

KAPITOLA 4

Gröbnerove bázy

1. Usporiadanie monómov

Pracujeme v okruhu polynómov $k[x_1, \dots, x_n]$. Pripomeňme si označenie: ak $\alpha \in (\mathbb{N}_0)^n$, čiže $\alpha = (\alpha_1, \dots, \alpha_n)$ kde $\alpha_i \in \mathbb{N}_0$, potom x^α označuje monóm

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

DEFINÍCIA 1.1. Reláciu $>$ budeme nazývať *usporiadanie monómov*, ak

- $>$ je lineárne usporiadanie monómov (má vlastnosť trichotómie),
- $>$ je kompatibilné s násobením (ak $x^\alpha > x^\beta$ potom $x^\alpha x^\gamma > x^\beta x^\gamma$ pre ľubovoľné $\alpha, \beta, \gamma \in (\mathbb{N}_0)^n$),
- $>$ je dobré usporiadanie (každá množina monómov má najmenší prvok).

Bude užitočné si uvedomiť, že podmienka, aby usporiadanie bolo dobré, je ekvivalentná podmienke, že každá klesajúca postupnosť monómov

$$(4) \quad x^\alpha > x^\beta > x^\gamma > \dots$$

je konečná. Naozaj, majme klesajúcu postupnosť monómov (4). Ak táto postupnosť je nekonečná, potom množina $\{x^\alpha, x^\beta, x^\gamma, \dots\}$ nemá najmenší prvok, čiže usporiadanie $>$ nie je dobré. Opačne, nech usporiadanie $>$ nie je dobré, čiže existuje množina $M = \{x^\alpha\}_{\alpha \in \mathcal{A}}$, ktorá nemá najmenší prvok, teda pre každý prvok $x^\alpha \in M$ ($\alpha \in \mathcal{A}$) existuje v M prvok $x^{\alpha'}$ ($\alpha' \in \mathcal{A}$), ktorý je od neho menší. Takto sme ale zostrojili nekonečnú klesajúcu postupnosť.

Uvedieme si teraz najdôležitejšie príklady usporiadaní monómov.

Lexikografické usporiadanie. Pre monómy x^α, x^β ($\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in (\mathbb{N}_0)^n$) platí, že $x^\alpha >_{lex} x^\beta$, ak pre prvý index i taký, že $\alpha_i \neq \beta_i$, platí $\alpha_i > \beta_i$. Tiež inak povedané, prvé nenulové číslo v $\alpha - \beta = (\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)$ je kladné.

PRÍKLAD 1.2. V lexikografickom usporiadaní máme

$$\begin{aligned} x_1 >_{lex} x_2 >_{lex} x_3 >_{lex} \dots \\ x_1 >_{lex} x_2^3 >_{lex} x_2 x_3 >_{lex} x_3^{100} \end{aligned}$$

TVRDENIE 1.3. *Lexikografické usporiadanie je usporiadanie monómov.*

Dôkaz. Každé dva rôzne monómy vieme porovnať: ak $x^\alpha \neq x^\beta$, čiže $\alpha \neq \beta$, potom existuje $i \in \{1, \dots, n\}$ také, že $\alpha_i \neq \beta_i$, a o poradí týchto dvoch monómov rozhodneme podľa prvého takého exponentu.

Nech teraz $x^\alpha >_{lex} x^\beta$, teda existuje také i , že $\alpha_i > \beta_i$, a pre všetky $j < i$ platí $\alpha_j = \beta_j$. Potom platí aj $\alpha_j + \gamma_j = \beta_j + \gamma_j$ pre $j < i$, a $\alpha_i + \gamma_i > \beta_i + \gamma_i$, čo je presne podmienka pre $x^\alpha x^\gamma >_{lex} x^\beta x^\gamma$.

Pre vlastnosť dobrého usporiadania, nech $\{x^\alpha\}_{\alpha \in \mathcal{A}}$ je ľubovoľná množina monómov, ukážeme, že má najmenší prvok. Nech $\mathcal{M}_0 = \{x^\alpha\}_{\alpha \in \mathcal{A}}$ je celá množina, a nech

$$\mathcal{M}_j = \{x^\alpha \in \mathcal{M}_{j-1} \mid \alpha_j \text{ je minimálne vyskytujúce sa v monómoch v } \mathcal{M}_{j-1}\}, \quad j = 1, \dots, n.$$

Pre každú množinu $\mathcal{M}_j$ potom platí, že všetky jej prvky sú menšie ako ľubovoľný prvok z $\mathcal{M}_{j-1} \setminus \mathcal{M}_j$, a teda aj ľubovoľný prvok z $\mathcal{M} \setminus \mathcal{M}_j$. Navyše platí, že $\mathcal{M}_n$ obsahuje jediný monóm, čiže sme našli najmenší prvok množiny $\mathcal{M}$. $\square$

Graduované lexikografické usporiadanie. Pre monómy x^α, x^β platí, že $x^\alpha >_{\text{lex}} x^\beta$, ak $\deg x^\alpha > \deg x^\beta$, alebo ak $\deg x^\alpha = \deg x^\beta$ a $x^\alpha >_{\text{lex}} x^\beta$.

Graduované reverzné lexikografické usporiadanie. Pre monómy x^α, x^β platí, že $x^\alpha >_{\text{revlex}} x^\beta$, ak $\deg x^\alpha > \deg x^\beta$, alebo ak $\deg x^\alpha = \deg x^\beta$ a $x^\alpha <_{\text{lex}} x^\beta$.

PRÍKLAD 1.4. V graduovaných usporiadaniach máme

$$\begin{aligned} x_1 x_2^2 x_3^2 &<_{\text{lex}} x_2^7 x_3 & x_1 x_2^2 x_3^2 &<_{\text{revlex}} x_2^7 x_3, \\ x_1 x_2^2 x_3^2 &>_{\text{lex}} x_2^4 x_3 & x_1 x_2^2 x_3^2 &<_{\text{revlex}} x_2^4 x_3, \end{aligned}$$

DEFINÍCIA 1.5. Majme v $k[x_1, \dots, x_n]$ zvolené usporiadanie monómov a uvažujme polynóm

$$f = \sum_{\alpha} c_{\alpha} x^{\alpha} \in k[x_1, \dots, x_n].$$

Vedúci monóm polynómu f (označovať ho budeme $\text{LM}(f)$) je najväčší taký monóm x^{α} , pre ktorý $c_{\alpha} \neq 0$. Člen $c_{\alpha} x^{\alpha}$ sa potom nazýva *vedúci člen* (označovaný $\text{LT}(f)$) a koeficient c_{α} zas *vedúci koeficient* polynómu f (označovaný $\text{LC}(f)$).

