Algebraická geometria 1

KAG FMFI UK Bratislava
Email address: jana.chalmovianska@fmph.uniba.sk

Obsah

KAPITOLA 1

Variety a ideály (Základné pojmy)

1. Afinné algebraické variety

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).

Pre ľubovoľné pole k budeme symbolom $k[x_1, x_2, \ldots, x_n]$ označovať množinu všetkých polynómov s premennými $x_1, x_2, \ldots, x_n$ a s koeficientami v poli k. Čoskoro si uvedieme rigoróznejšiu definíciu tohto pojmu, nateraz si vystačíme s týmto menej formálnym opisom.

Polynóm $f \in k[x_1, x_2, \ldots, x_n]$ predstavuje funkciu na priestore $\mathbb{A}^n(k)$ s hodnotami v k: za premennú x_i budeme dosadzovať i-tu súradnicu bodu z $\mathbb{A}^n(k)$. 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 $f_1, \ldots, f_r$ (tiež sa na ňu budeme odvolávať ako na *afinnú varietu*, *algebraickú varietu* alebo jednoducho *varietu*).

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 $X = \{(1, 2), (3, 4)\} \subset \mathbb{A}^2(\mathbb{Q})$, $X = V((x-1)(x-3), (x-1)(y-4), (y-2)(x-3), (y-2)(y-4))$ (presvedčte sa o tom!) Tú istú varietu môžme tiež popísať ako $X = V((x-1)(x-3), x-y+1)$. Vidíme, že jedna algebraická varieta môže byť popísaná viacerými spôsobmi. Vo všeobecnosti nie je ľahké overiť, že dve sústavy polynomických rovníc opisujú tú istú algebraickú varietu.

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 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 $X = V(f) \subset \mathbb{A}^2(k)$ sa nazýva *rovinná (algebraická) krivka*. Uveďme si príklady takýchto kriviek:

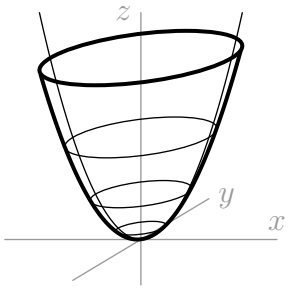
(i) *Regulárna kuželosečka* je množina bodov v $\mathbb{A}^2$ vyhovujúcich rovnici $f(x, y) = 0$, kde $f \in k[x, y]$ je ireducibilný kvadratický polynóm.
(ii) Graf polynomickej funkcie $y = g(x)$ ($g \in k[x]$) je množina $X = V(y - g(x))$.
(iii) Graf racionálnej funkcie je tiež rovinná algebraická 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 $X = V(yq(x) - p(x))$.

PRÍKLAD 1.6. *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 1.7. 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 $X = V(z - (x^2 + y^2))$.

PRÍKLAD 1.8. *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, $X = V(y - x^2, z - x^3)$.

Vinutá kubika je príklad tzv. *racionálnej normálnej krivky*, čo je krivka s parametrizáciou

$$\{(t, t^2, t^3, \ldots, t^n), t \in k\} \subset \mathbb{A}^n.$$

Zjavne ide tiež o algebraickú varietu – vedeli by ste napísať polynómy, ktorými je ako varieta definovaná?

PRÍKLAD 1.9. Krivka v reálnom trojrozmernom priestore daná parametrizáciou (t^3, t^4, t^5), $t \in \mathbb{R}$ je tiež algebraickou varietou

$$V(x^3 - yz, y^2 - xz, z^2 - x^2y).$$

Všimnite si, že ak by sme vynechali ktorýkoľvek z definujúcich polynómov, dostali by sme inú krivku – k pôvodným bodom by pribudli aj body niektorej zo súradnicových osí.

Ide o výrazný rozdiel oproti lineárnym varietám (Príklad 1.4), kde je jednoznačný súvis medzi dimenziou variety a minimálnym počtom rovníc, ktoré ju určujú.

Exaktne sme si definovali 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 1.10. 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 1.11. 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.

Príklad 1.12. Špeciálnymi algebraickými varietami sú tzv. súradnicové podpriestory:

- Súradnicová priamka v $\mathbb{A}^n(k)$ je množina $\{(0, \dots, 0, a, 0, \dots, 0) \mid a \in k\}$ je lineárna varieta daná $n-1$ lineárnymi rovnicami.
- Súradnicová rovina je daná $n-2$ lineárnymi rovnicami.
- Súradnicová nadrovina je množina $H_i = V(x_i)$.

Príklad 1.13. Nech $f_1, \dots, f_r$ sú monómy, napr. v $\mathbb{R}[x, y, z]$:

$$f_1 = y^2z^3$$
$$f_2 = x^5z^4$$
$$f_3 = x^2yz^2$$

Ako vyzerá varieta $X = V(f_1, f_2, f_3)$?

Polynóm f_1 popisuje varietu

$$X_1 = V(f_1) = V(y^2z^3) = V(yz) = V(y) \cup V(z) = H_y \cup H_z.$$

Podobne rozpíšeme variety určené polynómami f_1, f_2:

$$X_2 = V(f_2) = H_x \cup H_z$$
$$X_3 = V(f_3) = H_x \cup H_y \cup H_z.$$

Odtiaľ potom zistíme, že $X = X_1 \cap X_2 \cap X_3 = H_z \cup o_z$.

Iný prístup: riešime sústavu rovníc

$$y^2z^3 = 0$$
$$x^5z^4 = 0$$
$$x^2yz^2 = 0.$$

Pozorovanie. Monomiálne polynómy popisujú variety pozostávajúce zo zjednotenia súradnicových priestorov. Ide o veľmi jednoduché variety, ktoré sa ukazujú byť neskôr veľmi užitočnými.

Tvrdenie 1.14. *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 $f_1, \ldots, f_r, g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$, že

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

Ukážeme, že

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

Prvá rovnosť (o prieniku) je jednoduchá:

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

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 $a \in V(f_i g_j \mid i = 1, \ldots, r, j = 1, \ldots, s)$. 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 $l \in \{1, \ldots, r\}$, 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.*

Príklad 1.15. Nech $X \subset \mathbb{A}^m$ a $Y \subset \mathbb{A}^n$ sú algebraické variety:

$$X = V(f_1, \ldots, f_r), \quad f_i \in k[x_1, \ldots, x_m]$$
$$Y = V(g_1, \ldots, g_s), \quad g_j \in k[y_1, \ldots, y_n]$$

Súčinom variet X a Y rozumieme množinu

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\} \subset \mathbb{A}^m \times \mathbb{A}^m = \mathbb{A}^{m+n}.$$

Zrejme súčin algebraických variet je tiež algebraická varieta:

$$X \times Y = V(f_1, \ldots, f_r, g_1 \ldots, g_s),$$

kde f_i a g_j chápeme ako polynómy okruhu $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$.

Príklad 1.16. Špeciálne, nech X je rovinná krivka, napríklad

$$X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2$$

.

(i) Nech $Y = \mathbb{A}^1$. Potom

$$X \times Y = V(x^2 + y^2 - 1) \subset \mathbb{A}^3$$

je valcová plocha nad kružnicou X.

(ii) Nech $Y = V((z-1)z(z+1)) \subset \mathbb{A}^1$. Ako by ste v tomto prípade popísali súčin $X \times Y$?

Príklad 1.17. Znovu, nech $X \subset \mathbb{A}^2$ je rovinná krivka $V(f)$, $f \in k[x, y]$. Nech $F \in k[x, y, z]$ je homogenizáciou polynómu f, t.j. ak d je stupeň f, tak každý monóm v f vynásobíme takou mocninou premennej z, aby mal stupeň d. Výsledná varieta $V(F) \subset \mathbb{A}^3$ je *kuželom* nad $V(f)$. Naozaj prienik $V(F)$ s rovinou $V(z-1)$ je pôvodná krivka (tzv.

určujuca krivka kužeľovej plochy): jej bodmi sú rozšírené súradnice bodu krivky X. Tiež je priamočiare sa presvedčiť, že ak $(a, b, 1) \in V(F)$ (t.j. $(a, b) \in V(f) = X$), potom celá priamka prechádzajúca bodmi $(a, b, 1)$ a bodom $(0, 0, 0)$ (tzv. *vrcholom kužeľa*) leží na variete $V(F)$.

PRÍKLAD 1.18. Vdaka predchádzajúcemu príkladu sa presvedčíme, že rezmi kužeľovej plochy sú naozaj kužeľosečky:

Nech $K = V(x^2 + y^2 - 1) \subset \mathbb{A}^3$ je rotačná kužeľová plocha. Nech Y je ľubovoľná rovina. Zvoľme si súradicovú sústavu tak, aby Y bola súradnicová rovina $V(z)$. Plocha K bude v tejto sústave popísaná kvadratickým polynómom $g \in k[x, y, z]$. Prienik $K \cup Y$ je potom krivka $V(g(x, y, 0)) \subset \mathbb{A}^2 = V(z)$, teda je tiež definovaná (nanajvýš) kvadratickým polynómom.

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 1.19. 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.

TVRDENIE 1.20. *Afinná algebraická varieta v $\mathbb{A}^n(\mathbb{R})$ je v topológii, ktorá pochádza zo štandardnej euklidovskej metriky, uzavretou množinou.*

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

PRÍKLAD 1.21. 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.

2. Okruhy polynómov

Ak chceme hlbšie študovať afinné algebraické variety, potrebujeme dôkladnejšie porozumieť polynómom. Tomu sa budeme venovať vo zvyšku kapitoly.

Na začiatok neformálne úvahy: čo sú polynómy o premennej x nad poľom k?

(a) Je to funkcia: $f(x) = 3x^2 - 2x + 1$ zobrazuje $a \mapsto 3a^2 - 2a + 1$.

(b) Je to objekt, prvok nejakej množiny:

$$k[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in k\}.$$

Akú štruktúru má táto množina?

– $k[x]$ je vektorový priestor nad k. (Akú má dimenziu? Akú má bázu?) Vieme teda jednotlivé vektory (= polynómy) sčítavať, vzhľadom na násobenie tvorí $k[x]$ grupu.
– Vektory vieme spolu aj násobiť. (Tvorí množina $k[x]$ vzhľadom na násobenie grupu?)

$k[x]$ nie je pole, je to tzv. komutatívny okruh.

DEFINÍCIA 1.22. *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 1.23. Znamienko násobenia budeme zvyčajne zo zápisu vynechávať.
Slovo "komutatívny" v definícii sa vzťahuje na komutatívnosť násobenia. Slovo "jednotka" sa vzťahuje na neutrálny prvok vzhľadom na násobenie.

PRÍKLAD 1.24. V nasledovných množinách máme štandardne definované operácie sčítania a násobenia:

- Množina $\mathbb{Z}$ všetkých celých čísel tvorí komutatívny okruh s jednotkou.
- Množina $2\mathbb{Z}$ všetkých párnych celých čísel neobsahuje jednotku, preto my ju nebudeme považovať za okruh.
- $\mathbb{Z}[i]$, tzv. Gaussove čísla tvoria komutatívny okruh s jednotkou.
- $\mathcal{M}_n(\mathbb{R})$ – množina všetkých štvorcových matíc stupňa n (n je prirodzené číslo) nad poľom reálnych čísel tvorí okruh s jednotkou, ale nie komutatívny, lebo násobenie matíc nie je komutatívne.
- $\mathcal{M}_n(\mathbb{Z})$ – to isté ako $\mathcal{M}_n(\mathbb{R})$.

DEFINÍCIA 1.25. Nech R je okruh (komutatívny s jednotkou), potom množina $R[x]$ s operáciami + a $\cdot$ definovanými nasledovne: $\forall f,g\in R[x]$, kde $f=f_0+f_1x+\cdots+f_mx^m$, $g=g_0+g_1x+\cdots+g_nx^n$ je

- $f+g=(f_0+g_0)+(f_1+g_1)x+\ldots$ (až po najvyššiu mocninu x)
- $f\cdot g=(f_0g_0)+(f_1g_0+f_0g_1)x+\cdots+f_mg_nx^{m+n}$

je *okruhom polynómov* o premennej x nad R.

Je priamočiare overiť, že pre okruh R je aj $R[x]$ okruhom.

DEFINÍCIA 1.26. Ak k je pole, tak $k[x_1,x_2,\ldots,x_n]=(k[x_1,x_2,\ldots,x_{n-1}])[x_n]$. Podobne pre ľubovoľný okruh R zadefinujeme $R[x_1,x_2,\ldots,x_n]$.

Nech k je ľubovoľné pole, symbolom $k[x_1,x_2,\ldots,x_n]$ teda 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

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

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 $c_\alpha \in k$, $c_\alpha \neq 0$, 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.

3. Ideály

Príklad 1.27. Nech $X = V(f_1, f_2) \subset \mathbb{A}^2(\mathbb{R})$, kde $f_1 = x^2 + y^2 - 2$, $f_2 = x - y$, t.j. algebraická varieta X pozostáva z dvoch bodov. Polynómy f_1, f_2 nie sú jediné také, že body variety X sú ich koreňmi. Napríklad aj pre $(-f_2) = y - x$ platí, že $(-f_2)(a) = 0$ pre všetky $a \in X$. To isté môžme povedať aj o polynóme $7f_2$, i o polynóme $f_1 + f_2$. Ľubovoľná kombinácia polynómov f_1 a f_2 má požadovanú vlastnosť, a to nielen kombinácia nad $\mathbb{R}$ (teda polynómy tvaru $c_1 f_1 + c_2 f_2$, pre $c_1, c_2 \in \mathbb{R}$), ale i kombinácia nad $\mathbb{R}[x, y]$ (čiže polnómy tvaru $g_1 f_1 + g_2 f_2$, kde $g_1, g_2 \in \mathbb{R}[x, y]$). To nás motivuje k nasledovnej definícii.

Definícia 1.28. 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 $a.r \in I$.

V algebre ste sa zrejme stretli s inou definíciou ideálu, ktorá sa štandardne vyslovuje v prípade všeobecnejších okruhov, teda nie nutne komutatívnych a dokonca nie nutne s jednotkou:

Definícia 1.29. Ak R je okruh, tak jeho podmnožina $I \subset R$ je *ideál*, ak platí:

(i) pre každé $a, b \in I$ platí $a - b \in I$,
(ii) pre každé $a \in I$ a pre každé $r \in R$ platí $a.r \in I$ a $ir \in I$.

Pristavme sa chvíľu a porovnajme si tieto dve definície.

Pokiaľ je okruh R komutatívny, jednostranné ideály sa stávajú automaticky (obojstrannými) ideálmi a teda namiesto podmieky (ii) v Definícii 1.29 stačí uviesť podmienku z Definície 1.28.

S podmienkou (i) v týchto definíciách je to trochu zložitejšie. Nech $I \subset R$ je ideálom podľa Definície 1.29. Potom je I ideálom aj podľa Definície 1.28. Naozaj, nech $a, b \in I$, potom $-b = 0 - b \in I$, lebo $0 \in I$. Potom využijúc (i) Definície 1.29 dostávame

$$a + b = a - (-b) \in I,$$

čiže je splnená podmienka (i) Definície 1.28.

Nech teraz naopak $I \subset R$ je ideálom podľa Definície 1.28, chceme overiť, či je I ideálom aj podľa druhej definície. Nech $a, b \in I$. Ak $1 \in \mathbb{R}$, potom aj $-1 \in R$, keďže $(R, +)$ je grupa. Z $b \in I$ tak máme aj $-b = (-1).b \in I$. Potom podľa (i) v Definícii 1.28 dostávame

$$a - b = a + (-b) = a + (-1).b \in I,$$

teda I je ideálom aj podľa Definícii 1.29.

Teda ak R je komutatívny okruh s jednotkou, sú obe definície ideálu ekvivalentné. Ak by sme pripustili, že okruh R jendotku neobsahuje, je medzi týmito definíciami rozdiel:

Príklad 1.30. Nech

$$R = \{ax + bx^2 \mid a, b, \in \mathbb{R}\},$$

kde pri násobení platí rovnosť $x^3 = 0$ (t.j. počítame „modulo x^3“). Množina

$$\mathcal{M} = \{ax + bx^2 \mid a, b, \in \mathbb{R},\ a \geq 0\}$$

je ideálom podľa Definície 1.28, ale nie je ideálom podľa Definície 1.29.

Vráťme sa naspäť k ideálom, ako sa s nimi pracuje v komutatívnej algebre. My budeme používať výlučne Definíciu 1.28.

Nech $G \subset R$ je ľubovoľná množina. Zápisom (G) budeme označovať množinu všetkých konečných kombinácií prvkov z G nad okruhom R, t.j. množinu $\{r_1g_1 + r_2r_2 + \cdots + r_kg_k\}$. Zrejme G tvorí ideál v R. (Dôkaz: dú.)

Definícia 1.31. Neprázdna 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

$$a = r_1g_1 + r_2r_2 + \cdots + r_kg_k.$$

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

Každý ideál má množinu generátorov, napríklad pre ideál I platí, že $I = (I)$. Zaujímavejšie je prirodzene pre daný ideál nájsť čo najmenšiu množinu, ktorá ho generuje.

Príklad 1.32.

- 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?)
- Ďalšie ideály v $\mathbb{Z}$ sú $(3), (5), (8), \ldots$.

Príklad 1.33. 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 kominácu pôvodných dvoch čísiel:

$$\begin{aligned} 21 &= 1.15 + 6 \\ 15 &= 2.6 + 3 \\ 6 &= 2.3 + 0 \end{aligned}$$

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 $I = (21, 15) = (3)$.

