

ÚVOD DO ALGEBRAICKEJ GEOMETRIE

JANA CHALMOVIANSKÁ

AFINNÝ PRIESTOR (VEELMI NEFORMÁLNE OPAKOVANIE)

Afinné/euklidovské priestory: pracoval s nimi (a veľmi dobre im rozumel) už Euklides cca. 300 rokov pr.n.l.

Vektorové priestory:

- objekty: vektory
- štruktúra: vektory vieme sčítavať a násobiť skalármi
- významný vektor: $\mathbf{0}$:
 - v každom vektorovom priestore,
 - v každom podpriestore,
 - nemení sa pri zmene bázy
 - po zavedení skalárneho súčinu má vždy nulovú dĺžku,
 - je kolmý na všetky ostatné vektory
 - ...

Vektorový priestor nad poľom k dimenzie n je izomorfný s k^n : vektory sú n -tice čísel z k .

Afinný priestor: podobný vektorovému, ale “neukotvený”, neexistuje nič ako nulový bod (jediná zásadná odlišnosť od vektorového priestoru).

- bod – poloha
- vektor – posunutie, pohyb, translácia

Afinný priestor ste zrejme mali definovaný ako trojicu:

- $\mathcal{B}$ – množina bodov,
- V – vektorový priestor nad poľom k ,
- $+$: $\mathcal{B} \times V \rightarrow \mathcal{B}$ – binárna operácia spĺňajúca nejaké vlastnosti.

Afinný priestor ste asi označovali $\mathbb{A} = (\mathcal{B}, V, +)$, kvôli zdôrazneniu jeho bodovo-vektorovej štruktúry. Dimenzia $\dim \mathbb{A} = \dim V$.

Tak ako v prípade vektorových priestorov, aj v afinnom priestore máme po zavedení súradníc bijekciu medzi $\mathcal{B}$ a k^n , kde $n = \dim \mathbb{A}$.

Odteraz pre nás afinný priestor nad poľom k bude $\mathbb{A} = \mathbb{A}^n = \mathbb{A}^n(k) = k^n$. Bodovo-vektorová štruktúra je stále prítomná, ale už ju v označení nebudeme zdôrazňovať.

Spravidla budeme pracovať v afinnej rovine, t.j. v $\mathbb{A}^2$, neskôr v projektívnej rovine.

1. AFINNÉ ALGEBRAICKÉ MNOŽINY

Symbolmi $k[x]$, $k[x, y]$, všeobecne $k[x_1, \dots, x_n]$ budeme označovať množinu všetkých polynómov nad poľom k . Polynómy zjavne tvoria vektorový priestor. Okrem sčítania máme aj operáciu násobenia dvoch polynómov (s nejakými vlastnosťami). Takejto štruktúre budeme hovoriť *okruh*. Pre úplnosť formálna definícia (detailnejšie ich budete študovať na algebre):

Definícia 1.1. *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 1.2. 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 1.3. V nasledovných množinách máme štandardne definované operácie sčítania a násobenia:

- $\mathbb{Z}$ – množina všetkých celých čísel tvorí komutatívny okruh s jednotkou.
- Ak k je pole, tak k je aj komutatívny okruh s jednotkou. Byť poľom je silnejšia vlastnosť než byť okruhom.
- $M_n(\mathbb{R})$ – 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.
- $k[x_1, \dots, x_n]$ je komutatívny okruh s jednotkou.

Stupeň polynómu $f \in k[x_1, \dots, x_n]$, $\deg f$, je maximálny stupeň člena, ktorý sa v f vyskytuje s nenulovým koeficientom. Pre $f = 0$ definatoricky $\deg f = -\infty$.

Nech $f \in k[x, y]$. Bod $A = (a_1, a_2) \in \mathbb{A}^2(k)$, pre ktorý platí $f(a_1, a_2) = 0$, nazývame *koreňom polynómu* f , analogicky pre $f \in k[x_1, \dots, x_n]$. Pre $A = (a_1, a_2)$ budeme $f(a_1, a_2)$ zapisovať aj $f(A)$.

Nech $f_1, \dots, f_r \in k[x, y]$. Množinu všetkých spoločných koreňov daných polynómov (t.j. množinu $\{A \in \mathbb{A}^2(k) \mid f_i(A) = 0, i = 1, \dots, r\}$) nazývame *afinnou algebraickou množinou*, označovať ju budeme $V(f_1, \dots, f_r)$.

Príklad 1.4. Lineárna varieta je afinná algebraická množina: je to množina všetkých riešení sústavy lineárnych rovníc.

Príklad 1.5.