PRÍKLAD 1.6. Majme polynóm $f = 5x_1x_2 + 7x_2^5 + 19x_3^{17} \in k[x_1, x_2, x_3]$. Ak uvažujeme lexikografické usporiadanie, tak vedúcim členom je $5x_1x_2$. Ak by sme však uvažovali niektoré z graduovaných usporiadaní, tak vedúcim členom je $19x_3^{17}$.

2. Algoritmus delenia

Uvedieme si teraz algoritmus delenia polynómu konečnou množinou polynómov v okruhu s viacerými premennými. Našou motiváciou je pre daný polynóm g a polynómy $f_1, \dots, f_k$ zistiť, či g patrí ideálu, ktorý je generovaný polynómami $f_1, \dots, f_k$. Budeme sa snažiť polynóm g zredukovať pomocou $f_1, \dots, f_k$ na čo najjednoduchší tvar, a následne rozhodnúť tento problém. Algoritmus by mohol vyzeráť takto:

VSTUP: polynóm g a polynómy $f_1, \dots, f_k$ z $k[x_1, \dots, x_n]$ so zvoleným usporiadaním monómov.

VÝSTUP: polynóm r taký, že $g = \sum h_i f_i + r$, kde $r = 0$ alebo $\text{LM}(f_i) \nmid \text{LM}(r) \forall f_i$.

ALGORITMUS:

- inicializácia: $g_0 := g$.
- iterácia (cez i): Ak $g_i = 0$, potom $r := 0$, a ukonči delenie.
Ak pre nejaké j platí, že $\text{LM}(f_j) \mid \text{LM}(g_i)$, tak

$$g_{i+1} := g_i - (\text{LT}(g_i)/\text{LT}(f_j))f_j.$$

Inak (vedúci monóm žiadneho polynómu spomedzi $f_1, \dots, f_k$ nedelí vedúci koeficient g_i) $r := g_i$, ukonči delenie.

PRÍKLAD 2.1. Predvedme algoritmus delenia pre $f_1 = xy + 1$, $f_2 = y + 1$ a $g = xy^2 + 1$. Uvažujeme $k[x, y]$ s lexikografickým usporiadaním.

- $g_0 = g$,
- $g_1 = g_0 - yf_1 = -y + 1$,

- $g_2 = g_1 + f_2 = 2$.

Nie je to ale jediný možný postup: mohli by sme hneď na začiatku začať redukovať polynóm g polynómom f_2 (vyskúšajte si to!).

TVRDENIE 2.2. *Výpočet pomocou algoritmu delenia skončí po konečnom počte krokov. Navyše, ak $g_i = 0$ pre nejaké i , potom $g \in (f_1, \dots, f_k)$.*

Dôkaz. Skúmame vedúce monómy polynómov g_i . Pri konštrukcii polynómu g_{i+1} sa vedúci člen g_i vykrátí s vedúcim členom polynómu $(\text{LT}(g_i)/\text{LT}(f_j))f_j$ a namiesto neho pribudnú ostatné členy tohoto polynómu. Z kompatibility usporiadania monómov s násobením však vidíme, že tieto nové monómy už budú menšie (v našom zvolenom usporiadaní), preto $\text{LM}(g_{i+1}) < \text{LM}(g_i)$. Takže máme klesajúcu postupnosť monómov

$$\text{LM}(g_0) = \text{LM}(g) > \text{LM}(g_1) > \text{LM}(g_2) > \dots$$

Z vlastnosti dobrého usporiadania vyplýva, že táto postupnosť je konečná, čiže sa počas výpočtu vykoná len konečne veľa redukcií. Na konci nám ostane buď $g_i = 0$ alebo také nenulové g_i , ktorého vedúci koeficient nie je deliteľný vedúcim koeficientom žiadneho f_j . V prvom prípade spätným dosadzovaním (ako v prípade Euklidovho algoritmu) dostávame

$$g = h_1 f_1 + \dots + h_k f_k,$$

teda vidíme, že $g \in (f_1, \dots, f_k)$. □

Bohužiaľ to, že deliacim algoritmom sa nám podarí g zredukovať na 0, je len postačujúca, a nie aj nutná podmienka pre $g \in (f_1, \dots, f_k)$, ako uvidíme v nasledujúcich príkladoch.

PRÍKLAD 2.3. Nech $f_1 = xy + 1$, $f_2 = y^2 - 1$ a $g = xy^2 - x$, uvažujme lexikografické usporiadanie. Deľme dvoma spôsobmi, pričom volíme vždy iné poradie polynómov, ktorými redukujeme g . Jedným spôsobom tak dostaneme výsledok $-x - y$, druhým sa nám podarí zredukovať g na 0. Teda $g \in (f_1, f_2)$.

PRÍKLAD 2.4. V domácej úlohe ste si overili, že

$$((x-1)(x-3), (x-1)(y-4), (y-2)(x-3), (y-2)(y-4)) = ((x-1)(x-3), x-y+1).$$

Naším algoritmom delenia sa nám však podarí ukázať iba o polynóme $(x-1)(x-3)$, že patrí do oboch ideálov.

3. Monomiálne ideály

DEFINÍCIA 3.1. Ideál $J \subset k[x_1, \dots, x_n]$ sa nazýva *monomiálny*, ak je generovaný nejakou (nie nutne konečnou) množinou monómov.

TVRDENIE 3.2. *Nech $J = (x^\beta \mid \beta \in \mathcal{B})$ je monomiálny ideál. Potom každý monóm v J je deliteľný niektorým z generátorov x^β .*

Dôkaz. (Ide viac o uvedomovacie cvičenie než o nejaké počítanie.)