Príklad 1.34.

- Nech $R = k[x]$. Všetky polynómy bez absolútneho člena tvoria ideál v $k[x]$. Tento ideál je generovaný polynómom x.
- Z akých polynómov pozostáva ideál (x^2)?
- Iným príkladom ideálu v tomto okruhu je množina všetkých násobkov polynómu $x-1$. Ide o $(x-1)$, t.j. ideál generovaný polynómom $x-1$. Ide o všetky polynómy, pre ktoré je jedným z koreňov 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).

Príklad 1.35. V každom okruhu R, kde $0 \neq 1$, sú aspoň dva ideály: (0) a R.

Lema 1.36. *Pre ideál $I \subseteq R$ platí*

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

Dôkaz. Zjavné. □

Definícia 1.37. Ideál I v okruhu R sa nazýva

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

Príklad 1.38. 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 prvoideálom aj maximálnym ideálom.

Podobne $(3) \subseteq \mathbb{Z}$, ideál obsahujúci presne všetky celé čísla deliteľné číslom 3, je hlavný, maximálny aj 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 $a \notin (6)$, $b \notin (6)$.

Ideál $(21, 15)$, hoci je zadaný pomocou dvoch generátorov, je tiež hlavný, lebo ako sme videli, $(21, 15) = (3)$. Vďaka Euklidovmu algoritmu je každý ideál v $\mathbb{Z}$ hlavným.

Príklad 1.39. 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 $I = (x + 1)$.

Definícia 1.40. Okruh R sa nazýva *okruhom hlavných ideálov*, ak každý ideál v R je hlavný.

VETA 1.41.

(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 1.42. Nech $R = k[x, y]$. Ideál $I = (x, y)$ nie je hlavný. (Dôkaz: ak by platilo $(x, y) = (f)$, potom musí platiť $f \mid x$ aj $f \mid y$. Túto vlastnosť však majú len konštantné polynómy.) 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 1.36 platí $J = k[x, y]$.

4. Afinné algebraické variety a ideály

Vráťme sa k pozorovaniu, ktoré nás motivovalo k definícii ideálu.

PRÍKLAD 1.43. Existuje súvis medzi varietami a ideálmi: Nech $X = V(f_1, f_2) \subset \mathbb{A}^2(\mathbb{R})$, kde $f_1 = x^2 + y^2 - 2$, $f_2 = x - y$, t.j. algebraická varieta X pozostáva z dvoch bodov. Nech $I = (f_1, f_2) = (x^2 + y^2 - 2, x - y)$ je ideál. Nech $g = x^2 - 1$. Platí, že $g = \frac{1}{2}f_1 + \frac{x+y}{2}f_2$. Obidva body variety sú koreňmi f_1 aj f_2, a preto sú aj koreňmi g. Všeobecnejšie, ak $g \in I$, čiže $g(x, y) = h_1 f_1 + h_2 f_2$ pre nejaké $h_1, h_2 \in \mathbb{R}[x, y]$, potom pre $a = (a_1, a_2) \in V(f)$ platí $g(a) = h_1(a)f_1(a) + h_2(a)f_2(a) = 0$.

Už sme sa stretli so situáciou (Príklad 1.3, (iv)), keď jedna algebraická varieta bola popísaná rôznymi polynómami. Zjavne každej skupine polynómov môžeme prirodzene priradiť celý ideál generovaný polynómami, ktorými sme varietu definovali. Taktiež platí, že algebraickej variete môžme priradiť ideál pozostávajúci z polynómov, ktoré sú nulové vo všetkých bodoch variety (bližšie to budeme skúmať čoskoro). Vyvstáva nám nová otázka: ako je to so vzájomnou jednoznačnosťou medzi varietami a ideálmi?

Najprv potrebujeme kritérium pre porovnávanie dvoch ideálov.

LEMA 1.44. *V komutatívnom okruhu R platí, že $(f_1, \dots, f_r) = (g_1, \dots, g_s)$ práve vtedy, keď*

$$f_i \in (g_1, \dots, g_s)\ \forall i,\ \text{a tiež } g_j \in (f_1, \dots, f_r)\ \forall j. \tag{2}$$

Dôkaz. Je zrejmé, že ak $(f_1, \dots, f_r) = (g_1, \dots, g_s)$, potom platí (2). Pre opačnú implikáciu predpokladajme, že platí (2). 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 1.45. *Ak v okruhu $k[x_1, \ldots, x_n]$ polynómy $f_1, \ldots, f_r$ generujú ten istý ideál ako polynómy $g_1, \ldots, g_s$, potom $V(f_1, \ldots, f_r) = V(g_1, \ldots, g_s)$.*

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

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

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

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

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

ZÁVER. Algebraickú varietu môžme priradiť ideálu, nezávisí od konkrétnych generátorov:

$$f_1, \ldots, f_r \rightsquigarrow I = (f_1, \ldots, f_r) \rightsquigarrow V(f_1, \ldots, f_r).$$

Varietu definovanú ideálom I budeme označovať $V(I)$.

Pri skúmaní vzťahu variet a ideálov nám stále ostávajú nevyriešené dva problémy:

(1) Možno každému ideálu priradiť varietu? Inak: má každý ideál konečnú množinu generátorov?
(2) Ako je to s jednoznačnosťou vzťahu ideál – varieta?

Rýchlu odpoveď (nie veľmi uspokojivú, no nateraz si s ňou vystačíme) na druhú otázku nám poskytnú nasledovné príklady.

PRÍKLAD 1.46. Obrátená implikácia z Lemy 1.45 neplatí: ak $V(f_1, \ldots, f_r) = V(g_1, \ldots, g_s)$, ešte to nemusí znamenať, že $(f_1, \ldots, f_r) = (g_1, \ldots, g_s)$. Nech $f = (x-1)^2(x+1)$ a $g = (x-1)(x+1)$. Vtedy $V((f)) = V((g))$, avšak $(f) \neq (g)$: $f \in (g)$, ale $g \notin (f)$. Preto aj ak chceme overiť, či $(f_1, \ldots, f_r) = (g_1, \ldots, g_s)$, nestačí overiť, že obe sústavy rovníc majú to isté riešenie, treba naozaj postupovať podľa Lemy 1.44.

PRÍKLAD 1.47. Podobne ako v predchádzjúcom príklade, majme $f_1 = y^2z^3, f_2 = x^5z^4, f_3 = x^2yz^2$. Na druhej strane nech $g_1 = xz, g_2 = yz$. Znovu platí, že $V(f_1, f_2, f_3) = V(g_1, g_2)$, hoci zjavne $(f_1, f_2, f_3) \neq (g_1, g_2)$. Vidíme, že ideálov v $k[x_1, \ldots, x_n]$ akoby bolo viac než variet v $\mathbb{A}^n(k)$.

K zodpovedaniu prvej otázky potrebujeme nejaké vedomosti o štruktúre ideálov v $k[x_1, \ldots, x_n]$.

LEMA 1.48 (**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 $I_0 \subset I_1 \subset I_2 \subset \ldots$ je konečná, čiže $I_n = I_{n+1}$ pre dostatočne veľké n.*

DEFINÍCIA 1.49. Okruh R, v ktorom platia tvrdenia Lemy 1.48, sa nazýva *noetherovský.*

Dôkaz Lemmy 1.48. Predpokladajme, že každý ideál v R je konečne generovaný. Majme rastúcu reťaz ideálov $I_0 \subset I_1 \subset I_2 \subset \dots$. Potom

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

ideál (dôkaz: dú). 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 $\alpha \in A$. Zostrojme rastúcu reťaz navzájom rôznych ideálov

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

teda $f_{\alpha_{j+1}} \notin I_j$. Podľa predpokladu musí byť zostrojená reťaz ideálov konečná, teda po konečnom počte krokov už nevieme vybrať $f_{\alpha_{j+1}}$ také, že nepatrí I_j, a teda ideál I je generovaný konečným počtom prvkov. □

Príklad 1.50. 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, $k[x]$ je tiež okruhom hlavných ideálov, a teda je noetherovský.

Veta 1.51 (**Hilbertova veta o báze**). *Ak R je noetherovský okruh, potom aj $R[x]$ je noetherovský okruh.*

Dôkaz. Nech $I \subset R[x]$ je ideál, ukážeme, že je konečne generovaný.

Pre každé $m \in \mathbb{N}_0$ uvažujme množinu

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

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 (dú). Taktiež platí, že $J_m \subset J_{m+1}$ pre všetky m (dú). 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:

$$\begin{aligned} J_0 &= (a_{01}, \dots, a_{0n_0}) \\ J_1 &= (a_{11}, \dots, a_{1n_1}) \\ &\dots \\ J_N &= (a_{N1}, \dots, a_{Nn_N}) \end{aligned}$$

Pre každé a_{ij} $(i = 0, \dots, N, j = 1, \dots, n_i)$ 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 $a_{0j} = f_{0j}$, $(j = 1, \dots n_0)$. 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 pre nejaké $h_j \in R$

$$c_d = \sum_j h_j a_{d'j} \quad \text{kde} \quad d' = \min\{d, N\}.$$

Polynóm $g = f - \sum_j h_j f_{d'j} x^{d-d'}$ 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 $k[x_1, \dots, x_n]$ noetherovský.*

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

Z Hilbertovej vety o báze vyplýva, že pre každý ideál I je $V(I)$ afinná algebraická varieta: keďže $k[x_1, \dots, x_n]$ je noetherovský, $I = (f_1, \dots, f_r)$ pre nejaké $f_1, \dots, f_r \in k[x_1, \dots, x_n]$, a teda máme $V(I) = V(f_1, \dots, f_r)$.

Príklad 1.52. Okruh $\mathbb{Z}[x]$ je noetherovský.

Definícia 1.53. Pre ľubovoľnú podmnožinu $F \subset k[x_1, \dots, x_n]$ definujeme

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

Napriek tomu, že F môže byť ľubovoľná a nie nutne konečná množina, je $V(F)$ algebraicou varietou: ak $I = (F)$, teda I je ideál generovaný polynómami z F, potom zrejme $V(F) = V(I)$, o čom sme sa už presvedčili, že je algebraickou varietou.

Definícia 1.54. Pre ľubovoľnú podmnožinu $S \subset \mathbb{A}^n(k)$ definujeme

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

Ak X je algebraická varieta, budeme $I(X)$ ho nazývať *ideálom variety X*.

Príklad 1.55. V príklade 1.19 sme o množine $M = \{\dots, (-1,0), (0,0), (1,0), (2,0), \dots\}$ ukázali, že nie je algebraickou varietou. Ideál $I(M)$ však existuje, v spomenutom príklade sme sa presvedčili, že $I(M) = (y)$.

Príklad 1.56. Vráťme sa zas k monomiálneho ideálu $I = (f_1, f_2, f_3)$, kde $f_1 = y^2z^3, f_2 = x^5z^4, f_3 = x^2yz^2$. Platí, že $V(I) = H_z \cup o_z$ (o čom sme sa už presvedčili). Pre ideál $I(V(I))$ platí

$$I(V(I)) = I(H_z \cup o_z) = (xz, yz).$$

Pozorovanie.

- $I(X)$ je najväčší ideál popisujúci varietu X.
- $V(I(M))$ je najmenšia varieta obsahujúca množinu M.

Tvrdenie 1.57. *V nasledovnom F, G sú podmnožiny $k[x_1, \dots, x_n]$ a S, T zas podmnožiny $\mathbb{A}^n(k)$. Platí:*

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

Dôkaz. dú. □

5. Nullstellensatz

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

5.1. Radikál ideálu.

PRÍKLAD 1.58. 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 1.59. 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 1.60. (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) dú.
(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 $e \in \mathbb{N}$ také, že $(f^d)^e = f^{de} \in I$, a teda $f \in \sqrt{I}$. □

PRÍKLAD 1.61. Radikály niektorých ideálov v okruhu $\mathbb{Z}$: $\sqrt{(4)} = (2)$, $\sqrt{(5)} = (5)$, $\sqrt{(12)} = (6)$, $\sqrt{(18)} = (6)$. Ako vo všeobecnosti nájdeme radikál ideálu $(n), n \in \mathbb{N}$?

PRÍKLAD 1.62. 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 $\sqrt{I} = ((x+y^2+3)(2x-y))$.

PRÍKLAD 1.63. Radikál ideálu $I = (x^2, y) \subset k[x,y]$ je ideál $\sqrt{I} = (x,y)$.

PRÍKLAD 1.64. Vo všeobecnosti nájsť radikál ideálu je ťažká úloha. Nech napríklad $I = (x^4 - y^2, x^3 - y^2)$. Jeho radikál nájdeme s pomocou vhodného systému počítačovej algebry: $\sqrt{I} = (-x + y^2, xy - y, x^2 - x)$.

PRÍKLAD 1.65. (zo začiatku prednášky:)

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

nech sú ideály v $\mathbb{R}[x,y]$. Platí, že $I_1 \neq I_2$, ale $V(I_1) = V(I_1)$. Všimnime si, že $\sqrt{I_1} = \sqrt{I_2}$. Toto je geometrickým zmyslom radikálov.

PRÍKLAD 1.66. $p(x) = (x-1)^2(x+1)^3(x-2) \in \mathbb{R}[x]$. Platí, že $V(p(x))$ je tá istá algebraická varieta ako $V(\sqrt{(p(x))})$.

TVRDENIE 1.67. *Nech $I \subset k[x_1, \ldots, x_n]$ je ideál. Potom $V(I) = V(\sqrt{I})$.*

Dôkaz. Keďže $I \subseteq \sqrt{I}$, tak $V(\sqrt{I}) \subseteq V(I)$ (Tvrdenie 1.57).

Pre dôkaz opačnej inklúzie nech a je bod variety $V(I)$. Pre ľubovoľný polynóm $g \in \sqrt{I}$ a dostatočne veľké $d \in \mathbb{N}$ potom $g^d \in I$, a teda $g^d(a) = 0$. Potom ale aj $g(a) = 0$. Odtiaľ už vyplýva, že $a \in V(I)$. □

DÔSLEDOK. *Nech $I, J \subseteq k[x_1, \ldots, x_n]$ sú ideály. Ak $\sqrt{I} = \sqrt{J}$, potom $V(I) = V(J)$.*

Dôkaz. $V(I) = V(\sqrt{I}) = V(\sqrt{J}) = V(J)$. □

5.2. Tvrdenie vety.

TVRDENIE 1.68. *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 $d \in \mathbb{N}$. Potom $f^d(a) = 0$ pre všetky $a = (a_1, \ldots, a_n) \in V(I)$ a preto aj $f(a) = 0$ pre všetky $a \in V(I)$. Teda $f \in I(V(I))$. □

VETA 1.69 (**Hilbertova veta o koreňoch, Nullstellensatz, 1)**. *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 chvíľu uvedieme ešte iné verzie tejto vety a ukážeme, že tieto 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 $\sqrt{I} = \sqrt{J}$.

Opačná implikácia je dôsledkom Tvrdenia 1.67. □

PRÍKLAD 1.70. 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 1.71 (**Nullstellensatz, 2)**. *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 1.72. Implikácia $\Leftarrow$ je triviálna, tvrdenie Nullstellensatz spočíva v implikácii $\Rightarrow$.

PRÍKLAD 1.73. Analogicky s prvou 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 druhá verzia Nullstellensatz akoby bola zúžením prvej verzie na jeden konkrétny ideál a jednu konkrétnu algebraickú varietu. Ukážeme už spomínané

TVRDENIE 1.74. *Obe tvrdenia Nullstellensatz (1 a 2) sú ekvivalentné.*

Dôkaz. Nech platí tvrdenie Nullstellensatz 1. Podľa Poznámky 1.72 potrebujeme vo verzii 2 ukázať implikáciu $\Rightarrow$.

Nech $V(I) = \emptyset$, odtiaľ dostávame, že $1 \in I(V(I))$. Z 1. 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 2. verzie Nullstellensatz. Majme $I = (f_1, \ldots, f_r) \subset k[x_1, \ldots, x_n]$. Predpokladajme, 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 $(f_1, \ldots, f_r, 1 - yf) \subset k[x_1, \ldots, x_n, y]$ a skúmajme zodpovedajúcu varietu $V(f_1, \ldots, f_r, 1 - yf)$. 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 $f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0$, 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 $V(f_1, \ldots, f_r, 1 - yf)$.
- 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 $V(f_1, \ldots, f_r, 1 - yf) = \emptyset$. Z Nullstellnsatz 2 potom vyplýva, že $1 \in (f_1, \ldots, f_r, 1 - yf)$, takže existujú polynómy $p_1, \ldots, p_r, p \in k[x_1, \ldots, x_n, y]$ také, že

$$1 = p_1 f_1 + \cdots + p_r f_r + p(1 - yf).$$

Nahraďme v tejto rovnosti premennú y racionálnym výrazom $1/f$. Dostaneme tak rovnosť racionálnych výrazov, pričom v menovateľoch budú len mocniny f:

$$\begin{aligned} 1 &= p_1(x_1, \ldots, x_n, \frac{1}{f})f_1 + \cdots + p_r(x_1, \ldots, x_n, \frac{1}{f})f_r + p(x_1, \ldots, x_n, \frac{1}{f})(1 - \frac{1}{f}f) \\ &= p_1(x_1, \ldots, x_n, \frac{1}{f})f_1 + \cdots + p_r(x_1, \ldots, x_n, \frac{1}{f})f_r \end{aligned}$$

Po vynásobení rovnosti dostatočne vysokou mocninou f tak dostávame rovnosť polynómov:

$$f^d = q_1 f_1 + \ldots q_k f_k,$$

teda $f^d \in I$, čo sme chceli dokázať. □

TVRDENIE 1.75. *Nech $a_1, \ldots, a_n \in k$. Potom $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) \subset k[x_1, \ldots, x_n]$ je maximálny ideál.*

Dôkaz. Hľadajme ideál $J \supset \mathfrak{m}$. Nech $f \in J$. Pomocou polynómu $x_1 - a_1$ zredukujeme f na f_1 taký, že premenná x_1 sa v f_1 nevyskytuje:

$$f_1 = f + p_1 \cdot (x_1 - a_1),\ p_1 \in k[x_1, \ldots, x_n].$$

Podobne f_1 "vyčistíme" pomocu $x_2 - a_2$ od x_2:

$$f_2 = f_1 + p_2 \cdot (x_2 - a_2),\ p_2 \in k[x_2, \ldots, x_n].$$

Takto pokračujeme, až získame f_n, ktorý už neobsahuje žiadne z premenných, čiže f_n je konštantný polynóm, o ktorom navyše platí, že $f_n \in J$.

