LOKÁLNA PRIESEKOVÁ NÁSOBNOSŤ A BÈZOUTOVA VETA

ŠTUDENTSKÁ VEDECKÁ KONFERENCIA
FMFI UK BRATISLAVA
2009

Autor: Alexander Maťašovský
Školiteľ: doc. RNDr. Eduard Boďa, CSc.
Preferovaná sekcia: Matematika

Abstrakt

Klasická Bèzoutova veta hovorí o počte spoločných bodov dvoch rovinných algebraických kriviek v projektívnej rovine nad algebraicky uzavretým poľom, pričom sa predpokladá, že krivky nemajú spoločný komponent. Tvrdenie vety súvisí s pojmom násobnosti bodu v prieniku kriviek a jeho definíciou. V tejto práci podávame algebraickú definíciu tejto násobnosti a dokážeme klasickú formuláciu Bèzoutovej vety. Rozanalyzujeme tiež tvrdenie Bydžovského, ktoré hovorí o násobnosti bodu v prieniku v súvislosti s násobnosťou bodu na jednotlivých krivkách. Klasická Bèzoutova veta totiž nehovorí o násobnosti priesečníka dvoch kriviek vo vzťahu k jeho násobnosti na jednotlivých krivkách a dotykovej situácie v ňom. B. Bydžovský v roku 1947 publikoval detailnejšiu formuláciu tejto vety. Dokázal tvrdenie:

„Dve rovinné algebraické krivky stupňov m a n, ktoré nemajú spoločnú súčasť, majú spoločných práve mn bodov, ak sa každý bod počíta s príslušnou násobnosťou. Priesečník, ktorý je na jednej krivke r-násobný, na druhej krivke s-násobný a v ktorom majú krivky spoločných h dotyčníc, je priesečníkom aspoň $(rs + h)$-násobným."

Oboznámime sa s lokálnou priesekovou násobnosťou (Samuelova) m-primárneho ideálu I v lokálnom neotherovskom okruhu (A, m), maximálnym ideálom m a podávame klasické metódy na jej výpočet. Uvedieme tiež špeciálne bázy ideálu (Gröbnerovu a štandardnú) a popíšeme ich aplikácie v teórii násobnosti.

Dokážeme niektoré jednoduché tvrdenia týkajúce sa Bydžovského čísla $rs + h$, teóriu doložíme niekoľkými príkladmi umožňujúcimi formulovať hypotézy a niektoré v závere sformulujeme.

Obsah

Úvod

Historické korene Bèzoutovej vety sú v základnej vete algebry, ktorá hovorí o počte koreňov ľubovoľného nenulového polynómu s komplexnými koeficientami. Tento počet sa rovná stupňu polynómu, ak každý koreň počítame s jeho násobnosťou. Inými slovami pre každý komplexný polynóm f stupňa $n > 0$ rovnica $f(x) = 0$ má práve n komplexných koreňov, ak sa každý koreň počíta toľkokrát, koľko je jeho násobnosť.

Otázky, ktoré sa objavili pri skúmaní platnosti Bèzoutovej vety vyvolali vznik teórie násobnosti. Klasická Bèzoutova veta tvrdí, že počet spoločných bodov dvoch rovinných algebraických kriviek v projektívnej rovine nad algebraicky uzavretým poľom (ktoré majú len konečný počet spoločných bodov) je menej, alebo sa rovná súčinu stupňov kriviek. Skúmalo sa, ako priradiť každému bodu v prieniku dvoch rovinných algebraických kriviek takú násobnosť, aby v Bèzoutovej vete namiesto nerovnosti nastala rovnosť. Spomínaná veta je pomenovaná po Étiennovi Bèzoutovi (1730–1783).

1 Lokálna prieseková násobnosť (Samuelova)

1.1 Lokálne okruhy

Jedna z najdôležitejších techník komutatívnej algebry je proces lokalizácie. V algebraicko-geometrickom ponímaní pomocou lokalizácie môžeme skúmať vlastnosti algebraických variet v niektorých špeciálnych bodoch.

Definícia 1.1.1 Komutatívny neotherovský okruh A, ktorý má práve jeden maximálny ideál m nazývame ***lokálnym okruhom***.

Príklad 1.1.1 Každý faktorový okruh $A = \mathbb{Z}/(p^\varrho)$, kde p je prvočíslo a ϱ je nejaké prirodzené číslo, je lokálny s maximálnym ideálom pA. Naproti tomu, okruh celých čísel $\mathbb{Z}$ nie je lokálny okruh, lebo v ňom existuje viac maximálnych ideálov.

Príkladom lokálneho okruhu je okruh, ktorý dostaneme z oblasti integrity pomocou *lokalizácie*. Naznačme si proces lokalizácie.

Nech p je prvoideál v okruhu A. Konštruujme nový okruh A_p nasledovne. Označme

$$A_p = \left\{ \frac{f}{g} \mid f, g \in A,\ g \notin p \right\}.$$

Teda A_p je podmnožina poľa podielov z A. Definujme reláciu rovnosti na množine A_p nasledovne

$$\frac{f}{g} = \frac{f'}{g'} \Longleftrightarrow (fg' - f'g)u = 0,$$

pre nejaký prvok u, ktorý nepatrí do prvoideálu p. Definujme operácie sčitovania a násobenia na množine A_p vzťahom

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + f'g}{gg'},$$
$$\frac{f}{g}.\frac{f'}{g'} = \frac{ff'}{gg'}.$$

Keďže každý prvok $\frac{f}{g} \in A_p$ kde $f \notin p$, je v okruhu A_p jednotka, je ideál pA_p jediný maximálny ideál v A_p. Teda okruh A_p je lokálnym okruhom. Dôkaz tohto tvrdenia možno nájsť v [1], kap. 3. Rings and Modules of Fractions, s. 36–49.

Nech $k[x_1, \ldots, x_n]$ je okruh polynómov n neurčitých nad algebraicky uzavretým poľom k. Potom $k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$ označuje lokálny okruh, presnejšie lokalizáciu okruhu $k[x_1, \ldots, x_n]$ ideálom $\langle x_1, \ldots, x_n \rangle$.

V ďalšom budeme symbolom (A, m) označovať lokálny neotherovský okruh A s maximálnym ideálom m. Pripomeňme, že v lokálnom neotherovskom okruhu sú všetky rastúce reťazce ideálov konečné a tento okruh má jediný maximálny ideál.

Definícia 1.1.2 Pod rozmerom lokálneho neotherovského okruhu A budeme rozumieť dĺžku maximálneho reťazca prvoideálov v A tvaru

$$p_0 \subset p_1 \subset \cdots \subset p_d = m.$$

Označenie $d = \dim A$.

Všetky lokálne okruhy $\mathbb{Z}/(p^\varrho)$ pre nejaké prirodzené číslo ϱ sú nularozmerné, t.j. $\dim \mathbb{Z}/(p^\varrho) = 0$.

Veta 1.1.1 *Ak A je lokálny neotherovský okruh, potom rozmer okruhu A je konečný, t.j.* $\dim A = d < +\infty$.

Dôkaz. [1], kap. 11. Dimension Theory, Corollary 11.11. s. 120. □

Definícia 1.1.3 Rozmerom ideálu I z lokálneho neotherovského okruhu A rozumieme rozmer faktorového okruhu A/I. Označenie $\dim I = \dim A/I$.

Veta 1.1.2 *Nech I je m-primárny ideál v lokálnom neotherovskom okruhu (A, m) a $I = \langle a_1, \ldots, a_t \rangle$, potom $t \geq \dim A$.*

Dôkaz. [1], kap. 11. Dimension Theory, Proposition 11.7. s. 119. □

Definícia 1.1.4 Nech (A, m) je lokálny neotherovský okruh a $\dim A = d$. Ak ideál $I = \langle a_1, \ldots, a_d \rangle$ je m-primárny, potom množinu $\{a_1, \ldots, a_d\}$ nezveme ***systémom parametrov*** v A a ideál I nazývame ***parametrický ideál***.

Pre každý m-primárny ideál I v lokálnom neotherovskom okruhu A je faktorový okruh A/I nularozmerným okruhom, t.j. $\dim I = 0$. Nularozmerné lokálne neotherovské okruhy sú charakterizované konečnou dĺžkou maximálnych reťazcov m-primárnych ideálov a rovnosťou počtu ich členov.

Nech A je ľubovoľný lokálny neotherovský okruh a I je m-primárny ideál v A. Nech

$$I = I_1 \subset I_2 \subset \cdots \subset I_s = m$$

je maximálny reťazec m-primárnych ideálov so začiatkom v I a koncom v m. Všetky takéto reťazce majú tú istú dĺžku. Podrobnejšie v [1], kap. 6. Chain Condition, s. 74–79. Počet členov takéhoto maximálneho reťazca ideálov v A nazývame ***dĺžkou*** ideálu I, resp. faktorového okruhu A/I a označujeme

$$\ell(I) = \ell(A/I) = s.$$

Príklad 1.1.2 1. Počítajme dĺžku ideálu $I = \langle x + y^2, x^2y^2 \rangle$, kde I je ideál z okruhu polynómov $k[x, y]$. Zostrojíme maximálny reťazec:

$$\left\langle x + y^2, x^2y^2 \right\rangle \subset \left\langle x + y^2, x^2y \right\rangle \subset \left\langle x + y^2, x^2 \right\rangle \subset \left\langle x + y^2, xy, x^2 \right\rangle \subset \left\langle x, y^2 \right\rangle \subset \langle x, y \rangle ,$$

kde $I = \langle x + y^2, x^2y^2 \rangle$ a $m = \langle x, y \rangle$ je maximálny ideál v $k[x, y]$. Dĺžka tohto ideálu v okruhu $k[x, y]$ je $\ell(I) = 6$.

2. Počítajme dĺžku ideálu $J = \langle x^2 - y^3, xy^2 \rangle$. Zostrojíme maximálny reťazec:

$\langle x^2 - y^3, xy^2 \rangle \subset \langle x^2 - y^3, xy^2, y^4 \rangle \subset \langle x^2 - y^3, xy^2, y^3 \rangle \subset \langle x^2 + y^3, y^2 \rangle \subset$
$\subset \langle x^2 - y^3, y^2, xy \rangle \subset \langle x^2 - y^3, y \rangle \subset \langle x, y \rangle.$

Dĺžka tohto ideálu je $\ell(J) = 7$.

Nech I je m-primárny ideál v (A, m). Je zrejmé, že I^n je opäť m-primárny ideál pre každé prirodzené číslo n, pretože obsahuje mocninu ideálu m. Teda pre ľubovoľné prirodzené číslo n je

$$\ell(I^n) = \ell(A/I^n) < +\infty.$$

Pomocou tejto dĺžky možno definovať ďalšie číslo, ktoré bližšie charakterizuje ideál I, totiž jeho násobnosť.

1.2 Samuelova násobnosť ideálu

V tejto časti uvedieme niektoré klasické metódy pre výpočet Samuelovej násobnosti. Predpokladáme, že ideál I je m-primárny v lokálnom neotherovskom okruhu (A, m) s maximálnym ideálom m.

Veta 1.2.1 *Pre dostatočne veľké prirodzené číslo $n \gg 0$ je dĺžka $\ell(I^n)$ polynóm s celočíselnými koeficientami v neurčitej n stupňa $d = \dim A$. Tento polynóm sa nazýva* **Hilbert–Samuelov polynóm**. *Možno ho napísať v tvare*

$$\ell(A/I^n) = \ell(I^n) = e_0(I)\binom{n+d}{d} + \cdots + (-1)^d e_d(I),$$

kde $e_0(I) > 0$ a $e_0(I), \ldots, e_d(I)$ sú celé čísla a jednoznačne určené ideálom I.

Dôkaz. [18], kap. 8. □

Koeficienty $e_0(I), \ldots, e_d(I)$ sa nazývajú Hilbertove koeficienty ideálu I. Vedúci koeficient Hilbertovho–Samuelovho polynómu $e_0(I)$ hrá významnú úlohu v algebraickej geometrii.

Definícia 1.2.1 Nezáporné celé číslo $e_0(I)$ nazývame ***Samuelovou násobnosťou*** m-primárneho ideálu I v lokálnom neotherovskom okruhu (A, m) a budeme ju označovať $e_0(I, A)$.

Nech $k[x, y]$ je okruh polynómov nad poľom k. $A = k[x, y]_{\langle x,y\rangle}$ je lokálny okruh s maximálnym ideálom $m = \langle x, y\rangle$. Potom pre m-primárny ideál Q v A Hilbert–Samuelov polynóm pre $n \gg 0$ stupňa 2 má tvar

$$\ell(A/Q^n) = e_0(Q)\frac{n^2}{2} + e_1(Q)n + e_2(Q).$$

Podrobnosti v [5].

V nasledujúcej vete uvedieme niektoré praktické metódy na výpočet Samuelovej násobnosti m-primárneho ideálu I, pričom naďalej predpokladáme, že (A, m) je lokálny neotherovský okruh s rozmerom $\dim A = d$, a $e_0(I, A)$ je Samuelova násobnosť ideálu I.

Veta 1.2.2 *Nech (A, m) je d-rozmerný lokálny neotherovský okruh. Potom platí:*

1. *ak I_1, I_2 sú m-primárne ideály z (A, m) a $I_1 \subset I_2$, potom pre násobnosti týchto ideálov platí $e_0(I_1, A) \geq e_0(I_2, A)$,*
2. *ak I je m-primárny ideál z (A, m), potom pre ľubovoľné prirodzené číslo s platí $e_0(I^s, A) = s^d e_0(I, A)$,*
3. *ak $I_1 = \langle a_1, a_2, \ldots, a_d\rangle$, $I_2 = \langle b_1, a_2, \ldots, a_d\rangle$ sú parametrické ideály v A, potom aj ideál $I = \langle a_1 b_1, a_2, \ldots, a_d\rangle$ je parametrický v A a pre jeho násobnosť platí vzťah $e_0(I, A) = e_0(I_1, A) + e_0(I_2, A)$,*
4. *$e_0(\langle a_1^m, a_2, \ldots, a_d\rangle, A) = m e_0(\langle a_1, a_2, \ldots, a_d\rangle, A)$ pre každý parametrický ideál $\langle a_1, a_2, \ldots, a_d\rangle$ v okruhu A,*
5. *$e_0(\langle a_1^s, a_2^s, \ldots, a_d^s\rangle, A) = e_0(\langle a_1, a_2, \ldots, a_d\rangle^s, A) = s^d e_0(\langle a_1, a_2, \ldots, a_d\rangle, A)$ pre každý parametrický ideál $\langle a_1, a_2, \ldots, a_d\rangle$ a ľubovoľné prirodzené číslo s.*

Dôkaz. [12], kap. 7. §7.1. □

Príklad 1.2.1 Počítajme násobnosť ideálu $I = \langle x + y^2, x^2y^2\rangle$ v $A = k[x, y]_{\langle x,y\rangle}$.

$$\begin{aligned} e_0(\langle x + y^2, x^2y^2\rangle, A) &\overset{3}{=} e_0(\langle x + y^2, x^2\rangle, A) + e_0(\langle x + y^2, y^2\rangle, A) \\ &\overset{4}{=} 2e_0(\langle x + y^2, x\rangle, A) + 2e_0(\langle x + y^2, y\rangle, A) \\ &= 2e_0(\langle y^2, x\rangle, A) + 2e_0(\langle x, y\rangle, A) \\ &\overset{4}{=} 2.2e_0(\langle y, x\rangle, A) + 2e_0(\langle x, y\rangle, A) \\ &= 4.1 + 2.1 = 6. \end{aligned}$$

Všimnime si, že v bode 1 príkladu 1.1.2 dĺžka daného ideálu je $\ell(I) = 6$ a Samuelova násobnosť toho istého ideálu $e_0(I, A) = 6$.

Vo všeobecnosti medzi dĺžkou ideálu I a Samuelovou násobnosťou toho istého ideálu platí nerovnosť

$$\ell(I) \geq e_0(I, A).$$

Rovnosťou sú charakterizované Cohen–Maculayho okruhy. V príklade 1.2.1 lokálny okruh $A = k[x, y]_{\langle x,y \rangle}$ je Cohen–Maculayho a ideál I je parametrický, teda naozaj platí rovnosť.

Príklad 1.2.2 Nech $I = \langle x^a - y^b, x^c - y^d \rangle$ je m-primárny ideál v $A = k[x, y]_{\langle x,y \rangle}$ a a, b, c, d sú kladné celé čísla. Porom

$$e_0(I) = \min\{ad, bc\}.$$

Dôkaz možno nájsť v [5].

