

AFINNÉ ALGEBRAICKÉ VARIETY

1. DEFINÍCIA, PRÍKLADY, ZÁKLADNÉ VLASTNOSTI

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

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

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 odlišenie jeho štruktúry od vektorového priestoru (napríklad body na rozdiel od vektorov nemôžeme sčítavať).

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

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

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

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

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

Príklad 1.3. Najjednoduchšie príklady afinných algebraických variet:

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

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

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

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

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

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

Úloha 1. Načrtnite aspoň štyri z nasledujúcich rovinných kriviek (algebraické variety v $\mathbb{A}^2(\mathbb{R})$):

- $V(x^3 - y^2)$,
- $V(x^3 + x^2 - y^2)$,
- $V(x^3 + x^2 + y^2)$,
- $V(x^4 - x^2 + y^2)$,
- $V(x^5 + x^4 + y^2)$,
- $V(x^6 - x^4 + y^2)$,

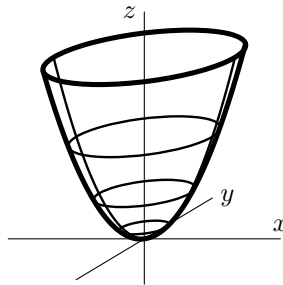
- $V((x^2 + y^2)^3 - 4x^2y^2)$,
- $V(x^n + y^n - 1)$, kde $n \geq 3$.

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

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

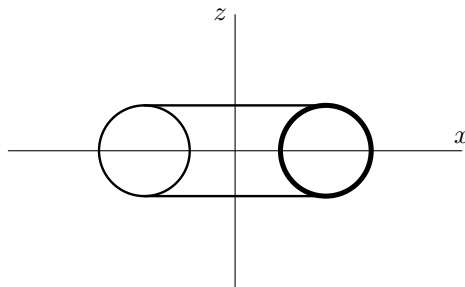
Príklad 1.7. *Nadplocha* je algebraická varieta v $\mathbb{A}^n(k)$ definovaná jediným nekonštantným polynómom z $k[x_1, \dots, x_n]$. Nadplocha v \mathbb{A}^3 sa nazýva tiež *plocha*. *Dimenzia nadplochy v \mathbb{A}^n* je (definitórsky) $n - 1$. (Niekedy sa nadplocha definuje len pre $n \geq 3$.)

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



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

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



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

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

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

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

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

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

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

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 varietyou. Presnejšie, najmenšou algebraickou varietyou obsahujúcou množinu M je celá x -os.

Úloha 3. V $\mathbb{A}^2(\mathbb{R})$ majme množiny

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

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

O každej zistíte, či je algebraickou varietyou: ak nie, dokážte, ak áno, najdite definujúce rovnice.

* **Úloha 4.** Nech $M \subset \mathbb{A}^1(\mathbb{C})$ pozostáva z tých bodov komplexnej afinnej priamky, ktorých súradnica je reálna. Je množina M algebraickou varietyou v $\mathbb{A}^1(\mathbb{C})$?

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

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

$$X_1 = V(f_1, \dots, f_r),$$

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

Ukážeme, že

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

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

Prvá rovnosť (o prieniku) je jednoduchá:

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

Druhú rovnosť ukážeme tak, že ukážeme obe inklúzie.

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

Dôsledok. Zjednotenie konečného počtu algebraických variety a prienik konečného počtu algebraických variety sú tiež algebraické variety.

Úloha 5. Zapište jednotkovú kružnicu spolu so svojím stredom ako algebraickú varietu, čiže nájdite polynomicke rovnice, ktorých riešením sú presne body jednotkovej kružnice a jej stred.

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

Dôkaz. Nech $X \subset \mathbb{A}^n(\mathbb{R})$, $X = V(f_1, \dots, f_r)$. Polynóm $f_i(x_1, \dots, x_n)$ predstavuje spojitú funkciu $\mathbb{A}^n(\mathbb{R}) \rightarrow \mathbb{R}$, 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 $X = X_1 \cap X_2 \cap \dots \cap X_r$ je preto tiež uzavretá množina. \square

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

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

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

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

$$(1) \quad f = \sum_{i=0}^d f_i(x_1, \dots, x_{n-1})x_n^i, \quad \text{kde } d > 0, f_i \in k[x_1, \dots, x_{n-1}] \forall i \text{ a } f_d \neq 0.$$

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

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

Úloha 6. Overte, že dodatočné predpoklady v tvrdení (ii) predchádzajúcej vety sú nevyhnutné: nájdite kontrapríklad, keď k nie je algebraicky uzavreté pole.

