

Úvod do algebraickej geometrie

Jana Chalmovianská

KAG FMFI UK BRATISLAVA

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

KAPITOLA 1

Afinné algebraické množiny

Afinný priestor (veľmi 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 $n = \dim \mathbb{A}$.

Odtiaľ 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. 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 1.2. 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.
- $\mathcal{M}_n(\mathbb{R})$ – 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.
- $k[x_1, \dots, x_n]$ 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 1.3. Lineárna varieta je afinná algebraická množina: je to množina všetkých riešení sústavy lineárnych rovníc.

PRÍKLAD 1.4.

- $\{(\cos t, \sin t \mid t \in (0, 2\pi))\}$ 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 $\mathbb{A}^1$.

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, 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*. Všeobecne, *stupeň krivky* $[f]$ je stupeň polynómu f .

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 poznať 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.

2.1. 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 2.1. 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 2.2. 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.

V nasledovnej Leme využijeme, že na okruh $k[x, y]$ sa môžeme pozeráť aj ako na okruh $(k[y])[x]$. Ďalej $k(y)$ bude označovať všetky racionálne funkcie premennej y . Táto množina tvorí nielen okruh, ale dokonca pole. Ide o tzv. *podielové pole* okruhu $k[y]$.

LEMA 2.3. *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 2.4. *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 polynomických 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 (dôsledok ukázaného Tvrdenia) 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)).

Lokálne vlastnosti rovinných kriviek

1. Priamka a krivka v afinnej rovine

Nech $f \in k[x, y]$ je rovinná krivka, nech l je priamka $\overleftrightarrow{AB}$, kde $A = (a_1, a_2)$, $B = (b_1, b_2)$. Budeme skúmať prienik priamky a krivky v afinnej rovine. Priamku l si vyjadríme parametricky: $X = (1 - t)A + tB$ ($= A + (B - A)t$), po rozpísaní do súradníc tak máme

$$\begin{aligned} x(t) &= (1 - t)a_1 + tb_1 \quad (= a_1 + (b_1 - a_1)t) \\ y(t) &= (1 - t)a_2 + tb_2 \quad (= a_2 + (b_2 - a_2)t). \end{aligned}$$

Prienik priamky l s krivkou f nájdeme pomocou rovnice

$$(2) \quad f(x(t), y(t)) = 0.$$

Nastane jedna z dvoch možností:

- (i) Ľavá strana v rovnosti (2) je nulová. To znamená, že pre ľubovoľnú hodnotu parametra t leží bod $(x(t), y(t))$ priamky l na krivke f . Priamka l je teda komponentou krivky f .
- (ii) Ľavá strana v rovnosti (2) nie je nulová, máme tak polynomickeú rovnicu pre t , ktorej stupeň nie je väčší ako stupeň f . Na krivke f teda ležia tie body $(x(t), y(t))$ priamky l , keď t je koreňom rovnice (2).

Na polynóm na ľavej strane rovnosti (2) sa budeme odkazovať aj ako na *priesekový polynóm* krivky f a priamky l . Celú rovnicu (2) budeme nazývať tiež *priesekovou rovnicou*.

Ako jednoduchý dôsledok predchádzajúceho pozorovania dostávame nasledovný lemu.

LEMA 1.1. *Nech f je krivka stupňa $d \geq 1$ a nech l je priamka. Ak l nie je komponentou f (t.j. ak $V(l) \not\subseteq V(f)$), tak priamka l pretína krivku f v najviac d bodoch.*

Veľkú časť semestra sa budeme zaoberať zdokonaľovaním tohto výsledku až po známu Bézoutovu vetu, ktorá presne popisuje počet priesekov dvoch rovinných kriviek.

CVIČENIE 1.2. Nájdite spoločné body jednotkovej kružnice $x^2 + y^2 - 1$ a priamky určenej bodmi $(-1, 0)$ a $(1, 1)$.

PRÍKLAD 1.3. Nech $f = y - x^2$ je parabola v $\mathbb{A}^2(\mathbb{R})$ a p nech je priamka prechádzajúca začiatkom súradnicovej sústavy, teda p má rovnicu $y = cx$, kde $c \in k$ popisuje sklon (smernicu) priamky.

Priamka a krivka majú takmer vždy dva spoločné body: $(0, 0)$ a (c, c^2) . Keď sa hodnota c blíži k $(0, 0)$, oba priesečníky sa k sebe približujú, až nakoniec splynú do jedného bodu.

Opačným smerom sa na túto situáciu môžeme pozrieť takto: parabola $y - x^2$ a priamka $y = 0$ majú spoločný iba jeden bod. Avšak pokiaľ by sme zadanie trošička pozmenili, čiže ak by sme veľmi málo zmenili koeficienty v definujúcich rovniciach, tento bod sa rozpadne na dva body.

Všimnime si, že priesekový polynóm má v tomto prípade v danom prieseku dvojnásobnú koreň. Situáciu teda vieme podchytiť aj algebraicky.

CVIČENIE 1.4. Uvažujte kubickú parabolu $y = x^3$ a podobne ako v predchádzajúcom príklade sledujte jej prieseky s priamkami cez $(0, 0)$. Koľko spoločných bodov viete vo všeobecnosti nájsť? Čo sa deje, keď smernica priamky ide k nule?

Nech f je rovinná krivka, l priamka a P bod. Potom symbolom $I_P(f, l)$ budeme označovať *priesekové číslo* alebo *priesekovú násobnosť*, a budeme ním rozumieť nasledovnú hodnotu:

- (i) Ak $P \notin V(l)$, potom $I_P(f, l) = 0$.
- (ii) Ak $P \in V(l)$ a l je komponentou f , potom $I_P(f, l) = \infty$.
- (iii) Ak $P \in V(l)$ a l nie je komponentou f , potom $I_P(f, l)$ je násobnosť t_0 ako koreňa priesekového polynómu $\Phi(t) = (f(x(t_0), y(t_0)))$ (t.j. exponent pri $(t - t_0)$ vo faktorizácii $\Phi(t)$), kde t_0 je parameter zodpovedajúci bodu P na priamke (čiže $P = (x(t_0), y(t_0))$).

Z doterajších úvah dostávame aj spresnenie Lemy 1.1:

LEMA 1.5. *Nech f je krivka stupňa $d \geq 1$ a nech l je priamka. Ak l nie je komponentou f , tak*

$$\sum_{P \in V(l)} I_P(f, l) \leq \deg(f).$$

Nie je možné namiesto nerovnosti v Leme 1.5 dokázať rovnosť, aj keď počítame všetky priesečníky so správnymi násobnosťami:

CVIČENIE 1.6. Nech $f = y^2 - x^3 - x^2$. Nájdite pomocou priesekového polynómu priesečníky tejto krivky

- (a) s x -osou,
- (b) so zvislou priamkou cez $(-1, 0)$.

Naša definícia priesekového čísla má jeden problém: jeho výpočet je viazaný na konkrétnu reprezentáciu krivky a konkrétnu parametrizáciu priamky. Rýchlo nahliadneme, že iná reprezentácia krivky (t.j. iný polynóm určujúci tú istú krivku) vedie k tej istej priesekovej násobnosti. Aby sme mali istotu, že definícia je korektná, potrebujeme sa ešte presvedčiť, že $I_P(f, l)$ nezávisí od toho, akú parametrizáciu priamky si zvolíme.

TVRDENIE 1.7. *Priesekové číslo $I_P(f, l)$ nezávisí od parametrizácie priamky l .*

Dôkaz. Nech $l = \overleftrightarrow{AB} = \overleftrightarrow{CD}$, čo nám dáva dve parametrizácie priamky l , kvôli prehľadnosti budeme parametre v nich označovať rôznymi písmenami:

$$\begin{aligned} X(t) &= (1 - t)A + tB, \\ X(u) &= (1 - u)C + uD. \end{aligned}$$

Priesekové polynómy vzhľadom na jednotlivé parametrizácie označíme Φ a Ψ :

$$\begin{aligned}\Phi(t) &= f((1-t)A + tB), \\ \Psi(u) &= f((1-u)C + uD).\end{aligned}$$

Medzi parametrizáciami pomocou t a u existuje súvislosť, ktorú vieme vyjadriť lineárne. Nech bod A zodpovedá v parametrizácii pomocou C, D parametru u_A , podobne pre B :

$$\begin{aligned}A &= (1 - u_A)C + u_AD, \\ B &= (1 - u_B)C + u_BD.\end{aligned}$$

Potom

$$\begin{aligned}X(t) &= (1-t)A + tB \\ &= (1-t)((1-u_A)C + u_AD) + t((1-u_B)C + u_BD) \\ &= (1 - ((1-t)u_A + tu_B))C + ((1-t)u_A + tu_B)D = X(u(t)).\end{aligned}$$

Máme tak, že $u = u(t) = (1-t)u_A + tu_B$, čiže keď máme priamku l parametrizovanú parametrom u (pomocou C, D), vieme ju jednoducho reparametrizovať pomocou A, B . Podobne, keď poznáme priesekový polynóm $\Psi(u)$ (= priesekový polynóm vzhľadom na parametrizáciu pomocou C, D), ľahko z neho získame aj priesekový polynóm Φ (= priesekový polynóm vzhľadom na parametrizáciu pomocou A, B): $\Phi(t) = \Psi(u(t))$. Bod priamky l , ktorý v parametrizácii cez A, B zodpovedá parametru t_i , v parametrizácii cez C, D zodpovedá parametru $u_i = (1-t_i)u_A + t_iu_B$. Odtiaľ potom máme, že

$$u - u_i = (1-t)u_A + tu_B - ((1-t_i)u_A + t_iu_B) = (t - t_i)(u_B - u_A).$$

Teda ak

$$\Psi(u) = (u - u_1)^{d_1} \dots (u - u_n)^{d_n}$$

je faktorizácia $\Psi(u)$ nad $\bar{k}$, potom

$$\Phi(t) = (u_B - u_A)^{\deg f} (t - t_1)^{d_1} \dots (t - t_n)^{d_n}$$

je faktorizácia $\Phi(t)$ nad $\bar{k}$. □

Na záver si ešte ukážeme, že prieseková násobnosť nezávisí ani od voľby súradnicovej sústavy. Vyskúšajme si to najprv na príklade.

PRÍKLAD 1.8. Majme krivku $f = y - x^2$, uvažujme jej prieseky s priamkou $l = y - 2x$.

Priamku si parametrizujme:

$$x(t) = t, \quad y(t) = 2t,$$

ide o parametrizáciu cez body $A = (0, 0)$ a $B = (1, 2)$, teda $X(t) = (1-t)A + tB$. Zodpovedajúci priesekový polynóm je

$$\Phi(t) = f(X(t)) = f(x(t), y(t)) = y(t) - x^2(t) = 2t - t^2,$$

odkiaľ už ľahko vyčítame, že f a l majú dva priesečníky násobnosti 1: $(0, 0)$ a $(2, 4)$.

Zobrazme teraz f aj l afinnou transformáciou φ :

$$\varphi : (a, b) \mapsto (\tilde{a}, \tilde{b}) = (1 + a + b, 1 + b).$$

Pre inverznú transformáciu tak máme

$$\varphi^{-1} : (\tilde{a}, \tilde{b}) \mapsto (a, b) = (\tilde{a} - \tilde{b}, \tilde{b} - 1).$$

Odtiaľ rovnica pre transformovanú krivku je

$$\tilde{f} = f(\tilde{a} - \tilde{b}, \tilde{b} - 1) = -\tilde{a}^2 + 2\tilde{a}\tilde{b} - \tilde{b}^2 + \tilde{b} - 1.$$

Parametrizácia transformovanej priamky je

$$\begin{aligned}\tilde{x}(t) &= 1 + 3t \\ \tilde{y}(t) &= 1 + 2t.\end{aligned}$$

(Všimnite si, že bod priamky $(0,0)$ zodpovedajúci parametru 0 sa zobrazí do bodu $(1,1)$, ktorý na transformovanej priamke zodpovedá tiež parametru 0; podobne pre bod priamky zodpovedajúci parametru 1.)

Pre priesekový polynóm po transformácii tak máme

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

TVRDENIE 1.9. *Nech f je krivka, l je priamka a P je bod v $\mathbb{A}^2$. Nech ďalej $\varphi : \mathbb{A}^2 \rightarrow \mathbb{A}^2$ je afinná transformácia. Nech $\tilde{f}$ resp. $\tilde{l}$ označujú transformovanú krivku resp. priamku, potom $I_{\varphi(P)}(\tilde{f}, \tilde{l}) = I_P(f, l)$.*

Dôkaz. Pre transformovanú krivku máme $\tilde{f}(X) = f(\varphi^{-1}(X))$. Ak $X(t) = (x(t), y(t))$ je parametrizácia priamky l pred transformáciou, potom $\varphi(X(t))$ je jej parametrizácia po transformácii. Pre priesekový polynóm tak máme

$$\tilde{f}(\varphi(X(t))) = f(\varphi^{-1}(\varphi(X(t)))) = f(X(t)),$$

kde naľavo je priesekový polynóm krivky a priamky pred transformáciou, a napravo je ich priesekový polynóm po transformácii. Týmto je tvrdenie ukázané. $\square$

2. Singulárne body rovinnej krivky

PRÍKLAD 2.1. Nech $f \in \mathbb{R}[x, y]$, $f = y^2 - x^3 - x^2$ je singulárna kubická krivka, *nód* (angl. *node*) a $l = y - cx$ je priamka cez $(0,0)$ s parametrizáciou

$$x(t) = t, \quad y(t) = ct.$$

Priesekový polynóm je potom

$$\Phi(t) = f(x(t), y(t)) = f(t, ct) = t^2(c^2 - t - 1).$$

Čiže $t = 0$ je dvojnásobný koreň priesekového polynómu, a v prípade (a len v prípade) keď $c = \pm 1$ je $t = 0$ dokonca trojnásobným koreňom. Inými slovami, takmer pre všetky priamky cez $O = (0,0)$ je $I_O(f, l) = 2$, a v prípade dvoch priamkoch, konkrétne keď $c = \pm 1$, je $I_O(f, l) = 3$.