1.3 Usporiadanie

Definícia 1.3.1 Relácia $>$ na množine A sa nazýva ***lineárne (alebo totálne) usporiadanie*** množiny A, ak pre každé $x, y, z \in A$ platí:

1. $(x > y) \Rightarrow \neg(y > x)$ (antisymetria),
2. $[(x > y) \wedge (y > z)] \Rightarrow (x > z)$ (tranzitívnosť),
3. $(x = y) \vee (x > y) \vee (y > x)$ (trichotómia).

Nech $k[x_1, \ldots, x_n]$ je okruh polynómov nad algebraicky uzavretým poľom k a relácia $>$ je lineárnym usporiadaním v okruhu $k[x_1, \ldots, x_n]$ presnejšie, lineárne usporiadanie na množine všetkých monómov v $k[x_1, \ldots, x_n]$, pričom predpokladá základné usporiadanie neurčitých $x_1 > x_2 > \cdots > x_n$. Nech $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ je ľubovoľný monóm z okruhu $k[x_1, \ldots, x_n]$. Potom usporiadaná n-tica $\alpha = (\alpha_1, \ldots, \alpha_n)$, kde $\alpha_i \in \mathbb{N}_0$, $1 \leq i \leq n$, jednoznačne popisuje daný monóm, pričom α sa dá chápať ako vektor. Ak α je nulový vektor, teda $\alpha = (0, \ldots, 0)$, potom definujeme $x^\alpha = x_1^0 x_2^0 \ldots x_n^0 = 1$.

Definícia 1.3.2 Lineárne usporiadane $>$ nazveme ***monomiálnym*** ak

1. je kompatibilné s násobením v $k[x_1, \ldots, x_n]$, teda ak x^α, x^β a x^γ sú monómy v $k[x_1, \ldots, x_n]$ a $x^\alpha > x^\beta$, potom $x^\alpha x^\gamma > x^\beta x^\gamma$,
2. je dobrým usporiadaním na $k[x_1, \ldots, x_n]$, t.j. každá neprázdna množina monómov v $k[x_1, \ldots, x_n]$ obsahuje najmenší prvok.

Dá sa ukázať, že druhá podmienka z definície 1.3.2 je ekvivalentná s podmienkou $x_i > 1$ pre všetky $i = 1, 2, \ldots, n$.

V okruhu polynómov $k[x_1, \ldots, x_n]$ sa najčastejšie používa monomiálne usporiadanie lexikografické a gradované lexikografické usporiadanie.

Nech x^α, x^β sú monómy v $k[x_1, \ldots, x_n]$. Nech vo vektore $\alpha - \beta$ je prvý nenulový člen (zľava) prvok $\alpha_k - \beta_k$, teda platí $\alpha - \beta = (0, \ldots, 0, \alpha_k - \beta_k \neq 0, \ldots, \alpha_n - \beta_n)$. Ďalej označme stupeň monómu x^α ako $|\alpha| = \sum_{i=1}^{n} \alpha_i$. Teraz už môžeme definovať spomínané usporiadanie.

Definícia 1.3.3 (Lexikografické usporiadanie) Usporiadanie $>$ nazveme ***lexikografickým*** usporiadaním na $k[x_1, \ldots, x_n]$, ak $\alpha_k - \beta_k > 0$. Označenie $>_{lex}$.

Ako aj názov tohto usporiadania hovorí, monómy sú usporiadané tak, ako slová v slovníkoch. Napríklad v lexikografickom usporiadaní platí $x >_{lex} y >_{lex} z$, $xy^3 >_{lex} y^2z^3$ alebo $x^4y^2z^3 >_{lex} x^4y^2z$.

Definícia 1.3.4 (Gradované lexikografické usporiadanie) Usporiadanie $>$ nazveme ***gradovaným lexikografickým*** usporiadaním na $k[x_1, \ldots, x_n]$, ak $|\alpha| > |\beta|$, alebo $|\alpha| = |\beta|$ a $\alpha_k - \beta_k > 0$. Označenie $>_{glex}$.

Pre korektnosť by sme museli dokázať, že tie usporiadania sú monomiálne, t.j. splňajú podmienky definície 1.3.2.

Príklad 1.3.1 Nech $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ je polynóm v $k[x_1, \ldots, x_n]$. Usporiadajte monómy v lexikografickom a v gradovanom lexikografickom usporiadaní.

Riešenie. Pretože $-5x^3 >_{lex} 7x^2z^2 >_{lex} 4xy^2z >_{lex} 4z^2$ polynóm f môžeme napísať nasledovne

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2 \qquad (lex)$$

a $7x^2z^2 >_{glex} 4xy^2z >_{glex} -5x^3 >_{glex} 4z^2$ potom

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2 \qquad (glex)$$

Definícia 1.3.5 Nech $>$ je pevne zvolené monomiálne usporiadanie na $k[x_1, \ldots, x_n]$ a

$$f = \sum_\alpha c_\alpha x^\alpha = c_{\alpha_0} x^{\alpha_0} + c_{\alpha_1} x^{\alpha_1} + \cdots, \quad x^{\alpha_0} > x^{\alpha_1} > \cdots$$

je nenulový polynóm v $k[x_1, \ldots, x_n]$. Potom

1. ***vedúci koeficient*** polynómu f je $\mathrm{Lc}(f) = c_{\alpha_0}$,

2. ***vedúci monóm*** polynómu f je $\mathrm{Lm}(f) = x^{\alpha_0}$,

3. ***vedúci člen*** polynómu f je $\mathrm{Lt}(f) = c_{\alpha_0} x^{\alpha_0}$.

Príklad 1.3.2 Pre polynóm f z príkladu 1.3.1 v lexikografickom usporiadaní platí, že $\mathrm{Lc}(f) = -5$, $\mathrm{Lm}(f) = x^3$, $\mathrm{Lt}(f) = -5x^3$ a v gradovanom lexikografickom usporiadaní $\mathrm{Lc}(f) = 7$, $\mathrm{Lm}(f) = x^2z^2$ a $\mathrm{Lt}(f) = 7x^2z^2$.

Definícia 1.3.6 Nech $I \subseteq k[x_1, \ldots, x_n]$ je ideál rôzny od $\{0\}$.

1. ***Vedúci ideál*** $\mathrm{Lt}(I)$ ideálu I je množina vedúcich členov prvkov ideálu I

$$\mathrm{Lt}(I) = \{\mathrm{Lt}(f) \mid f \in I\}.$$

2. $\langle \mathrm{Lt}(I) \rangle$ je ideál ***generovaný prvkami z*** $\mathrm{Lt}(I)$.

Nech $I = \langle f_1, \ldots, f_s \rangle$ je ideál v $k[x_1, \ldots, x_n]$. Potom $\mathrm{Lt}(f_i) \in \mathrm{Lt}(I) \subseteq \langle \mathrm{Lt}(I) \rangle$ z čoho vyplýva $\langle \mathrm{Lt}(f_1), \ldots, \mathrm{Lt}(f_s) \rangle \subseteq \langle \mathrm{Lt}(I) \rangle$. Obrátená inklúzia neplatí vo všeobecnosti ako to ukazuje nasledujúci príklad.

Príklad 1.3.3 Nech $I = \langle f_1, f_2 \rangle$ pričom $f_1 = x^3 - 2xy$ a $f_2 = x^2y - 2y^2 + x$, a nech na $k[x, y]$ je zvolené monomiálne usporiadanie $>_{glex}$. Potom

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

teda $x^2 \in I$. Platí $x^2 = \mathrm{Lt}(x^2) \in \langle \mathrm{Lt}(I) \rangle$. Lenže x^2 nie je deliteľný ani s $\mathrm{Lt}(f_1) = x^3$ ani $\mathrm{Lt}(f_2) = x^2y$ z čoho $x^2 \notin \langle \mathrm{Lt}(f_1), \mathrm{Lt}(f_2) \rangle$.

Rovnosťou je charakterizovaná Gröbnerova báza.

1.4 Gröbnerova báza ideálu a deliaci algoritmus

Definícia 1.4.1 Nech I je ideál v $k[x_1, \ldots, x_n]$. Nech $>$ je monomiálne usporiadanie na $k[x_1, \ldots, x_n]$. Potom konečná podmnožina $G = \{g_1, \ldots, g_t\}$ ideálu I sa nazýva ***Gröbnerova báza*** ak

$$\langle \mathrm{Lt}(I) \rangle = \langle \mathrm{Lt}(g_1), \ldots, \mathrm{Lt}(g_t) \rangle .$$

Jedna najdôležitejšia veta lineárnej algebry je veta o delení so zvyškom na množine všetkých celých čísel, ktorá hovorí, že k daným dvom celým číslam $a, b,\ b \neq 0$, existuje práve jedna dvojica celých čísel q, r tak, že $a = bq + r,\ 0 \leq r < |b|$. Analogicky sa dá sformulovať vetu o delení so zvyškom na okruhu polynómov $k[x]$ v jednej neurčitej x, ktorú možno nájsť napr. v [10], kap. 5. Okruhy polynómov, s. 211. Našou základnou algebraickou štruktúrou je okruh polynómov v neurčitých $x_1, \ldots, x_n$ nad k.

Veta 1.4.1 (Deliaci algoritmus) *Nech $F = (f_1, \ldots, f_s)$ je usporiadaná s-tica polynómov v $k[x_1, \ldots, x_n]$ s monomiálnym usporiadaním $>$. Potom každý polynóm f z okruhu polynómov $k[x_1, \ldots, x_n]$ sa dá napísať v tvare*

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

kde $a_1, \ldots, a_s, r \in k[x_1, \ldots, x_n]$, pričom $r = 0$ alebo r je lineárna kombinácia monómov s koeficientmi v k z ktorých žiadny nie je deliteľný monómami $\mathrm{Lt}(f_1), \ldots, \mathrm{Lt}(f_s)$.

DÔKAZ. [8], kap. 2. §3. A Division Algorithm in $k[x_1, \ldots, x_n]$, s. 64. □

Nasledujúce vety hovoria o vlastnostiach Gröbnerovej bázy.

Veta 1.4.2 *Nech $G = \{g_1, \ldots, g_t\}$ je Gröbnerova báza ideálu $I \subset k[x_1, \ldots, x_n]$, a nech f je polynóm z tohto okruhu. Potom zvyšok po delení polynómu f množinou $\{g_1, \ldots, g_t\}$ je určený jednoznačne.*

DÔKAZ. Nech existujú také $a_1, \ldots, a_t, b_1, \ldots, b_t, r, r' \in k[x_1, \ldots, x_n]$ pričom $r \neq r'$, že

$$f = a_1 g_1 + \cdots + a_t g_t + r = b_1 g_1 + \cdots + b_t g_t + r'.$$

Potom $r - r' = (b_1 - a_1)g_1 + \cdots + (b_t - a_t)g_t \in I$, teda $\mathrm{Lt}(r - r') \in \langle \mathrm{Lt}(I) \rangle = \langle \mathrm{Lt}(g_1), \ldots, \mathrm{Lt}(g_t) \rangle$. $\mathrm{Lt}(r - r')$ je väčší z vedúcich monómov r alebo r', je tento monóm deliteľný niektorým $\mathrm{Lt}(g_i)$ čo je spor. Teda $r = r'$. □

Veta 1.4.3 *Nech $G = \{g_1, \ldots, g_t\}$ je Gröbnerova báza ideálu $I \subset k[x_1, \ldots, x_n]$, a nech f je polynóm z tohto okruhu. Potom f je z ideálu I vtedy a len vtedy, keď zvyšok po delení polynómu f množinou $\{g_1, \ldots, g_t\}$ je nulový.*

DÔKAZ. Nech $f = a_1 g_1 + \cdots + a_t g_t + r$. Ak $f \in I$ potom aj $r \in I$ teda $\mathrm{Lt}(r)$ je deliteľný niektorým z $\mathrm{Lt}(g_i)$, teda $r = 0$. Obrátene ak $r = 0$, potom je zrejmé, že $f \in I$. □

1.5 Štandardná báza ideálu

Doteraz sme hovorili o monomiálnom usporiadaní $>$. Ďalší typ usporiadania je lokálne usporiadanie.

Definícia 1.5.1 Lineárne usporiadane $>$ nazveme ***lokálnym*** ak

1. je kompatibilné s násobením v $k[x_1, \ldots, x_n]$, teda ak x^α, x^β a x^γ sú monómy v $k[x_1, \ldots, x_n]$ a $x^\alpha > x^\beta$, potom $x^\alpha x^\gamma > x^\beta x^\gamma$,
2. $1 > x_i$ pre všetky $i = 1, 2, \ldots, n$.

Nech x^α, x^β sú monómy v $k[x_1, \ldots, x_n]$. Nech vo vektore $\alpha - \beta$ je prvý nenulový člen (zľava) prvok $\alpha_k - \beta_k$ a posledný nenulový člen (zľava) je $\alpha_s - \beta_s$, teda platí $\alpha - \beta = (0, \ldots, 0, \alpha_k - \beta_k \neq 0, \ldots, \alpha_s - \beta_s \neq 0, 0, \ldots, 0)$. Ďalej označme stupeň monómu x^α ako $|\alpha| = \sum_{i=1}^n \alpha_i$. Zadefinujeme si najčastejšie používané lokálne usporiadanie.

Definícia 1.5.2 (Antigradované lexikografické usporiadanie) Usporiadanie $>$ nazveme ***antigradovaným lexikografickým*** usporiadaním na $k[x_1, \ldots, x_n]$, ak

$$|\alpha| = \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i = |\beta|, \text{ alebo } |\alpha| = |\beta| \text{ a } \alpha_k - \beta_k > 0.$$

Označenie $>_{alex}$.

Príklad 1.5.1 V okruhu polynómov $k[x, y]$ pre usporiadanie $>_{alex}$ platí: $1 >_{alex} x >_{alex} y >_{alex} x^2 >_{alex} xy >_{alex} y^2 >_{alex} \ldots$

Definícia 1.5.3 (Reverzné lexikografické usporiadanie) Usporiadanie $>$ nazveme ***reverzným lexikografickým*** usporiadaním na $k[x_1, \ldots, x_n]$, ak

$$\alpha_s - \beta_s < 0.$$

Označenie $>_{revlex}$.

Definícia 1.5.4 (Antigradované reverzné lexikografické usporiadanie) Usporiadanie $>$ nazveme ***antigradovaným reverzným lexikografickým*** usporiadaním na $k[x_1, \ldots, x_n]$, ak

$$|\alpha| = \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i = |\beta|, \text{ alebo } |\alpha| = |\beta| \text{ a } \alpha_s - \beta_s < 0.$$

Označenie $>_{arevlex}$.

Príklad 1.5.2 V okruhu polynómov $k[x, y, z]$ platí: $1 >_{arevlex} x >_{arevlex} y >_{arevlex} z >_{arevlex} x^2 >_{arevlex} xy >_{arevlex} y^2 >_{arevlex} xz >_{arevlex} yz \ldots$

Pre korektnosť by sme museli dokázať, že lineárne usporiadanie $>_{alex}$, $>_{revlex}$ a $>_{arevlex}$ sú lokálne usporiadanie, tento dôkaz teraz vynecháme.

V prípade lokálneho usporiadania Gröbnerova báza sa nazýva štandardná báza, ktoré hrajú významnú úlohu v teórii násobnosti.

Podľa doteraz povedaného vznikne otázka ako vypočítať Gröbnerovu resp. štandardnú bázu ideálu, ktorý je generovaný polynómami. Efektívnu metódu na túto problematiku našiel Bruno Buchberger v roku 1965. Skôr než by sme vyslovili jeho metódu treba ozrejmiť pojem *S-polynómu.*

Definícia 1.5.5 Nech $f, g \in k[x_1, \ldots, x_n]$ sú nenulové polynómy. Nech $\mathrm{Lt}(f) = cx^\alpha$, $\mathrm{Lt}(g) = dx^\beta$ a x^γ je najmenší spoločný násobok monómov x^α a x^β. ***S-polynóm*** polynómov f a g je polynóm

$$S(f,g) = \frac{x^\gamma}{\mathrm{Lt}(f)} f - \frac{x^\gamma}{\mathrm{Lt}(g)} g.$$

Príklad 1.5.3 Nech $f = x^3y^2 - x^2y^3 + x$ a $g = 3x^4y + y^2$ v $\mathbb{R}[x,y]$ s monomiálnym usporiadaním $>_{glex}$. Potom najmenší spoločný násobok $\mathrm{Lm}(f) = x^3y^2$ a $\mathrm{Lm}(g) = x^4y$ je x^4y^2. Vedúce členy polynómov f, g sú $\mathrm{Lt}(f) = x^3y^2$ a $\mathrm{Lt}(g) = 3x^4y$. S-polynóm

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g \\ &= xf - \frac{1}{3} yg \\ &= -x^3y^3 + x^2 - \frac{1}{3} y^3. \end{aligned}$$

Nech teraz $\Gamma = \{f_1, \ldots, f_s\}$ je množina polynómov z okruhu $k[x_1, \ldots, x_n]$. Potom každý polynóm $f \in k[x_1, \ldots, x_n]$ sa dá napísať v tvare

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

kde $a_i, r \in k[x_1, \ldots, x_n]$ a alebo $r = 0$ alebo monómy z r nie sú deliteľné monómami $\mathrm{Lt}(f_1), \ldots, \mathrm{Lt}(f_s)$. Polynóm r sa nazýva zvyšok po delení polynómu f množinou Γ, ktorý budeme označovať $\overline{f^\Gamma}$.