Keďže $x^\alpha \in J$, kde $J = (x^\beta \mid \beta \in \mathcal{B})$, existujú polynómy $h_1, \dots, h_{k'}$ také, že

$$x^\alpha = \sum_{i=1}^{k'} h_i x^{\beta_i}, \quad \beta_i \in \mathcal{B}.$$

Každý z polynómov h_i rozdelíme na súčet jednotlivých členov, máme teda rovnosť

$$x^\alpha = \sum_{i=1}^k m_i x^{\beta_i}, \quad \beta_i \in \mathcal{B},$$

kde m_i sú len konštantné násobky monómov. Je zrejmé, že monóm x^α z ľavej strany rovnosti sa musí nachádzať spolu s nejakými nenulovými koeficientami aj na pravej strane; nech $m_{i_1} x^{\beta_{i_1}}, \dots, m_{i_l} x^{\beta_{i_l}}$ sú všetky tieto výskyty, čiže máme, že

$$x^\alpha = \sum_{j=1}^l m_{i_j} x^{\beta_{i_j}},$$

$$x^{\beta_{i_j}} \mid x^\alpha.$$

□

TVRDENIE 3.3. *Nech J je monomiálny ideál a $f = \sum c_\alpha x^\alpha \in J$. Potom každý člen $c_\alpha x^\alpha \in J$.*

Dôkaz. (Veľmi podobný dôkazu Tvrdenia 3.2) Nech $f \in J$, a preto

$$\sum c_\alpha x^\alpha = \sum_{i=1}^k m_i x^{\beta_i}, \quad \beta_i \in \mathcal{B},$$

kde m_i sú polynómy pozostávajúce len z jedného člena. Každý z monómov pri nenulovom koeficiente na ľavej strane rovnosti (t.j. každé x^α , pre ktoré $c_\alpha \neq 0$) sa musí nachádzať spolu s nejakými nenulovými koeficientami aj na pravej strane; nech $m_{i_1} x^{\beta_{i_1}}, \dots, m_{i_l} x^{\beta_{i_l}}$ sú všetky tieto výskyty, čiže máme, že

$$c_\alpha x^\alpha = \sum_{j=1}^l m_{i_j} x^{\beta_{i_j}},$$

a teda $c_\alpha x^\alpha \in J$.

□

DÔSLEDOK. *Monomiálny ideál je generovaný konečnou množinou monómov.*

Dôkaz. Nech J je monomiálny ideál. Z Hilbertovej vety o báze vieme, že ideál J je konečne generovaný, t.j. existujú $f_1, \dots, f_k \in k[x_1, \dots, x_n]$, že $J = (f_1, \dots, f_k)$. Nech $\{x^\alpha\}_{\alpha \in \mathcal{A}}$ je množina všetkých monómov, ktoré sa vyskytujú v $f_1, \dots, f_k$ s nenulovým koeficientom, teda je to konečná množina. Potom $J = (x^\alpha \mid \alpha \in \mathcal{A})$. Jedna inklúzia je zrejmá z vlastností ideálov, druhá vyplýva z Tvrdenia 3.3, pretože J je monomiálny. □

Z uvedených vlastností vyplýva, že monomiálne ideály sú výpočtovo veľmi jednoduché: vieme ľahko rozhodnúť, či nejaký polynóm patrí danému monomiálnemu ideálu, lebo algoritmus delenia nám v tomto prípade dá vždy správnu odpoveď, stačí redukovať monómami, ktoré generujú ideál: ak $g \in J$, J monomiálny, potom podľa Tvrdenia 3.3 každý člen polynómu g patrí do J , špeciálne, $\text{LT}(g) \in J$. Z Tvrdenia 3.2 potom vidíme, že $\text{LT}(g)$ je deliteľný niektorým generátorom, a teda g môžeme redukovať, až dostaneme $g_i = 0$ pre nejaké i .

Tiež pre monomiálny ideál vieme ľahko nájsť príslušnú algebraickú varietu:

PRÍKLAD 3.4. V $\mathbb{A}^3$ je $V(xy, yz, xz)$ zjednotením súradnicových osí. Algebraická varieta $V(xz, yz)$ je zas zjednotením súradnicovej roviny $z = 0$ a z -osi.

DEFINÍCIA 3.5. V $k[x_1, \dots, x_n]$ majme zvolené usporiadanie monómov. Nech $I \subset k[x_1, \dots, x_n]$ je ideál. *Ideál vedúcich členov* ideálu I je

$$\text{LT}(I) = (\text{LT}(f) \mid f \in I).$$

DEFINÍCIA 3.6. V $k[x_1, \dots, x_n]$ majme zvolené usporiadanie monómov a nech $I \subset k[x_1, \dots, x_n]$ je ideál. Gröbnerova báza ideálu I je množina polynómov

$$\{f_1, \dots, f_k\} \subset I$$

taká, že $\text{LT}(I) = (\text{LT}(f_1), \dots, \text{LT}(f_k))$.

Je zrejmé, že ak $\{f_1, \dots, f_k\}$ je Gröbnerova báza ideálu I , potom $(f_1, \dots, f_k) \subset I$, ale zatiaľ nie je jasné, či tieto dva ideály sa rovnajú, t.j. či Gröbnerova báza generuje celý ideál I .

VETA 3.7. V $k[x_1, \dots, x_n]$ majme zvolené usporiadanie monómov. Nech $I \subset k[x_1, \dots, x_n]$ je ideál a nech $\{f_1, \dots, f_k\}$ je jeho Gröbnerova báza. Potom algoritmom delenia, keď redukuje polynómami $f_1, \dots, f_k$, vieme vždy správne rozhodnúť, či daný polynóm patrí I . Presnejšie, ak $g \in I$, tak delením polynómami $f_1, \dots, f_k$ zredukujeme g na 0.

DÔSLEDOK. Gröbnerova báza ideálu je jeho množinou generátorov.

Dôkaz. Vieme, že ak $\{f_1, \dots, f_k\}$ je Gröbnerova báza ideálu I , potom $(f_1, \dots, f_k) \subset I$. Nech teraz $g \in I$. Podľa Vety 3.7 algoritmus delenia tento polynóm zredukuje do 0 a preto podľa Tvrdenia 2.2 $g \in (f_1, \dots, f_k)$. $\square$

Dôkaz Vety 3.7. Nech $g \in I$. Pri aplikovaní deliaceho algoritmu vypočítame g_1 ako $g_1 = g_0 - mf_j$, kde m je podiel vedúcich členov g_0 a f_j . Keďže $g_0 = g \in I$, potom zrejme aj $g_1 \in I$. Indukciou takto dostávame, že $g_i \in I$ pre všetky g_i v priebehu výpočtu.

Predpokladajme, že v algoritme dospejeme k takému g_i , že $g_i \neq 0$, ale g_i sa už nedá redukovať ďalej. Že sa nedá redukovať znamená, že vedúci člen g_i už nie je deliteľný vedúcim členom žiadneho z polynómov $f_1, \dots, f_k$. Podľa Tvrdenia 3.2 to znamená, že

$$\text{LT}(g_i) \notin (\text{LT}(f_1), \dots, \text{LT}(f_k)).$$

Avšak toto je ideál vedúcich členov ideálu I , a preto potom $g_i \notin I$, čo je spor. Polynóm g sa preto v každom kroku algoritmu dá redukovať, až kým nezostane 0. $\square$

PRÍKLAD 3.8. Nech $f_1 = x^2 - 4x + 3$, $f_2 = x - y + 1 \in k[x, y]$, uvažujme lexikografické usporiadanie. Zoberme ideál dvojbodovej algebraickej variety $I = (f_1, f_2) \subset k[x, y]$. Už v Príklade 2.4 sme sa presvedčili, že pomocou týchto dvoch generátorov nie je možné deliacim algoritmom zredukovať každý polynóm ideálu I na nulu. Z Vety 3.7 potom už vyplýva, že $\{f_1, f_2\}$ nie je Gröbnerova báza ideálu I . Bude ale poučné tento fakt overiť aj priamo pomocou definície Gröbnerovej bázy.

