Martina Ernestová

Soustavy algebraických rovnic

Učitel matematiky, Vol. 10 (2002), No. 4, 193–208

Persistent URL: http://dml.cz/dmlcz/150549

SOUSTAVY ALGEBRAICKÝCH ROVNIC

MARTINA ERNESTOVÁ

Při hodinách matematiky věnovaných soustavám rovnic nebo úlohám na ně vedoucím se na střední škole většinou setkáváme pouze se soustavami lineárních rovnic, soustavami sestávajícími z lineárních rovnic a jedné rovnice vyššího stupně, případně s jednoduchými soustavami nealgebraických rovnic, které je možno na předchozí typy převést. Později se při výuce analytické geometrie řeší soustavy algebraických rovnic druhého stupně. Soustavy algebraických rovnic vyššího stupně a s více neznámými (často s parametry) se čas od času vyskytují v matematické olympiádě; k vyřešení je nutno použít nějakého triku, protože metoda, která by vždy vedla k cíli jako Gaussova eliminace, není studentům známa.

V tomto článku se pokusíme přiblížit obecnou metodu pro řešení soustav algebraických rovnic, metodu Gröbnerových bází, a poukážeme na možnosti využití matematického softwaru pro jejich výpočet.

Následující soustava dvou rovnic o dvou neznámých představuje úlohu, s kterou se běžně setkáváme v učebnicích pro 3. ročník čtyřletých gymnázií – nalezení průsečíků dvou kuželoseček. Úloha je obtížnější, neboť kuželosečky jsou vzhledem k souřadnému systému nejen posunuty, ale i pootočeny.

$$\begin{aligned} x^2 + 2xy - 8y^2 - 6x + 18y - 7 &= 0, \\ 2x^2 - 5xy - 10y^2 - 3x + 9y + 7 &= 0. \end{aligned} \tag{I}$$

Přičtením (-2)-násobku první rovnice k druhé dostaneme rovnici, která je v neznámé x lineární:

$$3xy - 3x - 2y^2 + 9y - 7 = 0.$$

Jestliže je $y \neq 1$, pak můžeme za x dosadit do některé z rovnic v (I) výraz

$$x = \frac{2y^2 - 9y + 7}{3(y-1)} = \frac{1}{3}(2y - 7);$$

snadno pak najdeme řešení příslušné kvadratické rovnice s neznámou y i jemu odpovídající hodnoty x:

$$[x_1, y_1] = [-3, -1], \qquad [x_2, y_2] = [-1, 2].$$

Jestliže je $y = 1$, pak jsou po dosazení obě rovnice soustavy (I) kvadratickými rovnicemi s neznámou x; snadno získáme řešení

$$[x_3, y_3] = [3, 1], \qquad [x_4, y_4] = [1, 1].$$

Soustava (I) má tedy čtyři řešení:[1] $[-3,-1], [-1,2], [3,1], [1,1]$.[2]

Zkusme nyní vyřešit obtížnější úlohu:

$$\begin{aligned} x^3 + x^2y - y^3 &= 1, \\ x^3 - 2xy^2 + 4y^3 &= -5. \end{aligned} \tag{II}$$

Odečtením rovnic soustavy (II) jednodušší rovnici nezískáme. Pokusme se odstranit absolutní členy přičtením 5-násobku první rovnice ke druhé:

$$6x^3 + 5x^2y - 2xy^2 - y^3 = 0$$

Postupnými úpravami zjistíme, že polynom na levé straně rovnice je součinem tří lineárních činitelů:

$$\begin{aligned} 6x^3 + 5x^2y - y^2(2x+y) &= \\ &= x^2(2x+y) + 4x^2(x+y) - y^2(2x+y) = \\ &= (x+y)(x-y)(2x+y) + 4x^2(x+y) = \\ &= (x+y)(6x^2 - 2xy + xy - y^2) = \\ &= (x+y)(6x^2 - 3xy + 2xy - y^2) = \\ &= (x+y)(3x+y)(2x-y). \end{aligned}$$

[1] Pro n-tici reálných čísel, která je řešením dané soustavy o n neznámých, budeme užívat také termíny *kořen soustavy* a *nulový bod polynomů příslušných soustavě*.

[2] Jde o průsečíky dvou kuželoseček; různoběžek $x + 4y = 7$, $x - 2y = -1$ a hyperboly $(25x - 5y - 24)^2 - 105(x + 5y - 2)^2 + 1664 = 0$.

Snadno najdeme řešení soustav

$$\begin{aligned} x^3 + x^2y - y^3 &= 1, \\ x + y &= 0, \end{aligned} \qquad \begin{aligned} x^3 + x^2y - y^3 &= 1, \\ 3x + y &= 0, \end{aligned}$$

$$\begin{aligned} x^3 + x^2y - y^3 &= 1, \\ 2x - y &= 0. \end{aligned}$$

Soustava (II) tedy má tři řešení:

$$[1, -1], \qquad \left[\sqrt[3]{\frac{1}{25}}, -3\sqrt[3]{\frac{1}{25}}\right], \qquad \left[\sqrt[3]{\frac{1}{5}}, 2\sqrt[3]{\frac{1}{5}}\right].$$

Uvažujme nyní soustavu

$$\begin{aligned} 2x^3 + xy - x + y^3 &= -1, \\ x^2y - xy + y^2 &= 1. \end{aligned} \tag{III}$$

Třebaže je to soustava pouze dvou rovnic o dvou neznámých, patrně se nám hned nepodaří najít vhodnou kombinaci jejích rovnic, která by vedla ke zjednodušení výpočtu. Dosazením $x = 0$ do soustavy (III) zjistíme, že dvojice $[0, -1]$ je jejím řešením. Pokusme se tohoto poznatku využít pro vyřešení soustavy (III) nebo alespoň k nalezení dalších kořenů této soustavy.