Nech $P = (p_1, p_2)$ je bod krivky $f \in k[x, y]$, čiže pre ľubovoľnú priamku l prechádzajúcu bodom P platí $I_P(f, l) \geq 1$. *Násobnosť bodu P na krivke f* označujeme $m_P(f)$ a rozumieme ňou

$$m_P(f) = \min\{I_P(f, l) \mid l \ni P\}.$$

Násobnosť $m_P(f) = 0$ práve vtedy, keď P nie je bod krivky f . Ak $m_P(f) = 1$, bod P sa nazýva *jednoduchý* alebo *regulárny* bod krivky f . Ak $m_P(f) = 2$ ($m_P(f) = 3$, $m_P(f) = r$), bod P sa nazýva *dvojnásobný* (*trojnásobný*, *r-násobný*) bod krivky f . Tiež

môžeme povedať, že krivka f má v P dvojnásobný (trojnásobný, r -násobný) bod. Ak $m_P(f) > 1$, hovoíme tiež, že P je *singulárny* bod krivky f .

PRÍKLAD 2.2. Krivka $f = (x^2 + y^2)^2 + 3x^2y - y^3 \in \mathbb{R}[x, y]$ má v $(0, 0)$ trojnásobný bod. Týmto bodom prechádzajú tri vetvy krivky.

PRÍKLAD 2.3. Pozor, nie je pravda, že násobnosť bodu je rovná počtu vetiev krivky prechádzajúcich cez tento bod, viď napr. krivka $f = y^2 - x^3 \in \mathbb{R}[x, y]$ (singulárna kubika, *hrot*, angl. *cusp*.)

PRÍKLAD 2.4. Singulárny bod krivky nemusí byť viditeľný na obrázku, viď bumerang $y(x^2 + y^2) - x^4 - y^4$: v reálnej rovine krivka “vyzerá hladko” v $(0, 0)$. V komplexnej rovine by sme videli, že jej dotykový kužeľ v $(0, 0)$ pozostáva z troch priamok.

CVIČENIE 2.5. *Astroida* je krivka $f = (1 - x^2 - y^2)^3 - 27x^2y^2 \in \mathbb{R}[x, y]$. Podobne ako kružnica má aj astroida jednoduchú parametrizáciu pomocou goniometrických funkcií:

$$(x(t), y(t)) = (\cos^3 t, \sin^3 t), \quad t \in \langle 0, 2\pi \rangle.$$

Overte, že $(1, 0)$ je singulárnym bodom krivky. Aké ďalšie singulárne body ešte nájdete? (Zatiaľ len metóda pokus - omyl.)

3. Formálne derivovanie

Nech R je okruh bez deliteľov nuly, nech $R[x]$ sú polynómy nad R . Nech

$$f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_dx^d \in R[x].$$

Potom *deriváciou* polynómu f nazývame polynóm

$$f'(x) = f_1 + 2f_2x + \cdots + df_nx^{d-1}.$$

Indukciou r -tá derivácia polynómu f je

$$f^{(r)} = (f^{(r-1)})'.$$

Takto máme deriváciu polynómu definovanú nad ľubovoľným poľom, dokonca aj nad okruhom. Takisto máme týmto už zadefinované aj parciálne derivácie polynómov o viac premenných, keďže

$$k[x_1, x_2, \dots, x_n] = (k[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n])[x_i].$$

Takto definovaná derivácia má rovnaké vlastnosti ako derivácia nad $\mathbb{R}$ definovaná pomocou limit:

TVRDENIE 3.1. *Derivácia nad R má nasledovné vlastnosti:*

- (i) $(f + g)' = f' + g'$ pre $f, g \in R[x]$,
- (ii) $(cf)' = cf'$ pre $c \in R$ a $f \in R[x]$,
- (iii) $(fg)' = f'g + fg'$ pre $f, g \in R[x]$,
- (iv) $(f^r)' = rf^{r-1}f'$ pre $f \in R[x]$,
- (v) pre $g_i \in R[x]$ a $f \in R[x_1, \dots, x_n]$ platí

$$f'(g_1(x), \dots, g_n(x)) = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(g_1(x), \dots, g_n(x))g'_i(x).$$

Dôkaz. dú ((i)–(iv)) je len mechanické rozpisovanie definície, (v) stačí ukázať pre f zostávajúce z jedného člena, a potom aplikovať (i) a (ii). $\square$

Nech

$$(3) \quad f(x) = f_0 + f_1x + f_2x^2 + \dots + f_dx^d.$$

Postupným derivovaním a dosadzovaním sa ľahko presvedčíme, že

$$f(0) = f_0, \quad f'(0) = f_1, \quad f''(0) = 2!f_2, \quad \dots \quad f^{(d)}(0) = d!f_d.$$

Teda zápis (3) polynómu f je aj jeho Taylorovým rozvojom v 0. Všeobecnejšie Taylorov rozvoj f v bode a máme, ak polynóm zapíšeme v tvare

$$f(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \dots + c_d(x-a)^d.$$

VETA 3.2. (*Taylorov rozvoj polynómu.*) Nech $f \in R[x]$, $\deg f = d$ a nech $a \in R$. Potom

$$f(x) = f(a) + f'(a)(x-a) + \frac{1}{2!}f''(a)(x-a)^2 + \dots + \frac{1}{d!}f^{(d)}(a)(x-a)^d.$$

Dôkaz. Nech

$$(4) \quad f(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \dots + c_d(x-a)^d.$$

Aby sme zistili hodnoty koeficientov $c_0, c_1, \dots, c_d$, derivujme túto rovnosť:

$$\begin{aligned} f'(x) &= c_1 + 2c_2(x-a) + \dots + dc_d(x-a)^{d-1} \\ f''(x) &= 2c_2 + 2 \cdot 3c_3(x-a) + \dots + (d-1)dc_d(x-a)^{d-2} \\ &\vdots \\ f^{(d)}(x) &= d!c_d \end{aligned}$$

Keď v týchto rovnostiach (všetne (4)) dosadíme $x = a$, dostávame, že $f^{(i)}(a) = i!c_i$, a tvrdenie vety je dokázané. $\square$

VETA 3.3. (*Taylorov rozvoj polynómu viacerých premenných.*) Nech $f \in R[x_1, \dots, x_n]$, $\deg f = d$ a nech $(a_1, \dots, a_n) \in R^n$. Potom

$$\begin{aligned} f(x_1, \dots, x_n) &= f(a_1, \dots, a_n) + \\ &\quad \sum_i \frac{\partial f}{\partial x_i}(a_1, \dots, a_n)(x_i - a_i) + \\ &\quad \frac{1}{2!} \sum_{i,j} \frac{\partial^2 f}{\partial x_i \partial x_j}(a_1, \dots, a_n)(x_i - a_i)(x_j - a_j) + \dots \\ &\quad (\text{až po } d\text{-tú mocninu}). \end{aligned}$$

Dôkaz. Označme

$$(5) \quad g(t) = f(a_1 + (x_1 - a_1)t, \dots, a_n + (x_n - a_n)t).$$

Urobme teraz Taylorov rozvoj polynómu $g(t)$ v 0:

$$g(t) = g(0) + g'(0)t + \frac{g''(0)}{2!}t^2 + \dots + \frac{g^{(d)}(0)}{d!}t^d,$$

kde jednotlivé koeficienty získame derivovaním zloženej funkcie:

$$\begin{aligned} g(0) &= f(a_1, \dots, a_n) \\ g'(0) &= \sum_i \frac{\partial f}{\partial x_i}(a_1, \dots, a_n)(x_i - a_i) \\ g''(0) &= \sum_{i,j} \frac{\partial^2 f}{\partial x_i \partial x_j}(a_1, \dots, a_n)(x_i - a_i)(x_j - a_j) \\ &\dots \end{aligned}$$

Na záver v (5) nahradíme $g(t)$ jeho Taylorovým rozvojom, položíme $t = 1$, a tým dostaneme dokazovanú rovnosť. $\square$

4. Hľadanie singulárnych bodov krivky

Zatiaľ vieme pre danú krivku a daný bod overiť, či je krivka v tomto bode singulárna, a prípadne zistiť aj jej násobnosť v tomto bode. Teraz by sme chceli pre ľubovoľnú danú krivku jej singulárne body nájsť.

TVRDENIE 4.1. *Nech $P = (p_1, p_2)$ je bod a $f \in k[x, y]$ je rovinná krivka. Potom P je r -násobným bodom krivky f práve vtedy, keď sú splnené nasledovné podmienky:*

- $P \in V(f)$ (t.j. $f(P) = 0$),
- všetky parciálne derivácie f rádu menšieho ako r sú v P nulové,
- existuje parciálna derivácia f rádu r , ktorá je nenulová v P .

Dôkaz. Nech

$$f(x, y) = a_{00} + a_{10}(x - p_1) + a_{01}(y - p_2) + a_{20}(x - p_1)^2 + a_{11}(x - p_1)(y - p_2) + a_{02}(y - p_2)^2 + \dots$$

je Taylorov rozvoj polynómu f v bode P , teda

$$a_{ij} = \binom{i+j}{i} \frac{1}{(i+j)!} \frac{\partial^{i+j} f}{\partial x^i \partial y^j}(P) = \frac{1}{i!j!} \frac{\partial^{i+j} f}{\partial x^i \partial y^j}(P).$$

Priamku cez P parametrizujeme

$$x(t) = p_1 + ut, \quad y(t) = p_2 + vt,$$

bod P teda zodpovedá parametru $t = 0$. Priesekový polynóm potom je

$$\Phi(t) = a_{00} + (a_{10}u + a_{01}v)t + (a_{20}u^2 + a_{11}uv + a_{02}v^2)t^2 + \dots \text{ členy vyšších stupňov.}$$

Odtiaľ vidíme, že P leží na krivke f práve vtedy, keď

$$(6) \quad a_{00} = 0$$

Bod P je aspoň dvojnásobným bodom krivky f práve vtedy, keď (6) a navyše $(a_{10}u + a_{01}v) = 0$ pre všetky (u, v) . Špeciálne, ak $(u, v) = (1, 0)$, dostaneme, že $a_{10} = 0$, a ak $(u, v) = (0, 1)$, potom $a_{01} = 0$. Dostávame teda, že P je aspoň dvojnásobným bodom krivky f práve vtedy, keď (6) a navyše

$$(7) \quad \frac{\partial f}{\partial x}(P) = 0 \quad \text{a} \quad \frac{\partial f}{\partial y}(P) = 0.$$

Ďalej bod P je aspoň trojnásobným bodom krivky f práve vtedy, keď (6), (7) a navyše $(a_{20}u^2 + a_{11}uv + a_{02}v^2) = 0$ pre všetky (u, v) . Podobne ako predtým môžeme postupne

položiť $(u, v) = (1, 0), (0, 1), (1, 1)$ a dostaneme tak podmienku, že bod P je aspoň trojnásobným práve vtedy, keď (6), (7) a navyše

$$\frac{\partial^2 f}{\partial x^2}(P) = 0, \quad \frac{\partial^2 f}{\partial x \partial y}(P) = 0 \quad \text{a} \quad \frac{\partial^2 f}{\partial y^2}(P) = 0.$$

Týmto spôsobom môžeme formulovať podmienky pre r -násobnosť bodu na krivke a tvrdenie je dokázané. $\square$

DÔSLEDOK 4.2. *Nech $O = (0, 0)$ je bod a $f \in k[x, y]$ je rovinná krivka. Potom O je r -násobným bodom krivky f práve vtedy, keď najnižší stupeň člena, ktorý sa v polynóme f nachádza s nenulovým koeficientom, je r .*

DÔSLEDOK 4.3. *Bod $P = (p_1, p_2)$ je singulárnym bodom krivky f práve vtedy, keď*

$$f(P) = 0, \quad \frac{\partial f}{\partial x}(P) = 0 \quad \text{a} \quad \frac{\partial f}{\partial y}(P) = 0.$$

CVIČENIE 4.4. Nájdite všetky singularity astroidy

- (a) nad $\mathbb{R}$,
- (b) nad $\mathbb{C}$.

CVIČENIE 4.5. Overte, že priamka nemá singulárne body.

PRÍKLAD 4.6. Krivka $y^2 + x^3 + x^2 \in \mathbb{R}[x, y]$ má v $(0, 0)$ tzv. *izolovaný singulárny bod* (*izolovanú singularitu*). Ide o jav vyskytujúci sa v reálnej rovine. V komplexnej rovine izolovaná singularita na krivke neexistuje.

5. Dotyčnica krivky, dotykový kužeľ

Nech f je krivka a nech $P \in V(f)$ (t.j. $m_P(f) \geq 1$). Ak $m_P(f) = r$ a l je taká priamka, že $I_P(f, l) > r$, potom l nazývame *dotyčnicou* krivky f v bode P . Pre daný bod P krivky l sa zjednotenie všetkých dotyčníc krivky f v bode P nazýva *dotykovým kužeľom* v bode P .

Krivky f, g sa *dotýkajú* v P , ak

- $P \in V(f)$ a $P \in V(g)$,
- existuje priamka l , ktorá je zároveň dotyčnicou f aj g v bode P .

