Geometria 2
(Algebraická geometria a komutatívna algebra)

Jana Chalmovianská Pílniková

Katedra algebry, geometrie a didaktiky matematiky
Fakulta matematiky, fyziky a informatiky
Komenského univerzita
Bratislava

2009

Autor: Jana Chalmovianská Pílniková
Názov: Geometria 2
Podnázov: Algebraická geometria a komutatívna algebra
Vydavateľ: Knižničné a edičné centrum FMFI UK
Grafická úprava: Jana Chalmovianská Pílniková
Rok vydania: 2009
Miesto vydania: Bratislava
Vydanie: prvé
Počet strán: 69
Internetová adresa: http://www.fmph.uniba.sk/index.php?id=el_st_m
ISBN: 978-80-89186-52-5

Obsah

KAPITOLA 1

Základné pojmy

1. Okruhy a polynómy

DEFINÍCIA 1.1. *Komutatívny okruh s jednotkou* je neprázdna množina R s dvoma binárnymi operáciami $+\colon R \times R \to R$, $.\colon R \times R \to R$, ktoré spĺňajú nasledovné vlastnosti:

(i) $(R, +)$ je komutatívna grupa, čiže
- $a + (b + c) = (a + b) + c$ pre všetky $a, b, c \in R$,
- $a + b = b + a$ pre všetky $a, b \in R$,
- $\exists 0 \in R$ s vlastnosťou, že $0 + a = a$ pre ľubovoľné $a \in R$,
- pre každé $a \in R$ existuje $(-a) \in R$ také, že $a + (-a) = 0$,

(ii) $(R, .)$ je komutatívny monoid, čiže
- $a.(b.c) = (a.b).c$ pre všetky $a, b, c \in R$,
- $a.b = b.a$ pre všetky $a, b \in R$,
- $\exists 1 \in R$ s vlastnosťou, že $1.a = a$ pre ľubovoľné $a \in R$,

(iii) pre všetky $a, b, c \in R$ platí $a.(b + c) = a.b + a.c$

POZNÁMKA 1.2. Znamienko násobenia budeme zvyčajne zo zápisu vynechávať.

PRÍKLAD 1.3. Nasledovné množiny so štandardne definovanými operáciami sčítania a násobenia predstavujú komutatívne okruhy:
- $\mathbb{Z}$ – množina všetkých celých čísel,
- $2\mathbb{Z}$ – množina všetkých párnych celých čísel,
- $\mathbb{Q}[x]$ – množina polynómov nad racionálnymi číslami (t.j. koeficienty sú racionálne čísla) s premennou x,
- $\mathbb{R}[x_1, x_2, \ldots, x_n]$ – množina polynómov nad reálnymi číslami s n premennými

Nech k je ľubovoľné pole, symbolom $k[x_1, x_2, \ldots, x_n]$ označujeme okruh polynómov nad k s neurčitými $x_1, x, \ldots, x_n$. Prvok z $k[x_1, x_2, \ldots, x_n]$ tvaru

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}, \qquad \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{N}_0 (= \mathbb{N} \cup \{0\}). \tag{1}$$

nazývame *monóm*. Ak $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}_0^n$, skrátene budeme zapisovať

$$x^\alpha = x_1^{\alpha_1}.x_2^{\alpha_2}.\ldots.x_n^{\alpha_n}.$$

Celé číslo

$$\deg x^\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

sa nazýva *stupeň monómu* (1).

Každý polynóm sa dá zapísať ako konečný súčet monómov

$$f = \sum_\alpha c_\alpha x^\alpha, \qquad c_\alpha \in k,$$

kde sčítavame cez konečne veľa navzájom rôznych n-tíc $\alpha \in \mathbb{N}_0^n$. Skalár $c_\alpha \in k$ nazývame *koeficientom* pri monóme x^α. Ak $c_\alpha \in k \neq 0$, tak hovoríme, že $c_\alpha x^\alpha$ je *členom* polynómu f. *Stupeň polynómu* f je číslo

$$\deg f = \max_{c_\alpha \neq 0} \{\deg x^\alpha\},$$

t.j. maximálny stupeň monómu, ktorý sa v polynóme vyskytuje s nenulovým koeficiencom.

2. Ideály

DEFINÍCIA 2.1. Nech R je komutatívny okruh s jednotkou. *Ideálom* v okruhu R je taká jeho neprázdna podmnožina $I \subseteq R$, pre ktorú platí

(i) ak $a, b \in I$, tak aj $a + b \in I$,
(ii) ak $a \in I$ a $r \in R$, tak $a.r \in I$.

Množina $G \subset R$ sa nazýva množina *generátorov* ideálu I, ak

(i) $G \subset I$,
(ii) každý element $a \in I$ sa dá napísať ako konečná kombinácia prvkov z G nad okruhom R, t.j. existujú $r_1, r_2, \ldots, r_k \in R$ a $g_1, g_2, \ldots, g_k \in G$ také, že

$$a = r_1 g_1 + r_2 r_2 + \cdots + r_k g_k.$$

Zápis $(G) = I$ znamená, že množina G generuje ideál I. Podobne $(g_1, g_2, \ldots, g_k)$ označuje ideál generovaný prvkami $g_1, g_2, \ldots, g_k$.

PRÍKLAD 2.2.

- Ak $R = \mathbb{Z}$, tak množina všetkých párnych celých čísel je ideálom: súčet párnych čísel je párne číslo, a tiež súčin párneho čísla s ľubovoľným celým číslom je párne číslo. Tento ideál je generovaný číslom 2.
- Nech stále $R = \mathbb{Z}$. Množina všetkých nepárnych čísel netvorí ideál. (Prečo?)
- Nech $R = k[x]$. Všetky polynómy bez absolútneho člena tvoria ideál v $k[x]$. Tento ideál je generovaný polynómom x. Iným príkladom ideálu v tomto okruhu je množina všetkých násobkov polynómu $x - 1$. Ide o ideál generovaný polynómom $x - 1$
- Pre $R = k[x, y]$ je množina všetkých polynómov bez absolútneho člena ideálom, ktorý je generovaný množinou $\{x, y\}$, ide teda o ideál (x, y).
- V každom okruhu R, kde $0 \neq 1$, sú aspoň dva ideály: (0) a R.

LEMA 2.3. *Pre ideál $I \subseteq R$ platí*

$$I = R \quad \textit{práve vtedy, keď} \quad 1 \in I.$$

DEFINÍCIA 2.4. Ideál I v okruhu R sa nazýva

(i) *hlavný ideál*, ak existuje jednoprvková množina, ktorá ho generuje,
(ii) *maximálny ideál*, ak neexistuje ideál J taký, že $I \subsetneq J \subsetneq R$.
(iii) *prvoideál*, ak pre každé $a, b \in R$ také, že $ab \in I$, platí $a \in I$ alebo $b \in I$.

PRÍKLAD 2.5. Množina všetkých párnych čísel v okruhu $\mathbb{Z}$ je ideálom, ktorý je hlavný, lebo je generovaný číslom 2, ide teda o ideál (2). Tento ideál je zároveň maximálny a je aj prvoideálom.

Podobne $(3) \subseteq \mathbb{Z}$, ideál obsahujúci presne všetky celé čísla deliteľné číslom 3, je hlavný, maximálny a prvoideál.

Ideál $(6) \subseteq \mathbb{Z}$ čísel deliteľných číslom 6 je hlavný, ale nie je maximálny, lebo napríklad $(6) \subsetneq (2) \subsetneq \mathbb{Z}$. Taktiež to nie je prvoideál: nech $a = 2, b = 3$, potom $a.b = 6 \in (6)$, ale $a \notin (6)$, $b \notin (6)$.

PRÍKLAD 2.6. Nech $R = k[x, y]$. Ideál $I = (x, y)$ nie je hlavný. Je to ale maximálny ideál, čo ukážeme sporom: nech J je ideál, pre ktorý platí $I \subsetneq J \subsetneq k[x, y]$. Keďže $I \subsetneq J$, existuje polynóm f taký, že $f \in J$ ale $f \notin I$. I je ideál všetkých polynómov bez absolútneho člena, preto f osahuje nenulový absolútny člen, teda

$$f = a_0 + f_1, \quad \text{kde } a_0 \in k,\ a_0 \neq 0,\ f_1 \text{ obsahuje len členy stupňa aspoň 1.}$$

Máme preto, že $f_1 \in I$ (je to polynóm bez absolútneho člena). Odtiaľ

$$1 = a_0^{-1}.a_0 = a_0^{-1}(f - f_1) \in J \quad \text{lebo } f \in J, f_1 \in J,$$

a teda podľa lemy 2.3 platí $J = k[x, y]$.

DEFINÍCIA 2.7. Okruh R sa nazýva *okruhom hlavných ideálov*, ak každý ideál v R je hlavný.

VETA 2.8.

(i) *Okruh $\mathbb{Z}$ celých čísel je okruhom hlavných ideálov.*
(ii) *Okruh $k[x]$ polynómov s jednou premennou nad poľom je okruhom hlavných ideálov.*

PRÍKLAD 2.9. Zoberme v okruhu $\mathbb{Z}$ ideál $I = (21, 15)$. Pomocou Euklidovho algoritmu zistíme, že najväčším spoločným deliteľom čísel 21 a 15 je číslo 3. Z algoritmu navyše vieme získať aj zápis čísla 3 ako kombináciu pôvodných dvoch čísiel:

$$21 = 1.15 + 6$$
$$15 = 2.6 + 3$$
$$6 = 2.3 + 0$$

Z predposlednej rovnice vyjadríme číslo 3 a z predchádzajúcich rovíc (v našom prípade len z jednej) dosadzujeme, až kým nedostame rovnosť v požadovanom tvare:

$$3 = 15 - 2.6 = 15 - 2.(21 - 1.15) = 3.15 - 2.21$$

Vidíme teda, že $3 \in (21, 15)$. Je zrejmé, že $21 \in (3)$ a tiež $15 \in (3)$, a preto $I = (21, 15) = (3)$ je hlavný ideál.

PRÍKLAD 2.10. Euklidov algoritmus možno jednoducho aplikovať aj v okruhu $k[x]$. Nech napríklad $I = (x^4 + x, x^2 - 1)$. Postupným delením so zvyškom dostávame:

$$x^4 + x = (x^2 + 1).(x^2 - 1) + (x + 1)$$
$$x^2 - 1 = (x - 1).(x + 1) + 0$$

Najväčším spoločným deliteľom polynómov $x^4 + x$ a $x^2 - 1$ je teda $x + 1$. Navyše hneď z prvej rovnosti máme

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

takže $(x + 1) \in I = (x^4 + x, x^2 - 1)$ a preto $I = (x + 1)$.

ÚLOHA 1. V okruhu $\mathbb{Q}[x]$ majme ideál $I = (f, g)$, kde

$$f = x^4 - x^3 - 2x^2 + 5x - 3$$
$$g = x^5 - 3x^3 + 2x^2.$$

Nájdite polynóm h taký, že $I = (h)$, a vyjadrite tento polynóm ako kombináciu f a g nad $\mathbb{Q}[x]$, t.j. nájdite polynómy $u, v \in \mathbb{Q}[x]$, pre ktoré platí

$$h = u.f + v.g$$

KAPITOLA 2

Afinné algebraické variety

1. Definícia, príklady, základné vlastnosti

DEFINÍCIA 1.1. Nech k je pole a nech $n \in \mathbb{N}$. *Afinný priestor* dimenzie n nad k je množina

$$\mathbb{A}^n(k) = \{(a_1, \ldots, a_n) \mid a_i \in k\}.$$

Ak je z kontextu zrejmé, nad ktorým poľom pracujeme, prípadne ak v danej situácii nebude pole dôležité, budeme ho často z označenia vynechávať a označovať afinný priestor ako $\mathbb{A}^n$. Prvky afinného priestoru nazývame *body*.

Podľa tejto definície je afinný priestor taká istá množina ako vektorový priestor k^n. Niekedy sa v literatúre dokonca používa aj pre afinný priestor označenie k^n. My však budeme používať označenie $\mathbb{A}^n(k)$ pre odlíšenie jeho štruktúry od vektorového priestoru (napríklad body na rozdiel od vektorov nemôžeme sčítavať).

V nasledovnom budeme pre bod $a \in \mathbb{A}^n(k)$ a polynóm $f \in k[x_1, \ldots, x_n]$ pod výrazom $f(a)$ rozumieť hodnotu $f(a_1, \ldots, a_n)$, kde $a = (a_1, \ldots, a_n)$.

DEFINÍCIA 1.2. Nech k je pole a nech $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$. Množinu

$$V(f_1, \ldots, f_r) = \{a \in \mathbb{A}^n(k) \mid f_i(a) = 0 \ \forall i \in \{1, 2, \ldots, r\}\}$$

budeme nazývať *afinnou algebraickou varietou* definovanou polynómami $f_1, \ldots, f_r$.

Afinná varieta je teda množina všetkých riešení nejakého systému polynomických rovníc.

PRÍKLAD 1.3. Najjednoduchšie príklady afinných algebraických variet:

(i) celý priestor $\mathbb{A}^n(k) = V(0)$ (0 predstavuje nulový konštantný polynóm),
(ii) prázdna množina $\emptyset = V(1)$,
(iii) jednobodová množina $\{(a_1, \ldots, a_n)\} = V(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$,
(iv) dvojbodová množina $X = \{(1, 2), (3, 4)\} \subset \mathbb{A}^2(\mathbb{Q})$, $X = V((x-1)(x-3), (x-1)(y-4), (y-2)(x-3))$ (presvedčte sa o tom!)

PRÍKLAD 1.4. Nech $l_1, \ldots, l_r \in k[x_1, \ldots, x_n]$ sú lineárne polynómy, označme $X = V(l_1, \ldots, l_r)$. Ak $X \neq \emptyset$, nazývame X *lineárnou varietou*. Ak sú naviac rovnice definujúce X sú nezávislé, potom $d = n - r$ je *dimenzia lineárnej variety* X.

PRÍKLAD 1.5. Nech $f \in k[x, y]$ nie je konštantný polynóm. Algebraická varieta $X \subset \mathbb{A}^2(k)$ sa nazýva *rovinná (algebraická) krivka*. Uveďme si príklady takýchto kriviek:

(i) *Kužeľosečka* je množina bodov v $\mathbb{A}^2$ vyhovujúcich kvadratickej rovnici $f(x, y) = 0$.
(ii) Graf polynomickej funkcie $y = g(x)$ ($g \in k[x]$) je množina $X = V(y - g(x))$.
(iii) Graf racionálnej funkcie je tiež rovinná algebraická krivka: ak

$$g(x) = \frac{p(x)}{q(x)}, \quad p, q \text{ sú nesúdeliteľné polynómy nad } k,$$

potom graf funkcie g je množina bodov $X = V(yq(x) - p(x))$.

ÚLOHA 2. Načrtnite aspoň štyri z nasledujúcich rovinných kriviek (algebraické variety v $\mathbb{A}^2(\mathbb{R})$):

- $V(x^3 - y^2)$,
- $V(x^3 + x^2 - y^2)$,

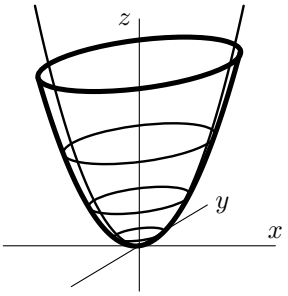
- $V(x^3 + x^2 + y^2)$,
- $V(x^4 - x^2 + y^2)$,
- $V(x^5 + x^4 + y^2)$,
- $V(x^6 - x^4 + y^2)$,
- $V((x^2 + y^2)^3 - 4x^2y^2)$,
- $V(x^n + y^n - 1)$, kde $n \geq 3$.

Pomôckou môže byť napríklad hľadanie prienikov krivky s rôznymi priamkami prechádzajúcimi bodom $(0, 0)$. Skúste pracovať bez pomoci systému počítačovej algebry (matlab, maple,...).

PRÍKLAD 1.6. *Vinutá kubika (priestorová kubika)* (angl. *twisted cubic*) je krivka X v trojrozmernom priestore $\mathbb{A}^3(k)$ parametrizovaná (t, t^2, t^3). Je to afinná algebraická varieta, $X = V(y - x^2, z - x^3)$.

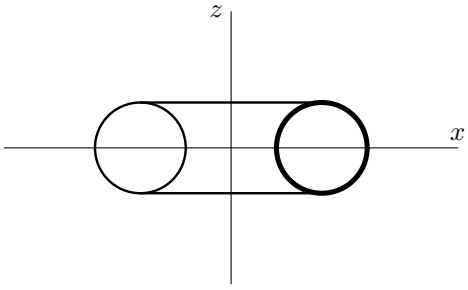
PRÍKLAD 1.7. *Nadplocha* je algebraická varieta v $\mathbb{A}^n(k)$ definovaná jediným nekonštantným polynómom z $k[x_1, \ldots, x_n]$. Nadplocha v $\mathbb{A}^3$ sa nazýva tiež *plocha. Dimenzia nadplochy v* $\mathbb{A}^n$ je (definitoricky) $n - 1$. (Niekedy sa nadplocha definuje len pre $n \geq 3$.)

PRÍKLAD 1.8. Skúsme popísať plochu X, ktorá vznikne rotáciu paraboly $z = x^2$ (parabola leží v rovine $y = 0$) okolo osi z.



Ak urobíme rezy plochy X rovinou rovnobežnou so súradnicovou rovinou xy, prienikom bude vždy kružnica so stredom na z-osi (keďže ide o rotačnú plochu). Súradnica z každého bodu na ploche závisí teda len od vzdialenosti tohto bodu od z-osi, čo je $r = \sqrt{x^2 + y^2}$. Stačí v rovnici pre pôvodnú parabolu napísať r namiesto x a máme $X = V(z - (x^2 + y^2))$.

ÚLOHA 3. Skúste nájsť rovnice nejakej ďalšej rotačnej plochy, napríklad torusu, ktorý vznikne rotáciou kružnice C okolo osi z, kde C je kružnica v súradnicovej rovine xz so stredom v $(2, 0, 0)$ a polomerom 1.



Definovali sme si dimenziu (rozmer) algebraickej variety v špeciálnych prípadoch nadroviny a lineárnej variety. Rozmer sa dá definovať všeobecne pre ľubovoľnú varietu, ale je to prekvapivo komplikovaná úloha, preto túto definíciu zatiaľ neuvádzame. Jeden špeciálny prípad ale ešte spomenúť môžme:

DEFINÍCIA 1.9. Nech $f_1, \dots, f_r \in k[x_1, \dots, x_n]$. Hovoríme, že $X = V(f_1, \dots, f_r)$ je *nularozmerná* algebraická varieta, ak sústava $f_1 = 0, \dots, f_r = 0$ je v $\bar{k}$ riešiteľná a má nad týmto poľom konečne veľa riešení ($\bar{k}$ označuje algebraický uzáver poľa k).

PRÍKLAD 1.10. Algebraické variety (iii) a (iv) z príkladu 1.3 sú nularozmerné. Algebraická varieta $V(x^2 + y^2) \subset \mathbb{A}^2(\mathbb{R})$ nie je 0-rozmerná, aj keď nad $\mathbb{R}$ má rovnica $x^2 + y^2 = 0$ jediné riešenie $(0, 0)$. Nad $\mathbb{C} = \bar{\mathbb{R}}$ má totiž táto rovnica nekonečne veľa riešení.

Zatiaľ sme si uviedli len príklady podmnožín $\mathbb{A}^n(k)$, ktoré sú afinnými varietami. Je poučné uviesť si aj iné množiny a ukázať o nich, že varietami nie sú.

PRÍKLAD 1.11. Majme v $\mathbb{A}^2(\mathbb{R})$ množinu $M = \{\dots, (-1, 0), (0, 0), (1, 0), (2, 0), \dots\}$. Ukážeme, že táto množina nie je algebraickou varietou.

Nech $p(x, y)$ je taký polynóm, že $p(a, b) = 0$ vždy, keď $b = 0$ a $a \in \mathbb{Z}$. Skúmajme reštrikciu tohto polynómu na x-os: pôjde o polynóm v jednej premennej

$$q(x) = p(x, 0) = a_n x^n + \cdots + a_1 x + a_0.$$

Keďže $q(n) = p(n, 0) = 0$ pre všetky $n \in \mathbb{Z}$, má polynóm q nekonečne veľa riešení, a teda $q \equiv 0$. Potom ale pre ľubovoľné $a \in \mathbb{R}$ platí, že

$$p(a, 0) = q(a) = 0.$$

Ukázali sme, že ak polynómu $p \in \mathbb{R}[x, y]$ vyhovujú ako korene všetky body množiny M, tak mu vyhovujú všetky body na x-osi. Preto M nie je algebraickou varietou. Presnejšie, najmenšou algebraickou varietou obsahujúcou množinu M je celá x-os.

ÚLOHA 4. V $\mathbb{A}^2(\mathbb{R})$ majme množiny

$$M_1 = \{(1, 1), (\frac{1}{2}, \frac{1}{2}), (\frac{1}{3}, \frac{1}{3}), \dots, (\frac{1}{n}, \frac{1}{n})\}$$
$$M_2 = \{(1, 1), (\frac{1}{2}, \frac{1}{2}), (\frac{1}{3}, \frac{1}{3}), \dots, (\frac{1}{n}, \frac{1}{n}), \dots\}$$

O každej zistite, či je algebraickou varietou: ak nie, dokážte, ak áno, najdite definujúce rovnice.

* ÚLOHA 5. Nech $M \subset \mathbb{A}^1(\mathbb{C})$ pozostáva z tých bodov komplexnej afinnej priamky, ktorých súradnica je reálna. Je množina M algebraickou varietou v $\mathbb{A}^1(\mathbb{C})$?

TVRDENIE 1.12. *Nech $X_1, X_2 \subset \mathbb{A}^n(k)$ sú afinné algebraické variety. Potom aj $X_1 \cap X_2$ a $X_1 \cup X_2$ sú afinné algebraické variety.*

Dôkaz. Keďže X_1 a X_2 sú algebraické variety, existujú polynómy $f_1, \dots, f_r, g_1, \dots, g_s \in k[x_1, \dots, x_n]$, že

$$X_1 = V(f_1, \dots, f_r),$$
$$X_2 = V(g_1, \dots, g_s).$$

Ukážeme, že

$$X_1 \cap X_2 = V(f_1, \dots, f_r, g_1, \dots, g_s),$$
$$X_1 \cup X_2 = V(f_i g_j \mid i = 1, \dots, r, j = 1, \dots, s).$$

Prvá rovnosť (o prieniku) je jednoduchá:

$$a = (a_1, \dots, a_n) \in X_1 \cap X_2 \;\Leftrightarrow\; a \in X_1 \;\wedge\; a \in X_2 \;\Leftrightarrow$$
$$f_i(a) = 0 \;\forall i \;\wedge\; g_j(a) = 0 \;\forall j \;\Leftrightarrow\; a \in V(f_1, \dots, f_r, g_1, \dots, g_s).$$

Druhú rovnosť ukážeme tak, že ukážeme obe inklúzie.

Nech $a \in X_1$, čiže $f_i(a) = 0 \;\forall i$. Potom ale platí aj $f_i g_j(a) = 0 \;\forall i, j$, teda $a \in V(f_i g_j \mid i = 1, \dots, r, j = 1, \dots, s)$. Ukázali sme, že $X_1 \subset V(f_i g_j)$. Podobne sa ukáže, že $X_2 \subset V(f_i g_j)$, a teda máme dokázanú inklúziu „$\subset$". Pre opačnú inklúziu predpokladajme, $a \in V(f_i g_j)$, t.j. $f_i g_j(a) = 0 \;\forall i, j$. Ak $a \in X_1$, sme hotoví. Ak $a \notin X_1$, tak existuje $l \in \{1, \dots, r\}$, že $f_l(a) \neq 0$.

Platí však, že $f_l g_j(a) = 0$ pre všetky $j = 1, \ldots, s$. Preto musí platiť, že $g_j(a) = 0$ pre všetky $j = 1, \ldots, s$, a teda $a \in X_2$. □

DÔSLEDOK. *Zjednotenie konečného počtu algebraických variet a prienik konečného počtu algebraických variet sú tiež algebraické variety.*

ÚLOHA 6. Zapíšte jednotkovú kružnicu spolu so svojím stredom ako algebraickú varietu, čiže nájdite polynomické rovnice, ktorých riešením sú presne body jednotkovej kružnice a jej stred.

TVRDENIE 1.13. *Afinná algebraická varieta v $\mathbb{A}^n(\mathbb{R})$ je v topológii, ktorá pochádza zo štandardnej euklidovskej metriky, uzavretou množinou.*

Dôkaz. Nech $X \subset \mathbb{A}^n(\mathbb{R})$, $X = V(f_1, \ldots, f_r)$. Polynóm $f_i(x_1, \ldots, x_n)$ predstavuje spojitú funkciu $\mathbb{A}^n(\mathbb{R}) \to \mathbb{R}$, a preto korene polynomickej rovnice $f_i(x_1, \ldots, x_n) = 0$ tvoria uzavretú podmnožinu $\mathbb{A}^n(\mathbb{R})$. Ak si označíme $X_i = V(f_i)$, tak $X_i, i = 1, \ldots, r$ sú uzavreté množiny, a $X = X_1 \cap X_2 \cap \cdots \cap X_r$ je preto tiež uzavretá množina. □

PRÍKLAD 1.14. Množina M všetkých bodov na jednotkovej kružnici okrem bodu $(1, 0)$ netvorí afinnú varietu. Bod $(1, 0)$ je totiž hraničným bodom množiny M, ale $(1, 0) \notin M$, takže M nie je uzavretá množina a podľa predchádzajúceho tvrdenia nemôže byť afinnou algebraickou varietou.

VETA 1.15. *Nech je pole k nekonečné, nech $n \in \mathbb{N}$ a nech $X \subset \mathbb{A}^n(k)$ je nadplocha.*

(i) *Existuje nekonečne veľa bodov nepatriacich X.*
(ii) *Ak navyše k je algebraicky uzavreté a $n \geq 2$, tak existuje nekonečne veľa bodov patriacich nadploche X.*

Dôkaz. (i) Postupujeme indukciou. Ak $n = 1$, tvrdenie vety platí, keďže každá nadplocha v tomto prípade pozostáva z konečného počtu bodov. Predpokladajme, že $n > 1$ a že tvdenie platí pre $n - 1$. Označme si $f(x_1, \ldots, x_n)$ nekonštantný polynóm definujúci nadplochu X. Bez ujmy na všeobecnosti môžme predpokladať, že x_n sa vyskytuje v zápise f, a tento polynóm teda môžeme napísať v tvare

$$f = \sum_{i=0}^{d} f_i(x_1, \ldots, x_{n-1}) x_n^i, \quad \text{kde } d > 0, f_i \in k[x_1, \ldots, x_{n-1}] \ \forall i \text{ a } f_d \not\equiv 0. \tag{2}$$

Polynóm f_d definuje nadrovinu v $\mathbb{A}^{n-1}(k)$ a podľa indukčného predpokladu existuje bod $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}(k) \setminus V(f_d)$, čiže $f_d(a_1, \ldots, a_{n-1}) \neq 0$. Potom $f(a_1, \ldots, a_{n-1}, x_n)$ je nenulový polynóm s premennou x_n a teda z tvrdenia pre $n = 1$ existuje nekonečne veľa a_n takých, že $f(a_1, \ldots, a_{n-1}, a_n) \neq 0$.

(ii) Nech f je ako v (2). Z tvrdenia (i) máme, že existuje nekonečne veľa bodov $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}(k)$ takých, že $f_d(a_1, \ldots, a_{n-1}) \neq 0$. Keďže k je algebraicky uzavreté, pre každý taký bod existuje $a_n \in k$, že $f(a_1, \ldots, a_{n-1}, a_n) = 0$. □

ÚLOHA 7. Overte, že dodatočné predpoklady v tvrdení (ii) predchádzajúcej vety sú nevyhnutné: nájdite kontrapríklad, keď k nie je algebraicky uzavreté pole.

* ÚLOHA 8. Nech k je pole, ktoré nie je algebraicky uzavreté. A nech $X \subset \mathbb{A}^n(k)$ je ľubovoľná algebraická varieta. Ukážte, že existuje polynóm $g \in k[x_1, \ldots, x_n]$ taký, že $X = V(g)$.

(Návod: Ak $X = V(f_1, \ldots, f_r)$, tak stačí ukázať, že existuje polynóm $h \in k[y_1, \ldots, y_r]$ taký, že $V(h) = \{(0, \ldots, 0)\}$. Potom $g = h(f_1, \ldots, f_r)$.)

2. Afinné algebraické variety a ideály

ÚLOHA 9. Zistite, či dané dve sústavy určujú tú istú lineárnu varietu v $\mathbb{A}^3(\mathbb{R})$, teda či platí $V(f_1, f_2(, f_3)) = V(g_1, g_2)$:

(a) $f_1 = x + y + z - 1, f_2 = x - y + 2z - 4$,
$g_1 = x + 5y - z + 5, g_2 = 3x + y + z - 2$.

(b) $f_1 = 2x + 3y - z, f_2 = x + y - 1, f_3 = x + z - 3$,
$g_1 = x + 3y - 2z + 3, g_2 = y - z + 2$.

(c) Navrhnite algoritmus, ktorý pre lineárne variety $X_1 = V(f_1, \dots, f_r)$, $X_2 = V(g_1, \dots, g_s) \subset \mathbb{A}^n$ rozhodne, či $X_1 = X_2$ (f_i, g_j sú lineárne polynómy).