Ideál generovaný vedúcimi členmi našich generátorov je

$$(\text{LT}(f_1), \text{LT}(f_2)) = (x^2, x) = (x).$$

Polynóm $g = (y-2)(y-4) = y^2 - 6y + 8$ patrí ideálu I , lebo $g = f_1 + (-x - y + 5)f_2$. Jeho vedúci člen je $\text{LT}(g) = y^2$ a zrejme $y^2 \notin (x)$, teda máme, že $\text{LT}(I) \neq (\text{LT}(f_1), \text{LT}(f_2))$, a preto podľa definície $\{f_1, f_2\}$ nie je Gröbnerovou bázou.

PRÍKLAD 3.9. Nech $I \subset k[x_1, \dots, x_n]$ je hlavný ideál, teda $I = (f)$, $f \in k[x_1, \dots, x_n]$. Každý polynóm $g \in I$ je násobkom polynómu f , t.j. $g = hf$ pre nejaké $h \in k[x_1, \dots, x_n]$. Keďže akékoľvek usporiadanie monómov je kompatibilné s násobením, platí $\text{LT}(g) = \text{LT}(h)\text{LT}(f)$, a teda $\text{LT}(g) \in (\text{LT}(f))$. V tomto prípade teda máme, že $\text{LT}(I) = (\text{LT}(f))$, preto generátor hlavného ideálu je aj jeho Gröbnerovou bázou vzhľadom na ktorékoľvek usporiadanie monómov.

PRÍKLAD 3.10. Majme ideál $I = (y - x^2, z - x^3) \subset \mathbb{R}[x, y, z]$, uvažujme lexikografické usporiadanie také, že $z > y > x$. Ukážeme, že $\{y - x^2, z - x^3\}$ je Gröbnerova báza ideálu I .

Platí, že $(\text{LT}(y - x^2), \text{LT}(z - x^3)) = (y, z)$. Nech g je nenulový polynóm taký, že $\text{LT}(g) \notin (y, z)$. Z lexikografického usporiadania dostávame, že g neobsahuje premennú y ani z , teda g je polynóm iba v premennej x : $g = x^n + a_{n-1}x^{n-1} + \dots + a_0$. Ak by platilo, že $g \in I$, znamenalo by to $(g) \subset I$, a teda $V(I) \subset V(g)$. Množina $V(I)$ je krivka (t, t^2, t^3) , množina $V(g)$ je zas zjednotením rovín $(x - b_i)$, kde b_i sú riešenia polynómu g . Keďže však pole $\mathbb{R}$ je nekonečné, vidíme, že $V(I) \not\subset V(g)$: nech $a \in \mathbb{R}$ je také, že $g(a) \neq 0$, potom $(a, a^2, a^3) \in V(I)$, ale $(a, a^2, a^3) \notin V(g)$.

4. Výpočet Gröbnerovej bázy

Videli, že overovať z definície, či daná množina polynómov tvorí Gröbnerovu bázu ideálu, ktorý generuje, si v každom konkrétnom prípade vyžaduje dosť invencie. Uvedieme si teraz kritérium, pomocou ktorého budeme môcť takýto test urobiť pre každú zadanú množinu generátorov. Jeho základná myšlienka je ilustrovaná nasledovným príkladom.

PRÍKLAD 4.1. Uvažujme $f_1 = xy^2 + x + 1, f_2 = x^2y - 1 \in k[x, y]$, usporiadanie lexikografické. Ak chceme zistiť, či $\{f_1, f_2\}$ je Gröbnerova báza ideálu $I = (f_1, f_2)$, snažíme sa najprv nájsť polynóm $g \in I$ taký, aby $\text{LT}(g) \notin (\text{LT}(f_1), \text{LT}(f_2)) = (xy^2, x^2y)$. Skúsme vytvoriť takú kombináciu f_1 a f_2 , aby sa vedúce členy oboch polynómov navzájom eliminovali:

$$g := xf_1 - yf_2 = x(xy^2 + x + 1) - y(x^2y - 1) = x^2 + x + y.$$

Platí, že

$$\text{LT}(g) = x^2 \notin (x^2y, xy^2),$$

a teda nejde o Gröbnerovu bázu.

DEFINÍCIA 4.2. Nech $x^\alpha, x^\beta \in k[x_1, \dots, x_n]$ sú monómy. *Najmenším spoločným násobkom* monómov x^α, x^β nazývame monóm $x^\gamma \in k[x_1, \dots, x_n]$, kde $\gamma_i = \max\{\alpha_i, \beta_i\}$.

DEFINÍCIA 4.3. *S-polynómom* polynómov $f, g \in k[x_1, \dots, x_n]$ nazývame polynóm

$$S(f, g) = \frac{x^\gamma}{\text{LT}(f)}f - \frac{x^\gamma}{\text{LT}(g)}g,$$

kde x^γ je najmenší spoločný násobok monómov $\text{LM}(f), \text{LM}(g)$.

PRÍKLAD 4.4. Nech $f = x^3y^2 - x^2y^3 + x, g = 3x^4y + y^2$. Najmenším spoločným násobkom vedúcich monómov je x^4y^2 . Teda

$$S(f, g) = \frac{x^4y^2}{x^3y^2}f - \frac{x^4y^2}{3x^4y}g = xf - \frac{y}{3}g = -x^3y^3 + x^2 - \frac{y^3}{3}.$$

VETA 4.5 (**Buchbergerovo kritérium**). *V okruhu $k[x_1, \dots, x_n]$ so zvoleným usporiadaním monómov majme polynómy $f_1, \dots, f_k$. Tieto polynómy tvoria Gröbnerovu bázu ideálu $(f_1, \dots, f_k)$ práve vtedy, keď algoritmus delenia (polynómami $f_1, \dots, f_k$) redukuje každý S-polynóm $S(f_i, f_j)$ ($i, j = 1, \dots, k$) do nuly.*

Dôkaz. Z Vety 3.7 vyplýva, že ak $\{f_1, \dots, f_k\}$ je Gröbnerova báza, tak každý S-polynóm je algoritmom delenia zredukovaný do nuly, lebo $S(f_i, f_j) \in (f_1, \dots, f_k)$ pre všetky i, j .