Ak pre nejaké $f \in J$ platí, že $f_n \neq 0$, tak $1 \in J$ a teda $J = k[x_1, \ldots, x_n]$. Ak pre všetky $f \in J$ platí $f_n = 0$, potom $f \in \mathfrak{m}$ a máme tak $J = \mathfrak{m}$. Teda $\mathfrak{m}$ je maximálny ideál. □

VETA 1.76 (**Nullstellensatz, 3)**. *Ak pole k je algebraicky uzavreté, potom každý maximálny ideál v $k[x_1, \ldots, x_n]$ má tvar $(x_1 - a_1, \ldots, x_n - a_n)$ pre nejaké $a_1, \ldots, a_n \in k$.*

Príklad 1.77. Znovu, ak pole k nie je algebraicky uzavreté, tvrdenie neplatí. V okruhu $\mathbb{R}[x]$ je okrem ideálov $(x-a),\ a \in \mathbb{R}$ maximálnym napríklad aj ideál (x^2+1).

Tvrdenie 1.78. *Tvrdenie Nullstellensatz 3 je ekvivalentné tvrdeniam 1 a 2.*

Dôkaz. Nech platí tvrdenie 3. Nech $1 \notin I$. Nech $\mathfrak{m}$ je maximálny ideál obsahujúci I, teda podľa tvrdenia 3

$$I \subset \mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n).$$

Odtiaľ

$$\{(a_1, \ldots, a_n)\} = V(\mathfrak{m}) \subset V(I),$$

a teda $V(I) \neq \emptyset$.

Nech teraz platia tvrdenia 1 a 2. Nech $\mathfrak{m}$ je maximálny. Keďže $\sqrt{\mathfrak{m}} \supset \mathfrak{m}$, tak buď $\sqrt{\mathfrak{m}} = \mathfrak{m}$ alebo $\sqrt{\mathfrak{m}} = k[x_1, \ldots, x_n]$. Druhú možnosť môžme vylúčiť, pretože ak by nastala, znamenalo by to, že $1 \in \sqrt{\mathfrak{m}}$ a teda $1 \in \mathfrak{m}$. Nech $X = V(\mathfrak{m})$. Podľa Nullstellensatz 2 je X neprázdna, čiže existuje $(a_1, \ldots, a_n) \in X$. Z $\{(a_1, \ldots, a_n)\} \subset X = V(\mathfrak{m})$ potom vyplýva

$$\mathfrak{m} = \sqrt{\mathfrak{m}} = I(V(\mathfrak{m})) \subset I(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n),$$

a teda $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, keďže $\mathfrak{m}$ je maximálny. □

5.3. Algebraicko-geometrický „slovník". Z Hilbertovej Nullstellensatz vyplýva, že nad algebraicky uzavretým poľom máme bijekciu medzi algebraickými varietami a radikálovými ideálmi. Môžme si tak zostaviť akýsi prekladový slovník medzi algebrou a geometriou, ktorý sa nám vlastne začal črtať už na konci predchádzajúcej podkapitoly.

geometria	algebra
algebraické variety	radikály
X	$I(X)$
$V(I)$	I
bod	maximálny ideál
$X \subset Y$	$I(X) \supset I(Y)$
$V(I) \supset V(J)$	$I \subset J$
$X \cap Y$	$\sqrt{I(X) + I(Y)}$
$V(I) \cap V(J)$	$\sqrt{I + J}$
$X \cup Y$	$I(X) \cap I(Y) = \sqrt{I(X) \cdot I(Y)}$
$V(I) \cup V(J)$	$I \cap J = \sqrt{I \cdot J}$

Príklad 1.79. V $\mathbb{R}[x, y]$ majme ideál $I = (y - x^2, y - x^3)$. Chceme nájsť $V(I) \subset \mathbb{A}^2(\mathbb{R})$ a $\sqrt{I}$. Aj keď existujú postupy a algoritmy, ktoré by bolo možné použiť na vyriešenie takéhoto zadania, často bývajú veľmi komplikované, zdĺhavé, a niekedy fungujú len pri istých typoch ideálov/variet. Preto je veľmi vhodné predtým, ako po nich siahneme, v maximálnej miere využívať vlastnú invenciu a medódu pokus/omyl. Možný postup:

(1) načtrnúť si obrázok a odhadnúť $V(I)$,
(2) overiť odhad: vypočítať sústavu rovníc,
(3) odhadnúť $I(V(I)) = \sqrt{I}$,
(4) ukázať, že odhad bol správny.

KAPITOLA 2

Zariskiho topológia

1. Zariskiho topológia na $\mathbb{A}^n$

DEFINÍCIA 2.1. Nech X je množina a τ je systém podmnožín X, pre ktorý platí:

(i) $X \in \tau$, $\emptyset \in \tau$,
(ii) ak $U_1, U_2 \in \tau$, potom $U_1 \cap U_2 \in \tau$,
(iii) ak $U_i \in \tau$, $i \in \mathcal{I}$, potom $\bigcup_{i\in\mathcal{I}} U_i \in \tau$.

Potom τ je *topológia na* X a (X, τ) je topologický priestor. Množiny $U \in \tau$ nazývame *otvorenými množinami*. Naopak množina $V \subset X$ je *uzavretá*, ak $X \setminus V$ je otvorená.

POZNÁMKA 2.2. Ako býva zvykom, budeme v označení upúšťať od zdôrazňovania, že topologický priestor je dvojica (X, τ). Keď je z kontextu zrejmé, akú topológiu na množine X uvažujeme, budeme príslušný topologický priestor označovať jednoducho X.

Budeme 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 1.14 v kapitole o varietách a ideáoch (viď aj dôsledok tohto tvrdenia) 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. Pre zjednotenie máme

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

Bod $a \in \mathbb{A}^n$ zrejme patrí prieniku $\bigcap_{i\in\mathcal{I}} X_i$ práve vtedy, keď $f(a) = 0$ pre všetky $f \in \bigcup_{i\in\mathcal{I}} I_i$, teda $(\bigcup_{i\in\mathcal{I}} I_i)$ je ideál popisujúci algebraickú varietu $X = \bigcap_{i\in\mathcal{I}} X_i$, a teda

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

je naozaj otvorená množina.

Popíšeme si teraz túto topológiu na afinnej priamke a v afinnej rovine.

1.1. Zariskiho topológia na $\mathbb{A}^1(k)$. Algebraická varieta v $\mathbb{A}^1(k)$ je množina spoločných riešení niekoľkých polynomických rovníc: $X = V(f_1, \ldots, f_r),\ f_i \in k[x]$. Keďže však je $k[x]$ okruhom hlavných ideálov, určite existuje $f \in k[x]$ tak, že $(f_1, \ldots, f_r) = (f)$, a teda $X = V(f)$. Máme len dva zásadne rôzne prípady:

(a) Nech f je nulový polynóm, vtedy máme, že $X = V(0) = \mathbb{A}^1$.
(b) Nech f nie je nulový polynóm, vtedy $V(f)$ je konečná (možno i prázdna) podmnožina $\mathbb{A}^1$.

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

1.2. 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 $k[x, y]$ hlavný ideál zodpovedá rovinnej algebraicej krivke. Okruh $k[x, y]$ však už nie je okruhom hlavných ideálov, preto musíme preskúmať dôkladnejšie prípad, keď je ideál generovaný viacerými polynómami.

LEMA 2.3. *Nech $f, g \in k[x, y]$, $f, g \neq 0$, nech f je ireducibilný a nech g nie je deliteľný polynómom f. Potom f a g majú len konečne veľa spoločných koreňov.*

Dôkaz. Nech f obsahuje premennú x, t.j. $f \notin k[y]$. Polynómy f a g môžme chápať ako prvky $k(y)[x]$, teda ako polynómy jednej premennej nad poľom $k(y)$ všetkých racionálnych funkcií nad k.

Platí, že f je ireducibilný aj v $k(y)[x]$: sporom predpokladajme, že naopak $f = \tilde{f}_1\tilde{f}_2$, kde $\tilde{f}_1, \tilde{f}_2 \in k(y)[x]$, $\deg \tilde{f}_1 \geq 1$, $\deg \tilde{f}_2 \geq 1$ (myslí sa stupeň v x). Po vynásobení rovnosti najmenším spoločným násobkom menovateľov d dostaneme rovnosť polynómov v $k[x, y]$: $df = f_1 f_2$, kde $d \in k[y]$, $1 \leq \deg_x f_1 < \deg_x f$, $1 \leq \deg_x f_2 < \deg_x f$. Keďže f je ireducibilný, musí platiť $f|f_1$ alebo $f|f_2$, čo je vzhľadom na stupne týchto polynómov pri x spor.

Ďalej rovnakým spôsobom ukážeme, že g nie je deliteľný polynómom f ani v $k(y)[x]$ (dú).

Polynómy f a g sú preto aj v $k(y)[x]$ nesúdeliteľné. Keďže $k(y)[x]$ je euklidovský okruh, z Euklidovho algoritmu dostaneme vyjadrenie $\tilde{p}f + \tilde{q}g = 1$, kde $\tilde{p}, \tilde{q} \in k(y)[x]$. Znovu po vynásobení rovnosti najmenším spoločným násobkom menovateľov máme rovnosť polynómov

$$pf + qg = d,$$

kde $p, q \in k[x, y]$ a $d \in k[y]$. Ak (a_1, a_2) je spoločný koreň f a g, potom a_2 je koreňom polynómu d. Teda máme len konečne veľa možností, akú hodnotu môže nadobúdať druhá súradnica spoločného koreňa.

Tak isto ukážeme, že existuje len konečne veľa možností pre hodnotu prvej súradnice spoločného koreňa, čím je tvdrenie lemy dokázané. □

TVRDENIE 2.4. *Nech $f, g \in k[x, y]$ sú (nenulové) nesúdeliteľné polynómy. Potom $V(f, g) = V(f) \cap V(g)$ je konečná množina.*

Dôkaz. Nech $f = f_1^{e_1} \ldots f_r^{e_r}$ je ireducibilný rozklad polynómu f. Zrejme

$$V(f) = V(f_1^{e_1} \ldots f_r^{e_r}) = V(f_1 \ldots f_r) = V(f_1) \cup \cdots \cup V(f_r).$$

Teraz už len stačí aplikovať predchádzajúcu lemu na dvojice f_i, g pre $i = 1, \ldots, r$. □

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 konštanty 0, potom $X = V(0) = \mathbb{A}^2$.
(b) Nech $f_1, \ldots, f_r$ nie sú nulové polynómy. Môžme potom predpokladať, že žiaden z polynómov nie je nulový (po vynechaní nulového polynómu sa varieta nezmení). Predpokladajme, že tieto polynómy sú nesúdeliteľné. Potom podľa Tvrdenia 2.4 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 $f_1, \ldots, f_r$:

$$(f_1, \ldots, f_r) = (df_1', \ldots, df_r') = (d)(f_1', \ldots, f_r').$$

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 2.5. Tak ako vidno v prípade $\mathbb{A}^1$ a $\mathbb{A}^2$, aj v $\mathbb{A}^n$ platí, že neprázdne otvorené množiny v Zariskiho topológii sú veľmi veľké. Dokonca platí, že každé dve neprázdne otvorené množiny majú neprázdny prienik. Inými slovami, Zariskiho topológia nie je Hausdorffovská.

Poznámka 2.6. Zariskiho topológia je "najhrubšia" topológia (t.j. obsahuje najmenej otvorených množín), v ktorej sú polynomické funkcie spojité (viď Tvrdenie 1.20 v kapitole o varietách a ideáloch).

2. Rozklad variety na ireducibilné komponenty

Zariskiho topológiu môžme definovať aj na algebraickej variete, ide o tzv. *indukovanú topológiu*. V tejto topológii je množina $U \subset X (\subset \mathbb{A}^n)$ je otvorená, ak $U = U' \cap X$, kde U' je otvorená množina v $\mathbb{A}^n$. Uzavreté množiny na variete X sú teda jej podvariety. Takže každú afinnú algebraickú varietu môžme vnímať ako topologický priestor.

Definícia 2.7. Algebraická varieta X sa nazýva *reducibilná*, ak existujú algebraické variety X_1, X_2 také, že $X_1, X_2 \subsetneq X$ a $X_1 \cup X_2 = X$. V opačnom prípade sa varieta X nazýva *ireducibilnou*.

Definíciu reducibilnej a ireducibilnej variety je možné jednoducho preložiť do jazyka topológie:

Definícia 2.8. Hovoríme, že topologický priestor X je *reducibilný*, ak existujú $X_1, X_2 \subsetneq X$ uzavreté také, že $X = X_1 \cup X_2$. V opačnom prípade sa priestor X nazýva *ireducibilým*.

Definícia 2.9. Hovoríme, že topologický priestor X je *nesúvislý*, ak existujú $X_1, X_2 \subsetneq X$ uzavreté také, že $X_1 \cap X_2 = \emptyset$ a $X = X_1 \cup X_2$. V opačnom prípade sa priestor X nazýva *súvislým*.

Iná charakterizácia nesúvislého topologického priestoru je, že ide o priestor, ktorý sa dá napísať ako zjednotenie dvoch neprázdnych disjunktných otvorených množín. Je uzitočné si uvedomiť, že ide o ekvivalentné charakterizácie: aby množiny X_1, X_2 spĺňali podmienky Definície 2.9, musia byť obe súčasne uzavreté aj otvorené.

Poznámka 2.10. V topológii ste sa zrejme už stretli s pojmom súvislého/nesúvislého topologického priestoru, no možno už nie s pojmom reducibilného/ireducibilného. Pre ireducibilitu ste možno nemali dostatočne zaujímavý model. Skutočne, ak by sme na $\mathbb{A}^n(\mathbb{R})$ či $\mathbb{A}^n(\mathbb{C})$ ($n \geq 1$) uvažovali štandardnú euklidovskú topológiu, pojem reducibility je dosť nezaujímavý: afinný priestor je reducibilný, stačí ho ľubovoľnou nadrovinou rozdeliť na dva polpriestory a ku každému pridať i hranicu. Toto však nie je prípad Zariskiho topológie, ako čoskoro uvidíme.

Zjavne ireducibilný priestor je aj súvislý. Naopak to platiť nemusí.

Príklad 2.11.

- $X = V(x^2-y^2) \subset \mathbb{A}^2$ je súvislý reducibilný priestor: $X = V(x-y) \cup V(x+y)$, kde obe podmnožiny $V(x-y)$ aj $V(x+y)$ sú ireducibilné. (Dôsledné dokazovanie, že varieta je ireducibilná, zvládneme čoskoro.)
- $X = V(z - xy, y - y^2) \subset \mathbb{A}^3$ je nesúvislý reducibilný priestor.
- $X = V(xy, yz) \subset \mathbb{A}^3$ je súvislý reducibilný priestor. Všimnime si, že na strane variet platí $V(xy, yz) = V(x, z) \cup V(y)$, a na strane ideálov zas $(xy, yz) = (x, z) \cap (y)$.
- V špeciálnom prípade, keď X je konečná množina, tak ako topologický priestor je X ireducibilná práve vtedy, keď je súvislá.
- $X = V(y^2 - x^3 - x) \subset \mathbb{A}^2$ je súvislý ireducibilný priestor.

Veta 2.12. *Každá afinná algebraická varieta je zjednotením konečného počtu ireducibilných variet.*

Dôkaz. Nech X je varieta, pre ktorú tvrdenie vety neplatí. Teda X sa dá napísať ako $X_1 \cup X_1'$, pričom tvrdenie neplatí pre niektorú z týchto podvariet, nech je to X_1. Potom aj X_1 sa dá napísať ako $X_2 \cup X_2'$, kde zas pre niektorú z podvariet tvrdenie neplatí. Takto dostávame nekonečnú postupnosť variet

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq \dots.$$

Tejto postupnosti zodpovedá postupnosť ideálov

$$I(X) \subsetneq I(X_1) \subsetneq I(X_2) \subsetneq \dots,$$

čo je ale v spore s faktom, že $k[x_1, \dots, x_n]$ je noetherovský okruh. □

Definícia 2.13. Rozklad variety X na ireducibilné podvariety

$$X = X_1 \cup X_2 \cup \dots \cup X_r \tag{3}$$

sa nazýva *iredundantný* alebo *neskrátiteľný, minimálny*, ak pre žiadne i, j, $i \neq j$ neplatí $X_i \subset X_j$. V takomto rozklade potom nazývame jednotlivé ireducibilné podvariety *komponentami variety* X.