- $\{(\cos t, \sin t) \mid t \in (0, 2\pi)\}$ je afinná algebraická množina $V(x^2 + y^2 - 1)$

- zjednotenie súradnicových osí v $\mathbb{A}^2$ tvorí afinnú algebraickú množinu $V(xy)$
- $V(y^2 - xy - x^2y + x^3)$ nájdeme ľahko, keď si všimneme, že $y^2 - xy - x^2y + x^3 = (y - x^2)(y - x)$.
- $V(y^2 - x^3 - x^2)$
- $V(y^2 - x^3 + x)$
- $V(x^2 - 1, y)$

1.1. Afinné algebraické množiny v $\mathbb{A}^1$. Afinná algebraická množina v $\mathbb{A}^1(k)$ je množina spoločných riešení niekoľkých polynomických rovníc: $X = V(f_1, \dots, f_r)$, $f_i \in k[x]$.

- Vybavme najprv špeciálny prípad, keď všetky polynómy sú konštanty 0. Vtedy máme, že $X = V(0) = \mathbb{A}^1$.
- Nech $f_1, \dots, f_r$ nie sú nulové polynómy. Predpokladajme, že tieto polynómy sú nesúdeliteľné, to znamená, že nemajú spoločný koreň, a preto $X = \emptyset$.
- Nech $d \in k[x]$ je najväčší spoločný deliteľ polynómov $f_1, \dots, f_r$, kde $\deg d > 0$. Ak k je algebraicky uzavreté, polynóm d faktorizuje na lineárne členy, $d = (x - a_1)(x - a_2) \dots (x - a_s)$ a $a_1, \dots, a_s$ sú všetky spoločné korene polynómov $f_1, \dots, f_r$, a preto $X = \{a_1, \dots, a_s\}$ je konečná množina. Ak k nie je algebraicky uzavreté, stále je X konečná množina, môže byť prípadne i prázdna.
- Opačne, nech $\mathcal{M} = \{a_1, \dots, a_n\} \subset \mathbb{A}^2$ je ľubovoľná konečná množina. Potom $\mathcal{M} = V((x - a_1)(x - a_2) \dots (x - a_n))$, teda $\mathcal{M}$ je afinná algebraická množina.

Vidíme, že afinné algebraické množiny v $\mathbb{A}^1(k)$ sú presne všetky konečné podmnožiny $\mathbb{A}^1(k)$, a samotná množina $\mathbb{A}^1$.

1.2. Krivky v $\mathbb{A}^2$. Definujme si na $k[x, y]$ nasledovnú binárnu reláciu: pre $f, g \in k[x, y]$ máme $f \sim g$ práve vtedy, keď existuje $a \in k$, $a \neq 0$ také, že $g = af$. Relácia $\sim$ je reláciou ekvivalencie (dú), preto definuje rozklad $k[x, y]$ do tried ekvivalencie. Triedy ekvivalencie $k[x, y]$ podľa tejto relácie okrem tried $[0]$ a $[1]$ nazývame *rovinné krivky*. Teda rovinná krivka je polynóm modulo násobenie nenulovými skalármi.

Tiež ste sa mohli stretnúť s terminológiou, že pri danej relácii sa ekvivalentné polynómy nazývajú *asociované* (líšia sa iba násobením jednotkou, t.j. invertibilným prvkom). Teda asociované polynómy určujú tú istú krivku.

Ak $\deg f = 1$, hovoríme, že $[f]$ je *priamka*. Ak $\deg f = 2$, potom $[f]$ je *kuželosečka*. Ak $\deg f = 3$, tak $[f]$ je *kubika* alebo *kubická krivka*.

S týmto porozumením budeme často samotný polynóm f v $k[x, y]$ nazývať rovinnou krivkou, rozumieť budeme triedu ekvivalencie polynómu, t.j. $[f]$. Napríklad namiesto “krivka $[y^2 - x^3 - x^2]$ ” budeme hovoriť “krivka $y^2 - x^3 - x^2$ ”, prípadne dokonca “krivka $y^2 = x^3 + x^2$ ”. Táto nepresnosť nám odľahčí inak ťažkopádne vyjadrovanie, a nemala by spôsobiť žiadne nedorozumenie.

Prečo nestotožniť krivku s polynómom: naozaj nechceme rozlišovať medzi $y - x^2$ a $2x^2 - 2y$, chceme, aby to bola tá istá krivka.

Prečo nestotožniť krivku s množinou koreňov polynómu: chceme rozlišovať napríklad medzi x^2 a x . Síce platí, že $V(x^2) = V(x)$, no prvá krivka je dvojnásobná priamka, krivka stupňa 2, možno ju poznáte ako singulárnu kuželosečku, a druhá krivka je obyčajná priamka, krivka stupňa 1, a takto ich chceme rozlišovať aj naďalej.