Z Tvrdenia 1.9 vyplýva, že vlastnosť priamky byť dotyčnicou krivky v danom bode nezávisí od zvolenej afinnej súradnicovej sústavy. Bez ujmy na všeobecnosti sa preto môžeme obmedziť na štúdium dotykového kužeľa krivky v bode $O = (0, 0)$.

Pre skrátenie zápisu budeme ďalej parciálne derivácie polynómu f podľa x resp. y označovať f_x resp. f_y .

Nech $m_P(f) = 1$, t.j. nech O je regulárny bod krivky:

$$f = f_x(O)x + f_y(O)y + \text{členy vyšších stupňov},$$

pričom platí, že $(f_x(O), f_y(O)) \neq (0, 0)$. Priamka l bude dotyčnicou f v O práve vtedy, keď pre jej smerový vektor (u, v) platí, že

$$f_x(O)u + f_y(O)v = 0,$$

čiže keď vektory $(f_x(O), f_y(O))$ a (u, v) sú na seba kolmé, a teda vidíme, že $(f_x(O), f_y(O))$ je normálovým vektorom dotyčnice. V regulárnom bode má teda krivka jedinou dotyčnicu:

TVRDENIE 5.1. *Nech $f \in k[x, y]$ je krivka a nech $P = (p_1, p_2)$ je regulárny bod krivky. Potom*

$$f_x(P)(x - p_1) + f_y(P)(y - p_2)$$

je rovnica dotyčnice krivky f v bode P .

Dôkaz. Uvedená priamka má podľa predchádzajúcich úvah smer dotyčnice. Navyše (dosadením) sa ľahko presvedčíme, že prechádza daným bodom krivky. $\square$

PRÍKLAD 5.2. Nech $P = (p_1, p_2)$ leží na priamke $l = ax + by + c$. Potom dotyčnicou priamky l v bode P je samotná priamka l .

PRÍKLAD 5.3. Jednotková kružnica $f = x^2 + y^2 - 1$ nemá singulárne body, v každom svojom bode má teda jednu dotyčnicu. Konkrétnejšie, ak $P = (p_1, p_2) \in V(f)$, tak dotyčnicou f v bode P je priamka $p_1x + p_2y - 1$.

Teraz zovšeobecníme Tvrdenie 5.1 na ľubovoľný (aj singulárny) bod krivky. Najprv nech $O = (0, 0)$ je je r -násobným bodom krivky $f \in k[x, y]$. Teda

$$f = a_{r0}x^r + a_{r-1,1}x^{r-1}y + \dots + a_{0r}y^r + \text{členy vyšších stupňov},$$

kde aspoň jeden z koeficientov a_{ij} , ($i + j = r$) je nenulový. Priamka l je dotyčnicou f v bode O , ak jej smerový vektor (u, v) je riešením homogénnej časti f r -tého stupňa, teda ak

$$(8) \quad a_{r0}u^r + a_{r-1,1}u^{r-1}v + \dots + a_{0r}v^r = 0.$$

Homogénne polynómy s dvoma premennými sa nápadne podobajú na ľubovoľné (čiže nie nutne homogénne) polynómy s jednou premennou. Špeciálne máme nasledovné tvrdenie:

LEMA 5.4. *Nech pole k je algebraicky uzavreté. Nech $F \in k[u, v]$ je homogénny polynóm, $F \neq 0$. Potom*

$$F(u, v) = (\alpha_1u + \beta_1v)^{r_1} \dots (\alpha_mu + \beta_mv)^{r_m}.$$

Dôkaz. Ide len o úpravu F na polynóm o jednej premennej:

$$\begin{aligned} F(u, v) &= \sum_{i=0}^d a_i u^i v^{d-i} = v^d \sum_{i=0}^c a_i \left(\frac{u}{v}\right)^i \\ &= a_c v^d \left(\frac{u}{v} - \gamma_1\right)^{r_1} \dots \left(\frac{u}{v} - \gamma_s\right)^{r_m} \\ &= a_c v^{d-c} (u - \gamma_1 v)^{r_1} \dots (u - \gamma_m v)^{r_m}. \end{aligned}$$

$\square$

Vráťme sa teraz k hľadaniu dotyčníc krivky v singulárnom bode. Videli sme, že rovnica (8) popisuje dotykový kužel krivky f v bode O . Ak je pole, nad ktorým pracujeme, algebraicky uzavreté, potom polynóm na ľavej strane faktorizuje na lineárne členy:

$$a_{r0}x^r + a_{r-1,1}x^{r-1}y + \dots + a_{0r}y^r = (\alpha_1x + \beta_1y)(\alpha_2x + \beta_2y) \dots (\alpha_rx + \beta_ry).$$

Vidíme, že dotyčnice krivky f v bode O sú presne lineárne faktory homogénnej časti f najnižšieho stupňa.

Ak hľadáme dotyčnice krivky v bode $P \neq (0,0)$, tak v prípade, že je bod P regulárny, je výhodné použiť Tvrdenie 5.1. Naopak, ak je bod P singulárny, zvyčajne sa urobí posunutie, ktorým bod P posunieme do $(0,0)$, a až potom sa hľadajú dotyčnice.

Presnejšie teraz vieme popísať niektoré typy singularít: *nód* je r -násobný bod krivky ($r \geq 2$) s r rôznymi dotyčnicami, *hrot* je zas dvojnásobný bod krivky jednou (dvojnásobnou) dotyčnicou.

PRÍKLAD 5.5. Krivka $y^2 - x^3 - x^2$ má v bode $(0,0)$ dotykový kužeľ $y^2 - x^2$ pozostávajúci z dvoch dotyčníc: $x - y$ a $x + y$.

Krivky v projektívnej rovine

1. Projektívna rovina

Projektívnu rovinu zrejme poznáte ako rozšírenie afinnej roviny pridaním priesečníkov rovnobežiek, tieto nové body sa zvyknú nazývať *nevlastnými bodmi* alebo *bodmi v nekonečne*.

S bodmi v afinnej rovine vieme pracovať vďaka tomu, že každý bod má svoje súradnice. Tie môžeme dosadiť do rovnice priamky (krivky) a zistiť tak, či daný bod leží na priamke (krivke) alebo nie. So súradnicami tiež pracujeme, keď aplikujeme na rovinu afinnú transformáciu.

Nevlastným bodom by sme tiež radi priradili súradnice, aby sme s nimi mohli neskôr počítať. Aby sme ich rozlíšili od súradníc bodom afinnej roviny, používajú sa tzv. *rozšírené súradnice*: rozšírené súradnice bodu $P = (p_1, p_2)$ afinnej roviny budú $(1, p_1, p_2)$. Bod v nekonečne, ktorým prechádza priamka l so smerovým vektorom (u, v) , bude mať rozšírené súradnice $(0, u, v)$. Avšak (u, v) nie je jediný smerový vektor tejto priamky, aj vektor $(5u, 5v)$ je jej smerovým vektorom. Všeobecnejšie, každý nenulový násobok (u, v) je smerovým vektorom tejto priamky. Nevlastný bod priamky l tak má aj súradnice $(0, 5u, 5v)$, všeobecnejšie $(0, \lambda u, \lambda v)$ pre ľubovoľné $\lambda \neq 0$. Aby sme sa vyhli nejednoznačnosti priradenia medzi nevlastnými bodmi a ich súradnicami, používame tzv. *homogénne súradnice*:

$$(0 : u : v) = (0 : \lambda u : \lambda v) \quad \text{pre všetky } \lambda \neq 0.$$

Nakoniec, aby sme udržali čo najväšciu podobnosť medzi súradnicami vlastných a nevlastných bodov, aj pri vlastných bodoch budeme používať homogénne súradnice, teda

$$(1 : p_1 : p_2) = (\lambda : \lambda p_1 : \lambda p_2) \quad \text{pre všetky } \lambda \neq 0.$$

Dostávame sa tak k formálnej konštrukcii projektívnej roviny, či všeobecnejšie, n -rozmerného projektívneho priestoru:

Nech k je pole, potom n -rozmerný projektívny priestor nad k je množina priamok v $\mathbb{A}^{n+1}(k)$, ktoré prechádzajú bodom $(0, \dots, 0)$. Presnejšie, nech $\sim$ je nasledovná relácia na $\mathbb{A}^{n+1}(k) \setminus \{(0, \dots, 0)\}$:

$$(a_0, \dots, a_n) \sim (a'_0, \dots, a'_n), \text{ ak } (a'_0, \dots, a'_n) = (\lambda a_0, \dots, \lambda a_n) \text{ pre nejaké } \lambda \neq 0, \lambda \in k.$$

Lahko sa overí, že $\sim$ je reláciou ekvivalencie, a teda rozkladá množinu $\mathbb{A}^{n+1}(k) \setminus \{(0, \dots, 0)\}$ na triedy ekvivalencie. Body *projektívneho priestoru* sú potom jednotlivé triedy:

$$\mathbb{P}^n(k) = (\mathbb{A}^{n+1}(k) \setminus \{(0, \dots, 0)\}) / \sim.$$

Každý bod v $\mathbb{P}^n$ je takto reprezentovaný viacerými $(n+1)$ -ticami čísel z k : $(a_0, \dots, a_n)$ a $(\lambda a_0, \dots, \lambda a_n)$ ($\lambda \neq 0$) určujú ten istý bod v $\mathbb{P}^n$. Tieto $(n+1)$ -tice nazývame *homogénnymi súradnicami* bodu v $\mathbb{P}^n$. Pri zápise bodu pomocou jeho súradníc používame

dvojbodku: $(a_0 : \dots : a_n)$. Z konštrukcie projektívneho priestoru vyplýva, že

$$(a_0 : \dots : a_n) \in \mathbb{P}^n \quad \text{práve vtedy, keď} \quad a_i \neq 0 \quad \text{pre nejaké } i.$$

PRÍKLAD 1.1. Kružnica v reálnej afinnej rovine predstavuje reálnu projektívnu priamku: stereografická projekcia je bijekcia medzi bodmi kružnice a bodmi projektívnej priamky.

PRÍKLAD 1.2. Sféra v $\mathbb{A}^3(\mathbb{R})$ *nie je* modelom reálnej projektívnej roviny! V tomto prípade stereografická projekcia zobrazí celú nevlastnú priamku na jediný bod. (Pozor, toto ešte nie je dôkaz, že sféra nie je modelom $\mathbb{P}^2$, iba sme sa presvedčili, že stereografická projekcia v tomto prípade nedáva bijekciu.)

PRÍKLAD 1.3. Jednotkový disk, čiže kruh v $\mathbb{A}^2(\mathbb{R})$ spolu s hranicou, t.j. množina

$$\{(a, b) \mid a^2 + b^2 \leq 1\}$$

je modelom reálnej projektívnej roviny, ak stotožníme dvojice protilehlých bodov na hranici. Bijekciu môžeme popísať v troch krokoch:

- (1) vnoríme $\mathbb{A}^2$ do $\mathbb{A}^3$ tak, že rovinu stotožníme so súradnicovou rovinou $z = 0$,
- (2) premietneme body disku v smere osi z na rotačný paraboloid $z = (x^2 + y^2)$
- (3) urobíme projekciu paraboloidu z bodu $(0, 0, 1)$ do roviny $z = 0$.

(dú: vypracovať)

2. Homogénne polynómy

PRÍKLAD 2.1. Krivky v projektívnej rovine chceme definovať podobne ako v afinnom prípade pomocou polynómov. Uvažujme napríklad polynóm $f = z_1 z_2 - 1 \in k[z_0, z_1, z_2]$ a skúsme zistiť, či takýto polynóm popisuje nejakú množinu v projektívnej rovine.

Nech $p = (1 : 1 : 1)$. Potom platí, že $f(1, 1, 1) = 1 \cdot 1 - 1 = 0$ a teda bod p by sme mohli zaradiť medzi body variety. Avšak pre ten istý bod p máme tiež $p = (2 : 2 : 2)$ a tentokrát $f(2, 2, 2) = 2 \cdot 2 - 1 \neq 0$. Množina $\{(a_0 : a_1 : a_2) \in \mathbb{P}^2 \mid f(a_0, a_1, a_2) = 0\}$ nie je korektne definovaná.

Použijeme premennú z_0 na homogenizáciu pôvodného polynómu: nech

$$f^h = z_1 z_2 - z_0^2.$$

Potom bod $p = (1 : 1 : 1)$ spĺňa rovnosť $f^h(p) = 0$ bez ohľadu na to, ktoré súradnice bodu p dosadíme za premenné v polynóme f^h . Všeobecnejšie, nech pre $q = (q_0 : q_1 : q_2) \in \mathbb{P}^2$ platí, že $f^h(q_0, q_1, q_2) = 0$. Ak $(q'_0 : q'_1 : q'_2)$ sú iné súradnice toho istého bodu q , potom $(q'_0 : q'_1 : q'_2) = (\lambda q_0 : \lambda q_1 : \lambda q_2)$ pre nejaké λ . Po dosadení týchto súradníc do zhomogenizovaného polynómu f^h dostávame

$$f^h(\lambda q_0, \lambda q_1, \lambda q_2) = \lambda q_1 \lambda q_2 - (\lambda q_0)^2 = \lambda^2 (q_1 q_2 - q_0^2) = \lambda^2 f^h(q_0, q_1, q_2) = 0.$$

Množina

$$\{(a_0 : a_1 : a_2) \in \mathbb{P}^2 \mid f^h(a_0, a_1, a_2) = 0\}$$

je tak korektne definovaná.

DEFINÍCIA 2.2. $F \in k[z_0, \dots, z_n]$ sa nazýva *homogénny polynóm (forma) stupňa d* , ak všetky jeho členy majú stupeň d :

$$(9) \quad F = \sum_{i_0 + \dots + i_n = d} c_{i_0, \dots, i_n} z_0^{i_0} \dots z_n^{i_n}, \quad c_{i_0, \dots, i_n} \in k.$$

PRÍKLAD 2.3.