Nech $X \subset \mathbb{A}^n(k)$ je afinná algebraická varieta,

$$X = V(f_1, \dots, f_r).$$

Skúsme nájsť ďalšie polynómy f také, že $f(a) = 0$ pre všetky $a \in X$. Ak pre $a \in \mathbb{A}^n$ a pre $f_1, f_2 \in k[x_1, \dots, x_n]$ platí, že $f_1(a) = 0$ a $f_2(a) = 0$, potom aj $(f_1 + f_2)(a) = 0$. Naviac, pre ľubovoľný polynóm $g \in k[x_1, \dots, x_n]$ platí aj $(gf_1)(a) = 0$. Z tohto pozorovania dostávame, že ak $X = V(f_1, \dots, f_r)$, tak pre každý polynóm f z ideálu $(f_1, \dots, f_r)$ potom $f(a) = 0$ pre všetky $a \in X$. Platí totiž, že

$$f \in (f_1, \dots, f_r) \;\Leftrightarrow\; \exists\, p_1, \dots, p_r \in k[x_1, \dots, x_n] \text{ také, že } f = p_1 f_1 + \cdots + p_r f_r.$$

Takže, ak $a \in X$, potom

$$f(a) = (p_1 f_1 + \cdots + p_r f_r)(a) = p_1(a) f_1(a) + \cdots + p_r(a) f_r(a) = 0.$$

LEMA 2.1. *V okruhu $k[x_1, \dots, x_n]$ platí, že $(f_1, \dots, f_r) = (g_1, \dots, g_s)$ práve vtedy,*

$$f_i \in (g_1, \dots, g_s)\ \forall i,\ \text{a tiež } g_j \in (f_1, \dots, f_r)\ \forall j. \tag{3}$$

Dôkaz. Je zrejmé, že ak $(f_1, \dots, f_r) = (g_1, \dots, g_s)$, potom platí (3). Pre opačnú implikáciu predpokladajme, že platí (3). Nech ďalej $f \in (f_1, \dots, f_r)$. To znamená, že

$$f = p_1 f_1 + \cdots + p_r f_r \text{ pre nejaké } p_1, \dots, p_r \in k[x_1, \dots, x_n].$$

Keďže pre všetky i máme $f_i \in (g_1, \dots, g_s)$, platí aj

$$f_i = q_{i1} g_1 + \cdots + q_{is} g_s \text{ pre nejaké } q_{i1}, \dots, q_{is} \in k[x_1, \dots, x_n].$$

Spolu odtiaľ potom dostávame

$$f = r_1 g_1 + \cdots + r_s g_s \text{ pre nejaké } r_1, \dots, r_s \in k[x_1, \dots, x_n],$$

teda $f \in (g_1, \dots, g_s)$. Podobne ukážeme aj $(g_1, \dots, g_s) \subseteq (f_1, \dots, f_r)$. □

LEMA 2.2. *Ak v okruhu $k[x_1, \dots, x_n]$ polynómy $f_1, \dots, f_r$ generujú ten istý ideál ako polynómy $g_1, \dots, g_s$, potom $V(f_1, \dots, f_r) = V(g_1, \dots, g_s)$.*

Dôkaz. Predpokladajme, že $a \in V(f_1, \dots, f_r)$, ukážeme, že potom $a \in V(g_1, \dots, g_s)$. Keďže $(f_1, \dots, f_r) = (g_1, \dots, g_s)$, pre každé j platí, že $g_j \in (f_1, \dots, f_r)$, teda g_j sa dá vyjadriť ako kombinácia polynómov $f_1, \dots, f_r$ nad $k[x_1, \dots, x_n]$:

$$g_j = p_{j1} f_1 + \cdots + p_{jr} f_r \text{ pre nejaké } p_{j1}, \dots, p_{jr} \in k[x_1, \dots, x_n].$$

Pre bod $a \in V(f_1, \dots, f_r)$ potom platí, že

$$g_j(a) = p_{j1}(a) f_1(a) + \cdots + p_{jr}(a) f_r(a) = 0,$$

a teda $a \in V(g_1, \dots, g_s)$, čiže $V(f_1, \dots, f_r) \subset V(g_1, \dots, g_s)$. Analogicky sa ukáže, že $V(g_1, \dots, g_s) \subset V(f_1, \dots, f_r)$. □

ÚLOHA 10. V príklade 1.3 (iv) bola dvojbodová množina $X = \{(1, 2), (3, 4)\} \subset \mathbb{A}^2(\mathbb{Q})$ popísaná ako riešenie sústavy troch kvadratických rovníc. Ukážte, že

$$((x-1)(x-3), (x-1)(y-4), (y-2)(x-3)) = (x^2 - 2x - 2y + 5, x - y + 1).$$

Preto tá istá algebraická varieta sa dá vyjadriť aj ako $V(x^2 - 2x - 2y + 5, x - y + 1)$.

POZNÁMKA 2.3. Pozor, obrátená implikácia z Lemy 2.2 neplatí: ak $V(f_1,\dots,f_r)=V(g_1,\dots,g_s)$, ešte to nemusí znamenať, že $(f_1,\dots,f_r)=(g_1,\dots,g_s)$. Nech napríklad $f=(x-1)^2(x+1)$ a $g=(x-1)(x+1)$. Vtedy $V((f))=V((g))$, avšak $(f)\neq(g)$: $f\in(g)$, ale $g\notin(f)$. Preto aj v predchádzajúcej úlohe nestačí overiť, že obe sústavy rovníc majú to isté riešenie.

Motivovaní predchádzajúcou lemou by sme radi algebraickú varietu namiesto nejakej konečnej množiny polynómov priradili ideálu. Najprv ale potrebujeme nejaké vedomosti o štruktúre ideálov v $k[x_1,\dots,x_n]$.

LEMA 2.4 (**Noetherová**). *V ľubovoľnom okruhu R sú nasledovné tvrdenia ekvivalentné:*

(1) *každý ideál v R je konečne generovaný (t.j. existuje konečná množina prvkov z R, ktorá ho generuje),*
(2) *každá rastúca reťaz ideálov $I_0\subset I_1\subset I_2\subset\dots$ je konečná, čiže $I_n=I_{n+1}$ pre dostatočne veľké n.*

DEFINÍCIA 2.5. Okruh R, v ktorom platia tvrdenia Lemy 2.4, sa nazýva *noetherovský*.

ÚLOHA 11. V okruhu R uvažujme rastúcu reťaz ideálov $I_0\subset I_1\subset I_2\subset\dots$. Ukážte, že

$$I_\infty=\bigcup_{i=0}^{\infty} I_i$$

je ideál v R.

Dôkaz Lemmy 2.4. Predpokladajme, že každý ideál v R je konečne generovaný. Majme rastúcu reťaz ideálov $I_0\subset I_1\subset I_2\subset\dots$. Podľa predchádzajúceho cvičenia je

$$I_\infty=\bigcup_{i=0}^{\infty} I_i$$

ideál. Nech $g_1,\dots,g_r\in I_\infty$ sú jeho generátory. Pre každé $j=1,\dots,r$ existuje $n_j\in\mathbb{N}$ také, že $g_j\in I_{n_j}$. Potom pre $N=\max\{n_1,\dots,n_r\}$ platí, že $I_N=I_\infty$.

Naopak teraz predpokladajme, že každá rastúca reťaz ideálov je konečná. Nech I je ideál generovaný prvkami f_α pre $\alpha\in A$. Ak I nie je generovaný konečným počtom f_α, môžme zostrojiť rastúcu reťaz ideálov

$$I_j=(f_{\alpha_1},\dots,f_{\alpha_j})\subset I_{j+1}=(f_{\alpha_1},\dots,f_{\alpha_{j+1}}),\quad \alpha_i\in A,$$

ktorá nie je konečná, čo je spor s naším predpokladom. □

PRÍKLAD 2.6. Okruh $\mathbb{Z}$ je okruhom hlavných ideálov: každý ideál v $\mathbb{Z}$ sa dá generovať jediným celým číslom (vyplýva to z Euklidovho algoritmu). Preto $\mathbb{Z}$ je príklad noetherovského okruhu.

Ak k je pole, v okruhu $k[x]$ je tiež definovaný Euklidov algoritmus na počítanie najväčšieho spoločného deliteľa. Preto aj $k[x]$ je okruhom hlavných ideálov, a teda je noetherovský.

ÚLOHA 12. Nech k je pole. Ukážte, že okruh polynómov s nekonečne veľa premennými $k[x_1,x_2,\dots]$ nie je noetherovský.

* ÚLOHA 13. Uvažujme množinu reálnych funkcií spojitých na intervale $\langle 0,1\rangle\subset\mathbb{R}$. Táto množina tvorí okruh. Ukážte, že ani tento okruh nie je noetherovský.

VETA 2.7 (**Hilbertova veta o báze**). *Ak R je noetherovský okruh, potom aj $R[x]$ je noetherovský okruh.*

Dôkaz. Nech $I\subset R[x]$ je ideál. Pre každé $m\in\mathbb{N}_0$ uvažujme množinu

$$J_m=\{a_m\in R\mid a_mx^m+a_{m-1}x^{m-1}+\dots+a_0\in I \text{ pre nejaké } a_0,\dots,a_{m-1}\in R\},$$

čiže J_m pozostáva z vedúcich koeficientov polynómov v I, ktoré sú stupňa m, a nuly. Ľahko sa ukáže, že J_m je ideál v R (overte si to!). Taktiež platí, že $J_m\subset J_{m+1}$ pre všetky m (overte si to!). Máme teda rastúcu reťaz ideálov v R,

$$J_0\subset J_1\subset J_2\subset\dots.$$

Keďže podľa predpokladu je R noetherovský, existuje $N \in \mathbb{N}$, že $J_n = J_N$ pre všetky $n > N$. Ďalej z noetherovskosti R máme, že každý z ideálov J_m je konečne generovaný:

$$J_0 = (a_{01}, \ldots, a_{0n_0})$$
$$J_1 = (a_{11}, \ldots, a_{1n_1})$$
$$\ldots$$
$$J_N = (a_{N1}, \ldots, a_{Nn_N})$$

Pre každé a_{ij} $(i = 0, \ldots, N, j = 1, \ldots, n_i)$ zvoľme polynóm $f_{ij} \in I$ stupňa i, ktorého vedúci člen je $a_{ij}x^i$. Ukážeme, že $I = (f_{ij})$.

Postupujeme indukciou na stupeň polynómu. Nech $f \in I$, je stupňa 0. Potom $f \in J_0$ a je teda kombináciou prvkov $a_{0j} = f_{0j}$, $(j = 1, \ldots n_0)$. Nech teda stupeň $f \in I$ je d a predpokladajme, že každý polynóm z I stupňa menšieho ako d sa dá napísať ako kombinácia polynómov f_{ij}. Máme, že

$$f = c_d x^d + \text{ členy nižších stupňov}$$

Potom $c_d \in J_d$, a preto

$$c_d = \sum_{i \le d} h_{ij} a_{ij} \quad \text{pre nejaké} \quad h_{ij} \in R.$$

Polynóm $g = f - \sum h_{ij} f_{ij} x^{d-i}$ má potom stupeň najviac $d-1$ a navyše $g \in I$. Podľa indukčného predpokladu preto $g \in (f_{ij})$, a teda aj $f \in (f_{ij})$. □

Dôsledok. *Nech k je pole. Potom je okruh $k[x_1, \ldots, x_n]$ noetherovský.*

Dôkaz. Pole k je noetherovský okruh, lebo má iba dva ideály, (0) a $k = (1)$, oba konečne generované. Okruh $k[x_1, \ldots, x_n]$ napíšeme ako $(k[x_1, \ldots, x_{n-1}])[x_n]$ a indukciou potom dostávame, že keď $k[x_1, \ldots, x_{n-1}]$ je noetherovský, potom aj $k[x_1, \ldots, x_n]$ je noetherovský. □

Definícia 2.8. Pre ľubovoľnú podmnožinu $F \subset k[x_1, \ldots, x_n]$ definujeme

$$V(F) = \{a \in \mathbb{A}^n(k) \mid f(a) = 0 \ \forall f \in F\}.$$

Z Hilbertovej vety o báze vieme, že $V(I)$ je afinná algebraická varieta, tak, ako sme si ju definovali na začiatku: ak $I = (F)$, teda I je ideál generovaný polynómami z F, potom zrejme $V(F) = V(I)$. Navyše, keďže $k[x_1, \ldots, x_n]$ je noetherovský, $I = (f_1, \ldots, f_r)$ pre nejaké $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, a teda máme $V(I) = V(f_1, \ldots, f_r)$.

Definícia 2.9. Pre ľubovoľnú podmnožinu $S \subset \mathbb{A}^n(k)$ definujeme

$$I(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \ \forall a \in S\}.$$

Podobne ako na začiatku prednášky ľahko overíme, že $I(S)$ je ideál v okruhu $k[x_1, \ldots, x_n]$.

Príklad 2.10. V priklade 1.11 sme o množine $M = \{\ldots, (-1, 0), (0, 0), (1, 0), (2, 0), \ldots\}$ ukázali, že nie je algebraickou varietou. Ideál $I(M)$ však existuje, v spomenutom príklade sme sa presvedčili, že $I(M) = (y)$.

Tvrdenie 2.11. *V nasledovnom I, J sú podmnožiny $k[x_1, \ldots, x_n]$ a S, T zas podmnožiny $\mathbb{A}^n(k)$. Platí:*

(i) *Ak $I \subset J$, potom $V(I) \supset V(J)$.*
Ak $S \subset T$, potom $I(S) \supset I(T)$.
(ii) $V(I(S)) \supset S$.
$I(V(I)) \supset I$.
(iii) $V(I(V(I))) = V(I)$.
$I(V(I(S))) = I(S)$.

Dôkaz. Dôkazy tvrdení (i) a (ii) sú len prepisovaním definícií pre $V()$ a $I()$. Tvrdenie (iii) potom vyplýva z (i) a (ii). □

DEFINÍCIA 2.12. Nech $\{I_\alpha\}_{\alpha\in A}$ je množina ideálov (nie nutne konečná). *Súčet ideálov* I_α je ideál

$$\sum_{\alpha\in A} I_\alpha = \{f_1 + \cdots + f_r \mid f_i \in I_{\alpha_i}, \alpha_i \in A\}.$$

POZNÁMKA 2.13. Presvedčte sa, že $\sum_{\alpha\in A} I_\alpha$ je naozaj ideál! Ide vlastne o najmenší ideál obsahujúci $\bigcup_{\alpha\in A} I_\alpha$.

TVRDENIE 2.14. *Nech* $I, J, I_\alpha \subset k[x_1, \ldots, x_n]$ *sú ideály. Potom*

- $\bigcap_{\alpha\in A} V(I_\alpha) = V(\sum_{\alpha\in A} I_\alpha)$,
- $V(I) \cup V(J) = V(IJ) = V(I \cap J)$.

Dôkaz. Keďže $\sum_{\alpha\in A} = (\bigcup_{\alpha\in A})$, platí

$$V(\sum_{\alpha\in A} I_\alpha) = V(\bigcup_{\alpha\in A} I_\alpha) = \{a \in \mathbb{A}^n \mid f(a) = 0 \ \forall f \in \bigcup_{\alpha\in A} I_\alpha\} =$$
$$\bigcap_{\alpha\in A} \{a \in \mathbb{A}^n \mid f(a) = 0 \ \forall f \in I_\alpha\} = \bigcap_{\alpha\in A} V(I_\alpha).$$

Pre dôkaz druhej rovnosti si všimnime, že

$$IJ \subset I \cap J \subset I, J.$$

Z predchádzajúceho tvdenia potom máme

$$V(I), V(J) \subset V(I \cap J) \subset V(IJ), \text{ čiže}$$
$$V(I) \cup V(J) \subset V(I \cap J) \subset V(IJ).$$

Stačí, keď ešte dokážeme, že $V(IJ) \subset V(I) \cup V(J)$.

Nech $a \in V(IJ)$ a predpokladajme, že $a \notin V(I)$. Potom existuje $f \in I$ také, že $f(a) \neq 0$. Keďže $a \in V(IJ)$, platí, že $fg(a) = 0$ pre všetky $g \in J$. Odtiaľ potom dostávame, že $g(a) = 0$ pre všetky $g \in J$, a teda že $a \in V(J)$. □

3. Zariskiho topológia

Vďaka tvrdeniu 2.14 môžme definovať špeciálnu topológiu v afinnom priestore $\mathbb{A}^n(k)$, nazývanú *Zariskiho topológia*. V nej uzavreté množiny budú presne všetky algebraické variety v $\mathbb{A}^n(k)$, a otvorené množiny teda doplnky k algberaickým varietám. Treba však overiť, že takto definovaný systém množín naozaj tvorí topológiu. Potrebujeme ukázať

(1) $\emptyset$ je otvorená množina,
(2) $\mathbb{A}^n$ je otvorená množina,
(3) ak U_1, U_2 sú otvorené, tak aj $U_1 \cap U_2$ je otvorená,
(4) ak $\{U_i\}_{i\in\mathcal{I}}$ sú otvorené, tak aj $\cup_{i\in\mathcal{I}} U_i$ je otvorená.

Preverme teda tieto axiómy:

(1) $\mathbb{A}^n$ je algebraická varieta ($\mathbb{A}^n = V(0)$), čiže podľa našej definície je to uzavretá množina, preto prázdna množina patrí medzi otvorené množiny.

(2) $\emptyset$ je algebraická varieta ($\emptyset = V(1)$), preto podobne aj $\mathbb{A}^n$ patrí medzi otvorené množiny.

(3) Nech U_1, U_2 sú otvorené množiny, chceme ukázať, že potom aj $U_1 \cap U_2$ je otvorená. Že U_1, U_2 sú otvorené, znamená, že $U_1 = \mathbb{A}^n \setminus X_1$, kde X_1 je algebraická varieta, podobne $U_2 = \mathbb{A}^n \setminus X_2$, kde X_2 je algebraická varieta. Prienik

$$U_1 \cap U_2 = (\mathbb{A}^n \setminus X_1) \cap (\mathbb{A}^n \setminus X_2) = \mathbb{A}^n \setminus X_1 \cup X_2.$$

Z tvrdenia 2.14 (prípadne dokonca už z dôsledku tvrdenia 1.12) vieme, že $X_1 \cup X_2$ je algebraická varieta, a teda $U_1 \cap U_2$ je otvorená množina.

(4) Nech $\{U_i\}_{i\in\mathcal{I}}$ sú otvorené množiny, čiže pre všetky $i \in \mathcal{I}$ platí $U_i = \mathbb{A}^n \setminus X_i$, kde X_i sú algebraické variety. Zjednotenie

$$\bigcup_{i\in\mathcal{I}} U_i = \bigcup_{i\in\mathcal{I}} (\mathbb{A}^n \setminus X_i) = \mathbb{A}^n \setminus (\bigcap_{i\in\mathcal{I}} X_i).$$

Znovu z tvrdenia 2.14 vidíme, že $\bigcap_{i\in\mathcal{I}} X_i$ je algebraická varieta, a teda $\cup_{i\in\mathcal{I}} U_i$ je naozaj otvorená množina.

Vo zvyšku kapitoly si podrobnejšie popíšeme túto topológiu na afinnej priamke a v afinnej rovine nad algebraicky uzavretým poľom k.

3.1. Zariskiho topológia na $\mathbb{A}^1(k)$. Algebraická varieta v $\mathbb{A}^1(k)$ je množina spoločných riešení niekoľkých polynomických rovníc: $X = V(f_1, \ldots, f_r),\ f_i \in k[x]$.

(a) Vybavme najprv špeciálny prípad, keď všetky polynómy sú konštanty 0. Vtedy máme, že $X = V(0) = \mathbb{A}^1$.
(b) Nech $f_1, \ldots, f_r$ nie sú nulové polynómy. Predpokladajme, že tieto polynómy sú nesúdeliteľné, to znamená, že nemajú spoločný koreň, a preto $X = \emptyset$.
(c) Nech $d \in k[x]$ je najväčší spoločný deliteľ polynómov $f_1, \ldots, f_r$, stupeň $d > 0$. Keďže k je algebraicky uzavreté, $g = (x-a_1)(x-a_2)\ldots(x-a_s)$ a $a_1, \ldots, a_s$ sú všetky spoločné korene polynómov $f_1, \ldots, f_r$, teda $X = \{a_1, \ldots, a_s\}$ je konečná množina.

Vidíme, že všetky neprázdne otvorené množiny v Zariskiho topológii na $\mathbb{A}^1$ sú doplnky konečných množín.

3.2. Zariskiho topológia na $\mathbb{A}^2(k)$. Popísať otvorené množiny v afinnej rovine je v porovnaní s priamkou omnoho komplikovanejšie. Musíme najprv trochu študovať polynómy v $k[x, y]$.

V nasledujúcej definícii, leme a jej dôsledkoch bude R predstavovať okruh $\mathbb{Z}$ alebo $k[t]$, kde k je pole. Pre nás budú dôležité konštrukcie a tvrdenia pre $R = k[t]$, ich význam sa však omnoho ľahšie predstavuje, ak $R = \mathbb{Z}$ – to je jediný dôvod, prečo nepracujeme priamo v $R = k[t]$. V oboch týchto okruhoch máme definovaný najväčší spoločný násobok či už celých čísel alebo polynómov s jednou premennou.

Definícia 3.1. Polynóm $p = p_0 + p_1 x + \cdots + p_d x^d \in R[x]$ sa nazýva *primitívny*, ak jeho koeficienty sú nesúdeliteľné t.j. ak najväčší spoločný deliteľ $p_0, p_1, \ldots, p_d$ je jednotka v R.

PRÍKLAD 3.2. Nech $R = \mathbb{Z}$. Polynóm $2x^2 + 6x + 5$ je primitívny, lebo najväčší spoločný deliteľ $\mathrm{nsd}(2, 6, 5) = 1$. Polynóm $8x^3 - 12x$ nie je primitívny, lebo $\mathrm{nsd}(8, 12) = 4$.

Nech $R = k[t]$. Polynóm $tx^2 + (t-1)x - t^2$ je primitívny, lebo $\mathrm{nsd}(t, t-1, t^2) = 1$. Polynóm $(t^2 - t)x^2 + (1 - t^2)x + (1 - t^3)$ nie je primitívny, lebo $\mathrm{nsd}(t^2 - t, 1 - t^2, 1 - t^3) = t - 1$.

LEMA 3.3 (**Gauss**). *Ak $p, q \in R[x]$ sú primitívne polynómy, potom aj ich súčin pq je primitívny.*

Dôkaz. Nech

$$\begin{aligned} p &= p_0 + p_1 x + \cdots + p_r x^r \\ q &= q_0 + q_1 x + \cdots + q_s x^s \end{aligned}$$

sú primitívne, predpokladajme, že ich súčin

$$pq = p_0 q_0 + (p_1 q_0 + p_0 q_1)x + \cdots + p_r q_s x^{r+s}$$

nie je. Teda existuje ireducibilný prvok $r \in R$ (prvočíslo, ak $R = \mathbb{Z}$, ireducibilný polynóm, ak $R = k[t]$) taký, že r delí všetky koeficienty polynómu pq. Keďže p, q sú primitívne, r nedelí niektoré z koeficientov p a tiež q. Nech i je najmenšie také, že $r \nmid p_i$, podobne nech j je najmenšie také, že $r \nmid q_j$. Pozrime sa na koeficient polynómu pq pri x^{i+j} – tento je rovný súčtu

$$\sum_{k+l=i+j} p_k q_l.$$

Prvok r delí v tomto súčte všetky $p_k q_l$ okrem jediného sčítanca $p_i q_j$, preto p nemôže deliť celý tento koeficient, čo je spor s naším predpokladom. □

DÔSLEDOK. *Ak je (nenulový) polynóm $f \in R[x]$ ireducibilný v $R[x]$, tak je ireducibilný aj v $F[x]$, kde F je podielové pole R (t.j. $F = \mathbb{Q}$ ak $R = \mathbb{Z}$, a $F = k(t)$ ak $R = k[t]$).*

Dôkaz. Predpokladajme najprv, že f je primitívny polynóm. Nech $p, q \in F[x]$ sú nekonštantné polynómy také, že $f(x) = p(x)q(x)$. Ľahko sa presvedčíme, že bez ujmy na všeobecnosti môžeme predpokladať, že najvačší spoločný deliteľ menovateľov všetkých koeficientov polynómu p je 1, podobne pre polynóm q, a to isté platí pre najväčšie spoločné delitele čitateľov koeficientov. Potom existujú $u, v \in R$ také, že polynómy $up(x)$ a $vq(x)$ patria $R[x]$ a sú primitívne. Takže máme

$$(up(x))(vq(x)) = (uv)f(x),$$

a teda podľa Gaussovej lemy je uv jednotkou v okruhu R. Potom ale aj u, v sú jednotky, a preto $p(x)$ a $q(x)$ sú polynómy v $R[x]$.

Na záver, nech polynóm f nie je primitívny, zapíšme potom $f(x) = dg(x)$, kde $d \in R$ a $g \in R[x]$ je primitívny. Nech $f(x) = p(x)q(x)$ pre nejaké $p, q \in F[x]$. Pre primitívny polynóm g potom máme, že

$$g(x) = \frac{p(x)}{d} q(x).$$

Z predchádzajúcej argumentácie dostávame, že $\frac{p(x)}{d}, q(x) \in R[x]$, a teda aj polynómy p, q z rozkladu polynómu f patria $R[x]$. □

DÔSLEDOK. *Ak sú (nenulové) polynómy $f, g \in R[x]$ nesúdeliteľné v $R[x]$, potom sú nesúdeliteľné aj v $F[x]$, kde F je podielové pole R.*

Dôkaz. Nech sú polynómy f a g súdeliteľné nad F, čiže $f(x) = d(x)p(x)$ a $g(x) = d(x)q(x)$, kde $d, p, q \in F[x]$ a d je nekonštantný, a polynómy d a p resp. d a q sú ako polynómy v rozklade f v predchádzajúcom dôkaze. Ak p aj q sú konštantné polynómy, tak f je konštantným násobkom polynómu g a polynómy f, g sú súdeliteľné nad R. Ak p resp. q je nekonštantný, tak nech sú d a p resp. d a q ako polynómy v rozklade f v predchádzajúcom dôkaze. Potom podobne usúdime, že polynómy d, p resp. d, q patria $R[x]$, a teda f a g sú súdeliteľné nad R. □

TVRDENIE 3.4. *Ak sú (nenulové) polynómy $f, g \in k[x, y]$ nesúdeliteľné, potom má sústava $f(x, y) = g(x, y) = 0$ len konečne veľa riešení.*

Dôkaz. Polynómy $f, g \in k[x, y] = (k[x])[y]$ môžme chápať aj ako prvky $(k(x))[y]$. Keďže f, g sú nesúdeliteľné v $(k[x])[y]$, podľa dôsledku Gaussovej lemy sú nesúdeliteľné aj v $(k(x))[y]$. Všimnime si, že $(k(x))[y]$ je okruh polynómov s jednou premennou nad poľom, a preto z Euklidovho algoritmu vieme nájsť $u', v' \in (k(x))[y]$ také, že

$$1 = u'f + v'g. \tag{4}$$

Nech $d \in k[x]$ je spoločný menovateľ koeficientov u' a v'. Vynásobením rovnosti (4) polynómom d dostávame novú rovnosť

$$d = uf + vg, \tag{5}$$

kde $d \in k[x]$ a $u, v, f, g \in k[x, y]$. Zoberme teraz bod $(a_1, a_2) \in \mathbb{A}^2$, ktorý je spoločným riešením sústavy z tvrdenia, teda platí $f(a_1, a_2) = g(a_1, a_2) = 0$. Z rovnosti (5) potom dostávame, že $d(a_1) = 0$. Avšak d je polynóm z $k[x]$ a preto má len konečne veľa riešení. Máme teda len konečne veľa možností pre hodnotu prvej súradnice bodu (a_1, a_2). Úplne analogicky (postupom cez $(k(y))[x]$) sa tiež ukáže, že ak (a_1, a_2) je spoločné riešenie sústavy $f = g = 0$, potom a_2 môže nadobúdať len niektorú z konečne veľa hodnôt. Môže teda existovať len konečne veľa spoločných riešení tejto sústavy. □

Teraz si už môžme popísať Zariskiho topológiu na $\mathbb{A}^2(k)$. Algebraická varieta v $\mathbb{A}^2(k)$ je množina definovaná niekoľkými polynómami: $X = V(f_1, \ldots, f_r),\ f_i \in k[x, y]$.

(a) Ak všetky f_i sú konštantny 0, potom $X = V(0) = \mathbb{A}^2$.
(b) Nech $f_1, \ldots, f_r$ nie sú nulové polynómy. Predpokladajme, že tieto polynómy sú nesúdeliteľné. Potom podľa Tvrdenia 3.4 existuje len konečne veľa bodov (a_1, a_2) takých, že $f_1(a_1, a_2) = \cdots = f_r(a_1, a_2) = 0$, čiže varieta X pozostáva z konečného (možno aj nulového) počtu bodov.
(c) Nech $d \in k[x]$ je najväčší spoločný deliteľ polynómov $f_1, \ldots, f_r$, stupeň $d > 0$. Potom máme polynómy $f_1', \ldots, f_r'$ také, že $f_1 = df_1', \ldots, f_r = df_r'$, pričom $\mathrm{nsd}(f_1', \ldots, f_r') = 1$. Skúmajme ideál generovaný polynómami $f_1, \ldots, f_r$:
$$(f_1, \ldots, f_r) = (df_1', \ldots, df_r') = (d)(f_1', \ldots, f_r')$$
(preverte si poslednú rovnosť!). Preto $X = X_1 \cup X_2$, kde $X_1 = V(d)$ a $X_2 = V(f_1', \ldots, f_r')$. Varieta X_1 je rovinná krivka a varieta X_2 pozostáva z konečného počtu bodov (viď prípad (b)).

Poznámka 3.5. Tak ako vidno v prípade $\mathbb{A}^1$ a $\mathbb{A}^2$, aj vo všeobecnosti platí, že neprázdne otvorené množiny v Zariskiho topológii sú veľmi veľké. Dokonca platí, že každé dve neprázdne otvorené množiny majú neprázdny prienik. Z toho vyplýva, že Zariskiho topológia nie je Hausdorffovská.

4. Problémy, príklady

4.1. Algebraizácia a porovnávanie algebraických variet. Geometriu sme si začali algebraizovať. Algebraická varieta $X \subset \mathbb{A}^n(k)$ bola pôvodne množina všetkých riešení sústavy polynomických rovníc:

$$a = (a_1, a_2, \ldots, a_n) \in X = V(f_1, \ldots, f_r) \text{ práve vtedy keď } f_1(a) = 0, f_2(a) = 0, \ldots, f_r(a) = 0,$$

kde f_i sú polynómy z $k[x_1, \ldots, x_n]$. V súvislosti s algebraickou varietou X sa nebudeme obmedzovať iba na množinu polynómov, ktorými sme ju definovali, ale budeme uvažovať celý ideál I v okruhu polynómov, generovaný polynómami, ktorými je táto algebraická varieta definovaná: $I = (f_1, f_2, \ldots, f_k) \subset k[x_1, \ldots, x_n]$. Toto nám umožní lepšie manipulovať s algebraickými varietami bez toho, aby sme explicitne museli napísať množinu bodov, ktoré patria X. Majme napríklad dve algebraické variety

$$X_1 = V(I_1), \quad I_1 = (f_1, \ldots, f_r)$$
$$X_2 = V(I_2), \quad I_2 = (g_1, \ldots, g_s),$$

Vieme už, že

ak $I_1 \subset I_2$, potom $X_1 \supset X_2$,
ak $I_1 = I_2$, potom $X_1 = X_2$.

