

## 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

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

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

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

Polynóm  $f \in k[x_1, x_2, \dots, x_n]$  predstavuje funkciu na priestore  $\mathbb{A}^n(k)$  s hodnotami v  $k$ : za premennú  $x_i$  budeme dosadzovať  $i$ -tú súradnicu bodu z  $\mathbb{A}^n(k)$ . V nasledovnom budeme pre bod  $a \in \mathbb{A}^n(k)$  a polynóm  $f \in k[x_1, \dots, x_n]$  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  $f_1, \dots, f_r$  (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  $\{(a_1, \dots, a_n)\} = V(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$ ,
- (iv) dvojbodová množina  $X = \{(1, 2), (3, 4)\} \subset \mathbb{A}^2(\mathbb{Q})$ ,  $X = V((x-1)(x-3), (x-1)(y-4), (y-2)(x-3), (y-2)(y-4))$  (presvedčte sa o tom!) Tú istú varietu môžeme 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  $l_1, \dots, l_r \in k[x_1, \dots, x_n]$  sú lineárne polynómy, označme  $X = V(l_1, \dots, l_r)$ . Ak  $X \neq \emptyset$ , nazývame  $X$  *lineárnou varietou*. Ak sú navyše rovnice definujúce  $X$  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) *Regulárna kuželosečka* je množina bodov v  $\mathbb{A}^2$  vyhovujúcich rovnici  $f(x, y) = 0$ , kde  $f \in k[x, y]$  je ireducibilný 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

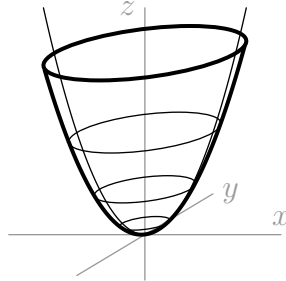
$$g(x) = \frac{p(x)}{q(x)}, \quad p, q \text{ sú nesúdeliteľné polynómy nad } k,$$

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

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

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

PRÍKLAD 1.8. Skúsme popísať plochu  $X$ , ktorá vznikne 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  $X = V(z - (x^2 + y^2))$ .

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  $\mathbb{C} = \bar{\mathbb{R}}$  má totiž táto rovnica nekonečne veľa riešení.

PRÍKLAD 1.11. Špeciálnymi algebraickými varietami sú tzv. súradnicové podpries-  
tory:

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

$$\begin{aligned} f_1 &= y^2 z^3 \\ f_2 &= x^5 z^4 \\ f_3 &= x^2 y z^2 \end{aligned}$$

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

Polynóm  $f_1$  popisuje varietu

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

Podobne rozpíšeme variety určené polynómami  $f_1, f_2$ :

$$\begin{aligned} X_2 &= V(f_2) = H_x \cup H_z \\ X_3 &= V(f_3) = H_x \cup H_y \cup H_z. \end{aligned}$$

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

Iný prístup: riešime sústavu rovníc

$$\begin{aligned} y^2 z^3 &= 0 \\ x^5 z^4 &= 0 \\ x^2 y z^2 &= 0. \end{aligned}$$

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

TVRDENIE 1.13. 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

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

Ukážeme, že

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

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

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 1.14.** 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  $a \in \mathbb{Z}$ . 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 varietou. Presnejšie, najmenšou algebraickou varietou obsahujúcou množinu  $M$  je celá  $x$ -os.

**TVRDENIE 1.15.** *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 1.16.** 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 a ideály

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:

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

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 2.1. *Komutatívny okruh (s jednotkou)* je neprázdna množina  $R$  s dvoma binárnymi operáciami  $+$ :  $R \times R \rightarrow R$ ,  $\cdot$ :  $R \times R \rightarrow R$ , 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)  $(R, \cdot)$  je komutatívny monoid, čiže
  - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  pre všetky  $a, b, c \in R$ ,
  - $a \cdot b = b \cdot a$  pre všetky  $a, b \in R$ ,
  - $\exists 1 \in R$  s vlastnosťou, že  $1 \cdot a = a$  pre ľubovoľné  $a \in R$ ,
- (iii) pre všetky  $a, b, c \in R$  platí  $a \cdot (b + c) = a \cdot b + a \cdot c$

POZNÁMKA 2.2. 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 2.3. 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 2.4. Nech  $R$  je okruh (komutatívny s jednotkou), potom množina  $R[x]$  s operáciami  $+$  a  $\cdot$  definovanými nasledovne:  $\forall f, g \in R[x]$ , kde  $f = f_0 + f_1x + \dots + f_mx^m$ ,  $g = g_0 + g_1x + \dots + g_nx^n$  je

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

je *okruhom polynómov* o premennej  $x$  nad  $R$ .