Kořenoví činitelé odpovídající nulovému bodu $[0, -1]$ jsou polynomy x, $y + 1$. Polynomy f_1, f_2 příslušející soustavě (III) proto můžeme zapsat jako jejich kombinace:

$$\begin{aligned} f_1 &= 2x^3 + xy - x + y^3 + 1 = xq_1 + (y+1)q_2 = \\ &= x(2x^2 + y - 1) + (y+1)(y^2 - y + 1) \\ f_2 &= x^2y - xy + y^2 - 1 = xq_3 + (y+1)q_4 = \\ &= x(xy - y) + (y+1)(y-1) \end{aligned}$$

Je to jistá obdoba Bézoutovy věty: prvek α je nulovým bodem polynomu $f(x)$ právě tehdy, když existuje polynom $q(x)$ takový, že $f(x) = (x - \alpha)q(x)$. Protože má polynom $f(x) = x^3 - x^2 - 4x + 4$ nulový bod 2, je $f(x)$ „kombinací“ kořenového činitele $x - 2$, tj.

jeho násobkem: $f(x) = (x-2)(x^2+x-2)$. Předchozí vztah můžeme také charakterizovat pomocí dělení polynomů; jestliže je číslo 2 kořenem rovnice $f(x) = 0$, pak lze polynom $f(x)$ beze zbytku vydělit polynomem $x - 2$. V tomto ohledu ukazují výše uvedené kombinace kořenových činitelů x a $y + 1$, že polynomy f_1, f_2 je možno vydělit beze zbytku dvojicí polynomů x, $y + 1$.

Poznamenejme na tomto místě důležitou věc týkající se uspořádání členů v polynomech. Jako samozřejmé přijmeme, že

$$1 \prec x \prec x^2 \prec x^3 \prec \dots .$$

Podobně uspořádejme členy[3] každého polynomu dvou neurčitých x, y relacemi

$$\begin{aligned} 1 \prec y \prec y^2 \prec y^3 \prec \dots \prec x \prec xy \prec xy^2 \prec \\ \prec xy^3 \prec \dots \prec x^2 \prec x^2y \prec x^2y^2 \prec x^2y^3 \prec \dots . \end{aligned}$$

Tento řetězec relací dostaneme, když každý člen 1, x, x^2, ... prvního řetězce „vynásobíme" řetězcem $1 \prec y \prec y^2 \prec y^3 \prec \dots$. V naznačeném uspořádání jsou členy tím větší, čím vyšší mocninu neurčité x obsahují. Jestliže má neurčitá x v daném členu stejnou mocninu jako v jiném členu, pak rozhoduje mocnina neurčité y. Takové uspořádání se nazývá *lexikografické.*[4] *Vedoucím členem* polynomu budeme rozumět jeho největší člen při daném uspořádání. Členy v polynomu vždy uspořádáme lexikograficky od největšího k nejmenšímu. To je důležité především při dělení polynomů.

Kdybychom přirozené uspořádání „mírně narušili" a zavedli uspořádání

$$1 \prec x^2 \prec x \prec x^3 \prec x^4 \prec x^5 \dots ,$$

pak by dělení

[3]Přesněji řečeno uspořádáme jen tzv. *termy* (součiny x^iy^j, $i, j = 0, 1, \dots$, neurčitých x, y), čímž bude dáno i uspořádání členů v polynomu. Koeficienty nemají na uspořádání členů v polynomu vliv.

[4]Součiny mocnin neurčitých x, y, obecněji výrazy $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$, je možno uspořádat mnoha dalšími způsoby. V článku budeme používat pouze lexikografické uspořádání, které se zdá být nejpřirozenějším.

$$
\begin{array}{l}
(x^4 - x + 2x^2 + 1) : (x + x^2 - 3) = x^3 - x^4 + \cdots \\
\underline{-x^4 - x^5 + 3x^3} \\
-x^5 + 3x^3 - x + 2x^2 + 1 \\
\underline{x^5 + x^6 - 3x^4} \\
x^6 - 3x^4 + 3x^3 - x + 2x^2 + 1 \\
\quad\vdots
\end{array}
$$

představovalo nekonečný proces.

Všimněme si, že vyjádřením polynomů f_1, f_2 jako kombinací kořenových činitelů x, $y+1$, tj. vydělením f_1, f_2 uvedenými činiteli, dostaneme „podíly"

$$q_1 = 2x^2 + y - 1, \quad q_2 = y^2 - y + 1, \quad q_3 = xy - y, \quad q_4 = y - 1,$$

jejichž vedoucí členy $2x^2$, y^2, xy, y jsou menší než vedoucí členy $2x^3$, x^2y polynomů f_1, f_2.