Z Lemmy 2.1 (presnejšie z jej dôkazu) tiež vieme, že ak chceme overiť, či $I_1 \subset I_2$, treba pre každý generátor f_i ideálu I_1 zistiť, či $f_i \in I_2$.

Príklad 4.1. Príklade 1.6 sme si uviedli krivku v trojrozmernom afinnom priestore $\mathbb{A}^3(k)$. Je to algebraická varieta

$$V(I), \quad \text{kde} \quad I = (y - x^2, z - x^3) \subset k[x, y, z].$$

Uvažujme ďalšiu algebraickú varietu v $\mathbb{A}^3(k)$, popísanú polynómami $y - x^2, z - xy$, teda varietu

$$V(J), \quad \text{kde} \quad J = (y - x^2, z - xy) \subset k[x, y, z].$$

Vieme overiť, či $V(I) = V(J)$?

Ak $I = J$, tak ide o tú istú algebraickú varietu. (V opačnom prípade by sme nevedeli usúdiť nič, lebo dva rôzne ideály môžu stále definovať tú istú algebraickú varietu!) Skúsme teda overiť, či $y - x^2, z - x^3 \in J$ a $y - x^2, z - xy \in I$. Zrejme stačí zistiť, či $z - x^3 \in J$ a $z - xy \in I$. Platí

$$z - x^3 = (z - xy) + x(y - x^2) \subset J, \quad \text{čiže } I \subset J,$$
$$z - xy = (z - x^3) - x(y - x^2) \subset I, \quad \text{čiže } J \subset I.$$

Zatiaľ ide o metódu pokus-omyl. Pre systematickejší prístup potrebujeme ešte doriešiť dve otázky:

výpočtová: Ako pre dané dva ideály I_1, I_2 overiť, či $I_1 \subset I_2$? Z Hilbertovej vety o báze vieme, že existuje konečná množina polynómov, ktorá generuje I_1. Stačí teda pre konečne veľa polynómov f_i overiť, či $f_i \in I_2$ Ostáva už len

Problém 1. nájsť metódu (algoritmus), ktorá pre daný ideál $I = (f_1, \ldots, f_r)$ v okruhu $k[x_1, \ldots, x_n]$ a daný polynóm $g \in k[x_1, \ldots, x_n]$ zistí, či $g \in I$.

teoretická: Korešpondencia medzi ideálmi a algebraickými varietami ešte nie je celkom uspokojivá. Každému ideálu v $k[x_1, \ldots, x_n]$ vieme priradiť algebraickú varietu (viď Hilbertova veta o báze) a tiež každej algebraickej variete vieme prisúdiť nejaký ideál, napríklad ideál generovaný polynómami, ktorými sme algebraickú varietu definovali. Toto priradenie však nie je jedno-jednoznačné: dva rôzne ideály môžu definovať tú istú algebraickú varietu. Túto nejednoznačnosť sa tiež pokúsime odstrániť:

Problém 2. nájsť jedno-jednoznačnú korešpondenciu medzi ideálmi v $k[x_1, \ldots, x_n]$ a afinnými algebraickými varietami v $\mathbb{A}^n(k)$.

Teoretickým problémom sa budeme zaoberať neskôr. Výpočtový si najprv ilustrujeme na niekoľkých príkladoch, potom sa ním začneme zaoberať podrobnejšie.

PRÍKLAD 4.2. V okruhu $k[t]$ (k je pole) majme ideál $I = (t^3+1)$. Patrí polynóm $g = t^5+t^3+1$ tomuto ideálu?

Vieme, že $g \in I$ práve vtedy, keď existuje $h \in k[t]$ také, že $g = (t^3+1)h$, teda keď g je násobkom generátora ideálu I. Treba len zistiť, či sa dá polynóm g vydeliť týmto generátorom bezo zvyšku. Máme, že

$$t^5 + t^3 + 1 \ : \ t^3 + 1 \ = \ t^2 + 1 \quad \text{so zvyškom } -t^2,$$

čiže $t^5 + t^3 + 1 = (t^2+1)(t^3+1) - t^2$. Polynóm g nie je násobkom generátora, a preto $g \notin I$.

PRÍKLAD 4.3. V okruhu $k[t]$ majme ideál $I = (t^3-1, t^5-1)$. Patrí polynóm $g = t^3+t^2-2$ tomuto ideálu?

Vieme, že $k[t]$ je okruh hlavných ideálov, preto aj ideál I sa dá generovať jediným prvkom – bude to najväčší spoločný deliteľ pôvodných dvoch generátorov. Ten vypočítame pomocou euklidovho algoritmu:

(1) $t^5 - 1 \ : \ t^3 - 1 \ = \ t^2$, zvyšok $t^2 - 1$,
(2) $t^3 - 1 \ : \ t^2 - 1 \ = \ t$, zvyšok $t - 1$,
(3) $t^2 - 1 \ : \ t - 1 \ = \ t + 1$, zvyšok 0.

Najväčším spoločným deliteľom $t^3 - 1$ a $t^5 - 1$ je preto $t - 1$ a ideál I je generovaný jediným polynómom: $I = (t-1)$. Aby sme zistili, či $g \in I$, stačí už len zistiť, či g je násobkom $t-1$. Platí

$$t^3 + t^2 - 2 \ : \ t - 1 \ = \ t^2 + 2t + 2 \quad \text{zvyšok } 0,$$

takže $t^3 + t^2 - 2 \in I$.

PONAUČENIE. Hoci v teórii nezáleží na tom, ktorú množinu generátorov ideálu máme, pri počítaní s konkrétnymi ideálmi naopak zisťujeme, že niektorá množina generátorov je „lepšia" než iná.

PONAUČENIE. V okruhu $k[t]$ je riešením Problému 1 Euklidov algoritmus.

PRÍKLAD 4.4. V okruhu $k[x,y]$ uvažujme ideál $I = (x+y, x-y)$. Ako by sme mohli čo najjednoduchšie charakterizovať polynómy tohto ideálu? Inými slovami: ako pre daný polynóm čo najrýchlejšie rozhodnúť, či patrí do I? Ak patrí, ako ho čo najrýchlejšie napísať ako kombináciu generátorov? Na tieto otázky sa omnoho jednoduchšie odpovedá, keď si uvedomíme, že $I = (x, y)$: zrejme $x+y, x-y \in (x,y)$, a tiež $x, y \in (x+y, x-y)$ lebo

$$x = \frac{1}{2}(x+y) + \frac{1}{2}(x-y) \quad \text{a} \quad y = \frac{1}{2}(x+y) - \frac{1}{2}(x-y).$$

Takže I je ideál všetkých polynómov v $k[x,y]$ bez absolútneho člena. Ak by sme I reprezentovali touto druhou množinou generátorov, tak vieme veľmi rýchlo a jednoducho pre každý polynóm $g \in I$ nájsť h_1, h_2 také, že $g = xh_1 + yh_2$.

PRÍKLAD 4.5. Tie isté otázky ako v predchádzajúcom príklade, pre ideál

$$I = (x + xy, y + xy, x^2, y^2) \subset k[x,y]. \tag{6}$$

Ukážeme, že znovu platí $I = (x,y)$. Na jednu stranu je zrejmé, že $x+xy, y+xy, x^2, y^2 \in (x,y)$, a teda $(x + xy, y + xy, x^2, y^2) \subset (x,y)$. Pre opačnú inklúziu potrebujeme x a y vyjadriť ako kombinácie generátorov (6):

$$\begin{aligned} x \ &= (x + xy) - x(y + xy) + yx^2, \\ y \ &= (y + xy) - y(x + xy) + xy^2. \end{aligned}$$

4.2. Hľadanie algebraických variet. Najzákladnejším a najprirodzenejším problémom v súvislosti so sústavou rovníc je hľadanie riešenia. V našom prípade máme sústavu polynomických rovníc

$$\begin{aligned} f_1(x_1, x_2, \ldots, x_n) &= 0, \\ &\ldots \\ f_k(x_1, x_2, \ldots, x_n) &= 0. \end{aligned}$$

Čo to však znamená, vyriešiť takýto systém rovníc? V prípade, že riešení je len konečne veľa, pochopiteľnou požiadavkou je chcieť ich všetky vymenovať a tým považovať sústavu rovníc za vyriešenú. Môžme si teda naformulovať ďalšie problémy, ktorými sa budeme zaoberať:

Problém 3. Pre danú sústavu rovníc rozhodnúť, či má riešenie, t.j. či algebraická varieta, ktorá je týmito polynómami definovaná, nie je prázdnou množinou.

Problém 4. Zistiť, či $X = V(f_1, \ldots, f_r)$ je nularozmerná algebraická varieta v $\mathbb{A}^n$, a ak áno, vymenovať všetky jej body.

Príklad 4.6. Nech $X = V(y - x^2, z - xy, x + y + z - 1) \subset \mathbb{A}^3(\mathbb{C})$. Je X konečná množina? Ak áno, ako nájdeme všetky jej body?

Všimnime si najprv, že prvé dve rovnice definujú našu známu vinutú kubiku (viď Príklad 4.1) a tiež že polynóm $z - xy$ môžme nahradiť polynómom $z - x^3$:

$$(y - x^2, z - xy, x + y + z - 1) = (y - x^2, z - x^3, x + y + z - 1)$$

(trochu sme modifikovali množinu generátorov). To znamená, že hľadáme prienik vinutej kubiky s rovinou, ktorá je definovaná rovnicou $x + y + z - 1 = 0$. O chvíľu tiež ukážeme, že

$$(y - x^2, z - x^3, x + y + z - 1) = (y - x^2, z - x^3, x^3 + x^2 + x - 1). \tag{7}$$

Odtiaľ už potom ľahko vidíme, že X je konečná: bod $(a_1, a_2, a_3) \in X$ musí spĺňať tretiu rovnicu, teda musí platiť

$$a_1^3 + a_1^2 + a_1 - 1 = 0.$$

Máme tak len tri možnosti pre hondnotu a_1. Pre každé také a_1 potom z prvých dvoch rovníc jednoznačne dopočítame a_2 a a_3.

Pre dôkaz rovnosti (7) potrebujeme ukázať, že

$$\begin{aligned} x + y + z - 1 &\in (y - x^2, z - x^3, x^3 + x^2 + x - 1) \quad \text{a} \\ x^3 + x^2 + x - 1 &\in (y - x^2, z - x^3, x + y + z - 1). \end{aligned}$$

To je ale pravda, lebo

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

Vidíme, že kľúčom k riešeniu bola znovu vhodná modifikácia množiny generátorov ideálu, ktorým sme definovali varietu X.

Ak má však algebraická varieta definovaná danou sústavou polynomických rovníc vyššiu dimenziu, úloha vyriešiť túto sústavu sa stáva veľmi problematickou.

Príklad 4.7. Z lineárnej geometrie: nájsť riešenie sústavy lineárnych rovníc

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n - a_{10} &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n - a_{20} &= 0 \\ &\ldots \\ a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rn}x_n - a_{r0} &= 0 \end{aligned}$$

znamená previesť vyjadrenie lineárnej variety $X \subset \mathbb{A}^n(k)$ zo všeobecných rovníc na parametrické, čiže nájsť bod $b = (b_1, b_2, \ldots, b_n)$ a vektory $\mathbf{u}_1 = (u_{11}, u_{12}, \ldots, u_{1n}), \ldots, \mathbf{u}_d = (u_{d1}, u_{d2}, \ldots, u_{dn})$, že každý bod lineárnej variety sa dá napísať ako

$$b + \mathbf{u}_1 t_1 + \mathbf{u}_2 t_2 + \cdots + \mathbf{u}_d t_d$$

pre nejaké $t_1, t_2, \ldots t_d \in k$.

Úloha 14. Vyriešte sústavu pre neznáme x_1, x_2, x_3, x_4:

$$\begin{aligned} x_1 + x_2 - 2x_3 + 3x_4 - 19 &= 0 \\ 2x_1 - x_2 + 3x_3 - x_4 - 8 &= 0. \end{aligned}$$

Parametrické vyjadrenie lineárnej variety považujeme za riešenie sústavy lineárnych rovníc, lebo je to nástroj na systematické generovanie bodov na lineárnej variete: ak $b + \mathbf{u}_1 t_1 + \mathbf{u}_2 t_2 + \cdots + \mathbf{u}_d t_d$ je parametrické vyjadrenie nejakej lineárnej variety nad k (t.j. b je bod patriaci variete a $\mathbf{u}_i$ sú vektory tvoriace bázu vektorovej zložky lineárnej variety), tak pre každú d-ticu $(c_1, \ldots, c_d) \in k^d$ je

$$b + c_1 \mathbf{u}_1 + \cdots + c_d \mathbf{u}_d \tag{8}$$

bod na tejto lineárnej variete. A naopak: každý bod lineárnej variety sa dá napísať v tvare (8) pre nejaké $(c_1, \ldots, c_d) \in k^d$. Hľadanie parametrického vyjadrenia je teda hľadanie „vhodného" zobrazenia z $\mathbb{A}^d(k)$ na varietu.

Príklad 4.8. V prípade vinutej kubiky (príklad 1.6) ide o algebraickú varietu X danú polynómami $y - x^2, y - x^3$. Za riešenie sústavy rovníc $y - x^2 = 0, y - x^3 = 0$ môžme považovať zobrazenie

$$\mathbb{A}^1 \to X \subset \mathbb{A}^3, \quad t \mapsto (t, t^2, t^3),$$

lebo toto zobrazenie je nástrojom na generovanie bodov na krivke.

Takže požiadavka hľadania riešenia algebraickej variety pozostávajúcej z nekonečného počtu bodov sa neformálne dá formulovať ako

Problém 5 (**parametrizácia**). Nájsť „dobré" zobrazenie $\mathbb{A}^d \to X \subset \mathbb{A}^n$, ktoré je popísané polynomickými prípadne racionálnymi funkciami, t.j.

$$(t_1, \ldots, t_d) \mapsto (\varphi_1(t_1, \ldots, t_d), \ldots, \varphi_n(t_1, \ldots, t_d)),$$

kde $\varphi_1, \ldots, \varphi_n \in k(t_1, \ldots, t_d)$.

Problém parametrizácie je však *veľmi* ťažký a preto sa ním tento semester ešte nebudeme zaoberať. Ľahšia je opačná úloha:

Problém 6 (**implicitizácia**). Pre dané zobrazenie

$$\varphi\colon\ \mathbb{A}^d \to \mathbb{A}^n,\ (t_1, t_2, \ldots, t_d) \mapsto (\varphi_1(t_1, t_2, \ldots, t_d), \ldots, \varphi_n(t_1, t_2, \ldots, t_d)), \quad \varphi_i \in k(t_1, \ldots, t_d)$$

nájsť rovnice popisujúce obraz.

V prípade lineárnych variet ide o hľadanie všeobecných rovníc lineárnej variety zadanej parametricky, lebo parametrické vyjadrenie

$$\begin{aligned} x_1 &= a_{10} + a_{11} t_1 + a_{12} t_2 + \cdots + a_{1d} t_d \\ x_2 &= a_{20} + a_{21} t_1 + a_{22} t_2 + \cdots + a_{2d} t_d \\ &\ldots \\ x_n &= a_{n0} + a_{n1} t_1 + a_{n2} t_2 + \cdots + a_{nd} t_d \end{aligned}$$

vlastne popisuje zobrazenie $\mathbb{A}^d \to \mathbb{A}^n$: $x_1, \ldots, x_n$ sú lineárne funkcie premenných $t_1, \ldots, t_d$.

Úloha 15. Pre zobrazenie

$$\varphi\colon\ \mathbb{A}^3(\mathbb{R}) \to \mathbb{A}^4(\mathbb{R}),\ (t_1, t_2, t_3) \mapsto (3t_1 + t_3, t_2 + 4t_3, t_1 + t_2 + t_3, t_1 - t_2 - t_3)$$

popíšte obraz $\varphi(\mathbb{A}^3(\mathbb{R}))$ ako algebraickú varietu, t.j. nájdite rovnicu (rovnice) popisujúcu obraz.

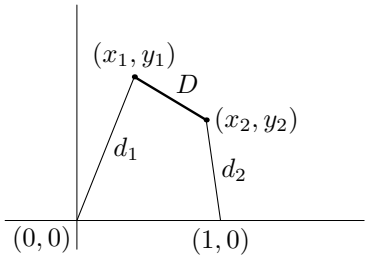
4.3. Stewartova platforma (príklad z robotiky). Ide o plošinu (mnohouholník alebo iný rovinný útvar) v reálnom trojrozmernom priestore, ktorá je niekoľkými „nohami" pripevnená k podložke. Poloha platformy sa určuje iba pomocou dĺžok nôh, teda pre každú nohu môžme pevne určiť len jej dĺžku, ale už nie natočenie v priestore. Nôh musí byť toľko, koľko je stupňov voľnosti Stewartovej platformy, teda 6. Celý tento systém sa dá popísať polynomickými rovnicami, takže dostávame nejakú algebraickú varietu.

V súvislosti s takouto platformou sa v robotike formulujú dva problémy:

(1) problém (priamej) kinematiky: dané sú dĺžky nôh, treba nájsť polohu platformy, prípadne zistiť, nakoľko jednoznačne je táto poloha určená,
(2) problém inverznej kinematiky: daná je poloha platformy, treba nájsť dĺžky nôh.

Problém inverznej kinematiky je triviálny, stačí zrátať vzdialenosti bodov. Pre ilustráciu prvého problému zíďme pre jednoduchosť o dimenziu nižšie: platforma bude jednorozmerný útvar (úsečka) v reálnej rovine $\mathbb{A}^2(\mathbb{R})$, pevnú podložku umiestnime na x-os. Skúsme zistiť, či platforma je uspokojivo ovládaná dvoma nohami.

Obe nohy nech sú na platforme uchytené v koncových bodoch úsečky, ktorých súradnice sú (x_1, y_1) a (x_2, y_2) – tieto body sa pohybujú v rovine. Na podložke nech sú nohy uchytené v bodoch $(0, 0)$, $(1, 0)$ – tieto body sú pevné. Polohu platformy budeme riadiť dĺžkami nôh $d_1, d_2 \in \mathbb{R}$.



Stav platformy je jej poloha v rovine, čiže je určený polohou jej koncových bodov. Môžme ho teda reprezentovať ako bod v 4-rozmernom priestore $\mathbb{A}^4(\mathbb{R})$, v algebraickej reči pracujeme s okruhom polynómov $\mathbb{R}[x_1, y_1, x_2, y_2]$. Nie každý bod v $\mathbb{A}^4$ však reprezentuje nejaký stav platformy: platforma je pevná, teda dĺžka úsečky ostáva nemenná, označme si ju D ($D \in \mathbb{R}$). Bod (a_1, b_1, a_2, b_2) reprezentuje stav platformy práve vtedy, keď $\sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2} = D$. Takže množina všetkých stavov tvorí v $\mathbb{A}^4(\mathbb{R})$ algebraickú varietu

$$X = V((x_1 - x_2)^2 + (y_1 - y_2)^2 - D^2). \tag{9}$$

Otázka teraz znie: ak zvolíme dĺžky nôh d_1, d_2, bude poloha takejto platformy jednoznačne určená?

Voľba dĺžok je reprezentovaná rovnicami

$$\begin{aligned} x_1^2 + y_1^2 - d_1^2 &= 0 \\ (x_2 - 1)^2 + y_2^2 - d_2^2 &= 0. \end{aligned}$$

Ide teda o to, koľko majú tieto rovnice spolu s rovnicou popisujúcou množinu stavov (9) riešení.

Intuícia 1 (pochádzajúca z lineárnej geometrie, v algebraickej geometrii často zavádzajúca!): X je trojrozmerná algebraická varieta v $\mathbb{A}^4$, lebo je popísaná jednou rovnicou. Jedna dodatočná rovnica zmenší dimenziu o 1, ďalšia zase o 1, takže algebraická varieta popísaná uvedenými troma rovnicami je jednorozmerná – malo by ísť o krivku v $\mathbb{A}^4$. Takáto platforma preto nie je stabilná: úsečka uchytená len v koncových bodoch spadne.

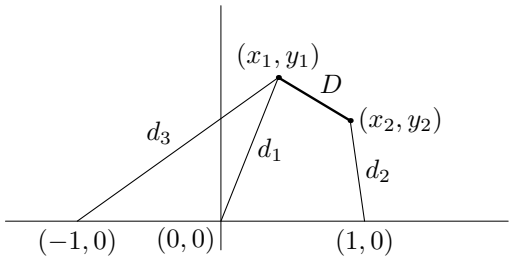
Intuícia 2: Rátajme stupne voľnosti: jeden koncový bod jednoznačne určíme dvoma skalármi (kartézske súradnice alebo polárne súradnice). Pre určenie druhého koncového bodu potrebujeme ešte jednu súradnicu. Teda táto platforma má tri stupne voľnosti. My sme však dodali len dve nohy, čiže platforme zadávame len dve súradnice. Takáto platforma preto spadne.

Dôkladný exaktný postup: Postupovalo by sa prostriedkami komutatívnej algebry. Napríklad, našli by sme „dobrú" množinu generátorov ideálu

$$((x_1 - x_2)^2 + (y_1 - y_2)^2 - D^2, x_1^2 + y_1^2 - d_1^2, (x_2 - 1)^2 + y_2^2 - d_2^2) \subset \mathbb{R}[x_1, y_1, x_2, y_2]$$

(niečo analogické ako sme robili v príklade 4.6), z ktorej by sme už ľahko vyčítali, že algebraická varieta definovaná týmto ideálom má vyššiu dimenziu než 0.

Každopádne zistíme, že tejto jednoduchej platforme treba ešte dodať jednu nohu, napríklad nech je na platforme uchytená v prvom bode a na podložke v bode $(-1, 0)$.



Dostávame tak ďalšiu rovnicu

$$(x_2 + 1)^2 + y_2^2 - d_3^2 = 0,$$

ktorá spolu s troma predchádzajúcimi už určí nularozmernú algebraickú varietu.

V prílohe je uvedený zoznam príkazov pre systém počítačovej algebry Singular, ktorý rieši problém priamej kinematiky pre túto jednoduchú platformu.

* Úloha 16. Popíšte rovnicami Stewardovu platformu (môžte sa obmedziť na špeciálny prípad z prednášky):

(i) treba nájsť systém rovníc popisujúci množinu všetkých stavov platformy ako algebraickú varietu v nejakom afinnom priestore,

(ii) treba napísať dodatočné rovnice popisujúce polohu platformy, keď určíme dĺžky nôh.

KAPITOLA 3

Výpočtové metódy algebraickej geometrie

1. Gröbnerove bázy

1.1. 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

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

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

$$x^\alpha > x^\beta > x^\gamma > \dots \tag{10}$$

je konečná. Naozaj, majme klesajúcu postupnosť monómov (10). 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

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

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 $\mathcal{M}$. □

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

Graduované reverzné lexikografické usporiadanie. Pre monómy x^α, x^β platí, že $x^\alpha >_{grevlex} x^\beta$, ak $\deg x^\alpha > \deg x^\beta$, alebo ak $\deg x^\alpha = \deg x^\beta$ a pre posledný index i taký, že $\alpha_i \neq \beta_i$, platí $\alpha_i < \beta_i$.

Príklad 1.4. V graduovaných usporiadaniach máme

$$x_1x_2^2x_3^2 <_{glex} x_2^7x_3 \qquad x_1x_2^2x_3^2 <_{grevlex} x_2^7x_3,$$
$$x_1x_2^2x_3^2 >_{glex} x_2^4x_3 \qquad x_1x_2^2x_3^2 <_{grevlex} x_2^4x_3,$$

Úloha 17. Ukážte, že obe graduované usporiadania sú naozaj usporiadaniami monómov.

Úloha 18. Ukážte, že v okruhu $k[x]$ existuje jediné usporiadanie monómov.

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

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

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

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 $19x_3^{17}$.

1.2. 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 $f_1, \ldots, f_k$ zistiť, či g patrí ideálu, ktorý je generovaný polynómami $f_1, \ldots, f_k$ (jeden z problémov, ktoré sme si v predchádzajúcich týždňoch sformulovali). Budeme sa snažiť polynóm g zredukovať pomocou $f_1, \ldots, f_k$ na čo najjednoduchší tvar, a následne rozhodnúť tento problém. Algoritmus by mohol vyzerať takto:

Vstup: polynóm g a polynómy $f_1, \ldots, f_k$ z $k[x_1, \ldots, x_n]$ so zvoleným usporiadaním monómov.
Výstup: rozhodnutie, či $g \in (f_1, \ldots, f_k)$.
Algorimus:

- inicializácia: $g_0 := g$.
- iterácia (cez i): Ak $g_i = 0$, potom prehlás, že $g \in (f_1, \ldots, f_k)$, a ukonči delenie.
  Ak pre nejaké j platí, že $\mathrm{LM}(f_j) \mid \mathrm{LM}(g_i)$, tak
  $$g_{i+1} := g_i - (\mathrm{LT}(g_i)/\mathrm{LT}(f_j))f_j.$$
  Inak (vedúci monóm žiadneho polynómu spomedzi $f_1, \ldots, f_k$ nedelí vedúci koeficient g_i) ukonči delenie.

Príklad 1.7. Predveďme 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 1.8. *Výpočet pomocou algoritmu delenia skončí po konečnom počte krokov. Navyše, ak $g_i = 0$ pre nejaké i, potom naozaj $g \in (f_1, \ldots, f_k)$.*

Dôkaz. Skúmajme vedúce monómy polynómov g_i. Pri konštrukcii polynómu g_{i+1} sa vedúci člen g_i vykráti s vedúcim členom polynómu $(\mathrm{LT}(g_i)/\mathrm{LT}(f_j))f_j$ 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 $\mathrm{LM}(g_{i+1}) < \mathrm{LM}(g_i)$. Takže máme klesajúcu postupnosť monómov

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

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_i. 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 1.9. 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 1.10. V úlohe 10 v Kapitole 2 sme overili, že

$$((x-1)(x-3), (x-1)(y-4), (y-2)(x-3)) = (x^2 - 2x - 2y + 5, x - y + 1).$$

Naším algoritmom delenia sa nám však podarí ukázať iba, že

$$(x-1)(x-3) \in (x^2 - 2x - 2y + 5, x - y + 1) :$$

nech $g = (x-1)(x-3) = x^2 - 4x + 3$, $f_1 = x^2 - 2x - 2y + 5$, $f_2 = x - y + 1$.

- $g_0 = g$,
- $g_1 = g_0 - f_1 = -2x + 2y - 2$,
- $g_2 = g_1 + 2f_2 = 0$.

Spätným dosadzovaním dostaneme, že $g = f_1 - 2f_2$.

Úloha 19. V $\mathbb{A}^3$ majme krivku $C = V(y - x^2, z - x^3)$ (naša známa vinutá kubika) a plochu $S = V(z^2 - x^4 y)$. Ukážte dvoma spôsobmi, že krivka C leží celá v ploche S:

(a) Ukážte, že $(z^2 - x^4 y) \subset (y - x^2, z - x^3)$, potom z vlastností korešpondencie ideálov a variet vyplýva požadované tvrdenie. Pre dokazovanie $z^2 - x^4 y \in (y - x^2, z - x^3)$ použite algoritmus delenia s takým lexikografickým usporiadaním, kde $z > y > x$. Na záver aj vyjadrite $z^2 - x^4 y$ ako kombináciu $y - x^2$ a $z - x^3$.

(b) Použite parametrizáciu krivky C.

1.3. Monomiálne ideály.

Definícia 1.11. Ideál $J \subset k[x_1, \dots, x_n]$ sa nazýva *monomiálny*, ak je generovaný nejakou množinou monómov.

Tvrdenie 1.12. *Nech J je monomiálny ideál a $f = \sum c_\alpha x^\alpha \in J$. Potom každý člen $c_\alpha x^\alpha \in J$.*

Dôkaz. (Ide viac o uvedomovacie cvičenie než o nejaké počítanie.)
Keďže $f \in J$, kde $J = (x^\beta \mid \beta \in \mathcal{B})$, existujú polynómy $h_1, \dots, h_{k'}$ také, že

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

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

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

kde m_i sú len konštantné násobky monómov. Je zrejmé, že 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 $m_{i_1} x^{\beta_{i_1}}, \ldots, m_{i_l} x^{\beta_{i_l}}$ 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 $f_1, \ldots, f_k \in k[x_1, \ldots, x_n]$, že $J = (f_1, \ldots, f_k)$. Nech $\{x^\alpha\}_{\alpha \in \mathcal{A}}$ je množina všetkých monómov, ktoré sa vyskytujú v $f_1, \ldots, f_k$ s nenulovým koeficientom, teda je to konečná množina. Potom $J = (x^\alpha \mid \alpha \in \mathcal{A})$. Jedna inklúzia je zrejmá z vlastnosti ideálov, druhá vyplýva z Tvrdenia 1.12, pretože J je monomiálny. □

Tvrdenie 1.13. *Nech $J = \{x^\beta\}_{\beta \in \mathcal{B}}$ je monomiálny ideál. Potom každý monóm v J je deliteľný niektorým z generátorov x^β.*

Dôkaz. (Veľmi podobný dôkazu Tvrdenia 1.12.) Nech $x^\alpha \in J$, a preto

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

kde m_i sú polynómy pozostávajúce len z jedného člena. Monóm x^α sa nutne musí nachádzať medzi členmi na pravej strane rovnosti, čiže existuje i také, že x^α je konštantným násobkom $m_i x^{\beta_i}$, a teda x^α je deliteľný monómom x^{β_i}. □

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 1.12 každý člen polynómu g partí do J, špeciálne, $\mathrm{LT}(g) \in J$. Z Tvrdenia 1.13 potom vidíme, že $\mathrm{LT}(g)$ je deliteľný niektorým generátorom, a teda g môžme redukovať, až dostaneme $g_i = 0$ pre nejaké i.