Príklad 1.5.4 Nech $\Gamma = \{x^2y - y^2, x^4y^2 - y^2\} \subseteq k[x,y]$ v monomiálnom usporiadaní $>_{lex}$. Potom

$$\overline{x^5y^\Gamma} = xy^3$$

pretože podľa deliaceho algoritmu

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0.(x^4y^2 - y^2) + xy^3.$$

Veta 1.5.1 (Buchbergerovo kritérium) *Množina polynómov $\Gamma = \{f_1, \ldots, f_s\}$ patriacich ideálu I tvorí Gröbnerovu resp. štandardnú bázu ideálu I práve vtedy, keď pre všetky dvojice $f_i, f_j \in \Gamma$, $i, j = 1, \ldots, s$ platí*

$$\overline{S(f_i, f_j)^\Gamma} = 0.$$

Dôkaz. [8], kap. 2. §6. Properties of Groebner Bases, s. 85. □

Príklad 1.5.5 Nech $k[x,y]$ je okruh polynómov v ktorom je definované monomiálne usporiadanie $>_{glex}$ a nech $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Množina $\Gamma = \{f_1, f_2\}$ nie je Gröbnerova báza ideálu I, pretože $S(f_1, f_2) = -x^2 \notin \langle \mathrm{Lt}(f_1), \mathrm{Lt}(f_2) \rangle$. Označme

$f_3 = -x^2$. Pridajme do množiny Γ polynóm f_3, teda $\Gamma = \{f_1, f_2, f_3\}$. Počítajme S-polynómy

$$\begin{aligned} S(f_1, f_2) &= f_3, \\ \overline{S(f_1, f_2)^{\Gamma}} &= 0, \\ S(f_1, f_3) &= (x^3 - 2xy) - (-x)(-x^2) = -2xy, \\ \overline{S(f_1, f_3)^{\Gamma}} &= -2xy \neq 0. \end{aligned}$$

Pridajme polynóm $f_4 = -2xy$ do množiny Γ. Teraz $\Gamma = \{f_1, f_2, f_3, f_4\}$ a opäť vypočítame S-polynómy

$$\begin{aligned} \overline{S(f_1, f_2)^{\Gamma}} &= \overline{S(f_1, f_3)^{\Gamma}} = 0, \\ S(f_1, f_4) &= y(x^3 - 2xy) - (-1/2)x^2(-2xy) = -2xy^2 = yf_4, \\ \overline{S(f_1, f_4)^{\Gamma}} &= 0, \\ S(f_2, f_3) &= (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \\ \overline{S(f_2, f_3)^{\Gamma}} &= -2y^2 + x \neq 0. \end{aligned}$$

Opäť pridajme polynóm $f_5 = -2y^2 + x$ do množiny Γ, teda $\Gamma = \{f_1, f_2, f_3, f_4, f_5\}$ a keby sme vypočítali S-polynómy dostali by sme

$$\overline{S(f_i, f_j)^{\Gamma}} = 0 \text{ pre všetky } 1 \leq i < j \leq 5.$$

Podľa vety 1.5.1 množina

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$$

tvorí Gröbnerovu bázu ideálu I.

Je zrejmé, že každý ideál môže mať viacero Göbnerových resp. štandardných báz. V prípade Gröbnerovej bázy počítame s monomiálnym, v prípade štandardnej bázy s lokálnym usporiadaním. Môžeme ho zostrojiť podľa algoritmu popísané v príklade vyššie, ktorý sa nazýva ***Buchbergerov algoritmus***. Princíp algoritmu je pridávanie zvyšku S-polynómu po delení polynómami $f_1, \ldots, f_s$ do množiny Γ. Tento algoritmus po konečnom počte krokov musí skončiť. Dôkaz tohto algoritmu možno nájsť v práci [8], kap. 2. §7. Buchberger's Algorithm, s. 90.

Lema 1.5.1 *Nech $f, g \in k[x_1, \ldots, x_n]$ a $\mathrm{Lt}(f)$ a $\mathrm{Lt}(g)$ sú nesúdeliteľné. Označme $\Gamma = \{f, g\}$, potom*

$$\overline{S(f, g)^{\Gamma}} = 0.$$

Dôkaz. Nech $\mathrm{Lt}(f) = cx^\alpha$ a $\mathrm{Lt}(g) = dx^\beta$ sú nesúdeliteľné, t.j. najmenší spoločný násobok je $\mathrm{Lt}(f).\mathrm{Lt}(g) = cdx^\alpha x^\beta$. Počítajme S-polynóm polynómov $f = cx^\alpha + f_0$ a $g = dx^\beta + g_0$, teda

$$\begin{aligned} S(f,g) &= \frac{cdx^\alpha x^\beta}{cx^\alpha} f + \frac{cdx^\alpha x^\beta}{dx^\beta} g \\ &= \frac{cdx^\alpha x^\beta}{cx^\alpha}(cx^\alpha + f_0) + \frac{cdx^\alpha x^\beta}{dx^\beta}(dx^\beta + g_0) \\ &= cdx^\alpha x^\beta + dx^\beta f_0 - cdx^\alpha x^\beta - cx^\alpha g_0 \\ &= (g - g_0)f_0 - (f - f_0)g_0 \\ &= f_0 g - g_0 f. \end{aligned}$$

□

Dôsledok 1.5.1 *Nech $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ a $\mathrm{Lt}(f_i)$, $\mathrm{Lt}(f_j)$ sú nesúdeliteľné pre všetky $i, j = 1, 2, \ldots, s$ a $i \neq j$. Potom $\Gamma = \{f_1, \ldots, f_s\}$ tvorí Gröbnerovu resp. štandardnú bázu ideálu $I = \langle f_1, \ldots, f_s \rangle$ vzľadom na monomiálne resp. lokálne usporiadanie.*

1.6 Aplikácia Gröbnerových a štandardných báz ideálov

Nech $I = \langle f_1, \ldots, f_r \rangle \subset k[x_1, \ldots, x_n]$. Okruh $k[x_1, \ldots, x_n]/I$ je konečnorozmerný vektorový priestor nad poľom k práve vtedy, keď $\dim I = 0$, teda keď algebraická verieta $\mathbf{V}(I)$ v $\mathbb{A}^n(k)$ je zjednotením konečného počtu bodov, čiže

$$I = Q_1 \cap Q_2 \cap \ldots \cap Q_s$$

je neskrátiteľný primárny rozklad ideálu I, kde Q_i sú nularozmerné primárne ideály definujúce body $C_i \in \mathbb{A}^n(k)$ a $\mathrm{rad}(Q_i) = P_i$, $\mathbf{V}(I) = \{C_1, \ldots, C_s\}$. Násobnosť bodu C_i je daná rozmerom vektorového priestoru $k[x_1, \ldots, x_n]/Q_i$ nad poľom k, pričom platí rovnosť

$$\dim_k k[x_1, \ldots, x_n]/Q_i = \ell(Q_i)$$

kde $\ell(Q_i)$ je dĺžka P_i-primárneho ideálu Q_i. Celkový počet bodov algebraickej variety $\mathbf{V}(I)$ je daný číslom

$$\sum_{i=1}^{s} \dim_k k[x_1, \ldots, x_n]/Q_i,$$

pričom každý bod sa počíta príslušnou násobnosťou.

Príklad 1.6.1 Nech $I = \langle x^2 - y^3, x^4 - y^5 \rangle$, potom primárny rozklad ideálu I je $I = \langle x+1, y-1 \rangle \cap \langle x-1, y-1 \rangle \cap \langle x^2 - y^3, y^5 \rangle$, kde $Q_1 = \langle x+1, y-1 \rangle$, $Q_2 = \langle x-1, y-1 \rangle$, $Q_3 = \langle x^2 - y^3, y^5 \rangle$ a navyše $\mathrm{rad}(Q_1) = Q_1$, $\mathrm{rad}(Q_2) = Q_2$ a $\mathrm{rad}(Q_3) = \langle x, y \rangle$ s $\ell(Q_3) = 10$. Teda body $C_1 = (-1, 1)$ a $C_2 = (1, 1)$ majú násobnosť jedna a bod $C_3 = (0, 0)$ má násobnosť desať. Celkový počet bodov algebraickej variety definovaná ideálom I je dvanásť.

Veta 1.6.1 *Nech I, Q_i sú ako predtým, potom*

$$\dim_k k[x_1,\ldots,x_n]/I = \sum_{i=1}^{s} \dim_k k[x_1,\ldots,x_n]/Q_i.$$

Aby sme túto vetu vedeli dokázať potrebujeme najprv dokázať pomocnú vetu.

Veta 1.6.2 *Homomorfizmus*

$$\begin{array}{rccl} \varphi\colon & k[x_1,\ldots,x_n] & \to & k[x_1,\ldots,x_n]/Q_1 \oplus \cdots \oplus k[x_1,\ldots,x_n]/Q_s \\ & f & \mapsto & (f+Q_1,\ldots,f+Q_s) \end{array}$$

je surjektívny práve vtedy, keď $Q_i + Q_j = (1)$ pre všetky $i,j = 1,2,\ldots,s$ a $i \neq j$.

Dôkaz. Nech homomorfizmus φ je surjektívny, to znamená, že existuje $f \in k[x_1,\ldots,x_n]$ také, že $\varphi(f) = (\overline{0},\ldots,\overline{1},\ldots,\overline{0})$, pričom jednotka je na j-tom mieste, čiže $f-1 \in Q_j$ a $f-0 \in Q_i$ pre všetky $j \neq i$ a $i = 1,2,\ldots,s$. Potom $(f-0)-(f-1) = 1$ a $(1) \in Q_j + Q_i$ pre všetky $j \neq i$. Obrátene nech $(\overline{a_1},\ldots,\overline{a_s}) \in \bigoplus_{j=1}^{s} k[x_1,\ldots,x_n]/Q_j$, teda

$$(\overline{a_1},\ldots,\overline{a_s}) = a_1(\overline{1},\overline{0},\ldots,\overline{0}) + \cdots + a_s(\overline{0},\ldots,\overline{0},\overline{1}),$$

pre určité $a_1,\ldots,a_s \in k$. Ak existujú $f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$ také, že

$$\begin{aligned} \varphi(f_1) &= (\overline{1},\overline{0},\ldots,\overline{0}) \\ \varphi(f_2) &= (\overline{0},\overline{1},\ldots,\overline{0}) \\ &\vdots \\ \varphi(f_s) &= (\overline{0},\overline{0},\ldots,\overline{1}) \end{aligned}$$

potom $(\overline{a_1},\ldots,\overline{a_s}) = \varphi(a_1f_1 + a_2f_2 + \cdots + a_sf_s)$. Stačí teda ukázať, že napríklad $(\overline{1},\overline{0},\ldots,\overline{0})$ má vzor. Z predpokladu $Q_1 + Q_j = (1)$ pre každé $j \neq 1$ vyplýva existencia $u_2,\ldots,u_s \in Q_1$ a $v_j \in Q_j$ pre všetky $j = 2,3,\ldots,s$ že

$$u_2 + v_2 = 1, u_3 + v_3 = 1, \ldots, u_s + v_s = 1.$$

Nech $c = v_2v_3\ldots v_s$. Potom $c = (1-u_2)(1-u_3)\ldots(1-u_s)$ a teda $c-1 \in Q_1$ a $c-0 \in Q_j$ pre všetky $j \neq 1$. Z toho už je zrejmé že $\varphi(c) = (\overline{1},\overline{0},\ldots,\overline{0})$. □

Teraz môžeme dokázať vetu 1.6.1.

Dôkaz. Dôkaz spočíva v tom, že dokážeme izomorfizmus vektorových priestorov nad poľom k. Stačí nájsť jadro homomorfizmu φ z vety 1.6.2. $f \in \ker(\varphi)$ práve vtedy, keď $(f+Q_1,\ldots,f+Q_s) = (\overline{0},\ldots,\overline{0})$, t.j. keď $f \in Q_1, f \in Q_2, \ldots, f \in Q_s$ teda ak

$$f \in Q_1 \cap Q_2 \cap \ldots \cap Q_s = I.$$

To znamená, že $\ker(\varphi) = I$. □

Veta 1.6.3 *Nech I je ideál v okruhu $k[x_1,\dots,x_n]$ a $\mathrm{Lt}(I)$ je vedúci ideál vzhľadom na isté monomiálne usporiadanie v $k[x_1,\dots,x_n]$. Potom*

$$k[x_1,\dots,x_n]/I \simeq k[x_1,\dots,x_n]/\mathrm{Lt}(I).$$

Dôkaz. Definujme homomorfizmus $\psi\colon k[x_1,\dots,x_n]/I \to k[x_1,\dots,x_n]/\mathrm{Lt}(I)$ nasledovne: Nech $\Gamma = \{g_1\dots,g_t\}$ je Gröbnerova báza ideálu I. Podľa deliaceho algoritmu každý polynóm $f \in k[x_1,\dots,x_n]$ sa dá vyjadriť v tvare $f = a_1g_1+\cdots+a_tg_t+\overline{f^\Gamma}$, kde $a_1,\dots,a_t \in k[x_1,\dots,x_n]$. Podľa vety 1.4.2 je $\overline{f^\Gamma}$ polynómom f jednoznačne určený, definujme obraz polynómu f v homomorfizme φ ako $\overline{f^\Gamma} + \mathrm{Lt}(I)$. Je zrejmé, že $\overline{f^\Gamma} + \mathrm{Lt}(I) = 0 + \mathrm{Lt}(I)$ práve vtedy, keď $\overline{f^\Gamma} \in \mathrm{Lt}(I)$, čo je ekvivalentné $\overline{f^\Gamma} = 0$, teda $f \in I$. Dokázali sme, že $\ker(\psi) = I$. □

Nech ako doteraz I je nularozmerný ideál v $k[x_1,\dots,x_n]$ s primárnym rozkladom $Q_0 \cap Q_1 \cap \ldots \cap Q_s$, kde každý P_i-primárny ideál Q_i definuje bod C_i v $\mathbb{A}^n(k)$ pre $0 \le i \le s$, teda algebraická varieta $\mathbf{V}(Q_i) = C_i$. Násobnosť bodu C_i na variete $\mathbf{V}(I)$ definujeme ako rozmer vektorového priestoru $k[x_1,\dots,x_n]/Q_i$. Ak označíme násobnosť bodu C_i ako $j(C_i)$, potom

$$\dim_k k[x_1,\dots,x_n]/Q_i = j(C_i)$$

pre všetky $i = 0,1,\dots,s$.

Z doteraz povedaného a z viet 1.6.1, 1.6.2 a 1.6.3 vyplýva platnosť nasledujúcich viet.

Veta 1.6.4 *Nech $I = \langle f_1,\dots,f_s\rangle$ a $>$ je pevne zvolené monomiálne usporiadanie v $k[x_1,\dots,x_n]$. Nech $\mathrm{Lt}(I)$ je vedúci ideál ideálu I, teda I je generovaný Gröbnerovou bázou, potom*

$$\boxed{\dim_k k[x_1,\dots,x_n]/\mathrm{Lt}(I) = \sum_{i=0}^{s} j(C_i)}.$$

Veta 1.6.5 *Nech $I = \langle f_1,\dots,f_s\rangle$ a $>$ je pevne zvolené lokálne usporiadanie v okruhu $k[x_1,\dots,x_n]$. Nech $\mathrm{Lt}(I)$ je vedúci ideál ideálu I, teda I je generovaný štandardnou bázou, potom*

$$\boxed{\dim_k k[x_1,\dots,x_n]/\mathrm{Lt}(I) = j(C_0) = e_0(Q_0)},$$

kde $C_0 = (0,0,\dots,0)$ je začiatok súradnicovej sústavy priestoru $\mathbb{A}^n(k)$.

Praktická aplikácia spomínaných viet je v tom, že na rozdiel od ideálu I je ideál $\mathrm{Lt}(I)$ monomiálny, t.j. generovaný monómami a jeho dĺžka sa dá ľahšie vypočítať.