V případě, že rovnice $f(x) = 0$ má kořen α, jsou všechny její další kořeny nulovými body polynomu, který je podílem $f(x)$ a kořenového činitele $x - \alpha$. (Ve výše uvedeném příkladu má rovnice $x^3 - x^2 - 4x + 4 = 0$ vedle nulového bodu 2 jen kořeny, které jsou nulovými body polynomu $x^2 + x - 2$, tj. čísla 1 a -2.) Podobně bychom mohli očekávat, že další kořeny soustavy (III) dostaneme vyřešením soustavy

$$
\text{(III.A)}\quad
\begin{aligned}
q_1 &= 2x^2 + y - 1 = 0,\\
q_2 &= y^2 - y + 1 = 0,\\
q_3 &= xy - y = 0,\\
q_4 &= y - 1 = 0.
\end{aligned}
$$

Při řešení soustavy rovnic s více neznámými musíme být opatrnější. Z kombinací

$$
\begin{aligned}
f_1 &= x(2x^2 + y - 1) + (y+1)(y^2 - y + 1),\\
f_2 &= x(xy - y) + (y+1)(y-1)
\end{aligned}
$$

kořenových činitelů x, $y+1$ můžeme totiž sestavit ještě jiné soustavy, jejichž kořeny by mohly být řešením soustavy (III):

$$\text{(III.B)} \quad \begin{aligned} x &= 0, \\ q_2 = y^2 - y + 1 &= 0, \\ q_4 = y - 1 &= 0, \end{aligned} \qquad \text{(III.C)} \quad \begin{aligned} y + 1 &= 0, \\ q_1 = 2x^2 + y - 1 &= 0, \\ q_3 = xy - y &= 0. \end{aligned}$$

Soustavy (III.A) a (III.B) nemají řešení. Poslední soustava má kořen $[1, -1]$; „podíly“ q_1, q_3 můžeme zapsat jako kombinace kořenových činitelů $x - 1$, $y + 1$:

$$\begin{aligned} q_1 &= 2x^2 + y - 1 = 2(x-1)(x+1) + (y+1), \\ q_3 &= y(x-1), \end{aligned}$$

a tedy i polynomy f_1, f_2 mohou být zapsány jako kombinace polynomů $x - 1$, $y + 1$. Dvojice $[1, -1]$ je proto řešením soustavy (III).

Postup, kterým jsme našli další kořen soustavy (III), je méně vhodný pro soustavy s větším počtem neznámých. Navíc nevíme, zda dvojice $[0, -1]$, $[1, -1]$ představují všechna (reálná) řešení soustavy.

Věnujme se nyní problému řešení obecné soustavy

$$\begin{aligned} f_1(x_1, x_2, \ldots, x_n) &= 0, \\ f_2(x_1, x_2, \ldots, x_n) &= 0, \\ \ldots\ldots\ldots&\ldots\ldots\ldots \\ f_m(x_1, x_2, \ldots, x_n) &= 0, \end{aligned} \tag{IV}$$

kde $f_1, f_2, \ldots, f_m \in \mathbb{R}[x_1, x_2, \ldots, x_n]$; symbolem $\mathbb{R}[x_1, x_2, \ldots, x_n]$ rozumíme okruh všech polynomů neurčitých $x_1, x_2, \ldots, x_n$ nad tělesem reálných čísel, tj. $f_1, f_2, \ldots, f_m$ jsou polynomy neurčitých $x_1, x_2, \ldots, x_n$ s reálnými koeficienty. Předně si uvědomme, že každé řešení $[\alpha_1, \alpha_2, \ldots, \alpha_n]$ soustavy (IV) je zároveň řešením libovolné kombinace

$$k_1 f_1 + k_2 f_2 + \ldots + k_m f_m = 0$$

rovnic této soustavy, kde $k_i \in \mathbb{R}[x_1, x_2, \ldots, x_n]$. Množinu všech takovýchto kombinací nazýváme *ideálem* okruhu $\mathbb{R}[x_1, x_2, \ldots, x_n]$ generovaným polynomy $f_1, f_2, \ldots, f_m$; píšeme

$$\mathfrak{I} = \langle f_1, f_2, \ldots, f_m \rangle \subset \mathbb{R}[x_1, x_2, \ldots, x_n].$$

Řešení $[\alpha_1, \alpha_2, \ldots, \alpha_n]$ soustavy (IV) je tedy rovněž řešením soustavy tvořené nekonečně mnoha rovnicemi; příslušné polynomy jsou všechny prvky ideálu $\mathfrak{I} = \langle f_1, f_2, \ldots, f_m \rangle$.