- $z_1 + z_2 - 5z_3$ – lineárna forma
- $z_1z_2 + z_2z_3 + z_1z_3$ – kvadratická forma
- $z_1^3 - z_2^2z_3$ – kubická forma

LEMA 2.4. *Nech k je nekonečné pole. Potom polynóm $F \in k[z_0, \dots, z_n]$ je homogénny stupňa d práve vtedy, keď pre všetky $\lambda \in k$ platí*

$$F(\lambda z_0, \dots, \lambda z_n) = \lambda^d F(z_0, \dots, z_n).$$

Dôkaz. Zapišme F ako v (9). Nech

$$F(a_0, \dots, a_n) = \sum c_{i_0, \dots, i_n} a_0^{i_0} \dots a_n^{i_n} = 0.$$

Nech $\lambda \in k$. Potom platí

$$\begin{aligned} F(\lambda a_0, \dots, \lambda a_n) &= \sum c_{i_0, \dots, i_n} (\lambda a_0)^{i_0} \dots (\lambda a_n)^{i_n} = \sum \lambda^d c_{i_0, \dots, i_n} a_0^{i_0} \dots a_n^{i_n} \\ &= \lambda^d \sum c_{i_0, \dots, i_n} a_0^{i_0} \dots a_n^{i_n} = \lambda^d F(a_0, \dots, a_n) = 0. \end{aligned}$$

Pre opačnú implikáciu rozpíšme F ako súčet foriem:

$$F = F_0 + F_1 + \dots + F_{d'}, \quad \text{kde } F_i \text{ je forma stupňa } i.$$

Potom pre ľubovoľné $\lambda \in k$ platí

$$F(\lambda z_0, \dots, \lambda z_n) = F_0(\lambda z_0, \dots, \lambda z_n) + F_1(\lambda z_0, \dots, \lambda z_n) + \dots + F_{d'}(\lambda z_0, \dots, \lambda z_n)$$

a podľa predchádzajúcej časti dôkazu potom

$$F_0(z_0, \dots, z_n) + \lambda F_1(z_0, \dots, z_n) + \dots + \lambda^{d'} F_{d'}(z_0, \dots, z_n) - \lambda^d F(z_0, \dots, z_n) = 0.$$

Keďže tento vzťah musí platiť pre všetky λ a tiež všetky body projektívneho priestoru, musí ísť o nulový polynóm, čiže $d = d'$ a $F_i \equiv 0$ pre $i \neq d$. $\square$

DÔSLEDOK 2.5. *Nech $F \in k[z_0, \dots, z_n]$ je homogénny polynóm. Ak $F(a_0, \dots, a_n) = 0$, potom aj $F(\lambda a_0, \dots, \lambda a_n) = 0$ pre ľubovoľné $\lambda \in k$.*

Formy nad k s premennými $z_0, z_1, \dots, z_n$ sú polynómy z okruhu $k[z_0, z_1, \dots, z_n]$. Dajú sa teda rozložiť na súčin ireducibilných polynómov. Z nasledujúcej lemy navyše dostaneme, že ireducibilné členy vo faktorizácii polynómu sú tiež formy.

LEMA 2.6. *Nech $F \in k[z_0, \dots, z_n]$ je forma a nech $g \in k[z_0, \dots, z_n]$ je deliteľom g . Potom g je tiež forma.*

Dôkaz. Nech $F = gh$ a nech g nie je forma. Rozpíšme si g aj h ako súčet foriem:

$$\begin{aligned} g &= G_a + G_{a+1} + \dots + G_b \\ h &= H_c + H_{c+1} + \dots + H_d \quad G_a G_b H_c H_d \neq 0, \end{aligned}$$

kde G_i resp. H_j je forma stupňa i resp. j . Potom

$$gh = G_a H_c + \dots + G_b H_d,$$

kde $G_a H_c \neq 0$ je forma stupňa $a + c$, podobne $G_b H_d$ je forma stupňa $b + d$. Ak by $a < b$ tak $a + c < b + d$, čo je spor. $\square$

Teda ak $F \in k[z_0, \dots, z_n]$ je forma a

$$F = c F_1^{r_1} \dots F_s^{r_s}$$

je jej jednoznačný rozklad, tak F_i sú tiež formy.

Afinnú krivku sme si definovali ako prvok v $(k[x, y] \setminus k) / \sim$, teda je to nekonštantný polynóm v $k[x, y]$ modulo násobenie nenulovými skalármi.

Podobne *projektívna rovinná krivka* alebo krivka v $\mathbb{P}^2(k)$ bude nekonštantná forma F z $k[x_0, x_1, x_2]$ modulo násobenie nenulovými skalármi. Bod $P = (p_0, p_1, p_2) \in \mathbb{P}^2$ leží na krivke F , ak $F(p_0, p_1, p_2) = 0$. Množinu všetkých bodov projektívnej krivky F označujeme podobne ako pri afinných krivkách $V(F)$.

Analogicky ako pri afinných krivkách, ak $F \in k[x_0, x_1, x_2]$ je forma a

$$F = cF_1^{r_1} \dots F_s^{r_s}$$

je jej faktorizácia, potom krivka F_i je *komponentou* krivky F a r_i je *násobnosť* komponenty F_i .

3. Pokrytie projektívneho priestoru afinnými mapami

Projektívny priestor dimenzie n sme formálne definovali ako množinu priamok v $\mathbb{A}^{n+1}$ prechádzajúcich začiatkom súradnicovej sústavy (ekvivalentne ako jednorozmerné podpriestory k^{n+1}).

Na druhej strane si ho často predstavujeme ako rozšírenie afinného priestoru rovnakej dimenzie. Priestor $\mathbb{A}^n$ je tak podmnožinou priestoru $\mathbb{P}^n$. Nevlastné body (body v nekonečne) sú body v $\mathbb{P}^n \setminus \mathbb{A}^n$.

Budeme teraz bližšie skúmať súvis týchto dvoch konštrukcií.

Nech $(a_1, \dots, a_n) \in \mathbb{A}^n$. Priestor $\mathbb{A}^n$ uvažujme ako vložený do $\mathbb{P}^n$, takže bodu $(a_1, \dots, a_n)$ priradíme homogénne súradnice, napríklad $(1 : a_1 : \dots : a_n)$. Týmto spôsobom skonštruujeme všetky také body $\mathbb{P}^n$, ktorých prvá homogénna súradnica je nenulová. Body s prvou súradnicou nulovou sú nevlastné, pričom bod $(0 : a_1 : \dots : a_n)$ zodpovedá všetkým priamkam, ktorých smerový vektor je $(a_1, \dots, a_n)$. Naopak, vezmime bod $(a_0 : \dots : a_n) \in \mathbb{P}^n$ taký, že $a_0 \neq 0$. K tomuto bodu projektívneho priestoru vieme priradiť bod v $\mathbb{A}^n$: platí, že

$$(a_0 : \dots : a_n) = \left(1 : \frac{a_1}{a_0} : \dots : \frac{a_n}{a_0} \right),$$

takže dostávame bod $(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}) \in \mathbb{A}^n$. S afinným priestorom $\mathbb{A}^n$ sme týmto postupom v $\mathbb{P}^n$ stotožnili množinu

$$U_0 = \{(a_0 : \dots : a_n) \in \mathbb{P}^n \mid a_0 \neq 0\}.$$

Vynechali sme nevlastné body

$$\mathbb{P}^n \setminus U_0 = \{(a_0 : \dots : a_n) \in \mathbb{P}^n \mid a_0 = 0\},$$

Množina U_0 nevlastných bodov nie je v $\mathbb{P}^n$ nijak špeciálna. Analogicky definujeme množiny $U_1, \dots, U_n$:

$$U_i = \{(a_0 : \dots : a_n) \in \mathbb{P}^n \mid a_i \neq 0\}.$$

Každá z týchto množín sa dá stotožniť s n -rozmerným afinným priestorom, tak ako sme to urobili v prípade U_0 :

$$\begin{aligned}\varphi_i: \mathbb{A}^n &\rightarrow U_i, & (a_1, \dots, a_n) &\mapsto (a_1 : \dots : a_i : 1 : a_{i+1} : \dots : a_n) \\ \varphi^{-1}: U_i &\rightarrow \mathbb{A}^n, & (a_0 : \dots : a_n) &\mapsto \left(\frac{a_0}{a_i} : \dots : \frac{a_{i-1}}{a_i} : \frac{a_{i+1}}{a_i} : \dots : \frac{a_n}{a_i} \right).\end{aligned}$$

Množiny $U_0, \dots, U_n$ sa nazývajú *afinnými mapami* a všetky spolu pokrývajú celý afinný priestor:

$$\mathbb{P}^n = U_0 \cup U_1 \cup \dots \cup U_n.$$

Inklúzia „ $\supseteq$ ” je zrejmá, keďže $U_i \subset \mathbb{P}^n$, opačná inklúzia platí, lebo ak $(a_0 : \dots : a_n) \in \mathbb{P}^n$, potom existuje $i \in \{0, \dots, n\}$ také, že $a_i \neq 0$, a teda $(a_0 : \dots : a_n) \in U_i$.

4. Krivky v projektívnej rovine

Nás bude takmer výlučne zaujímať projektívna rovina:

$$\mathbb{P}^2(\mathbb{R}) = U_0 \cup U_1 \cup U_2, \quad U_i = \{(a_0 : a_1 : a_2) | a_i \neq 0\}$$

Príklad. $F = z_1^2 + z_2^2 - z_0^2$ je kvadratická krivka v $\mathbb{P}^2(\mathbb{R})$. Skúsme túto krivku vizualizovať, teda načrtnúť V_F . Najjednoduchšie je nakresliť vždy nejakú afinnú časť krivky, uvažujme napríklad body krivky F , ktoré ležia v affinej mape U_0 :

$$V_F \cap U_0 = \{(a_0 : a_1 : a_2) | a_1^2 + a_2^2 - a_0^2 = 0 \wedge a_i \neq 0\}$$

Pre bodu v U_0 platí, že $a_0 \neq 0$, preto môžeme písať

$$(a_0 : a_1 : a_2) = (1 : \frac{a_1}{a_0} : \frac{a_2}{a_0}).$$

Vidíme, že potom $(\frac{a_1}{a_0}, \frac{a_2}{a_0})$ sú afinné súradnice v tejto mape (t.j. keď $U_0 \cong \mathbb{A}^2 \hookrightarrow \mathbb{P}^2$). Afinné súradnice krivky tak musia spĺňať rovnosť $(\frac{a_1}{a_0})^2 + (\frac{a_2}{a_0})^2 - 1 = 0$, teda rovnica danej krivky v afinných súradniciach je $x^2 + y^2 - 1 = 0$, kde $x = z_1/z_0$ a $y = z_2/z_0$.

Nejaké body krivky F ale táto rovnica nepopisuje, presnejšie nepopisuje body krivky F , ktoré neležia v U_0 . Sú to body:

$$z_1^2 + z_2^2 - z_0^2 = 0 \quad \wedge \quad z_0 = 0.$$

Tomuto vyhovujú body $(0 : 1 : i), (0 : 1 : -i)$ – tzv. *kružnicové body*.

Vidíme, že forma stupňa d s $n + 1$ premennými je podobná polynómu stupňa d s n premennými. Medzi nimi sa môžeme presúvať *homogenizáciou* a *dehomogenizáciou*:

- nech $F \in k[z_0, z_1, \dots, z_n]$ je forma, potom polynóm $f(x_1, \dots, x_n) = F(1, x_1, \dots, x_n)$ je dehomogenizáciou F (t.j. $x_i = z_i/z_0$)
- nech $f \in k[x_1, \dots, x_n]$, $\deg f = d$, potom forma $F \in k[z_0, z_1, \dots, z_n]$ stupňa d taká, že $F(1, x_1, \dots, x_n) = f(x_1, \dots, x_n)$ je homogenizáciou f (zapisujeme aj $F = f^h$)

Pomocou homogenizácie a dehomogenizácie vieme prepojiť projektívnu krivku a jej afinnú časť: ak $F \in k[z_0, z_1, z_2]$ popisuje projektívnu krivku, potom dehomogenizácia $f(x, y) = F(1, x, y)$ popisuje jej časť v affinej mape U_0 (analogicky vieme nájsť časti krivky v afinných mapách U_1 a U_2). Naopak, ak $f \in k[x, y]$ je afinná rovinná krivka, potom homogenizácia F polynómu f popisuje *zúplnenie* krivky f .

Pozor, homogenizácia a dehomogenizácia nie sú to celkom inverzné akcie:

$$\begin{aligned} F &= z_0^2 z_1 - z_0 z_1 z_2 + z_0^3 \\ f &= F(1, x_1, x_2) = x_1 - x_1 x_2 + 1 \\ f^h &= z_0 z_1 - z_1 z_2 + z_0^2 \neq F \end{aligned}$$

PRÍKLAD 4.1. Uvažujme reálnu afinnú krivku $(x - 1)^2 + y^2 = 1$. Afinnú rovinu vnoríme do projektívnej ako U_0 :

$$\mathbb{A}^2(\mathbb{R}) \hookrightarrow \mathbb{P}^2(\mathbb{R}), \quad (a, b) \mapsto (1 : a : b).$$

Rovnica krivky potom bude

$$(z_1 - z_0)^2 + z_2^2 = z_0^2.$$

Ako táto krivka “vyzerá” v afinných mapách U_1 a U_2 ?