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

DEFINÍCIA 2.5. Ak  $k$  je pole, tak  $k[x_1, x_2, \dots, x_n] = (k[x_1, x_2, \dots, x_{n-1}])[x_n]$ . Podobne pre ľubovoľný okruh  $R$  zdefinujeme  $R[x_1, x_2, \dots, x_n]$ .

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

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

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

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

Celé číslo

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

sa nazýva *stupeň monómu* (1).

Každý polynóm sa dá zapísať ako konečný súčet monómov

$$f = \sum_{\alpha} c_{\alpha} x^{\alpha}, \quad c_{\alpha} \in k,$$

kde sčítavame cez konečne veľa navzájom rôznych  $n$ -tíc  $\alpha \in \mathbb{N}_0^n$ . Skalár  $c_{\alpha} \in k$  nazývame *koefficientom* pri monóme  $x^{\alpha}$ . 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 koeficientom.

### 3. Ideály

**PRÍKLAD 3.1.** 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 môžeme 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 3.2.** 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  $a \cdot r \in I$ .

Nech  $G \subset R$  je ľubovoľná množina. Zápisom  $\langle G \rangle$  budeme označovať množinu všetkých konečných kombinácií prvkov z  $G$  nad okruhom  $R$ , t.j. množinu  $\{r_1 g_1 + r_2 g_2 + \dots + r_k g_k\}$ . Zrejme  $G$  tvorí ideál v  $R$ . (Dôkaz: dú.)

**DEFINÍCIA 3.3.** 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  $r_1, r_2, \dots, r_k \in R$  a  $g_1, g_2, \dots, g_k \in G$  také, že

$$a = r_1 g_1 + r_2 g_2 + \dots + r_k g_k.$$

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

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

**PRÍKLAD 3.4.**

- 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  $(3), (5), (8), \dots$

PRÍKLAD 3.5. Zoberme v okruhu  $\mathbb{Z}$  ideál  $I = (21, 15)$ . Pomocou Euklidovho algoritmu zistíme, že najväčším spoločným deliteľom čísel 21 a 15 je číslo 3. Z algoritmu navyše vieme získať aj zápis čísla 3 ako kombináciu pôvodných dvoch čísel:

$$21 = 1 \cdot 15 + 6$$

$$15 = 2 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

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

$$3 = 15 - 2 \cdot 6 = 15 - 2 \cdot (21 - 1 \cdot 15) = 3 \cdot 15 - 2 \cdot 21$$

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 3.6.

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

LEMA 3.8. Pre ideál  $I \subseteq R$  platí

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

Dôkaz. Zjavné. □

DEFINÍCIA 3.9. Ideál  $I$  v okruhu  $R$  sa nazýva

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

PRÍKLAD 3.10. 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  $a \cdot b = 6 \in (6)$ , 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 3.11. Euklidov algoritmus možno jednoducho aplikovať aj v okruhu  $k[x]$ . Nech napríklad  $I = (x^4 + x, x^2 - 1)$ . Postupným delením so zvyškom dostávame:

$$x^4 + x = (x^2 + 1) \cdot (x^2 - 1) + (x + 1)$$

$$x^2 - 1 = (x - 1) \cdot (x + 1) + 0$$

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

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

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

**DEFINÍCIA 3.12.** Okruh  $R$  sa nazýva *okruhom hlavných ideálov*, ak každý ideál v  $R$  je hlavný.

**VETA 3.13.**

- (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 3.14.** 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  $f$  obsahuje 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

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

a teda podľa lemy 3.8 platí  $J = k[x, y]$ .

#### 4. Afinné algebraické variety a ideály

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

**PRÍKLAD 4.1.** 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  $g(x, y) = h_1f_1 + h_2f_2$  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 môžeme priradiť ideál pozostávajúci z polynómov, ktoré sú nulové vo všetkých bodoch variety (bližšie to budeme skúmať čoskoro). Vychádza nám nová otázka: ako je to so vzájomnou jednoznačnosťou medzi varietami a ideálmi?

Najprv potrebujeme kritérium pre porovnávanie dvoch ideálov.

**LEMA 4.2.** V komutatívnom okruhu  $R$  platí, že  $(f_1, \dots, f_r) = (g_1, \dots, g_s)$  práve vtedy, keď

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

*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

$$f = p_1f_1 + \dots + p_rf_r \text{ pre nejaké } p_1, \dots, p_r \in k[x_1, \dots, x_n].$$

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

$$f = r_1g_1 + \dots + r_sg_s \text{ pre nejaké } r_1, \dots, r_s \in k[x_1, \dots, x_n],$$

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

**LEMA 4.3.** *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  $V(g_1, \dots, g_s) \subset V(f_1, \dots, f_r)$ .  $\square$

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

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

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 4.4.** Obrátená implikácia z Lemy 4.3 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  $f = (x-1)^2(x+1)$  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  $(f_1, \dots, f_r) = (g_1, \dots, g_s)$ , nestačí overiť, že obe sústavy rovníc majú to isté riešenie, treba naozaj postupovať podľa Lemy 4.2.