Inými slovami, rozklad variety je neskrátiteľný, ak žiadnu podvarietu nemôžeme zo zápisu (3) vynechať.

Veta 2.14. *Iredundantný rozklad variety na konečné zjednotenie ireducibilných podvariet je jednoznačný.*

Dôkaz. Nech $X = X_1 \cup X_2 \cup \dots \cup X_r$ a tiež $X = X_1' \cup X_2' \cup \dots \cup X_s'$ sú neskrátiteľné rozklady variety V. Platí

$$X_j = X_j \cap X = X_j \cap (X_1' \cup X_2' \cup \dots \cup X_s') = \bigcup_{i=1}^{s} (X_j \cap X_i').$$

Keďže X_j je ireducibilná, tak $X_j = (X_j \cap X_i')$ pre nejaké i, a teda $X_j \subset X_i'$. Podobne ukážeme, že $X_i' \subset X_l$ pre nejaké l. Odtiaľ potom $X_j \subset X_l$. Z neskrátiteľnosti rozkladu potom máme $X_l = X_i$ a teda aj $X_i' = X_j$. Takto ukážeme pre každú komponentu, že sa nachádza v oboch rozkladoch. Odtiaľ potom už vyplýva tvrdenie vety. □

Teraz chceme skúmať, ako sa reducibilnosť či ireducibilnosť algebraickej variety odrazí na strane ideálov.

Pripomeňme, že ideál $I \subset R$ v okruhu R sa nazýva *prvoideálom*, ak pre všetky $f, g \in R$ také, že $fg \in R$ platí, že $f \in R$ alebo $g \in R$.

PRÍKLAD 2.15. V okruhu $\mathbb{Z}$ je (p) prvoideálom práve vtedy, keď je p prvočíslo.

PRÍKLAD 2.16. V okruhu $\mathbb{C}[x]$ máme:

- $(x^2 - 1)$ nie je prvoideál,
- $(x - 1)$ je prvoideál.

TVRDENIE 2.17. *V okruhu $k[x_1, x_2, \ldots, x_n]$ je (f) prvoideálom práve vtedy, keď je f ireducibilným polynómom.*

Dôkaz. Nech f nie je ireducibilný: $f = f_1 f_2$, $\deg f_i \geq 1$. Vtedy $f_1 f_2 \in (f)$, ale $f_1 \notin (f)$, $f_2 \notin (f)$: keby platilo $f_1 \in (f)$, teda $f_1 = gf$ pre nejaké $g \in k[x_1, x_2, \ldots, x_n]$. Vtedy $f_1 = gf = gf_1 f_2 = (gf_2) f_1$, teda gf_2 je konštanta, čo však nie je možné, lebo $\deg f_2 \geq 1$.

Nech f je ireducibilný a nech $f_1 f_2 \in (f)$, teda $f_1 f_2 = hf$ pre nejaké $h \in k[x_1, x_2, \ldots, x_n]$. Z ireducibility f potom ale máme, že $f \mid f_1$ alebo $f \mid f_2$, čo ale znamená, že $f_1 \in (f)$ alebo $f_2 \in (f)$, teda (f) je prvoideál. □

TVRDENIE 2.18. *Nech $X \subset \mathbb{A}^n(k)$ Nasledovné tvrdenia sú ekvivalentné:*

(i) *X je ireducibilná varieta.*
(ii) *$I(X)$ je prvoideál.*
(iii) *$k[x_1, \ldots, x_n]/I(X)$ je oborom integrity (okruhom bez deliteľov nuly).*

Dôkaz. (i)⇒(ii) Nech X je ireducibilná varieta a nech $fg \in I(X)$. Označme

$$X_1 = X \cap V(f) \quad \text{a} \quad X_2 = X \cap V(g).$$

Potom zrejme $X_1 \cup X_2 \subset X$. Tiež platí, že $X \subset X_1 \cup X_2$ lebo $fg \in I(X)$: keďže $(fg)(a) = 0$ pre $a \in X$, tak platí $f(a) = 0$ (a teda $a \in X_1$) alebo $g(a) = 0$ (a teda $a \in X_2$). Ďalej z faktu, že X je ireducibilná, musí platiť, že $X = X_1$ alebo $X = X_2$; nech $X = X_1 = X \cap V(f)$, teda $X \subset V(f)$, odtiaľ $f \in I(X)$, a teda $I(X)$ je prvoideál.

(ii)⇒(i) Nech $I(X)$ je prvoideál a nech $X = X_1 \cup X_2$. Nech $X_1 \neq X$, teda existuje $f \in I(X_1)$, $f \notin I(X)$. Nech $g \in I(X_2)$ je ľubovoľný. Potom $fg \in I(X)$ a teda $f \in I(X)$ alebo $g \in I(X)$, čiže $g \in I(X)$. Takže $I(X) = I(X_2)$ a preto $X = X_2$, čiže X je ireducibilná.

(iii) je v podstate len preformulovaním tvrdenia (ii): Nech $I(X)$ nie je prvoideál, t.j. existujú f, g také, že $f \notin I(X), g \notin I(X)$ a $fg \in I(X)$. Potom f, g chápané ako prvky $k[X]$ sú nenulové, a s nulovým súčinom. Naopak, nech $f, g \in k[X]$ sú delitele nuly, t.j. $f, g \notin I(X)$ a $fg \in I(X)$, čo však znamená, že $I(X)$ nie je prvoideál. □

PRÍKLAD 2.19. Pre ireducibilné variety v Príklade 2.11 teraz už vieme ukázať, že sú naozaj ireducibilné. Podobne o redicibilných varietách, že komponenty v rozklade sú naozaj ireducibilné.

PRÍKLAD 2.20. Afinný priestor $\mathbb{A}^n$ je ireducibilný. Pre $\mathbb{A}^1$ a $\mathbb{A}^2$ to vyplýva už z našej znalosti Zariskiho topológie. Všeobecne pre $\mathbb{A}^n$ z faktu, že $I(\mathbb{A}^n) = (0)$, a vieme, že (0)

je prvoideál. Ekvivalentne (viď Tvrdenie 2.18):

$$k[x_1, \ldots, x_n]/I(\mathbb{A}^n) = k[x_1, \ldots, x_n]/(0) = k[x_1, \ldots, x_n]$$

nemá delitele nuly.

Príklad 2.21. Prienik ireducibilných variet nemusí byť ireducibilná varieta. Teda ireducibilné polynómy nemusia určovať ireducibilnú varietu: $V(xy - z^2, z)$ je reducibilná.

KAPITOLA 3

Afinné variety

1. Podielové okruhy (opakovanie)

DEFINÍCIA 3.1. Nech R_1, R_2 sú komutatívne okruhy s jednotkou. Zobrazenie $\varphi\colon R_1 \to R_2$ sa nazýva *homomorfizmus okruhov*, ak pre všetky $u, v \in R_1$ platí

- $\varphi(u+v) = \varphi(u) + \varphi(v)$,
- $\varphi(u \cdot v) = \varphi(u) \cdot \varphi(v)$,
- $\varphi(1_{R_1}) = 1_{R_2}$.

Nech R je okruh a $I \subset R$ je ideál. Potom R/I je tiež okruh, v ktorom sú dobre definované operácie + a .

DEFINÍCIA 3.2. Nech I je ideál v okruhu R. Okruh R/I nazývame *podielový* alebo *faktorový okruh*. Homomorfizmus $\varphi\colon R \to R/I$, $u \mapsto [u] = u + I$ sa nazýva *projekcia* R *na* R/I.

PRÍKLAD 3.3. Nech $R = \mathbb{Z}$ a nech $n \in \mathbb{Z}$. Potom $\mathbb{Z}/(n) = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ je podielový okruh, kde operácie + a . sa vykonávajú modulo n.

2. Regulárne funkcie na afinných varietách, regulárne zobrazenia variet

Odteraz k bude algebraicky uzavreté pole, a teda platí Hilbertova Nullstellensatz.

2.1. Regulárne funkcie.

DEFINÍCIA 3.4. Nech $X \subset \mathbb{A}^n(k)$ je afinná algebraická varieta. Funkcia $f : X \to k$ sa nazýva *regulárna funkcia na* X, ak existuje polynóm $F \in k[x_1, \ldots, x_n]$ taký, že $f(a) = F(a)$ pre všetky $a \in X$.

DEFINÍCIA 3.5. Množinu všetkých regulárnych funkcií na variete $X \subset \mathbb{A}^n$ nazývame *súradnicovým okruhom variety* X a označujeme $k[X]$.

PRÍKLAD 3.6. Polynóm F v definícii regulárnej funkcie nie je určený jednoznačne. Napríklad na kružnici $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2$ polynómy $F_1 = 1$ a $F_2 = x^2 + y^2$ popisujú tú istú regulárnu funkciu.

Pozorovanie z príkladu môžme zovšeobecniť. Nech $F \in k[x_1, \ldots, x_n]$ popisuje nejakú regulárnu funkciu na variete X a nech $G \in k[x_1, \ldots, x_n]$ je taký polynóm, že $G(a) = 0$ pre všetky $a \in X$, čiže $G \in I(X)$. Potom $F + G$ popisuje na X tú istú regulárnu funkciu ako F.

Algebraicky tak máme zobrazenie, ktoré $k[x_1, \ldots, x_n]$ zobrazuje na regulárne funkcie na X, $\pi\colon k[x_1, \ldots, x_n] \to k[X]$, kde π je reštrikcia polynómu na X. Toto zobrazenie je zjavne homomorfizmom okruhov. Jeho jadrom sú presne funkcie, ktorých hodnota všade na X je 0, t.j. je to ideál $I(X)$, ideál variety X. Ak $X = V(I)$, tak z Hilbertovej Nullstellensatz $I(X) = \sqrt{I}$.

Z predchádzajúcej diskusie tak máme

$$k[X] \cong k[x_1, \ldots, x_n]/I(X).$$

Často sa práve takto súradncový okruh variety definuje. Aj my budeme odteraz namiesto izomorfizmu písať v tomto vyjadrení rovnosť.

PRÍKLAD 3.7. Na jednotkovej kružnici $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2(k)$ je funkcia

$$f : \ X \to k, \quad (x, y) \mapsto x^2$$

totožná s funkciou

$$g : \ X \to k, \quad (x, y) \mapsto 1 - y^2.$$

Inak povedané, polynómy x^2 a $1 - y^2$ sú dva rôzne reprezentanty ten istej regulárnej funkcie v $k[X] = k[x, y]/(x^2 + y^2 - 1)$.

PRÍKLAD 3.8. Ak $X = \mathbb{A}^n(k)$, potom $k[X] = k[x_1, \ldots, x_n]$, lebo $I(\mathbb{A}^n) = 0$.

PRÍKLAD 3.9. Ak X je jeden bod, potom $k[X] = k$.

PRÍKLAD 3.10. Nech $X = V(xy - 1) \subset \mathbb{A}^2$. Potom

$$k[X] = k[x, y]/(xy - 1) \cong k[x, x^{-1}],$$

a teda pozostáva z racionálnych funkcií tvaru $G(x)/x^n$, kde $G(x)$ je polynóm v x.

PRÍKLAD 3.11. Nech $X = V(y^2 - x^3)$. Potom každú funkciu f z $k[X]$ môžme jednoznačne napísať v tvare $f = F_0(x) + yF_1(x)$, kde $F_0, F_1, \in k[x]$. Vyplýva to z faktu, že polynóm $G_0(x) + yG_1(x)$ reprezentuje nulu v $k[X]$ práve vtedy, keď G_0 a G_1 sú nulové polynómy v $k[x]$.

TVRDENIE 3.12. *Nech $X \subset \mathbb{A}^n$ je algebraická varieta. Potom jej súradnicový okruh $k[X] = k[x_1, \ldots, x_n]/I(X)$ je noetherovský.*

Dôkaz. Nech $J \subset k[X]$ je ideál. Potom $\pi^{-1}(J)$ je ideál v $k[x_1, \ldots, x_n]$, kde π je kanonická projekcia $k[x_1, \ldots, x_n] \to k[X]$. Keďže $k[x_1, \ldots, x_n]$ je noetherovský, máme $\pi^{-1}(J) = (F_1, \ldots, F_r)$ pre nejaké $F_1 \ldots, F_r \in k[x_1, \ldots, x_n]$. Odtiaľ ľahko ukážeme, že $J = (f_1, \ldots, f_r)$, kde $f_i = \pi(F_i)$: ak $f \in J$, potom $f = \pi(F)$ pre nejaké $F \in \pi^{-1}(J)$, teda $F = G_1F_1 + \ldots G_rF_r$ pre nejaké $G_1, \ldots, G_r \in k[x_1, \ldots, x_n]$, a preto $f = g_1f_1 + \cdots + f_rg_r$, kde $g_i = \pi(f_i)$. □

POZNÁMKA 3.13. Vďaka súradnicovému okruhu variety a faktu, že je noetherovský, si môžme na ľubovoľnej algebraickej variete definovať Zariskiho topológiu. Uzavreté množiny v nej budú spoločné korene danej sady regulárnych funkcií na X. Inak povedané, každému ideálu $J \subset k[X]$ priradíme uzavretú množinu pozostávajúcu z takých bodov a na X, pre ktoré platí, že $f(a) = 0$ pre všetky $f \in J$. Je len uvedomovacím cvičením si všimnúť, že je to presne tá istá topológia, ktorú sme získali reštrikciou Zariskiho topológie v $\mathbb{A}^n$ na varietu X (indukovaná topológia).

2.2. Regulárne zobrazenia afinných variet.

DEFINÍCIA 3.14. Nech $X \subset \mathbb{A}^n$ je afinná algebraická varieta. Zobrazenie $f : \ X \to \mathbb{A}^m$ je *regulárne (morfizmus)*, ak existuje m regulárnych funkcií $f_1, \ldots, f_m$ na X tak, že $f(a) = (f_1(a), \ldots, f_m(a))$ pre všetky $a \in X$.

Zjednodušene povedané, zobrazenie $X \to \mathbb{A}^m$ je regulárne, ak je na úrovni súradníc popísané polynomicky. Presne ako pri regulárnych funkciách, ani tu nemáme bijekciu medzi morfizmami $X \to \mathbb{A}^m$ a m-ticami polynómov s n premennými: dve rôzne m-tice polynómov môžu popisovať ten istý morfizmus.

PRÍKLAD 3.15. Afinné zobrazenie $\mathbb{A}^n \to \mathbb{A}^m$ je regulárnym zobrazením.

PRÍKLAD 3.16. Funkcia na X je zobrazenie $X \to \mathbb{A}^1$.

PRÍKLAD 3.17. Premietanie na prvú súradnicu $(a, b) \mapsto (a)$ je regulárnym zobrazením (= morfizmom), ktoré zobrazí hyperbolu $X = V(xy-1)$ na afinnú priamku, t.j. ide o zobrazenie $X \to \mathbb{A}^1$. Jeho obrazom je priamka bez bodu (0).

DEFINÍCIA 3.18. Nech $X \subset \mathbb{A}^n$ a $Y \subset \mathbb{A}^m$ sú afinné algebraické variety, a nech $f : X \to \mathbb{A}^m$ je morfizmus (regulárne zobrazenie). Ak $f(X) \subset Y$ (t.j. ak pre všetky $a \in X$ je $f(a) \in Y$), tak f je *regulárnym zobrazením (morfizmom)* variety X do variety Y, $f : X \to Y$.

PRÍKLAD 3.19. Uvažujme zobrazenie $f : \mathbb{A}^1 \to \mathbb{A}^2$ dané predpisom $(a) \mapsto (a^2, a^3)$. Obrazom tohto zobrazenia je krivka $V(y^2 - x^3) \subset \mathbb{A}^2$. Ide teda aj o zobrazenie $\mathbb{A}^1 \to V(y^2 - x^3)$.

DEFINÍCIA 3.20. Regulárne zobrazenie $f : X \to Y$ je *izomorfizmus*, ak existuje regulárne zobrazenie $g : Y \to X$ také, že $g \circ f = \mathrm{id}_X$ a $f \circ g = \mathrm{id}_Y$. Vtedy hovoríme, že X a Y sú *izomorfné*.

PRÍKLAD 3.21. Parabola $X = V(y-x^2)$ a afinná priamka sú izomorfné: $f : \mathbb{A}^1 \to X$, $(a) \mapsto (a, a^2)$, inverzným zobrazením je $g : X \to \mathbb{A}^1$, $(a, b) \mapsto (a)$.

PRÍKLAD 3.22. Všeobecnejšie, graf ľubovoľnej polynomickej funkcie je izomorfný s afinnou pramkou.

PRÍKLAD 3.23. Zobrazenie $f : \mathbb{A}^1 \to X$, kde $X = V(y^2 - x^3)$ dané predpisom $(a) \mapsto (a^2, a^3)$ je síce regulárne, aj bijekcia, ale nie je to izomorfizmus. Aby sme sa o tom presvedčili, pokúsime sa nájsť inverzné zobrazenie $g : X \to \mathbb{A}^1$. Podľa príkladu 3.11 toto zobrazenie môžme hľadať v tvare $g(x, y) = g_0(x) + yg_1(x)$, kde $f_0, f_1 \in k[x]$. Keďže f a g majú byť navzájom inverzné, musí platiť, že $g(f(a)) = a$ pre všetky $a \in \mathbb{A}^1$. Ale

$$g(f(a)) = g(a^2, a^3) = g_0(a^2) + a^3 g_1(a^2).$$

Prvý sčítanec na pravej strane obsahuje len členy párneho stupňa, druhý sčitanec obsahuje členy nepárneho stupňa počnúc stupňom 3. Teda $g \circ f \neq \mathrm{id}$, inverzný morfizmus neexistuje.