PRÍKLAD 4.2. Uvažujme reálnu afinnú krivku $y = x^3$ v $\mathbb{A}^2(\mathbb{R})$. Vnoríme $\mathbb{A}^2(\mathbb{R})$ do $\mathbb{P}^2(\mathbb{R})$ ako U_0 a postupnou vizualizáciou krivky v U_1 a U_2 (pre úplnosť a poučenie aj zistíme, aké nevlastné body má krivka v jednotlivých mapách) odhalíme aj singulárny bod tejto krivky.

Krivku môžeme skúsiť vizualizovať aj globálne. Projektívnu rovinu si môžeme predstaviť ako dvojrozmernú sféru, na ktorej sme dva protilahlé body stotožnili. Postupovať pri vizualizácii krivky môžeme napríklad takto:

- (1) vizualizovať časť krivky v $U_0 \cong \mathbb{A}^2(\mathbb{R})$,
- (2) vložiť U_0 do $\mathbb{A}^3(\mathbb{R})$ (ako xy -rovinu),
- (3) zdvihnúť U_0 do roviny $z = 1$,
- (4) premietnuť na jednotkovú sféru - uvidíme aj body v ∞ .

PRÍKLAD 4.3. *Vivianiho krivka* je prienik guľovej a valcovej plochy:

$$\begin{aligned} x^2 + y^2 + z^2 &= 1 \\ (x - \frac{1}{2})^2 + y^2 &= \frac{1}{4} \end{aligned}$$

Ide o priestorovú krivku. Presvedčíme sa, že jej projekciou do yz -roviny je tzv. *Geronova lemniskata*:

$$y^2 - x^2 + x^4 = 0.$$

Vnoríme $\mathbb{A}^2(\mathbb{R})$ do $\mathbb{P}^2(\mathbb{R})$ ako U_0 . V mape U_2 , (t.j. pôvodná y -os sa stane nevlastnou priamkou) má krivka v $(0, 0)$ izolovaný (singulárny) bod.

5. Výpočty v projektívnej rovine

Vo všeobecnosti sa výpočty na projektívnych krivkách, (či na projektívnych algebraických množinách) robia tak, že sa najprv zúžime na afinnú časť krivky obsahujúcu body, o ktoré sa zaujímate (pracujeme s krivkou “lokálne”). No niektoré výpočty sa dajú robiť priamo v projektívnej rovine, špeciálne rovinné krivky sú spravidla výbornými objektami pre takéto “globálne” výpočty.

Nech $F \in k[z_0, z_1, z_2]$ je forma, t.j. ide o krivku v projektívnej rovine. Potom dehomogenizácia $f(x, y) = F(1, x, y)$ popisuje krivku lokálne, presnejšie popisuje jej body, ktoré sa nachádzajú v affinej mape

$$U_0 = \{(a_0 : a_1 : a_2) \mid a_0 \neq 0\},$$

t.j. $f(a_1, a_2) = 0$ práve vtedy, keď $F(1, a_1, a_2) = 0$.

Skúmame teraz derivácie polynómov f a F . Nech najprv F je monóm: $F = z_0^{d_0} z_1^{d_1} z_2^{d_2}$ a teda $f = x^{d_1} y^{d_2}$. Lahko sa presvedčíme, že derivácia dehomogenizácie F sa rovná dehomogenizácii derivácie (inak povedané, dehomogenizácia a derivácia komutujú):

$$F_1 = \frac{\partial F}{\partial z_1} \big|_{(1,x,y)} = d_1 z_0^{d_0} z_1^{d_1-1} z_2^{d_2} \big|_{(1,x,y)} = d_1 x^{d_1-1} y^{d_2} = \frac{\partial f}{\partial x} = f_x.$$

(Deriváciu F podľa z_i zapisujeme skráteno F_i .) Keďže derivácia lineárnej kombinácie monómov je súčet lineárnej kombinácie derivácií, dokázaný vzťah platí pre ľubovoľnú formu a jej dehomogenizáciu, nielen pre monóm.

TVRDENIE 5.1. (Eulerov vzorec) Pre formu $F \in k[z_0, z_1, z_2]$ stupňa d platí

$$z_0 F_0 + z_1 F_1 + z_2 F_2 = dF.$$

Dôkaz. dú □

DÔSLEDOK 5.2. Bod P je singulárnym bodom projektívnej krivky $F \in k[z_0, z_1, z_2]$ práve vtedy, keď

$$F_0(P) = F_1(P) = F_2(P) = 0.$$

TVRDENIE 5.3. Ak P je regulárny bod projektívnej krivky $F \in k[z_0, z_1, z_2]$, potom jej dotyčnica v bode P je

$$F_0(P)z_0 + F_1(P)z_1 + F_2(P)z_2 = 0.$$

Dôkaz. Nech $P = (p_0 : p_1 : p_2)$ a nech napr. $p_0 \neq 0$, budeme teda predpokladať, že $p_0 = 1$, a tak afinné súradnice P sú (p_1, p_2) . Nech f je dehomogenizácia F vzhľadom na z_0 , t.j. $f(x, y) = F(1, x, y)$. Potom dotyčnica f v P má rovnicu

$$f_x(P)(x - p_1) + f_y(P)(y - p_2) = 0.$$

Homogenizáciou tejto rovnice získame rovnicu dotyčnice v $\mathbb{P}^2$:

$$f_x(P)(z_1 - p_1 z_0) + f_y(P)(z_2 - p_2 z_0) = 0$$

a túto upravíme na tvar v tvrdení pomocou Eulerovho vzorca a rovností $F_1(P) = f_x(P)$, $F_2(P) = f_y(P)$ pre bod P s homogénnymi súradnicami $(1 : p_1 : p_2)$. □

Podobne ako sme si v afinnej rovine definovali priesekový polynóm popisujúci priesečníky krivky s parametrizovanou priamkou, si môžeme definovať priesekovú formu projektívnej krivky a parametrizovanej projektívnej priamky:

Nech $F \in k[z_0, z_1, z_2]$ je projektívna krivka a nech $A = (a_0 : a_1 : a_2)$, $B = (b_0 : b_1 : b_2)$ sú rôzne body v $\mathbb{P}^2$. Priamku L cez A, B môžeme parametricky zapísať ako množinu bodov

$$X = sA + tB, \quad \text{kde} \quad (s : t) \neq (0 : 0).$$

Na parametrizáciu sa teda (podobne ako v afinnom prípade) môžeme pozeráť ako na zobrazenie $\mathbb{P}^1 \hookrightarrow \mathbb{P}^2$, $(s : t) \mapsto sA + tB$. Priesekovú formu potom už ľahko dostaneme dosadením parametrizácie L do rovnice krivky:

$$\Phi(s, t) = F(z_0(s, t), z_1(s, t), z_2(s, t)).$$

Naozaj $\Phi(s, t)$ je binárna forma stupňa rovnakého ako bol stupeň krivky F - tu máme prvý rozdiel oproti afinnému prípadu, kde priesekový polynóm mohol mať nižší stupeň, než bol stupeň krivky.

Porovnajme si práve definovanú priesekovú formu s priesekovým polynómom, ktorý sme počítali v afinnom prípade.

Nech F je krivka a L priamka v projektívnej rovine, a nech L nie je komponentou F . Uvažujme bod $P \in V(F) \cap V(L)$. Bez ujmy na všeobecnosti môžeme predpokladať, že $P = (1 : p_1 : p_2)$. Priamka L bude parametrizovaná pomocou svojich bodov $A = (1 : a_1 : a_2)$ a $B = (0 : b_1 : b_2)$ (určite také dva body na priamke ležia). V $\mathbb{P}^2$ je teda jej parametrizácia $(s : a_1s + b_1t : a_2s + b_2t)$ a tak prieseková forma je

$$\Phi = F(s, a_1s + b_1t, a_2s + b_2t).$$

Parametrizácia priamky v $\mathbb{A}^2$ je $(a_1 + b_1\lambda, a_2 + b_2\lambda)$ a zodpovedajúci priesekový polynóm je potom

$$\Psi = f(a_1 + b_1\lambda, a_2 + b_2\lambda).$$

Zrejme $(0 : 1)$ je koreňom Φ , ak bod $B = (0 : b_1 : b_2)$ leží na krivke F . Tento bod neleží v affinej časti f krivky F . Ostatné korene Φ môžeme hľadať v tvare $(1 : t)$. Vidíme, že

$$(10) \quad \Phi(1, t_0) = \Psi(t_0),$$

čiže v affinej mape U_0 pomocou Φ a Ψ dosávame tie isté násobnosti priesekov priamky s krivkou. Preto môžeme priesekovú násobnosť priamky a krivky s tým istým výsledkom počítať aj priamo v projektívnej rovine pomocou priesekovej formy.

Podobne ako pre priesekový polynóm v afinnom prípade, aj pre priesekovú formu sa dá ukázať, že projektívnou transformáciou sa zachováva. Tiež sa dá ukázať, že priesekové číslo definované pomocou priesekovej formy nezávisí od parametrizácie priamky. Môžeme to ukázať buď priamo pre formy, dôkazy by prebiehali úplne rovnako ako v afinnom prípade. Alebo sa obe vlastnosti dokážu reštrikciou na afinnú mapu s poukázaním na (10).

Z konštrukcie priesekovej formy máme aj analógiu Lemy 1.5 (ide už o špeciálny prípad Bézoutovej vety):

LEMA 5.4. *Nech F je krivka stupňa $d \geq 1$ a nech L je priamka v $\mathbb{P}^2$. Ak L nie je komponentou F , tak*

$$\sum_{P \in V(L)} I_P(F, L) \leq \deg(F).$$

V prípade, že je pole k , nad ktorým pracujeme, algebraicky uzavreté, potom

$$\sum_{P \in V(L)} I_P(F, L) = \deg(F).$$

PRÍKLAD 5.5. Uvažujme krivku v affinej rovine, $f = 2y^2 - x^3 - x^2$ a priamku cez body $A = (1, 0)$ a $B = (1, 1)$.

Priesekový polynóm krivky a priamky je kvadratický a nájdeme tak dva jednoduché priesečníky priamky a krivky:

$$\Phi(t) = f(1, t) = 2t^2 - 2 = 2(t - 1)(t + 1),$$

priesečníkmi sú tak body $(1, 1)$ a $(1, -1)$.

Keď túto krivku uvažujeme v projektívnej rovine, popísaná je formou $F = 2z_0z_2^2 - z_1^3 - z_0z_1^2$. Priamka cez A a B má parametrizáciu

$$z_0 = s + t, \quad z_1 = s + t, \quad z_2 = t$$

a prieseková forma je potom

$$\Phi(s, t) = -2(s + t)s(s + 2t).$$

Takto okrem priesečníkov, ktoré sme našli v afinnej mape, nájdeme ešte tretí spoločný priesečník, bod $(0 : 0 : 1)$.

KAPITOLA 4

Bézoutova veta

1. Tvrdenie vety

PRÍKLAD 1.1. Uvažujme priamky $f = y - 3x$ a $g = y - 3x - 1$ nad $\mathbb{C}$. Obe sú krivkami stupňa 1. Priesečník nájdeme až po zúplnení, t.j. nie v afinnej ale v projektívnej rovine.

PRÍKLAD 1.2. Uvažujme kružnice $f = (x + 2)^2 + y^2 - 1$ a $g = (x - 4)^2 + y^2 - 1$ nad $\mathbb{C}$. Ide o krivky stupňa 2, ktoré sa pretínajú v štyroch bodoch. Všetky štyri priesečníky majú komplexné súradnice. Dva sú vlastné a dva sú nevlastné.

PRÍKLAD 1.3. Ak kružnice, s ktorými pracujeme, budú sústredné, nájdeme len dva spoločné body, i keď hľadáme nad komplexnými číslami a v projektívnej rovine, konkrétne nájdeme len kružnicové body $(0 : 1 : i)$ a $(0 : 1 : -i)$. Nech napr. $f = x^2 + y^2 - 1$ a $g = x^2 + y^2 - 4$. Ak skúsime nájsť dotyčnice kriviek v týchto bodoch, zistíme, že v bode $(0 : 1 : i)$ majú obe kružnice spoločnú dotyčnicu $z_1 + iz_2$ (afinne $x + iy$). Podobná situácia je v druhom spoločnom bode. Ide o špeciálny typ dotyku. Ak každý zo spoločných bodov započítame dvojnásobne, aj tieto kružnice majú štyri priesečníky.

VETA 1.4. *Nech f, g sú rovinné krivky bez spoločnej komponenty. Potom počet priesečníkov kriviek f a g sa rovná číslu*

$$\deg f \cdot \deg g$$

za predpokladov:

- *krivky f a g uvažujeme v projektívnej rovine,*
- *pole, nad ktorým pracujeme, je algebraicky uzavreté,*
- *priesečníky sú počítané so správnou násobnosťou.*

2. Resultanty

LEMA 2.1. *Nech $f, g \in R[t]$, kde R je okruh s jednoznačným rozkladom. Potom f a g majú spoločného nekonštantého deliteľa práve vtedy, keď existujú $p, q \in R[t]$ také, že $pf + qg = 0$ a pre stupne p, q platí $\deg p < \deg g$, $\deg q < \deg f$.*

Dôkaz. Nech h je netriviálny spoločný deliteľ polynómov f, g , teda $f = hf_1$, $g = hg_1$, kde $\deg f_1 < \deg f$ a $\deg g_1 < \deg g$. Potom stačí zobrať $p = g_1$ a $q = -f_1$.