* **Úloha 7.** Nech k je pole, ktoré nie je algebraicky uzavreté. A nech $X \subset \mathbb{A}^n(k)$ je ľubovoľná algebraická varieta. Ukážte, že existuje polynóm $g \in k[x_1, \dots, x_n]$ taký, že $X = V(g)$.

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

2. AFINNÉ ALGEBRAICKÉ VARIETY A IDEÁLY

Úloha 8. Zistite, či dané dve sústavy určujú tú istú lineárnu varietu v $\mathbb{A}^3(\mathbb{R})$, teda či platí $V(f_1, f_2, f_3) = V(g_1, g_2)$:

- (a) $f_1 = x + y + z - 1, f_2 = x - y + 2z - 4,$
 $g_1 = x + 5y - z + 5, g_2 = 3x + y + z - 2.$
- (b) $f_1 = 2x + 3y - z, f_2 = x + y - 1, f_3 = x + z - 3,$
 $g_1 = x + 3y - 2z + 3, g_2 = y - z + 2.$
- (c) Navrhnite algoritmus, ktorý pre lineárne variety $X_1 = V(f_1, \dots, f_r), X_2 = V(g_1, \dots, g_s) \subset \mathbb{A}^n$ rozhodne, či $X_1 = X_2$ (f_i, g_j sú lineárne polynómy).

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

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

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

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

Takže, ak $a \in X$, potom

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

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

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

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

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

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

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

Spolu odtiaľ potom dostávame

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

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

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

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

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

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

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

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

Úloha 9. V príklade 1.3 (iv) bola dvojbodová množina $X = \{(1, 2), (3, 4)\} \subset \mathbb{A}^2(\mathbb{Q})$ popísaná ako riešenie sústavy troch kvadratických rovníc. Ukážte, že

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

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

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

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

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

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

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

Úloha 10. V okruhu R uvažujme rastúcu reťaz ideálov $I_0 \subset I_1 \subset I_2 \subset \dots$. Ukážte, že

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

je ideál v R .

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

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

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

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

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

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

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

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

Úloha 11. Nech k je pole. Ukážte, že okruh polynómov s nekonečne veľa premennými $k[x_1, x_2, \dots]$ nie je noetherovský.

*** Úloha 12.** Uvažujme množinu reálnych funkcií spojitých na intervale $(0, 1) \subset \mathbb{R}$. Táto množina tvorí okruh. Ukážte, že ani tento okruh nie je noetherovský.

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

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

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

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 (overte si to!). Taktiež platí, že $J_m \subset J_{m+1}$ pre všetky m (overte si to!). Máme teda rastúcu reťaz ideálov v R ,

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

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

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

Pre každé a_{ij} ($i = 0, \dots, N, j = 1, \dots, n_i$) zvolíme 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

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

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

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. \square

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

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

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

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

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

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

Príklad 2.10. V príklade 1.11 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 $I(M) = (y)$.

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

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

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

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

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

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

Tvrdenie 2.14. Nech $I, J, I_\alpha \subset k[x_1, \dots, x_n]$ sú ideály. Potom

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

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

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

Pre dôkaz druhej rovnosti si všimnime, že

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

Z predchádzajúceho tvrdenia potom máme

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

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

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

3. ZARISKIHO TOPOLOGIA

Vďaka tvrdeniu 2.14 môžeme 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 algebraickým variety. 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 axiomy:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Definícia 3.1. Polynóm $p = p_0 + p_1x + \dots + p_dx^d \in R[x]$ sa nazýva *primitívny*, ak jeho koeficienty sú nesúdeliteľné t.j. ak najväčší spoločný deliteľ p_0, p_1, \dots, p_d je jednotka v R .