Tiež pre monomiálny ideál vieme ľahko nájsť príslušnú algebraickú varietu:

Príklad 1.14. 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 1.15. V $k[x_1, \ldots, x_n]$ majme zvolené usporiadanie monómov. Nech $I \subset k[x_1, \ldots, x_n]$ je ideál. *Ideál vedúcich členov* ideálu I je

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

Definícia 1.16. V $k[x_1, \ldots, x_n]$ majme zvolené usporiadanie monómov a nech $I \subset k[x_1, \ldots, x_n]$ je ideál. *Gröbnerova báza* ideálu I je množina polynómov

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

taká, že $\mathrm{LT}(I) = (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_k))$.

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

VETA 1.17. *V $k[x_1, \ldots, x_n]$ majme zvolené usporiadanie monómov. Nech $I \subset k[x_1, \ldots, x_n]$ je ideál a nech $\{f_1, \ldots, f_k\}$ je jeho Gröbnerova báza. Potom algoritmom delenia, keď redukujeme polynómami $f_1, \ldots, f_k$, vieme vždy správne rozhodnúť, či daný polynóm patrí I. Presnejšie, ak $g \in I$, tak delením polynómami $f_1, \ldots, f_k$ zredukujeme g na 0.*

DÔSLEDOK. *Gröbnerova báza ideálu je jeho množinou generátorov.*

Dôkaz. Vieme, že ak $\{f_1, \ldots, f_k\}$ je Gröbnerova báza ideálu I, potom $(f_1, \ldots, f_k) \subset I$. Nech teraz $g \in I$. Podľa Vety 1.17 algoritmus delenia tento polynóm zredukuje do 0 a preto podľa Tvrdenia 1.8 $g \in (f_1, \ldots, f_k)$. □

Dôkaz Vety 1.17. 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 $f_1, \ldots, f_k$. Podľa Tvrdenia 1.13 to znamená, že

$$\mathrm{LT}(g_i) \notin (\mathrm{LT}(f_1,), \ldots, \mathrm{LT}(f_k)).$$

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. □

PRÍKLAD 1.18. Nech $f_1 = x^2 - 2x - 2y + 5, f_2 = x - y + 1 \in k[x, y]$, uvažujme lexikografické usporiadanie. Zoberme ideál dvojbodovej algebraickej variety $I = (f_1, f_2) \subset k[x, y]$. Už v Príklade 1.10 sme sa presvedčili, že pomocou týchto dvoch generátorov nie je možné deliacim algoritmom zredukovať každý polynóm ideálu I na nulu. Z Vety 1.17 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

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

Polynóm $g = (y - 2)(y - 4) = y^2 - 6y + 8$ patrí ideálu I, lebo $g = f_1 + (-x - y + 3)f_2$. Jeho vedúci člen je $\mathrm{LT}(g) = y^2$ a zrejme $y^2 \notin (x)$, teda máme, že $\mathrm{LT}(I) \neq (\mathrm{LT}(f_1), \mathrm{LT}(f_2))$, a preto podľa definície $\{f_1, f_2\}$ nie je Gröbnerovou bázou.

PRÍKLAD 1.19. Nech $I \subset k[x_1, \ldots, x_n]$ je hlavný ideál, teda $I = (f), f \in k[x_1, \ldots, x_n]$. Každý polynóm $g \in I$ je násobkom polynómu f, t.j. $g = hf$ pre nejaké $h \in k[x_1, \ldots, x_n]$. Keďže akékoľvek usporiadanie monómov je kompatibilné s násobením, platí $\mathrm{LT}(g) = \mathrm{LT}(h)\mathrm{LT}(f)$, a teda $\mathrm{LT}(g) \in (\mathrm{LT}(f))$. V tomto prípade teda máme, že $\mathrm{LT}(I) = (\mathrm{LT}(f))$, preto generátor hlavného ideálu je aj jeho Gröbnerovou bázou vzhľadom na ktorékoľvek usporiadanie monómov.

PRÍKLAD 1.20. 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 $(\mathrm{LT}(y - x^2), \mathrm{LT}(z - x^3)) = (y, z)$. Nech g je nenulový polynóm taký, že $\mathrm{LT}(g) \notin (y, z)$. Z lexikografického usporiadania dostávame, že g neobsahuje premennú y ani z, teda g je polynóm iba v premennej x: $g = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. 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 $(a, a^2, a^3) \notin V(g)$.

Vidíme, že overovať z definície, či daná množina polynómov tvorí Gröbnerovu bázu ideálu, ktorý generuje, si v každom konkrétnom príklade 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 1.21. 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 $\mathrm{LT}(g) \notin (\mathrm{LT}(f_1), \mathrm{LT}(f_2)) = (xy^2, x^2y)$. 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

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

a teda nejde o Gröbnerovu bázu.

Definícia 1.22. Nech $x^\alpha, x^\beta \in k[x_1, \ldots, x_n]$ sú monómy. *Najmenším spoločným násobkom* monómov x^α, x^β nazývame monóm $x^\gamma \in k[x_1, \ldots, x_n]$, kde $\gamma_i = \max\{\alpha_i, \beta_i\}$.

Definícia 1.23. *S-polynómom* polynómov $f, g \in k[x_1, \ldots, x_n]$ nazývame polynóm

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

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

Príklad 1.24. 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 1.25 (**Buchbergerovo kritérium**). *V okruhu $k[x_1, \ldots, x_n]$ so zvoleným usporiadaním monómov majme polynómy $f_1, \ldots, f_k$. Tieto polynómy tvoria Gröbnerovu bázu ideálu $(f_1, \ldots, f_k)$ práve vtedy, keď algoritmus delenia (polynómami $f_1, \ldots, f_k$) redukuje každý S-polynóm $S(f_i, f_j)$ $(i, j = 1, \ldots, k)$ do nuly.*

Dôkaz. Z Vety 1.17 vyplýva, že ak $\{f_1, \ldots, f_k\}$ je Gröbnerova báza, tak každý S-polynóm je algoritmom delenia zredukovaný do nuly, lebo $S(f_i, f_j) \in (f_1, \ldots, f_k)$ pre všetky i, j.

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

$$\mathrm{LT}(g) \notin (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_k)). \tag{11}$$

Nech

$$g = g_1 f_1 + \cdots + g_k f_k \tag{12}$$

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

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

Po vhodnom preusporiadaní $f_1, \ldots, f_k$ môžme predpokladať, že

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

Z (11) vyplýva, že $\mathrm{LM}(g) \neq x^\delta$, teda x^δ na pravej strane rovnosti (12) sa musí vykrátiť, preto existujú aspoň dva sčítance, ktorých vedúci monóm je x^δ, teda $\mathrm{LM}(g_1 f_1) = \mathrm{LM}(g_2 f_2) = x^\delta$.

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

$$S(f_1, f_2) = \frac{x^\gamma}{\mathrm{LT}(f_1)} f_1 - \frac{x^\gamma}{\mathrm{LT}(f_2)} f_2, \tag{13}$$

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

$$S(f_1, f_2) = \sum_{i=1}^{k} h_i f_i, \quad \text{pričom} \quad \mathrm{LM}(h_i f_i) \leq \mathrm{LM}(S(f_1, f_2)),\ i = 1, \ldots, k. \tag{14}$$

(Rozpíšte si to, aby ste si overili tvdenie o vedúcich monómoch!) Z (13) a (14) dostávame rovnosť

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

Túto rovnosť prenásobíme monómom x^δ / x^γ a pripočítame k (12). Takto dostaneme nové vyjadrenie

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

kde $\mathrm{LM}(\tilde{g}_2 f_2) < x^\delta$, 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 (12). Preto $\{f_1, \ldots, f_k\}$ je Gröbnerova báza. □

PRÍKLAD 1.26. Vyriešme Príklad 1.20 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 $k[x_1, \ldots, x_n]$ so zvoleným usporiadaním monómov majme polynómy $f_1, \ldots, f_k$. Gröbnerovu bázu ideálu $(f_1, \ldots, f_k)$ získame nasledovným spôsobom:*

VSTUP: *polynómy $f_1, \ldots, f_k$ z $k[x_1, \ldots, x_n]$ so zvoleným usporiadaním monómov.*
VÝSTUP: *Gröbnerova báza ideálu $(f_1, \ldots, f_k)$.*
ALGORIMUS:

- *Pre všetky $i, j = 1, \ldots, k$, $i \neq j$ nech r_{ij} je zvyšok po aplikovaní algorimu delenia na polynóm $S(f_i, f_j)$ (t.j. $\mathrm{LT}(r_{ij})$ nie je deliteľný žiadnym vedúcim členom spomedzi polynómov $f_1, \ldots, f_k$).*
- *Ak všetky $r_{ij} = 0$, potom $\{f_1, \ldots, f_k\}$ je Gröbnerova báza, koniec algoritmu.*
- *Inak $\{f_1, \ldots, f_k, f_{k+1}, \ldots, f_{k+s}\}$ je nová množina generátorov ideálu, kde $f_{k+1}, \ldots, f_{k+s}$ sú nenulové r_{ij}. Opakuj výpočet od začiatku na túto novú množinu generátorov.*

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

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

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

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

$$J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \ldots.$$

Okruh $k[x_1, \ldots, x_n]$ 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 $(f_1, \ldots, f_k)$. □

PRÍKLAD 1.27. 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

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

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 $\{f_1, f_2, f_3, f_4, f_5\}$.

ÚLOHA 20. Použite Buchbergerov algoritmus na nájdenie Gröbnerovej bázy ideálu $(z - x^5, y - x^3) \subset k[x, y, z]$. Použite

(a) lexikografické usporiadanie, $(x > y > z)$,
(b) graduované reverzné lexikografické usporiadanie.

Uveďte aj všetky výpočty a redukcie S-polynómov.

ÚLOHA 21. Nech $I \subset k[x_1, \ldots, x_n]$ je ideál generovnaný lineárnymi polynómami (čiže popisujúci lineárnu varietu). Čo viete povedať o Gröbnerovej báze ideálu I?

ZÁVER. Problém 1 z Kapitoly 2 sme vyriešili: pre dané polynómy g a $f_1, \ldots, f_k$ z $k[x_1, \ldots, x_n]$ vieme rozhodnúť, či $g \in (f_1, \ldots, f_k)$:

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

2. Teória eliminácie

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 2.1. 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. *čiastočné riešenia*).
(3) Budeme sa snažiť rozširovať čiastočné 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 2.2. Nech $X = V(xy - 1) \subset \mathbb{A}^2$. Nech π je priemietanie na os y:

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

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 môžme 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.

ÚLOHA 22. Nech $S \subset \mathbb{A}^n$, potom $V(I(S)) = \overline{S}$. Dokážte.

VETA 2.3. *Nech $X \subset \mathbb{A}^n(k)$ je algebraická varieta a nech $J = I(X)$. Nech ďalej π je premietanie*

$$\pi\colon\ \mathbb{A}^n \to \mathbb{A}^{n-r}, \quad (x_1, \ldots, x_n) \mapsto (x_{r+1}, \ldots, x_n).$$

Potom

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

Dôkaz. Ak $f \in k[x_{r+1}, \ldots, x_n]$, tak symbol $\pi^* f$ znamená, že polynóm f uvažujeme ako polynóm v okruhu $k[x_1, \ldots, x_n]$.

Ukážeme najprv inklúziu $\pi(X) \subset V(J \cap k[x_{r+1}, \ldots, x_n])$, z nej už potom vyplýva inklúzia $\overline{\pi(X)} \subset V(J \cap k[x_{r+1}, \ldots, x_n])$ (stačí zobrať uzáver týchto množín, inklúzia sa uzáverom zachováva). Bod $a' = (a_{r+1}, \ldots, a_n) \in \pi(X)$ patrí variete $V(J \cap k[x_{r+1}, \ldots, x_n])$, ak je riešením všetkých polynómov v $J \cap k[x_{r+1}, \ldots, x_n]$. Nech teda $a' \in \pi(X)$, čiže existujú $a_1, \ldots, a_r \in k$ také, že $a = (a_1, \ldots, a_n) \in X$. Ďalej nech $f \in J \cap k[x_{r+1}, \ldots, x_n]$. Potom

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

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

Pre dôkaz opačnej iklúzie $V(J \cap k[x_{r+1}, \ldots, x_n]) \subset \overline{\pi(X)}$ zoberme $f \in I(\pi(X))$, ukážeme, že $f \in J \cap k[x_{r+1}, \ldots, x_n]$. Keďže $f \in k[x_{r+1}, \ldots, x_n]$, 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 $I(\pi(X)) \subset J \cap k[x_{r+1}, \ldots, x_n]$, a tak

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

□

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 by potom vyzerala nasledovne:

VETA 2.4. *Nech pole k je algebraicky uzavreté (napr. $k = \mathbb{C}$). Nech $J \subset k[x_1, \ldots, x_n]$ je ideál, $X = V(J) \subset \mathbb{A}^n(k)$ a $\pi\colon \mathbb{A}^n \to \mathbb{A}^{n-r}$ je premietanie na posledných $n-r$ súradníc. Potom*

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

Aby sme mohli túto verziu vety dokázať, potrebujeme ešte hlbšie porozumieť vzťahu medzi ideálmi a algebraickými varietami (Problém 2 v Kapitole 2), preto to odložíme na neskôr.

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

TVRDENIE 2.5. *Nech $J \subset k[x_1, \ldots, x_n]$ je ideál, $X = V(J) \subset \mathbb{A}^n$ a nech π je premietanie*

$$\pi\colon \mathbb{A}^n \to \mathbb{A}^{n-r}, \quad (x_1, \ldots, x_n) \mapsto (x_{r+1}, \ldots, x_n).$$

Potom

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

Dôkaz. Z Tvrdenia 2.11 v Kapitole 2 vieme, že $J \subseteq I(V(J))$. Preto platí aj, že

$$J \cap k[x_{r+1}, \ldots, x_n] \subseteq I(V(J)) \cap k[x_{r+1}, \ldots, x_n],$$

a teda podľa spomenutého tvrdenia

$$V(I(V(J)) \cap k[x_{r+1}, \ldots, x_n]) \subseteq V(J \cap k[x_{r+1}, \ldots, x_n]).$$

Keďže tiež platí $V(I(V(J))) = V(J)$, tak ľavá strana posledného výroku je podľa práve dokázanej Vety 2.3 rovná množine $\overline{\pi(V(I(V(J))))} = \overline{\pi(V(J))} = \overline{\pi(X)}$. □

PRÍKLAD 2.6. 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 súradicu: $(x, y) \mapsto (y)$). Naproti tomu, $J \cap \mathbb{R}[y] = (y-1)$ (bude vysvetlené v nasledujúcej vete), teda $V(J \cap \mathbb{R}[y]) = \{(1)\} \neq \emptyset$.

Veta 2.3 ani Veta 2.4 sa nedajú 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 2.7 (**o eliminácii**). *V okruhu $k[x_1, \ldots, x_n]$ uvažujme lexikografické usporiadanie ($x_1 > x_2 > \cdots > x_n$). Nech $J \subset k[x_1, \ldots, x_n]$ je ideál a G jeho Gröbnerova báza. Potom*

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

Dôkaz. Zrejme platí, že $(G \cap k[x_{r+1}, \ldots, x_n]) \subset J \cap k[x_{r+1}, \ldots, x_n]$. Potrebujeme teda ešte dokázať, že ak $f \in J \cap k[x_{r+1}, \ldots, x_n]$, potom f je generovaný polynómami z $G \cap k[x_{r+1}, \ldots, x_n]$. 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 $G \cap k[x_{r+1}, \ldots, x_n]$ sú presne tie polynómy z G, ktorých vedúci monóm obsahuje len $x_{r+1}, \ldots, x_n$. Keďže aj $f \in k[x_{r+1}, \ldots, x_n]$, pri redukcii budeme používať len polynómy z $G \cap k[x_{r+1}, \ldots, x_n]$, preto

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

□

DEFINÍCIA 2.8. Nech $J \in k[x_1, \ldots, x_n]$ je ideál. Ideál

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

nazývame *r-tý eliminačný ideál* ideálu J.

ÚLOHA 23. Majme ideál

$$I = (x^2 + y^2 + z^2 + 2, 3x^2 + 4y^2 + 4z^2 + 5) \subset k[x, y, z].$$

Nech

$$I_1 = I \cap k[y, z].$$

je prvý eliminačný ideál – vypočítate ho pomocou Vety 2.7. (Môžte si pomôcť nejakým systémom počítačovej algebry, napríklad na prednáške sme si zbežne predviedli Singular.)

(i) Overte, že ak $k = \mathbb{C}$, tak $V(I_1) = \pi_1(V(I))$.
(ii) Overte, že ak $k = \mathbb{R}$, tak $V(I) = \emptyset$, hoci množina $V(I_1)$ je nekonečná, teda Veta 2.3' neplatí.

PRÍKLAD (dokončenie príkladu 2.1). 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, nájdenú pomocou Singuláru, viď aj nasledujúcu úlohu):

$$\begin{aligned} g_1 &= z^6 - 4z^4 + 4z^3 - z^2, \\ g_2 &= 2yz^2 + z^4 - z^2, \\ g_3 &= y^2 - y - z^2 + z, \\ g_4 &= x + y + z^2 - 1. \end{aligned}$$

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 $g_1 = 0$ nájdeme pomocou faktorizácie polynómu g_1:

$$g_1 = z^2(z-1)^2(z^2 + 2z - 1),$$

teda máme $z \in \{0, 1, -1 \pm \sqrt{2}\}$. Súradnicu y dopočítame k týmto čiastočným riešeniam pomocou g_2 a g_3, a napokon súradnicu x pomocou g_4. Dostávame spolu päť riešení

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

ÚLOHA 24. (Doplnok ku Gröbnerovým bázam). V okruhu $k[x_1, \ldots, x_n]$ majme zvolené usporiadanie monómov. Nech $G = \{f_1, \ldots, f_k\}$ je Gröbnerova báza ideálu $I \subset k[x_1, \ldots, x_n]$. Ak $\mathrm{LT}(f_i) \mid \mathrm{LT}(f_j)$ $(i \neq j)$, tak potom aj $\{f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_k\}$ je Gröbnerova báza ideálu I. Dokážte.

ÚLOHA 25. Vyriešte pomocou Gröbnerových báz:

$$\begin{aligned} x^2 + y^2 + z^2 &= 4, \\ x^2 + 2y^2 &= 5, \\ xz &= 1. \end{aligned}$$

Pomôžte si nejakým systémom počítačovej algebry.

PRÍKLAD 2.9. Hľadajme 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 2.3) 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 troma súradnicami) použijeme zostávajúci polynóm $xz - 1$ z Gröbnerovej bázy. Okrem riešenia $(y, z) = (0, 0)$ vieme všetky rozšíriť. 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. Nasledujúci vetu si uvedieme pre ilustráciu ako jedno z tvrdení o rozširovaní riešení (bez dôkazu):

VETA 2.10 (**o rozširovaní riešení**). *Nech $J = (f_1, \ldots, f_k) \subset \mathbb{C}[x_1, \ldots, x_n]$ a nech $J_1 = J \cap \mathbb{C}[x_2, \ldots, x_n]$ je jeho prvý eliminačný ideál. Zapíšme f_i v tvare*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{n_i} + \text{ členy, v ktorých } x_1 \text{ má stupeň menší ako } n_i,$$

kde $g_i \in \mathbb{C}[x_2, \ldots, x_n]$ je nenulový polynóm. Nech $(a_2, \ldots, a_n)$ je čiastočné riešenie (t.j. patrí $V(J_1)$). Ak $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_k)$, potom existuje $a_1 \in \mathbb{C}$ také, že $(a_1, \ldots, a_n) \in V(J)$.

ZÁVER. Gröbnerove bázy nám pomohli odpovedať aj na obe otázky položené v Probléme 4 v Kapitole 2. Algebraická varieta je nularozmerná, ak jej priemet na poslednú súradnicovú os je nularozmerný, a každé čiastočné riešenie sa dá na úplné rozšíriť konečne veľa spôsobmi. Týmto postupom aj nájdeme všetky body na danej variete. Problém 4 môžme teda považovať za uzavretý.

Intuícia z lineárnej geometrie nás zvádza k nasledovnému počítaniu dimenzie variety v $\mathbb{A}^n$: jednou rovnicou je zadaná nadplocha, ďalšiou rovnicou sa dimenzia algebraickej variety zmenší na $n - 2$, a tak ďalej, každá ďalšia rovnica zmenší dimenziu o 1, takže ak popíšeme varietu k rovnicami, ktoré sú dostatočne nezávislé, tak jej dimenzia bude $n - k$. Variety, pre ktoré toto platí nad algebraicky uzavretým poľom, nazývame *úplným prienikom.* Už sme si spomenuli, že ak pole, nad ktorým pracujeme, nie je algebraicky uzavreté, tak jednou rovnicou vieme popísať varietu, ktorej dimenzia je menej než $n - 1$ (Úlohy 7 a 8 z Kapitoly 2). Aj nad algebraicky uzavretým poľom však existujú algebraické variety, pri ktorých nás táto intuícia klame:

PRÍKLAD 2.11. Uvažujme v $\mathbb{A}^4(\mathbb{C})$ množinu bodov

$$X = \{(s^3, s^2t, st^2, t^3) \mid s, t \in \mathbb{C}\}.$$

Ide o dvojrozmernú plochu v 4-rozmernom priestore. Navyše je to algebraická varieta, lebo máme, že

$$X = V(I), \text{ kde } I = (x_1x_3 - x_2^2, x_2x_4 - x_3^2, x_1x_4 - x_2x_3).$$

Inklúzia $X \subset V(I)$ sa overí jednoducho dosadením. Pre opačnú inklúziu, nech $(a_1, a_2, a_3, a_4) \in V(I)$, nájdeme také $s, t \in \mathbb{C}$, že $x_1 = s^3$, $x_2 = s^2t$, $x_3 = st^2$, $x_4 = t^3$.

Ak $a_4 = 0$, potom aj $a_3 = a_2 = 0$ a máme, že $s = \sqrt[3]{a_1}$ a $t = 0$ Nech teraz $a_4 \neq 0$ a nech $t \in \mathbb{C}$ je také, že $t^3 = a_4$. Ďalej nech $s = \frac{x_3}{t^2}$. Z polynómov generujúcich I potom už dopočítame, že aj $x_2 = s^2t$ a $x_1 = s^3$.

X je dvojrozmerná varieta v štvorrozmernom priestore, ktorú sme ale popísali troma rovnicami. Tiež sa dá elemntárnymi úvahami a výpočtami presvedčiť, že neexistujú dva polynómy

$f_1, f_2 \in \mathbb{C}[x_1, x_2, x_3, x_4]$ také, že $I = (f_1, f_2)$. Hovoríme, že varieta X nie je ideálovo úplným prienikom.

Na druhej strane, zoberme si ideál

$$J = (g_1, g_2), \text{ kde } g_1 = x_1x_3 - x_2^2, g_2 = x_3(x_2x_4 - x_3^2) - x_4(x_1x_4 - x_2x_3)).$$

Vidíme, že $J \subset I$, čiže $X = V(I) \subset V(J)$. Tiež ľahko overíme, že

$$\begin{aligned}(x_2x_4 - x_3^2)^2 &= -x_4^2g_1 - x_3g_2\\ (x_1x_4 - x_2x_3)^2 &= -x_3^2g_1 - x_1g_2.\end{aligned}$$

Teda ak $p \in V(J)$, tak potom $p \in V(I)$.

Ideály I a J sú síce rôzne, ale popisujú tú istú algebraickú varietu. Hovoríme, že varieta X je množinovo úplným prienikom.

Príklad 2.12. Znovu v štvorrozmernom priestore $\mathbb{A}^4(\mathbb{C})$ uvažujme zjednotenie dvoch rovín $X = X_1 \cup X_2$, kde $X_1 = V(x_1, x_2)$ a $X_2 = (x_3, x_4)$. Ide o algebraickú varietu popísanú napríklad ideálom $(x_1x_3, x_1x_4, x_2x_3, x_2x_4)$ Podobne ako v predchádzajúcom príklade táto varieta nie je ideálovo úplným prienikom. Navyše v tomto prípade sa dá ukázať, že dokonca nie je úplným prienikom ani množinovo, teda neexistujú dva polynómy g_1, g_2 také, že $X = V(g_1, g_2)$ (Hartshorne, 1962).

Ak chceme zistiť, či daná algebraická varieta je nularozmerná, nestačí len pozrieť na počet polynómov, ktoré ju definujú!

3. Rezultanty

3.1. Definícia a základná vlastnosť.

VETA 3.1. *Nech $f, g \in k[x]$ sú polynómy stupňov m a n:*

$$\begin{aligned} f &= f_m x^m + \cdots + f_1 x + f_0, \quad f_m \neq 0, \\ g &= g_n x^n + \cdots + g_1 x + g_0, \quad g_n \neq 0. \end{aligned}$$

Nasledovné tvrdenia sú ekvivalentné:

(i) *f, g majú spoločný koreň nad nejakým rozšírením poľa k.*
(ii) *f, g majú spoločný nekonštantný deliteľ nad k (t.j. existuje $h \in k[x], \deg h \geq 1$ také, že $h \mid f, h \mid g$).*
(iii) *Neexistujú polynómy $p, q \in k[x]$ také, že $pf + qg = 1$.*
(iv) *$(f, g) \subsetneq k[x]$.*

Dôkaz. Budeme zaradom dokazovať jednotlivé ekvivalencie.

(i)⇒(ii): Nech α je spoločný koreň polynómov f a g ($k[\alpha]$ je algebraické rozšírenie k obsahujúce koreň). Definujme si zobrazenie

$$\varphi\colon\ k[x] \to k[\alpha], \quad x \mapsto \alpha,$$

čiže φ je dosadzovanie α za x. Takto definované zobrazenie φ je homomorfizmus okruhov, jeho jadrom je preto ideál okruhu $k[x]$ (dokážte si to!). Navyše $k[x]$ je okruh hlavných ideálov, takže existuje $h \in k[x]$, že $\ker \varphi = (h)$.

Pre polynómy f, g máme

$$\varphi(f) = f(\alpha) = 0, \quad \text{a tiež} \quad \varphi(g) = g(\alpha) = 0,$$

takže $f, g \in \ker \varphi$. Odtiaľ máme, že $h \mid f$ a $h \mid g$. Navyše, h je určite nekonštantný polynóm: ak by $h \in k$ (h je zrejme nenulové, lebo jadro φ je netriviálne), potom máme, že $1 = hh^{-1} \in (h)$ a teda $(h) = k[x]$ (Lema 2.3 v Kapitole 1, dokážte si ju!), čo však nie je pravda, lebo napríklad $\varphi(1) = 1$ a teda $1 \notin \ker \varphi$. Našli sme tak nekonštantný spoločný deliteľ polynómov f a g.

(ii)⇒(i): Nech $h \in k[x]$ je spoločný deliteľ f, g, $\deg h \geq 1$, môžme predpokladať, že h je ireducibilný. Potom $k[x]/(h)$ je pole: nech $[a]$ označuje triedu $\varphi(a)$, kde φ je projekcia $k[x] \to k[x]/(h)$. Pre ľubovoľné nenulové $[a] \in k[x]/(h)$ potrebujeme nájsť k nemu inverzný prvok. Ak $a \in (h)$, potom $[a] = 0$. V opačnom prípade sú polynómy a a h nesúdeliteľné, a teda existujú $u, v \in k[x]$ také, že $ua + vh = 1$. Máme tak

$$[u][a] = \varphi(u)\varphi(a) = \varphi(ua) = \varphi(1 - vh) = \varphi(1) - \varphi(v)\varphi(h) = 1,$$

takže $[u]$ je inverzný ku $[a]$, čiže $k[x]/(h)$ je pole.

Jadrom zobrazenia $\varphi\colon\ k[x] \to k[x]/(h)$ je ideál (h). Keďže h je deliteľom f aj g, tieto dva polynómy patria do jadra. Na druhej strane máme, že

$$\varphi(f) = f_m \varphi(x)^m + \cdots + f_1 \varphi(x) + f_0,$$

takže $\varphi(x) \in k[x]/(h)$ je koreňom polynómu f. Analogicky ukážeme, že $\varphi(x)$ je koreňom g. Našli sme spoločný koreň polynómov f a g v rozšírení $k[x]/(h)$.

(ii)⇒(iii): Ak $h \mid f$ a $h \mid g$ potom $h \mid pf + qg$ pre ľubovoľné $p, q \in k[x]$ a teda nemôže platiť, že $pf + qg = 1$.

(iii)⇒(ii): Nevieme 1 zapísať ako kombináciu f a g, to znamená, že $(f, g) = (h)$, kde stupeň h je aspoň 1. Potom h je spoločným deliteľom polynómov f, g.

(iii)⇔(iv): Tvrdenie (iii) znamená, že $1 \notin (f, g)$, čo je zas ekvivalentné tomu, že $(f, g) \neq k[x]$ (Lema 2.3 v Kapitole 1). □

POZNÁMKA 3.2. Možno ste si všimli, že pri dôkaze implikácie (ii)⇒(i) sme vlastne použili ekvivalenciu (ii)⇔(iii), ktorú sme v tom momente ešte nemali dokázanú. Nejde však o dôkaz v kruhu, lebo ekvivalenciu (ii)⇔(iii), sme dokázali úplne nezávisle od implikácie (ii)⇒(i).

LEMA 3.3. *Nech $f, g \in k[x]$ sú polynómy stupňov m a n:*

$$\begin{aligned} f &= f_m x^m + \cdots + f_1 x + f_0, \quad f_m \neq 0, \\ g &= g_n x^n + \cdots + g_1 x + g_0, \quad g_n \neq 0. \end{aligned}$$

Nasledovné tvrdenia sú ekvivalentné:

(i) *Existujú polynómy $p, q \in k[x]$ také, že $pf + qg = 1$.*
(ii) *Existujú polynómy $p, q \in k[x]$ také, že $\deg p \leq n-1$, $\deg q \leq m-1$ a $pf + qg = 1$.*
(iii) *Pre každý polynóm $h \in k[x]$, pre ktorý $\deg h \leq m+n-1$, existujú polynómy $p, q \in k[x]$ také, že $\deg p \leq n-1$, $\deg q \leq m-1$ a $pf + qg = h$.*

Dôkaz. Implikácie (iii)⇒(ii) a (ii)⇒(i) sú zrejmé. Stačí preto, ak dokážeme implikáciu (i)⇒(iii).