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

$$pf = -qg.$$

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

DEFINÍCIA 2.2. Nech $f, g \in R[t]$ sú polynómy stupňov m a n nad okruhom s jednoznačným rozkladom:

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

Štvorcová matica

$$\text{Syl}(f, g) = \left(\begin{array}{cccccc} f_m & f_{m-1} & \cdots & f_0 & 0 & \cdots & 0 \\ 0 & f_m & \cdots & f_1 & f_0 & \cdots & 0 \\ & & \ddots & & & \ddots & \\ 0 & \cdots & 0 & f_m & \cdots & f_1 & f_0 \\ g_n & g_{n-1} & \cdots & g_0 & 0 & \cdots & 0 \\ 0 & g_n & \cdots & g_1 & g_0 & \cdots & 0 \\ & & \ddots & & & \ddots & \\ 0 & \cdots & 0 & g_n & \cdots & g_1 & g_0 \end{array} \right) \quad \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \begin{array}{l} n - \text{krát} \\ \\ m - \text{krát} \end{array}$$

sa nazýva *Sylvestrova matica* polynómov f a g .

Rezultant polynómov f a g je determinant

$$\text{Res}(f, g) = \det \text{Syl}(f, g).$$

POZNÁMKA. Niekedy budeme označovať rezultant polynómov f a g aj $\text{Res}_t(f, g)$, a to v prípade, keď budeme chcieť zdôrazniť, že f, g sú polynómy v premennej t .

TVRDENIE 2.3. *Polynómy $f, g \in R[t]$ majú netriviálneho spoločného deliteľa práve vtedy, keď $\text{Res}(f, g) = 0$.*

Dôkaz. Podľa Lemy 2.1 majú f, g netriviálneho spoločného deliteľa práve vtedy, keď existujú polynómy

$$\begin{aligned} p &= p_{n-1} t^{n-1} + \cdots + p_1 t + p_0, \\ q &= q_{n-1} t^{n-1} + \cdots + q_1 t + q_0 \end{aligned}$$

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

$$\begin{aligned} f_0 p_0 + g_0 q_0 &= 0 \\ f_1 p_0 + f_0 p_1 + g_1 q_0 + g_0 q_1 &= 0 \\ &\vdots \\ f_m p_{n-1} + g_m q_{n-1} &= 0. \end{aligned}$$

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

DÔSLEDOK 2.4. *Ak k je pole a $f, g \in k[t]$, potom f a g majú spoločný koreň nad nejakým rozšírením poľa k práve vtedy, keď $\text{Res}(f, g) = 0$.*

PRÍKLAD 2.5. Polynóm $f \in k[x]$ (k je algebraicky uzavreté pole) má viacnásobný koreň práve vtedy, keď polynómy f a f' majú spoločný koreň. To je ekvivalentné tvrdeniu, že $\text{Res}(f, f') = 0$.

3. Využitie resultantov pri práci s projektívnymi krivkami

Budeme pracovať s projektívnymi krivkami nad k , teda s formami v $k[z_0, z_1, z_2]$. Každú takúto formu môžeme uvažovať ako polynóm v $(k[z_1, z_2])[z_0]$. Okruh $k[z_1, z_2]$ má jednoznačný rozklad, preto môžeme používať vedomosti o resultantoch.

Ak F resp. G sú formy $k[z_0, z_1, z_2]$ stupňa m resp. n , budeme ich často zapisovať ako polynómy v z_0 , t.j.

$$\begin{aligned} F &= F_0 z_0^m + F_1 z_0^{m-1} + \cdots + F_m \\ G &= G_0 z_0^n + G_1 z_0^{n-1} + \cdots + G_n, \end{aligned}$$

kde F_i resp. G_j je forma v z_1, z_2 stupňa i resp. j .

LEMA 3.1. *Nech $F, G \in k[z_0, z_1, z_2]$ sú formy, kde stupeň F je m a stupeň G je n . Nech $(1, 0, 0)$ nie je koreňom F ani G . Uvažujme F a G ako polynómy v z_0 nad $k[z_1, z_2]$. Vtedy $\deg_{z_0} F = m$, $\deg_{z_0} G = n$ a $\text{Res}_{z_0}(F, G)$ je buď 0 alebo forma stupňa mn v premenných z_1, z_2 .*

Dôkaz. Keďže $(1, 0, 0)$ nie je koreňom F , tak F_0 (koeficient pri z_0^m) je nenulový, a tak $\deg_{z_0} F = m$; podobne pre G .

Označme si $R = \text{Res}_{z_0}(F, G)$, ide zrejme o polynóm v z_1, z_2 , $R = R(z_1, z_2)$. Rozpíšeme si determinant $R(\lambda z_1, \lambda z_2)$. Keď druhý riadok príslušnej Sylvestrevej matice vynásobíme λ , tretí λ^2 , ..., n -tý λ^n , $(n+2)$ -hý vynásobíme λ , ..., posledný vynásobíme λ^m , dostaneme rovnosť

$$\lambda^{(\sum_{i=1}^n i + \sum_{i=1}^m i)} R(\lambda z_1, \lambda z_2) = \lambda^{(\sum_{i=1}^{m+n} i)} R(z_1, z_2),$$

odkiaľ po skrátaní dostávame

$$R(\lambda z_1, \lambda z_2) = \lambda^{mn} R(z_1, z_2),$$

čo podľa Lemy 2.4 znamená, že polynóm $R = \text{Res}_{z_0}(F, G)$, ak nie je nulový, je forma stupňa mn . $\square$

V projektívnej rovine môžeme uvažovať projekciu z bodu na priamku: nech L je priamka a S bod, ktorý na nej neleží. Potom pre každý bod $Q \in \mathbb{P}^2$ rôzny od S pretína priamka $\overleftrightarrow{QS}$ priamku L presne v jednom bode, ktorý nazývame *priemetom bodu Q* .

Ak $S = (1 : 0 : 0)$ a L je nevlastná priamka $z_0 = 0$, potom bod $Q = (q_0 : q_1 : q_2)$ sa premietne na bod $(0 : q_1 : q_2)$ (premietacia priamka má rovnicu $q_2 z_1 - q_1 z_2$).

Túto konštrukciu využijeme pri dôkaze nasledovnej vety.

VETA 3.2. *Nech F resp. G sú krivky stupňov m resp. n v $\mathbb{P}^2$ bez spoločnej komponenty. Potom F a G majú nanaľvýš mn spoločných bodov.*

Dôkaz. Nech bod $S = (1 : 0 : 0)$ neleží na krivke F ani na krivke G . Budeme premietat z bodu S na priamku z_0 .

Formy F a G budeme teraz chápať ako polynómy v z_0 nad $k[z_1, z_2]$. Podľa práve dokázanej lemy majú tieto polynómy v z_0 stupeň m a n . Nasledovné tvrdenia sú nad algebraickým uzáverom k zjavne ekvivalentné:

- $(0 : a_1 : a_2)$ je priemet spoločného bodu kriviek F a G ,
- existuje a_0 také, že $F(a_0, a_1, a_2) = G(a_0, a_1, a_2) = 0$,

- $F(z_0, a_1, a_2)$ a $G(z_0, a_1, a_2)$ majú ako polynómy v z_0 spoločný koreň,
- $\text{Res}_{z_0}(F, G)|_{z_1=a_1, z_2=a_2} = 0$.

Vidíme teda, že priemety priesečníkov kriviek F a G zodpovedajú koreňom $(a_1 : a_2)$ formy $\text{Res}_{z_0}(F, G)$. Podľa predchádzajúcej lemy je rezultant $\text{Res}_{z_0}(F, G)$ buď 0 alebo forma stupňa mn v premenných z_1, z_2 . Ak je rezultant nulový, potom polynómy F a G majú spoločného deliteľa (Tvrdenie 2.3), čiže krivky F a G majú spoločnú komponentu, čo sme však v predpokladoch vylúčili.

Máme tak maximálne mn priemetov priesečníkov. Stále môže ale nastať situácia, že jeden priemet zodpovedá viacerým priesečníkom: to sa stane, keď priamka spájajúca dva priesečníky kriviek F a G prechádza cez bod $S = (1 : 0 : 0)$. Tejto situácii sa ľahko vyhneme tak, že bod S zvolíme mimo týchto priamok a následne afinnou transformáciou posunieme do $(0, 0)$. $\square$

DEFINÍCIA 3.3. Nech F, G sú krivky v $\mathbb{P}^2$ a nech $P \in \mathbb{P}^2$ je bod. Potom *priesekovú násobnosť* (priesekové číslo) kriviek F a G v bode P definujeme nasledovne:

- $I_P(F, G) = \infty$, ak P leží na spoločnej komponente,
- $I_P(F, G) = 0$, ak $P \notin V(F) \cap V(G)$,
- ak $F = F_1^{d_1} \dots F_r^{d_r}$ a $G = G_1^{e_1} \dots G_s^{e_s}$ sú rozklady F a G na ireducibilné komponenty, potom $I_P(F, G) = \sum_i \sum_j d_i e_j I_P(F_i, G_j)$,
- ak F, G nemajú spoločnú komponentu a $(1 : 0 : 0)$ neleží na žiadnej spojnici priesečníkov, potom $I_P(F, G)$ je násobnosť $(p_1 : p_2)$ ako koreňa $\text{Res}_{z_0}(F, G)$, kde $(p_0 : p_1 : p_2)$ sú súradnice bodu $P \neq (1 : 0 : 0)$.

Pre overenie korektnosti definície je potrebné ukázať nezávislosť $I_P(F, G)$ od súradnicovej sústavy. To však pre technickú náročnosť na tejto prednáške robiť nebudeme.

DÔSLEDOK 3.4. (Bézoutova veta) *Nech F resp. G sú krivky stupňov m resp. n v $\mathbb{P}^2(k)$, (k je algebraicky uzavreté pole), a nech F a G nemajú spoločnú komponentu. Potom*

$$\sum_{P \in V(F) \cap V(G)} I_P(F, G) = mn.$$

TVRDENIE 3.5. *Nech F je krivka a L priamka v $\mathbb{P}^2$, ktorá nie je komponentou F . Potom obe definície priesekovej násobnosti súhlasia.*

Dôkaz. Nech $L = z_0$ a nech $(1 : 0 : 0)$ neleží na F , teda

$$F = F_d(z_1, z_2) + F_{d-1}(z_1, z_2)z_0 + \dots + F_0(z_1, z_2)z_0^d,$$

kde F_i je forma stupňa i a $F_0 \neq 0$. Nech $P = (0 : 1 : 0)$ je spoločný bod priamky L a krivky F . Násobnosť prieseku F a L v bode P pomocou novej definície spočítame pomocou rezultantov:

$$\text{Res}_{z_0}(F, L) = \begin{vmatrix} F_0 & F_1 & \dots & F_{d-1} & F_d \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \ddots & & \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix} = (-1)^d F_d(z_1, z_2).$$

Prieseková násobnosť potom je násobnosť $(p_1 : p_2) = (1 : 0)$ ako koreňa $F_d(z_1, z_2)$.

Pre výpočet priesekovej násobnosti podľa starej definície potrebujeme najprv parametrizovať priamku L :

$$z_0 = 0, \quad z_1 = s, \quad z_2 = t.$$

Bod P zodpovedá v tejto parametrizácii parametru $(s : t) = (1 : 0)$. Prieseková forma je

$$\Phi(s, t) = F(0, s, t) = F_d(s, t).$$

Vidíme, že prieseková násobnosť priamky L a krivky F je tak ako v predchádzajúcom prípade rovná násobnosti $(1 : 0)$ ako koreňa $F_d(z_1, z_2)$. $\square$

PRÍKLAD 3.6. Nájdime všetky spoločné body parabol

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

aj s ich násobnosťami. Lahko overíme, že v $\mathbb{A}^2$ nemajú tieto krivky žiaden spoločný bod, spoločný majú nevlastný bod $(0 : 0 : 1)$. Pre overenie násobnosti tohto priesečníka budeme premietť z bodu $(0, 0)$ na nevlastnú priamku. Homogénne rovnice kriviek v $\mathbb{P}^2$ sú

$$\begin{aligned} F &= z_0 z_2 - z_1^2 - z_0^2, \\ G &= z_0 z_2 - z_1^2 + z_0^2. \end{aligned}$$

Dostaneme tak

$$\text{Res}_{z_0}(F, G) = \begin{vmatrix} -1 & z_2 & -z_1^2 & 0 \\ 0 & -1 & z_2 & -z_1^2 \\ 1 & z_2 & -z_1^2 & 0 \\ 0 & 1 & z_2 & -z_1^2 \end{vmatrix} = 4z_1^4.$$

Bod $(0 : 0 : 1)$ (ktorý sa vo výpočte rezultantu premieta na bod $(0 : 1)$) je teda štvornásobným priesečníkom daných kriviek.

4. Dodatok: využitie rezultantov pri riešení sústav polynomických rovníc

PRÍKLAD 4.1. Pomocou rezultantov nájdeme spoločné body dvoch rovinných kriviek: hyperboly popísanej polynómom $f = xy - 1$ a kružnice popísanej $g = x^2 + y^2 - 4$. Hľadáme teda riešenia sústavy dvoch rovníc o dvoch neznámych.

Kľúčovým je nasledovné preformulovanie problému: ak f a g chápeme ako polynómy jednej premennej x nad $k[y]$, kedy majú tieto dva polynómy spoločný koreň? Podľa Vety 2.3 je to práve vtedy, keď $\text{Res}_x(f, g) = 0$. Polynóm f je lineárny v x , polynóm g zas kvadratický. Máme

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

Sústava má štyri riešenia: y -súradnica je riešením rovnice $y^4 - 4y^2 + 1 = 0$. Každému z týchto riešení zodpovedá jedna hodnota pre x -súradnicu, čiže dokopy tak dostaneme presne štyri spoločné korene dvoch polynómov z $k[x]$.

