

4. BÉZOUTOVA VETA

4.1. Tvrdenie vety.

Príklad 4.1. 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 4.2. 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 4.3. 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 4.4. *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.

4.2. Rezultanty.

Lema 4.5. *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. Faktorizujeme 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 $\deg p < \deg g$, niektorý z deliteľov polynómu g musí byť deliteľom polynómu f . $\square$

Definícia 4.6. 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

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

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

Dôkaz. Podľa Lemy 4.5 majú f, g netriviálneho spoločného deliteľa práve vtedy, keď existujú polynómy

$$\begin{aligned} p &= p_{n-1}t^{n-1} + \cdots + p_1t + p_0, \\ q &= q_{n-1}t^{n-1} + \cdots + q_1t + q_0 \end{aligned}$$

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

$$\begin{aligned} f_0p_0 + g_0q_0 &= 0 \\ f_1p_0 + f_0p_1 + g_1q_0 + g_0q_1 &= 0 \\ &\vdots \\ f_mp_{n-1} + g_mq_{n-1} &= 0. \end{aligned}$$

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

Príklad 4.9. 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 $\text{Res}(f, f') = 0$.

4.3. 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 rezultantoch.

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 4.10. *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 Sylvestrovej matice vynásobíme λ , tretí $\lambda^2, \dots, n$ -tý λ^n , $(n+2)$ -hý vynásobíme $\lambda, \dots$, 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 3.7 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 $q_2 z_1 - q_1 z_2 = 0$).

Túto konštrukciu využijeme pri dôkaze nasledovnej vety.

Veta 4.11. *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 4.7), 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 4.12. 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 4.13. (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 4.14. 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 4.15. Nájďme 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.

KAG FMFI UK BRATISLAVA

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