Pre opačnú implikáciu nech sa všetky S-polynómy algoritmom delenia zredukujú do 0. Predpokladajme, že $\{f_1, \dots, f_k\}$ nie je Gröbnerova báza, teda existuje polynóm $g \in (f_1, \dots, f_k)$ taký, že

$$(5) \quad \text{LT}(g) \notin (\text{LT}(f_1), \dots, \text{LT}(f_k)).$$

Nech

$$(6) \quad g = g_1 f_1 + \dots + g_k f_k$$

je reprezentácia polynómu g pomocou generátorov ideálu, ktorá spĺňa nasledovné podmienky:

- (1) $x^\delta = \max\{\text{LM}(g_i f_i) \mid i = 1, \dots, k\}$ je minimálny,
- (2) počet takých i , že $\text{LM}(g_i f_i) = x^\delta$ je minimálny.

Po vhodnom preusporiadaní $f_1, \dots, f_k$ môžeme predpokladať, že

$$x^\delta = \text{LM}(g_1 f_1) = \text{LM}(g_2 f_2) = \dots = \text{LM}(g_s f_s) \quad \text{a} \quad \text{LM}(g_i f_i) < x^\delta \text{ pre } i > s.$$

Z (5) vyplýva, že $\text{LM}(g) \neq x^\delta$, teda x^δ na pravej strane rovnosti (6) sa musí vykrátiť, preto existujú aspoň dva sčítance, ktorých vedúci monóm je x^δ , teda $\text{LM}(g_1 f_1) = \text{LM}(g_2 f_2) = x^\delta$.

Zoberme si teraz S-polynóm $S(f_1, f_2)$:

$$(7) \quad S(f_1, f_2) = \frac{x^\gamma}{\text{LT}(f_1)} f_1 - \frac{x^\gamma}{\text{LT}(f_2)} f_2,$$

kde x^γ je najmenším spoločným násobkom monómov $\text{LM}(f_1), \text{LM}(f_2)$, a preto $x^\gamma \mid x^\delta$. Keďže tento polynóm sa deliacim algoritmom pomocou $\{f_1, \dots, f_k\}$ zredukuje do 0, spätným dosadzovaním dostaneme vyjadrenie

$$(8) \quad S(f_1, f_2) = \sum_{i=1}^k h_i f_i, \quad \text{pričom} \quad \text{LM}(h_i f_i) \leq \text{LM}(S(f_1, f_2)), \quad i = 1, \dots, k.$$

(Rozpíšte si to, aby ste si overili tvrdenie o vedúcich monónoch!) Z (7) a (8) dostávame rovnosť

$$\frac{x^\gamma}{\text{LT}(f_1)} f_1 - \frac{x^\gamma}{\text{LT}(f_2)} f_2 - \sum_{i=1}^k h_i f_i = 0.$$

Túto rovnosť prenášobíme monómom x^δ/x^γ , vhodnou konštantou a pripočítame k (6). Takto dostaneme nové vyjadrenie

$$g = \tilde{g}_1 f_1 + \dots + \tilde{g}_k f_k,$$

kde $\text{LM}(\tilde{g}_2 f_2) < x^\delta$, vedúci monóm v $\tilde{g}_1 f_1$ nevzrástol a vedúce monómy v ostatných sčítancoch ostali menšie ako x^δ , čo je spor s minimalitou vo vyjadrení (6). Preto $\{f_1, \dots, f_k\}$ je Gröbnerova báza. $\square$

PRÍKLAD 4.6. Vyriešme Príklad 3.10 pomocou Buchbergerovho kritéria. Ideál je generovaný dvoma polynómami, $f_1 = y - x^2$, $f_2 = z - x^3$, preto potrebujeme overiť len jeden S-polynóm:

$$S(f_1, f_2) = z f_1 - y f_2 = -z x^2 + y x^3.$$

Aplikujme na tento polynóm deliaci algoritmus:

- $g_0 = S(f_1, f_2) = -z x^2 + y x^3$,
- $g_1 = g_0 + x^2 f_2 = y x^3 - x^5$,
- $g_2 = g_1 - x^3 f_1 = 0$.

DÔSLEDOK (Buchbergerov algoritmus). V okruhu $k[x_1, \dots, x_n]$ so zvoleným usporiadaním monómov máme polynómy $f_1, \dots, f_k$. Gröbnerovu bázu ideálu $(f_1, \dots, f_k)$ získame nasledovným spôsobom:

VSTUP: polynómy $f_1, \dots, f_k$ z $k[x_1, \dots, x_n]$ so zvoleným usporiadaním monómov.

VÝSTUP: Gröbnerova báza G ideálu $(f_1, \dots, f_k)$.

ALGORITMUS:

- inicializácia: $G := \{f_1, \dots, f_k\}$
- iterácia:
 - Pre všetky $i, j = 1, \dots, |G|$, $i \neq j$ nech r_{ij} je zvyšok po aplikovaní algoritmu delenia na polynóm $S(f_i, f_j)$ (t.j. $\text{LT}(r_{ij})$ nie je deliteľný žiadnym vedúcim členom spomedzi polynómov $f_1, \dots, f_k$).
 - Ak všetky $r_{ij} = 0$, potom G je Gröbnerova báza, koniec algoritmu.
 - Inak $G := G \cup \{f_{|G|+1}, \dots, f_{|G|+s}\}$ je nová množina generátorov ideálu, kde $f_{|G|+1}, \dots, f_{|G|+s}$ sú nenulové r_{ij} .
 - Opakuj iteráciu pre túto novú množinu generátorov.

Dôkaz. Z Buchbergerovho kritéria vyplýva, že ak sa algoritmus zastaví, na konci dostaneme Gröbnerovu bázu ideálu $(f_1, \dots, f_k)$. Treba len ukázať, že algoritmus naozaj zastane po konečnom počte krokov.

Označme $G_1 = \{f_1, \dots, f_k\}$ (množina generátorov), $J_1 = (\text{LM}(f_1), \dots, \text{LM}(f_k))$ (ideál generovaný vedúcimi monómami generátorov). Ak sa niektorý z S-polynómov nedá pomocou G_1 zredukovať na 0, znamená to, $\text{LT}(r_{ij}) \notin J_1$ pre príslušný S-polynóm. V ďalšom kroku algoritmu potom dostávame

$$G_2 = \{f_1, \dots, f_k, f_{k+1}, \dots, f_{k+s}\} \text{ a } J_2 = (\text{LM}(f_1), \dots, \text{LM}(f_k), \text{LM}(f_{k+1}), \dots, \text{LM}(f_{k+s})),$$

pričom platí $J_1 \subsetneq J_2$. Ku každej iterácii algoritmu teda môžeme skonštruovať monomiálny ideál (generovaný vedúcimi monómami množiny generátorov), pričom platí

$$J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \dots$$

Okruh $k[x_1, \dots, x_n]$ je ale noetherovský (dôsledok Hilbertovej vety o báze), a preto táto postupnosť ideálov musí byť konečná. Posledný ideál J_N potom zodpovedá množine generátorov G_N , ktorá je už Gröbnerovou bázou ideálu $(f_1, \dots, f_k)$. $\square$

PRÍKLAD 4.7. Nájdime Gröbnerovu bázu ideálu $(x^2 - y, x^3 - z)$ v lexikografickom usporiadaní ($x > y > z$).