PRÍKLAD 4.2. Nájdime prienik kriviek $V(f), V(g) \subset \mathbb{A}^2(\mathbb{C})$, kde

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

Rezultant polynómov f, g vzhľadom na premennú x je

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

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

Zdanlivo tu ide o konflikt s Dôsledkom 2.4. Treba si ale všimnúť, že v prípade, keď dosadíme $y = 0$, už nepracujeme s polynómami stupňov 1 resp. 2 a teda ich Sylvestrova matica nemá stupeň 3. Inak: nie je pravda, že $\text{Res}_x(f, g)(0)$ by bolo rovné $\text{Res}_x(f(x, 0), g(x, 0))$.

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

Skúsme sa pozrieť na Sylvestrovu maticu ako na maticu zobrazenia. Pre jednoduchosť uvažujme situáciu, keď $f, g \in k[x]$, kde k je pole. Sylvestrovu maticu polynómov f a g môžeme chápať aj ako maticu zobrazenia lineárnych priestorov.

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

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

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

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

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

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

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

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

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

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

VETA 4.3. *Nech $f, g \in k[x_1, \dots, x_n]$. Potom existujú polynómy $p, q \in k[x_1, \dots, x_n]$ také, že*

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

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

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

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

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

$$A \cdot \text{ad}A = \text{ad}A \cdot A = |A|I_n.$$

Aplikovaním tohto pravidla na Sylvestrovu maticu dostávame

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

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

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

Už sme si vysvetlili, že Sylvestrová matica je maticou zobrazenia lineárnych priestorov alebo všeobecnejšie modulov nad R , kde teraz $R = k[x_2, \dots, x_n]$: išlo o zobrazenie, ktoré dvojici polynómov (p, q) priradí polynóm $pf + qg$. Vidíme, že toto zobrazenie vektor so súradnicami $v_1, \dots, v_N$, ktorý reprezentuje dvojicu polynómov $(v_1x_1^{n-1} + \dots + v_{n-1}x_1 + v_n, v_{n+1}x_1^{m-1} + \dots + v_{N-1}x_1 + v_N)$, zobrazí na vektor so súradnicami $0, \dots, 0, \text{Res}_{x_1}(f, g)$, ktorý zas reprezentuje polynóm $0x_1^{N-1} + \dots + 0x_1 + \text{Res}_{x_1}(f, g)$. Teda našli sme $p, q \in k[x_1, \dots, x_n]$ také, že $\text{Res}_{x_1}(f, g) = pf + qg$. $\square$

DÔSLEDOK 4.4. Ak $(a_1, a_2, \dots, a_n)$ je spoločným koreňom f a g , potom jeho priemet

$$\pi(a_1, a_2, \dots, a_n) = (a_2, \dots, a_n)$$

je koreňom $\text{Res}_{x_1}(f, g)$.

Používať rezultanty pri hľadaní spoločných bodov dvoch kriviek je teda korektný postup: v Príklade 4.1 polynóm $\text{Res}_x(f, g)$ popisuje varietu, ktorá určite obsahuje všetky body priemetu prieniku $V(f)$ a $V(g)$ na y -os. Potom x -súradnicu môžeme dopočítať buď dosadením konkrétnej y -súradnice do f a g , alebo ešte nájdeme rezultant

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

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

Príklad 4.2 zas ukazuje, že $V((f, g) \cap k[x_2, \dots, x_n])$ naozaj môže byť vlastnou podmnožinou $V(\text{Res}_{x_1}(f, g))$.

PRÍKLAD 4.5. Rezultanty môžeme úspešne použiť aj v prípade, keď krivky, ktorých prienik hľadáme, majú nekonečne veľa spoločných bodov, teda majú spoločnú komponentu.

Nájdime všetky racionálne body (t.j. body, ktorých súradnice sú racionálne čísla) ležiace na krivkách $V(f)$ a $V(g)$, ak

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

Vypočítame rezultanty (aj výpočet rezultantu aj faktorizáciu urobíme pomocou nejakého systému počítačovej algebry):

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

Priemet priesečníkov na y -os teda obsahuje najviac 2 racionálne body. Podobne nájdeme priemet priesečníkov na x -os:

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

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

Ak $y = -1$, potom $f(x, -1) = 0$ pre všetky x , podobne $g(x, -1) = 0$ pre všetky x . Krivky f a g teda obsahujú priamku $y + 1$.

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

Síce je resultant definovaný len pre dva polynómy, možno ho použiť aj na hľadanie spoločných koreňov viacerých polynomických rovníc. Napríklad, ak chceme nájsť spoločné korene polynómov $f, g, h \in k[x, y, z]$, môžeme konštruovať priemety postupne:

$$V(\text{Res}_z(f, g)) \subset \mathbb{A}^2$$

obsahuje priemety koreňov $f = 0, g = 0$ do xy -roviny, podobne

$$V(\text{Res}_z(f, h)) \subset \mathbb{A}^2$$

obsahuje priemety koreňov $f = 0, h = 0$, takže

$$V(\text{Res}_z(f, g), \text{Res}_z(f, h)) \subset \mathbb{A}^2$$

obsahuje priemety koreňov $f = 0, g = 0, h = 0$ do xy -roviny. Pomocou resultantov nájdeme potenciálne priemety na x -os, podobne potenciálne priemety na y -os. Potom ešte analogickým postupom nájdeme potenciálne priemety na z -os. Ak dostaneme len konečne veľa možností pre hodnotu každej súradnice, jednoducho dosadíme všetky možnosti do pôvodných rovníc $f = g = h = 0$, a tak nájdeme všetky korene polynómov $f, g, h \in k[x, y, z]$.

Inflexné body projektívnej krivky

1. Hessián

Nech $F \in k[z_0, z_1, z_2]$ je forma popisujúca krivku v $\mathbb{P}^2$. Nech P je regulárny bod krivky F a nech L je dotyčnica ku krivke F v bode P , teda platí, že $I_P(F, L) \geq 2$. Ak $I_P(F, L) \geq 3$, potom P nazývame **inflexným bodom** krivky F .

Keďže, ako sme ukázali, je $I_P(F, L)$ projektívny invariant, “inflexnosť” bodu sa zachováva pri projektívnych transformáciách, inými slovami inflexný bod krivky sa projektívnou transformáciou zobrazí zas na inflexný bod.

PRÍKLAD 1.1. Skúsme nájsť inflexné body krivky zúplnenia krivky $y^2 = x^3$ v projektívnej rovine. V $\mathbb{P}^2$ je rovnica tejto krivky $F = z_0 z_2^2 - z_1^3$. Jej derivácie sú $(F_i$ znamená $\frac{\partial F}{\partial z_i})$:

$$F_0 = z_2^2, \quad F_1 = -3z_1^2, \quad F_2 = 2z_0 z_2.$$

Odtiaľ zistíme, že krivka F má jediný singulárny bod, a síce $(z_0 : z_1 : z_2) = (1 : 0 : 0)$.

Nech A je regulárny bod krivky F . Dotyčnica F v bode A je potom daná lineárnou formou

$$L : a_2^2 z_0 - 3a_1^2 z_1 + 2a_0 a_2 z_2.$$

Potrebuje túto priamku parametrizovať, aby sme mohli skonštruovať priesekovú formu priamky L a krivky F . K tomu potrebujeme poznať dva body na priamke L . Jedným je bod $A = (a_0 : a_1 : a_2)$. Druhý bod na L nájdeme v tvare $B = (b_0 : b_1 : 0)$. Keďže B leží na L , dostávame tak, že $B = (3a_1^2 : a_2^2 : 0)$.

Teraz môžeme L parametrizovať: $X = sA + tB$. Rozpísané do súradníc:

$$\begin{aligned} z_0 &= a_0 s + 3a_1^2 t, \\ z_1 &= a_1 s + a_2^2 t, \\ z_2 &= a_2 s. \end{aligned}$$

Prieseková forma je potom

$$\Phi(s, t) = F(sA + tB) = \dots = -3a_1 a_2^4 s t^2 - a_2^6 t^3.$$

Vidíme, že $(s : t) = (1 : 0)$ je v každom prípade aspoň dvojnásobným koreňom formy Φ , čo zodpovedá faktu, že priamka L je dotyčnicou krivky F v bode A . Bod A je inflexný, ak $(1 : 0)$ je trojnásobným koreňom, teda ak $-3a_1 a_2^4 = 0$. Tejto podmienke zodpovedá jediný regulárny bod na krivke F , a síce $(0 : 0 : 1)$.

Dotyčnica krivky v regulárnom bode je popísaná prvými deriváciami definujúceho polynómu. Druhé derivácie zas charakterizujú inflexné body.

Matica

$$(F_{ij}) = \left(\frac{\partial^2 F}{\partial z_i \partial z_j} \right)_{i,j=0,1,2}$$

sa nazýva **Hesseho matica** polynómu F . Jej determinant sa nazýva **Hessián** polynómu (alebo krivky) F a označuje sa H_F . Krivka v $\mathbb{P}^2$ určená Hessiánom polynómu (krivky) F je **Hesseho krivka** polynómu (krivky) F . Niekedy sa tiež krivka určená determinantom Hesseho matice nazýva Hessián.

LEMA 1.2. *Nech je na $\mathbb{P}^2$ definovaná bijektívna projektívna transformácia. Nech krivka F sa touto transformáciou zobrazí na krivku G a konkrétne bod $P \in V(F)$ na bod $Q \in V(G)$. Potom $H_F(P) = 0$ práve vtedy, keď $H_G(Q) = 0$.*

Dôkaz. Nech A je matica inverznej transformácie, čiže $\mathbf{p} = A\mathbf{q}$, kde $\mathbf{p}$ resp. $\mathbf{q}$ je stĺpcový vektor so súradnicami bodu P resp. Q . Čiže transformácia $\mathbf{z} \mapsto A\mathbf{z}$ ($\mathbf{z}$ je stĺpcová matica $(z_0 \ z_1 \ z_2)^T$) zobrazí body krivky G na body krivky F , teda pre polynómy F a G platí

$$G(\mathbf{z}) = F(A\mathbf{z}).$$

Derivovaním tejto rovnosti zistíme, že pre Hesseho matice platí

$$(G_{ij})(Q) = (A^T(F_{ij})(P)A).$$

Pre Hessiány potom platí:

$$\begin{aligned} H_G(Q) &= \det((G_{ij})(Q)) = \det(A^T(F_{ij})(P)A) = \det A^T \det(F_{ij}(P)) \det A \\ &= (\det A)^2 H_F(P). \end{aligned}$$

Matica A je regulárna, keďže ide o projektívnu transformáciu, a tak dostávame tvrdenie lemy. $\square$

META 1.3. *Nech P je regulárny bod krivky F . Bod P je inflexný práve vtedy, keď*

$$H_F(P) = 0.$$

Dôkaz. Ak P je priamka, potom každý jej bod je inflexný a ľahko sa presvedčíme, že v tomto špeciálnom prípade je tvrdenie vety pravdivé.

Nech teda stupeň krivky je aspoň 2. Keďže inflexnosť sa zachováva pri projektívnych transformáciách, môžeme predpokladať, že inflexný bod má projektívne súradnice $(1 : 0 : 0)$ (afinné $(0, 0)$) a navyše tiež, že x -os je dotyčnicou krivky v tomto bode, teda dotyčnica má rovnicu $y = 0$ v afinných súradniciach alebo $z_2 = 0$ v projektívnych. Rovnica krivky v afinných súradniciach je teda

$$f(x, y) = ay + (bx^2 + 2cxy + dy^2) + \dots$$

(pokračuje členmi stupňa aspoň 3), kde $a \neq 0$. V projektívnych súradniciach bude potom jej rovnica (d je stupeň krivky)

$$F(z_0, z_1, z_2) = az_2z_0^{d-1} + (bz_1^2 + 2cz_1z_2 + dz_2^2)z_0^{d-2} + \dots$$

Bod dotyku $P = (1 : 0 : 0)$ leží na dotyčnici, ďalší bod na nej je napríklad $Q = (0 : 1 : 0)$, a teda dotyčnica má parametrizáciu $sP + tQ$, v súradniciach $z_0 = s, z_1 = t, z_2 = 0$. Prieseková forma $\Phi(s, t)$ má potom tvar

$$\Phi(s, t) = F(s, t, 0) = bt^2s^{d-2} + \dots$$

Bod P je inflexným práve vtedy, keď $(1 : 0)$ je 3-násobným koreňom Φ , čo nastáva práve vtedy, keď $b = 0$. Ostáva ešte ukázať, že táto podmienka je ekvivalentná s tvrdením, že $H_F(P) = 0$. O tom sa ľahko presvedčíme, keď nájdeme Hessián krivky F v bode P :

$$H_F(P) = \begin{vmatrix} 0 & 0 & a(d-1) \\ 0 & 2b & 2c \\ a(d-1) & 2c & 2d \end{vmatrix} = -2a^2b(d-1)^2.$$

□

PRÍKLAD 1.4. Znovu uvažujme kubickú krivku $F = z_0z_2^2 - z_1^3$. Jej Hessián (a Hesseho krivka) je

$$H_F = \begin{vmatrix} 0 & 0 & 2z_2 \\ 0 & -6z_1 & 0 \\ 2z_2 & 0 & 2z_0 \end{vmatrix} = 24z_1z_2^2.$$

Odtiaľ už ľahko dostaneme, že jediným regulárnym bodom krivky F , ktorý leží zároveň aj na Hesseho krivke, je bod $(0 : 0 : 1)$

DÔSLEDOK 1.5. *Nech F je regulárna krivka v $\mathbb{P}^2$ stupňa aspoň 3. Potom F má inflexný bod.*

DÔSLEDOK 1.6. *Nech F je ireducibilná kubická krivka v $\mathbb{P}^2$. Potom F má najviac 9 inflexných bodov.*

Dôkaz. Ak F má stupeň d , potom jej Hessián má stupeň $3(d-2)$. Z Bézoutovej vety potom už dostávame oba dôsledky. □

Inflexné body Steinerovej kubiky

Nech $F = z_0^3 + z_1^3 + z_2^3 + 3\lambda z_0z_1z_2$ ($\lambda^3 \neq -1$) je regulárna Steinerova kubika. Nájdeme všetky jej inflexné body.