Okruh $k[x, y]$ je *okruhom s jednoznačným rozkladom*, teda každý polynóm $f \in k[x, y]$ sa dá jednoznačne zapísať v tvare

$$(1) \quad f = f_1^{e_1} f_2^{e_2} \dots f_r^{e_r}, \quad e_i \geq 1,$$

kde f_i sú ireducibilné polynómy a $f_i \not\sim f_j$ pre $i \neq j$. Zápis (1) sa nazýva *ireducibilným rozkladom polynómu f* . Jednoznačnosť sa myslí až na poradie a asociovanosť, t.j. ak

$$f = g_1^{d_1} g_2^{d_2} \dots g_s^{d_s}$$

je iný ireducibilný rozklad, tak $s = r$ a po vhodnom preusporiadaní $g_1, \dots, g_r$ máme $f_i \sim g_i$ a $e_i = d_i$, $i = 1, \dots, r$.

Nech teraz $f \in k[x, y]$ je rovinná krivka a nech

$$f = f_1^{e_1} f_2^{e_2} \dots f_r^{e_r}$$

je ireducibilný rozklad polynómu. Potom krivky f_i nazývame *komponentami* krivky f , pričom e_i je *násobnosť* komponenty f_i .

Ak $r = 1$, krivka f je *ireducibilná*. Ak $e_1 = \dots = e_r = 1$, krivka f je *redukovaná*.

Pozor, pojem ireducibilnej krivky nie je ekvivalentný pojmu ireducibilného polynómu! Ireducibilný polynóm zodpovedá ireducibilnej redukovanej krivke, no naopak to neplatí.

1.3. Afinné algebraické množiny v $\mathbb{A}^2$. *Euklidovský okruh* (neformálne) je taký okruh s jednoznačným rozkladom, v ktorom funguje Euklidov algoritmus na nájdenie najväčšieho spoločného deliteľa dvoch prvkov.

Cvičenie 1.6. Okruh celých čísel $\mathbb{Z}$ je okruhom s jednoznačným rozkladom. Pomocou Euklidovho algoritmu nájdite najväčší spoločný deliteľ čísel 21 a 15 a vyjadrite ho ako ich kombináciu.

Cvičenie 1.7. Okruh polynómov o jednej premennej nad poľom je okruhom s jednoznačným rozkladom. Pomocou Euklidovho algoritmu nájdite najväčší spoločný deliteľ polynómov $x^4 + x$ a $x^2 - 1$ a vyjadrite ho ako ich kombináciu.

Lema 1.8. *Nech $f, g \in k[x, y]$, nech f je ireducibilný a nech g nie je deliteľný polynómom f . Potom f a g majú len konečne veľa spoločných koreňov.*

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

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

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

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

po vynásobení rovnosti najmenším spoločným násobkom menovateľov máme rovnosť polynómov

$$pf + qg = d,$$

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

Tak isto ukážeme, že existuje len konečne veľa možností pre hodnotu prvej súradnice spoločného koreňa, čím je tvrdenie lemy dokázané. $\square$

Tvrdenie 1.9. *Nech $f, g \in k[x, y]$ sú nesúdeliteľné polynómy. Potom $V(f, g) = V(f) \cap V(g)$ je konečná množina.*

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

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

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

Afinná algebraická množina v $\mathbb{A}^2(k)$ je množina spoločných koreňov niekoľkých polynómických rovníc: $X = V(f_1, \dots, f_r)$, $f_i \in k[x, y]$. Zistíme teraz, ako môžu afinné algebraické množiny vyzeráť.

- (a) Ak všetky f_i sú konštanty 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 ukázanej vety 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 X pozostáva z konečného (možno aj nulového) počtu bodov.
- (c) Nech $d \in k[x]$ je najväčší spoločný deliteľ polynómov $f_1, \dots, f_r$, kde $\deg d > 0$. Potom máme polynómy $f'_1, \dots, f'_r$ také, že $f_1 = df'_1, \dots, f_r = df'_r$, pričom $\text{NSD}(f'_1, \dots, f'_r) = 1$. Potom zrejme $X = X_1 \cup X_2$, kde $X_1 = V(d)$ a $X_2 = V(f'_1, \dots, f'_r)$. Množina X_1 je množinou bodov rovinnej krivky d a množina X_2 pozostáva z konečného počtu bodov (viď prípad (b)).

KAG FMFI UK BRATISLAVA

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