Kořeny soustavy (I) jsou nulovými body libovolného polynomu z ideálu

$$\mathfrak{K} = \langle p_1, p_2 \rangle,$$

kde

$$\begin{aligned} p_1 &= x^2 + 2xy - 8y^2 - 6x + 18y - 7, \\ p_2 &= 2x^2 - 5xy - 10y^2 - 3x + 9y + 7. \end{aligned}$$

Z postupu řešení soustavy (I) je zřejmé, že jsme našli kořeny soustavy

$$\text{(I')} \quad \begin{aligned} -2p_1 + p_2 &= 0, \\ p_1 &= 0, \end{aligned} \qquad \text{nebo} \qquad \text{(I")} \quad \begin{aligned} -2p_1 + p_2 &= 0, \\ p_2 &= 0. \end{aligned}$$

Řešení soustavy (II), tj. nalezení nulových bodů všech polynomů ideálu

$$\mathfrak{L} = \langle q_1, q_2 \rangle = \langle x^3 + x^2y - y^3 - 1,\ x^3 - 2xy^2 + 4y^3 + 5 \rangle,$$

jsme nahradili řešením soustavy

$$\text{(II')} \qquad \begin{aligned} q_1 &= 0, \\ 5q_1 + q_2 &= 0. \end{aligned}$$

Soustavy (I'), (I"), resp. (II'), jejichž vyřešení je snazší, jsou ekvivalentní s původními soustavami (I), resp. (II). Ekvivalentnost soustav (I), (I'), (I") a (II), (II') můžeme pomocí ideálů generovaných příslušnými polynomy zapsat jako rovnosti

$$\begin{aligned} \langle p_1, p_2 \rangle &= \langle -2p_1 + p_2, p_1 \rangle = \langle -2p_1 + p_2, p_2 \rangle, \\ \langle q_1, q_2 \rangle &= \langle q_1, 5q_1 + q_2 \rangle. \end{aligned}$$

Inspirováni dvěma předchozími příklady (soustavami (I) a (II)) chceme nyní generátory $f_1, f_2, \dots, f_m$ ideálu $\mathfrak{I}$, které přísluší soustavě (IV), nahradit jinými generátory $g_1, g_2, \dots, g_s$ ideálu $\mathfrak{I}$ tak, aby soustava

$$\begin{aligned} g_1(x_1, x_2, \dots, x_n) &= 0, \\ g_2(x_1, x_2, \dots, x_n) &= 0, \\ \dots\dots&\dots\dots \\ g_s(x_1, x_2, \dots, x_n) &= 0 \end{aligned} \tag{V}$$

byla pro řešení jednodušší. Svoje požadavky budeme charakterizovat následujícími podmínkami:

(i) $\langle g_1, g_2, \dots, g_s\rangle = \langle f_1, f_2, \dots, f_m\rangle$, tj.

$$\forall j = 1, \dots, s \quad g_j = \sum_{i=1}^{m} a_i f_i$$

a

$$\forall i = 1, \dots, m \quad f_i = \sum_{j=1}^{s} b_j g_j,$$

kde $a_i, b_j \in \mathbb{R}[x_1, x_2, \dots, x_n]$.

(ii) Polynomy $g_1, g_2, \dots, g_s$ jsou normované, tj. koeficienty u jejich vedoucích členů jsou rovny jedné.

(iii) Pro každé j, k, $1 \leq j, k \leq s$, $j \neq k$, je polynom g_j zbytkem po dělení polynomu g_j polynomem g_k, tj. polynom g_j „nelze vydělit“ polynomem g_k (podíl je roven nule).

(iv) Pro každé j, k, $1 \leq j, k \leq s$, $j \neq k$, platí tato podmínka: Jsou-li z_j, z_k nejmenší možné součiny neurčitých $x_1, \dots, x_n$, pro které se vedoucí členy polynomů $z_j g_j$ a $z_k g_k$ v rozdílu $z_j g_j - z_k g_k$ vyruší,[5] potom je tento rozdíl možno vyjádřit jako kombinaci polynomů $g_1, g_2, \dots, g_s$, tj.

$$z_j g_j - z_k g_k = l_1 g_1 + l_2 g_2 + \dots + l_j g_j + \dots + l_k g_k + \dots + l_s g_s,$$

kde $l_1, l_2, \dots, l_s \in \mathbb{R}[x_1, x_2, \dots, x_n]$ a $l_j \neq z_j, l_k \neq z_k$.

[5] Takové z_j, z_k vždy existují a jsou určeny jednoznačně.

Podmínkami (i)–(iv) je pro dané uspořádání neznámých a jejich součinů množina $G = \{g_1, g_2, \ldots, g_s\}$ určena jednoznačně. Je to tzv. *Gröbnerova báze* ideálu $\mathfrak{I} = \langle f_1, f_2, \ldots, f_m \rangle$. Za *snáze řešitelnou* soustavu budeme považovat takovou soustavu, k níž příslušné polynomy tvoří Gröbnerovu bázi.

Jako příklad Gröbnerovy báze uveďme množinu

$$\{x - y^3 + 3y, y^4 - 3y^2 + 1\};$$

její prvky jsou jinými generátory ideálu $\langle x^2 + y^2 - 3, xy + 1 \rangle$.