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

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

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

Dôkaz. Nech

$$\begin{aligned} p &= p_0 + p_1x + \cdots + p_r x^r \\ q &= q_0 + q_1x + \cdots + q_s x^s \end{aligned}$$

sú primitívne, predpokladajme, že ich súčin

$$pq = p_0q_0 + (p_1q_0 + p_0q_1)x + \cdots + p_rq_s x^{r+s}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(3) \quad 1 = u'f + v'g.$$

Nech $d \in k[x]$ je spoločný menovateľ koeficientov u' a v' . Vynásobením rovnosti (3) polynómom d dostávame novú rovnosť

$$(4) \quad d = uf + vg,$$

kde $d \in k[x]$ a $u, v, f, g \in k[x, y]$. Zoberme teraz bod $(a_1, a_2) \in \mathbb{A}^2$, ktorý je spoločným riešením sústavy z tvrdenia, teda platí $f(a_1, a_2) = g(a_1, a_2) = 0$. Z rovnosti (4) potom dostávame, že $d(a_1) = 0$. Avšak d je polynóm z $k[x]$ a preto má len konečne veľa riešení. Máme teda len konečne veľa možností pre hodnotu prvej súradnice bodu (a_1, a_2) . Úplne analogicky (postupom cez $(k(y))[x]$) sa tiež ukáže, že ak (a_1, a_2) je spoločné riešenie sústavy $f = g = 0$, potom a_2 môže nadobúdať len niektorú z konečne veľa hodnôt. Môže teda existovať len konečne veľa spoločných riešení tejto sústavy. \square

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

- (a) Ak všetky f_i sú konštantny 0, potom $X = V(0) = \mathbb{A}^2$.
- (b) Nech f_1, \dots, f_r nie sú nulové polynómy. Predpokladajme, že tieto polynómy sú nesúdeliteľné. Potom podľa Tvrdenia 3.4 existuje len konečne veľa bodov (a_1, a_2) takých, že $f_1(a_1, a_2) = \dots = f_r(a_1, a_2) = 0$, čiže varieta X pozostáva z konečného (možno aj nulového) počtu bodov.
- (c) Nech $d \in k[x]$ je najväčší spoločný deliteľ polynómov f_1, \dots, f_r , stupeň $d > 0$. Potom máme polynómy f'_1, \dots, f'_r také, že $f_1 = df'_1, \dots, f_r = df'_r$, pričom $\text{nsd}(f'_1, \dots, f'_r) = 1$. Skúmame ideál generovaný polynómami f_1, \dots, f_r :

$$(f_1, \dots, f_r) = (df'_1, \dots, df'_r) = (d)(f'_1, \dots, f'_r)$$

(preverte si poslednú rovnosť!). Preto $X = X_1 \cup X_2$, kde $X_1 = V(d)$ a $X_2 = V(f'_1, \dots, f'_r)$. Varieta X_1 je rovinná krivka a varieta X_2 pozostáva z konečného počtu bodov (viď prípad (b)).

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

4. PROBLÉMY, PŘÍKLADY

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

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

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

$$\begin{aligned} X_1 &= V(I_1), & I_1 &= (f_1, \dots, f_r) \\ X_2 &= V(I_2), & I_2 &= (g_1, \dots, g_s), \end{aligned}$$

Vieme už, že

$$\begin{aligned} \text{ak } I_1 &\subset I_2, \text{ potom } X_1 \supset X_2, \\ \text{ak } I_1 &= I_2, \text{ potom } X_1 = X_2. \end{aligned}$$

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

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

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

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

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

Vieme overiť, či $V(I) = V(J)$?

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

$$\begin{aligned} z - x^3 &= (z - xy) + x(y - x^2) \in J, & \text{čiže } I &\subset J, \\ z - xy &= (z - x^3) - x(y - x^2) \in I, & \text{čiže } J &\subset I. \end{aligned}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

takže $t^3 + t^2 - 2 \in I$.