Nech platí (i), teda existujú polynómy $p, q \in k[x]$ také, že $pf + qg = 1$. Po vynásobení tejto rovnosti polynómom h dostávame

$$(hp)f + (hq)g = h, \quad \text{čiže} \quad p'f + q'g = h. \tag{15}$$

Polynóm h sa teda dá nakombinovať z polynómov f a g, treba ešte ukázať, že môžme nájsť p', q' s dostatočne malým stupňom. Nech $M = \max\{\deg p'f, \deg q'g\}$. Ukážeme, že ak $M > m+n-1$ (t.j. $\deg p' > n-1$ alebo $\deg q' > m-1$), potom vieme p', q' nahradiť polynómami s nižším stupňom. Z vlastnosti dobrého usporiadania prirodzených čísel potom vieme medzi týmito M nájsť také, že $M \leq m+n-1$.

Nech teda $M > m+n-1$. Keďže stupeň h je menší, vedúce členy sčítancov $p'f$ a $q'g$ v (15) sa vykrátia:

$$\mathrm{LT}(p')\mathrm{LT}(f) + \mathrm{LT}(q')\mathrm{LT}(g) = 0. \tag{16}$$

Vytvoríme teraz nové polynómy p'' a q'' tak, že vedúci člen v polynóme p' zredukujeme vedúcim členom polynómu g (všimnite si, že z predpokladu o p' platí $\deg(p') \geq \deg(g)$, a teda dá sa redukovať ako to navrhujeme), podobne pre polynóm q'':

$$\begin{aligned} p'' &= p' - \frac{\mathrm{LT}(p')}{\mathrm{LT}(g)} g, \quad \text{a teda } \deg p'' < \deg p', \\ q'' &= q' - \frac{\mathrm{LT}(q')}{\mathrm{LT}(f)} f, \quad \text{a teda } \deg q'' < \deg q'. \end{aligned}$$

Potom dostávame

$$p''f + q''g = (p' - \frac{\mathrm{LT}(p')}{\mathrm{LT}(g)}g)f + (q' - \frac{\mathrm{LT}(q')}{\mathrm{LT}(f)}f)g = h - fg\frac{\mathrm{LT}(p')\mathrm{LT}(f) + \mathrm{LT}(q')\mathrm{LT}(g)}{\mathrm{LT}(g)\mathrm{LT}(f)} = h,$$

kde predposledná rovnosť vyplýva z (15) a posledná z (16). □

PRÍKLAD 3.4. Smerujeme k tomu, nájsť kritérium, kedy majú dva polynómy v $k[x]$ spoločný koreň. Najjednoduchší príklad dostaneme, keď si zoberieme dva lineárne polynómy:

$$f = f_1 x + f_0, \quad g = g_1 x + g_0, \quad \text{kde } f_1, g_1 \neq 0.$$

Lineárny polynóm má iba jeden koreň, a polynómy f a g budú mať tento koreň spoločný práve vtedy, keď f je konštantným násobkom polynómu g, čiže vtedy, keď

$$\det \begin{pmatrix} f_1 & f_0 \\ g_1 & g_0 \end{pmatrix} = 0.$$

DEFINÍCIA 3.5. Nech $f, g \in k[x]$ sú polynómy stupňov m a n:

$$\begin{aligned} f &= f_m x^m + \cdots + f_1 x + f_0, \quad f_m \neq 0, \\ g &= g_n x^n + \cdots + g_1 x + g_0, \quad g_n \neq 0. \end{aligned}$$

Štvorcová matica

$$\mathrm{Syl}(f,g) = \begin{pmatrix} f_m & f_{m-1} & \dots & f_0 & 0 & \dots & 0 \\ 0 & f_m & \dots & f_1 & f_0 & \dots & 0 \\ & & \ddots & & & \ddots & \\ 0 & \dots & 0 & f_m & \dots & f_1 & f_0 \\ g_n & g_{n-1} & \dots & g_0 & 0 & \dots & 0 \\ 0 & g_n & \dots & g_1 & g_0 & \dots & 0 \\ & & \ddots & & & \ddots & \\ 0 & \dots & 0 & g_n & \dots & g_1 & g_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\b\\c\end{matrix}}\right\} n-\text{krát} \\ \\ \\ \\ \left.\vphantom{\begin{matrix}a\\b\\c\end{matrix}}\right\} m-\text{krát} \\ \\ \\ \end{matrix}$$

sa nazýva *Sylvestrova matica* polynómov f a g.
Rezultant polynómov f a g je determinant $\mathrm{Res}(f,g) = \det \mathrm{Syl}(f,g)$.

Poznámka 3.6. Niekedy budeme označovať rezultant polynómov f a g aj $\mathrm{Res}_x(f,g)$, a to v prípade, keď budeme chcieť zdôrazniť, že f, g sú polynómy v premennej x.

Veta 3.7. *Polynómy $f, g \in k[x]$ majú spoločný koreň nad nejakým rozšírením k práve vtedy, keď $\mathrm{Res}(f,g) = 0$.*

Poznámka 3.8. Všimnite si, že Príklad 3.4 je vlastne dôkazom Vety 3.7 pre prípad $m = n = 1$.

Dôkaz Vety 3.7. Najdôležitejším krokom dôkazu je vysvetlenie tvaru Sylvestrovej matice.

Označme si ako P_d množinu všetkých polynómov v $k[x]$, ktorých stupeň nie je vačší ako d, P_d je $(d+1)$-rozmerným vektorovým priestorom nad k. Uvažujme zobrazenie

$$\delta\colon\ (p,q) \mapsto pf + qg \quad (p,q \in k[x]).$$

Ak budeme za p brať len polynómy stupňa maximálne $n-1$, a za q stupňa maximálne $m-1$, máme zobrazenie priestorov

$$\delta\colon\ P_{n-1} \oplus P_{m-1} \to P_{m+n-1}, \quad (p,q) \mapsto pf + qg.$$

Oba priestory, $P_{n-1} \oplus P_{m-1}$ aj P_{m+n-1} sú vektorovými priestormi dimenzie $m+n$ a zobrazenie δ je lineárnym zobrazením. Preto po zvolení báz v oboch priestoroch sa dá takéto zobrazenie popísať štvorcovou maticou stupňa $m+n$.

V priestore P_{m+n-1} si zvoľme štandardnú monomiálnu bázu

$$x^{m+n-1}, x^{m+n-2}, \dots, x, 1,$$

v priestore $P_{n-1} \oplus P_{m-1}$ zas kombináciu štandardných báz podpriestorov, čiže

$$(x^{n-1},0), (x^{n-2},0), \dots, (x,0), (1,0), (0,x^{m-1}), \dots, (0,x), (0,1).$$

Matica zobrazenia δ potom v i-riadku obsahuje súradnice obrazu i-teho bázového vektora priestoru $P_{n-1} \oplus P_{m-1}$ vzhľadom na zvolenú bázu priestoru P_{m+n-1} (to platí pre riadkovú konvenciu, keď vektory zapisujeme ako riadky súradníc, pri stĺpcovej konvencii bude matica transponovaná). Pre bázy priestorov, ktoré sme si zvolili, budú koeficienty obrazov prvých n bázových vektorov $(x^i, 0)$ tie isté ako koeficienty polynómu f, len „posunuté" doľava podľa stupňa i. Podobne pre zvyšných m bázových vektorov dostaneme príslušné posunutie koeficientov polynómu g. Vidíme, že matica nášho zobrazenia je presne Sylvestrova matica polynómov f a g.

Zvyšok dôkazu je už krátky. Podľa Vety 3.1 sú polynómy f a g nesúdeliteľné práve keď existujú $p, q \in k[x]$ také, že $pf + qg = 1$. Podľa Lemy 3.3 je to ekvivalentné s tvrdením, že pre každé $h \in P_{m+n-1}$ existuje dvojica polynómov $(p,q) \in P_{n-1} \oplus P_{m-1}$ tak, že $pf + qg = h$, čo vlastne znamená, že zobrazenie δ je surjektívne. Keďže dimenzia oboch vektorových priestorov (vzoru aj obrazu) je rovnaká, je zobrazenie δ surjektívne práve práve vtedy keď je injektívne, čo zas platí práve vtedy, keď jeho matica je regulárna, t.j. keď $\mathrm{Res}(f,g) \neq 0$. □

PRÍKLAD 3.9. Pomocou rezultantov nájdeme spoločné body dvoch rovinných kriviek: hyperboly popísanej polynómom $f = xy - 1$ a kružnice popísanej $g = x^2 + y^2 - 4$. Hľadáme teda riešenia sústavy dvoch rovníc o dvoch neznámych.

Kľúčovým je nasledovné preformulovanie problému: ak f a g chápeme ako polynómy jednej premennej x nad $k[y]$, kedy majú tieto dva polynómy spoločný koreň? Podľa Vety 3.7 by to mohlo byť vtedy, keď $\mathrm{Res}_x(f, g) = 0$. Trochu máme ale problém, že spomínaná veta vypovedá niečo o polynómoch jednej premennej, kdežto v našom prípade sú f a g polynómami dvoch premenných. Napriek tomu skúsme pokračovať vo výpočtoch, a dodatočne si tento postup odôvodníme aj v teórii.

Polynóm f je lineárny v x, polynóm g zas kvadratický. Máme

$$\mathrm{Res}_x(f, g) = \begin{vmatrix} y & -1 & 0 \\ 0 & y & -1 \\ 1 & 0 & y^2 - 4 \end{vmatrix} = y^4 - 4y^2 + 1.$$

Sústava má štyri riešenia: y-súradnica je riešením rovnice $y^4 - 4y^2 + 1 = 0$, a x-súradnica je potom spoločný koreň dvoch polynómov z $k[x]$.

3.2. Diskriminant polynómu. Nech $f \in k[x]$ je polynóm stupňa n, teda nad algebraickým uzáverom k má n koreňov, keď ich počítame aj s násobnosťou. Nech $\alpha \in \overline{k}$ je aspoň dvojnásobný koreň, tedá platí, že

$$f = (x - \alpha)^2 f_1, \quad \text{kde } f_1 \in \overline{k}[x].$$

Pre deriváciu f potom platí

$$f' = 2(x - \alpha)f_1 + (x - \alpha)^2 f_1' = (x - \alpha)(2f_1 + (x - \alpha)f_1'),$$

teda α je koreňom polynómu f'.

Naopak teraz predpokladajme, že $\alpha \in \overline{k}$ je spoločným koreňom polynómu f aj jeho derivácie f'. Z $f = (x - \alpha)f_2$ dostávame

$$f' = (x - \alpha)f_2' + f_2, \quad \text{čiže} \quad f_2 = f' - (x - \alpha)f_2'.$$

Keďže sme predpokladali, že $(x - \alpha) \mid f'$, platí, že $(x - \alpha) \mid f_2$, a teda $f_2 = (x - \alpha)f_3$ pre nejaký polynóm f_3. Takže sme dostali

$$f = (x - \alpha)f_2 = (x - \alpha)^2 f_3,$$

a α je dvojnásobný koreň polynómu f.

Spolu s Vetou 3.7 sme ukázali, že f má nad $\overline{k}$ koreň násobnosti aspoň 2 práve vtedy, keď $\mathrm{Res}(f, f') = 0$.

PRÍKLAD 3.10. Nech $f = ax^2 + bx + c$, $a \neq 0$. Zistime, kedy má tento polynóm dvojnásobný koreň.

Derivácia $f' = 2ax + b$, takže rezultant $\mathrm{Res}(f, f')$ je

$$\mathrm{Res}(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a(4ac - b^2).$$

Platí, že f má dvojnásobný koreň práve vtedy, keď $\mathrm{Res}(f, f') = a(4ac - b^2) = 0$.

Tento príklad nás motivuje k definícii

DEFINÍCIA 3.11. Nech $f \in k[x]$, $f = f_n x^n + \cdots + f_1 x + f_0$, $f_n \neq 0$. *Diskriminant* polynómu f je

$$\mathrm{disc}(f) = \frac{(-1)^{\frac{n(n-1)}{2}}}{f_n} \mathrm{Res}(f, f').$$

Nasledovné tvrdenie je len refurmuláciou už dokázaného.

TVRDENIE 3.12. *Polynóm $f \in k[x]$ má viacnásobný koreň nad nejakým rozšírením k práve vtedy, keď* $\operatorname{disc}(f) = 0$.

ÚLOHA 26. Nech $f = x^3 + px + q$. Nájdite diskriminant polynómu f.

3.3. Rezultant ako funkcia koreňov polynómov.

PRÍKLAD 3.13. Nech $f, g \in k[x]$ sú polynómy s faktorizáciou nad vhodným rozšírením poľa k:

$$\begin{aligned} f &= f_1(x-\alpha) = f_1 x - f_1\alpha, \\ g &= g_2(x-\beta_1)(x-\beta_2) = g_2x^2 + g_2(-\beta_1-\beta_2)x + g_2\beta_1\beta_2, \end{aligned}$$

teda α je koreňom polynómu f a β_1, β_2 sú korene polynómu g. Ich rezultant potom je

$$\operatorname{Res}(f,g) = \begin{vmatrix} f_1 & -f_1\alpha & 0 \\ 0 & f_1 & -f_1\alpha \\ g_2 & g_2(-\beta_1-\beta_2) & g_2\beta_1\beta_2 \end{vmatrix} = f_1^2 g_2 \begin{vmatrix} 1 & -\alpha & 0 \\ 0 & 1 & -\alpha \\ 1 & -\beta_1-\beta_2 & \beta_1\beta_2 \end{vmatrix} = f_1^2 g_2(\alpha-\beta_1)(\alpha-\beta_2).$$

Toto pozorovanie teraz zovšeobecníme:

VETA 3.14. *Nech $f, g \in k[x]$ sú polynómy stupňov m a n. Nech*

$$\begin{aligned} f &= f_m(x-\alpha_1)\dots(x-\alpha_m), \\ g &= g_n(x-\beta_1)\dots(x-\beta_n) \end{aligned}$$

sú úplné faktorizácie nad rozšírením k. Potom

$$\operatorname{Res}(f,g) = f_m^n g_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j).$$

Dôkaz. Označme si

$$\Theta(f,g) = f_m^n g_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j),$$

chceme ukázať, že $\operatorname{Res}(f,g) = \Theta(f,g)$.

Ak f a g majú spoločný koreň, potom je tvrdenie pravdivé, na základe Vety 3.7. Predpokladajme teda, že f a g nemajú spoločný koreň a tiež bez ujmy na všeobecnosti predpokladajme, že $\deg f \geq \deg g$. Vetu ukážeme indukciou vzhľadom na dĺžku postupnosti nenulových zvyškov v euklidovom algoritme hľadania najväčšieho spoločného deliteľa f, g.

Nech zvyšok po delení polynómu f polynómom g je 0. Z toho vyplýva, že $\deg g = 0$, keďže podľa predpokladu sú polynómy f a g nesúdeliteľné. Polynóm g pozostáva len z absolútneho člena g_0, matica $\operatorname{Syl}(f,g) = g_0\mathrm{I}_m$, a platí

$$\operatorname{Res}(f,g) = g_0^m = g_0^m f_n^0 = \Theta(f,g).$$

(Indukčný krok.) Nech teraz

$$f = qg + r, \qquad \text{kde} \qquad r \neq 0,\ \deg r = d < \deg g,$$

označme vedúci koeficient polynómu r ako r_d. Postupovať budeme tak, že nájdeme predpis pre výpočet $\operatorname{Res}(f,g)$ pomocou $\operatorname{Res}(g,r)$, podobne predpis pre výpočet $\Theta(f,g)$ pomocou $\Theta(g,r)$, a uvidíme, že oba vyzerajú rovnako.

Zo vzťahu $r = f - qg = f - (\sum_{i=0}^{m-n} q_i x^i)g$ dostávame, že $\mathrm{Res}(f,g)$ je determinant

$$\begin{vmatrix} f_m & f_{m-1} & \dots & f_0 & 0 & \dots & 0 \\ 0 & f_m & \dots & f_1 & f_0 & & 0 \\ & & \ddots & & & \ddots & \\ 0 & \dots & 0 & f_m & \dots & f_1 & f_0 \\ g_n & g_{n-1} & \dots & g_0 & 0 & \dots & 0 \\ 0 & g_n & \dots & g_1 & g_0 & & 0 \\ & & \ddots & & & \ddots & \\ 0 & \dots & 0 & g_n & \dots & g_1 & g_0 \end{vmatrix} = \begin{vmatrix} 0 & \dots & 0 & r_d & \dots & r_0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & r_d & \dots & r_0 & & 0 \\ & & & & & \ddots & & \ddots & \\ 0 & \dots & 0 & 0 & \dots & 0 & r_d & \dots & r_0 \\ g_n & g_{n-1} & & \dots & & g_0 & 0 & \dots & 0 \\ 0 & g_n & & \dots & & g_1 & g_0 & & 0 \\ & & \ddots & & & & & \ddots & \\ 0 & \dots & 0 & g_n & & \dots & & g_1 & g_0 \end{vmatrix}.$$

Rovnosť platí, lebo maticu sme modifikovali tak, že k riadkom s koeficientami polynómu f sme pripočítali násobky riadkov s koeficientami g, čo je operácia nemeniaca hodnotu determinantu. Ďalej v tejto matici poprehadzujeme riadky (operácia mení znamienko determinantu) a dostávame, že predchádzajúci determinant je rovný

$$(-1)^{nm} \begin{vmatrix} g_n & g_{n-1} & & \dots & & g_0 & 0 & \dots & 0 \\ 0 & g_n & & \dots & & g_1 & g_0 & & 0 \\ & & \ddots & & & & & \ddots & \\ & & & g_n & & \dots & & g_1 & g_0 \\ 0 & \dots & 0 & r_d & \dots & r_0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & r_d & \dots & r_0 & & 0 \\ & & & & & \ddots & & \ddots & \\ 0 & \dots & 0 & 0 & \dots & 0 & r_d & \dots & r_0 \end{vmatrix} = (-1)^{nm} g_n^{m-d} \mathrm{Res}(g,r),$$

kde poslednú rovnosť sme získali niekoľkonásobným rozvojom determinanu podľa prvého stĺpca. Máme teda vzťah

$$\mathrm{Res}(f,g) = (-1)^{nm} g_n^{m-d} \mathrm{Res}(g,r).$$

Pre nájdenie analogického predpisu pre $\Theta(f,g)$ si najprv všimnine, že z $f = qg + r$ vyplýva, že $f(\beta_i) = r(\beta_i)$ pre všetky korene β_i polynómu g. Počítajme:

$$\begin{aligned} \Theta(f,g) &= f_m^n g_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = (-1)^{mn} f_m^n g_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\beta_j - \alpha_i) \\ &= (-1)^{mn} g_n^m \prod_{j=1}^{n} (f_m \prod_{i=1}^{m} (\beta_j - \alpha_i)) = (-1)^{mn} g_n^m \prod_{j=1}^{n} f(\beta_j) = (-1)^{mn} g_n^m \prod_{j=1}^{n} r(\beta_j) \\ &= (-1)^{mn} g_n^m \prod_{j=1}^{n} (r_d \prod_{i=1}^{d} (\beta_j - \gamma_i)) = (-1)^{nm} g_n^{m-d} \Theta(g,r). \end{aligned}$$

Takže pre výpočet $\Theta(f,g)$ máme ten istý predpis ako pre výpočet $\mathrm{Res}(f,g)$, a z indukčného predpokladu tak dostávame, že $\mathrm{Res}(f,g) = \Theta(f,g)$. □

3.4. Rezultanty a eliminácia. V Príklade 3.9 sme úspešne použili rezultanty na nájdenie spoločných bodov dvoch rovinných kriviek. V skutočnosti sme však túto metódu ešte nepostavili na solídne teoretické základy: Veta 3.7 síce hovorí niečo o tom, kedy majú dva polynómy spoločný koreň, ide však o polynómy o jednej premennej nad *poľom*. V Príklade 3.9 však išlo o polynómy $f, g \in k[x,y]$, s ktorými sme manipulovali ako s polynómami v $(k[y])[x]$, teda koeficienty boli z okruhu $k[y]$. Potrebujeme preto niečo vedieť o vlastnostiach rezultantu v takomto prípade.

Veta 3.15. *Nech* $f, g \in k[x_1, \dots, x_n]$. *Potom*

$$\mathrm{Res}_{x_1}(f,g) \in (f,g) \cap k[x_2, \dots, x_n].$$

Dôkaz. Z definície rezultantu je zrejmé, že $\mathrm{Res}_{x_1}(f,g)$ je polynóm, presnejšie $\mathrm{Res}_{x_1}(f,g) \in k[x_2,\ldots,x_n]$. Že platí aj $\mathrm{Res}_{x_1}(f,g) \in (f,g)$, ukážeme Cramerovým pravidlom:

Nech A je ľubovoľná štvorcová matica stupňa n, a nech $\mathrm{ad}A$ označuje adjungovanú maticu k matici A, čiže

$$\mathrm{ad}A_{i,j} = (-1)^{i+j}|A_{j,i}|,$$

kde $A_{j,i}$ je podmatica A, ktorú získame vynechaním j-teho riadku a i-teho stĺpca). Potom platí (Cramerovo pravidlo):

$$A \cdot \mathrm{ad}A = \mathrm{ad}A \cdot A = |A|\mathrm{I}_n.$$

Aplikovaním tohto pravidla na Sylvestrovu maticu dostávame

$$\mathrm{adSyl}(f,g) \cdot \mathrm{Syl}(f,g) = \mathrm{Res}_{x_1}(f,g)\mathrm{I}_N, \quad \text{kde } N = \deg f + \deg g,$$

teda po vynásobení zľava hocijakou riadkovou maticou $(c_1\ \ldots\ c_N)$ dostávame

$$(c_1\ \ldots\ c_N) \cdot \mathrm{adSyl}(f,g) \cdot \mathrm{Syl}(f,g) = \mathrm{Res}_{x_1}(f,g)(c_1\ \ldots\ c_N),$$

Nech špeciálne $(c_1\ \ldots\ c_N) = (0\ \ldots\ 0\ 1)$, a tak máme, že

$$\begin{aligned}(0\ \ldots\ 0\ 1) \cdot \mathrm{adSyl}(f,g) \cdot \mathrm{Syl}(f,g) &= \mathrm{Res}_{x_1}(f,g)(0\ \ldots\ 0\ 1), \quad \text{čiže}\\ (v_1\ \ldots\ v_N) \cdot \mathrm{Syl}(f,g) &= (0\ \ldots\ 0\ \mathrm{Res}_{x_1}(f,g)).\end{aligned}$$

V dôkaze Vety 3.7 sme si vysvetlili, že Sylvestrova matica je maticou zobrazenia lineárnych priestorov – vtedy išlo o priestory nad poľom k, teraz sú to „priestory" (presnejšie takzvané *moduly*) nad okruhom $k[x_2,\ldots,x_n]$: išlo o zobrazenie, ktoré dvojici polynómov (p,q) priradí polynóm $pf+qg$. Vidíme, že toto zobrazenie vektor so súradnicami $v_1,\ldots,v_N$, ktorý reprezentuje dvojicu polynómov $(v_1x_1^{n-1}+\cdots+v_{n-1}x_1+v_n, v_{n+1}x_1^{m-1}+\cdots+v_{N-1}x_1+v_N)$, zobrazí na vektor so súradnicami $0,\ldots,0,\mathrm{Res}_{x_1}(f,g)$, ktorý zas reprezentuje polynóm $0x_1^{N-1}+\cdots+0x_1+\mathrm{Res}_{x_1}(f,g)$. Teda našli sme $p,q \in k[x_1,\ldots,x_n]$ také, že $\mathrm{Res}_{x_1}(f,g) = pf+qg$, a preto $\mathrm{Res}_{x_1}(f,g) \in (f,g)$. □

Dôsledok.

$$V((f,g)\cap k[x_2,\ldots,x_n]) \subseteq V(\mathrm{Res}_{x_1}(f,g)), \tag{17}$$

kde na oboch stranách inklúzie sú variety priestoru $\mathbb{A}^{n-1}$.

Z Tvrdenia 2.5 pre premietanie $\pi\colon (a_1,a_2,\ldots,a_n) \mapsto (a_2,\ldots,a_n)$ máme, že

$$\overline{\pi(V(f,g))} \subseteq V((f,g)\cap k[x_2,\ldots,x_n]),$$

Spolu s (17) tak dostávame

$$\overline{\pi(V(f,g))} \subseteq V(\mathrm{Res}_{x_1}(f,g)).$$

Postup v Príklade 3.9 bol teda korektný: polynóm $\mathrm{Res}_x(f,g)$ popisoval varietu ktorá určite obsahovala všetky body priemetu prieniku kružnice a hyperboly na y-os. Potom x-súradnicu môžeme dopočítať buď dosadením konkrétnej y-súradnice do f a g, alebo ešte nájdeme rezultant

$$\mathrm{Res}_y(f,g) = x^4 - 4x^2 + 1.$$

Dostali sme štyri možnosti pre hodnotu x-súradnice, tiež máme štyri možnosti pre hodnotu y-súradnice, dokopy tak otestujeme 16 bodov, spomedzi ktorých tak vyberieme riešenia.

Príklad 3.16. Tento príklad ukazuje, že $V((f,g)\cap k[x_2,\ldots,x_n])$ naozaj môže byť vlastnou podmnožinou $V(\mathrm{Res}_{x_1}(f,g))$, dokonca aj nad algebraicky uzavretým poľom, t.j. inklúzia v (17) sa nedá nahradiť rovnosťou.

Nájdime prienik kriviek $V(f), V(g) \subset \mathbb{A}^2(\mathbb{C})$, kde

$$\begin{aligned}f &= xy-1\\ g &= x^2y+y^2-4.\end{aligned}$$

Rezultant polynómov f,g vzhľadom na premennú x popisuje algebraickú varietu na y-osi, ktorá obsahuje priemet $V(f)\cap V(g)$ na túto os:

$$\mathrm{Res}_x(f,g) = y^4 - 4y^2 + y = y(y^3-4y+1).$$

Algebraická varieta $V(\mathrm{Res}_x(f,g)$ obsahuje bod (0), avšak $V(f) \cap V(g)$ neobsahuje žiaden bod so súradnicami $(a,0)$.

PRÍKLAD 3.17. Neuviedli sme si žiadnu teóriu ohľadne použitia rezultantov pre variety, ktoré nie sú nularozmerné, napriek tomu si ukážeme, že ich môžme úspešne použiť aj v takýchto situáciách.

Nájdime všetky racionálne body (t.j. body, ktorých súradnice sú racionálne čisla) algebraickej variety $V(f,g)$, ak

$$\begin{aligned} f &= x^2y - 3xy^2 + x^2 - 3xy \\ g &= x^3y + x^3 - 4y^2 - 3y + 1. \end{aligned}$$

Vypočítame rezultanty (aj výpočet rezultantu aj faktorizáciu urobíme napríklad pomocou Singularu):

$$\begin{aligned} \mathrm{Res}_x(f,g) &= -108y^9 - 513y^8 - 929y^7 - 738y^6 - 149y^5 + 112y^4 + 37y^3 - 14y^2 - 3y + 1 \\ &= -108(y+1)^5(y - \frac{1}{4})(y^3 - \frac{4}{27}y + \frac{1}{27}) \end{aligned}$$

Priemet variety $V(f,g)$ na y-os teda obsahuje najviac 2 racionálne body. Podobne nájdeme množinu obsahujúcu priemet $V(f,g)$ na x-os:

$$\mathrm{Res}_y(f,g) = 0.$$

O tomto priemete tak nevieme povedať nič. Nemôžme preto jednoducho zobrať všetky možnosti pre x- a y-súradnice a dosadzovaním spomedzi nich vybrať riešenia, ale budeme rozširovať čiatočné riešenia získané z rovnice $\mathrm{Res}_x(f,g) = 0$.

Ak $y = -1$, potom $f(x,-1) = 0$ pre všetky x, podobne $g(x,-1) = 0$ pre všetky x. Varieta $V(f,g)$ teda obsahuje priamku $V(y+1)$.

Ak $y = \frac{1}{4}$, potom sústava $f(x,\frac{1}{4}) = g(x,\frac{1}{4}) = 0$ má riešenie $x = 0$, a tak posledným racionálnym bodom $V(f,g)$ je bod $(0,\frac{1}{4})$.

Síce je rezultant definovaný len pre dva polynómy, možno ho použiť aj na hľadanie spoločných koreňov viacerých polynómických rovníc. Napríklad, ak chceme nájsť body variety $V(f,g,h)$, kde $f,g,h \in k[x,y,z]$, môžme konštruovať priemety postupne: $V(\mathrm{Res}_z(f,g)) \subset \mathbb{A}^2$ obsahuje body priemetu variety $V(f,g)$ do xy-roviny, podobne $V(\mathrm{Res}_z(f,h)) \subset \mathbb{A}^2$ obsahuje body priemetu $V(f,h)$, takže $V(\mathrm{Res}_z(f,g), \mathrm{Res}_z(f,h))$ obsahuje priemet $V(f,g,h)$ do xy-roviny. Pomocou rezultantov nájdeme varietu obsahujúcu priemet na x-os, podobne priemet na y-os. Potom ešte analogickým postupom nájdeme varietu obsahujúcu priemet na z-os. Ak dostaneme len konečne veľa možností pre hodnotu každej súradnice, jednoducho dosadíme všetky možnosti do pôvodných rovníc $f = g = h = 0$, a tak nájdeme všetky body variety $V(f,g,h)$.

ÚLOHA 27. Použite rezultanty na nájdenie všetkých racionálnych bodov variety, ktorú sme si uviedli na začiatku časti o eliminániách:

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

Na záver si ešte urobíme malé porovnanie dvoch metód, ktoré sme si predstavili, na hľadanie riešení sústavy polynomických rovníc.

Na prvý pohľad sa medóda používajúca rezultanty javí ako menej efektívna. Teória spojená s nimi vyzerá omnoho komplikovanejšie, a navyše so slabšími tvrdeniami – uzáver priemetu algebraickej variety je Gröbnerovými bázami popísaný presne, no pomocou rezultantov nájdeme len varietu obsahujúcu uzáver priemetu. Tiež sa môže zdať, že pomocou rezultantov nevieme dobre uchopiť algebraické variety, ktoré majú nekonečne veľa bodov: že sa nám poradilo vyriešiť Príklad 3.17, bolo tak trochu štastie. Napriek tomu sa pri mnohých príležitostiach veľmi často používajú práve rezultanty. Dôvodov je na to niekoľko:

Postupy využívajúce rezultanty sú podstatne jednoduchšie než používanie Gröbnerových báz. Pomocou Gröbnerových báz síce jednoducho nájdeme priemet na jednu súradnicovú os, vyriešime príslušnú rovnicu, ale rozširovanie čiastočných riešení na úplné si vyžaduje dosť podrobnú analýzu jednotlivých eliminačných ideálov – ak by sme túto metódu chceli naprogramovať, program by bol pomerne komplikovaný.