2.3. Pullback regulárnej funkcie na variete. Každej afinnej algebraickej variete sme priradili jej súradnicový okruh, t.j. okruh všetkých regulárnych funkcií na variete. Teraz budeme skúmať, aký je vzťah medzi súradnicovými okruhmi, pokiaľ máme morfizmus (či dokonca izomorfizmus) medzi varietami.

Ak $f\colon X \to Y$ je morfizmus variet, potom vieme nájsť zobrazenie aj medzi ich súradnicovými okruhmi. Konkrétne, ak $u \in k[Y]$, t.j. $u\colon Y \to k$, potom zložením týchto dostávame fukciu $u \circ f\colon X \to k$.

TVRDENIE 3.24. *Nech $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ sú afinné algebraické variety.*

- *Nech $f : X \to Y$ je morfizmus variet. Potom f indukuje homomorfizmus ich súradnicových okruhov: $f^* : k[Y] \to k[X]$, $f^*(u) := u \circ f$.*
- *Pre každý homomorfizmus φ súradnicových okruhov dvoch algebraických variet $k[Y] \to k[X]$ fixujúci pole k existuje morfizmus variet $f : X \to Y$ taký, že $\varphi = f^*$.*

DEFINÍCIA 3.25. Homomorfizmus súradnicových okruhov f^* z tvrdenia prislúchajúci morfizmu $f : X \to Y$ nazývame *pulbackom* morfizmu f.

Dôkaz. Ak $u \in k[Y]$, t.j. u je funkcia $Y \to k$ daná polynomicky, potom $f^*(u) = u \circ f$ je funkcia $X \to k$ a zrejme je tiež daná polynomicky, keďže je zložením dvoch polynomických zobrazení. Rozpísané do detailov, ak $f : X \to Y$ je dané

$$f = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

kde $f_i \in k[X]$ a $u \in k[Y]$, $u = u(y_1, \ldots, y_m)$, tak

$$f^*(u) = u(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)).$$

Zobrazenie $f^* : k[Y] \to k[X]$ je homomorfizmom okruhov (len mechanické rozpisovanie).

Naopak, nech $\varphi : k[Y] \to k[X]$ je homomorfizmus okruhov. Nájdeme $f : X \to Y$ morfizmus taký, že $\varphi = f^*$.

Nech $y_1, \ldots, y_m$ sú funkcie jednotlivých súradníc v $\mathbb{A}^m$ (projekcie na príslušnú súradnicu) chápané ako prvky okruhu $k[Y]$. Označme $f_1 = \varphi(y_1), \ldots, f_m = \varphi(y_m)$; zrejme $f_1, \ldots, f_m \in k[X]$. Pre zobrazenie $f = (f_1, \ldots, f_m) : X \to \mathbb{A}^m$ potom platí, že $f^* = \varphi$, keďže obidva homomorfizmy sú zhodné na generátoroch okruhu $k[Y]$:

$$f^*(y_i) = y_i \circ f = f_i = \varphi(y_i).$$

Ostáva ukázať ešte, že $f(X) \subset Y$.

Nech $G \in I(Y)$, t.j. ak G chápeme ako prvok v $k[Y]$, tak $G = 0$. Preto $\varphi(G) = 0$ v $k[X]$. Nech teraz $a \in X$. Tento bod sa v zobrazení f zobrazí na $f(a) = (f_1(a), \ldots, f_m(a))$. Potom platí, že $G(f(a)) = (G \circ f)(a) = (\varphi(G))(a) = 0$. □

Dôsledok. *Zobrazenie $f : X \to Y$ je izomorfizmus afinných variet práve vtedy, keď $f^* : k[Y] \to k[X]$ je izomorfizmus okruhov. Variety X, Y sú izomorfné práve vtedy, keď ich súradicové okruhy sú izomorfné.*

Príklad 3.26. Nie je možné nájsť izomorfizmus $X = V(y^2 - x^3)$ a afinnej priamky $\mathbb{A}^1$. Z príkladu 3.11 totiž vyplýva, že $k[X]$ a $k[\mathbb{A}^1] = k[x]$ nie sú izomorfné.

Máme teda "pekné" zobrazenie $X \mapsto k[X]$ afinných algebraických variet do okruhov (vnorenie jednej kategórie do druhej): namiesto afinných variet môžme pracovať s okruhmi, namiesto morfizmov variet s homomorfizmami okruhov, kde izomorfizmus variet zodpovedá izomorfizmu okruhov.

Definícia 3.27. Izomorfizmus $f : X \to X$ sa nazýva *automorfizmom X*.

Automorfizmus variety X zodpovedá automorfizmu jeho súradnicového okruhu. Špeciálne môžme skúmať napríklad všetky automorfizmy afinnej priamky:

Príklad 3.28. Nech $\mathbb{A}^1 \to \mathbb{A}^1$ je automorfizmus. Na strane súradnicových okruhov mu zodpovedá automorfizmus okruhu $k[\mathbb{A}^1] = k[x]$, označme ho $\alpha : k[x] \to k[x]$. Obrazom x v tomto automorfizme je polynóm $\alpha(x)$. Potom $\alpha(x)$ musí generovať celý okruh $k[x]$, špeciálne x sa musí dať vyjadriť pomocou $\alpha(x)$: $x = p(\alpha(x)) = (p \circ \alpha)(x)$, kde p je polynóm o jednej premennej. Špeciálne musí teda platiť, že $\deg(p \circ \alpha) = \deg x = 1$, kde $p \circ \alpha$ je polynóm, ktorý získame zložením polynómov p a α, a teda $\deg(p \circ \alpha) = \deg p . \deg \alpha$. Odtiaľ máme, že $\deg \alpha = 1$, a preto všetky automorfizmy $\mathbb{A}^1$ sú tvaru $x \mapsto ax + b$, kde $a, b \in k$, $a \neq 0$, ide teda o množinu bijektívnych afinných zobrazení $\mathbb{A}^1 \to \mathbb{A}^1$.

Príklad 3.29. Afinná rovina $\mathbb{A}^2$ má zaujímavejšiu grupu automorfizmov ako afinná priamka. Sú to jednak afinné zobrazenia, potom zobrazenia tvaru $(x, y) \mapsto (x, y + f(x))$, $f \in k[x]$, a nakoniec všetky ich kombinácie (bez dôkazu).

3. Racionálne funkcie na variete, racionálne zobrazenia

3.1. Racionálne funkcie na variete. Rozlišovanie variet podľa izomorfizmu je príliš jemné. Chceme väčšiu triedu zobrazení než morfizmy, chceme pripustiť aj racionálne zobrazenia.

Bohužiaľ ale nie je možné tvoriť zlomky z regulárnych funkcií na ľubovoľnej variete:

Príklad 3.30. $X = V(x^2 - y^2) \subset \mathbb{A}^2$. Uvažujme na tejto variete regulárne funkcie $f = x + y$ a $g = x - y$. Obe funkcie sú nenulové, avšak ich súčin je v $k[X]$ nulový, ide o tzv. *delitele nuly*. Teda tieto funkcie sa nesmú vyskytnúť v menovateli, lebo by sme potom do menovateľa dostali aj nulu.

Problém v príklade bol spôsobený faktom, že varieta X bola reducibilná. Ak by sme však pripustili len ireducibilné variety, potom problém s deliteľmi nuly nenastane (viď Tvrdenie 2.18 predchádzajúcej kapitoly).

Definícia 3.31. Nech R je obor integrity. *Podielovým poľom* oboru R nazývame množinu

$$\{(u, v) \mid u, v \in R, v \neq 0\}/_\sim,$$

kde $(u_1, v_1) \sim (u_2, v_2)$ práve vtedy, keď $u_1v_2 - u_2v_1 = 0$. Násobenie a sčítanie v podielovom poli definujeme:

$$\begin{aligned}(u_1, v_1).(u_2, v_2) &= (u_1u_2, v_1v_2)\\ (u_1, v_1) + (u_2, v_2) &= (u_1v_2 + u_2v_1, v_1v_2)\end{aligned}$$

Dvojicu (u, v) tiež zapisujeme u/v.

Zrejme obor integrity R je podmnožinou svojho podielového poľa:

$$R = \{(a, 1) \mid a \in R\}.$$

Definícia 3.32. Nech X je ireducibilná varieta. Potom podielové pole súradnicového okruhu $k[X]$ nazývame *poľom racionálnych funkcií* variety X, označujeme ho $k(X)$.

Z definície súradnicového okruhu a podielového poľa máme, že F_1/G_1 a F_2/G_2 reprezentujú tú istú racionálnu funkciu, ak $F_1G_2 - F_2G_1 \in I(X)$.

Racionálna funkcia na variete nie je všadedefinovaným zobrazením. Nemusí však byť úplne zjavné, kde je daná racionálna funkcia definovaná a kde nie.

Príklad 3.33. Nech $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2(k)$. Zistíme, v ktorých bodoch kružnice je definovaná funkcia $(x+1)/y$. Určite je definovaná v bodoch, kde $y \neq 0$, teda všade okrem $(1, 0)$ a $(-1, 0)$. Ďalej platí

$$\frac{x+1}{y} = \frac{y(x+1)}{y^2} = \frac{y(x+1)}{1-x^2} = \frac{y(x+1)}{(1-x)(1+x)} = \frac{y}{1-x},$$

a teda funkcia je definovaná aj v bode $(-1, 0)$. (Môžte sa tiež priamo z definície podielového poľa súradnicového okruhu presvedčiť, že $(x + 1)/y$ a $y/(1 - x)$ definujú tú istú funkciu na X.)

Definícia 3.34. Nech r je racionálna funkcia na variete X a nech $a \in X$. Funkcia r sa nazýva *regulárnou v bode* x, ak existujú také $f, g \in k[X]$, že $r = f/g$ a $g(a) \neq 0$.

Tvrdenie 3.35. *Ak r je racionálna funkcia na X, ktorá je regulárna vo všetkých bodoch variety X, potom r je regulárna funkcia, t.j. $r \in k[X]$.*

Dôkaz. Z predpokladu tvrdenia pre každý bod $a \in X$ máme $p_a, q_a \in k[X]$ také, že $r = p_a/q_a$, pričom $q_a(a) \neq 0$. Nech I je ideál generovaný všetkými menovateľmi: $I = (q_a \mid a \in X)$. Pretože $k[X]$ je noetherovský, platí, že $I = (q_1, \ldots, q_s)$ pre nejaké $q_1, \ldots, q_s \in k[X]$. Ďalej $q_1, \ldots, q_s$ nemajú spoločný koreň v X, pretože potom by funkcia r nemala v tomto bode regulárnu reprezenáciu. Ak $X = V(F_1, \ldots, F_r) \in \mathbb{A}^n$, potom v okruhu $k[x_1, \ldots, x_n]$ to podľa Nullstellensatz znamená, že $1 \in (Q_1, \ldots, Q_s, F_1, \ldots, F_r)$, kde Q_i je polynóm v $k[x_1, \ldots, x_n]$ reprezentujúci q_i. Máme tak

$$1 = G_1Q_1 + \cdots + G_sQ_s + H_1F_1 + \cdots + H_rF_r$$

pre nejaké $G_i, H_i \in k[x_1, \ldots, x_n]$. Po premietnutí do okruhu $k[X]$ dostávame

$$1 = g_1q_1 + \cdots + g_sq_s$$

a následne po vynásobení tejto rovnosti funkciou r máme

$$r = g_1p_1 + \cdots + g_rp_r,$$

čiže $r \in k[X]$. □

3.2. Racionálne zobrazenia variet.

Definícia 3.36. Nech $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ sú afinné algebraické variety. *Racionálne zobrazenie* $f : X \to Y$ je m-tica racionálnych funkcií $(f_1, \ldots, f_m)$, pre ktorú platí, že ak všetky f_i sú regulárne v $a \in X$, tak $f(a) \in Y$. Vtedy hovoríme, že zobrazenie f je *regulárne v bode* a a bod $f(a) = (f_1(a), \ldots, f_m(a))$ nazývame *obrazom bodu* a.

Morfizmy variet $X \to Y$ sú podľa tejto definície a podľa Tvrdenia 3.35 zrejme racionálne zobrazenia, ktoré sú regulárne vo všetkých bodoch variety X.

Definícia 3.37. Racionálne zobrazenie $f : X \to Y$ je *dominantné*, ak množina $f(X)$ je hustá v Y.

Definícia 3.38. Racionálne zobrazenie $f : X \to Y$ je *biracionálne* alebo tiež *biracionálna ekvivalencia*, ak je dominantné a existuje dominantné racionálne zobrazenie $g : Y \to X$ také, že $f \circ g = \mathrm{id}_Y$ a $g \circ f = \mathrm{id}_X$ všade, kde sú definované. Variety X a Y sa vtedy nazývajú *biracionálne ekvivalntné*.

Príklad 3.39. Videli sme už, že kubická krivka s hrotom 3.11 síce nie je izomorfná s afinnou priamkou, no je s ňou biracionálna. Inverzné zobrazenie k zobrazeniu $f : \mathbb{A}^1 \to X$, $(a) \mapsto (a^2, a^3)$ je racionálne zobrazenie $(x, y) \mapsto y/x$.

Príklad 3.40. Projekcia hyperboly $V(xy - 1) \subset \mathbb{A}^2$ na afinnú priamku $\mathbb{A}^1$ (viď Príklad 3.17) je biracionálny morfizmus: invezným zobrazením je racionálne zobrazenie $(a) \mapsto (a, 1/a)$.

Veta 3.41. *Variety X a Y sú biracionálne ekvivalentné práve vtedy, keď ich polia racionálnych funkcií sú navzájom izomorfné.*

Dôkaz. Nech $f : X \to Y$ je biracionálna ekvivalencia, teda $f(X)$ je hustá v Y. Pre každú regulárnu funkciu $u \in k[Y]$ potom máme, že $u \circ f \in k(X)$ (ide o dosadzovanie racionálnych funkcií do f), toto zobrazenie budeme ako pri morfizmoch nazývať pullbackom f a označovať f^*. Zrejme f^* je homomorfizmom $k[Y] \to k(X)$. Overíme, že ide dokonca o vnorenie $k[Y]$ do $k(X)$.

Nech $f^*(u) = 0$ pre nejaké $u \in k[Y]$, t.j. $u \circ f(a) = 0$ pre všetky $a \in X$. Inými slovami to znamená, že funkcia u je nulová na $f(X)$. Ak u nie je nulová funkcia na Y,

potom $V(u)$ je uzavretá vlastná podmožina Y obsahujúca $f(X)$, čo je ale v rozpore s predpokladom, že f je dominantné zobrazenie.

Teda f^* je vnorenie $k[Y] \hookrightarrow k(X)$, a toto sa jednoznačne rozširuje na vnorenie $k(Y) \hookrightarrow k(X)$. Podobne ak $g : Y \to X$ je dominantné a $f \circ g$, $g \circ f$ sú identity na svojich definičných oboroch, máme tak, že $f^* : k(Y) \to k(X)$ je izomorfizmus polí.

Nech teraz naopak $\alpha : k(Y) \to k(X)$ je izomorfizmom polí racionálnych funkcií variet $X \subset \mathbb{A}^n$ a $Y \subset \mathbb{A}^m$. Presne ako v prípade morfizmov pomocou α zostrojíme zobrazenie $f : X \to Y$ také, že $\alpha = f^*$: zobrazenie f bude dané racionálnymi funkciami $f_i = \alpha(y_i)$, kde $y_i \in k[Y]$ je funkcia i-tej súradnice. Tak ako v prípade morfizmov, aj tu ľahko overíme, že $f^* = \alpha$ a tiež, že $f(X) \subset Y$. Z vlastnosti, že α je injektívne zobrazenie, usúdime, že f je dominantné. Rovnakým spôsobom nájdeme racionálne zobrazenie $g : Y \to X$ a následne ukážeme, že f je biracionálna ekvivalencia. □

Príklad 3.42. Súradnicové okruhy hyperboly (viď Príklad 3.10) a afinnej priamky sú rôzne, teda tieto variety nie sú izomorfné. No ich podielové polia izomorfné sú, teda variety sú biracionálne ekvivalentné, ako sme už videli v Príklade 3.40.

Definícia 3.43. Algebraická varieta, ktorá je biracionálne ekvivalentná $\mathbb{A}^n$ pre nejaké n, sa nazýva *racionálna*.

Príklad 3.44. Kružnica $X = V(x^2 + y^2 - 1)$ je racionálna krivka. Príslušné zobrazenia získame pomocou *stereografickej projekcie*: Nech $(a, b) \in X$ je pevne zvolený bod na krivke, napr. $(a, b) = (0, 1)$. Ďalej si pevne zvolíme v rovine priamku, napr. x-os. Bodom $(0, 1)$ budeme prekladať priamky. Každá taká priamka pretína kružnicu v dvoch bodoch: jedným z nich je bod $(0, 1)$, druhým je bod, ktorý biracionálnou ekvivalenciou previažeme s bodom na x-osi.