Rovnost ideálů v podmínce (i) zaručuje ekvivalentnost soustav (IV) a (V); tyto soustavy tedy mají stejnou množinu řešení. Splnění podmínky (ii) není pro „snadnou řešitelnost soustavy" nutné; druhá podmínka pouze zaručuje, že polynomy v Gröbnerově bázi jsou normované, čehož se využívá k jednodušší formulaci podmínky (iv). V dalším uvidíme, že podmínka (iii) zajišťuje, že členy v polynomech Gröbnerovy báze jsou co možná nejmenší (v lexikografickém uspořádání) a že v důsledku „minimalizuje" počet rovnic v soustavě (V). Rozhodující pro „snadnost řešení soustavy" je podmínka (iv), která zaručuje, že polynomy $g_1, g_2, \ldots, g_s$ (přesněji jejich vedoucí členy) jsou v lexikografickém uspořádání nejmenší, pro které je soustava (V) ekvivalentní se soustavou (IV); požaduje totiž, aby všechny polynomy $z_j g_j - z_k g_k$, tj. takové kombinace g_j, g_k, jejichž vedoucí člen je menší, bylo možno vygenerovat z polynomů $g_1, g_2, \ldots, g_s$.

V následujícím budeme trochu počítat, abychom čtenáři přiblížili podmínky (i)–(iv). Omlouváme se za tyto výpočty a úpravy, které méně laskavý čtenář může pouze „přelétnout očima".

Zjistěme, zda je soustava (III) podle podmínek (i)–(iv) snáze řešitelná. Nechť $G_0 = \{f_1, f_2\} = \{2x^3 + xy - x + y^3 + 1, x^2y - xy + y^2 - 1\}$.

Položme $g_1 = \frac{1}{2} f_1$, $g_2 = f_2$. Je zřejmé, že (i) a (ii) platí. Podmínka (iii) je také splněna, neboť největší člen polynomu g_1 nedělí žádný člen polynomu g_2, tj. g_2 není možné vydělit polynomem g_1, a obráceně největší člen polynomu g_2 nedělí žádný z členů g_1, tj. polynom g_1 nelze vydělit polynomem g_2. Pro dvojici g_1, g_2 je zřejmě $z_1 = y$, $z_2 = x$. Polynomy $z_1 = y$, $z_2 = x$

jsou totiž nejmenší možné součiny neznámých x, y, pro které se vedoucí členy x^3y, x^3y polynomů z_1g_1, z_2g_2 vyruší. Nyní je

$$z_1g_1 - z_2g_2 = yg_1 - xg_2 = x^2y - \frac{1}{2}xy^2 - \frac{1}{2}xy + x + \frac{1}{2}y^4 + \frac{1}{2}y.$$

Polynom $z_1g_1 - z_2g_2$ vydělme množinou $\{g_1, g_2\}$, tj. pokusme se ho vyjádřit jako kombinaci polynomů g_1, g_2.

$$\begin{aligned} x^2y - \frac{1}{2}xy^2 - \frac{1}{2}xy + x + \frac{1}{2}y^4 + \frac{1}{2}y &= \\ &= g_2 - \frac{1}{2}(xy^2 - xy - 2x - y^4 + 2y^2 - y - 2) \end{aligned}$$

Je vidět, že uvedený polynom není možno zapsat jako kombinaci $l_1g_1 + l_2g_2$, $l_1 \neq z_1, l_2 \neq z_2$, protože polynom s vedoucím členem xy^2 nelze vydělit ani polynomem g_1, ani polynomem g_2, neboť oba mají větší vedoucí člen. Podmínka (iv) proto není splněna, množina $G_1 = \{g_1, g_2\}$ není Gröbnerova báze ideálu $\langle f_1, f_2\rangle$ a odpovídající soustava není snáze řešitelná.

Polynom s vedoucím členem xy^2 sice není možno vydělit žádným z polynomů g_1, g_2, ale pomocí výše uvedených vztahů ho můžeme zapsat jako jejich kombinaci.

$$g_3 = xy^2 - xy - 2x - y^4 + 2y^2 - y - 2 = -2yg_1 + 2(x+1)g_2.$$

Jestliže je $[\alpha, \beta]$ řešením soustavy (III), tj. $f_1(\alpha, \beta) = 0$ a zároveň $f_2(\alpha, \beta) = 0$, pak je $[\alpha, \beta]$ také nulovým bodem polynomu g_3, protože $g_3 = -yf_1 + 2(x+1)f_2$ a

$$g_3(\alpha, \beta) = -\beta f_1(\alpha, \beta) + 2(\alpha + 1)f_2(\alpha, \beta) = 0.$$

Soustava

$$\begin{aligned} g_1 &= 0, \\ g_2 &= 0, \\ g_3 &= 0. \end{aligned} \tag{III'}$$

má proto stejnou množinu řešení jako soustava (III).

Upravujme soustavu (III'), resp. množinu $G_2 = \{g_1, g_2, g_3\}$ tak dlouho, dokud její polynomy nebudou vyhovovat podmínkám (i)–(iv); postupně budeme získávat množiny $G_3, G_4, \ldots$. Do množiny G_i budeme vždy přidávat jen kombinace polynomů množiny G_{i-1}. Tím bude zaručeno, že soustava příslušná množině G_i bude ekvivalentní se soustavou (III).