Ďalej u rezultantov máme lepšiu kontrolu nad zložitosťou (časovou aj pamäťovou) výpočtu. Pre dané dva polynómy totiž vieme, ako sa konštruuje rezultant a tak vieme odhadnúť, s akými veľkými polynómami sa bude počas výpočtu manipulovať. Naproti tomu pri hľadaní Gröbnerovej bázy je ťažko povedať, ako veľké S-polynómy sa budú musieť vypočítať. Nie je zriedkavosťou, že priebežné S-polynómy sú podstatne komplikovanejšie než vstupné polynómy (tie, ktorými ideál definujeme) a výsledná Gröbnerova báza. Preto nie je ani veľmi rozumné vyhýbať sa rezultantom aj rozširovaniu čiastočných riešení tak, že by sme hľadali Groebnerovu bázu viackrát a tak, aby sme zakaždým našli priemet na inú súradnicovú os.

Ak hľadáme približné riešenia sústavy, pri použití rezultantov máme lepšiu kontrolu nad chybou: v každej súradnici nájdeme dostatočne presnú aproximáciu, a tak vieme aká je maximálne výsledná chyba. Ak by sme použili Gröbnerove bázy a jednu súradnicu vypočítame s chybou, táto chyba vo všeobecnosti výrazne narastá v každej ďalšej súradnici, keď riešenie rozširujeme.

Teória rezultantov je omnoho rozvinutejšia než sme si uviedli a tento nástroj je omnoho mocnejší než sa môže zdať na základe tejto prednášky. Mnohé tvdrenia, ktoré hovoria o rozširovaní čiastočných riešení nájdených cez Gröbnerove bázy, sú dokazované práve pomocou rezultantov.

4. Reálne korene polynomickej rovnice

Pri mnohých úlohách nepotrebujeme nájsť všetky body nejakej algebraickej variety, špeciálne komplexné korene nás často nezaujímajú. Väčšinou chceme nájsť reálne korene, často sa dokonca uspokojíme aj s ich dostatočnou aproximáciou. Ukázali sme si, že problém hľadania riešení sústavy polynomických rovníc (v prípade, že ich je konečne veľa) vieme zredukovať na hľadanie koreňov jednej polynomickej rovnice s jednou neznámou. Stačia nám teda metódy, ktoré nám pomôžu nájsť korene takejto rovnice.

Numerická matematika ponúka niekoľko postupov hľadania koreňov (presnejšie ich aproximácií), každá z nich má nejaké obmedzenia. Všeobecná Newtonova metóda nájde jeden koreň, i to v prípade, že máme dobrý prvý odhad. Metóda Bezierovho orezávania nájde všetky korene na vopred zvolenom intervale, funguje ale len pre polynómy (na rozdiel od Newtonovej metódy, ktorá je použiteľná pri akejkoľvek diferencovateľnej funkcii). Takéto orezávanie je pomerne spoľahlivé, problémy sa môžu vyskytnúť pri nestabilných situáciách (viacnásobný koreň). V prípade, že máme korene rovnice vopred separované, čiže máme zoznam intervalov taký, že v každom intervale sa nachádza práve jeden koreň, použiteľná metóda na nájdenie koreňa je aj jednoduché binárne delenie intervalu.

V tejto kapitole si uvedieme tvrdenia a postupy na predspracovanie polynomickej rovnice, takže potom bude možné korene dohľadať numerickými metódami.

4.1. Ohraničenie koreňov.

VETA 4.1. *Nech* $f \in \mathbb{R}[x]$, $f = f_m x^m + \cdots + f_1 x + f_0$, $f_m \neq 0$. *Ak*

$$|a| \geq 2 \sum_{i=0}^{m} \frac{|f_i|}{|f_m|}, \tag{18}$$

potom $f(a)$ *a* $f_m a^m$ *majú rovnaké znamienko.*

Dôkaz. Najprv si všimnime, že z (18) vyplýva, že $|a| > 2$. Ďalej za predpokladu $a \neq 0$ ukážeme, že podiel $f(a)/f_m a^m$ je kladný.

$$\begin{aligned}
\frac{f(a)}{f_m a^m} &= 1 + \sum_{i=0}^{m-1} \frac{f_i}{f_m} a^{i-m} \geq 1 - \left(\sum_{i=0}^{m-1} \frac{|f_i|}{|f_m|} |a|^{i-m} \right) \\
&\geq 1 - \left(\sum_{i=0}^{m} \frac{|f_i|}{|f_m|} \right) \left(\frac{1}{|a|} + \cdots + \frac{1}{|a|^m} \right) \\
&\geq 1 - \frac{1}{2} \left(1 + \frac{1}{|a|} + \cdots + \frac{1}{|a|^{m-1}} \right) > 1 - \frac{1}{2} \cdot \frac{1}{1 - \frac{1}{|a|}} > 0.
\end{aligned}$$

□

DÔSLEDOK. *Všetky reálne korene rovnice* $f_m x^m + \cdots + f_1 x + f_0 = 0$, *(*$f_m \neq 0$*) sa nachádzajú v intervale*

$$\left(-2 \sum_{i=0}^{m} \frac{|f_i|}{|f_m|},\ 2 \sum_{i=0}^{m} \frac{|f_i|}{|f_m|} \right).$$

Existuje viacej ohraničení pre reálne korene, aj omnoho lepšie, pre nás však stačí takéto jednoduché. Podstatné je, že vieme explicitne napísať interval obsahujúci všetky reálne korene.

4.2. Sturmova veta.

ÚLOHA 28. Rovnica $f(x) = 0$ pre $f \in \mathbb{C}[x]$, kde $f \neq 0$, má presne $\deg f$ komplexných riešení, počítaných aj s násobnosťou. Ako ale zistiť počet navzájom rôznych komplexných riešení? Návod:

(a) $\alpha \in \mathbb{C}$ je r-násobný koreň polynómu f práve vtedy, keď α je spoločný $(r-1)$-násobný koreň polynómov f a f'. Dokážte.

(b) Využijúc predchádzajúce tvrdenie navrhnite algoritmus na zistenie počtu navzájom rôznych koreňov polynómu f.

Vo zvyšku kapitoly budeme používať nasledovné označenie: ak f, g sú polynómy z $k[x]$, tak $\mathrm{rem}(f, g)$ označuje zvyšok po delení polynómu f polynómom g, t.j. jediný taký polynóm $r \in k[x]$, že

$$f = qg + r, \quad \text{kde } \deg r < \deg g.$$

DEFINÍCIA 4.2. *Sturmova postupnosť polynómu* $p \in k[x]$ je postupnosť $(p_0, p_1, \ldots, p_k)$ polynómov, kde

$$\begin{aligned} p_0 &= p, \\ p_1 &= p', \\ p_i &= -\mathrm{rem}(p_{i-2}, p_{i-1}), \quad \text{pre } i \geq 2, \end{aligned}$$

kde p_k je posledný nenulový člen tejto postupnosti zvyškov (t.j. $p_k \mid p_{k-1}$).

V Sturmovej postupnosti zrejme platí

$$p_{i-1} = q_{i-1}p_i - p_{i+1}. \tag{19}$$

DEFINÍCIA 4.3. Nech $\mathbf{a} = (a_0, \ldots, a_k)$ je postupnosť nenulových reálnych čísel. Počet znamienkových zmien $\mathrm{var}(\mathbf{a})$ v postupnosti $\mathbf{a}$ je definovaný

$$\begin{aligned} \mathrm{var}(a_0) &= 0 \\ \mathrm{var}(a_0, \ldots, a_i) &= \begin{cases} 1 + \mathrm{var}(a_0, \ldots, a_{i-1}), & \text{ak } a_{i-1}a_i < 0 \\ \mathrm{var}(a_0, \ldots, a_{i-1}), & \text{ak } a_{i-1}a_i > 0. \end{cases} \end{aligned}$$

Ak $\mathbf{a} = (a_0, \ldots, a_k)$ je postupnosť reálnych čísel, potom $\mathrm{var}(\mathbf{a})$ definujeme ako počet znamienkových zmien v postupnosti, ktorú získame z $\mathbf{a}$ vynechaním všetkých núl.

PRÍKLAD 4.4. $\mathrm{var}(1, -2, 2, 0, 0, 3, 4, -5, -2, 0, 3) = 4$.

DEFINÍCIA 4.5. Nech $\mathbf{p} = (p_0, p_1, \ldots, p_k)$ je postupnosť polynómov v $\mathbb{R}[x]$ a nech a je reálne číslo. Potom označujeme

$$\mathrm{var}_{\mathbf{p}}(a) = \mathrm{var}(p_0(a), p_1(a), \ldots, p_k(a)).$$

VETA 4.6 (**Sturm**). *Nech* $p \in \mathbb{R}[x]$ *a nech* $\mathbf{p} = (p_i)_{i=0}^k$ *je jeho Sturmova postupnosť. Nech* $a, b \in \mathbb{R}$ *sú také, že* $a < b$, $p(a) \neq 0$, $p(b) \neq 0$. *Počet reálnych koreňov polynómu* p *na intervale* (a, b) *je rovný číslu*

$$\mathrm{var}_{\mathbf{p}}(a) - \mathrm{var}_{\mathbf{p}}(b).$$

Dôkaz Sturmovej vety rozdelíme na viacero tvrdení.

DEFINÍCIA 4.7. Nech $p \in \mathbb{R}[x]$ a nech $\mathbf{p} = (p_i)_{i=0}^k$ je jeho Sturmova postupnosť. Nech $a, b \in \mathbb{R}$, $a < b$. Interval $\langle a, b\rangle$ sa nazýva *fundamentálny interval polynómu* p, ak $p(a) \neq 0, p(b) \neq 0$, a existuje také $\gamma_0 \in (a, b)$, že pre všetky $\gamma \in \langle a, b\rangle$, $\gamma \neq \gamma_0$ platí $p_i(\gamma) \neq 0$ pre všeky p_i, $i = 0, \ldots, k$.

Neformálne, $\langle a, b\rangle$ je fundamentálnym intervalom polynómu p, ak každý z polynómov Sturmovej postupnosti má na (a, b) najviac jeden koreň, a ten je rovnaký pre všetky členy postupnosti.

TVRDENIE 4.8. *Nech* $\langle a, b\rangle$ *je fundamentálny interval polynómu* $p \in \mathbb{R}[x]$. *Ak* p *nemá reálny koreň na* $\langle a, b\rangle$, *potom* $\mathrm{var}_{\mathbf{p}}(a) = \mathrm{var}_{\mathbf{p}}(b)$.

Dôkaz. Predpokladajme najprv, že žiaden z polynómov p_i Sturmovej postupnosti nemá koreň na $\langle a, b\rangle$. Potom graf každého polynómu je buď celý nad osou x alebo pod ňou, takže $\mathrm{sgn}(p_i(a)) = \mathrm{sgn}(p_i(b))$, a preto $\mathrm{var}_{\mathbf{p}}(a) = \mathrm{var}_{\mathbf{p}}$.

Nech teraz existuje i také, že $p_i(\gamma_0) = 0$ pre nejaké $\gamma_0 \in (a, b)$. Z (19) vyplýva, že po sebe idúce polynómy v Sturmovej postupnosti nemajú koreň v γ_0, lebo inak by γ_0 bol koreňom všetkých polynómov postupnosti, aj $p_0 = p$, čo by bol spor s predpokladom. Teda $p_{i-1}(\gamma_0) \neq$

0 a tiež $p_{i+1}(\gamma_0) \neq 0$, a navyše z (19) dostávame aj $p_{i+1}(\gamma_0) = -p_{i-1}(\gamma_0)$. Keďže $\langle a, b\rangle$ je fundamentálny interval, p_{i+1} a p_{i-1} na ňom žiaden koreň nemajú, a tak

$$\operatorname{sgn}(p_{i+1}(a)) = \operatorname{sgn}(p_{i+1}(b)) = -\operatorname{sgn}(p_{i-1}(a)) = -\operatorname{sgn}(p_{i-1}(b)).$$

V oboch podpostupnostiach

$$(p_{i-1}(a), p_i(a), p_{i+1}(a))$$
$$(p_{i-1}(b), p_i(b), p_{i+1}(b))$$

tak dochádza presne k jednej znamienkovej zmene. Tým sme ukázali, že počet znamienkových zmien v oboch postupnostiach $(p_i(a))_{i=0}^k$ a $(p_i(b))_{i=0}^k$ je rovnaký. □

Tvrdenie 4.9. *Nech $\langle a, b\rangle$ je fundamentálny interval polynómu $p \in \mathbb{R}[x]$. Ak p má jeden reálny koreň na $\langle a, b\rangle$, potom* $\operatorname{var}_{\mathbf{p}}(a) = \operatorname{var}_{\mathbf{p}}(b) + 1$.

Dôkaz. Nech γ_0 je jednoduchý koreň polynómu p, čiže $p'(\gamma_0) \neq 0$. Tak ako v dôkaze predchádzajúceho tvrdenia potom zistíme, že žiadne dva za sebou idúce polynómy Sturmovej postupnosti nemajú koreň v γ_0, a tiež odtiaľ analogicky usúdime, že

$$\operatorname{var}(p_1(a), \ldots, p_k(a)) = \operatorname{var}(p_1(b), \ldots, p_k(b)).$$

Rozdiel medzi počtom znamienkových zmien tak môže nastať iba medzi prvými dvoma členmi postupností.

Keďže $p'(\gamma_0) \neq 0$, p' nemá koreň na $\langle a, b\rangle$ (ide o fundamentálny interval), je p' na celom intervale buď kladný (a p rastie na $\langle a, b\rangle$), alebo záporný (a p klesá). Možnosti pre znamienka prvých dvoch členov postupností ta sú

$p(a)$	$p'(a)$	$p(b)$	$p'(b)$
$-$	$+$	$+$	$+$
$+$	$-$	$-$	$-$

a tak v tomto prípade dostávame $\operatorname{var}_{\mathbf{p}}(a) = \operatorname{var}_{\mathbf{p}} + 1$.

Nech $p(\gamma_0) = p'(\gamma_0) = 0$, teda γ_0 je viacnásobný koreň polynómu p. Ak jeho násobnosť v p je r, potom jeho násobnosť v p' je $r - 1$. Navyše p_k je najväčším spoločným deliteľom p a p' (Sturmova postupnosť je až na znamienka postupnosťou zvyškov v euklidovom algoritme), takže γ_0 je $(r-1)$-násobný koreň aj v p_k.

Uvažujme postuponosť polynómov

$$\tilde{\mathbf{p}} = (\tilde{p}_0, \tilde{p}_1, \ldots, \tilde{p}_k = 1), \quad \text{kde } \tilde{p}_i = \frac{p_i}{p_k}.$$

(Toto už nie je Sturmova postupnosť, lebo $\tilde{p}_1$ nie je deriváciou $\tilde{p}_0$). Pre počty znamienkových zmien platí

$$\operatorname{var}_{\tilde{\mathbf{p}}}(a) = \operatorname{var}_{\mathbf{p}}(a), \quad \operatorname{var}_{\tilde{\mathbf{p}}}(b) = \operatorname{var}_{\mathbf{p}}(b).$$

Taktiež ostáva v platnosti vzťah

$$\tilde{p}_{i-1} = q_{i-1}\tilde{p}_i - \tilde{p}_{i+1}.$$

V postupnosti $\tilde{\mathbf{p}}$ už γ_0 je len jednoduchým koreňom polynómu $\tilde{p}_0$, a nie je koreňom $\tilde{p}_1$. Podobne ako v prvej časti dôkazu tak dostávame, že

$$\operatorname{var}(\tilde{p}_1(a), \ldots, \tilde{p}_k(a)) = \operatorname{var}(\tilde{p}_1(b), \ldots, \tilde{p}_k(b)),$$

rozdiel v počte znamienkových zmien tak znovu môže nastať len medzi prvými dvoma členmi postupnosti. Keďže $\tilde{p}_1$ nie je deriváciou $\tilde{p}_0$, máme tak viacej možností:

$\tilde{p}_0(a)$	$\tilde{p}_1(a)$	$\tilde{p}_0(b)$	$\tilde{p}_1(b)$
$+$	$+$	$-$	$+$
$+$	$-$	$-$	$-$
$-$	$+$	$+$	$+$
$-$	$-$	$+$	$-$

Potrebujeme ukázať, že možnosti v prvom a štvrtom riadku nenastanú. Pre tento účel potrebujeme rozlíšiť, či násobnosť r koreňa γ_0 v p je párna alebo nepárna.

Ak r je nepárne číslo, potom platí

$$\begin{aligned}\operatorname{sgn}(p(a)) &= -\operatorname{sgn}(p(b))\\ \operatorname{sgn}(p'(a)) &= \operatorname{sgn}(p'(b))\\ \operatorname{sgn}(p_k(a)) &= \operatorname{sgn}(p_k(b)).\end{aligned}$$

Z tabuľky pre znamienka p a p'

$p(a)$	$p'(a)$	$p(b)$	$p'(b)$
$-$	$+$	$+$	$+$
$+$	$-$	$-$	$-$

tak dostávame tabuľku pre $\tilde{p}_0$ a $\tilde{p}_1$:

$\tilde{p}_0(a)$	$\tilde{p}_1(a)$	$\tilde{p}_0(b)$	$\tilde{p}_1(b)$
$-$	$+$	$+$	$+$
$+$	$-$	$-$	$-$
$+$	$-$	$-$	$-$
$-$	$+$	$+$	$+$

V prípade, keď r je párne, sa postupuje analogicky. □

Dôkaz Vety 4.6. Dve predchádzajúce tvrdenia sú vlastne dôkazom Sturmovej vety v prípade, že interval $\langle a, b\rangle$ je fundamentálny. Ak $\langle a, b\rangle$ nie je fundamentálny, tak ho rozdelíme na fundamentálne intervaly: Nech $\gamma_0 < \gamma_1 < \cdots < \gamma_k$ sú všetky korene všetkých polynómov Sturmovej postupnosti na intervale (a, b). Zvolíme α_i, $i = 1, \ldots, k$ tak, že

$$a < \gamma_0 < \alpha_1 < \gamma_1 < \alpha_2 < \cdots < \alpha_k < \gamma_k < b.$$

Potom $\langle a_{i-1}, a_i\rangle$ sú fundamentálne intervaly polynómu p a pre počty koreňov tak máme

$$\begin{aligned}\#\text{koreňov na } (a,b) &= \#\text{koreňov na } (a,a_1) + \#\text{koreňov na } (a_1,a_2) + \cdots + \#\text{koreňov na } (a_k,b)\\ &= (\operatorname{var}_{\mathbf{p}}(a) - \operatorname{var}_{\mathbf{p}}(a_1)) + (\operatorname{var}_{\mathbf{p}}(a_1) - \operatorname{var}_{\mathbf{p}}(a_2)) + \cdots + (\operatorname{var}_{\mathbf{p}}(a_k) - \operatorname{var}_{\mathbf{p}}(b))\\ &= \operatorname{var}_{\mathbf{p}}(a) - \operatorname{var}_{\mathbf{p}}(b)).\end{aligned}$$

□

Príklad 4.10. Separujeme reálne korene polynómu

$$f = x^3 - 4x^2 + 3x + 1.$$

Pomocou Vety 4.1 najprv nájdeme interval obsahujúci všetky reálne korene polynómu:

$$M = 2\sum_{i=0}^{3} \frac{|f_i|}{|f_m|} = 2(1 + 4 + 3 + 1) = 18,$$

takže všetky reálne korene sú v intervale $(-18, 18)$. Sturmova postupnosť polynómu f je

$$\begin{aligned}p_0 &= f = x^3 - 4x^2 + 3x + 1,\\ p_1 &= f' = 3x^2 - 8x + 3,\\ p_2 &= -\operatorname{rem}(f, f') = \frac{14}{9}x - \frac{7}{3},\\ p_3 &= -\operatorname{rem}(p_1, p_2) = \frac{9}{4}.\end{aligned}$$

Pomocou Sturmovej vety zistíme počet reálnych koreňov:

$$\begin{aligned}\operatorname{var}_{\mathbf{p}}(-18) &= \operatorname{var}(p_0(-18), p_1(-18), p_2(-18), p_3(-18)) = 3\\ \operatorname{var}_{\mathbf{p}}(-18) &= \operatorname{var}(p_0(18), p_1(18), p_2(18), p_3(18)) = 0\end{aligned}$$

takže polynóm f má tri reálne korene. Z

$$\mathrm{var}_{\mathbf{p}}(0) = \mathrm{var}(1, 3, -\frac{7}{3}, \frac{9}{4}) \;=\; 2$$

vieme, že dva z koreňov sa nachádzajú v intervale $(0, 18)$ a jeden je v intervale $(-18, 0)$. Nakoniec

$$\mathrm{var}_{\mathbf{p}}(2) = \mathrm{var}(-1, -1, \frac{7}{9}, \frac{9}{4}) \;=\; 1,$$

nám hovorí, že jeden z kladných koreňov je na intervale $(0, 2)$ a druhý na intervale $(2, 18)$. Všetky korene sú jednoduchými koreňmi, takže ich ľahko dohľadáme ľubovoľnou numerickou metódou (napr. aj jednoduchou bisekciou intervalu).

KAPITOLA 4

Naspäť ku geometrii

1. Implicitizácia (Hľadanie obrazu zobrazenia)

1.1. Variety parametrizované polynómami.

PRÍKLAD 1.1. Majme zobrazenie $\varphi\colon \mathbb{A}^2 \to \mathbb{A}^3$

$$(t,u) \mapsto (t+u, t^2+2tu, t^3+3t^2u),$$

čiže obrazom bodu $(t,u) \in \mathbb{A}^2$ je bod $(x,y,z) \in \mathbb{A}^3$, pre súradnice ktorého platí

$$\begin{aligned} x &= t+u, \\ y &= t^2+2tu, \\ z &= t^3+3t^2u. \end{aligned}$$

Obrazom zobrazenia φ je plocha X určená rovnicou

$$4x^3z - 3x^2y^2 - 6xyz + 4y^3 + z^2 = 0$$

(zatiaľ bez dôkazu). Na zobrazenie φ sa môžme tiež pozerať, že je to parametrické vyjadrenie plochy, uvedená rovnica je zase implicitné vyjadrenie. Ak parametrické vyjadrenie dosadíme do implicitnej rovnice, dostaneme konštantný nulový polynóm. Tým sme overili, že pre všetky $(t,u) \in \mathbb{A}^2$ platí, že $\varphi(t,u) \in X$, a teda $\varphi(\mathbb{A}^2) \subset X$. Ostáva teda overiť, že namiesto inklúzie platí rovnosť. Hľadanie obrazu takéhoto zobrazenia sa nazýva aj *implicitizácia*.

Vo všeobecnosti obrazom algebraickej variety (v našom príklade je to $\mathbb{A}^2$) v polynomiálnom zobrazení nemusí byť algebraická varieta – videli sme napríklad, že priemet hyperboly na niektorú os je priamka bez jedného bodu. Preto pri implicitizácii sa snažíme nájsť rovnicu (rovnice) popisujúcu uzáver obrazu, čo je najmenšia algebraická varieta obsahujúca obraz. Presnejšie, máme zobrazenie $\varphi\colon \mathbb{A}^m \to \mathbb{A}^n$, $(t_1,\dots,t_m) \mapsto (x_1,\dots,x_n)$ dané predpisom

$$\begin{aligned} x_1 &= \varphi_1(t_1,\dots,t_m) \\ &\vdots \\ x_n &= \varphi_n(t_1,\dots,t_m) \end{aligned} \tag{20}$$

kde φ_i sú polynómy, a chceme nájsť algebraickú varietu $\overline{\varphi(\mathbb{A}^m)}$.

Uvažujme ideál $I \subset k[t_1,\dots,t_m,x_1,\dots,x_n]$,

$$I = (x_1 - \varphi_1(t_1,\dots,t_m), \dots, x_n - \varphi_n(t_1,\dots,t_m)).$$

Body na variete $V(I) \subset \mathbb{A}^{m+n}$ sú tvaru

$$(a_1,\dots,a_m,\varphi_1(a_1,\dots,a_m),\dots,\varphi_n(a_1,\dots,a_m)),$$

pre nejaké $(a_1,\dots,a_m)$, takže $V(I)$ je graf zobrazenia φ. (Analógia s funkciou jednej premennej: všetky body roviny, ktoré sú tvaru $(x,f(x))$, tvoria graf funkcie $f\colon x \mapsto f(x)$.) Každý bod $(t_1,\dots,t_m) \in \mathbb{A}^m$ vieme zobraziť na bod grafu:

$$\iota\colon (t_1,\dots,t_m) \mapsto (t_1,\dots,t_m,\varphi_1(t_1,\dots,t_m),\dots,\varphi_n(t_1,\dots,t_m)),$$

zrejme obrazom tohto zobrazenia je presne $V(I)$. Ďalej majme projekciu $\pi\colon \mathbb{A}^{m+n} \mapsto \mathbb{A}^n$ na posledných n súradníc:

$$\pi\colon (t_1,\dots,t_m,x_1,\dots,x_n) \mapsto (x_1,\dots,x_n).$$

Ľahko ukážeme, že zobrazenie φ je zložením zobrazenia ι a projekcie π:

$$\begin{aligned}\pi(\iota(t_1,\ldots,t_m)) &= \pi(t_1,\ldots,t_m,\varphi_1(t_1,\ldots,t_m),\ldots,\varphi_n(t_1,\ldots,t_m))\\ &= (\varphi_1(t_1,\ldots,t_m),\ldots,\varphi_n(t_1,\ldots,t_m))\\ &= \varphi(t_1,\ldots,t_m)\end{aligned}$$

Keďže $\iota(\mathbb{A}^m) = V(I)$, rovnice pre varietu $\overline{\varphi(\mathbb{A}^m)}$ budú presne rovnice pre $\pi(V(I))$.

VETA 1.2. *Nech k je nekonečné pole, $\mathbb{A}^m, \mathbb{A}^n$ sú afinné priestory nad k. Nech $\varphi\colon \mathbb{A}^m \to \mathbb{A}^n$ je zobrazenie popísané polynómami ako v (20). Nech ďalej $I \subset k[t_1,\ldots,t_m,x_1,\ldots,x_n]$ je ideál*

$$(x_1 - \varphi_1(t_1,\ldots,t_m),\ldots,x_n - \varphi_n(t_1,\ldots,t_m)).$$

Potom $\overline{\varphi(\mathbb{A}^m)} = V(I \cap k[x_1,\ldots.x_n])$

Dôkaz. V prípade, že k je algebraicky uzavreté, tvrdenie vety vyplýva z predchádzajúcej diskusie a z Vety 2.4 v Kapitole 3. Ak k nie je algebraicky uzavreté, namiesto rovnosti podľa Tvrdenia 2.5 tej istej kapitoly máme iba jednu inklúziu,

$$\overline{\varphi(\mathbb{A}^m)} \subset V(I \cap k[x_1,\ldots.x_n]).$$

Potrebujeme preto ešte ukázať, že $V(I \cap k[x_1,\ldots.x_n])$ je najmenšia algebraická varieta obsahujúca $\varphi(\mathbb{A}^m)$.

Pre algebraickú varietu Z takú, že $Z \supset \varphi(\mathbb{A}^m)$ ukážeme, že $Z \supset V(I \cap k[x_1,\ldots,x_n])$.

Nech $Z = V(g_1,\ldots,g_s)$ $(g_i \in k[x_1,\ldots,x_n])$ a nech $Z \supset \varphi(\mathbb{A}^m)$. To znamená, že každý bod z obrazu φ spĺňa rovnice pre Z:

$$g_i \circ \varphi(a_1,\ldots,a_m) = 0 \quad \forall (a_1,\ldots,a_m) \in \mathbb{A}^m. \tag{21}$$

Zároveň $g_i \circ \varphi$ je polynóm v premenných $t_1,\ldots,t_m$ – získali sme ho dosadením $\varphi_1,\ldots,\varphi_n$ za premenné $x_1,\ldots,x_n$. Ak by tento polynóm bol nenulový, potom by definoval nadrovinu v $\mathbb{A}^m$, a podľa Vety 1.15 v Kapitole 2 by potom existoval bod nepatriaci tejto nadrovine. Z (21) tak môžeme usúdiť, že $g_i \circ \varphi$ je nulový polynóm, takže $V(g_1 \circ \varphi,\ldots,g_s \circ \varphi) = \mathbb{A}^m$.

Budeme teraz symbolom $\mathbb{A}^m_{\overline{k}}$ označovať množinu bodov afinného priestoru, ktorých súradnice sú z algebraického uzáveru $\overline{k}$ poľa k, podobne $V_{\overline{k}}(J)$ bude množina bodov z $\mathbb{A}^n_{\overline{k}}$, ktoré vyhovujú polynómom ideálu J (t.j. berieme *všetky* riešenia polynómov, nielen riešenia z poľa k), a tiež $Z_{\overline{k}}$ bude označovať všetky body vyhovujúce polynómom $g_1,\ldots,g_s$, čiže $Z_{\overline{k}}$ je skratka pre $V_{\overline{k}}(g_1,\ldots,g_s)$.