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

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

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

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

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

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

$$(5) \quad I = (x + xy, y + xy, x^2, y^2) \subset k[x, y].$$

Ukážeme, že znovu platí $I = (x, y)$. Na jednu stranu je zrejme, že $x + xy, y + xy, x^2, y^2 \in (x, y)$, a teda $(x + xy, y + xy, x^2, y^2) \subset (x, y)$. Pre opačnú inklúziu potrebujeme x a y vyjadriť ako kombinácie generátorov (5):

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

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

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

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

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

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

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

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

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

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

$$(6) \quad (y - x^2, z - x^3, x + y + z - 1) = (y - x^2, z - x^3, x^3 + x^2 + x - 1).$$

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

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

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

Pre dôkaz rovnosti (6) potrebujeme ukázať, že

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

To je ale pravda, lebo

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

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

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

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

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

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

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

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

Úloha 13. Vyriešte sústavu pre neznáme x_1, x_2, x_3, x_4 :

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

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

$$(7) \quad b + c_1 \mathbf{u}_1 + \dots + c_d \mathbf{u}_d$$

bod na tejto lineárnej variete. A naopak: každý bod lineárnej variety sa dá napísať v tvare (7) pre nejaké $(c_1, \dots, c_d) \in k^d$. Hľadanie parametrického vyjadrenia je teda hľadanie „vhodného“ zobrazenia z $\mathbb{A}^d(k)$ na varietu.

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

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

lebo toto zobrazenie je nástrojom na generovanie bodov na krivke.

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

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

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

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

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

Problém 6 (implicitizácia). Pre dané zobrazenie

$$\varphi: \mathbb{A}^d \rightarrow \mathbb{A}^n, (t_1, t_2, \dots, t_d) \mapsto (\varphi_1(t_1, t_2, \dots, t_d), \dots, \varphi_n(t_1, t_2, \dots, t_d)), \quad \varphi_i \in k(t_1, \dots, t_d)$$

nájsť rovnice popisujúce obraz.

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

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

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

Úloha 14. Pre zobrazenie

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

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

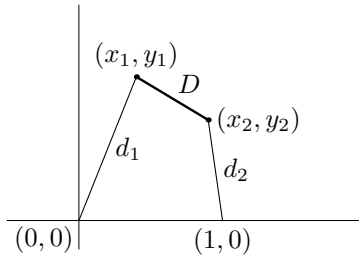
4.3. Stewartova platforma (príklad z robotiky). Ide o plošinu (mnohouholník alebo iný rovinný útvar) v reálnom trojrozmernom priestore, ktorá je niekoľkými „nohami“ pripravená k podložke. Poloha platformy sa určuje iba pomocou dĺžok nôh, teda pre každú nohu môžeme pevne určiť len jej dĺžku, ale už nie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

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

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

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

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



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

$$(8) \quad X = V((x_1 - x_2)^2 + (y_1 - y_2)^2 - D^2).$$

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

Voľba dĺžok je reprezentovaná rovnicami

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

Ide teda o to, koľko majú tieto rovnice spolu s rovnicou popisujúcou množinu stavov (8) riešení.

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

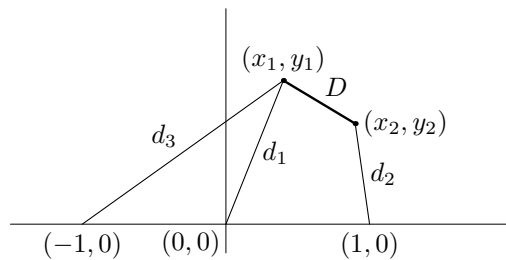
Intuícia 2: Rátajme stupne voľnosti: jeden koncový bod jednoznačne určíme dvoma skalárnymi (kartézskymi alebo polárnymi súradnicami). Pre určenie druhého koncového bodu potrebujeme ešte jednu súradnicu. Teda táto platforma má tri stupne voľnosti. My sme však dodali len dve nohy, čiže platforme zadávame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

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

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

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

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



Dostávame tak ďalšiu rovnicu

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

ktorá spolu s tromi predchádzajúcimi už určí nularozmernú algebraickú varietu.

* **Úloha 15.** Popíšte rovnicami Stewardovu platformu (môžete sa obmedziť na špeciálny prípad z prednášky):

- (i) treba nájsť systém rovníc popisujúci množinu všetkých stavov platformy ako algebraickú varietu v nejakom afinnom priestore,
- (ii) treba napísať dodatočné rovnice popisujúce polohu platformy, keď určíme dĺžky nôh.

KAGDM FMFI UK BRATISLAVA

E-mail address: jana.pilnikova@fmph.uniba.sk