Vedoucí člen přidaného polynomu g_3 je menší než vedoucí členy polynomů g_1, g_2. Podobně vedoucí člen každého polynomu, který přidáme do množiny G_i, bude menší než tyto vedoucí členy a nebude dělitelný žádným z vedoucích členů polynomů množiny G_{i-1}. Vedoucí členy polynomů množin G_i se neustále zmenšují. Protože ovšem neexistuje nekonečný klesající řetězec vedoucích členů, dojdeme po konečném počtu kroků k množině polynomů, které splňují podmínky (i)–(iv).

Množina G_2 splňuje podmínky (i)–(iii). Rozdíl $z_1g_1 - z_2g_2$ je kombinací polynomů příslušných soustavě (III'), protože $yg_1 - xg_2 = g_2 - \frac{1}{2}g_3$, tedy dvojice (g_1, g_2) vyhovuje podmínce (iv). Uvažujme polynomy g_1, g_3 a postupně vydělme jejich kombinaci $z_1'g_1 - z_3g_3$ polynomy g_1, g_2, g_3:[6]

$$\begin{aligned}z_1'g_1 - z_3g_3 = y^2g_1 - x^2g_3 &= (y+2)g_1 + (y^3 - 2y + 1)g_2 + \\ &+ (y^2 + \frac{3}{2}y + \frac{1}{2})g_3 + \\ &+ 2x^2 + 4xy + 2x + y^6 + y^5 - 2y^4 + 2y^2 + y + 1\end{aligned}$$

Polynom s vedoucím členem $2x^2$ již nelze vydělit žádným z polynomů g_1, g_2, g_3, rozdíl $z_1'g_1 - z_3g_3$ se proto nepodaří zapsat jako

[6] Je na místě upozornit, že dělení množinou polynomů $\{g_1, g_2, g_3\}$ je možno provést několika způsoby. Zde jsme dodrželi uvedené pořadí a rozdíl $z_1'g_1 - z_3g_3$ jsme skutečně dělili nejprve polynomem g_1, pak polynomem g_2 a nakonec polynomem g_3. Při dělení v pořadí g_2, g_3, g_1 bychom dostali:

$$\begin{aligned}y^2g_1 - x^2g_3 = 2g_1 + (x + y^3 - 2y + 2)g_2 + (y^2 + \frac{3}{2}y)g_3 + 2x^2 + 4xy + 2x + \\ + y^6 + y^5 - 2y^4 + 2y^2 + y + 1.\end{aligned}$$

Dodejme, že zbytek, kterým je v obou případech týž polynom s vedoucím členem $2x^2$, nemusí být obecně stejný, změníme-li pořadí polynomů, kterými dělíme.

kombinaci $l_1g_1 + l_2g_2 + l_3g_3$, $l_1 \neq z_1'$, $l_3 \neq z_3$, což je vyžadováno podmínkou (iv). Uvedený polynom normujeme,

$$g_4 = x^2 + 2xy + x + \frac{1}{2}y^6 + \frac{1}{2}y^5 - y^4 + y^2 + \frac{1}{2}y + \frac{1}{2},$$

přidáme do množiny G_2 a získáme tak množinu G_3. Soustava příslušná množině $G_3 = \{g_1, g_2, g_3, g_4\}$ je ekvivalentní se soustavou (III), protože $g_4 = \frac{1}{2}(y^2 - y - 2)g_1 - \frac{1}{2}(y^3 - 2y + 1)g_2 - \frac{1}{2}(x^2 + y^2 + \frac{3}{2}y + \frac{1}{2})g_3$, přičemž g_3 je kombinací polynomů g_1, g_2.

Množina G_3 nevyhovuje podmínce (iii), protože x^2, vedoucí člen polynomu g_4, dělí vedoucí členy polynomů g_1 a g_2. Nahraďme proto polynom g_1 jeho normovaným zbytkem g_1' po dělení ostatními polynomy množiny G_3. I po takové úpravě zůstane soustava příslušná polynomům množiny $G_4 = \{g_1', g_2, g_3, g_4\}$ ekvivalentní soustavě (III), neboť polynomy množiny G_4 jsou kombinacemi polynomů g_1, g_2 a obráceně polynomy g_1, g_2 dostaneme jako kombinace polynomů množiny G_4:

$$\begin{aligned} g_1 = &-(\frac{1}{2}y^4 + y^3 + y^2 + 3y + 2)g_3 + (x - 2y - 1)g_4 - 4xy - \\ &- 4x - \frac{1}{2}y^8 + \frac{3}{2}y^6 - 3y^5 - 3y^4 + \frac{11}{2}y^3 + y^2 - \frac{13}{2}y - 3 \end{aligned}$$

a tedy

$$g_1' = xy + x + \frac{1}{8}y^8 - \frac{3}{8}y^6 + \frac{3}{4}y^5 + \frac{3}{4}y^4 - \frac{11}{8}y^3 - \frac{1}{4}y^2 + \frac{13}{8}y + \frac{3}{4}.$$

V nové množině G_4 nahraďme polynom g_2 polynomem g_2', který dostaneme normováním zbytku po dělení tohoto polynomu ostatními polynomy množiny G_4.