Príklad 1.6.2 Pomocou viet 1.6.4 a 1.6.5 vypočítajme počet bodov algebraickej variety z príkladu 1.6.1 ganerovaný ideálom $I = \langle x^2 - y^3, x^4 - y^5 \rangle$. Nech najprv v $k[x, y]$ je definované lexikografické usporiadanie. Použitím Buchbergerovho algoritmu dostávame, že Göbnerovu bázu ideálu I tvoria polynómy $x^2 - y^3, x^4 - y^5, y^6 - y^5$. Je teda $\mathrm{Lt}(I) = \langle x^2, x^4, y^6 \rangle = \langle x^2, y^6 \rangle$, a bázu vektorového priestoru $k[x_1, \ldots, x_n]/\mathrm{Lt}(I)$ tvoria monómy $1, x, y, y^2, y^3, y^4, y^5, xy, xy^2, xy^3, xy^4, xy^5$. Podľa vety 1.6.4 je

$$\dim_k k[x, y]/\left\langle x^2, y^6 \right\rangle = 12.$$

Celkový počet bodov algebraickej variety je 12, pričom každý bod sa ráta toľkokrát, koľko je jeho násobnosť.

Teraz vypočítajme násobnosť bodu $C_0 = (0, 0)$. Nech na $k[x, y]$ je zvolené antigradované lexikografické usporiadanie. Použitím Buchbergerovho algoritmu dostávame, že štandardnú bázu ideálu I tvoria polynómy $x^2 - y^3, x^4 - y^5, y^5 - y^6$, teda $\mathrm{Lt}(I) = \langle x^2, x^4, y^5 \rangle = \langle x^2, y^5 \rangle$, a bázu vektorového priestoru $k[x_1, \ldots, x_n]/\mathrm{Lt}(I)$ tvoria monómy $1, x, y, y^2, y^3, y^4, xy, xy^2, xy^3, xy^4$. Podľa vety 1.6.5 je

$$\dim_k k[x, y]/\left\langle x^2, y^5 \right\rangle = 10.$$

Bod $C_0 = (0, 0)$ je teda desaťnásobným bodom algebraickej variety ako sme to zistili aj v príklade 1.6.1.

2 Bèzoutova veta

V prvej kapitole sme odvodili praktické metódy na výpočet priesekovej násobnosti algebraických variet definované nejakým ideálom. Podľa tých výsledkov vieme vypočítať počet spoločných bodov algebraických variet i príslušnú násobnosť každého bodu v prieseku.

V tejto kapitole pokúsime podať odpoveď na otázku týkajúce sa počtu spoločných bodov dvoch projektívnych rovinných algebraických variet pomocou stupní homogénnych polynómov definujúce uvažované variety, t.j. Bèzoutovu vetu.

Skôr než by sme vyslovili spomínanú vetu potrebujeme definovať niektoré základné pojmy, ktorými budeme pracovať.

2.1 Projektívny priestor a homogénne súradnice

Nech k je pole a n je prirodzené číslo. Definujme reláciu ekvivalencie $\sim$ na množine nenulových usporiadaných $n+1$-tíc z k^{n+1} nasledovne

$$(x'_0, \ldots, x'_n) \sim (x_0, \ldots, x_n)$$

ak existuje nenulový prvok $\lambda \in k$ taký, že $(x'_0, \ldots, x'_n) = \lambda(x_0, \ldots, x_n)$.

Definícia 2.1.1 Nech k je pole a n je prirodzené číslo. Potom ***n-rozmerný projektívny priestor nad poľom*** k je množina tried ekvivalencií $\sim$ na $k^{n+1} \setminus \{(0, \ldots, 0)\}$. Teda

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

Usporiadaná nenulová $n+1$-tica $(x_0, \ldots, x_n) \in k^{n+1}$ definuje bod A v $\mathbb{P}^n(k)$ a $(x_0, \ldots, x_n)$ sa nazýva ***homogénne súradnice bodu*** A.

Príklad 2.1.1

1. Ak $n = 1$ a $k = \mathbb{R}$, potom jedenrozmerný projektívny priestor nad poľom $\mathbb{R}$ je možina

   $$\mathbb{P}^1(\mathbb{R}) = \{(x_0, x_1) \mid (x_0, x_1) \in \mathbb{R}^2 \setminus \{(0,0)\},\ (x_0, x_1) \sim (\lambda x_0, \lambda x_1), \forall \lambda \in \mathbb{R} \setminus \{0\}\},$$

   ktorá sa nazýva projektívna priamka. Modelom takéhoto priestoru je rozšírená euklidovská priamka $\overline{\mathbb{E}^1}$, ktorú sa dá chápať ako „obyčajná" euklidovská priamka ktorú doplníme práve jedným bodom, ktorého homogénna súradnica je $(0, u_1)$ a budeme ho označovať ako U_∞ a nazývame ho *nevlastný bod* priestoru $\overline{\mathbb{E}^1}$. Ostatné body sa nazývajú *vlastné body* priestoru.

2. Nech $n = 2$ a $k = \mathbb{R}$, potom dvojrozmerný projektívny priestor nad poľom $\mathbb{R}$ je možina $\mathbb{P}^2(\mathbb{R})$ ktorú sa dá analogicky definovať ako jednorozmerný projektívny

pristor v bode 1 a nazýame ho projektívna rovina. Modelom takéhoto priestoru je rozšírená euklidovská rovina $\overline{\mathbb{E}^2}$, ktorú sa dá chápať ako „obyčajná" euklidovská rovina ktorú doplníme práve jednou priamkou, ktorej homogénna rovnica je $u_0 = 0$ a budeme ju označovať ako u_∞ a nazývame ju *nevlastná priamka* priestoru $\overline{\mathbb{E}^2}$. Nevlastná priamka je teda množina všetkých nevlastných bodov priestoru. Ostatné priamky resp. body sa nazývajú *vlastné priamky* resp. *vlastné body* priestoru. Viac v [15].

V ďalšom budeme pracovať len v projektívnej rovine nad algebraicky uzavretým poľom k, napr. nad poľom $\mathbb{C}$. Nech $k[x, y]$ je okruh polynómov v neurčitých x, y nad poľom k. Potom $f \in k[x, y]$ sa dá napísať v tvare

$$f = \sum c_{\alpha_1,\alpha_2} x^{\alpha_1} y^{\alpha_2}, \quad c_{\alpha_1,\alpha_2} \in k, \quad \alpha_1, \alpha_2 \in \mathbb{N}_0.$$

Ak označíme vektor $\alpha = (\alpha_1, \alpha_2)$ potom súčet mocnín $|\alpha| = \alpha_1 + \alpha_2$ je stupeň monómu $x^{\alpha_1} y^{\alpha_2}$. Vytvorme množinu všetkých stupňov monómov z polynómu f. Stupeň polynómu budeme označovať $\deg(f)$ a definujeme ho ako

$$\deg(f) = \max\{|\alpha|\}.$$

Príklad 2.1.2 Nech $f = 2x^3y^4 + \frac{3}{2}x^5y^2 - 3xy + y^2 + y \in \mathbb{R}[x, y]$, potom stupeň monómov z f sú $|^1\alpha| = 3 + 4 = 7$, $|^2\alpha| = 5 + 2 = 7$, $|^3\alpha| = 1 + 1 = 2$, $|^4\alpha| = 0 + 2 = 2$ a $|^5\alpha| = 0 + 1 = 1$. Stupeň polynómu f je teda

$$\deg(f) = \max\{|^1\alpha|, |^2\alpha|, |^3\alpha|, |^4\alpha|, |^5\alpha|\} = \max\{7, 7, 2, 2, 1\} = 7.$$

Teraz môžeme definovať pojem homogénneho polynómu.

Definícia 2.1.2 Polynóm f z okruhu polynómov $k[x_1, \ldots, x_n]$ sa nazýva ***homogénny polynóm*** ak každý monóm z f má ten istý stupeň.

Príklad 2.1.3 Polynóm $f = x_1^2 + x_2^2$ je homogénny, ale $g = x_2^2 + x_2$ nie je homogénny polynóm z okruhu polynómov $k[x_0, x_1, x_2]$.

Nech v afinnej rovine $\mathbb{A}^2(k)$ nad ľubovoľným poľom k je daná pevná súradnicová sústava, t.j. existuje bijektívne zobrazenie medzi bodmi roviny a usporiadanými dvojicami prvkov poľa k. Nech $A \in \mathbb{A}^2(k)$ je ľubovoľný bod so súradnicami (x, y). Otázkou je aké homogénne súradnice má bod A. Podľa definície 2.1.1 vieme, že homogénne súradnice bodu $A \in \mathbb{P}^2(k)$ je usporiadaná trojica (x_0, x_1, x_2). Medzi afinnými a homogénnymi súradnicami bodu A platí nasledovný vzťah

$$x = \frac{x_1}{x_0}, \qquad y = \frac{x_2}{x_0}.$$

Potom ak $x_0 = 1$ homogénne súradnice bodu A je $(1, x, y)$ a každá usporiadaná trojica $(\lambda, \lambda x, \lambda y)$, kde $\lambda \in k \setminus \{0\}$.

Nasledujúca veta dáva odpoveď na otázku ako získať z polynómu $f \in k[x, y]$ homogénny polynóm $F \in k[x_0, x_1, x_2]$. Homogénne polynómy z $k[x_0, x_1, \ldots, x_n]$ budeme označovať veľkými písmenami F, G, H atď.

Veta 2.1.1 *Nech $f(x, y) \in k[x, y]$ je polynóm stupňa $\deg(f) = d$. Potom*

1. *homogénnu formu polynómu f vieme vypočítať podľa formuly*

$$F(x_0, x_1, x_2) = x_0^d f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right),$$

2. *dehomogenizáciou F dostaneme polynóm f podľa formuly*

$$F(1, x, y) = f(x, y),$$

kde $F[x_0, x_1, x_2] \in k[x_0, x_1, x_2]$.

Dôkaz. [8], kap. 8. §2 Projective Space and Projective Varieties, Proposition 7. s. 373. □

Príklad 2.1.4 Z príkladu 2.1.2 k polynómu $f = 2x^3y^4 + \frac{3}{2}x^5y^2 - 3xy + y^2 + y$ z $\mathbb{R}[x, y]$ so stupňom $\deg(f) = 7$ nájdime homogénny polynóm F z $\mathbb{R}[x_0, x_1, x_2]$. Podľa predchádzajúcej vety

$$\begin{aligned} F(x_0, x_1, x_2) &= x_0^7 f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right) \\ &= x_0^7\left(2\left(\frac{x_1}{x_0}\right)^3\left(\frac{x_2}{x_0}\right)^4 + \frac{3}{2}\left(\frac{x_1}{x_0}\right)^5\left(\frac{x_2}{x_0}\right)^2 - 3\frac{x_1}{x_0}\frac{x_2}{x_0} + \left(\frac{x_2}{x_0}\right)^2 + \frac{x_2}{x_0}\right) \\ &= 2x_1^3x_2^4 + \frac{3}{2}x_1^5x_2^2 - 3x_0^5x_1x_2 + x_0^5x_2^2 + x_0^6x_2. \end{aligned}$$

Keď podľa bodu 2. predchádzajúcej vety vypočítame $F(1, x, y)$ dostaneme polynóm $f(x, y)$.

Podobne ako afinné algebraické variety definované polynómami $f_1, \ldots, f_s$ z okruhu polynómov $k[x_1, \ldots, x_n]$ sa dajú definovať aj projektívne algebraické variety ktoré sú definované homogénnymi polynómami $F_1, \ldots, F_s$ z okruhu polynómov $k[x_0, x_1, \ldots, x_n]$.

Definícia 2.1.3 Nech k je pole a nech $F_1, \ldots, F_s$ sú homogénne polynómy z okruhu $k[x_0, x_1, \ldots, x_n]$. Potom množina

$$\mathbf{V}(F_1, \ldots, F_s) = \{(a_0, a_1, \ldots, a_n) \in \mathbb{P}^n(k) \mid F_i(a_0, a_1, \ldots, a_n) = 0,\ \forall\ 1 \leq i \leq s\}$$

sa nazýva ***projektívna algebraická varieta definovaná polynómami*** $F_1, \ldots, F_s$.

Príklad 2.1.5 Každý nenulový homogénny polynóm stupňa 1,

$$F(x_0, \ldots, x_n) = c_0x_0 + \cdots + c_nx_n,$$

definuje projektívnu varietu $\mathbf{V}(F)$, ktorá sa nazýva *nadrovina*. V projektívnej rovine $\mathbb{P}^2(k)$ nad poľom k je to projektívna priamka. Projektívna algebraická varieta, ktorá je definovaná práve jedným nenulovým homogénym polynómom F stupňa $\deg(F) \geq 2$ sa nazýva *nadplocha*. V projektívnej rovine $\mathbb{P}^2(k)$ nad poľom k je to projektívna krivka. Nech $F = -x_0^2 + x_1^2 + x_2^2$ potom $\mathbf{V}(F) \subset \mathbb{P}^2(\mathbb{R})$ je neprázdna regulárna kužeľosečka.

2.2 Rezultant

Nech sú v projektívnej rovine $\mathbb{P}^2(k)$ dané algebraické rovinné krivky $\mathcal{C}$ a $\mathcal{D}$ rovnicami:

$$\begin{aligned} \mathcal{C}: \ & F(x_0, x_1, x_2) = 0, \qquad \deg(\mathcal{C}) = m, \\ \mathcal{D}: \ & G(x_0, x_1, x_2) = 0, \qquad \deg(\mathcal{D}) = n, \end{aligned}$$

kde $\deg(\mathcal{C})$ ($\deg(\mathcal{D})$) označuje stupeň krivky $\mathcal{C}$ ($\mathcal{D}$), ktorá je definovaná ako stupeň určujúceho polynómu F (G), t.j. $\deg(\mathcal{C}) = \deg(F)$ ($\deg(\mathcal{D}) = \deg(G)$).

Hľadajme spoločné body týchto kriviek. Bez obmedzenia všeobecnosti môžeme predpokladať, že bod $O_2 = (0, 0, 1)$ nie je bodom žiadnej z uvedených kriviek. Pre definujúce homogénne polynómy F a G to znamená, že majú nasledovný tvar

$$\begin{aligned} F(x_0, x_1, x_2) &= \sum_{i=0}^{m} u_i x_2^{m-i}, \quad u_i = u_i(x_0, x_1),\ \deg(u_i) = i,\ u_0 \neq 0, \\ G(x_0, x_1, x_2) &= \sum_{i=0}^{n} v_i x_2^{n-i}, \quad v_i = v_i(x_0, x_1),\ \deg(v_i) = i,\ v_0 \neq 0. \end{aligned}$$

Nech bod $A = (a_0, a_1, a_2) \in \mathcal{C} \cap \mathcal{D}$, teda usporiadaná trojica (a_0, a_1, a_2) je riešením sústavy dvoch homogénnych rovníc

$$F(x_0, x_1, x_2) = 0 \quad \text{a} \quad G(x_0, x_1, x_2) = 0.$$

Vynásobme prvú rovnicu postupne výrazom $x_2^{n-1}, x_2^{n-2}, \ldots, x_2, 1$ a druhú rovnicu výrazom $x_2^{m-1}, x_2^{m-2}, \ldots, x_2, 1$. Dostávame $m + n$ homogénnych rovníc o $m + n$ neurčitých $x_2^{m+n-1}, x_2^{m+n-2}, \ldots, x_2, 1$ tvaru

$$\begin{aligned}
u_0x_2^{m+n-1} + u_1x_2^{m+n-2} + \quad \cdots \quad + u_mx_2^{n-1} &= 0\\
u_0x_2^{m+n-2} + u_1x_2^{m+n-3} + \quad \cdots \quad + u_mx_2^{n-2} &= 0\\
&\vdots\\
u_0x_2^{m} \quad + u_1x_2^{m-1} + \quad \cdots \quad + u_m &= 0\\
v_0x_2^{m+n-1} + v_1x_2^{m+n-2} + \quad \cdots \quad + v_nx_2^{m-1} &= 0\\
v_0x_2^{m+n-2} + v_1x_2^{m+n-3} + \quad \cdots \quad + v_nx_2^{m-2} &= 0\\
&\vdots\\
v_0x_2^{n} \quad + v_1x_2^{n-1} + \quad \cdots \quad + v_n &= 0
\end{aligned}$$

Keďže nenulová trojica (a_0, a_1, a_2) je prirodzene riešením aj tohoto systému je posledný systém rovníc riešiteľný, teda determinant matice systému je rovný nule. Označme tento determinant $\mathrm{Res}(\mathcal{C}, \mathcal{D})$.