**PRÍKLAD 4.5.** Podobne ako v predchádzajúcom 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  $k[x_1, \dots, x_n]$  akoby bolo viac než variet v  $\mathbb{A}^n(k)$ .

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

**LEMA 4.6 (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 4.7. Okruh  $R$ , v ktorom platia tvrdenia Lemy 4.6, sa nazýva *noetherovský*.

Dôkaz Lemmy 4.6. 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  $f_\alpha$  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.  $\square$

PRÍKLAD 4.8. 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 4.9 (**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. Lahko 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  $R$ ,

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

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

$$J_0 = (a_{01}, \dots, a_{0n_0})$$

$$J_1 = (a_{11}, \dots, a_{1n_1})$$

...

$$J_N = (a_{N1}, \dots, a_{Nn_N})$$

Pre každé  $a_{ij}$  ( $i = 0, \dots, N, j = 1, \dots, n_i$ ) zvolme 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  $f \in (f_{ij})$ .  $\square$

**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.  $\square$

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 4.10.** Okruh  $\mathbb{Z}[x]$  je noetherovský.

**DEFINÍCIA 4.11.** 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  $V(F)$  algebraickou 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 4.12.** 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 4.13.** V príklade 1.14 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 4.14.** Vráťme sa zas k monomiálnemu ideálu  $I = (f_1, f_2, f_3)$ , kde  $f_1 = y^2 z^3, f_2 = x^5 z^4, f_3 = x^2 y z^2$ . 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 4.15.** *V nasledovnom  $F, G$  sú podmnožiny  $k[x_1, \dots, x_n]$  a  $S, T$  zas podmnožiny  $\mathbb{A}^n(k)$ . Platí:*

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

*Dôkaz.* dú.  $\square$

### 5. Nullstellensatz

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

#### 5.1. Radikál ideálu.

PRÍKLAD 5.1. V okruhu  $k[x, y]$  majme dva ideály:

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

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

DEFINÍCIA 5.2. Nech  $R$  je ľubovoľný okruh a  $I \subset R$  je ideál. *Radikál ideálu  $I$*  je

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

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

Nasledujúce tvrdenie popisuje niektoré základné vlastnosti radikálov.

- TVRDENIE 5.3. (i)  $\sqrt{I} \supset I$ ,  
(ii)  $\sqrt{I}$  je ideál.  
(iii)  $\sqrt{\sqrt{I}} = \sqrt{I}$ ,

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

(ii) dú.

(iii) Inklúzia „ $\supset$ “ 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  $f \in \sqrt{I}$ .  $\square$

PRÍKLAD 5.4. 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 5.5. 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  $f^d = (x - 1)^2(x + 1)^3g$ . 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 5.6. Radikál ideálu  $I = (x^2, y) \subset k[x, y]$  je ideál  $\sqrt{I} = (x, y)$ .

PRÍKLAD 5.7. 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 5.8. (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  $V(I_1) = V(I_2)$ . Všimnime si, že  $\sqrt{I_1} = \sqrt{I_2}$ . Toto je geometrickým zmyslom radikálov.

**PRÍKLAD 5.9.**  $p(x) = (x-1)^2(x+1)^3(x-2) \in \mathbb{R}[x]$ . Platí, že  $V(p(x))$  je tá istá algebraická varieta ako  $V(\sqrt{p(x)})$ .

### 5.2. Tvrdenie vety.

**TVRDENIE 5.10.** *Nech  $I \subset k[x_1, \dots, x_n]$  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  $a = (a_1, \dots, a_n) \in V(I)$  a preto aj  $f(a) = 0$  pre všetky  $a \in V(I)$ . Teda  $f \in I(V(I))$ .  $\square$

**META 5.11 (Hilbertova veta o koreňoch, Nullstellensatz, 1).** *Ak pole  $k$  je algebraicky uzavreté, potom pre ideál  $I \subset k[x_1, \dots, x_n]$  platí*

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

Nullstellensatz dokazovať nebudeme. Namiesto toho si o chvíľu uvedieme ešte inú verziu 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 radikálnymi ideálmi.*

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

Opačne, nech  $\sqrt{I} = \sqrt{J}$ , odkiaľ máme  $V(\sqrt{I}) = V(\sqrt{J})$ . Z Nullstellensatz potom  $V(I(V(I))) = V(I(V(J)))$ , kde ľavá strana je rovná  $V(I)$  a pravá  $V(J)$  (Tvrdenie 4.15 (iii) z časti o ideáloch a varietách).  $\square$

**PRÍKLAD 5.12.** 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 radikálnymi ideálmi. Avšak  $V(I) = V(J)$  – ide o jednobodovú varietu.