$$\begin{aligned} g_2 = &-2yg_1' + yg_4 + \frac{1}{4}(y^9 - 5y^7 + 4y^6 + 10y^5 - 11y^4 - 6y^3 + \\ &+ 15y^2 + 4y - 4), \end{aligned}$$

a tedy

$$g_2' = y^9 - 5y^7 + 4y^6 + 10y^5 - 11y^4 - 6y^3 + 15y^2 + 4y - 4.$$

Také polynom g_3 lze vydělit polynomem g_1'. Nahraďme ho tedy zbytkem g_3':

$$g_3 = (y-2)g_1' - (1/8)g_2' + \\ + \frac{1}{4}(y^8 - y^7 - 4y^6 + 8y^5 + 2y^4 - 13y^3 + 7y^2 + 8y - 4),$$
$$g_3' = y^8 - y^7 - 4y^6 + 8y^5 + 2y^4 - 13y^3 + 7y^2 + 8y - 4$$

Druhý člen polynomu g_4 je dělitelný vedoucím členem polynomu g_1', v $G_6 = \{g_1', g_2', g_3', g_4\}$ proto nahradíme poslední polynom zbytkem g_4':

$$g_4 = 2g_1' - \frac{1}{4}g_3' + x^2 - x - \frac{1}{4}y^7 + \frac{1}{4}y^6 + y^5 - 2y^4 - \frac{1}{2}y^3 + \\ + \frac{13}{4}y^2 - \frac{3}{4}y - 2$$
$$g_4' = x^2 - x - \frac{1}{4}y^7 + \frac{1}{4}y^6 + y^5 - 2y^4 - \frac{1}{2}y^3 + \frac{13}{4}y^2 - \frac{3}{4}y - 2$$

Množina $G_7 = \{g_1', g_2', g_3', g_4'\}$ stále ještě nevyhovuje podmínce (iii). Nahraďme proto její prvek g_1' zbytkem g_1'' po dělení podobně jako v předchozím.

$$g_1' = \frac{1}{8}g_3' + xy + x + \frac{1}{8}y^7 + \frac{1}{8}y^6 - \frac{1}{4}y^5 + \frac{1}{2}y^4 + \frac{1}{4}y^3 - \\ - \frac{9}{8}y^2 + \frac{5}{8}y + \frac{5}{4}$$
$$g_1'' = xy + x + \frac{1}{8}y^7 + \frac{1}{8}y^6 - \frac{1}{4}y^5 + \frac{1}{2}y^4 + \frac{1}{4}y^3 - \frac{9}{8}y^2 + \frac{5}{8}y + \frac{5}{4}$$
$$g_2' = (y+1)g_3'$$

Polynom g_2' můžeme z množiny $G_8 = \{g_1'', g_2', g_3', g_4'\}$ vynechat, protože je násobkem polynomu g_3'. Polynomy g_3' a g_4' už není možno vydělit ostatními polynomy, množina $G_9 = \{g_1'', g_3', g_4'\}$ vyhovuje podmínkám (i)–(iii).

Všechny dvojice různých polynomů množiny G_9 splňují navíc podmínku (iv), neboť

$$
\begin{aligned}
y^7 g_1'' - x g_3' &= x g_1'' - y^7 g_3', \\
x g_1'' - y g_4' &= \frac{1}{8}(y^6 - 2y^4 + 6y^3 - 4y^2 - 5y + 18) g_1'' - \\
&\quad - \frac{1}{64}(y^5 + 2y^4 + 2y^3 + 10y^2 + 8y - 13) g_3' + g_4', \\
x^2 g_3' - y^8 g_4' &= \\
&= \frac{1}{4}(4x + y^7 - y^6 - 4y^5 + 8y^4 + 2y^3 - 13y^2 + 3y + 8) g_3' - \\
&\quad -(y^7 + 4y^6 - 8y^5 - 2y^4 + 13y^3 - 7y^2 - 8y + 4) g_4'.
\end{aligned}
$$

Množina G_9 je tedy Gröbnerovou bází ideálu $\langle f_1, f_2 \rangle$ a příslušná soustava

$$
\begin{aligned}
xy + x + \frac{1}{8}y^7 + \frac{1}{8}y^6 - \frac{1}{4}y^5 + \frac{1}{2}y^4 + \frac{1}{4}y^3 - \frac{9}{8}y^2 + \frac{5}{8}y + \frac{5}{4} &= 0, \\
y^8 - y^7 - 4y^6 + 8y^5 + 2y^4 - 13y^3 + 7y^2 + 8y - 4 &= 0, \\
x^2 - x - \frac{1}{4}y^7 + \frac{1}{4}y^6 + y^5 - 2y^4 - \frac{1}{2}y^3 + \frac{13}{4}y^2 - \frac{3}{4}y - 2 &= 0
\end{aligned}
$$

je „snáze řešitelná“. Prostřední rovnice o jedné neznámé má čtyři reálné kořeny (a čtyři imaginární). Jeden z nich jsme našli již dříve ($y = -1$), zbývající tři bychom určili přibližně některou z numerických metod. Dosazením vypočtených hodnot kořene y do zbývajících dvou rovnic dostaneme soustavu dvou rovnic o jedné neznámé x. Jejími kořeny jsou nulové body největšího společného dělitele obou polynomů příslušných soustavě. Vedle nulových bodů $[0, -1]$, $[1, -1]$ je řešením soustavy (III) ještě jedna dvojice reálných čísel, a sice (po zaokrouhlení na tři desetinná místa) $[-0{,}929,\ 0{,}447]$.