Definícia 2.2.1 Determinant $\mathrm{Res}(\mathcal{C}, \mathcal{D})$ nazývame ***rezultantom*** kriviek $\mathcal{C}$ a $\mathcal{D}$ vzľadom na premennú x_2.

Z vlastností determinantov a z definície rezultantu platí

$$\mathrm{Res}(\mathcal{C}, \mathcal{D}) = \begin{vmatrix}
u_0 & 0 & \cdots & 0 & v_0 & 0 & \cdots & 0\\
u_1 & u_0 & \cdots & 0 & v_1 & v_0 & \cdots & 0\\
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots\\
u_m & u_{m-1} & \cdots & u_0 & v_n & v_{n-1} & \cdots & v_0\\
0 & u_m & \cdots & u_1 & 0 & v_n & \cdots & v_1\\
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots\\
0 & 0 & \cdots & u_m & 0 & 0 & \cdots & v_n
\end{vmatrix}$$

Determinant $\mathrm{Res}(\mathcal{C}, \mathcal{D})$ je typu $(m+n) \times (m+n)$.

Veta 2.2.1 *Rezultant* $\mathrm{Res}(\mathcal{C}, \mathcal{D})$ *je alebo identicky rovný nule, alebo je to homogénny polynóm v* x_0, x_1 *stupňa* mn, *teda* $\mathrm{Res}(\mathcal{C}, \mathcal{D}) = \mathrm{Res}(x_0, x_1)$.

Dôkaz. Nenulový prvok v i-tom riadku a j-tom stĺpci determinantu $\mathrm{Res}(\mathcal{C}, \mathcal{D})$ označme c_{ij}, pre ktorý platí

$$c_{ij} = \begin{cases} u_{i-j} & \text{ak } j \leq n\\ v_{i+n-j} & \text{ak } j > n \end{cases}$$

Inými slovami c_{ij} je homogénny polynóm v neurčitých x_0, x_1 stupňa $i-j$ resp. $i+n-j$ ak $j \leq n$ resp. $j > n$. Determinant môžeme vypočítať nasledovne

$$\sum_{\sigma \in P(M)} \mathrm{sign}(\sigma) \prod_{i=1}^{m+n} c_{i\sigma(i)},$$

kde $M = \{1, 2, \ldots, m+n\}$, $P(M)$ je množina všetkých permutácií množiny M a σ je permutácia množiny M. Podrobnejšie v [10], kap. 2. Lineárna algebra. Potom súčin

$$\prod_{i=1}^{m+n} c_{i\sigma(i)} = \prod_{\sigma(i)\leq n} c_{i\sigma(i)} \prod_{\sigma(i)>n} c_{i\sigma(i)},$$

je homogénny polynóm stupňa mn pretože

$$\begin{aligned}
\deg\left(\prod_{\sigma(i)\leq n} c_{i\sigma(i)} \prod_{\sigma(i)>n} c_{i\sigma(i)}\right) &= \sum_{\sigma(i)\leq n} \deg(c_{i\sigma(i)}) + \sum_{\sigma(i)>n} \deg(c_{i\sigma(i)}) \\
&= \sum_{\sigma(i)\leq n} (i - \sigma(i)) + \sum_{\sigma(i)>n} (i + n - \sigma(i)) \\
&= \sum_{\sigma(i)>n} n \\
&= mn.
\end{aligned}$$

Teda rezultant $\mathrm{Res}(\mathcal{C}, \mathcal{D})$ je homogénny polynóm v x_0, x_1 stupňa mn. □

Veta 2.2.2 *Nech k je algebraicky uzavreté pole ($\mathbb{C}$). Ak $H \in k[x_0, x_1]$ je nekonštantný homogénny polynóm stupňa d, potom H vieme napísať v tvare*

$$H = c(s_1 x_0 - r_1 x_1)^{m_1} \ldots (s_t x_0 - r_t x_1)^{m_t},$$

kde $c \neq 0$, $c \in k$ a $(r_1, s_1), \ldots, (r_t, s_t)$ sú po dvojiciach rôzne body z $\mathbb{P}^1(k)$. Naviše,

$$\mathbf{V}(H) = \{(r_1, s_1), \ldots, (r_t, s_t)\} \subseteq \mathbb{P}^1(k).$$

Dôkaz. Predpokladajme, že $H = \sum_{i=0}^{d} c_i x_0^i x_1^{d-i}$. Označme $h(x, y) = H(x_0, 1) = \sum_{i=0}^{d} c_i x^i$. Teda polynóm $h(x, y) \in k[x]$ sa dá napísať ako súčin koreňových činiteľov [10], kap. 5. Veta 5.5.4. c), t.j.

$$h(x, y) = c \prod_{i=1}^{t} (s_i x - r_i)^{m_i},$$

kde $c \neq 0$, $c \in k$ a $(r_i, s_i) \neq (r_j, s_j)$ pre $i \neq j$, $i, j = 1, 2, \ldots, t$ a $\sum_{i=1}^{t} m_i = d$ je stupeň polynómu h. Teraz

$$H(x_0, x_1) = x_0^d h\left(\frac{x_1}{x_0}\right) = x_0^d c \prod_{i=1}^{t} \left(s_i \frac{x_1}{x_0} - r_i\right)^{m_i} = c \prod_{i=1}^{t} (s_i x_0 - r_i x_1)^{m_i}.$$

Dokázali sme prvú časť tvrdenia, druhá je triviálna. □

Veta 2.2.3 *Ak bod $A = (a_0, a_1, a_2)$ je spoločným bodom kriviek $\mathcal{C}$ a $\mathcal{D}$, potom rezultant $\mathrm{Res}(a_0, a_1) = 0$. Ak $\mathrm{Res}(b_0, b_1) = 0$ pre určité $b_0, b_1 \in k$, potom existuje $b_2 \in k$ také, že pre bod $B = (b_0, b_1, b_2)$ platí $B \in \mathcal{C} \cap \mathcal{D}$.*

DÔKAZ. Prvá časť dôkazu je zrejmá. Nech teraz $\mathrm{Res}(b_0, b_1) = 0$ pre určité $b_0, b_1 \in k$. Potom existuje usporiadaná nenulová $n+m$-tica $(l_1, \ldots, l_n, l_{n+1}, \ldots, l_{n+m})$ prvkov poľa k že platí:

$$\begin{aligned} l_1u_0 + \cdots\cdots\cdots\cdots + l_{n+1}v_0 &= 0 \\ l_1u_1 + l_2u_0 + \cdots + l_{n+1}v_1 + l_{n+2}v_0 &= 0 \\ &\vdots \\ l_nu_n \ + \cdots + l_{n+m}v_m &= 0 \end{aligned}$$

Vynásobme postupne prvú rovnicu číslom x_2^{m+n-1}, druhú x_2^{m+n-2}, i-tu x_2^{m+n-i} a poslednú jednotkou. Ak vynásobené rovnice spočítame, tak po jednoduchých úpravách dostaneme

$$F(b_0, b_1, x_2)(l_1x_2^{n-1} + \cdots + l_n) = -G(b_0, b_1, x_2)(l_{n+1}x_2^{m-1} + \cdots + l_{n+m}).$$

Polynóm $F(b_0, b_1, x_2)$ jednej neurčitej x_2 stupňa m nad algebraicky uzavretým poľom sa dá vyjadriť ako súčin m nie nutne rôznych lineárnych činiteľov. Každý z nich musí vystupovať aj v rozklade polynómu na pravej strane rovnosti, teda minimálne jeden v rozklade polynómu $G(b_0, b_1, x_2)$. Teda existuje prvok b_2 z poľa k taký, že $F(b_0, b_1, b_2) = G(b_0, b_1, b_2) = 0$. □

Príklad 2.2.1 Hľadajme spoločné body krivky $\mathcal{C}$ a paraboly $\mathcal{D}$, teda algebraických rovinných kriviek danými rovnicami nehomogénnymi i homogénnymi

$$\begin{aligned} \mathcal{C}: \ & f(x,y) = x^3 + x^2 - y^2 = 0, \qquad F(x_0, x_1, x_2) = x_1^3 + x_0x_1^2 - x_0x_2^2 = 0 \\ \mathcal{D}: \ & g(x,y) = x^2 - y = 0, \qquad G(x_0, x_1, x_2) = x_1^2 - x_0x_2 = 0 \end{aligned}$$

Vidíme že bod $(0,1,0) \notin \mathcal{C}$ $(\notin \mathcal{D})$. Rezultant $\mathrm{Res}(\mathcal{C}, \mathcal{D})$ môžeme vyjadriť vzhľadom na premennú x_1.

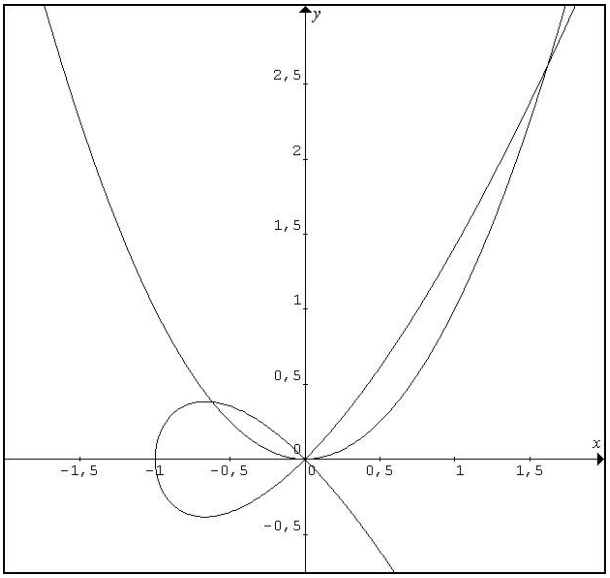
$$\mathrm{Res}(\mathcal{C}, \mathcal{D}) = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 \\ x_0 & 1 & 0 & 1 & 0 \\ 0 & x_0 & -x_0x_2 & 0 & 1 \\ -x_0x_2^2 & 0 & 0 & -x_0x_2 & 0 \\ 0 & -x_0x_2^2 & 0 & 0 & -x_0x_2 \end{vmatrix} = (x_0x_2)^2(x_0^2 - 3x_0x_2 + x_2^2)$$

Koreňmi rezultantu sú teda nasledovné dvojice (x_0, x_2)

$$\begin{aligned} (1,0) \ &- \ \text{dvojnásobný}, \\ (0,1) \ &- \ \text{dvojnásobný}, \\ \left(1, \tfrac{3+\sqrt{5}}{2}\right) \ &- \ \text{jednonásobný}, \\ \left(1, \tfrac{3-\sqrt{5}}{2}\right) \ &- \ \text{jednonásobný}, \end{aligned}$$

ktoré dávajú spoločné body kriviek $\mathcal{C}$ a $\mathcal{D}$ s príslušnými násobnosťami, teda

$$\begin{aligned} (1,0,0) &\quad - \quad \text{dvojnásobný,} \\ (0,0,1) &\quad - \quad \text{dvojnásobný,} \\ \left(1, \tfrac{1+\sqrt{5}}{2}, \tfrac{3+\sqrt{5}}{2}\right) &\quad - \quad \text{jedennásobný,} \\ \left(1, \tfrac{1-\sqrt{5}}{2}, \tfrac{3-\sqrt{5}}{2}\right) &\quad - \quad \text{jedennásobný.} \end{aligned}$$



Obrázok 1: Krivka a parabola

Vidíme, že krivky $\mathcal{C}$ a $\mathcal{D}$ stupňa tretieho a druhého majú spoločné práve šesť bodov. Platí to aj vo všeobecnosti? Áno, ale o tom neskôr.

Lema 2.2.1 *Nech k je algebraicky uzavreté pole a $F, G \in k[x_0, x_1, x_2]$ sú nenulové homogénne polynómy. Nech $l_1, \ldots, l_n$, $n \in \mathbb{N}$ sú ľubovoľné projektívne priamky v $\mathbb{P}^2(k)$. Potom existuje bod $Q = (q_0, q_1, q_2) \in \mathbb{P}^2(k)$ taký, že*

$$Q \notin \bigcup_{i=0}^{n} l_i \cup \mathbf{V}(F) \cup \mathbf{V}(G)$$

Dôkaz. Ak $L_1 = 0, \ldots, L_n = 0$ sú homogénne polynómy stupňa 1 definujúce projektívne priamky $l_1, \ldots, l_n$, potom

$$F.G. \prod_{i=1}^{n} L_i = 0$$

je polynóm definujúci projektívnu varietu $\bigcup_{i=0}^{n} l_i \cup \mathbf{V}(F) \cup \mathbf{V}(G)$. Stačí teda ukázať, že existuje bod $Q \notin \mathbf{V}(F)$. Nech taký bod Q neexisteje. Potom každý bod projektívnej roviny leží va variete $\mathbf{V}(F)$. Pole k je algebraicky uzavreté z čoho vyplýva $\mathbf{V}(F) = \mathbb{P}^2(k)$ a to len vtedy, keď F je nulový polynóm, čo je spor s predpokladom, teda $\mathbf{V}(F) \neq \mathbb{P}^2(k)$. Existuje teda bod $Q \notin \mathbf{V}(F)$. □

Veta 2.2.4 *Nech k je algebraicky uzavreté pole. Nech nenulový homogénny polynóm $F \in k[x_0, x_1, x_2]$ stupňa m definuje krivku $\mathcal{C}$ a nenulový homogénny polynóm $G \in k[x_0, x_1, x_2]$ stupňa n definuje krivku $\mathcal{D}$. Ak projektívne krivky $\mathcal{C}$ a $\mathcal{D}$ v $\mathbb{P}^2(k)$ nemajú spoločný komponent, potom počet spoločných bodov kriviek $\mathcal{C}$, $\mathcal{D}$ je konečný a $|\mathcal{C} \cap \mathcal{D}| \leq mn$.*

Dôkaz. Dokážeme nepriamo. Nech F a G sú homogénne polynómy definujúce krivky $\mathcal{C}$ a $\mathcal{D}$. Ak $|\mathcal{C} \cap \mathcal{D}| > mn$ potom z množiny priesečníkov vieme vybrať $mn+1$ rôznych bodov $A_i = (a_{i0}, a_{i1}, a_{i2})$, $i = 1, 2, \ldots, mn+1$ a pre $i < j$ označme l_{ij} priamku prechádzajúcu bodmi A_i, A_j, $j = 1, 2, \ldots, mn+1$. Podľa lemy 2.2.1 existuje bod $Q \in \mathbb{P}^2(k)$, že

$$Q \notin \bigcup_{i<j} l_i \cup \mathbf{V}(F) \cup \mathbf{V}(G) = \bigcup_{i<j} l_i \cup \mathcal{C} \cup \mathcal{D}.$$

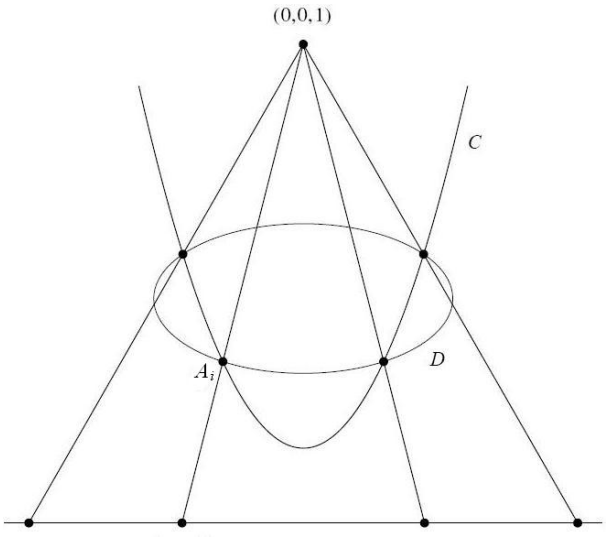
Nech je to bod $(0, 0, 1)$. To sa dá vždy dosiahnuť pozri [6], kap. 7. Věta 4.1 s. 218. Rovnice krivky $\mathcal{C}$ a $\mathcal{D}$ teda majú tvar

$$F(x_0, x_1, x_2) = \sum_{i=0}^{m} u_i x_2^{m-i}, \quad u_i = u_i(x_0, x_1),\ \deg(u_i) = i,\ u_0 \neq 0,$$

$$G(x_0, x_1, x_2) = \sum_{i=0}^{n} v_i x_2^{n-i}, \quad v_i = v_i(x_0, x_1),\ \deg(v_i) = i,\ v_0 \neq 0.$$

Pretože bod $(0, 0, 1)$ neleží na žiadnej priamke l_{ij} spájajúce body A_i, A_j sú všetky body (a_{j0}, a_{j1}), $j = 1, 2, \ldots, mn+1$ rôzne. Keby totiž pre $j, k, j \neq k$ bolo $(a_{j0}, a_{j1}) = (a_{k0}, a_{k1})$, t.j. $a_{j0}a_{k1} = a_{k0}a_{j1}$, na ich spojnici, priamke s rovnicou $x_0 a_{k1} - x_1 a_{k0}$ by ležal bod $(0, 0, 1)$ čo nie je možné podľa predpokladu.

