1. Polynomy více proměnných, Gröbnerova báze

1.1. Monomiální uspořádání. Jaké je lexikografické a gradované lexikografické uspořádání monomů polynomu $f = 4xy^2z+4z^2-5x^3+7x^2z^2$ s uspořádáním proměnných $x > y > z$? Určete $LM(f), LC(f)$ a $LT(f)$.

Řešení. V lexikografickém uspořádání sledujeme prvně stupeň největší proměnné, tj. x. Potom stupeň y, pak z. Proto $x^3 \geq_{\text{lex}} x^2z^2 \geq_{\text{lex}} xy^2z \geq_{\text{lex}} z^2$. Vedoucí monom, koeficient a člen jsou po řadě $LM(f) = x^3$, $LC(f) = -5$ a $LT(f) = -5x^3$. Při gradovaném uspořádání se díváme nejprve na součet stupňů všech proměnných. Je-li stejný, pak pokračujeme jako v lex, tj. $x^2z^2 \geq_{\text{grlex}} xy^2z \geq_{\text{grlex}} x^3 \geq_{\text{grlex}} z^2$, a proto $LM(f) = x^2z^2$, $LC(f) = 7$ a $LT(f) = 7x^2z^2$.

1.2. Dělení se zbytkem. Vydělte polynom $f = xy^2 + 1$ polynomem $f_1 = xy + 1$ a polynomem $f_2 = y + 1$ (uvažujte obvyklé lexikografické uspořádání).

Řešení. Narozdíl od číselných okruhů nám algoritmus dělení se zbytkem v okruhu polynomů nedává obecně jednoznačný výsledek. Budeme nejprve dělit f/f_1. Stejně jako přidělení polynomů jedné proměnné dělíme vedoucí členy $LT(f)/LT(f_1) = y$ a přičteme zbytek, tj. $f = yf_1 - y + 1$. Protože vedoucí člen zbytku y není dělitelný $LT(f_1)$, je algoritmus u konce. Pokračujeme ale dělením polynomem f_2 a dostaneme $LT(1-y)/LT(f_2) = -1$, a proto celkem $f = y(xy+1)+(-1)(y+1)+2$.

Pokud budeme dělit napřed polynomem f_2, pak dostaneme $LT(f)/LT(f_2) = xy$, konkrétně $f = xyf_2 - xy + 1$. Můžeme dělit dál $LT(-xy)/LT(f_2) = -x \rightsquigarrow f = (xy - x)f_2 + x + 1$. Dále už nemůžeme dělit ani jedním z polynomů f_1, f_2.

1.3. Ideál, algebraická varieta, Gröbnerova báze. Najděte Gröbnerovu bázi ideálu generovaného polynomy $f_1 = x^3 - 2xy$, $f_2 = x^2y + x - 2y^2$ a určete příslušnou algebraickou varietu v $\mathbb{R}^2$.

Řešení. Ideál je tořen všemi polynomiálními kombinacemi polynomů f_1, f_2, tj.

$$I = \langle f_1, f_2\rangle = \{f \in \mathbb{R}[x, y] : f = a_1f_1 + a_2f_2 \,; a_1, a_2 \in \mathbb{R}[x, y]\}.$$

Není úplně jednoduché rozhodnout, zda jsou dva ideály totožné nebo také, zda daný polynom f leží v I. Víme sice, že pokud dá algoritmus dělení se zbytkem polynomu f polynomy f_1, f_2 zbytek nula, pak $f \in I$. Pokud je ale nenulový, pak můžeme usoudit $f \in I$ jen pokud f_1 a f_2 splňují $LM(I) = \langle LM(f_1), LM(f_2)\rangle$ (je třeba si rozmyslet). Taková báze ideálu I se nazývá Gröbnerova a vždy existuje.