Keďže, ako sme ukázali, $g_i \circ \varphi$ je nulový polynóm, aj po prejdení do algebraického uzáveru $\overline{k}$ máme, $V_{\overline{k}}(g_1 \circ \varphi,\ldots,g_s \circ \varphi) = \mathbb{A}^m_{\overline{k}}$, a tak hodnota g_i $(i = 1,\ldots,s)$ je nula na celej množine $\varphi(\mathbb{A}^m_{\overline{k}})$. Preto platí, že $Z_{\overline{k}} \supset \varphi(\mathbb{A}^m_{\overline{k}})$. Inklúzia sa zachová, keď prejdeme k uzáverom množín, takže máme

$$Z_{\overline{k}} = \overline{Z_{\overline{k}}} \supset \overline{\varphi(\mathbb{A}^m_{\overline{k}})} = V_{\overline{k}}(I \cap \overline{k}[x_1,\ldots,x_n]) = V_{\overline{k}}(I \cap k[x_1,\ldots,x_n]).$$

Predposledná rovnosť vyplýva z Vety 2.4 (Kapitola 3), posledná zas z Vety 2.7 (Kapitola 3) a z faktu, že pri výpočte Gröbnerovej bázy nepotrebujeme rozširovať pôvodné pole. Takže máme inklúziu

$$Z_{\overline{k}} \supset V_{\overline{k}}(I \cap k[x_1,\ldots,x_n]).$$

Inklúzia pre množinu riešení sa zachová, keď sa zaujímame iba o riešenia nad podpoľom k poľa $\overline{k}$, čiže sme ukázali, že

$$Z \supset V(I \cap k[x_1,\ldots,x_n]).$$

□

Dôkaz okrem iného ilustruje fakt, že algebraicky uzavreté pole je „pekné": mnohé tvdenia a postupy v algebraickej geometrii sú jednoduché a priamočiare, kým pracujeme nad algebraicky uzavretým poľom. Akonáhle ale pole nie je algebraicky uzavreté, situácia sa veľmi komplikuje.

Teraz už vieme nielen ukázať, že rovnica v Príklade 1.1 popisuje uzáver obrazu φ, vieme takú rovnicu aj nájsť: I nech je ideál v $k[t,u,x,y,z]$:

$$I = (x-(t+u), y-(t^2+2tu), z-(t^3+3t^2u)),$$

a podľa predchádzajúcej vety potom máme, že

$$\overline{\varphi(\mathbb{A}^2)} = V(I \cap k[x,y,z]).$$

Vypočítame Gröbnerovu bázu vzhľadom na lexikografické usporiadanie, kde $t,u > x,y,z$, a táto bude obsahovať jediný polynóm, v ktorom sa nevyskytujú premenné t,u, čo bude presne polynóm uvedený v príklade.

Príklad 1.3. Nájdeme implicitné vyjadrenie variety, ktorá je parametrizovaná zobrazením $\varphi\colon \mathbb{A}^2 \to \mathbb{A}^3$, $(u,v) \mapsto (x,y,z)$:

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

Graf zobrazenia zodpovedá ideálu $I \in k[u,v,x,y,z]$:

$$I = (x-uv, y-uv^2, z-u^2).$$

Obrazom φ je potom priemet $V(I)$ na posledné tri súradnice, ktorý je popísaný ideálom

$$I \cap k[x,y,z] = (x^4 - y^2 z).$$

Na tomto príklade si môžme všimnúť, že parametrizácia φ nepokrýva celú plochu $V(x^4-y^2z)$: body so súradnicami $(0,b,0)$ vyhovujú rovnici x^4-y^2z, ale ak $b \neq 0$, tak neexistujú také u,v, pre ktoré by platilo, že $(0,b,0) = \varphi(u,v)$.

Pre účely nasledovnej úlohy si zadefinujeme varietu sečníc. Ilustrujme si tento pojem na príklade.

Nech varieta X je zjednotenie dvoch mimobežných priamok v $\mathbb{A}^3$ – zrejme ide o algebraickú varietu: $X = V(y,z) \cup V(x,z-1)$, napríklad. Sečnica je priamka spájajúca dva body variety X. V prípade našej variety je sečnica buď jedna z priamok, ak sme oba body zvolili na tej istej priamke, alebo to bude priečka mimobežiek, ak sme každý z bodov zvolili na inej priamke. Ľahko sa presvedčíme (predstavíme si situáciu), že sečnice pokryjú takmer celý trojrozmerný priestor: nepokryté budú len body, ktoré ležia v rovine obsahujúcej jednu z priamok a rovnobežnej s druhou priamkou. *Varieta sečníc* algebraickej variety X je uzáver množiny bodov ležiacich na všetkých sečniciach variety X. V našom príklade mimobežiek to bude teda celý priestor $\mathbb{A}^3$. (Pozor, neukázali sme to formálne! Len sme si situáciu predstavili a predstave sme uverili, lebo varieta X bola dostatočne jednoduchá.)

Úloha 29. (a) Ukážte, že varieta sečníc vinutej kubiky (Príklad 1.6 v Kapitole 2) je celý priestor $\mathbb{A}^3$. Návod: využite parametrizáciu vinutej kubiky, parametrizujte sečnicu a tak získate parametrizáciu variety sečníc.

(b) Ukážte, že sečnice nepokryjú celý afinný priestor $\mathbb{A}^3$.

1.2. Variety parametrizované racionálnymi funkciami.

Príklad 1.4. Nájdime obraz zobrazenia $\varphi\colon \mathbb{A}^2 \to \mathbb{A}^3$ (t.j. najmenšiu algebraickú varietu obsahujúcu $\varphi(\mathbb{A}^2)$), kde $\varphi\colon (u,v) \mapsto (x,y,z)$ je dané predpisom

$$\begin{aligned} x &= \frac{u^2}{v}, \\ y &= \frac{v^2}{u}, \\ z &= u. \end{aligned}$$

Inšpirovaní predchádzajúcimi výpočtami a Príkladom 1.5 (iii) v Kapitole 2 by sme postupovali nasledovne:

(1) zoberieme ideál $I = (vx - u^2, uy - v^2, z - u) \subset k[u, v, x, y, z]$
(2) nájdeme (pomocou Gröbnerovej bázy) eliminačný ideál $I \cap k[x, y, z] = (x^2yz - z^4)$.

Ľahko sa presvedčíme, že $\varphi(\mathbb{A}^2) \subset V(x^2yz - z^4)$, ale bohužiaľ, $V(x^2yz - z^4)$ nie je najmenšia algebraická varieta, ktorá obsahuje $\varphi(\mathbb{A}^2)$. Platí totiž

$$V(x^2yz - z^4) = V(z(x^2y - z^3)) = V(z) \cup V(x^2y - z^3),$$

a overíme, že

$$\varphi(\mathbb{A}^2) \subset V(x^2y - z^3) \subsetneqq V(x^2yz - z^4).$$

Problém vznikol, lebo $V(I)$ *nie je* grafom zobrazenia φ: varieta $V(I)$ obsahuje body, pre ktoré $u = v = z = 0$, x, y ľubovoľné, avšak zobrazenie φ nie je pre $u = v = 0$ definované.

Všeobecnejšie, majme zobrazenie $\varphi\colon\ \mathbb{A}^m \to \mathbb{A}^n$, $(t_1, \ldots, t_m) \mapsto (x_1, \ldots, x_n)$

$$\begin{aligned} x_1 &= \tfrac{\varphi_1(t_1,\ldots,t_m)}{\psi_1(t_1,\ldots,t_m)} \\ &\vdots \\ x_n &= \tfrac{\varphi_n(t_1,\ldots,t_m)}{\psi_n(t_1,\ldots,t_m)} \end{aligned}$$

kde φ_i, ψ_i sú polynómy. Chceme skonštruovať graf tohto zobrazenia, teda podobnú algebraickú varietu ako v predchádzajúcom príklade, ale potrebujeme z definičného oboru vylúčiť tie $(t_1, \ldots, t_m)$, pre ktoré je $\psi_i(t_1, \ldots, t_m) = 0$ pre nejaké i. Inými slovami, ak urobíme priemet grafu naspať na súradnice zodpovedajúce $t_1, \ldots, t_m$, chceme dostať definičný obor, čiže množinu

$$\mathbb{A}^m \setminus V(\psi_1\psi_2 \ldots \psi_n).$$

Takýto definičný obor už nie je algebraická varieta, je to však priemet algebraickej variety, konkrétne nadplochy v $\mathbb{A}^{m+1}$, ktorá je definovaná polynómom $1 - y\psi_1\psi_2 \ldots \psi_n \in k[y, t_1, \ldots, t_m]$. Graf zobrazenia φ je tak bude pre nás varieta $V(I) \in \mathbb{A}^{m+n+1}$, kde

$$I = (1 - y\psi_1\psi_2 \ldots \psi_n, \psi_1x_1 - \varphi_1, \ldots, \psi_nx_n - \varphi_n).$$

Body $V(I)$ sú tvaru

$$(\frac{1}{\psi_1\psi_2 \ldots \psi_n}, t_1, \ldots, t_m, \frac{\varphi_1}{\psi_1}, \ldots, \frac{\varphi_n}{\psi_n}).$$

Každému bodu $(t_1, \ldots, t_m) \in \mathbb{A}^m \setminus V(\psi_1\psi_2 \ldots \psi_n)$ tak zodpovedá práve jeden bod na $V(I)$, a každému bodu na $V(I)$ zodpovedá práve jeden bod v definičnom obore φ.

Obraz φ v našom príklade teda nájdeme takto: ideál popisujúci graf zobrazenia je

$$I = (1 - wuv, vx - u^2, uy - v^2, z - u) \subset k[w, u, v, x, y, z],$$

obraz φ je potom priemet grafu na posledné tri súradnice:

$$\overline{\varphi(\mathbb{A}^2)} = V(I \cap k[x, y, z]) = V(x^2y - z^3).$$

2. Hilbertova veta o koreňoch (Nullstellensatz)

2.1. Tvrdenie vety. V tejto časti budeme bližšie skúmať súvis medzi ideálmi a algebraickými varietami.

Príklad 2.1. V okruhu $k[x,y]$ majme dva ideály:

$$I_1 = (x^2 - y^2), \quad I_2 = ((x-y)^2(x+y)).$$

Tieto ideály sú rôzne (presnejšie vidíme, že $I_2 \subsetneq I_1$), avšak $V(I_1) = V(I_2)$ - ide o zjednotenie dvoch priamok.

Definícia 2.2. Nech R je ľubovoľný okruh a $I \subset R$ je ideál. *Radikál ideálu* I je

$$\sqrt{I} = \{f \in R \mid f^d \in I \text{ pre nejaké } d \in \mathbb{N}\}$$

Ak $I = \sqrt{I}$, potom I nazývame *radikálový ideál* (skrátene aj *radikál*).

Nasledujúce tvrdenie popisuje niektoré základné vlastnosti radikálov.

Tvrdenie 2.3. (i) $\sqrt{I} \supset I$,
(ii) $\sqrt{I}$ *je ideál.*
(iii) $\sqrt{\sqrt{I}} = \sqrt{I}$,

Dôkaz. (i) Ak $f \in I$, teda $f^1 \in I$ a tak máme, že $f \in \sqrt{I}$.

(ii) Zrejme $\sqrt{I}$ je neprázdna množina, lebo $\sqrt{I} \supset I$. Nech teraz $f \in \sqrt{I}$ a $r \in R$, takže $f^d \in I$ pre nejaké $d \in \mathbb{N}$. Uvažujme prvok rf. Platí, že $(rf)^d = r^d f^d \in I$, a teda $rf \in \sqrt{I}$. Nakoniec nech $f, g \in \sqrt{I}$, čiže $f^d \in I$ a $g^e \in I$ pre nejaké $d, e \in \mathbb{N}$. Pre súčet $f+g$ potom máme, $(f+g)^{d+e-1} \in I$ – po roznásobení sa totiž v každom sčítanci bude buď f alebo g nachádzať v dostatočne veľkej mocnine. Ukázali sme tak, že $f+g \in \sqrt{I}$.

(iii) Inkúzia „$\supset$" vyplýva z predchádzajúcich dvoch vlastností. Pre druhú inklúziu, nech $f \in \sqrt{\sqrt{I}}$. Takže existuje $d \in \mathbb{N}$ také, že $f^d \in \sqrt{I}$, čo ďalej znamená, že existuje $d' \in \mathbb{N}$ také, že $(f^d)^{d'} = f^{dd'} \in I$, a teda $f \in \sqrt{I}$. □

Príklad 2.4. Ak uvažujeme len hlavné ideály, dá sa radikál ideálu nájsť pomerne ľahko. Uvedieme si tri príklady, pri jednom si aj urobíme dôkladný dôkaz, že nájdený ideál je naozaj radikálom daného ideálu (skúste si podobné dôkazy urobiť aj v ostatných prípadoch!):

(a) Radikál ideálu $I = (x^3) \subset k[x]$ je $\sqrt{I} = (x)$.
(b) Radikál ideálu $I = ((x-1)^2(x+1)^3) \subset k[x]$ je $\sqrt{I} = ((x-1)(x+1))$: pre $(x-1)(x+1)$ platí, že $((x-1)(x+1))^3 \in I$, a teda $((x-1)(x+1)) \subset \sqrt{I}$. Nech teraz $f \in \sqrt{I}$, čiže existuje $d \in \mathbb{N}$ také, že $f^d \in I$, teda $f^d = (x-1)^2(x+1)^3 g$. Máme tak, že $(x-1) \mid f^d$, a keďže $(x-1)$ je ireducibilný, tak $(x-1) \mid f$. Podobne ukážeme, že $(x+1) \mid f$, a teda $f = (x-1)(x+1)h$, čiže $f \in ((x-1)(x+1))$.
(c) Radikál ideálu $I = ((x+y^2+3)^3(2x-y)^5) \subset k[x,y]$ je $\sqrt{I} = ((x+y^2+3)(2x-y))$.

Úloha 30. Dokážte, že radikál ideálu $I = (x^2, y) \subset k[x,y]$ je ideál $\sqrt{I} = (x,y)$.

Príklad 2.5. Radikál ideálu $I = (x^2+y^2, x^2-y^2) \subset k[x,y]$ je $\sqrt{I} = (x,y)$ (skúste si to dokázať!) – je to ešte príklad ideálu s ľahko nájditeľným radikálom. Vo všeobecnosti nájsť radikál ideálu je však ťažká úloha. Nech napríklad $I = (x^4 - y^2, x^3 - y^2)$. Jeho radikál nájdeme s pomocou Singularu: $\sqrt{I} = (-x + y^2, xy - y, x^2 - x)$. Algoritmami pre nájdenie radikálu sa nebudeme zaoberať.

Tvrdenie 2.6. *Nech* $I \subset k[x_1, \ldots, x_n]$ *je ideál. Potom* $\sqrt{I} \subseteq I(V(I))$.

Dôkaz. Nech $f \in \sqrt{I}$, čiže $f^d \in I$ pre nejaké $d \in \mathbb{N}$. Odtiaľ máme, že $(f^d) \subset I$. Ďalej polynómy f a f^d zrejme určujú tú istú nadplochu v $\mathbb{A}^n$ takže pre variety platí

$$V(f) = V(f^d) \supset V(I).$$

Preto $f(a) = 0$ pre všetky $a \in V(f)$ a teda $f \in I(V(I))$. □

VETA 2.7 (**Hilbertova veta o koreňoch, Nullstellensatz, silná verzia**). *Ak pole k je algebraicky uzavreté, potom pre ideál $I \subset k[x_1, \ldots, x_n]$ platí*

$$I(V(I)) = \sqrt{I}$$

Nullstellensatz dokazovať nebudeme. Namiesto toho si o chvilu uvedieme ešte inú verziu tejto vety a ukážeme, že obe verzie sú ekvivalentné.

DÔSLEDOK. *Nad algebraicky uzavretým poľom platí, že*

$$V(I) = V(J) \quad \text{práve vtedy, keď} \quad \sqrt{I} = \sqrt{J}.$$

Máme teda bijekciu medzi algebraickými varietami a radikálovými ideálmi.

Dôkaz. Nech $V(I) = V(J)$, potom $I(V(I)) = I(V(J))$ a z Nullstellensatz dostávame, že $\sqrt{I} = \sqrt{J}$.

Opačne, nech $\sqrt{I} = \sqrt{J}$, odkiaľ máme $V(\sqrt{I}) = V(\sqrt{J})$. Z Nullstellensatz potom $V(I(V(I))) = V(I(V(J)))$, kde ľavá strana je rovná $V(I)$ a pravá $V(J)$ (Tvrdenie 2.11 (iii) v Kapitole 2). □

PRÍKLAD 2.8. Predpoklad, že pole k musí byť algebraicky uzavreté, je kľúčový. Nech napríklad $k = \mathbb{R}$ a uvažujme dva ideály v $\mathbb{R}[x, y]$: $I = (x, y)$, $J = (x^2 + y^2)$. Tieto ideály sú rôzne, a obidva sú radikálovými ideálmi. Avšak $V(I) = V(J)$ – ide o jednobodovú varietu.

VETA 2.9 (**Nullstellensatz, slabá verzia**). *Ak pole k je algebraicky uzavreté, potom pre ideál $I \subset k[x_1, \ldots, x_n]$ platí*

$$V(I) = \emptyset \quad \text{práve vtedy keď} \quad 1 \in I \ (\text{t.j. } I = k[x_1, \ldots, x_n]).$$

POZNÁMKA 2.10. Implikácia $\Leftarrow$ je triviálna, tvrdenie Nullstellensatz spočíva v implikácii $\Rightarrow$.

PRÍKLAD 2.11. Analogicky so silnou verziou, predpoklad algebraickej uzavretosti je podstatný: nech $I = (x^2 + y^2 + 1) \subset \mathbb{R}[x, y]$. Zrejme $V(I) = \emptyset$, hoci $1 \notin I$.

Všimnime si, že slabá verzia Nullstellensatz akoby bola zúžením silnej verzie na jeden konkrétny ideál a jednu konkrétnu algebraickú varietu. Ukážeme už spomínané

TVRDENIE 2.12. *Obe tvrdenia Nullstellensatz (silná a slabá verzia) sú ekvivalentné.*

Dôkaz. Nech platí tvrdenie silnej verzie. Podľa Poznámky 2.10 potrebujeme v slabej verzii ukázať implikáciu $\Rightarrow$.

Nech $V(I) = \emptyset$, odtiaľ dostávame, že $1 \in I(V(I))$. Zo silnej verzie Nullstellensatz môžme usúdiť, že $1 \in \sqrt{I}$, teda $1^d \in I$ pre nejaké $d \in \mathbb{N}$, čo však znamená, že $1 \in I$.

Opačne, nech teraz platí tvrdenie slabej verzie Nullstellensatz. Majme $I = (f_1, \ldots, f_k) \subset k[x_1, \ldots, x_n]$. Prepokladajme, že nejaký polynóm f leží v $I(V(I))$, chceme ukázať, že $f \in \sqrt{I}$, čiže, že existuje $d \in \mathbb{N}$ také, že $f^d \in I$.

Uvažujme ideál $(f_1, \ldots, f_k, 1 - yf) \subset k[x_1, \ldots, x_n, y]$ a skúmajme zodpovedajúcu varietu $V(f_1, \ldots, f_k, 1 - yf)$. Nech $(a_1, \ldots, a_{n+1})$ je nejaký bod $\mathbb{A}^{n+1}$, skúsme zistiť, kedy tento bod patrí našej variete:

- ak $a_1, \ldots, a_n$ sú také, že $f_1(a_1, \ldots, a_n) = \cdots = f_k(a_1, \ldots, a_n) = 0$, potom aj $f(a_1, \ldots, a_n) = 0$ (lebo $f \in I(V(I))$), a následne $1 - a_{n+1}f(a_1, \ldots, a_n) = 1 \neq 0$. Bod $(a_1, \ldots, a_{n+1})$ nevyhovuje poslednej rovnici a preto nepatrí variete $V(f_1, \ldots, f_k, 1 - yf)$.
- ak $a_1, \ldots, a_n$ sú také, že $f_i(a_1, \ldots, a_n) \neq 0$ pre nejaké i, potom toto je už rovnica, ktorej bod $(a_1, \ldots, a_{n+1})$ nevyhovuje, a teda nepatrí variete $V(f_1, \ldots, f_k, 1 - yf)$.

Zistili sme, že $V(f_1, \ldots, f_k, 1 - yf) = \emptyset$. Zo slabej verzie Nullstellnsatz potom vyplýva, že $1 \in (f_1, \ldots, f_k, 1 - yf)$, takže existujú polynómy $p_1, \ldots, p_k, p \in k[x_1, \ldots, x_k, y]$ také, že

$$1 = p_1 f_1 + \cdots + p_k f_k + p(1 - yf).$$

Nahraďme v tejto rovnosti premennú y racionálnym výrazom $1/f$. Dostaneme tak rovnosť racionálnych výrazov, pričom v menovateľoch budú len mocniny f:

$$\begin{aligned} 1 &= p_1(x_1,\dots,x_n,\frac{1}{f})f_1+\cdots+p_k(x_1,\dots,x_n,\frac{1}{f})f_k+p(x_1,\dots,x_n,\frac{1}{f})(1-\frac{1}{f}f)\\ &= p_1(x_1,\dots,x_n,\frac{1}{f})f_1+\cdots+p_k(x_1,\dots,x_n,\frac{1}{f})f_k \end{aligned}$$

Po vynásobení rovnosti dostatočne vysokou mocninou f tak dostávame rovnosť polynómov:

$$f^d = q_1f_1+\dots q_kf_k,$$

teda $f^d\in I$, čo sme chceli dokázať. □

2.2. Testovanie rovnosti radikálov. Ako sme už spomenuli, nájsť radikál ideálu nie je jednoduchá úloha. Ukážeme si, že napriek tomu vieme zistiť, či daný polynóm leží v radikáli daného ideálu, a následne vieme porovnať radikály dvoch daných ideálov. Nad algebraicky uzavretým poľom tak budeme mať algoritmicky úplne vyriešený problém porovnania algebraických variet.

TVRDENIE 2.13. *Nech $I=(f_1,\dots,f_k)\subset k[x_1,\dots,x_n]$ je ideál. (Pole k nemusí byť algebraicky uzavreté.) Potom*

$$f\in\sqrt{I} \quad \textit{práve vtedy, keď} \quad (f_1,\dots,f_k,1-yf)=k[x_1,\dots,x_n,y].$$

Dôkaz. Nech $1\in(f_1,\dots,f_k,1-yf)$. Potom úplne takým istým postupom ako v poslednej časti dôkazu 2.12 (nahradenie premennej y výrazom $1/f$) zistíme, že $f^d\in I$ pre nejaké $d\in\mathbb{N}$.

Nech teraz naopak $f^d\in I$ pre nejaké $d\in\mathbb{N}$. Takže máme polynómy $p_1,\dots,p_k\in k[x_1,\dots,x_n]$, že

$$\begin{aligned} f^d &= p_1f_1+\cdots+p_kf_k \qquad |\cdot y^d\\ f^dy^d &= p_1f_1y^d+\cdots+p_kf_ky^d\\ 1 &= p_1f_1y^d+\cdots+p_kf_ky^d+(1-f^dy^d)\\ 1 &= p_1f_1y^d+\cdots+p_kf_ky^d+(1-fy)(1+fy+f^2y^2+\cdots+f^{d-1}y^{d-1}), \end{aligned}$$

čiže $1\in(f_1,\dots,f_k,1-yf)$, čo presne znamená, že $(f_1,\dots,f_k,1-yf)=k[x_1,\dots,x_n,y]$. □

Než si uvedieme algoritmus pre testovanie, či daný polynóm patrí radikálu daného ideálu, všimnime si, že ak $1\in I$, tak 1 sa určite nachádza v Gröbnerovej báze ideálu I. Naozaj, vedúce členy polynómov Gröbnerovej bázy generujú ideál vedúcich členov. Ak $1\in I$, tak Gröbnerova báza musí obsahovať polynóm, ktorého vedúci člen je (až na násobok nenulovou konštantou) rovný 1, čiže musí obsahovať priamo polynóm 1.

VSTUP: ideál $(f_1,\dots,f_k)\subset k[x_1,\dots,x_n]$ a poynóm $f\in k[x_1,\dots,x_n]$.
VÝSTUP: Rozhodnutie, či $f\in\sqrt{(f_1,\dots,f_k)}$.
ALGORIMUS:

- Nájdi Gröbnerovu bázu G ideálu $(f_1,\dots,f_k,1-yf)\subset k[x_1,\dots,x_n,y]$ (pri ľubovoľnom usporiadaní).
- $f\in k[x_1,\dots,x_n]$ práve vtedy, keď $1\in G$.

Pre porovnanie radikálov dvoch daných ideálov I a J potrebujeme overiť, že $I\subset\sqrt{J}$ a $J\subset\sqrt{I}$. Naozaj, ak $I\subset\sqrt{J}$, potom platí $\sqrt{I}\subset\sqrt{\sqrt{J}}=\sqrt{J}$ a naopak, inklúzia $J\subset\sqrt{I}$ implikuje inklúziu $\sqrt{J}\subset\sqrt{I}$.

VSTUP: ideály $I=(f_1,\dots,f_k), J=(g_1,\dots,g_l)\subset k[x_1,\dots,x_n]$.
VÝSTUP: Rozhodnutie, či $\sqrt{I}=\sqrt{J}$.
ALGORIMUS:

- Pre každý generátor f_i ideálu I zisti, či $f_i \in \sqrt{J}$ (predchádzajúci algoritmus).
- Pre každý generátor g_j ideálu J zisti, či $g_j \in \sqrt{I}$.
- $\sqrt{I} = \sqrt{J}$ práve vtedy, keď všetky testy prešli s pozitívnym výsledkom.

2.3. Dôkaz vety o projekcii. Mali by sme si ešte dokázať Vetu 2.4 z Kapitoly 3 Vo Vete 2.3 sme predtým ukázali, že ak X je algebraická varieta a $I = I(X)$, potom

$$\overline{\pi(X)} = V(I \cap k[x_{i+1}, \ldots, x_n]),$$

pre π je projekcia „zabúdania" prvých i súradníc. Potrebujeme ukázať, že ak pole k je algebraicky uzavreté, tak uvedená rovnosť platí pre *ľubovoľný* ideál popisujúci algebraickú varietu X.

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

$$\sqrt{I} \cap k[x_{i+1}, \ldots, x_n] = \sqrt{I \cap k[x_{i+1}, \ldots, x_n]}.$$

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

Takže môžme písať

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

kde prvá rovnosť vyplýva z dokázanej Vety 2.3 (Kapitola 3) o projekcii, štvrtá rovnosť z práve ukázanej rovnosti ideálov a tretia a piata rovnosť z Nullstellensatz, resp. tvrdenia, ktoré sme si uviedli ako jej dôsledok.

3. Projektívne zúplnenie algebraických variet

3.1. Projektívny priestor. S projektívnym priestorom ste sa už stretli, preto táto podkapitola má skôr prehľadový charakter a slúži najmä na zavedenie terminológie.

Formálne sa n-rozmerný projektívny priestor definuje ako množina priamok v $\mathbb{A}^{n+1}$, ktoré prechádzajú bodom $(0,\dots,0)$. Presnejšie, nech $\sim$ je nasledovná relácia na $\mathbb{A}^{n+1}(k)\setminus\{(0,\dots,0)\}$:

$$(a_0,\dots,a_n)\sim(a_0',\dots,a_n') \quad \text{ak} \quad (a_0',\dots,a_n')=(\lambda a_0,\dots,\lambda a_n) \quad \text{pre nejaké} \quad \lambda\in k\ (\lambda\neq 0).$$

Ľahko sa overí, že $\sim$ je reláciou ekvivalencie, a teda rozkladá množinu $\mathbb{A}^{n+1}(k)\setminus\{(0,\dots,0)\}$ na triedy ekvivalencie. Body *projektívneho priestoru* sú potom jednotlivé triedy:

$$\mathbb{P}^n(k)=(\mathbb{A}^{n+1}(k)\setminus\{(0,\dots,0)\})/\sim .$$

Každý bod v $\mathbb{P}^n$ je takto reprezentovaný viacerými $(n+1)$-ticami čísiel z k: $(a_0,\dots,a_n)$ a $(\lambda a_0,\dots,\lambda a_n)$ $(\lambda\neq 0)$ určujú ten istý bod v $\mathbb{P}^n$. Tieto $(n+1)$-tice nazývame *homogénnymi súradnicami* bodu v $\mathbb{P}^n$. Pri zápise bodu pomocou jeho súradníc používame dvojbodku: $(a_0:\dots:a_n)$. Z definície vyplýva, že

$$(a_0:\dots:a_n)\in\mathbb{P}^n \quad \text{práve vtedy, keď} \quad a_i\neq 0 \quad \text{pre nejaké } i.$$

Iný prístup k projektívnemu priestoru je, predstaviť si ho ako rozšírenie afinného priestoru rovnakej dimenzie. Priestor $\mathbb{A}^n$ je tak podmnožinou priestoru $\mathbb{P}^n$. Body v $\mathbb{P}^n\setminus\mathbb{A}^n$ sa nazývajú *nevlastnými bodmi* a predstavujeme si ich ako body „v nekonečne". Každý takýto nevlastný bod zodpovedá všetkým navzájom rovnobežným priamkam, teda akoby sme k $\mathbb{A}^n$ pridali priesečníky rovnobežiek.

Overíme, že obe uvedené konštrukcie vedú k rovnakému projektívnemu priestoru.
Nech $(a_1,\dots,a_n)\in\mathbb{A}^n$. Priestor $\mathbb{A}^n$ uvažujme ako vložený do $\mathbb{P}^n$, takže bodu $(a_1,\dots,a_n)$ priradíme homogénne súradnice, napríklad $(1:a_1:\dots:a_n)$. Týmto spôsobom skonštuujeme všetky také body $\mathbb{P}^n$, ktorých prvá homogénna súradnica je nenulová. Body s prvou súradnicou nulovou sú nevlastné, pričom bod $(0:a_1:\dots:a_n)$ zodpovedá všetkým priamkam, ktorých smerový vektor je $(a_1,\dots,a_n)$. Naopak, vezmime bod $(a_0:\dots:a_n)\in\mathbb{P}^n$ taký, že $a_0\neq 0$. K tomuto bodu projektívneho priestoru vieme priradiť bod v $\mathbb{A}^n$: platí, že

$$(a_0:\dots:a_n)=\left(1:\frac{a_1}{a_0}:\dots:\frac{a_n}{a_0}\right),$$

takže dostávame bod $(\frac{a_1}{a_0},\dots,\frac{a_n}{a_0})\in\mathbb{A}^n$. S afinným priestorom $\mathbb{A}^n$ sme týmto postupom v $\mathbb{P}^n$ stotožnili množinu

$$U_0=\{(a_0:\dots:a_n)\in\mathbb{P}^n\mid a_0\neq 0\}.$$

Vynechali sme nevlastné body

$$\mathbb{P}^n\setminus U_0=\{(a_0:\dots:a_n)\in\mathbb{P}^n\mid a_0=0\},$$

Množina U_0 nevlastných bodov nie je v $\mathbb{P}^n$ nijak špeciálna. Analogicky definujeme množiny $U_1,\dots,U_n$:

$$U_i=\{(a_0:\dots:a_n)\in\mathbb{P}^n\mid a_i\neq 0\}.$$

Každá z týchto množín sa dá stotožniť s n-rozmerným afinným priestorom, tak ako sme to urobili v prípade U_0:

$$\varphi_i\colon\ \mathbb{A}^n\to U_i,\quad (a_1,\dots,a_n)\mapsto(a_1:\dots:a_i:1:a_{i+1}:\dots:a_n)$$
$$\varphi^{-1}\colon\ U_i\to\mathbb{A}^n,\quad (a_0:\dots:a_n)\mapsto\left(\frac{a_0}{a_i}:\dots:\frac{a_{i-1}}{a_i}:\frac{a_{i+1}}{a_i}:\dots:\frac{a_n}{a_i}\right).$$

Množiny $U_0,\dots,U_n$ sa nazývajú *afinnými mapami* a všetky spolu pokrývajú celý afinný priestor:

$$\mathbb{P}^n=U_0\cup U_1\cup\dots\cup U_n.$$

Inklúzia „$\supseteq$" je zrejmá, keďže $U_i\subset\mathbb{P}^n$, opačná inklúzia platí, lebo ak $(a_0:\dots:a_n)\in\mathbb{P}^n$, potom existuje $i\in\{0,\dots,n\}$ také, že $a_i\neq 0$, a teda $(a_0:\dots:a_n)\in U_i$.