Označme $f_1 = x^2 - y$, $f_2 = x^3 - z$.

$$S(f_1, f_2) = xf_1 - f_2 = -xy + z.$$

Tento polynóm sa nedá redukovať pomocou $\{f_1, f_2\}$. Preto ho pridáme do množiny generátorov: $f_3 = -xy + z$. Pre ďalšiu iteráciu programu máme teraz generátory $\{f_1, f_2, f_3\}$. S-polynóm polynómov f_1, f_2 už nemusíme uvažovať, lebo touto novou množinou generátorov sa určite dá redukovať do 0 (vyskúšajte si to, ak Vám to nie je zrejmé!). Potrebujeme teraz preskúšať

$$\begin{aligned} S(f_1, f_3) &= yf_1 + xf_3 = xz - y^2, \\ S(f_2, f_3) &= yf_2 + x^2f_3 = x^2z - yz. \end{aligned}$$

Polynóm $S(f_1, f_3)$ sa pomocou $\{f_1, f_2, f_3\}$ nedá redukovať, teda označíme $f_4 = xz - y^2$. Polynóm $S(f_2, f_3)$ deliacim algoritmom pomocou $\{f_1, f_2, f_3\}$ zredukujeme do 0. Nová množina generátorov je $\{f_1, f_2, f_3, f_4\}$.

V ďalšej iterácii zistíme, že okrem $S(f_2, f_4) = y^3 - z^2$ sa nám všetky S-polynómy podarí zredukovať, preto nová množina generátorov je $\{f_1, f_2, f_3, f_4, f_5\}$, s $f_5 = y^3 - z^2$. V tejto sa už všetky S-polynómy redukujú, takže Gröbnerova báza ideálu $(x^2 - y, x^3 - z)$ je $\{f_1, f_2, f_3, f_4, f_5\}$.

POZNÁMKA 4.8. Ak $\{f_1, \dots, f_r\}$ je Gröbnerova báza ideálu $I = (f_1, \dots, f_r)$ a ak $f \in I$, potom zrejme aj $\{f_1, \dots, f_r, f\}$ je Gröbnerova báza I .

ZÁVER. Vyriešili sme problém, ktorý sme si v tejto kapitole sformulovali: pre dané polynómy g a $f_1, \dots, f_k$ z $k[x_1, \dots, x_n]$ vieme rozhodnúť, či $g \in (f_1, \dots, f_k)$:

- Zvolíme si usporiadanie monómov (najvhodnejšie je spravidla graduované reverzné lexikografické, vtedy je výpočet Gröbnerovej bázy najrýchlejší).
- Nájdeme Gröbnerovu bázu $\{h_1, \dots, h_r\}$ ideálu $(f_1, \dots, f_k)$.
- Aplikujeme deliaci algoritmus, kde g redukujeme polynómami $h_1, \dots, h_r$.
- $g \in (f_1, \dots, f_k)$ práve vtedy, keď sa nám ho podarí zredukovať do 0.

5. Systémy počítačovej algebry (CAS, computer algebra systems)

Gröbnerove bázy sú veľmi užitočným nástrojom pri manipulácii s polynómami, no na druhej strane ich výpočet je veľmi pracný. Prirodzene preto sú príslušné algoritmy implementované v špeciálnych tzv. systémoch počítačovej algebry a neustále optimalizované. Medzi tieto systémy patria:

- Komerčné:
 - Magma, Maple, Mathematica,...
- Voľne dostupné:
 - Macaulay2 (macaulay2.com, web.macaulay2.com), špeciálne zameraný na algebraickú geometriu,
 - Singular (www.singular.uni-kl.de) - asi sa už nevyvíja (?),
 - Sage (www.sagemath.org) - ambiciózny projekt, alternatíva k Magma,
 - Maxima,
 - CoCoA,
 - ...

6. Gröbnerove bázy a eliminácia

Podstatou teórie eliminácie je snaha zredukovať sústavu rovníc s veľa premennými na sústavu s menej premennými. Existuje viacero prístupov k tomuto problému. V tejto časti si uvedieme prístup pomocou Gröbnerových báz, v nasledujúcej cez rezultanty.

PRÍKLAD 6.1. Chceme nájsť všetky riešenia sústavy rovníc v $\mathbb{C}[x, y, z]$:

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

čiže chceme vymenovať všetky body algebraickej variety

$$X = V(x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1).$$

Postupovať budeme nasledovne:

- (1) Premietneme X na z -os a nájdeme body tohto priemetu. Algebraicky potrebujeme nájsť polynóm $f(z)$, ktorého korene budú presne body priemetu X do z -osi.
- (2) Nájdeme riešenia rovnice $f(z) = 0$ (tzv. *čiasťové riešenia*).
- (3) Budeme sa snažiť rozširovať čiasťové riešenia na *úplné riešenia*, teda skúsime postupne dopočítať druhú a prvú súradnicu.

S ťažkosťami sa stretávame hneď pri prvom kroku, pretože priemet algebraickej variety nemusí byť algebraická varieta:

PRÍKLAD 6.2. Nech $X = V(xy - 1) \subset \mathbb{A}^2$. Nech π je priemietanie na os y :

$$\pi: \mathbb{A}^2 \rightarrow \mathbb{A}^1, \quad (x, y) \mapsto y.$$

Potom $\pi(X)$ pozostáva zo všetkých bodov na y -osi, okrem počiatku $(0, 0)$, čo podľa našej definície nie je afinná algebraická varieta.

Z tohto príkladu vidíme, že čo sa týka popisu priemetu algebraickej variety, najlepšie, v čo môžeme dúfať, je nájsť rovnice najmenšej algebraickej variety, ktorá tento priemet obsahuje.

Ak $S \subset \mathbb{A}^n$ je ľubovoľná množina, symbolom $\overline{S}$ označujeme uzáver množiny S v Zariskiho topológii, teda je to najmenšia algebraická varieta obsahujúca S .