Hessián F je

$$H_F = 27 \cdot 2(-\lambda^2(z_0^3 + z_1^3 + z_2^3) + (4 + \lambda^3)z_0z_1z_2).$$

Pre nájdanie inflexných bodov potrebujeme vyriešiť sústavu rovníc

$$\begin{aligned} (z_0^3 + z_1^3 + z_2^3) + 3\lambda z_0z_1z_2 &= 0 \\ -\lambda^2(z_0^3 + z_1^3 + z_2^3) + (4 + \lambda^3)z_0z_1z_2 &= 0. \end{aligned}$$

Keďže $\lambda^3 \neq -1$, je táto sústava ekvivalentná sústave

$$\begin{aligned} z_0^3 + z_1^3 + z_2^2 &= 0 \\ z_0z_1z_2 &= 0, \end{aligned}$$

ktorej riešenia už ľahko nájdeme:

$$\begin{aligned} P_{00} &= (0 : -1 : 1) & P_{01} &= (0 : \epsilon : 1) & P_{02} &= (0 : \epsilon^2 : 1) \\ P_{10} &= (1 : 0 : -1) & P_{11} &= (1 : 0 : \epsilon) & P_{12} &= (1 : 0 : \epsilon^2) \\ P_{20} &= (-1 : 1 : 0) & P_{21} &= (\epsilon : 1 : 0) & P_{22} &= (\epsilon^2 : 1 : 0) \end{aligned}$$

kde ϵ je primitívna tretia odmocnina z -1 , t.j. je to komplexné číslo, ktoré je riešením rovnice $x^2 - x + 1 = 0$. Steinerova kubika má tak presne deväť inflexných bodov. Všimnime si, že tieto body vôbec nezávisia od parametra λ . Ide o veľmi zaujímavú konfiguráciu bodov. Po trojiciach ležia na priamkach a pre ľubovoľné dva inflexné body

existuje na ich spojnici aj tretí. Inflexné body Steinerovej kubiky tvoria vlastne afinnú rovinu nad trojprvkovým poľom $\mathbb{Z}/3\mathbb{Z}$.

Lineárne systémy kriviek

1. Priestor rovinných kriviek

Pripomeňme, že n -rozmerný projektívny priestor nad poľom k je množina jednorozmerných podpriestorov vektorového priestoru k^{n+1} .

Bod Q v $\mathbb{P}^n$ tak zodpovedá jednorozmernému vektorovému podpriestoru V . Vektor $(a_0, a_1, \dots, a_n)$ v podpriestore V potom určuje homogénne súradnice $(a_0 : a_1 : \dots : a_n)$ bodu Q . Rôzne vektory podpriestoru V určia rôzne homogénne súradnice toho istého bodu Q .

Všeobecnejšie, $(d+1)$ -rozmerný podpriestor k^{n+1} zodpovedá d -rozmernému podpriestoru (t.j. d -rozmernej lineárnej variete) v $\mathbb{P}^n$.

LEMA 1.1. *Krivky v $\mathbb{P}^2(k)$ stupňa d tvoria projektívny priestor nad k stupňa $\frac{1}{2}d(d+3)$.*

Dôkaz. Nech $m_0, m_1, \dots, m_N$ sú všetky monómy stupňa n v premenných z_0, z_1 a z_2 . Nech $F = a_0m_0 + a_1m_1 + \dots + a_Nm_N$ je krivka v $\mathbb{P}^2$ stupňa d . Pre ľubovoľné nenulové λ je potom $\lambda a_0m_0 + \lambda a_1m_1 + \dots + \lambda a_Nm_N$ tá istá krivka. Koeficienty $(a_0 : a_1 : \dots : a_N)$ teda predstavujú homogénne súradnice bodu v N -rozmernom projektívnom priestore. Ostáva ešte určiť dimenziu tohto priestoru. Tá bude o 1 menšia než počet monómov v z_0, z_1 a z_2 stupňa d , čo je rovné kombinačnému číslu $\binom{d+2}{2}$, a teda hľadaná dimenzia je

$$N = \binom{d+2}{2} - 1 = \frac{(d+1)(d+2) - 2}{2} = \frac{d(d+3)}{2}.$$

□

PRÍKLAD 1.2. Priamky v $\mathbb{P}^2$ tvoria dvojrozmerný projektívny priestor, tzv. *duálnu rovinu*: priamka $a_0z_0 + a_1z_1 + a_2z_2$ reprezentuje v duálnej rovine bod s homogénnymi súradnicami $(a_0 : a_1 : a_2)$.

PRÍKLAD 1.3. Kuželosečka $a_{00}z_0^2 + a_{01}z_0z_1 + a_{11}z_1^2 + a_{02}z_0z_2 + a_{12}z_1z_2 + a_{22}z_2^2$ reprezentuje bod $(a_{00} : a_{01} : a_{11} : a_{02} : a_{12} : a_{22})$ 5-rozmerného projektívneho priestoru; množina všetkých rovinných kuželosečiek tvorí $\mathbb{P}^5$.

2. Zväzok kriviek

Nech $A = (a_0 : a_1 : \dots : a_n)$, $B = (b_0 : b_1 : \dots : b_n)$ sú body projektívneho priestoru $\mathbb{P}^n$. Priamka cez A, B je množina

$$\overleftrightarrow{AB} = \{\lambda A + \mu B \mid (\lambda : \mu) \in \mathbb{P}^1\}.$$

Ak A, B reprezentujú krivky v projektívnej rovine, potom body priamky $\overleftrightarrow{AB}$ reprezentujú tzv. *zväzok kriviek*.

PRÍKLAD 2.1. Nech

$$A = a_0z_0 + a_1z_1 + a_2z_2 \quad \text{a} \quad B = b_0z_0 + b_1z_1 + b_2z_2$$

sú rôzne priamky pretínajúce sa v bode $P = (p_0 : p_1 : p_2)$, t.j.

$$a_0p_0 + a_1p_1 + a_2p_2 = 0, \quad b_0p_0 + b_1p_1 + b_2p_2 = 0.$$

Ich lineárna kombinácia (t.j. v duálnej rovine bod na priamke $\overleftrightarrow{AB}$) je zjavne tiež priamka prechádzajúca bodom P . Naopak, ľubovoľná priamka prechádzajúca bodom P leží v duálnej rovine na priamke $\overleftrightarrow{AB}$ (vyplýva z lineárnej algebry).

LEMA 2.2. *Nech $\lambda F + \mu G$ je zväzok kriviek v projektívnej rovine. Nech $\tilde{F}$ a $\tilde{G}$ sú dve rôzne krivky tohto zväzku. Potom $\tilde{F}$ a $\tilde{G}$ majú tie isté spoločné body ako F a G .*

Dôkaz. Keďže $\tilde{F}$ a $\tilde{G}$ patria zväzku $\lambda F + \mu G$, ľahko overíme, že spoločné body kriviek F a G ležia aj na krivkách $\tilde{F}$ a $\tilde{G}$. Z faktu, že $\tilde{F}$ a $\tilde{G}$ určujú ten istý zväzok ako F a G potom už vyplýva tvrdenie lemy. $\square$

PRÍKLAD 2.3. Bez toho, aby sme museli prevádzať náročné výpočty vieme už ľahko určiť, z akých kriviek pozostáva zväzok určený dvoma kružnicami pretínajúcimi sa v dvoch bodoch, napr.

$$\begin{aligned} F &= x^2 + y^2 - 1 \\ G &= (x - 1)^2 + y^2 - 2. \end{aligned}$$

Budú to kružnice (lebo ide o kvadratické krivky prechádzajúce kružnicovými bodmi $(0 : 1 : i)$, $(0 : 1 : -i)$) prechádzajúce bodmi $(0, 1)$ a $(0, -1)$.

PRÍKLAD 2.4. (Hľadanie prieniku dvoch kuželosečiek.) Nech F a G sú kuželosečky v $\mathbb{P}^2$ pretínajúce sa v štyroch bodoch vo všeobecnej polohe. Každú kuželosečku vo zväzku $\lambda F + \mu G$ môžeme reprezentovať symetrickou maticou. Kuželosečka bude singulárna (t.j. pozostávajúca z dvojice priamok) práve vtedy, keď zodpovedajúca matica je singulárna, čiže jej determinant je nulový. Determinant matice kuželosečky $\lambda F + \mu G$ je kubická forma v premenných λ a μ . Zväzok $\lambda F + \mu G$ teda obsahuje tri singulárne kuželosečky: naozaj, existujú tri dvojice priamok prechádzajúce danými štyrmi bodmi.

PRÍKLAD 2.5. V Príklade 1.3 v Kapitole 4 sme videli, že sústredné kružnice sa pretínajú len v kružnicových bodoch. Skúsme sa teraz na túto situáciu pozrieť z hľadiska zväzkov kriviek.

Nech $x^2 + y^2 - r^2$ a $x^2 + y^2 - s^2$ sú dve rôzne kružnice so stredom v $(0, 0)$. Zväzok kružníc nimi určený obsahuje dve singulárne kuželosečky: dvojásobnú nevlastnú priamku a dvojicu komplexne združených priamok cez $(0, 0)$. Odtiaľ zas vidíme, že tieto kuželosečky majú len dva spoločné body: $(0 : 1 : i)$ a $(0 : 1 : -i)$.

PRÍKLAD 2.6. Množina všetkých kuželosečiek v $\mathbb{P}^2$ prechádzajúcich bodmi

$$(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1) \text{ a } (1 : 1 : 1)$$

tvorí zväzok. Naozaj, ak kuželosečka obsahuje dané body, tak je daná formou

$$az_0z_1 + bz_0z_2 + cz_1z_2, \quad \text{kde} \quad a + b + c = 0.$$

Teda ak položíme $c = -a - b$, dostávame, že ide o zväzok určený dvojicou

$$z_1(z_0 - z_2) \text{ a } z_2(z_0 - z_1).$$

DÔSLEDOK 2.7. *Pre ľubovoľnú generickú štvoricu bodov v $\mathbb{P}^2$ (t.j. takú štvoricu, že žiadne tri body neležia na priamke) je množina všetkých kuželosečiek prechádzajúcich cez tieto body zväzkom.*

TVRDENIE 2.8. *Nech $\lambda F + \mu G$ je zväzok kriviek a nech P je ľubovoľný bod v $\mathbb{P}^2$. Potom v zväzku $\lambda F + \mu G$ existuje aspoň jedna krivka prechádzajúca bodom P .*

Dôkaz. Nech $\lambda F + \mu G$ je zväzok kriviek stupňa d . Uvažujme teraz všetky krivky stupňa d prechádzajúce bodom P . Tieto tvoria v priestore $\mathbb{P}^N$ ($N = d(d+3)/2$) nadrovinu, teda projektivizáciu N -rozmerného vektorového priestoru V v k^{N+1} . Zväzok $\lambda F + \mu G$ v priestore k^{N+1} zodpovedá dvojrozmernému podpriestoru W . Z lineárnej algebry vieme, že buď $W \subset V$ alebo je prienikom V a W jednorozmerný podpriestor. Prienik je v každom prípade neprázdny a zodpovedá krivke (krivkám) ktoré jednak prechádzajú bodom P a tiež ležia vo zväzku $\lambda F + \mu G$. $\square$

PRÍKLAD 2.9. Steinerove kubiky tvoria zväzok určený dvojicou

$$z_0^3 + z_1^3 + z_2^3 \quad \text{a} \quad z_0 z_1 z_2.$$

Všetky krivky zväzku prechádzajú deviatimi inflexnými bodmi nesesingulárnych kriviek zväzku. Platí to aj naopak: kubická krivka prechádzajúca všetkými deviatimi inflexnými bodmi (viď časť 1) je nevyhnutne Steinerovou kubikou:

Všeobecne rovnica kubickej krivky je

$$\sum_{i+j+k=3} a_{ijk} z_0^i z_1^j z_2^k.$$

Uvažujme najprv trojicu

$$P_{00} = (0 : -1 : 1), \quad P_{01} = (0 : -\alpha : 1), \quad P_{02} = (0 : -\alpha^2 : 1),$$

kde α je primitívna tretia odmocnina z 1 ($\alpha^2 + \alpha + 1 = 0$). Ak krivka prechádza týmito tromi bodmi, potom koeficienty a_{ijk} musia spĺňať rovnice

$$\begin{aligned} a_{003} - a_{012} + a_{021} - a_{030} &= 0 \\ a_{003} - \alpha a_{012} + \alpha^2 a_{021} - a_{030} &= 0 \\ a_{003} - \alpha^2 a_{012} + \alpha a_{021} - a_{030} &= 0. \end{aligned}$$

Odtiaľ už ľahko dostaneme, že $a_{012} = a_{021} = 0$ a $a_{003} = a_{030}$. Uvažovaním ďalších trojíc inflexných bodov nájdeme analogické podmienky pre ostatné koeficienty okrem a_{111} . Odtiaľ už dostávame, že krivka je zo zväzku Steinerových kubík.

Takže analogicky ako v predchádzajúcom príklade máme, že množina kriviek prechádzajúcich cez uvažovanú deväťicu bodov tvorí zväzok.