Priamka cez $(0, 1)$ a $(t, 0)$ má rovnicu $x + t(y - 1) = 0$. Jej prienik s kružnicou je bod

$$\left(\frac{2t}{t^2 + 1}, \frac{t^2 - 1}{t^2 + 1} \right),$$

čím máme dané zobrazenie $\mathbb{A}^1 \to X$. Inverzné zobrazenie $X \to \mathbb{A}^1$ nájdeme analogicky:

$$(x, y) \mapsto \frac{x}{1 - y}.$$

KAPITOLA 4

Gröbnerove bázy

1. Usporiadanie monómov

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

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

Definícia 4.1. Reláciu $>$ budeme nazývať *usporiadanie monómov*, ak

- $>$ je lineárne usporiadanie monómov (je tranzitívne a 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

$$x^\alpha > x^\beta > x^\gamma > \ldots \tag{4}$$

je konečná. Naozaj, majme klesajúcu postupnosť monómov (4). Ak táto postupnosť je nekonečná, potom množina $\{x^\alpha, x^\beta, x^\gamma, \ldots\}$ 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 ($\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in (\mathbb{N}_0)^n$) 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 $\alpha - \beta = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ je kladné.

Príklad 4.2. V lexikografickom usporiadaní máme

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

Tvrdenie 4.3. *Lexikografické usporiadanie je usporiadanie monómov.*

Dôkaz. Každé dva rôzne monómy vieme porovnať: ak $x^\alpha \neq x^\beta$, čiže $\alpha \neq \beta$, potom existuje $i \in \{1, \ldots, n\}$ také, že $\alpha_i \neq \beta_i$, a o poradí týchto dvoch monómov rozhodneme podľa prvého takého exponentu. Navyše z definície usporiadania priamočiaro vyplýva aj tranzitívnosť tejto relácie.

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

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

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 $x^\alpha <_{lex} x^\beta$.

Príklad 4.4. V graduovaných usporiadaniach máme

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

Definícia 4.5. 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 4.6. Majme polynóm $f = 5x_1x_2+7x_2^5+19x_3^{17} \in k[x_1, x_2, x_3]$. Ak uvažujeme lexikografické usporiadanie, tak vedúcim členom je $5x_1x_2$. Ak by sme však uvažovali niektoré z graduovaných usporiadaní, tak vedúcim členom je $19x_3^{17}$.

2. Algoritmus delenia

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

Vstup: polynóm g a polynómy $f_1, \ldots, f_s$ z $k[x_1, \ldots, x_n]$ so zvoleným usporiadaním monómov.
Výstup: polynóm r taký, že $g = \sum h_i f_i + r$, kde $r = 0$ alebo $\mathrm{LM}(f_i) \nmid \mathrm{LM}(r)\ \forall f_i$.
Algorimus:

- inicializácia: $g_0 := g$.
- iterácia (cez i): Ak $g_i = 0$, potom $r := 0$, 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 $f_1, \ldots, f_s$ nedelí vedúci koeficient g_i) $r := g_i$, ukonči delenie.

PRÍKLAD 4.7. 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 4.8. *Výpočet pomocou algoritmu delenia skončí po konečnom počte krokov. Navyše, ak $g_i = 0$ pre nejaké i, potom $g \in (f_1, \dots, f_s)$.*

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_j. V prvom prípade spätným dosadzovaním (ako v prípade rozšíreného Euklidovho algoritmu) dostávame

$$g = h_1 f_1 + \dots + h_s f_s,$$

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

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

PRÍKLAD 4.9. 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 4.10. V Príklade 1.3(iv) sme uvažovali dvojbodovú množinu v rovine a neskôr sme videli, že ideál, ktorý ju definuje vieme generovať viacerými spôsobmi, napríklad nasledovné dva ideály sa rovnajú:

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

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

3. Monomiálne ideály

DEFINÍCIA 4.11. Ideál $J \subset k[x_1, \dots, x_n]$ sa nazýva *monomiálny*, ak je generovaný nejakou (nie nutne konečnou) množinou monómov.

TVRDENIE 4.12. *Monomiálny ideál je generovaný konečnou množinou monómov.*

Dôkaz. Nech

$$J = (x^\alpha)_{\alpha \in \mathcal{A}}$$

je monomiálny ideál. Uvažujme nasledovnú postupnosť ideálov: zoľme ľubovoľné x^{α_1} spomedzi generátorov ideálu J a označme

$$J_1 = (x^{\alpha_1}).$$

Ak $J_1 \neq J$, potom existuje medzi generátormi ideálu J monóm nepatriaci J_1, nech je to x^{α_2}. Označme

$$J_2 = (x^{\alpha_2}).$$

Takto dostaneme postupnosť ideálov

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

Keďže okruh $k[x_1, \dots, x_n]$ je noetherovský, táto reťaz ideálov je konečná, teda pre nejaké $N \in \mathbb{N}$ máme

$$J_N = (x^{\alpha_1}, x^{\alpha_2}, \dots, x^{\alpha_N}) = J.$$

□

Ukážeme si teraz základné a veľmi užitocné vlastnosti práce s monomiálnymi polynómami.

Tvrdenie 4.13. *Nech*

$$J = (x^{\alpha_i})_{i\in\{1,\dots,r\}} \subset k[x_1, \dots, x_n]$$

je monomiálny ideál. Potom x^β patrí ideálu J práve vtedy, keď je násobkom niektorého z generátorov ideálu J.

Dôkaz. Jedna implikácia je triviálna. Dôkaz druhej je viac uvedomovacie cvičenie než nejaké počítanie. Keďže

$$x^\beta \in J = (x^{\alpha_i})_{i\in\{1,\dots,r\}},$$

existujú polynómy $p_1, \dots, p_r$ také, že

$$x^\beta = \sum_{i=1}^{r} p_i x^{\alpha_i}.$$

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

$$x^\beta = \sum_{i=1}^{r} \left(\sum c_{ij} x^{\gamma_{ij}}\right) x^{\alpha_i}.$$

Je zrejmé, že monóm x^β z ľavej strany rovnosti sa musí nachádzať spolu s nejakými nenulovými koeficientami aj na pravej strane; nech $x^{\gamma_u} x^{\alpha_v}$ sú všetky tieto výskyty, čiže máme, že

$$x^\beta = \sum_{u,v} c_u x^{\gamma_u} x^{\alpha_v}$$

a teda $x^{\alpha_v} \mid x^\beta$. □

Tvrdenie 4.14. *Nech J je monomiálny ideál a $f = \sum d_\beta x^\beta$ je polynóm. Potom $f \in J$ práve vtedy keď každý člen $d_\beta x^\beta$ patrí ideálu J.*

Dôkaz. Dokazuje sa presne ako Tvrdenie 4.13: jedna implikácia je zjavná, pre dôkaz druhej nech $f \in J$, a preto

$$\sum d_\beta x^\beta = \sum_{i=1}^{r} p_i x^{\alpha_i} = \sum_{i=1}^{r} \left(\sum c_{ij} x^{\gamma_{ij}}\right) x^{\alpha_i}.$$

pre nejaké polynómy p_i. Každý z monómov pri nenulovom koeficiente na ľavej strane rovnosti (t.j. každé x^β, pre ktoré $d_\beta \neq 0$) sa musí nachádzať spolu s nejakými nenulovými koeficientami aj na pravej strane; nech $x^{\gamma_u}x^{\alpha_v}$ sú všetky tieto výskyty, čiže máme, že

$$d_\beta x^\beta = \sum_{u,v} c_u x^{\gamma_u} x^{\alpha_v}$$

a teda $d_\beta x^\beta \in J$. □

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 4.14 každý člen polynómu g partí do J, špeciálne, $\mathrm{LT}(g) \in J$. Z Tvrdenia 4.13 potom vidíme, že $\mathrm{LT}(g)$ je deliteľný niektorým generátorom, a teda g môžme redukovať, až dostaneme $g_i = 0$ pre nejaké i.

Aj geometricky sú monomiálne ideály veľmi jednoduché, viď Príklady 1.12 a 1.13.

Definícia 4.15. 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 4.16. 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 generuje celý ideál I.

Veta 4.17. *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 algoritmus delenia redukovaním polynómami $f_1, \ldots, f_k$, vždy správne rozhodne, 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 4.17 algoritmus delenia tento polynóm zredukuje do 0 a preto podľa Tvrdenia 4.8 $g \in (f_1, \ldots, f_k)$. □

Dôkaz Vety 4.17. 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 4.13 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 4.18. Nech $f_1 = x^2-4x+3, f_2 = x-y+1 \in k[x,y]$, uvažujme lexikografické usporiadanie. Zoberme ideál dvojbodovej algebraickej variety $I = (f_1, f_2) \subset k[x,y]$. Už v Príklade 4.10 sme sa presvedčili, že pomocou týchto dvoch generátorov nie je možné deliacim algoritmom zredukovať každý polynóm ideálu I na nulu. Z Vety 4.17 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 $g = f_1+(-x-y+5)f_2$. 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 4.19. 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 4.20. 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 $(a, a^2, a^3) \notin V(g)$.

4. Výpočet Gröbnerovej bázy

Videli sme, 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 4.21. 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 4.22. 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 4.23. *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 4.24. 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 4.25 (**Buchbergerovo kritérium**). *V okruhu $k[x_1, \ldots, x_n]$ so zvoleným usporiadaním monómov majme polynómy $f_1, \ldots, f_s$. Tieto polynómy tvoria Gröbnerovu bázu ideálu $(f_1, \ldots, f_s)$ práve vtedy, keď algoritmus delenia (polynómami $f_1, \ldots, f_s$) redukuje každý S-polynóm $S(f_i, f_j)$ $(i, j = 1, \ldots, k)$ do nuly.*

Dôkaz. Z Vety 4.17 vyplýva, že ak $\{f_1, \ldots, f_s\}$ je Gröbnerova báza, tak každý S-polynóm je algoritmom delenia zredukovaný do nuly, lebo $S(f_i, f_j) \in (f_1, \ldots, f_s)$ pre všetky i, j.

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

$$\mathrm{LT}(g) \notin (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)). \tag{5}$$

Nech

$$g = g_1 f_1 + \cdots + g_s f_s \tag{6}$$

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 $f_1, \ldots, f_s$ môžme predpokladať, že

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

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

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

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

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 $\{f_1, \ldots, f_s\}$ zredukuje do 0, spätným dosadzovaním dostaneme vyjadrenie

$$S(f_1, f_2) = \sum_{i=3}^{s} h_i f_i, \quad \text{pričom} \quad \mathrm{LM}(h_i f_i) \leq \mathrm{LM}(S(f_1, f_2)),\ i = 3, \ldots, s. \tag{8}$$

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

$$\frac{x^\gamma}{\mathrm{LT}(f_1)} f_1 - \frac{x^\gamma}{\mathrm{LT}(f_2)} f_2 - \sum_{i=3}^{s} h_i f_i = 0.$$

Túto rovnosť prenásobíme monómom x^δ/x^γ, vhodnou konštantou a pripočítame k (6), aby sme dostali nové vyjadrenie

$$g = \tilde{g}_1 f_1 + \cdots + \tilde{g}_s f_s,$$

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

Príklad 4.26. Vyriešme Príklad 4.20 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:

$$S(f_1, f_2) = zf_1 - yf_2 = -zx^2 + yx^3.$$

Aplikujme na tento polynóm deliaci algoritmus:

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

Dôsledok (**Buchbergerov algoritmus**). *V okruhu $k[x_1, \ldots, x_n]$ so zvoleným usporiadaním monómov majme polynómy $f_1, \ldots, f_s$. Gröbnerovu bázu ideálu $(f_1, \ldots, f_s)$ získame nasledovným spôsobom:*

Vstup: *polynómy $f_1, \ldots, f_s$ z $k[x_1, \ldots, x_n]$ so zvoleným usporiadaním monómov.*
Výstup: *Gröbnerova báza G ideálu $(f_1, \ldots, f_s)$.*
Algorimus:

- *inicializácia:* $G := \{f_1, \ldots, f_s\}$
- *iterácia:*
  - *Pre všetky $i, j = 1, \ldots, |G|$, $i \neq j$ 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 $f_1, \ldots, f_s$).*
  - *Ak všetky $r_{ij} = 0$, potom G je Gröbnerova báza, koniec algoritmu.*
  - *Inak $G := G \cup \{f_{|G|+1}, \ldots, f_{|G|+s}\}$ je nová množina generátorov ideálu, kde $f_{|G|+1}, \ldots, f_{|G|+s}$ sú nenulové r_{ij}.*
  - *Opakuj iteráciu pre túto novú množinu generátorov.*

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

Označme $G_1 = \{f_1, \ldots, f_s\}$ (množina generátorov), $J_1 = (\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s))$ (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

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

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 $(f_1, \ldots, f_s)$. □

PRÍKLAD 4.27. 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 $\{f_1, f_2, f_3, f_4, f_5\}$.

POZNÁMKA 4.28. Ak $\{f_1, \ldots, f_r\}$ je Gröbnerova báza ideálu $I = (f_1, \ldots, f_r)$ a ak $f \in I$, potom zrejme aj $\{f_1, \ldots, f_r, f\}$ je Gröbnerova báza I.

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

- 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 $(f_1, \ldots, f_s)$.
- Aplikujeme deliaci algoritmus, kde g redukujeme polynómami $h_1, \ldots, h_r$.
- $g \in (f_1, \ldots, f_s)$ práve vtedy, keď sa nám ho podarí zredukovať do 0.

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

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

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

– ... a mnohé ďalšie.

KAPITOLA 5

Gröbnerove bázy a eliminácia

1. Premietanie a eliminačný ideál

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, neskôr sa zoznámime ešte s postupom využívajúcim rezultanty.

PRÍKLAD 5.1. 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

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

Geometrisky môžme postup popísať 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 5.2. 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 $\overline{S}$ budeme označovať uzáver množiny S v Zariskiho topológii, teda je to najmenšia algebraická varieta obsahujúca S.

LEMA 5.3. *Nech $S \subset \mathbb{A}^n$, potom $V(I(S)) = \overline{S}$.*

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

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

TVRDENIE 5.4. *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. Pullback premietania π je vnorenie

$$\pi^* : k[x_{r+1}, \ldots, x_n] \hookrightarrow k[x_1, \ldots, x_n].$$

Teda ak $f \in k[x_{r+1}, \ldots, x_n]$, tak $\pi^* f$ je polynóm f chápaný ako polynóm v okruhu $k[x_1, \ldots, x_n]$.

Ukážeme inklúziu $\pi(X) \subset V(J \cap k[x_{r+1}, \ldots, x_n])$, z nej už potom vyplýva inklúzia $\overline{\pi(X)} \subset V(J \cap k[x_{r+1}, \ldots, x_n])$. Nech $a' = (a_{r+1}, \ldots, a_n) \in \pi(X)$, 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. □

VETA 5.5. *Nech $X \subset \mathbb{A}^n(k)$ je varieta, nech $J = I(X)$ 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

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

Dôkaz. Jedna inklúzia vyplýva z Tvrdenia 5.4. Pre dôkaz opačnej iklúzie zoberme $f \in I(\pi(X))$, ukážeme, že $f \in J \cap k[x_{r+1}, \ldots, x_n]$.

Zjavne $I(\pi(X)) \subset k[x_{r+1}, \ldots, x_n]$, preto $f \in k[x_{r+1}, \ldots, x_n]$. Potrebujeme ešte overiť, že f chápaný ako polynóm okruhu $k[x_1, \ldots, x_n]$ patrí ideálu J. Keďže $f \in I(\pi(X))$, máme $f(a') = 0$ pre všetky $a' \in \pi(X)$. Ak a je ľubovoľný bod na variete X, potom analogicky ako v predchádzajúcom dôkaze

$$(\pi^* f)(a) = f(a') = 0 \quad \forall a \in X.$$

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

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

□

VETA 5.6. *V predpokladoch Vety 5.4 nech je pole k algebraicky uzavreté (napr. $k = \mathbb{C}$). Potom*

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

Dôkaz. Najprv sa presvedčíme, že

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

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

Takže môžme písať

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

kde prvá rovnosť vyplýva z dokázanej Vety 5.5 o projekcii, štvrtá rovnosť z práve preverenej rovnosti ideálov a tretia z Nullstellensatz, a na záver piatu rovnosť sme ukázali s vlastnosťami radikálu ideálu. □

Ak $X = V(J)$, kde J je ľubovoľný ideál, a pole, nad ktorým pracujeme, nie je algebraicky uzavreté, rovnosť skutočne dokázať nemôžeme:

PRÍKLAD 5.7. Majme ideál $J = (y, x^2+1) \subset \mathbb{R}[x, y]$ 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: $(a, b) \mapsto (b)$). Naproti tomu, môžme sa presvedčiť, že $J \cap \mathbb{R}[y] = (y)$: učite $(y) \subseteq J \cap \mathbb{R}[y]$, keďže $y \in J \cap \mathbb{R}[y]$, pričom (y) obsahuje všetky polynómy v premennej y bez absolútneho člena; ak by $J \cap \mathbb{R}[y]$ mal obsahovať viac polynómov, obsahoval by už aj 1, ale $1 \notin J$, spor. Preto $V(J \cap \mathbb{R}[y]) = \{(0)\} \neq \emptyset$.

Tvrdenie 5.5 ani Tvrdenie 5.6 sa nedá v tomto prípade aplikovať, lebo jednak pole $\mathbb{R}$ nie je algebraicky uzavreté, a tiež $I(X) \neq J$, lebo $I(X) = (1) = \mathbb{R}[x, y]$. V tomto príklade naozaj nastáva vlastná inklúzia $\overline{\pi(X)} \subsetneq V(J \cap k[y])$.

DEFINÍCIA 5.8. 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.