3.2. Pojektívne algebraické variety.

PRÍKLAD 3.1. Algebraické variety v projektívnom priestore chceme definovať podobne ako v afinnom prípade pomocou polynómov. Uvažujme napríklad polynóm $f = z_1z_2 - 1 \in k[z_0, z_1, z_2]$ a skúsme zistiť, či takýto polynóm popisuje nejakú množinu v projektívnej rovine

$$\mathbb{P}^2(k) = \{(a_0 : a_1 : a_2) \mid a_i \in k,\ \exists i\colon\ a_i \neq 0\}.$$

Nech $p = (1 : 1 : 1)$. Potom platí, že $f(1, 1, 1) = 1 \cdot 1 - 1 = 0$ a teda bod p by sme mohli zaradiť medzi body variety. Avšak pre ten istý bod p máme tiež $p = (2 : 2 : 2)$ a tentokrát $f(2, 2, 2) = 2 \cdot 2 - 1 \neq 0$. Množina $\{(a_0 : a_1 : a_2) \in \mathbb{P}^2 \mid f(a_0, a_1, a_2) = 0\}$ nie je korektne definovaná.

Použijeme premennú z_0 na homogenizáciu pôvodného polynómu: nech

$$f^h = z_1z_2 - z_0^2.$$

Potom bod $p = (1 : 1 : 1)$ spĺňa rovnosť $f^h(p) = 0$ bez ohľadu na to, ktoré súradnice bodu p dosadíme za premenné v polynóme f^h. Všeobecnejšie, nech pre $q = (q_0 : q_1 : q_2) \in \mathbb{P}^2$ platí, že $f^h(q_0, q_1, q_2) = 0$. Ak $(q_0' : q_1' : q_3')$ sú iné súradnice toho istého bodu q, potom $(q_0' : q_1' : q_3') = (\lambda q_0 : \lambda q_1 : \lambda q_2)$ pre nejaké λ. Po dosadení týchto súradníc do zhomogenizovaného polynómu f^h dostávame

$$f^h(\lambda q_0, \lambda q_1, \lambda q_2) = \lambda q_1 \lambda q_2 - (\lambda q_0)^2 = \lambda^2(q_1q_2 - q_0^2) = \lambda^2 f^h(q_0, q_1, q_2) = 0.$$

Množina

$$\{(a_0 : a_1 : a_2) \in \mathbb{P}^2 \mid f^h(a_0, a_1, a_2) = 0\}$$

je tak korektne definovaná.

DEFINÍCIA 3.2. $f \in k[z_0, \ldots, z_n]$ sa nazýva *homogénny polynóm (forma) stupňa* d, ak všetky jeho členy majú stupeň d:

$$f = \sum_{i_0+\cdots+i_n=d} c_{i_0,\ldots,i_n} z_0^{i_0} \ldots z_n^{i_n}, \quad c_{i_0,\ldots,i_n} \in k. \tag{22}$$

LEMA 3.3. *Nech $f \in k[z_0, \ldots, z_n]$ je homogénny polynóm. Ak $f(a_0, \ldots, a_n) = 0$, potom aj $f(\lambda a_0, \ldots, \lambda a_n) = 0$ pre ľubovoľné $\lambda \in k$.*

Dôkaz. Zapíšme f ako v (22). Nech

$$f(a_0, \ldots, a_n) = \sum c_{i_0,\ldots,i_n} a_0^{i_0} \ldots a_n^{i_n} = 0.$$

Nech $\lambda \in k$. Potom platí

$$\begin{aligned} f(\lambda a_0, \ldots, \lambda a_n) &= \sum c_{i_0,\ldots,i_n} (\lambda a_0)^{i_0} \ldots (\lambda a_n)^{i_n} = \sum \lambda^d c_{i_0,\ldots,i_n} a_0^{i_0} \ldots a_n^{i_n} \\ &= \lambda^d \sum c_{i_0,\ldots,i_n} a_0^{i_0} \ldots a_n^{i_n} = \lambda^d f(a_0, \ldots, a_n) = 0. \end{aligned}$$

□

DEFINÍCIA 3.4. Ideál $I \subset k[z_0, \ldots, z_n]$ sa nazýva *homogénny ideál*, ak $I = (f_1, \ldots, f_k)$, kde $f_i \in k[z_0, \ldots, z_n]$ sú homogénne polynómy (nie nutne rovnakého stupňa).

TVRDENIE 3.5. *Nech $I \subset k[z_0, \ldots, z_n]$ je homogénny ideál, nech $g \in I$. Zapíšme*

$$g = g_0 + g_1 + \cdots + g_d,$$

kde g_i je forma stupňa i. Potom $g_i \in I$ pre všetky $i = 0, \ldots, d$.

Dôkaz. (Podobný dôkazu analogického tvrdenia pre monomiálne ideály.) Ak $g \in I$, potom

$$g = h_1f_1 + \cdots + h_kf_k$$

pre nejaké $h_i \in k[z_0, \ldots, z_n]$. Zapíšme každý z polynómov h_i ako súčet foriem:

$$\begin{aligned} g &= (h_{10} + \cdots + h_{1d_1})f_1 + \cdots + (h_{k0} + \cdots + h_{kd_k})f_k \\ &= h_{10}f_1 + \cdots + h_{1d_1}f_1 + \cdots + h_{k0}f_k + \cdots + h_{kd_k}f_k, \end{aligned}$$

kde h_{ij} je forma supňa j. V poslednom riadku je každý zo sčítancov $h_{ij}f_i$ homogénnym polynómom. Každé g_i na pravej strane je tak kombináciou polynómov $f_1, \dots, f_k$, a teda $g_i \in I$. □

DEFINÍCIA 3.6. Nech $I \subset k[z_0, \dots, z_n]$ je homogénny ideál. Množina

$$V(I) = \{(a_0 : \cdots : a_n) \in \mathbb{P}^n \mid f(a_0, \dots, a_n) = 0 \ \forall f \in I\}$$

sa nazýva *projektívna algebraická varieta*.

Z Lemmy 3.3 a Tvrdenia 3.5 vyplýva, že projektívna varieta je korektne definovaná.

PRÍKLAD 3.7. Homogénny lineárny polynóm $f = c_0z_0 + \cdots + c_nz_n \in k[z_0, \dots, z_n]$ definuje *nadrovinu* v $\mathbb{P}^n$. Napríklad v $\mathbb{P}^2$ je množina $V(z_0) = \{(a_o : a_1 : a_2) \in \mathbb{P}^2 \mid a_0 = 0\} = \{(0 : a_1 : a_2) \in \mathbb{P}^2\}$ priamkou. Ak si predstavíme projektívnu rovinu ako rozšírenie afinnej roviny, kde pôvodnú afinnú rovinu stotožníme s mapou U_0, potom $V(z_0)$ je presne množina nevlastných bodov. Podobne v $\mathbb{P}^3$ je množina $V(z_0)$ rovinou obsahujúcou presne všetky nevlastné body.

Ak $f_1, \dots, f_k \in k[z_0, \dots, z_n]$ sú lineárne formy, potom $V(f_1, \dots, f_k)$ je *lineárna varieta* v $\mathbb{P}^n$.

PRÍKLAD 3.8. Podobne ako v afinnom priestore, množinu bodov v $\mathbb{P}^n$ definovanú hlavným ideálom, t.j. množinu $V(f) \subset \mathbb{P}^n$, kde $f \in k[z_0, \dots, z_n]$ je forma, nazývame *nadplochou*.

PRÍKLAD 3.9. Pre konkrétnejší príklad uvažujme

$$V(f) \subset \mathbb{P}^2, \quad \text{kde} \quad f = z_1^2 + z_2^2 - z_0^2 \in k[z_0, z_1, z_2].$$

Predstavme si túto projektívnu rovinu ako rozšírenie afinnej, kde pôvodnú afinnú rovinu stotožníme s mapou U_0. Body variety $V(f)$, ktoré sa nachádzajú v tejto afinnej rovine, sú

$$V(f) \cap U_0 = \{(a_0 : a_1 : a_2) \mid a_1^2 + a_2^2 - a_0^2 \wedge a_0 \neq 0\}.$$

Ak bod $(a_0 : a_1 : a_2)$ patrí U_0, potom tento bod má aj súradnice $(1 : \frac{a_1}{a_0} : \frac{a_2}{a_0})$, a teda $(\frac{a_1}{a_0}, \frac{a_2}{a_0})$ boli afinné súradnice tohoto bodu, keď sme afinnú rovinu vkladali do projektívnej.

Ďalšia podmienka $((a_0 : a_1 : a_2) \in V(f))$ znamená, že

$$a_1^2 + a_2^2 - a_0^2 = 0, \quad \text{teda} \quad \left(\frac{a_1}{a_0}\right)^2 + \left(\frac{a_2}{a_0}\right)^2 - 1 = 0.$$

Vidíme, že afinné súradnice bodu $(a_0 : a_1 : a_2) \in V(f) \cap U_0$ spĺňajú rovnicu

$$x_1^2 + x_2^2 - 1 = 0,$$

množina $V(f) \cap U_0$ je tak jednotková kružnica. Body projektívnej variety $V(f)$, ktoré sme vynechali, keď sme sa zúžili na U_0, sú body $V(f) \cap V(z_0)$, čiže body $(0 : 1 : i)$ a $(0 : 1 : -i)$.

Všimnime si v predchádzajúcom príklade, že prienik projektívnej variety s afinnou mapou U_0 bola afinná varieta, ktorej rovnicu môžme dostať tak, že v rovnici projektívnej variety za z_0 dosadíme jednotku, a namiesto z_i napíšeme x_i pre $i \geq 1$. Toto pozorovanie teraz zovšeobecníme:

TVRDENIE 3.10 (**o dehomogenizácii**). *Nech $X = V(f_1, \dots, f_k) \subset \mathbb{P}^n$ je projektívna algebraická varieta. Potom $Y = X \cap U_0$ je afinná algebraická varieta $V(g_1, \dots, g_k) \subset \mathbb{A}^n$, kde*

$$g_i(x_1, \dots, x_n) = f_i(1, x_1, \dots, x_n).$$

Dôkaz. Nájdeme invertibilné zobrazenie medzi $X \cap U_0$ a $V(g_1, \dots, g_k) \subset \mathbb{A}^n$.

Pri konštrukcii projektívneho priestoru sme si uviedli bijekciu $\varphi_0 \colon \mathbb{A}^n \to U_0$ a $\varphi_0^{-1} \colon U_0 \to \mathbb{A}^n$. Zobrazenie φ_0^{-1} zobrazilo bod $(a_0 : \cdots : a_n)$ na bod $(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0})$. Ak $f_i(a_0, a_1 \dots, a_n) = 0$, potom aj $f_i(1, \frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}) = 0$, kde ľavá strana je presne $g_i(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0})$. Čiže φ_0^{-1} zobrazí bod z $X \cap U_0$ na bod z $V(g_1, \dots, g_k) \subset \mathbb{A}^n$.

Opačne, zoberme teraz zobrazenie $\varphi_0 \colon (a_1, \dots, a_n) \mapsto (1 : a_1 : \cdots : a_n)$ Ak $g_i(a_1, \dots, a_n) = 0$, tak $f_i(1, a_1, \dots, a_n) = 0$, čiže bod $\varphi_0(a_1, \dots, a_n)$ spĺňa rovnice pre X a tak vidíme, že φ_0 zobrazuje body $V(g_1, \dots, g_k) \subset \mathbb{A}^n$ na body z $X \cap U_0$. □

Premenná z_0 nie je nijak významná medzi ostatnými premennými, celá predchádzajúca veta aj s dôkazom ostáva v platnosti, aj nahradíme premennú z_0 niektorou inou premennou z_i. Takže máme

DÔSLEDOK. *Ak $X \subset \mathbb{P}^n$ je projektívna varieta, potom $X \cap U_i$ je afinná algebraická varieta. Jej rovnice dostaneme dehomogenizáciou rovníc pre X vzhľadom na premennú z_i (t.j. z_i nahradíme jednotkou a ostatné premenné premenujeme).*

PRÍKLAD 3.11. Vráťme sa k príkladu projektívnej algebraickej variety

$$X = V(f) \subset \mathbb{P}^2, \quad \text{kde} \quad f = z_1^2 + z_2^2 - z_0^2.$$

Prienik $X \cap U_0$ bola jednotková kružnica. Zvoľme si teraz priamku $z_1 = 0$ ako nevlastnú, teda afinnú rovinu stotožníme s afinnou mapou U_1. Rovnica afinnej variety $X \cap U_1$ sa dá nájsť ako dehomogenizácia polynómu f vzhľadom na premennú z_1:

$$V(f) \cap U_1 = V(g), \quad \text{kde} \quad g = 1 + y_2^2 - y_0^2 \in k[y_0, y_2].$$

(Afinná premenná y_0 zodpovedá podielu z_0/z_1, premenná y_2 zas podielu z_2/z_1.) V afinnej mape U_1 teda varieta X „vyzerá" ako hyperbola. Ukazuje sa, že v projektívnej rovine nemá veľký zmysel rozlišovať jednotlivé regulárne kužeľosečky.

Zatiaľ sme si ukázali, že zúženie projektívnej variety na afinný priestor je afinná algebraická varieta. Ostáva nám ešte opačná konštrukcia – či každú afinnú algebraickú varietu môžme dostať ako zúženie projektívnej variety na afinný priestor. Inými slovami, ako môžme afinnú varietu rozšíriť na projektívnu.

PRÍKLAD 3.12. Majme $f = x_2 - x_1^3 \in k[x_1, x_2]$, takže $V(f)$ je krivka v afinnej rovine $\mathbb{A}^2$ (kubická parabola). Nájdime projektívnu varietu v $\mathbb{P}^2$, ktorej zúženie na afinnú rovinu bude $V(f)$. Takáto varieta existuje, a dokonca nie jediná:

$$X_1 = V(z_0^2 z_2 - z_1^3): \quad X_1 \cap U_0 = V(f)$$
$$X_2 = V(z_0^3 z_2 - z_0 z_1^3): \quad X_2 \cap U_0 = V(f)$$

Keďže $X_1 \cap U_0 = X_2 \cap U_0$, tieto dve variety sa môžu líšiť len množinou nevlastných bodov:

$$X_1 \cap V(z_0) = V(z_0^2 z_2 - z_1^3, z_0) = \{(0:0:1)\},$$
$$X_2 \cap V(z_0) = V(z_0^3 z_2 - z_0 z_1^3, z_0) = V(z_0).$$

Kým X_1 má jediný bod v nekonečne, X_2 v sebe obsahuje celú priamku $V(z_0)$. (Skúste si nakresliť časť variety X_1 a X_2, ktorá sa nachádza napríklad v afinnej mape U_2, teda za nevlastnú budete považovať priamku $V(z_2)$.)

Je asi prirodzené snažiť sa pre danú afinnú varietu nájsť čo najmenšiu projektívnu varietu, ktorá tú zadanú obsahuje. V prípade nadplochy je prirodzené urobiť takú homogenizáciu definujúceho polynómu, ktorá jeho stupeň zbytočne nezväčšuje, ako sme práve videli v našom príklade. Formálne máme:

DEFINÍCIA 3.13. Nech $f \in k[x_1, \ldots, x_n]$. *Homogenizácia polynómu* f je polynóm $f^h \in k[z_0, \ldots, z_n]$ taký, že

- $f^h(1, x_1, \ldots, x_n) = f$,
- $z_0 \nmid f^h$.

Homogenizácia ideálu $I \subset k[x_1, \ldots, x_n]$ je ideál

$$I^h = (f^h \mid f \in I) \subset k[z_0, \ldots, z_n].$$

Všimnime si, že homogenizácia a dehomogenizácia (dosadenie $1, x_1, \ldots, x_n$ za $z_0, z_1, \ldots, z_n$) nie sú navzájom inverzné: ak $f \in k[z_0, \ldots, z_n]$, tak $(f(1, x_1, \ldots, x_n))^h$ (urobíme dehomogenizáciu a následne homogenizáciu) nemusí byť presne f, ale sa môže stať, že $f = z_0^d f^h(1, x_1, \ldots, x_n)$ pre nejaké $d \in \mathbb{N}$.

PRÍKLAD 3.14. Nech $I = (x_2 - x_1^2, x_3 - x_1^2) \subset k[x_1, x_2, x_3]$, varieta $V(I) \subset \mathbb{A}^3$ je krivka v priestore. Ľahšie si ju predstavíme, keď overíme, že $I = (x_2 - x_1^2, x_2 - x_3)$ (skúste si to!), takže $V(I)$ je vlastne parabola v rovine $V(x_2 - x_3)$.

Ideál $J = (z_0z_2 - z_1^2, z_0z_3 - z_1^2) \subset k[z_0, z_1, z_2, z_3]$ sme získali z ideálu I tak, že sme zhomogenizovali jeho generátory. Varieta $V(J) \subset \mathbb{P}^3$ je projektívnou varietou, ktorej zúženie na U_0 je naozaj naša krivka $V(I)$. Pozrime sa teraz, ktorými bodmi sme varietu $V(I) \subset \mathbb{A}^3$ doplnili na varietu $V(J) \subset \mathbb{P}^3$:

$$\begin{aligned} V(J) \cap V(z_0) &= \{(a_0 : a_1 : a_2 : a_3) \in \mathbb{P}^3 \mid a_0a_2 - a_1^2 = 0,\ a_0a_3 - a_1^2 = 0,\ a_0 = 0\} \\ &= \{(0 : 0 : a : b) \in \mathbb{P}^3\}. \end{aligned}$$

Prienik $V(J) \cap V(z_0)$ je priamka $V(z_0, z_1)$ – ide o nevlastné body roviny $V(z_1)$. Očakávali by sme ale, že krivke $V(I)$ stačí pridať jeden nevlastný bod, keďže ide o parabolu. Táto situácia nastala preto, lebo J nie je homogenizáciou ideálu I: polynóm $x_2 - x_3$ patrí ideálu I, jeho homogenizácia $z_2 - z_3$ však v J neleží.

Z príkladu vidíme, že stále potrebujeme vyriešiť otázku nájdenia homogenizácie daného ideálu. Nestačí totiž zhomogenizovať ľubovoľnú množinu generátorov.

DEFINÍCIA 3.15. Usporiadanie monómov sa nazýva *graduované*, ak je kompatibilné s čiastočným usporiadaním indukovaným stupňom, t.j. ak $x_1^{\alpha_1} \dots x_n^{\alpha_n} > x_1^{\beta_1} \dots x_n^{\beta_n}$, potom $\alpha_1 + \dots + \alpha_n \geq \beta_1 + \dots + \beta_n$.

Z usporiadaní, ktoré poznáme, graduovanými sú graduované lexikografické a graduované reverzné lexikografické usporiadanie. Lexikografické usporiadanie nie je graduovaným usporiadaním.

VETA 3.16 (**o homogenizácii**). *Nech $I \subset k[x_1, \dots, x_n]$ je ideál a nech $\{f_1, \dots, f_k\}$ je jeho Gröbnerova báza vzhľadom na nejaké graduované usporiadanie. Nech $f_i^h \in k[z_0, \dots, z_n]$ je homogenizáciou polynómu f_i. Potom*

$$I^h = (f_1^h, \dots, f_k^h).$$

Dôkaz. Definujme si reláciu $>_h$ na množine monómov v okruhu $k[z_0, \dots, z_n]$: Nech

$$\begin{aligned} z_0^{\alpha_0} \dots z_n^{\alpha_n} >_h z_0^{\beta_0} \dots z_n^{\beta_n}, \quad \text{ak} \quad & x_1^{\alpha_1} \dots x_n^{\alpha_n} > x_1^{\beta_1} \dots x_n^{\beta_n} \text{ alebo} \\ & x_1^{\alpha_1} \dots x_n^{\alpha_n} = x_1^{\beta_1} \dots x_n^{\beta_n} \text{ a } \alpha_0 > \beta_0. \end{aligned}$$

Ľahko sa overí, že táto relácia je usporiadaním monómov v $k[z_0, \dots, z_n]$. Ukážeme, že $\{f_1^h, \dots, f_k^h\}$ je Gröbnerova báza ideálu I^h vzhľadom na usporiadanie $>_h$, odkiaľ už vyplynie tvrdenie vety. Pre nasledovnú Lemu platí doterajšie označenie:

LEMA 3.17. *Nech $g \in k[x_1, \dots, x_n]$, nech $g^h \in k[z_0, \dots, z_n]$ je jeho homogenizácia. Ak stotožníme x_i so z_i, tak $\mathrm{LM}_{>_h}(g^h) = \mathrm{LM}_>(g)$.*

Dôkaz. Keďže $>$ je graduované usporiadanie, vedúci monóm polynómu g sa pri homogenizácii ničím nenásobí, akurát sa x_i preznačí na z_i. Nech $z_0^{\alpha_0} \dots z_n^{\alpha_n}$ je ďalší monóm, ktorý sa v g^h vyskytuje s nenulovým koeficientom. Ak $\alpha_0 > 0$, potom tento monóm je menší ako homogenizácia vedúceho monómu g, lebo g^h je homogénny polynóm a $>$ je graduované usporiadanie. Ak $\alpha_0 = 0$, potom tento monóm je tiež menší, lebo menším bol aj pred homogenizáciou. □

Pokračujeme teraz v dôkaze Vety. $\{f_1^h, \dots, f_k^h\}$ je Gröbnerova báza ideálu I^h, ak $\mathrm{LT}(I^h) = (\mathrm{LT}(f_1^h), \dots, \mathrm{LT}(f_k^h))$. Chceme ukázať, že ak $f \in I^h$, potom $\mathrm{LT}(f) \in (\mathrm{LT}(f_1^h), \dots, \mathrm{LT}(f_k^h))$.

Nech $f \in I^h$. Keďže I^h je homogénny ideál, každá homogénna časť polynómu f patrí do I^h (Tvrdenie 3.5), a tak môžme bez ujmy na všeobecnosti predpokladať, že f je homogénny polynóm.

Z $f \in I^h$ vieme, že

$$f = \sum p_i f_i^h \quad \text{pre nejaké} \quad p_i \in k[z_0, \dots, z_n].$$

Za $z_0, z_1, \ldots, z_n$ dosaďme $1, x_1, \ldots, x_n$ (t.j. dehomogenizujme), dostávame tak

$$f(1, x_1, \ldots, x_n) = \sum p_i(1, x_1, \ldots, x_n) f_i^h(1, x_1, \ldots, x_n) = \sum p_i(1, x_1, \ldots, x_n) f_i,$$

čiže $f(1, x_1, \ldots, x_n) \in I$, a preto $\mathrm{LT}_>(f(1, x_1, \ldots, x_n)) \in (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_k))$. Keď polynóm $f(1, x_1, \ldots, x_n)$ zase zhomogenizujeme, dostávame polynóm v $k[z_0, \ldots, z_n]$, pre ktorý platí

$$f = z_0^d (f(1, x_1, \ldots, x_n))^h.$$

Takže $\mathrm{LM}_{>_h}(f) = z_0^d \mathrm{LM}_{>_h}((f(1, x_1, \ldots, x_n))^h)$, kde $\mathrm{LM}_{>_h}((f(1, x_1, \ldots, x_n))^h)$ je podľa práve dokázanej Lemy rovný monómu $\mathrm{LM}_>(f(1, x_1, \ldots, x_n))$, ak x_i stotožníme so z_i. Keďže $\{f_1, \ldots, f_k\}$ je Gröbnerova báza, tak $\mathrm{LM}_>(f_i) \mid \mathrm{LM}_>(f(1, x_1, \ldots, x_n))$ pre nejaké i, odkiaľ už máme

$$\mathrm{LM}_{>_h}(f_i^h) \mid \mathrm{LM}_{>_h}((f(1, x_1, \ldots, x_n))^h),$$

a teda $\mathrm{LM}_{>_h}(f) \in (\mathrm{LM}_{>_h}(f_1^h), \ldots, \mathrm{LM}_{>_h}(f_k^h))$. □

Definícia 3.18. Nech $X \subset \mathbb{A}^n$ je afinná algebraická varieta, a nech $I = I(X)$. Potom $V(I^h)$ je *projektívny uzáver* variety X.

Pre projektívny uzáver uzáver afinnej variety berieme ideál $I(X)$ a nie ľubovoľný ideál, ktorý túto varietu definuje. Je to preto, aby konštrukcia projektívneho uzáveru bola geometricky intuitívna aj v prípade, keď pole k nie je algebraicky uzavreté:

Príklad 3.19. Nech $I = (x_1^2 + x_2^4) \subset \mathbb{R}[x_1, x_2]$. Potom $V(I) = \{(0, 0)\}$. Ak by sme homogenizovali ideál I, dostali by sme v $\mathbb{P}^2$

$$V(I^h) = V(z_0^2 z_1^2 + z_2^4) = \{(1 : 0 : 0), (0 : 1 : 0)\}.$$

Prirodzenejšie je očakávať len jednobodovú algebraickú varietu ako projektívny uzáver jednobodovej množiny v afinnej rovine. Naozaj,

$$J = I(V(I)) = (x_1, x_2)$$

Množina $\{x_1, x_2\}$ je Gröbnerovou bázou pri akomkoľvek usporiadaní, takže homogenizácia tohto ideálu je $J^h = (z_1, z_2)$. Potom v $\mathbb{P}^2$ dostávame

$$V(J^h) = V(z_1, z_2) = \{(1 : 0 : 0)\}.$$

Ak hľadáme projektívny uzáver afinnej algebraickej variety $X = V(J)$, musíme teda urobiť nasledujúce výpočty:

- Nájsť ideál $I = I(V(J))$. Ak je pole k algebraicky uzavreté, tak $I = \sqrt{(J)}$.
- Nájsť Gröbnerovu bázu ideálu I vzhľadom na nejaké graduované usporiadanie.
- Zhomogenizovať polynómy nájdenej Gröbnerovej bázy.

DODATOK A

Riešenie dvojrozmernej platformy pomocou `Singularu`

Uvedený je zoznam príkazov pre systém počítačovej algebry `Singular`, ktorý rieši problém platformy z konca Kapitoly 2.

```
ring r = (0, d1,d2,d3), (x1,y1,x2,y2), lp;
r;
//  r je okruh nad racionalnymi cislami,
//    s parametrami d1,d2,d3,
//    so styrmi premennymi x1,y1,x2,y2
//    a lexikografickym usporiadanim


//  f1 popisuje mnozinu vsetkych stavov platformy
poly f1 = (x1-x2)^2 + (y1-y2)^2 - 1;
//  f2,f3,f4 urcuju polohu platformy po zadani dlzok "noh"
poly f2 = x1^2 + y1^2 - d1^2;
poly f3 = (x2-1)^2 + y2^2 - d2^2;
poly f4 = (x1+1)^2 + y1^2 - d3^2;

ideal I = f1,f2,f3,f4;

//  chceme overit, ze mnozina V(I) je konecna,
//  pripadne i najst pocet rieseni
ideal gbI = groebner(I);
gbI;

poly g1 = gbI[1];
coeffs(g1, x1);
size(coeffs(g1, x1));
coeffs(g1, y1);
size(coeffs(g1, y1));
coeffs(g1, x2);
size(coeffs(g1, x2));
coeffs(g1, y2);
size(coeffs(g1, y2));
//  g1 je polynom stvrteho stupna,
//  v ktorom sa vyskytuje iba y2
//  => styri riesenia pre y2

poly g2 = gbI[2];
size(coeffs(g2, x1));
size(coeffs(g2, y1));
size(coeffs(g2, x2));
size(coeffs(g2, y2));
```

```
//  okrem y2 sa vyskytuje aj x2
coeffs(g2, x2);
//  g2 je linearny v x2
//  => pre zvolene y2 existuje len jedno x2

poly g3 = gbI[3];
size(coeffs(g3, x1));
size(coeffs(g3, y1));
size(coeffs(g3, x2));
size(coeffs(g3, y2));
//  okrem y2 a x2 sa vyskytuje uz aj y1
coeffs(g3, y1);
//  g3 je linearny v y1
//  => pre zvolene y2 a dopocitane x2 existuje len jedno y1

poly g4 = gbI[4];
size(coeffs(g4, x1));
//  g4 je linearny v x1
//  => pre zvolene y2 a dopocitane x2, y1 existuje len jedno x1


//  sustava f1 = f2 = f3 = f4 = 0 ma styri riesenia
//  (niektore mozno komplexne)
//  a pomocou groebnerovej bazy s lexikografickym usporiadanim
//  ich vieme najst
```

Literatúra

[CLO96] David Cox, John Little, and Donal O'Shea, *Ideals, varieties and algorithms*, Springer Verlag, 1996.

[Has07] Brendan Hassett, *Algebraic geometry*, Cambridge University Press, 2007.

[Kun85] Ernst A. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhauser, 1985.

[SB03] M.-F. Roy S. Basu, R. Pollack, *Algorithms in real algebraic geometry springer*, Springer, 2003.

[Sha94] Igor R. Shafarevich, *Basic algebraic geometry 1*, Springer Verlag, 1994.