V našem případě je $LM(f_1) = x^3$ a $LM(f_2) = x^2y$. Zároveň ale vidíme, že tzv. S–polynom

$$yf_1 - xf_2 = yx^3 - 2xy^2 - x^3y - x^2 + 2y^2x = -x^2 \in I,$$

ale $x^2 \notin \langle x^3, x^2y\rangle$. Báze f_1, f_2 tedy není Gröbnerova – "chybí tam x^2". Algoritmus nalezení Gröbnerovy báze spočívá právě v přidávání těchto "chybějících" S–polynomů ke stávající bázi a její následné redukování. V našem případě tedy máme $\langle f_1, f_2, x^2\rangle$. Redukování není nic jiného než vzájemné dělení se zbytkem těchto bázových polynomů tak, aby vedoucí členy byly vzájemně nesoudělné. Můžeme dělit následovně:

$$f_1 = x^3 - 2xy = x \cdot x^2 - 2xy, \quad f_2 = y \cdot x^2 + x - 2y^2.$$

Máme tak novou bázi $I = \langle xy, x - 2y^2, x^2\rangle$. Můžeme ovšem dělit dál:

$$xy = y(x - 2y^2) + 2y^3, \quad x^2 = x(x - 2y^2) + 2xy^2 = (x + 2y^2)(x - 2y^2) + 4y^4.$$

Dostáváme tak bázi $I = \langle x - 2y^2, y^3, y^4\rangle$, kterou ovšem můžeme zredukovat na $I = \langle x - 2y^2, y^3\rangle$. Tato báze už je Gröbnerova, protože jediný S–polynom, který můžeme vytvořit je $y^3(x-2y^2)-xy^3 = -2y^5$ a ten je dělitelný bázovým polynomem y^3. Tím se nám algoritmus nalezení báze zastavil.

Výhodou Gröbnerovy báze je, že pomůže nalézt algebraickou varietu $V(I)$. tj. body v $(x, y) \in \mathbb{R}^2$, pro které je $f_1 = f_2 = 0$ – jinými slovy řešení těchto dvou polynomiálních rovnic. Pro Gröbnerovu bázi totiž příslušné bázové polynomy mají separované proměnné. Místo původních polynomiálních rovnic $f_1 = f_2 = 0$ máme ekvivalentní soustavu rovnic $x - 2y^2 = 0$ a $y^3 = 0$, kterou vyřešíme zpětnou eliminací. V našem případě je vidět, že vyhovuje jediný bod, $V(I) = (0, 0)$.

1.4. Vyřešte soustavu polynomiálních rovnic

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

Řešení. Nalezneme Gröbnerovu bázi vzhledem k lexikografickému uspořádání s $x > y > z$. Vedoucí monomy polynomů nejsou nesoudělné, a proto můžeme dělit a tím redukovat bázi. Zafixujme například $f_1 := x + y + z^2 - 1$ a dělme tímto polynomem zbylé dva. Dostáváme

$$x + y^2 + z - 1 = f_1 + y^2 - y - z^2 + z$$

a

$$x^2 + y + z - 1 = (x - y - z^2 + 1)f_1 + y^2 + 2yz^2 - y + z^4 - 2z^2 + z.$$

První zbytek označme f_2. Druhý zbytek můžeme dělit prvním a dostaneme

$$y^2 + 2yz^2 - y + z^4 - 2z^2 + z = f_2 + 2yz^2 + z^4 - z^2.$$

Tento zbytek označme f_3. Nyní už máme redukovanou bázi

$$\langle f_1, f_2, f_3 \rangle = \langle x + y + z^2 - 1, y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2 \rangle.$$

Na řadu přichází vytvoření S–polynomu

$$2z^2 f_2 - y f_3 = -yz^4 - yz^2 - 2z^4 + 2z^3.$$

Tento polynom (nebo raději jeho dvojnásobek) vydělíme polynomem f_3:

$$-2yz^4 - 2yz^2 - 4z^4 + 4z^3 = -(z^2 + 1)f_3 + z^6 - 4z^4 + 4z^3 - z^2$$

Do naší báze přidáme tento zbytek $f_4 := z^6 - 4z^4 + 4z^3 - z^2$ a tím už dostaneme bázi $\langle f_1, f_2, f_3, f_4 \rangle$ s eliminovanými proměnnými. Daň, kterou platíme za vyloučení proměnných je, že polynom f_4 je sice o jedné neznámé (eliminační ideál), ale má vysoký stupeň. V tomto případě lze ale jednoduše přijít na to, že $f_4 = z^2(z - 1)^2(z^2 + 2z - 1)$. Odtud plyne, že $z = 0$ nebo $z = 1$ nebo $z = -1 \pm \sqrt{2}$. Zpětnou eliminací dopočítáme zbylé proměnné. Zjistíme, že řešením soustavy jsou body $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ a $(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})$.