VETA 5.9 (**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

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

□

PRÍKLAD (dokončenie príkladu 5.1). 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 Sage):

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

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

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

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

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

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

$$(1,0,0), (0,1,0), (0,0,1),$$
$$(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}),$$
$$(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

Príklad 5.10. 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 5.6) 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. Toto presne zodpovedá geometrickej situácii: bod $(0,0) \in \overline{\pi(X)}$, ale $(0,0) \notin \pi(X)$. Teda riešenia počiatočnej sústavy sú tvaru $(a^{-1}, a, a),\ a \neq 0$.

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

Záver. Gröbnerove bázy sú nástrojom na riešenie sústavy algebraických rovníc. Pomáhajú nám zodpovedať o danej sústave otázky, či je táto sústava riešiteľná, či má konečne veľa riešení a v prípade, že áno, vieme pomocou Gröbnerových báz nájsť všetky riešenia.

2. Radical membership

Ohľadne práce s radikálovými ideálmi existujú a v systémoch počítačovej algebry môžete nájsť implementované algoritmy pre riešenie týchto promlémov (s rastúcou obtiažnosťou):

- zitiť, či daný polynóm patrí radikálu dan0ho ideálu,
- overiť, či je daný ideál radikálový,

- nájsť radikál daného ideálu.

Uvedieme si tu riešenie len pvého z týchto problémov.

Pole k nemusí byť algebraicky uzavreté.

TVRDENIE 5.11. *Nech $I = (f_1, \dots, f_r) \subset k[x_1, \dots, x_n]$ je ideál. Potom*

$$f \in \sqrt{I} \quad \textit{práve vtedy, keď} \quad (f_1, \dots, f_r, 1 - yf) = k[x_1, \dots, x_n, y].$$

Dôkaz. Nech $1 \in (f_1, \dots, f_r, 1-yf)$. Potom úplne takým istým postupom ako v poslednej časti dôkazu 1.74 (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 $p_1, \dots, p_r \in k[x_1, \dots, x_n]$, že

$$\begin{aligned} f^d &= p_1 f_1 + \cdots + p_r f_r \qquad | \cdot y^d \\ f^d y^d &= p_1 f_1 y^d + \cdots + p_r f_r y^d \\ 1 &= p_1 f_1 y^d + \cdots + p_r f_r y^d + (1 - f^d y^d) \\ 1 &= p_1 f_1 y^d + \cdots + p_r f_r y^d + (1 - fy)(1 + fy + f^2 y^2 + \cdots + f^{d-1} y^{d-1}), \end{aligned}$$

čiže $1 \in (f_1, \dots, f_r, 1-yf)$, čo presne znamená, že $(f_1, \dots, f_r, 1-yf) = k[x_1, \dots, x_n, y]$. □

Pre využitie tohto tvrdenia v algoritme potrebujeme urobiť ešte jedno drobné pozorovanie: ak $1 \in I$, tak 1 sa určite nachádza v Gröbnerovej báze ideálu I pri akomkoľvek usporiadaní monómov. 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 $1 \in G$.

Práve ukázaný algoritmus môžme využiť aj pre porovnanie radikálov dvoch daných ideálov I a J, presnejšie zistiť, či $\sqrt{I} = \sqrt{J}$. Za týmto cieľom potrebujeme overiť, či $I \subset \sqrt{J}$ 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.

PRÍKLAD 5.12. Nech

$$I = (xy^2 + 2y^2, x^4 - 2x^2 + 1) \in k[x, y].$$

Zistíme, či $f = y - x^2 + 1$ partí $\sqrt{I}$.

V okruhu $k[x, y, z]$ s lexikografickým usporiadaním nájdeme Gröbnerovu bázu ideálu

$$\tilde{I} = (xy^2 + 2y^2, x^4 - 2x2 + 1, 1 - z(y - x^2 + 1)) \subseteq k[x, y, z].$$

Vypočítaná báza obsahuje polynóm 1. To znamená, že $f = y - x^2 + 1 \in \sqrt{I}$.

3. Prienik ideálov

TVRDENIE 5.13. *Nech $I, J \subset k[x_1, \ldots, x_n]$ sú ideály. Potom*

$$I \cap J = ((1 - t).I + (t).J) \cap k[x_1, \ldots, x_n].$$

Dôkaz. *** doplniť *** □

Algoritmus:

VSTUP: ideály $I, J \subset k[x_1, \ldots, x_n]$
VÝSTUP: Ideál $I \cap J$.
ALGORIMUS:

- Z generátorov ideálov I a J skonštruuj generátory ideálu $(1 - t).I + (t).J$.
- V usporiadaní monómov, kde $t > x_i$ pre všetky $i = 1, \ldots, n$ nájdi Gröbnerovu bázu G ideálu $(1 - t).I + (t).J$
- $I \cap J = G \cap k[x_1, \ldots, x_n]$.

---

4. Implicitizácia

4.1. Parametrizácia polynomickými funkciami.

PRÍKLAD 5.14 (**varieta dotyčníc vinutej kubiky**). Vieme už, že body vinutej kubiky $V(y - x^2, z - x^3) \subset \mathbb{A}^3(\mathbb{R})$ môžme parametrizovať (t, t^2, t^3), $t \in \mathbb{R}$. Skúsme teraz popísať plochu, ktorú vytvoria dotyčnice tejto krivky v každom jej bode.

Dotyčnica v pevne zvolenom bode (t_0, t_0^2, t_0^3) tejto krivky má smer

$$(1, 2t_0, 3t_0^2),$$

čiže jej parametrické vyjadrenie je

$$(t_0 + u, t_0^2 + 2t_0u, t_0^3 + 3t_0^2u),$$

kde u je parameter priamky. Parametrizácia plochy dotyčníc je tak zobrazenie

$$\begin{aligned} \varphi\colon\ & \mathbb{A}^2 \to \mathbb{A}^3 \\ & (t, u) \mapsto (t + u, t^2 + 2tu, t^3 + 3t^2u). \end{aligned}$$

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

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

Presvedčíme sa, že obrazom zobrazenia φ je plocha X určená rovnicou

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

Jedna inklúzia je priamočiara: 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 rovníc 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. Algebraickou varietou nemusí byť dokonca ani obraz afinného priestoru:

Príklad 5.15. Parametrizácia pokrývajúca jednodielny rotačný hyperboloid priamkami *** doplniť ***

Pri implicitizácii sa preto snažíme nájsť rovnicu (rovnice) popisujúcu uzáver obrazu parametrizácie v Zariskiho topológii. Majme teda zobrazenie $\varphi\colon\ \mathbb{A}^m \to \mathbb{A}^n$, $(t_1,\dots,t_m) \mapsto (x_1,\dots,x_n)$ dané predpisom

$$\begin{aligned} x_1 &= \varphi_1(t_1,\dots,t_m) \\ &\vdots \\ x_n &= \varphi_n(t_1,\dots,t_m) \end{aligned} \tag{9}$$

kde φ_i sú polynómy, 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. (Ine o analógiu s funkciou jednej premennej: všetky body roviny, ktoré sú tvaru $(x,f(x))$, tvoria graf funkcie $f\colon\ x \mapsto f(x)$.) Každý bod $(t_1,\dots,t_m) \in \mathbb{A}^m$ zobrazíme na bod grafu zobrazenia φ:

$$\tilde{\varphi}\colon\ (t_1,\dots,t_m) \mapsto (t_1,\dots,t_m,\varphi_1(t_1,\dots,t_m),\dots,\varphi_n(t_1,\dots,t_m)),$$

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:

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

Zjavne

$$\pi \circ \tilde{\varphi} = \varphi.$$

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

Veta 5.16. *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 (9). Nech ďalej I je ideál*

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

Potom

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

Dôkaz. V prípade, že k je algebraicky uzavreté, tvrdenie vety vyplýva z predchádzajúcej diskusie a z Tvrdenia 5.6. Ak k nie je algebraicky uzavreté, máme podľa Tvrdenia 5.4 zatiaľ iba jednu inklúziu.

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

Potrebujeme preto ešte ukázať, že $V(I \cap k[x_1, \ldots . x_n])$ je skutočne najmenšia algebraická varieta obsahujúca $\varphi(\mathbb{A}^m)$. To overíme tak, že pre algebraickú varietu $Y \subset \mathbb{A}^n$ ukážeme, že ak $Y \supset \varphi(\mathbb{A}^m)$, potom $Y \supset V(I \cap k[x_1, \ldots, x_n])$.

Nech $Y \supset \varphi(\mathbb{A}^m)$ a nech $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ sú polynómy definujúce varietu Y, t.j. $Y = V(g_1, \ldots, g_s)$. Potom každý bod z obrazu φ spĺňa rovnice pre Y:

$$g_i(\varphi(a_1, \ldots, a_m)) = 0 \quad \forall (a_1, \ldots, a_m) \in \mathbb{A}^m. \tag{10}$$

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 $x_1, \ldots, x_n$. Keďže tento polynóm má nulovú hodnotu vo všetkých bodoch priestoru $\mathbb{A}^m$ nad nekonečným poľom, ide o nulový polynóm, preto

$$V(g_1 \circ \varphi, \ldots, g_s \circ \varphi) = \mathbb{A}^m.$$

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

Keďže, ako sme ukázali, $g_i \circ \varphi$ je nulový polynóm, aj po rozšírení poľa k na jeho algebraický uzáver $\bar{k}$ máme, $V_{\bar{k}}(g_1 \circ \varphi, \ldots, g_s \circ \varphi) = \mathbb{A}^m_{\bar{k}}$, a tak hodnota g_i $(i = 1, \ldots, s)$ je nulová na celej množine $\varphi(\mathbb{A}^m_{\bar{k}})$. Preto platí, že $Z_{\bar{k}} \supset \varphi(\mathbb{A}^m_{\bar{k}})$. Inklúzia sa zachová, keď prejdeme k uzáverom množín v Zariskiho topológii, takže máme

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

Predposledná rovnosť vyplýva z Tvrdenia 5.6 posledná zas z faktu, že ideál I je definovaný nad pôvodným poľom k. Takže máme inklúziu

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

Inklúzia pre množinu riešení sa zachová, keď sa zaujímame iba o riešenia nad podpoľom k poľa $\bar{k}$, 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 môže značne skomplikovať.

Teraz už vieme nielen ukázať, že rovnica v Príklade 5.14 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.

4.2. Parametrizácia racionálnymi funkciami. Len stručne si si vysvetlíme, ako môžme modifikovať predchádzajúci postup, aby sme našli obraz parametrizácie danej racionálnymi funkciami.

Príklad 5.17. 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) z časti o algebraických varietách 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

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

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 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

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

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 nasledovne: 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:

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

KAPITOLA 6

Rezultanty

1. Definícia a základná vlastnosť

TVRDENIE 6.1. *Nech $f, g \in k[t]$ (k je pole). Potom f a g majú spoločný koreň nad nejakým rozšírením poľa k práve vtedy, keď majú v $k[x]$ nekonštantného spoločného deliteľa.*

Dôkaz. Nech α je spoločný koreň polynómov f a g, $\alpha \in \overline{k}$. Okruh $k[\alpha]$ tak obsahujuje koreň α a tiež obsahuje pole k. 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 $k[x]$. Keďže $k[x]$ je okruh hlavných ideálov, 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 $f, g \in \ker\varphi$. Preto $\ker\varphi = (h)$ je nenulový ideál. Navyše, h je určite nekonštantný polynóm: ak by $h \in k$ ($h \neq 0$, ako sme už overili), potom máme, že $1 = hh^{-1} \in (h)$ a teda $(h) = k[x]$, čo však nie je pravda, lebo napríklad $\varphi(1) = 1$ a teda $1 \notin \ker\varphi$. Máme tak, že h je nekonštantný spoločný deliteľ polynómov f a g.

Nech teraz existuje spoločný deliteľ $h \in k[x]$ polynómov 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 je zjavné, že $\varphi(x)$ je koreňom g. Našli sme spoločný koreň polynómov f a g v rozšírení $k[x]/(h)$. □

LEMA 6.2. *Nech $f, g \in R[x]$, kde R je okruh s jednoznačným rozkladom. Potom f a g majú spoločného nekonštantného deliteľa práve vtedy, keď existujú nenulové $p, q \in R[x]$ také, že $pf + qg = 0$ a pre stupne p, q platí $\deg p < \deg g$, $\deg q < \deg f$.*

Dôkaz. Nech h je netriviálny spoločný deliteľ polynómov f, g, teda $f = h\tilde{f}$, $g = h\tilde{g}$, kde $\deg\tilde{f} < \deg f$ a $\deg\tilde{g} < \deg g$. Potom stačí zobrať $p = \tilde{g}$ a $q = -\tilde{f}$.

Opačne, nech p, q sú polynómy s vlastnosťami uvedenými v tvrdení lemy. Faktorizujme obe strany rovnosti

$$pf = -qg.$$

Každý ireducibilný faktor polynómu g sa musí nachádzať aj na ľavej strane, a tak je deliteľom polynómu f alebo polynómu p. Keďže $\deg p < \deg q$, niektorý z deliteľov polynómu g musí byť deliteľom polynómu f. □

PRÍKLAD 6.3. Smerujeme k tomu, nájsť kritérium, kedy majú dva polynómy v $k[x]$ (alebo všeobecnejšie v $R[x]$, kde R je okruh s jednoznačným rozkladom) spoločný koreň. Najjednoduchší príklad dostaneme, keď si zoberieme dva lineárne polynómy:

$$f = f_1x + f_0, \quad g = g_1x + g_0, \qquad \text{kde } f_1, g_1 \neq 0.$$

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 6.4. Nech $f, g \in R[x]$ sú polynómy stupňov m a n nad okruhom s jednoznačným rozkladom:

$$\begin{aligned} f &= f_mx^m + \cdots + f_1x + f_0, \quad f_m \neq 0, \\ g &= g_nx^n + \cdots + g_1x + g_0, \quad g_n \neq 0. \end{aligned}$$

Štvorcová matica

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

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 6.5. 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 6.6. *Polynómy $f, g \in R[x]$ majú netriviálneho spoločného deliteľa práve vtedy, keď* $\mathrm{Res}(f,g) = 0$.

POZNÁMKA 6.7. Všimnite si, že Príklad 6.3 je vlastne dôkazom Vety 6.6 pre prípad $m = n = 1$.

Dôkaz Vety 6.6. Podľa Lemy 6.2 majú f, g netriviálneho spoločného deliteľa práve vtedy, keď existujú polynómy

$$\begin{aligned} p &= p_{n-1}x^{n-1} + \cdots + p_1x + p_0, \\ q &= q_{m-1}x^{m-1} + \cdots + q_1x + q_0 \end{aligned}$$

také, že $pf + qg = 0$. Na ľavej strane máme polynóm, ktorý má podľa rovnosti byť nulový. Dostávame tak, že

$$\begin{aligned} f_0p_0 + g_0q_0 &= 0 \\ f_1p_0 + f_0p_1 + g_1q_0 + g_0q_1 &= 0 \\ &\dots \\ f_mp_{n-1} + g_nq_{m-1} &= 0. \end{aligned}$$

Toto je sústava lineárnych rovníc pre neznáme p_i, q_j, ktorá má netriviálne riešenie práve vtedy, keď $\mathrm{Res}(f, g) = 0$. □

Poznámka 6.8. Sylvestrovu maticu polynómov f a g môžeme chápať aj ako maticu zobrazenia lineárnych priestorov (v prípade, že $R = k$ je pole) či všeobecnejšie tzv. *modulov* (ak R je okruh). Ide o alternatívnu formuláciu dôkazu Vety 6.6, ktorá bude užitočná pre neskoršie úvahy.

Pre prehľadnosť uvažujme situáciu, keď $R = k$ je pole. Analogicky celá úvaha vyzerá aj v prípade, keď ide o moduly nad okruhom R.

Označme si ako P_d množinu všetkých polynómov v $k[x]$, ktorých stupeň nie je vačší ako d, potom 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 zas polynómy 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.

Zobrazenie δ má nenulové jadro práve vtedy, keď existujú nenulové polynómy $p \in P_{n-1}$ a $q \in P_{m-1}$ také, že $pf + qg = 0$, čo je podľa Lemy 6.2 ekvivalentné tvrdeniu, že f a g sú súdeliteľné, a na druhej strane je to ekvivalentné faktu, že matica zobrazenia δ, teda Sylvestrova matica, je singulárna.

2. Diskriminant polynómu

TVRDENIE 6.9. *Polynóm $f \in k[x]$ má v nejakom rozšírení poľa k viacnásobný koreň práve vtedy, keď* $\mathrm{Res}(f, f') = 0$.

Dôkaz. Nech $\alpha \in \overline{k}$ je aspoň dvojnásobný koreň, teda platí, že

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

Pre deriváciu f potom platí

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

čiže 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. □

PRÍKLAD 6.10. 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 6.11. Nech $f \in k[x]$, $f = f_n x^n + \cdots + f_1 x + f_0$, $f_n \neq 0$. *Diskriminant* polynómu f je

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

Nasledovné tvrdenie je len reformuláciou už dokázaného.

TVRDENIE 6.12. *Polynóm $f \in k[x]$ má viacnásobný koreň nad nejakým rozšírením k práve vtedy, keď* $\mathrm{Discr}(f) = 0$.