**META 5.13 (Nullstellensatz, 2).** *Ak pole  $k$  je algebraicky uzavreté, potom pre ideál  $I \subset k[x_1, \dots, x_n]$  platí*

$$V(I) = \emptyset \quad \text{práve vtedy keď} \quad 1 \in I \quad (\text{t.j. } I = k[x_1, \dots, x_n]).$$

**POZNÁMKA 5.14.** Implikácia  $\Leftarrow$  je triviálna, tvrdenie Nullstellensatz spočíva v implikácii  $\Rightarrow$ .

**PRÍKLAD 5.15.** Analogicky s prvou verzou, 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 5.16.** *Obe tvrdenia Nullstellensatz (1 a 2) sú ekvivalentné.*

*Dôkaz.* Nech platí tvrdenie Nullstellensatz 1. Podľa Poznámky 5.14 potrebujeme vo verzii 2 ukázať implikáciu  $\Rightarrow$ .

Nech  $V(I) = \emptyset$ , odtiaľ dostávame, že  $1 \in I(V(I))$ . Z 1. verzie Nullstellensatz môžeme 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  $I = (f_1, \dots, f_r) \subset k[x_1, \dots, x_n]$ . 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  $(f_1, \dots, f_r, 1 - yf) \subset k[x_1, \dots, x_n, y]$  a skúmame zodpovedajúcu varietu  $V(f_1, \dots, f_r, 1 - yf)$ . Nech  $(a_1, \dots, a_{n+1})$  je nejaký bod  $\mathbb{A}^{n+1}$ , skúsme zistiť, kedy tento bod patrí našej variete:

- ak  $a_1, \dots, a_n$  sú také, že  $f_1(a_1, \dots, a_n) = \dots = f_r(a_1, \dots, a_n) = 0$ , potom aj  $f(a_1, \dots, a_n) = 0$  (lebo  $f \in I(V(I))$ ), a následne  $1 - a_{n+1}f(a_1, \dots, a_n) = 1 \neq 0$ . Bod  $(a_1, \dots, a_{n+1})$  nevyhovuje poslednej rovnici a preto nepatrí variete  $V(f_1, \dots, f_r, 1 - yf)$ .
- ak  $a_1, \dots, a_n$  sú také, že  $f_i(a_1, \dots, a_n) \neq 0$  pre nejaké  $i$ , potom toto je už rovnica, ktorej bod  $(a_1, \dots, a_{n+1})$  nevyhovuje, a teda nepatrí variete  $V(f_1, \dots, f_r, 1 - yf)$ .

Zistili sme, že  $V(f_1, \dots, f_r, 1 - yf) = \emptyset$ . Z Nullstellensatz 2 potom vyplýva, že  $1 \in (f_1, \dots, f_r, 1 - yf)$ , takže existujú polynómy  $p_1, \dots, p_r, p \in k[x_1, \dots, x_n, y]$  také, že

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

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

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

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

$$f^d = q_1 f_1 + \dots + q_r f_r,$$

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

**TVRDENIE 5.17.** *Nech  $a_1, \dots, a_n \in k$ . Potom  $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n) \subset k[x_1, \dots, x_n]$  je maximálny ideál.*

*Dôkaz.* Hľadáme 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:

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

Podobne  $f_1$  “vyčistíme” pomocou  $x_2 - a_2$  od  $x_2$ :

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

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  $J = k[x_1, \dots, x_n]$ . 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.  $\square$

**LEMA 5.18 (Nullstellensatz, 3).** *Ak pole  $k$  je algebraicky uzavreté, potom každý maximálny ideál v  $k[x_1, \dots, x_n]$  má tvar  $(x_1 - a_1, \dots, x_n - a_n)$  pre nejaké  $a_1, \dots, a_n \in k$ .*

**PRÍKLAD 5.19.** 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 5.20.** *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

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

Odtiaľ

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

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  $\sqrt{\mathfrak{m}} = k[x_1, \dots, x_n]$ . Druhú možnosť môžeme 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  $(a_1, \dots, a_n) \in X$ . Z  $\{(a_1, \dots, a_n)\} \subset X = V(\mathfrak{m})$  potom vyplýva

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

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

### 5.3. Algebraicko-geometrický “slovník”.

| 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 5.21.** 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 metódu 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.