Z viet 2.2.1 a 2.2.3 vyplýva, že polynóm $\mathrm{Res}(\mathcal{C}, \mathcal{D})$ stupňa mn má $mn + 1$ rôznych koreňov, musí byť teda nulový. Krivky $\mathcal{C}$ a $\mathcal{D}$ teda majú spoločný komponent. □



Obrázok 2: K vete 2.2.4

Rezultant dvoch kriviek stupňa m a n v projektívnej rovine nad algebraicky uzavretým poľom k je homogénny polynóm jednej neurčitej stupňa mn. Spĺňa všetky podmienky vety 2.2.2, teda platí

$$\mathrm{Res}(\mathcal{C},\mathcal{D}) = c\prod_{i=1}^{t}(s_i x_0 - r_i x_1)^{d_i},$$

kde $c \neq 0$ a $\sum_{i=1}^{t} d_i = mn$. Koreňmi tohoto polynómu sú usporiadané dvojice (r_i, s_i) pre $i = 1, 2, \ldots, t$. Každej usporiadanej dvojici (r_i, s_i) vieme jednoznačne priradiť prirodzené číslo d_i. Nech $P = (p_0, p_1, p_2)$ je bodom $\mathcal{C} \cap \mathcal{D}$, t.j (p_0, p_1) je koreňom rezultantu $\mathrm{Res}(\mathcal{C},\mathcal{D})$ a k tomuto je priradené číslo d_p.

Definícia 2.2.2 Prirodzené číslo d_p sa nazýva ***prieseková násobnosť*** bodu $P \in \mathcal{C} \cap \mathcal{D}$ a označujeme ju $j(\mathcal{C} \cap \mathcal{D}, P)$.

Príklad 2.2.2 Z príkladu 2.2.1 rezultant kriviek $\mathcal{C}$ a $\mathcal{D}$ sa rovná $(x_0x_2)^2(x_0^2 - 3x_0x_2 + x_2^2)$ ktorú môžeme upraviť na tvar

$$x_0^2x_2^2\left(x_0 + x_2\frac{\sqrt{5}-3}{2}\right)\left(x_0 - x_2\frac{\sqrt{5}+3}{2}\right).$$

Teda násobnosť bodu $P_1 = (1,0,0)$ je $j(\mathcal{C} \cap \mathcal{D}, P_1) = 2$, bodu $P_2 = (0,0,1)$ je $j(\mathcal{C} \cap \mathcal{D}, P_2) = 2$, bodu $P_3 = (1, (1+\sqrt{5})/2, (3+\sqrt{5})/2)$ je $j(\mathcal{C} \cap \mathcal{D}, P_3) = 1$ a bodu $P_4 = (1, (1-\sqrt{5})/2, (3-\sqrt{5})/2)$ je $j(\mathcal{C} \cap \mathcal{D}, P_4) = 1$.

Z doteraz povedaného vyplýva platnosť nasledujúcej vety.

Veta 2.2.5 (Bèzoutova veta) *Nech $\mathcal{C}$ a $\mathcal{D}$ sú projektívne krivky v $\mathbb{P}^2(k)$, kde k je algebraicky uzavreté pole, bez spoločných komponentov a nech m resp. n je stupeň nenulového homogénneho polynómu F resp. G definujúca krivku $\mathcal{C}$ resp. $\mathcal{D}$ z okruhu polynómov $k[x_0, x_1, x_2]$, potom*

$$\sum_{P \in \mathcal{C}\cap\mathcal{D}} j(\mathcal{C} \cap \mathcal{D}, P) = \deg(F).\deg(G) = mn,$$

kde $j(\mathcal{C} \cap \mathcal{D}, P)$ je prieseková násobnosť bodu $P \in \mathcal{C} \cap \mathcal{D}$.

Je teda jasné, že počet spoločných bodov dvoch rovinných algebraických kriviek v projektívnej rovine nad algebraicky uzavretým poľom (ktoré nemajú spoločnú súčasť) počítaných s príslušnou násobnosťou je rovný súčinu stupňov týchto kriviek.

2.3 Lokálna Bèzoutova veta

Bèzoutova veta (veta 2.2.5) hovorí globálne o počte spoločných bodov dvoch rovinných algebraických kriviek v $\mathbb{P}^2(k)$ nad algebraicky uzavretým poľom k. Nezaoberá sa lokálnou otázkou násobnosti jedného bodu v prieseku. Nerieši problém súvis medzi násobnosti spoločného bodu prieniku s jeho násobnosťou na jednotlivých krivkách.

V tejto časti vysovíme lokálnu formuláciu Bèzoutovej vety od Bydžovského a odvodíme jednoduché tvrdenia tykajúce sa tohoto problému.

Definícia 2.3.1 Nech $\mathcal{C}$ je krivka v $\mathbb{P}^2(k)$ definovaná rovnicou $F(x_0, x_1, x_2) = 0$ a nech m je stupeň krivky $\mathcal{C}$. Potom

1. bod $A = (a_0, a_1, a_2) \in \mathcal{C}$ nazveme ***regulárnym*** bodom $\mathcal{C}$ ak
$$\frac{\partial F(A)}{\partial x_i} \neq 0$$
aspoň pre jedno $i = 0, 1, 2$,

2. bod $A = (a_0, a_1, a_2) \in \mathcal{C}$ nazveme ***singulárnym*** bodom $\mathcal{C}$ ak
$$\frac{\partial F(A)}{\partial x_i} = 0$$
pre všetky $i = 0, 1, 2$,

3. singulárny bod $A = (a_0, a_1, a_2) \in \mathcal{C}$ nazveme r***-násobným*** bodom $\mathcal{C}$ ak
$$\frac{\partial^k F(A)}{\partial x_0^{k_0} \partial x_1^{k_1} \partial x_2^{k_2}} = 0$$
pre všetky $k \leq r-1$ a všetky prístupné trojice (k_0, k_1, k_2) a aspoň pre jednu trojicu (r_0, r_1, r_2) s $r_0 + r_1 + r_2 = r$ platí
$$\frac{\partial^r F(A)}{\partial x_0^{r_0} \partial x_1^{r_1} \partial x_2^{r_2}} \neq 0.$$

Nasledovná veta hovorí o dotyčniciach v regulárnom i singulárnom bode krivky. Uvedieme ju bez dôkazu.

Veta 2.3.1 *Krivka $\mathcal{C}$ má v regulárnom bode $A = (a_0, a_1, a_2)$ práve jednu dotyčnicu t_A. Jej rovnica je*
$$t_A : \ \frac{\partial F(A)}{\partial x_0} x_0 + \frac{\partial F(A)}{\partial x_1} x_1 + \frac{\partial F(A)}{\partial x_2} x_2 = 0.$$
V r-násobnom bode $A = (a_0, a_1, a_2)$ krivky $\mathcal{C}$ má krivka práve r dotyčníc. Rovnica tohoto zväzku dotyčníc je
$$\tau_A : \ \left(\sum \frac{\partial F(A)}{\partial x_i} x_i \right)^r = 0,$$

kde pre symbolický zápis $\left(\sum \frac{\partial F(A)}{\partial x_i} x_i\right)^r$ *platí*

$$\left(\sum \frac{\partial F(A)}{\partial x_i} x_i\right)^r = \sum \frac{r!}{r_0! r_1! r_2!} \frac{\partial^r F(A)}{\partial x_0^{r_0} \partial x_1^{r_1} \partial x_2^{r_2}} x_0^{r_0} x_1^{r_1} x_2^{r_2},$$

pričom suma prebieha cez všetky usporiadané trojice (r_0, r_1, r_2) *pre ktoré* $r_0 + r_1 + r_2 = r$.

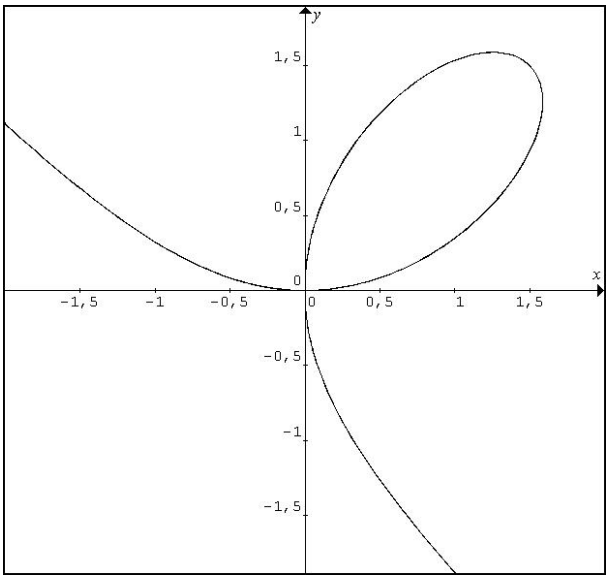
Príklad 2.3.1 Nech krivka $\mathcal{C}$ je daná rovnicou $f(x, y) = x^3 + y^3 - 3xy = 0$. Homogénna rovnica je $F(x_0, x_1, x_2) = x_1^3 + x_2^3 - 3x_0x_1x_2$. Riešenie systému rovníc $\frac{\partial F}{\partial x_0} = -3x_1x_2$, $\frac{\partial F}{\partial x_1} = 3x_1^2 - 3x_0x_2$ a $\frac{\partial F}{\partial x_2} = 3x_2^2 - 3x_0x_1$ je bod $(\lambda, 0, 0)$ a pre $\lambda = 1$ je to bod $(1, 0, 0)$. V euklidovskej rovine $\mathbb{E}^2$ je to začiatok súradnicovej sústavy $O = (0, 0)$. Krivka $\mathcal{C}$ má jediný singulárny bod, všetky ostatné sú regulárne. Bod $A = (1, 0, 0)$ je dvojnásobým bodom krivky, pretože $\frac{\partial^2 F(A)}{\partial x_1 \partial x_2} = -3x_0 = -3 \neq 0$. Rovnica zväzku dotyčníc v bode A má tvar

$$\frac{2!}{2!0!0!}\frac{\partial^2 F(A)}{\partial x_0^2}x_0^2 + \frac{2!}{0!2!0!}\frac{\partial^2 F(A)}{\partial x_1^2}x_1^2 + \frac{2!}{0!0!2!}\frac{\partial^2 F(A)}{\partial x_2^2}x_2^2 +$$
$$+\frac{2!}{1!1!0!}\frac{\partial^2 F(A)}{\partial x_0 \partial x_1}x_0x_1 + \frac{2!}{1!0!1!}\frac{\partial^2 F(A)}{\partial x_0 \partial x_2}x_0x_2 + \frac{2!}{0!1!1!}\frac{\partial^2 F(A)}{\partial x_1 \partial x_2}x_1x_2 = 0,$$

teda

$$\tau_A : \; x_1x_2 = 0.$$

Zväzok dotyčníc v bode A je teda zjednotenie priakom $x_1 = 0$ a $x_2 = 0$. V euklidovskej rovine $\mathbb{E}^2$ sú to súradnicové osi. Krivka $\mathcal{C}$ sa nazýva *Descartesov list*.



Obrázok 3: Descartesov list

Teraz vyslovíme Bydžovského formuláciu Bèzoutovej vety.

Veta 2.3.2 (Bydžovský) *Dve rovinné algebraické krivky stupňov m a n, ktoré nemajú spoločnú súčasť, majú spoločných práve mn bodov, ak sa každý bod počíta s príslušnou násobnosťou. Priesečník, ktorý je na jednej krivke r-násobný, na druhej s-násobný a v ktorom majú krivky spoločných h dotyčníc, je priesečníkom aspoň $(rs + h)$-násobným.*

Dôkaz. [7], kap. 11. 134 f) □

Ekvivalentná veta k vete Bydžovského je, že existuje nezáporné celé číslo ϱ také, že bod A je práve $(rs + h) + \varrho$ násobným priesečníkom daných kriviek.

Zatiaľ nie je zrejmá geometrická interpretácia korekcie ϱ. V nasledujúcich riadkoch pokúsime vysloviť hodnovernú hypotézu na číslo ϱ.

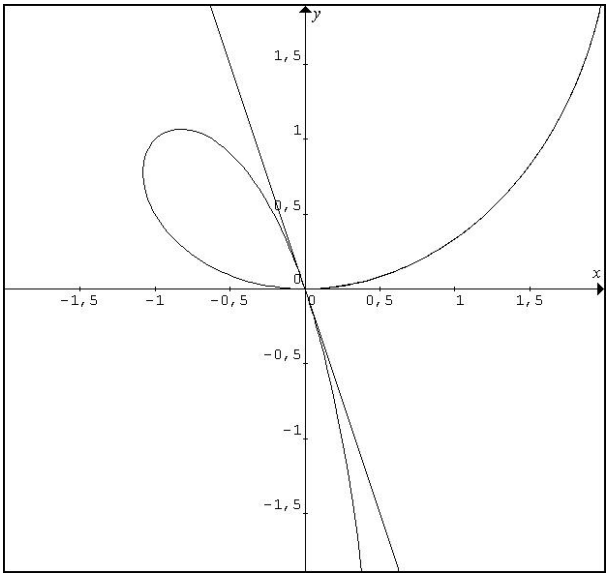
Otázka násobnosti izolovaného bodu v prieseku dvoch kriviek je lokálnou vlastnosťou, preto stači sa nám obmedziť na algebraické krivky v afinnej rovine. Pomocou afinnej transformácie súradnicovej sústavy vždy môžeme dosiahnuť aby skúmaný bod prieniku bol totožný so začiatkom súradnicovej sústavy so súradnicami $(0, 0)$.

Nech $f \in k[x, y]$ je polynóm stupňa m definujúci krivku $\mathcal{C}$. Keďže bod $(0, 0)$ leží na krivke $\mathcal{C}$, teda $f(0, 0) = 0$, polynóm f nemá absolútny člen. Môžeme teda f napísť v tvare

$$f(x, y) = \sum c_{ij} x^i y^j = f_0 + f^*,$$

kde f^* je homogénny polynóm najnižšieho stupňa $\deg(f^*) = r$. Pre polynóm $f = x^3 + xy^2 - y^2 - 3xy$ je $f^* = -y^2 - 3xy$ a $\deg(f^*) = 2$. Nech polynómu f prislúcha homogénny polynóm $F \in k[x_0, x_1, x_2]$, ktorý vieme určiť podľa vety 2.1.1. Potom z definície 2.3.1 r-násobného bodu a z vety 2.3.1 pre zväzok dotyčníc v tomto bode vyplýva, že násobnosť bodu $(0, 0)$ na krivke $\mathcal{C}$ sa rovná stupni homogénnej časti polynómu f najnižšieho stupňa, t.j. f^* a zväzok dotyčníc v tomto bode je definovaný rovnicou $f^* = 0$. V našom konkrétnom príklade je násobnosť začiatku súradnicovej sústavy 2 a zväzok dotyčníc je určený rovnicou $y^2 + 3xy = y(y + 3x) = 0$, čo je zjednotenie priamok $y = 0$ a $y + 3x = 0$ (obrázok 4).

Skúmajme teraz dve krivky $\mathcal{C}$ a $\mathcal{D}$ v afinnej rovine $\mathbb{A}^2(k)$ definované polynómami $f(x, y)$ a $g(x, y)$ z okruhu $k[x, y]$ pre ktorých ideál $I = \langle f, g \rangle$ je m-primárny v lokálnom okruhu polynómov $A = k[x, y]_{\langle x,y \rangle}$, $m = \langle x, y \rangle$ to znamená, že bod $(0, 0)$ patrí do prieniku $\mathbf{V}(f) \cap \mathbf{V}(g) = \mathcal{C} \cap \mathcal{D} \subset \mathbb{A}^2(k)$. Nech f^* a g^* sú polynómy popísané vyššie s $\deg(f^*) = r$ resp. $\deg(g^*) = s$, potom r je násobnosť bodu $(0, 0)$ na krivke $\mathcal{C}$ resp. s je násobnosť bodu $(0, 0)$ na krivke $\mathcal{D}$. Samuelova násobnosť $e_0(\langle f, g \rangle, A)$ je násobnosť bodu $(0, 0)$ v prieniku $\mathcal{C} \cap \mathcal{D}$ a rovnica $f^* = 0$ resp. $g^* = 0$ definuje zväzok dotyčníc v tomto bode ku krivke $\mathcal{C}$ resp. $\mathcal{D}$. Je zrejmé, že najväčší spoločný deliteľ polynómov f^* a g^* definuje zväzok spoločných dotyčníc k obidvom krivkám v bode $(0, 0)$.