áno, to už bolo ok, teraz prosím prelož toto:

3. Rezultant ako funkcia koreňov polynómov

PRÍKLAD 6.13. Nech $f, g \in k[x]$ sú polynómy s faktorizáciou nad vhodným rozšírením poľa k:

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

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

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

Toto pozorovanie teraz zovšeobecníme:

VETA 6.14. *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

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

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

Ak f a g majú spoločný koreň, potom je tvrdenie pravdivé, na základe Vety 6.6. 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 $\mathrm{Syl}(f,g) = g_0\mathrm{I}_m$, a platí

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

(Indukčný krok.) Nech teraz

$$f = qg + r, \quad \text{kde} \quad r \neq 0,\ \deg r = d < \deg g, \quad r = r_d x^d + \dots + r_0.$$

Postupovať budeme tak, že nájdeme predpis pre výpočet $\mathrm{Res}(f,g)$ pomocou $\mathrm{Res}(g,r)$, 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 $\mathrm{Res}(f,g) = \Theta(f,g)$. □

4. Rezultanty a eliminácia

Príklad 6.15. 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 6.6 je to práve vtedy, keď $\mathrm{Res}_x(f,g) = 0$. 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 $y^4 - 4y^2 + 1 = 0$. Každému z týchto riešení zodpovedá jedna hodnota pre x-súradnicu, čiže dokopy tak dostaneme presne štyri spoločné korene dvoch polynómov z $k[x]$.

Príklad 6.16. Nájdime prienik kriviek $V(f), V(g) \subset \mathbb{A}^2(\mathbb{C})$, kde

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

Rezultant polynómov f, g vzhľadom na premennú x je

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

Pre $y = 0$ však neexistuje žiadna hodnota x taká, aby bod s týmito súradnicami ležal na oboch krivkách.

Skúsme teda preskúmať bližšie, čo geometricky popisuje rezultant dvoch polynómov v $k[x, y]$.

VETA 6.17. *Nech $f, g \in k[x_1, \ldots, x_r]$. Potom*

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

Dôkaz. Z definície rezultantu je zrejmé, že $\mathrm{Res}_{x_1}(f,g)$ je polynóm, presnejšie $\mathrm{Res}_{x_1}(f,g) \in k[x_2, \ldots, x_r]$. 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

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

Po vynásobení zľava maticou $(0\ \ldots\ 0\ 1)$ dostávame

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

V Poznámke 6.8 sme si vysvetlili, že Sylvestrova matica je maticou zobrazenia lineárnych priestorov alebo všeobecnejšie modulov nad R, kde teraz $R = k[x_2, \ldots, x_r]$: 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 $p, q \in k[x_1, \ldots, x_r]$ také, že $\mathrm{Res}_{x_1}(f,g) = pf + qg$, a preto $\mathrm{Res}_{x_1}(f,g) \in (f,g)$. □

DÔSLEDOK. *Nech $f, g \in k[x_1, \ldots, x_r]$. Potom*

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

kde π je premietanie $(a_1, a_2, \ldots, a_r) \mapsto (a_2, \ldots, a_r)$.

Dôkaz 1. Z predchádzajúcej vety máme

$$V((f,g) \cap k[x_2, \ldots, x_r]) \subseteq V(\mathrm{Res}_{x_1}(f,g)). \tag{11}$$

Z Tvrdenia 5.4 v kapitole o Gröbnerových bázach máme, že

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

Spolu tak dostávame dokazovanú inklúziu. □

Dôkaz 2. Z predchádzajúcej vety máme, že existujú polynómy $p, q \in k[x_1, \ldots, x_r]$ také, že

$$\mathrm{Res}_{x_1}(f,g) = pf + qg.$$

Preto ak $(a_1, a_2, \ldots, a_r)$ je spoločným koreňom f a g, potom jeho priemet

$$\pi(a_1, a_2, \ldots, a_r) = (a_2, \ldots, a_r)$$

je koreňom $\mathrm{Res}_{x_1}(f, g)$. □

Používať rezultanty pri hľadaní spoločných bodov dvoch kriviek je teda korektný postup: v Príklade 6.15 polynóm $\mathrm{Res}_x(f, g)$ popisuje varietu, ktorá určite obsahuje všetky body priemetu prieniku $V(f)$ a $V(g)$ na y-os. Potom x-súradnicu môžeme dopočítať buď dosadením konkrétnej y-súradnice do f a g, alebo ešte nájdeme rezultant

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

Dostaneme tak 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 6.16 zas 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 (11) sa nedá nahradiť rovnosťou. Pre porovnanie môžme skúsiť nájsť Gröbnerovu bázu ideálu (f, g), a zistíme, že obsahuje polynóm $y^3 - 4y + 1$.

Príklad 6.18. 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 pomocou nejakého systému počítačovej algebry):

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

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 čiastočné 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 polynomických 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 $V(f, g, h)$.

5. Eliminácia pomocou rezultantov a Gröbnerových báz – zhrnutie

Na prvý pohľad sa medóda používajúca rezultanty môže javiť ako menej atraktívna. 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 6.18, bolo tak trochu šťastie: išlo o špeciálnu varietu so špeciálnou polohou. 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 ak by sme sa chceli vyhnúť rozširovaniu čiastočných riešení (a teda komplikovanej analýze eliminačných ideálov) tak, že by sme hľadali Gröbnerovu bázu viackrát (t.j. hľadali by sme Gröbnerovými bázami priemety na ostatné súradnicové osi), z hľadiska výpočtovej zložitosti to rozhodne nie je dobrý nápad.

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 maximálna 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.

6. Slabá Bézoutova veta

V Príklade 6.15 sme videli, že kružnica a hyperbola (t.j. dve kvadratické krivky) sa preťali v štyroch bodoch. Podobná situácia nastane v nasledujúcich príkladoch:

Príklad 6.19. V reálnej rovine nech

$$\begin{aligned} C_1 &= V(x^2 + 4y^2 - 1), \\ C_2 &= V(4x^2 + y^2 - 1), \end{aligned}$$

teda C_1, C_2 sú dve elipsy pretínajúce sa v štyroch bodoch.

Príklad 6.20. V reálnej rovine uvažujme kubickú eliptickú krivku

$$C_1 = V(y^2 - x^3 + x)$$

a parabolu

$$C_2 = V(5y^2 - x - 2).$$

Tieto krivky sa pretínajú v šiestich bodoch, čo ľahko overíme výpočtom.

PRÍKLAD 6.21. Uvažujme znovu reálnu rovinu a v nej kubickú parabolu a priamku:

$$\begin{aligned} C_1 &= V(y - x^3), \\ C_2 &= V(y - x). \end{aligned}$$

Zrejme sa tieto krivky pretínajú v troch bodoch. Navyše v tomto špeciálnom prípade (prienik ľubovoľnej rovinnej algebraickej krivky s priamkou) pozorovanie ľahko zovšeobecníme: krivka môže mať s priamkou nanajvýš d spoločných bodov, kde d je stupeň danej krivky. (Porovnaj s Gaussovou fundamentálnou vetou algebry.)

Všetky tieto pozorovania nás vedú k nasledovnému tvrdeniu.

VETA 6.22 (**Slabá Bézoutova veta**). *Nech $f, g \in k[x, y]$, teda $V(f)$ a $V(g)$ sú rovinné krivky. Ak f je stupňa m a g je stupňa n a polynómy f a g sú nesúdeliteľné, potom krivky $V(f)$ a $V(g)$ majú najviac mn spoločných bodov.*

Dôkaz. Keďže f a g sú nesúdeliteľné, majú spoločných len konečne veľa koreňov (Tvrdenie 2.4 v časti o Zariskiho topológii). Môžme preto predpokladať, že po vhodnej voľbe súradnicovej sústavy žiadne dva spoločné body kriviek $V(f)$ a $V(g)$ nemajú rovnakú x-súradnicu. Tiež môžme bez ujmy na všeobecnosti predpokladať, že polynóm f obsahuje člen cy^m ($c \in k$), analogicky pre polynóm g (dosiahneme to zase vhodnou generickou lineárnou transformáciou x a y).

Uvažujme f a g ako polynómy v premennej y s koeficientami v $k[x]$:

$$\begin{aligned} f &= a_0(x)y^m + a_1(x)y^{m-1} + \cdots + a_m(x), \\ g &= b_0(x)y^n + b_1(x)y^{n-1} + \cdots + b_n(x), \end{aligned}$$

kde a_i, b_i sú polynómy stupňa najviac i. Rezultant $\mathrm{Res}_y(f, g)$ je zrejme polynóm v $k[x]$. Tento polynóm je nenulový, inak by polynómy f a g boli podľa Vety 6.6 súdeliteľné, čo by bolo v spore s predpokladom. Navyše všetky x-súradnice spoločných bodov sú koreňmi polynómu $\mathrm{Res}_y(f, g)$, teda f a g majú najviac $\deg \mathrm{Res}_y(f, g)$ spoločných bodov.

Keď druhý riadok Sylvestrovej matice $\mathrm{Syl}_y(f, g)$ vynásobíme x, tretí x^2, ..., n-tý x^{n-1}, $(n+2)$-hý vynásobíme x, ..., posledný vynásobíme x^{m-1}, dostaneme rovnosť, kde na ľavej strane máme $x^{(\sum_{i=1}^{n-1} i + \sum_{i=1}^{(m-1)m} i)}\mathrm{Res}_y(f, g)$ a na pravej determinant

$$\begin{vmatrix} a_0(x) & a_1(x) & \dots & a_m(0) & 0 & \dots & 0 \\ 0 & xa_0(x) & \dots & xa_{m-1}(x) & xa_m(x) & \dots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \dots & 0 & x^{n-1}a_0(x) & \dots & x^{n-1}a_{m-1}(x) & x^{n-1}a_m(x) \\ b_0(x) & b_1(x) & \dots & b_n(x) & 0 & \dots & 0 \\ 0 & xb_0(x) & \dots & xb_{n-1}(x) & xb_n(x) & \dots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \dots & 0 & x^{m-1}b_0(x) & \dots & x^{m-1}b_{n-1}(x) & x^{m-1}b_n(x) \end{vmatrix}.$$

V ňom sú v prvom stĺpci konštanty, v druhom stĺpci sú polynómy stupňa najviac 1, v treťom stĺpci sú polynómy stupňa najviac 2, až v poslednom stĺpci sú polynómy stupňa najviac $m + n - 1$. Na ľavej strane tak máme súčin

$$x^{\frac{(n-1)n}{2} + \frac{(m-1)m}{2}}\mathrm{Res}_y(f, g)$$

a na pravej strane máme polynóm stupňa najviac $\sum_{i=0}^{m+n-1} = \frac{(m+n-1)(m+n)}{2}$. Odtiaľ už ľahko vypočítame, že $\mathrm{Res}_y(f,g)$ je stupňa najviac mn. □

POZNÁMKA 6.23. Podľa Bézoutovej vety platí, že dve rovinné krivky so stupňami m a n, ktoré nemajú spoločnú komponentu, sa pretínajú presne v mn bodoch za predpokladov, že

- pole, v ktotom pracujeme, je algebraicky uzavreté,
- uvažujeme nielen afinnú ale celú projektívnu rovinu (teda aj tzv. „body v nekonečne"),
- priesečníky počítame so správnou násobnosťou.

7. Hľadanie implicitnej rovnice pre parametrizovanú krivku

Niekedy môže byť rovinná krivka zadané nie rovnicou, ale parametricky (analógia z lineárnej geometrie: všeobecná rovnica priamky verzus jej parametrické vyjadrenie).

PRÍKLAD 6.24. V afinnej rovine majme parametricky dané krivky:

- $(x,y) = (t,t^2)$ je parabola $V(y-x^2)$,
- $(x,y) = (t^2,t^3)$ je bikubická parabola $V(y^2-x^3)$,
- $(x,y) = (t,1/t)$ je hyberbola $V(xy-1)$,
- $(x,y) = \left(\frac{-t^3}{1+t^4}, \frac{t}{1+t^4}\right)$ je krivka $V(xy+(x^2+y^2)^2)$,

Krivka zadaná parametricky sa napríklad veľmi ľahko vykresľuje. No pre skúmanie niektorých jej vlastností (napr. hľadanie tzv. singulárnych bodov) je naopak výhodné mať krivku popísanú implicitne, t.j. polynómom z $k[x,y]$.

Nájsť parametrizáciu krivky zadanej rovnicou pomocou polynómov či racionálnych funkcií je ťažký problém, ktorý vo všeobecnosti ani nie je riešiteľný. My sa ale v tejto časti budeme zaoberať opačným postupom, a síce hľadaním všeobecnej (implicitnej) rovnice pre krivku danú jej parametrickým vyjadrením.

Nech je krivka $C \subset \mathbb{A}^2(k)$ daná parametricky

$$\begin{aligned} x &= \frac{p_1(t)}{q_1(t)}, \\ y &= \frac{p_2(t)}{q_2(t)}, \end{aligned}$$

kde $p_1, q_1, p_2, q_2 \in k[t]$, kde p_1 a q_1 sú navzájom nesúdeliteľné, to isté platí aj pre p_2 a q_2. Chceme nájsť polynóm $f \in k[x,y]$ taký, že $C = V(f)$.

Parametrické vyjadrenie je ekvivalentné sústave

$$\begin{aligned} p_1(t) - xq_1(t) &= 0, \\ p_2(t) - yq_2(t) &= 0. \end{aligned}$$

Hľadáme teda také x a y, že tieto dve rovnice (chápané ako polynomické rovnice v t) majú spoločný koreň. Zrejme rezultant

$$\mathrm{Res}_t(p_1(t) - xq_1(t), p_2(t) - xq_2(t))$$

bude polynóm z $k[x,y]$ taký, že všetky body parametricky zadanej krivky sú jeho koreňmi.

PRÍKLAD 6.25. Nech je krivka $C \in \mathbb{A}^2(\mathbb{R})$ daná parametricky

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

Jej implicitné vyjadrenie je

$$f(x,y) = \mathrm{Res}_t(t^2-x, t^3+t-y) = \begin{vmatrix} 1 & 0 & -x & 0 & 0 \\ 0 & 1 & 0 & -x & 0 \\ 0 & 0 & 1 & 0 & -x \\ 1 & 1 & 0 & -y & 0 \\ 0 & 1 & 1 & 0 & -y \end{vmatrix} = -x^3+y^2-2xy+x^2 = -x^3+(x-y)^2,$$

t.j. ide o bikubickú parabolu.

KAPITOLA 7

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.

1. Ohraničenie koreňov

VETA 7.1. *Nech* $f \in \mathbb{R}[x]$, $f = f_m x^m + \cdots + f_1 x + f_0$, $f_m \neq 0$. *Ak*

$$|a| \geq 2 \sum_{i=0}^{m} \frac{|f_i|}{|f_m|}, \tag{12}$$

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

Dôkaz. Najprv si všimnime, že z (12) vyplýva, že $|a| \geq 2$. Odtiaľ ukážeme, že podiel $f(a)/f_m a^m$ je kladný.

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

□

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.

2. Sturmova veta

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

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

DEFINÍCIA 7.2. *Sturmova postupnosť polynómu* $p \in \mathbb{R}[x]$ je postupnosť $(p_0, p_1, \ldots, p_k)$ polynómov, kde

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

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

V Sturmovej postupnosti zrejme platí

$$p_{i-1} = q_{i-1} p_i - p_{i+1}. \tag{13}$$

DEFINÍCIA 7.3. Nech $\mathbf{a} = (a_0, \ldots, a_k)$ je postupnosť nenulových reálnych čísel. Počet znamienkových zmien $\operatorname{var}(\mathbf{a})$ v postupnosti $\mathbf{a}$ je definovaný

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

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

PRÍKLAD 7.4. $\operatorname{var}(1, -2, 2, 0, 0, 3, 4, -5, -2, 0, 3) = 4$.

DEFINÍCIA 7.5. 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

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

VETA 7.6 (**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*

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

Dôkaz Sturmovej vety rozdelíme na viacero tvrdení.

DEFINÍCIA 7.7. 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 $[a, b]$ sa nazýva *fundamentálny interval polynómu* p, ak existuje také $\gamma_0 \in (a, b)$, že pre všetky $\gamma \in [a, b]$, $\gamma \neq \gamma_0$ platí $p_i(\gamma) \neq 0$ pre všeky p_i, $i = 0, \ldots, k$.

Neformálne, $[a,b]$ 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. Navyše, žiaden polynóm Sturmovej postupnosti polynómu p nemá koreň v a ani v b.

TVRDENIE 7.8. *Nech $[a,b]$ je fundamentálny interval polynómu $p \in \mathbb{R}[x]$. Ak p nemá reálny koreň na $[a,b]$, 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 $[a,b]$. 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 $\mathrm{var}_{\mathbf{p}}(a) = \mathrm{var}_{\mathbf{p}}(b)$.

Nech teraz existuje i také, že $p_i(\gamma_0) = 0$ pre nejaké $\gamma_0 \in (a,b)$. Z (13) 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 (13) dostávame aj $p_{i+1}(\gamma_0) = -p_{i-1}(\gamma_0)$. Keďže $[a,b]$ je fundamentálny interval, p_{i+1} a p_{i-1} na ňom žiaden koreň nemajú, a tak

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

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

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

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

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

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

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

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

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 postupnosť polynómov

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

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

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

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

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

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

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

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 7.6. Dve predchádzajúce tvrdenia sú vlastne dôkazom Sturmovej vety v prípade, že interval $[a, b]$ je fundamentálny. Ak $[a, b]$ 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 $[a_{i-1}, a_i]$ sú fundamentálne intervaly polynómu p a pre počty koreňov tak máme

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

□

PRÍKLAD 7.10. Separujeme reálne korene polynómu

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

Pomocou Vety 7.1 najprv nájdeme interval obsahujúci všetky reálne korene polynómu:

$$M = 2\sum_{i=0}^{3} \frac{|f_i|}{|f_3|} = 2(1 + 4 + 3 + 1) = 18,$$

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

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

Pomocou Sturmovej vety zistíme počet reálnych koreňov:

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

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).