LEMA 6.3. Nech $S \subset \mathbb{A}^n$, potom $V(I(S)) = \overline{S}$.

Dôkaz. Platí, že $V(I(S)) \supset S$, a odtiaľ potom máme, že $\overline{V(I(S))} \supset \overline{S}$. Navyše platí, že $\overline{V(I(S))} = V(I(S))$, a jednu inklúziu sme ukázali.

Pre opačnú inklúziu, zrejme $S \subset \overline{S}$, a keďže $\overline{S}$ je algebraická varieta, tak $\overline{S} = V(J)$ pre nejaký ideál J . Z $S \subset V(J)$ potom máme $V(I(S)) \subset V(I(V(J))) = V(J) = \overline{S}$. $\square$

META 6.4 (o projekcii). Nech $X \subset \mathbb{A}^n(k)$ je algebraická varieta a nech $J = I(X)$. Nech ďalej π je premietanie

$$\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-r}, \quad (x_1, \dots, x_n) \mapsto (x_{r+1}, \dots, x_n).$$

Potom

$$\overline{\pi(X)} = V(J \cap k[x_{r+1}, \dots, x_n]).$$

Dôkaz. Ak $f \in k[x_{r+1}, \dots, x_n]$, tak pullback π^*f v tomto prípade znamená len toľko, že polynóm f uvažujeme ako polynóm v okruhu $k[x_1, \dots, x_n]$.

Ukážeme najprv inklúziu $\pi(X) \subset V(J \cap k[x_{r+1}, \dots, x_n])$, z nej už potom vyplýva inklúzia $\overline{\pi(X)} \subset V(J \cap k[x_{r+1}, \dots, x_n])$. Nech $a' = (a_{r+1}, \dots, a_n) \in \pi(X)$, čiže existujú $a_1, \dots, a_r \in k$ také, že $a = (a_1, \dots, a_n) \in X$. Ďalej nech $f \in J \cap k[x_{r+1}, \dots, x_n]$. Potom

$$f(a') = f(a_{r+1}, \dots, a_n) = (\pi^*f)(a_1, \dots, a_n) = (\pi^*f)(a) = 0,$$

lebo $\pi^*f \in J$, pričom π^*f je ten istý polynóm ako f .

Pre dôkaz opačnej inklúzie $V(J \cap k[x_{r+1}, \dots, x_n]) \subset \overline{\pi(X)}$ zoberme $f \in I(\pi(X))$, ukážeme, že $f \in J \cap k[x_{r+1}, \dots, x_n]$. Keďže $f \in k[x_{r+1}, \dots, x_n]$, stačí ukázať $f \in J$. Platí, že $f(a') = 0$ pre všetky $a' \in \pi(X)$, a teda $(\pi^*f)(a) = 0$ pre všetky $a \in X$ (ako v dôkaze prvej inklúzie). Preto $\pi^*f \in I(X) = J$. Ukázali sme, že $I(\pi(X)) \subset J \cap k[x_{r+1}, \dots, x_n]$, a tak

$$V(J \cap k[x_{r+1}, \dots, x_n]) \subset V(I(\pi(X))) = \overline{\pi(X)}.$$

$\square$

V predpokladoch vety sme museli uvažovať ideál $I(X)$ algebraickej variety, nie ľubovoľný ideál, ktorý ju definuje. Ak by sme chceli oslabiť tento predpoklad (teda mali

by sme *nejaký* ideál, ktorým je varieta X popísaná), potom musíme na druhej strane predpokladať, že pole k je algebraicky uzavreté. Naša veta potom vyzerá nasledovne:

VETA 6.5 (o projekcii). *Nech pole k je algebraicky uzavreté (napr. $k = \mathbb{C}$). Nech $J \subset k[x_1, \dots, x_n]$ je ideál, $X = V(J) \subset \mathbb{A}^n(k)$ a $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-r}$ je premietanie na posledných $n - r$ súradníc. Potom*

$$\overline{\pi(X)} = V(J \cap k[x_{r+1}, \dots, x_n]).$$

Dôkaz. Nech k je teda algebraicky uzavreté, $J \subset k[x_1, \dots, x_n]$ je *nejaký* ideál a $X = V(J) \subset \mathbb{A}^n$. Overíme najprv, že

$$\sqrt{J} \cap k[x_{r+1}, \dots, x_n] = \sqrt{J \cap k[x_{r+1}, \dots, x_n]}.$$

Nech $f \in \sqrt{J} \cap k[x_{r+1}, \dots, x_n]$. Lahko overíme, že to je ekvivalentné s tvrdením $f^d \in J \cap k[x_{r+1}, \dots, x_n]$ pre nejaké $d \in \mathbb{N}$ (preverte si detailne obe implikácie!), čo je už zrejme ekvivalentné s tvrdením, že $f \in \sqrt{J \cap k[x_{r+1}, \dots, x_n]}$.

Takže môžeme písať

$$\begin{aligned} \overline{\pi(X)} &= V(I(X) \cap k[x_{r+1}, \dots, x_n]) = V(I(V(J)) \cap k[x_{r+1}, \dots, x_n]) \\ &= V(\sqrt{J} \cap k[x_{r+1}, \dots, x_n]) = V(\sqrt{J \cap k[x_{r+1}, \dots, x_n]}) \\ &= V(J \cap k[x_{r+1}, \dots, x_n]), \end{aligned}$$

kde prvá rovnosť vyplýva z dokázanej Vety 6.4 o projekcii, tretia z Nullstellensatz, štvrtá z práve ukázanej rovnosti ideálov a piata rovnosť z tvrdenia, ktoré ste si dokazovali na úlohu (pre ideály I, J také, že $\sqrt{I} = \sqrt{J}$ platí $V(I) = V(J)$). $\square$

Ak $X = V(J)$, kde J je ľubovoľný ideál, a pole, nad ktorým pracujeme, nie je algebraicky uzavreté, môžeme vysloviť len slabšie tvrdenie:

TVRDENIE 6.6. *Nech $J \subset k[x_1, \dots, x_n]$ je ideál, $X = V(J) \subset \mathbb{A}^n$ a nech π je premietanie*

$$\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-r}, \quad (x_1, \dots, x_n) \mapsto (x_{r+1}, \dots, x_n).$$

Potom

$$\overline{\pi(X)} \subseteq V(J \cap k[x_{r+1}, \dots, x_n]).$$

Dôkaz. Dôkaz príslušnej inklúzie vo Vete 6.4 bezo zmien platí aj v tomto prípade. $\square$

PRÍKLAD 6.7. Majme ideál $J = (y - 1, x^2 + 1) \subset \mathbb{R}[x, y]$ a označme $X = V(J) \subset \mathbb{A}^2(\mathbb{R})$. Platí, že $X = \emptyset$, preto aj $\pi(X) = \emptyset$ a $\overline{\pi(X)} = \emptyset$ (π je projekcia za druhú súradnicu: $(x, y) \mapsto (y)$). Naproti tomu, $J \cap \mathbb{R}[y] = (y - 1)$ (bude vysvetlené v nasledujúcej vete), teda $V(J \cap \mathbb{R}[y]) = \{(1)\} \neq \emptyset$.