Obrázok 4: Zväzok dotyčníc krivky v začiatku súradnicovej sústavy

Veta 2.3.3 *Ak krivky $\mathcal{C}$, $\mathcal{D}$ v bode O nemajú spoločnú dotyčnicu, t.j. $h = 0$, potom $\varrho = 0$ a násobnosť bodu O v prieseku je rs.*

Dôkaz. Nech f, g sú polynómy v okruhu $k[x, y]$ ktoré definujú dve rovinné algebraické krivky v $\mathbb{A}^2(k)$, $\mathcal{C} = \mathbf{V}(f)$, $\mathcal{D} = \mathbf{V}(g)$. Podľa predpokladu majú $\mathcal{C}$ a $\mathcal{D}$ len konečný počet spoločných bodov a bod $O = (0, 0)$ je jeden z nich. Nech f^* a g^* sú formy najnižšieho stupňa vystupujúce v polynómoch f a g (v poradí). Nech $A = k[x, y]_{\langle x,y\rangle}$ je lokálny okruh polynómov, $m = \langle x, y\rangle$ je jediný maximálny ideál v ňom. Keďže monómy f^* a g^* sú nesúdeliteľné, tvoria systém parametrov v A. V opačnom prípade by $\dim \langle f^*, g^*\rangle = 1$, teda by existoval jednorozmerný prvoideál obsahujúci ideál $\langle f^*, g^*\rangle$. Jeho generátor by bol ale deliteľom tak f^* ako aj g^*, čo je v spore s predpokladom. Je teda $\{f^*, g^*\}$ systém parametrov v A. Tvrdenie teraz vyplýva z lemy 3.1. práce [14]. □

Poznámka. V prípade, že f^* a g^* sú monómy, existuje elegantný a jednoduchý dôkaz tejto vety. Nech $>$ je gradované lexikografické usporiadanie v $k[x, y]$. Ak f^* a g^* sú monómy, potom $f^* = \mathrm{Lt}(f)$ a $g^* = \mathrm{Lt}(g)$. Keďže podľa predpokladu $\mathrm{Lt}(f)$ a $\mathrm{Lt}(g)$ sú nesúdeliteľné, je na základe lemy 1.5.1 a dôsledku 1.5.1 dvojica $\{f, g\}$ štandardnou bázou ideálu $I = \langle f, g\rangle$, teda na základe vety 1.6.5

$$e_0(\langle f, g\rangle, A) = \dim_k k[x, y]/\mathrm{Lt}(I) = \dim_k k[x, y]/\langle f^*, g^*\rangle = \deg(f^*).\deg(g^*) = r.s.$$

Je teda $h = \varrho = 0$.

Obrátená veta neplatí vo všeobecnosti ako to ukazuje nasledujúci príklad.

Príklad 2.3.2 Krivky $\mathcal{C}$ a $\mathcal{D}$ v afinnej rovine sú dané rovnicami

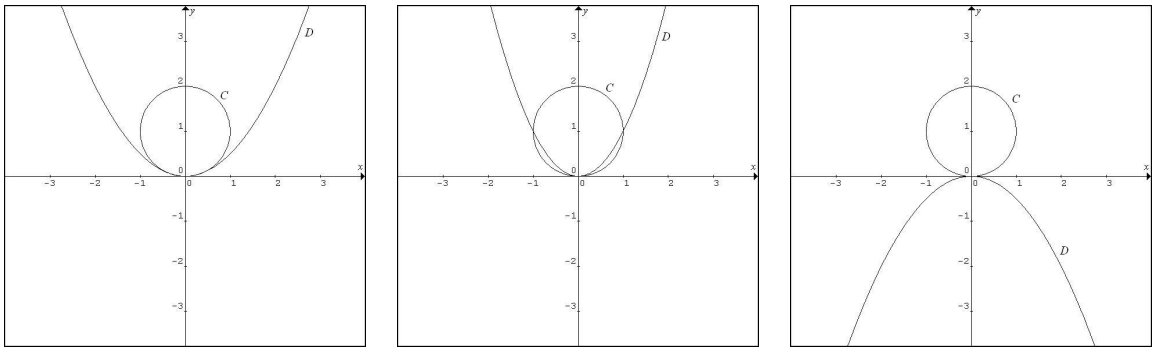
$$\mathcal{C}: \ f = x^2 + y^2 - 2y,$$

$$\mathcal{D}: \ g = x^2 - \lambda y, \quad \lambda \neq 0.$$

Je zrejmé, že začiatok súradnicovej sústavy $O = (0,0)$ je bodom prieniku $\mathcal{C} \cap \mathcal{D}$. Potom $f^* = -2y$ a $g^* = -\lambda y$, teda jedinou spoločnou dotyčnicou obidvoch kriviek je $y = 0$. Pre násobnosť bodu O platí

$$\begin{aligned} j(\mathcal{C} \cap \mathcal{D}, O) &= e_0(\langle f, g \rangle, A) \\ &= e_0(\langle x^2 + y^2 - 2y, x^2 - \lambda y \rangle, A) \\ &= e_0(\langle y^2 + (\lambda - 2)y, x^2 - \lambda y \rangle, A). \end{aligned}$$

Ak $\lambda = 2$, potom $j(\mathcal{C} \cap \mathcal{D}, O) = e_0(\langle y^2, x^2 - 2y \rangle, A) = 4$. $\deg(f^*) = 1$, $\deg(g^*) = 1$ a počet spoločných dotyčníc $h = 1$, potom $j(\mathcal{C} \cap \mathcal{D}, O) = 4 = 1.1 + 1 + 2$, teda korekcia $\varrho = 2$. Ak $\lambda \neq 2$, potom $j(\mathcal{C} \cap \mathcal{D}, O) = e_0(\langle y, x^2 - \lambda y \rangle, A) = 2 = 1.1 + 1 + 0$, teda korekcia $\varrho = 0$.



$\lambda = 2$ $\lambda = 1$ $\lambda = -2$

Obrázok 5: Rôzne hodnoty λ

Skúmajme súčet $h + \varrho$, kde h je počet spoločných dotyčníc dvoch kriviek a ϱ nezáporné celé číslo. Vypočítajme styk rádu n daných kriviek a porovnajme so súčtom $h + \varrho$. Použijeme pritom známe tvrdenia z diferenciálnej geomtrie tzv. *beta podmienky styku.* Krivky $P_1(t)$ a $P_2(t)$ majú v bode $P_1(t_1) = P_2(t_2)$ styk rádu 4 práve vtedy, keď existujú také čísla β_i pre $i = 1, \ldots, 4$, $\beta_1 \neq 0$, že

$$P_2'(t_2) = \beta_1 P_1'(t_1) \tag{1}$$

$$P_2''(t_2) = \beta_1^2 P_1''(t_1) + \beta_2 P_1'(t_1) \tag{2}$$

$$P_2'''(t_2) = \beta_1^3 P_1'''(t_1) + 3\beta_1\beta_2 P_1''(t_1) + \beta_3 P_1'(t_1) \tag{3}$$

$$P_2^{(iv)}(t_2) = \beta_1^4 P_1^{(iv)}(t_1) + 6\beta_1^2\beta_2 P_1'''(t_1) + (4\beta_1\beta_3 + \beta_2^2) P_1''(t_1) + \beta_4 P_1'(t_1) \tag{4}$$

Aby sme vedeli vypočítať styk kriviek $\mathcal{C}$ a $\mathcal{D}$ potrebujeme parametrické vyjadrenia daných kriviek. Nech parametrické rovnice krivky $\mathcal{C}$ je $P_1(t_1) = (\cos t_1, \sin t_1 + 1)$, kde $t_1 \in \langle 0; 2\pi \rangle$ a krivky $\mathcal{D}$ je $P_2(t_2) = \left(t_2, \frac{t_2^2}{\lambda}\right)$, kde $t_2 \in \mathbb{R}$ a $\lambda \neq 0$. Bod O na krivke $\mathcal{C}$ prislúcha parametru $t_1 = \frac{3}{2}\pi$ a na krivke $\mathcal{D}$ parametru $t_2 = 0$. Najprv určíme hodnoty derivácií:

$$
\begin{aligned}
P_1'(t_1) &= (-\sin t_1, \cos t_1) & P_1'\left(\tfrac{3}{2}\pi\right) &= (1,0)\\
P_1''(t_1) &= (-\cos t_1, -\sin t_1) & P_1''\left(\tfrac{3}{2}\pi\right) &= (0,1)\\
P_1'''(t_1) &= (\sin t_1, -\cos t_1) & P_1'''\left(\tfrac{3}{2}\pi\right) &= (-1,0)\\
P_1^{iv}(t_1) &= (\cos t_1, \sin t_1) & P_1^{iv}\left(\tfrac{3}{2}\pi\right) &= (0,-1)\\
P_2'(t_2) &= \left(1, \tfrac{2t}{\lambda}\right) & P_2'(0) &= (1,0)\\
P_2''(t_2) &= \left(0, \tfrac{2}{\lambda}\right) & P_2''(0) &= \left(0, \tfrac{2}{\lambda}\right)\\
P_2'''(t_2) &= (0,0) & P_2'''(0) &= (0,0)\\
P_2^{iv}(t_2) &= (0,0) & P_2^{iv}(0) &= (0,0)
\end{aligned}
$$

Ukážeme, že v bode O krivky $\mathcal{C}$ a $\mathcal{D}$ majú styk rádu práve 1 pre $\lambda \neq 2$ a styk rádu práve 3 ak $\lambda = 2$. Po vyriešení (1) dostaneme hodnotu pre $\beta_1 = 1 \neq 0$. Potom zo vzťahu (2) pre β_2 dostaneme 0 ak $\lambda = 2$, v inom prípade sústava (2) nie je riešiteľná. Krivky $\mathcal{C}$ a $\mathcal{D}$ v bode O pre hodnotu $\lambda \neq 2$ majú styk rádu práve $n = 1$, a teda platí rovnosť $n = 1 = 1 + 0 = h + \varrho$. Ak $\lambda = 2$ potom z (3) máme $\beta_3 = 1$, ale sústava (4) už nie je riešiteľná. Znamená to, že uvažované krivky v bode O majú styk rádu práve $n = 3$, teda opäť platí $n = 3 = 1 + 2 = h + \varrho$. Pripomeňme, že ak dve krivky majú v spoločnom bode styk rádu 1, tak v tom bode majú spoločnú dotyčnicu, ak majú styk rádu 2, tak v tom bode majú spoločnú dotyčnicu, oskulačnú kružnicu a krivosť. To znamená, že pre hodnotu $\lambda = 2$ kružnica $\mathcal{C}$ je oskulačnou kružnicou paraboly $\mathcal{D}$.

Príklad 2.3.3 Nech sú v afinnej rovine nad $\mathbb{C}$ dané krivky $\mathcal{U}$, $\mathcal{V}$ a $\mathcal{W}$ rovnicami

$$
\begin{aligned}
\mathcal{U}:&\ f = x^3 + xy^2 - y^2 - 3xy\\
\mathcal{V}:&\ g = x^2 + y^2 - 3y\\
\mathcal{W}:&\ h = x^3 + y^3 - 3xy
\end{aligned}
$$

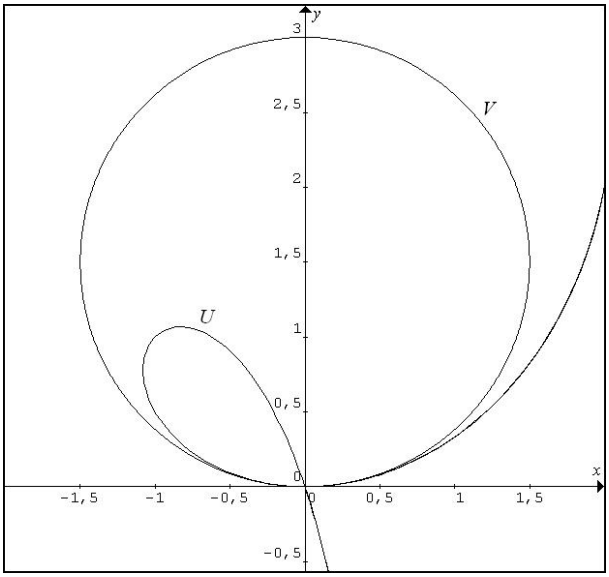
Je zrejmé, že bod $O = (0,0)$ je izolovaným bodom prieniku $\mathcal{U}\cap\mathcal{V}$, $\mathcal{U}\cap\mathcal{W}$, $\mathcal{V}\cap\mathcal{W}$. Vypočítajme jeho násobnosť vo všetkých troch prienikoch, teda čísla $e_0(\langle f,g\rangle, A)$, $e_0(\langle f,h\rangle, A)$, $e_0(\langle g,h\rangle, A)$, kde $A = k[x,y]_{\langle x,y\rangle}$ s maximálnym ideálom $m = \langle x,y\rangle$.

$$
\begin{aligned}
e_0(\langle f,g\rangle, A) &= e_0(\left\langle x^3 + xy^2 - y^2 - 3xy, x^2 + y^2 - 3y\right\rangle, A)\\
&= e_0(\left\langle y^2, x^2 + y^2 - 3y\right\rangle, A) = 4\\
e_0(\langle f,h\rangle, A) &= e_0(\left\langle x^3 + xy^2 - y^2 - 3xy, x^3 + y^3 - 3xy\right\rangle, A)\\
&= e_0(\left\langle y^2, x^3 + y^3 - 3xy\right\rangle, A) = 6\\
e_0(\langle g,h\rangle, A) &= e_0(\left\langle x^2 + y^2 - 3y, x^3 + y^3 - 3xy\right\rangle, A)\\
&= e_0(\left\langle x^2 + y^2 - 3y, x^3 - xy^2\right\rangle, A)\\
&= e_0(\left\langle x^2 + y^2 - 3y, y^2\right\rangle, A) + e_0(\left\langle x^2 + y^2 - 3y, y - x\right\rangle, A)\\
&= 4 + 1 = 5
\end{aligned}
$$

Priamka $y = 0$ je jedinou spoločnou dotyčnicou všetkých troch kriviek v bode O, pretože $f^* = -y^2 - 3xy = -y(y - 3x)$, $g^* = -3y$, $h^* = -3xy$ a ich najväčší spoločný deliteľ je y. Pre násobnosť j z Bèzoutovej vety s využitím tvrdenia Bydžovského vety platí

$$j(\mathcal{U} \cap \mathcal{V}, O) = 4 = 2.1 + 1 + 1$$
$$j(\mathcal{U} \cap \mathcal{W}, O) = 6 = 2.2 + 1 + 1$$
$$j(\mathcal{V} \cap \mathcal{W}, O) = 5 = 2.1 + 1 + 2$$

Skúmajme opäť súčet $h + \varrho$. Ako v predchádzajúcom príklade na zistenie styku rádu n kriviek $\mathcal{U}$ a $\mathcal{V}$, $\mathcal{U}$ a $\mathcal{W}$ a $\mathcal{V}$ a $\mathcal{W}$ potrebujeme parametrické vyjadrenia daných kriviek. Nech parametrické rovnice krivky $\mathcal{U}$ je $P_1(t_1) = \left(\frac{t_1(t_1+3)}{t_1^2+1}, \frac{t_1^2(t_1+3)}{t_1^2+1}\right)$, kde $t_1 \in \mathbb{R}$, krivky $\mathcal{V}$ je $P_2(t_2) = \left(\frac{3}{2}\cos t_2, \frac{3}{2}(\sin t_2 + 1)\right)$, kde $t_2 \in \langle 0; 2\pi \rangle$ a krivky $\mathcal{W}$ je $P_3(t_3) = \left(\frac{3t_3}{t_3^3+1}, \frac{3t_3^2}{t_3^3+1}\right)$, kde $t_3 \in \mathbb{R} \setminus \{-1\}$.