Postup, kterým jsme našli množinu G_9, se nazývá *Buchbergerův algoritmus.* V současné době je implementován v komerčních (Maple, Mathematica, Reduce, …) i volně dostupných (Singular, CoCoA, …) programech počítačové algebry, a tak můžeme zdlouhavé výpočty Gröbnerovy báze přenechat počítači, kterému zadáme jediný příkaz (`gbasis`, `groebner` apod.) na příkazovém řádku, např. v programu `Maple`:

```
gbasis({2x^3+xy-x+y^3+1,x^2y-xy+y^2-1},plex(x,y));
```

Počítač je rychlejší a spolehlivější než my:

$[y^8 - y^7 - 4y^6 + 8y^5 + 2y^4 - 13y^3 + 7y^2 + 8y - 4,$
$8xy + 8x + y^7 + y^6 - 2y^5 + 4y^4 + 2y^3 - 9y^2 + 5y + 10,$
$4x^2 - 4x - y^7 + y^6 + 4y^5 - 8y^4 - 2y^3 + 13y^2 - 3y - 8]$

Ve volně dostupných programech, které je možno získat na adresách[7]

http://cocoa.dima.unige.it/
http://www.singular.uni-kl.de/
http://maxima.sourceforge.net/index.html

může laskavý čtenář vypočítat Gröbnerovy báze ideálů příslušných k následujícím soustavám a pak najít kořeny snáze řešitelných soustav. Uvedené soustavy jsou snadno řešitelné i bez metody Gröbnerových bází.

1. $x^3 + 3x^2y + 5xy^2 + 6y^3 = 0,\quad 2y^2 - xy - x^2 = 0,$

2. $x^3 + y^3 = 1,\quad x^2y + 2xy^2 + y^3 = 2,$

3. $2y^2 + xy - x^2 = 0,\quad x^2 - xy + 3x - y^2 + 7y + 4 = 0,$

4. $x^2 + y^2 + xy = 3,\quad x^2 + z^2 + xz = 2,\quad y^2 + z^2 + yz = 1,$

Výsledky:[8]

$\{x^2 + xy - 2y^2, xy^2 + 2y^3\}$, $[-2p, p], p \in \mathbb{R}$;

$\{18y^6 - 25y^3 + 8, 14x + 18y^4 - 23y\}$, $[\frac{1}{3}\sqrt[3]{3}, \frac{2}{3}\sqrt[3]{3}], [\frac{1}{2}\sqrt[3]{4}, \frac{1}{2}\sqrt[3]{4}]$;

$\{y^4 + 17y^3 + 60y^2 + 68y + 16, 3x + y^2 + 7y + 4\}$, $[2, -2]$,
$[-13 - 3\sqrt{17}, -\frac{1}{2}(13 + 3\sqrt{17})]$, $[-13 + 3\sqrt{17}, -\frac{1}{2}(13 - 3\sqrt{17})]$;

$\{3z^3 - z, yz + 2z^2, y^2 - z^2 - 1, x^2 + xy + z^2 - 2\}$,
$[-2, 1, 0], [1, 1, 0], [-1, -1, 0], [2, -1, 0]$,
$[\frac{\sqrt{3}}{3} + \sqrt{2}, -\frac{2}{3}\sqrt{3}, \frac{1}{3}\sqrt{3}]$, $[-\frac{\sqrt{3}}{3} + \sqrt{2}, \frac{2}{3}\sqrt{3}, -\frac{1}{3}\sqrt{3}]$,
$[\frac{\sqrt{3}}{3} - \sqrt{2}, -\frac{2}{3}\sqrt{3}, \frac{1}{3}\sqrt{3}]$, $[-\frac{\sqrt{3}}{3} - \sqrt{2}, \frac{2}{3}\sqrt{3}, -\frac{1}{3}\sqrt{3}]$

[7] Nebo přímo na německém serveru marlene.zib.de. Informace o tom, jak se k serveru připojit jsou na adrese http://www.zib.de/Symbolik/reduce/testreduce.html.

[8] Uvedené množiny představují Gröbnerovy báze při lexikografickém uspořádání členů a neurčitých, uspořádané dvojice (trojice) reálná řešení.

Literatura

[1] Cox, D., Little, J., O'Shea, D., *Ideals, Varieties, and Algorithms*, New York, 1998

[2] Hora, J., *O některých otázkách souvisejících s využíváním programů počítačové algebry ve škole, kap. 5 – Teorie ideálů a Gröbnerovy báze aneb od „moderní algebry" k úlohám matematické olympiády*, Plzeň, 1998

[3] Kořínek, A., *Základy algebry*, Praha, 1953

[4] Kuščenko, V. S., *Sbornik konkursnych zadač po matematike s rešenijami*, Moskva, 1955

[5] Novoselov, S. I., *Specialnyj kurs elementarnoj algebry*, Moskva, 1958

Mgr. Martina Ernestová
MÚ UK, Sokolovská 83
186 00 Praha 8
e-mail: mernesto@karlin.mff.cuni.cz