Ani jedna verzia Vety 6.4 sa nedá v tomto prípade aplikovať, lebo jednak pole $\mathbb{R}$ nie je algebraicky uzavreté, a tiež $I(X) \neq J$, lebo $I(X) = (1) = \mathbb{R}[x, y]$.

VETA 6.8 (o eliminácii). *V okruhu $k[x_1, \dots, x_n]$ uvažujme lexikografické usporiadanie ($x_1 > x_2 > \dots > x_n$). Nech $J \subset k[x_1, \dots, x_n]$ je ideál a G jeho Gröbnerova báza. Potom*

$$J \cap k[x_{r+1}, \dots, x_n] = (G \cap k[x_{r+1}, \dots, x_n]).$$

Dôkaz. Zrejme platí, že $(G \cap k[x_{r+1}, \dots, x_n]) \subset J \cap k[x_{r+1}, \dots, x_n]$. Potrebujeme teda ešte dokázať, že ak $f \in J \cap k[x_{r+1}, \dots, x_n]$, potom f je generovaný polynómami z $G \cap k[x_{r+1}, \dots, x_n]$. Toto ukážeme pomocou algoritmu delenia. Keďže $f \in J$ a G je Gröbnerova báza ideálu J , algoritmom sa nám f podarí zredukovať na 0, a f napíšeme

ako kombináciu polynómov z G , ktoré sme pri redukcii použili. Uvažujeme lexikografické usporiadanie, a preto $G \cap k[x_{r+1}, \dots, x_n]$ sú presne tie polynómy z G , ktorých vedúci monóm obsahuje len $x_{r+1}, \dots, x_n$. Keďže aj $f \in k[x_{r+1}, \dots, x_n]$, pri redukcii budeme používať len polynómy z $G \cap k[x_{r+1}, \dots, x_n]$, preto

$$f = \sum h_i f_i, \quad \text{kde } f_i \in G \cap k[x_{r+1}, \dots, x_n] \text{ a } h_i \in k[x_{r+1}, \dots, x_n].$$

□

DEFINÍCIA 6.9. Nech $J \in k[x_1, \dots, x_n]$ je ideál. Ideál

$$J \cap k[x_{r+1}, \dots, x_n]$$

nazývame *r-tý eliminačný ideál* ideálu J .

PRÍKLAD (dokončenie príkladu 6.1). Nájdeme Gröbnerovu bázu ideálu $I = (x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1)$ pri lexikografickom usporiadaní (ide o redukovanú bázu, nájdenu pomocou Sage):

$$\begin{aligned} g_0 &= x + y + z^2 - 1, \\ g_1 &= y^2 - y - z^2 + z, \\ g_2 &= yz^2 + \frac{1}{2}z^4 - \frac{1}{2}z^2, \\ g_3 &= z^6 - 4z^4 + 4z^3 - z^2. \end{aligned}$$

Z predchádzajúcej vety vyplýva, že uzáver priemetu variety do z -osi je popísaný ideálom

$$I \cap k[z] = (z^6 - 4z^4 + 4z^3 - z^2).$$

Riešenia rovnice $g_3 = 0$ nájdeme pomocou faktorizácie polynómu g_3 (tiež použijeme Sage):

$$g_3 = z^2(z-1)^2(z^2 + 2z - 1),$$

teda máme $z \in \{0, 1, -1 \pm \sqrt{2}\}$. Súradnicu y dopočítame k týmto čiastočným riešeniam pomocou g_2 a g_1 , a napokon súradnicu x pomocou g_0 . Dostávame spolu päť riešení

$$\begin{aligned} &(1, 0, 0), (0, 1, 0), (0, 0, 1), \\ &(-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}), \\ &(-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}). \end{aligned}$$

PRÍKLAD 6.10. Hľadáme pomocou eliminácie (nad algebraicky uzavretým poľom) riešenia sústavy

$$\begin{aligned} xy &= 1 \\ xz &= 1. \end{aligned}$$

Gröbnerova báza príslušného ideálu pri lexikografickom usporiadaní je

$$G = \{y - z, xz - 1\}.$$

Druhý eliminačný ideál je

$$J \cap k[z] = (G \cap k[z]) = (0),$$

teda ľubovoľná hodnota z je čiastočným riešením. Geometricky (Veta 6.4) to znamená, že uzáverom priemetu tejto algebraickej variety na os z je celá os. V druhom kroku uvažujeme prvý eliminačný ideál

$$J \cap k[y, z] = (G \cap k[y, z]) = (y - z).$$

Vidíme, že každé čiastočné riešenie vieme jednoznačne rozšíriť na „dvojsúradnicové“, a síce riešeniami sú dvojice $(y, z) = (a, a)$ pre ľubovoľné $a \in k$. Znova si všimnime geometrický význam týchto riešení: uzáverom priemetu algebraickej variety do roviny yz je priamka definovaná rovnicou $y = z$. Nakoniec, pri hľadaní úplných riešení (teda s tromi súradnicami) použijeme zostávajúci polynóm $xz - 1$ z Gröbnerovej bázy. Okrem riešenia $(y, z) = (0, 0)$ vieme všetky rozšíriť. Toto presne zodpovedá geometrickej situácii: bod $(0, 0) \in \overline{\pi(X)}$, ale $(0, 0) \notin \pi(X)$. Teda riešenia počiatočnej sústavy sú tvaru (a^{-1}, a, a) , $a \neq 0$.

Videli sme, že nie každé čiastočné riešenie sa dá rozšíriť na úplné. Nie je ľahké charakterizovať situáciu, kedy sa riešenie rozširovať dá a kedy nie. Analýza podmienok pre možnosť rozšírenia je predmetom štúdia teórie eliminácie.

ZÁVER. Gröbnerove bázy sú nástrojom na riešenie sústavy algebraických rovníc. Pomáhajú nám zodpovedať o danej sústave otázky, či je táto sústava riešiteľná, či má konečne veľa riešení (pozor, nestačí len pozrieť na počet rovníc ako v prípade lineárnych variet!), a v prípade, že áno, vieme pomocou Gröbnerových báz nájsť všetky riešenia.