Obrázok 6: Krivky $\mathcal{U}$ a $\mathcal{V}$

Ukážeme, že styk kriviek $\mathcal{U}$, $\mathcal{V}$ v bode O je 2. Teda sústava dvoch vektorových rovníc (1), (2) s neznámymi reálnymi číslami β_1 a β_2 má riešenie, ale (1), (2), (3) už nie. Bod O na krivke $P_1(t_1)$ prislúcha parametru $t_1 = 0$, na krivke $P_2(t_2)$ parametru $t_2 = \frac{3}{2}\pi$. Najprv určíme hodnoty derivácií:

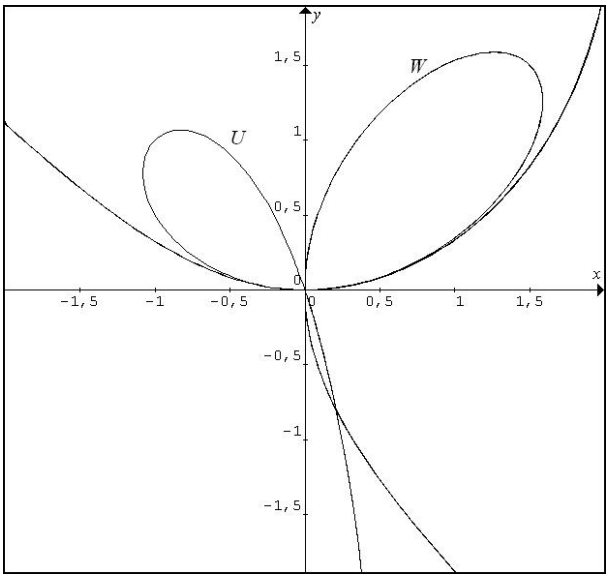
$$P_1'(t_1) = \left(-\frac{3t_1^2-2t_1-3}{(t_1^2+1)^2}, \frac{t_1(t_1^3+3t_1+6)}{(t_1^2+1)^2}\right) \qquad P_1'(0) = (3,0)$$
$$P_1''(t_1) = \left(\frac{2(3t_1^3-3t_1^2-9t_1+1)}{(t_1^2+1)^3}, -\frac{2(t_1^3+9t_1^2-3t_1-3)}{(t_1^2+1)^3}\right) \qquad P_1''(0) = (2,6)$$
$$P_1'''(t_1) = \left(-\frac{6(3t_1^4-4t_1^3-18t_1^2+4t_1+3)}{(t_1^2+1)^4}, \frac{6(t_1^4+12t_1^3-6t_1^2-12t_1+1)}{(t_1^2+1)^4}\right) \qquad P_1'''(0) = (-18,6)$$
$$P_2'(t_2) = \left(-\frac{3\sin t_2}{2}, \frac{3\cos t_2}{2}\right) \qquad P_2'\left(\tfrac{3}{2}\pi\right) = \left(\tfrac{3}{2},0\right)$$
$$P_2''(t_2) = \left(-\frac{3\cos t_2}{2}, -\frac{3\sin t_2}{2}\right) \qquad P_2''\left(\tfrac{3}{2}\pi\right) = \left(0,\tfrac{3}{2}\right)$$
$$P_2'''(t_2) = \left(\frac{3\sin t_2}{2}, -\frac{3\cos t_2}{2}\right) \qquad P_2'''\left(\tfrac{3}{2}\pi\right) = \left(-\tfrac{3}{2},0\right)$$

Rovnica (1) nám dáva dve rovnice $3 = \beta_1\frac{3}{2}$ a $0 = \beta_1 0$ s riešením $\beta_1 = 2$. Po dosadení β_1 do (2) podobne získame $\beta_2 = \frac{4}{3}$. Ak do (3) dosadíme β_1 a β_2, tak dostaneme, že rovnica nemá riešenie, t.j. neexistuje také β_3. Krivky $\mathcal{U}$, $\mathcal{V}$ majú v bode O styk rádu práve $n = 2$. Platí teda rovnosť $n = h + \varrho$.

Podobne ako predtým vypočítame styk kriviek $\mathcal{U}$ a $\mathcal{W}$. Bod O na krivke $\mathcal{W}$ s parametrickou rovnicou $P_3(t_3)$ prislúcha parametru $t_3 = 0$. Vypočítajme derivácie:

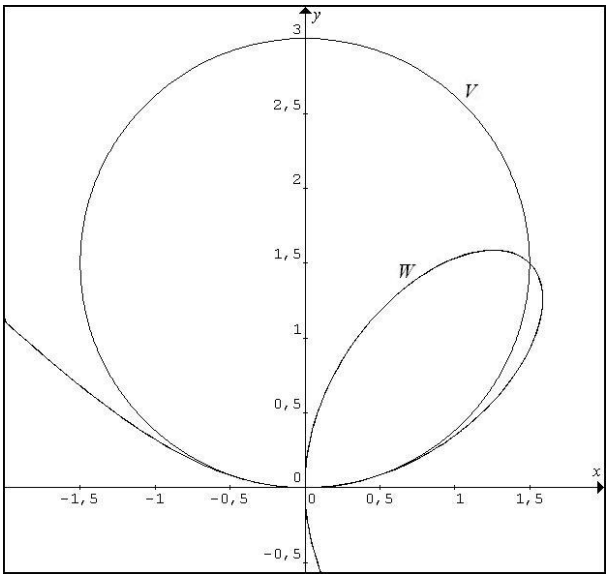
$$P_3'(t_3) = \left(\frac{3(1-2t_3^3)}{(t_3^3+1)^2}, \frac{3t_3(2-t_3^3)}{(t_3^3+1)^2}\right) \qquad P_3'(0) = (3,0)$$
$$P_3''(t_3) = \left(\frac{18t_3^2(t_3^3-2)}{(t_3^3+1)^3}, \frac{6(t_3^6-7t_3^3+1)}{(t_3^3+1)^3}\right) \qquad P_3''(0) = (0,6)$$
$$P_3'''(t_3) = \left(-\frac{18t_3(4t_3^6-19t_3^3+4)}{(t_3^3+1)^4}, -\frac{18(t_3^2(t_3^6-16t_3^3+10)}{(t_3^3+1)^4}\right) \qquad P_3'''(0) = (0,0)$$

Po vyriešení rovníc (1), (2) dostaneme $\beta_1 = 1,\ \beta_2 = -\frac{2}{3}$. Rovnica (3) nie je riešiteľna, teda krivky $\mathcal{U}$ a $\mathcal{W}$ majú styk rádu práve $n = 2$. Porovnaním so súčtom $h + \varrho$ opäť platí rovnosť.



Obrázok 7: Krivky $\mathcal{U}$ a $\mathcal{W}$

Nakoniec styk kriviek $\mathcal{V}$ a $\mathcal{W}$. Podobnými výpočtami získame hodnoty $\beta_1 = 2$, $\beta_2 = 0$, $\beta_3 = 8$. Sústava rovníc (1), (2), (3) je riešiteľná. Teda styk kriviek $\mathcal{V}$ a $\mathcal{W}$ je aspoň 3. Súčet $h + \varrho = 3$, teda aby rovnosť medzi n a $h + \varrho$ bola platná, rovnica (4) už nemôže mať riešenie.



Obrázok 8: Krivky $\mathcal{V}$ a $\mathcal{W}$

Potrebujeme k tomu derivácie štvrtého rádu daných kriviek:

$$P_2^{(iv)}(t_2) = \left(\tfrac{3\cos t_2}{2}, \tfrac{3\sin t_2}{2}\right) \qquad P_2^{(iv)}\left(\tfrac{3}{2}\pi\right) = \left(0, -\tfrac{3}{2}\right)$$
$$P_3^{(iv)}(t_3) = \left(\tfrac{72(5t_3^9-45t_3^6+30t_3^3-1)}{(t_3^3+1)^5}, \tfrac{72t_3(t_3^9-30t_3^6+45t_3^3-5)}{(t_3^3+1)^5}\right) \qquad P_3^{(iv)}(0) = (-72, 0)$$

Dostaneme dve rovnice s neznámou β_4. Z prvej rovnice $\beta_4 = -48$ a z druhej rovnice $0 = 72$ čo je spor. Krivky $\mathcal{V}$ a $\mathcal{W}$ teda v bode O majú práve styk rádu $n = 3$. Teda naozaj platí rovnosť $n = h + \varrho$.

Zdá sa že číslo ϱ vyjadruje kvalitu styku dvoch kriviek. Zatiaľ sa nepodarilo ani dokázať ani vyvrátiť nasledujúcu hypotézu.

Hypotéza 2.3.1 *Nech sú dané dve krivky $\mathcal{C}$ a $\mathcal{D}$ v afinnej rovine nad poľom k. Ak bod $O = (0, 0)$ je spoločným bodom kriviek $\mathcal{C}$, $\mathcal{D}$ v ktorom majú práve jednu spoločnú dotyčnicu, potom $n = 1 + \varrho$, kde n je styk rádu n kriviek v bode O a ϱ je korekcia z vety 2.3.2.*

Na záver uvedieme motivujúce príklady na vyslovenú hypotézu. Zistenie platnosti hypotézy ponechávame čitateľovi.

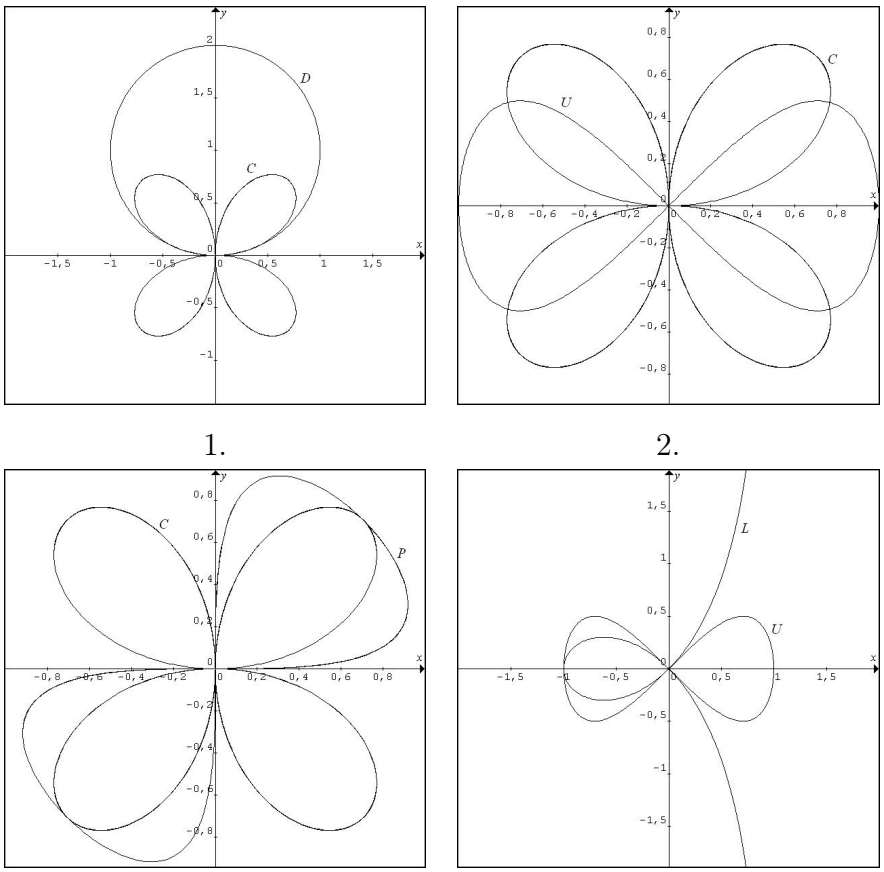
Príklad 2.3.4 Zistite násobnosť bodu $O = (0, 0)$ v prieseku nasledujúcich kriviek:

1. $\mathcal{C}: \ f = (x^2 + y^2)^3 - 4x^2y^2$ (štvorcipá ruža) a $\mathcal{D}: \ g = x^2 + y^2 - ay$ (kružnica), pre hodnotu parametra $a = \pm 2$ a $a \in \mathbb{R} \setminus \{0, +2, -2\}$,

2. $\mathcal{U}: \ f = x^2(1 - x^2) - y^2$ (lemniskáta) a $\mathcal{C}: \ g = (x^2 + y^2)^3 - 4x^2y^2$,

3.* $\mathcal{P}: \ f = x^4 + y^4 + 4xy\left((x + y)^2 - \frac{1}{2}xy - 2\right)$ a $\mathcal{C}: \ g = (x^2 + y^2)^3 - 4x^2y^2$,

4.* $\mathcal{U}: \ f = x^2(1 - x^2) - y^2$ a $\mathcal{L}: \ g = (1 - x)y^2 - (1 + x)x^2$ (strofoida).



1. 2.

3.* 4.*

Obrázok 9: K príkladu 2.3.4

Náročnosť hľadania prametrického vyjadrenia krivky však nie je jediným problémom, ktorý stojí v ceste dokazovania našej hypotézy. Odstránenie prekážok a hľadanie iných efektívnejších metód na vysvetlenie geometrického významu čísla ϱ je už predmetom ďalšieho skúmania.

Záver

Lokálna prieseková násobnosť (Samuelova) je významným teoretickým aparátom modernej komutatívnej algebry. Aplikáciou jej výsledkov sa dosiahlo vyriešenie niektorých problémov súčasnej algebraickej geometrie (teória prieseku a i.). Metódy výpočtu tejto násobnosti majú kľúčový význam pre rozvoj teórie. V práci sú uvedené klasické i moderné metódy (Gröbnerova, štandardná báza) výpočtu priesekovej násobnosti.

Násobnosť izolovaného bodu v prieniku dvoch rovinných algebraických kriviek súvisí s jeho násobnosťou na jednotlivých krivkách a s dotykovou situáciou v ňom. V prípade, že krivky v spoločnom bode nemajú spoločnú dotyčnicu, potom jeho násobnosť sa rovná súčinu násobnosti na jednotlivých krivkách. V prípade existencie h dotyčníc je táto násobnosť vyššia o číslo h a ďalšiu korekciu ϱ, závisiacu od styku n-tého rádu kriviek v tomto bode. Exaktné vyjadrenie tohto čísla ϱ a algebraizácia styku dvoch kriviek je však predmetom ďalšieho skúmania.

Dobrá znalosť teórie komutatívnej algebry a diferenciálnej geometrie je základným predpokladom správnej interpretácie a pochopeniu našej práce.

Referencie

[1] ATIYAH, M. F., MACDONALD, I. G.: *Introduction to Commutative Algebra.* Addison-Wesley, Reading, Massachusetts, 1969.

[2] BARTSCH, H. J.: *Matematické vzorce.* 4. vyd. 2006. ISBN 80-200-1448-9

[3] BECKER, T., WEISPFENNING, V.: *Gröbner Bases : A Computational Approach to Commutative Algebra.* 2. vyd. 1998. ISBN 0-387-97971-9

[4] BOĎA, E., FARNBAUER, R.: *On Standard Basis and Multiplicity of* $(X^a - Y^b, X^c - Y^d)$. Acta Math. Univ. Comenianae. Vol. LXXII, 1 (2003), pp. 15–22

[5] BOĎA, E., ORSZÁGHOVÁ, D.: *On the Multiplicity of* $(X^a - Y^b, X^c - Y^d)$. Acta Math. Univ. Comenianae. Vol. LXVII, 2 (1998), pp. 273–276

[6] BUREŠ, J., VANŽURA, J.: *Algebraická geometrie.* Praha : STNL, 1989.

[7] BYDŽOVSKÝ, B.: *Úvod do algebraické geometrie.* Praha : JČMF, 1948.

[8] COX, D., LITTLE, J., O'SHEA, D.: *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra.* 3. vyd. 2007. ISBN 978-0-387-35650-1

[9] HASSETT, B.: *Introduction to Algebraic Geometry.* 1. vyd. 2007. ISBN-13: 978-0-521-87094-8

[10] KATRIŇÁK, T. a i.: *Algebra a teoretická aritmetika 1.* 4. vyd. 2002. ISBN 80-223-1674-1

[11] KUNZ, E.: *Introduction to Plane Algebraic Curves.* 1. vyd. 2005. ISBN 978-0-8176-4381-2

[12] NORTHCOTT, D. G.: *Lesson on Rings, Modules and Multiplicities.* Cambridge Univ. Press 1968.

[13] PERRIN, D.: *Algebraic Geometry : An Introduction.* Prel. Catriona Maclean. 1. vyd. 2008. Prekl. z franc. orig. Géométrie algebrique by Daniel Perrin. ISBN 978-84800-055-1

[14] PRITCHARD, F. L.: *On the multiplicity of zeros of polynomials over arbitrary finite dimensional k-algebras.* Manusc. Math. 49(3), 1985, s. 267–292

[15] SOLČAN, Š.: *Projektívna geometria.* 1. vyd. 1993. ISBN 80-223-0887-0

[16] ŠALÁT, T. a i.: *Teória množín.* 2. vyd. 1995. ISBN 80-223-0974-5

[17] ZARISKI, O., SAMUEL, P.: *Commutative algebra I.* Van Nostrand Company, Princeton 1958.

[18] ZARISKI, O., SAMUEL, P.: *Commutative algebra II.* Van Nostrand Company, Princeton 1960.