* $f(x) = 0$ *v intervale* (a, b) *právě jeden reálný kořen.*

Věta 32 *Počet kladných kořenů rovnice*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, \quad a_n \neq 0, n \geq 1$$

s reálnými koeficienty je stejné parity jako počet znaménkových změn v této rovnici.

Věta 33 *(Descartesova) Rovnice*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, \quad a_n \neq 0, n \geq 1$$

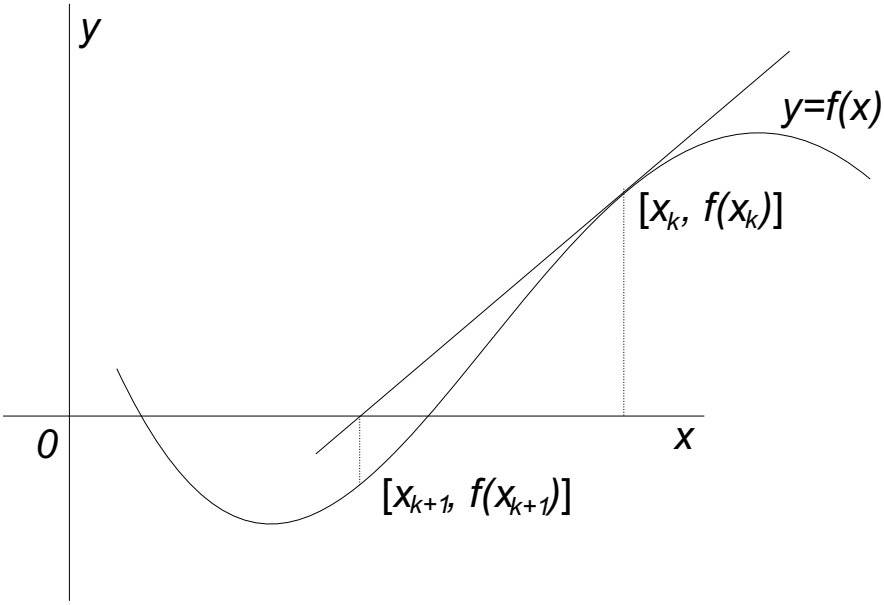
s reálnými koeficienty má stejně kladných kořenů jako znaménkových změn, nebo o sudý počet méně.

Metody aproximace reálných kořenů

Newtonova metoda Abychom řešili rovnici $f(x) = 0$, kde $f(x)$ je mnohočlen nebo obecněji funkce, která má derivaci v každém bodě nějakého intervalu (nebo komplexní oblasti), v němž hledáme kořeny, utvoříme při daném číslu x_0 posloupnost čísel $x_1, x_2, ...$ podle rekurentního vzorce

$$x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}.$$

Je-li číslo x_0 dosti blízké některému kořeni rovnice $f(x) = 0$, konvergují čísla x_k k tomuto kořeni. Pro jednoduchý kořen je tato konvergence velmi rychlá (s každým krokem se počet správných číslic prakticky zdvojnásobí). Zde čísla $x_0, x_1, ...$ mohou být i komplexní (a k nereálnému kořeni nemůže konvergovat posloupnost s reálným x_0, je-li $f(x)$ reálná funkce). V reálném oboru má Newtonova metoda jednoduchý geometrický význam:

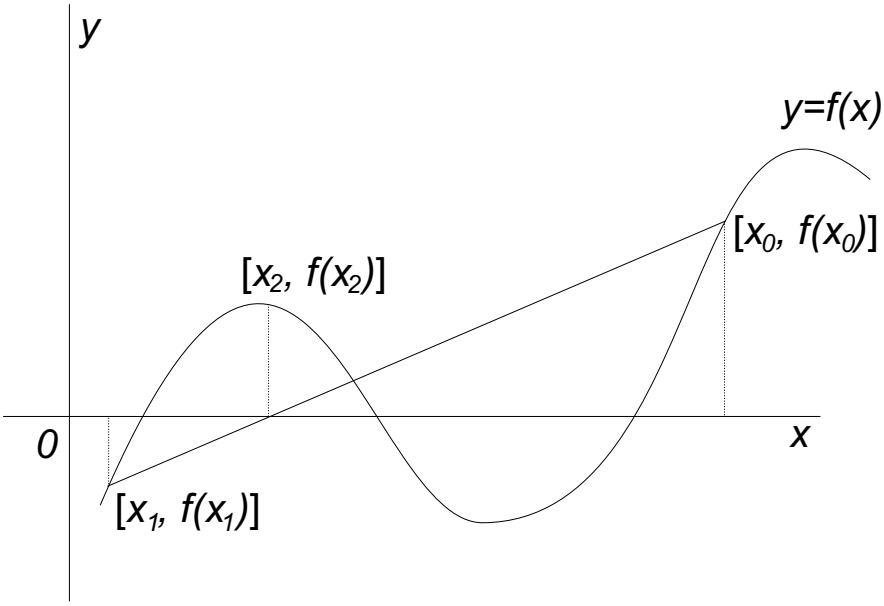


Vedeme-li v bodě $[x_k, f(x_k)]$ tečnu ke křivce $y = f(x)$ je x_{k+1} první souřadnice průsečíku tečny s osou x. Jestliže v nějakém intervalu $\langle a, b\rangle$ mají derivace $f'(x)$ a $f''(x)$ stálé znaménko a platí-li $f(a)f(b) < 0$, pak Newtonova metoda s počátečním číslem $x_0 = a$ resp. $x_0 = b$ (podle toho, zda $f(a)$ resp. $f(b)$ má totéž znaménko jako $f''(x)$), konverguje k některému kořenu dané rovnice v $\langle a, b\rangle$.

Metoda regula falsi Touto metodou lze řešit rovnici $f(x) = 0$ ($f(x)$ je reálná spojitá v nějakém intervalu I), jestliže známe dvě čísla x_0 a x_1 (z tohoto intervalu I), pro něž $f(x_0)$ a $f(x_1)$ mají opačná znaménka, tj. $f(x_0)f(x_1) < 0$. Potom si totiž vypočteme postupně čísla $x_2, x_3, ...$ takto: Položíme

$$x_2 = \frac{x_0 f(x_1) - x_1 f(x_0)}{f(x_1) - f(x_0)}$$

Je-li $f(x_2) = 0$, jsme hotovi. Je-li $f(x_2) \neq 0$, je buď $f(x_0)$, nebo $f(x_1)$ opačného znaménka než $f(x_2)$, takže s x_0 a x_2 nebo s x_1 a x_2 vypočítáme analogicky x_3. Dále zase pomocí x_3 a jednoho z čísel x_2 a předtím vybraného čísla z x_0 a x_1 vypočteme x_4 atd. Posloupnost čísel $x_0, x_1, x_2, ...$ takto utvořená vždy konverguje, zpravidla však dosti pomalu. Geometrický význam této metody je následující:



číslo x_2 je první souřadnicí průsečíku osy x s přímkou spojující dva body křivky $y = f(x)$ o (prvních) souřadnicích x_0 a x_1.

Iterační metoda Pišme rovnici $f(x) = 0$ v nějakém ekvivalentním tvaru

$$f_1(x) = f_2(x)$$

funkci $f_1(x)$ přitom volíme tak, aby rovnici $f_1(x) = c$ bylo možno snadno řešit. (např. lineární, tvaru x^n apod.) Potom můžeme k počáteční hodnotě

x_0 sestrojit rekurentně posloupnost čísel $x_1, x_2, ...$ tak, že x_{k+1} vypočteme z rovnice

$$f_1(x_{k+1}) = f_2(x_k)$$

Konverguje-li posloupnost $x_1, x_2, ...$ k limitě z a jsou-li funkce $f_1(x)$ a $f_2(x)$ v z spojité, je z kořen původní rovnice. Mají-li funkce $f_1(x)$ a $f_2(x)$ v nějakém okolí kořene z první derivace, pro něž v tomto okolí platí

$$|f_1'(x)| > |f_2'(x)|$$

pak uvedená posloupnost konverguje k z, jakmile x_0 je dostatečně blízko k z.