

7. VYUŽITIE REZULTANTOV PRI RIEŠENÍ SÚSTAV POLYNOMICKÝCH ROVNÍC

Príklad 7.1. Pomocou resultantov nájdeme spoločné body dvoch rovinných kriviek: hyperboly popísanej polynómom $f = xy - 1$ a kružnice popísanej $g = x^2 + y^2 - 4$. Hľadáme teda riešenia sústavy dvoch rovníc o dvoch neznámych.

Kľúčovým je nasledovné preformulovanie problému: ak f a g chápeme ako polynómy jednej premennej x nad $k[y]$, kedy majú tieto dva polynómy spoločný koreň? Podľa Vety 4.7 je to práve vtedy, keď $\text{Res}_x(f, g) = 0$. Polynóm f je lineárny v x , polynóm g zas kvadratický. Máme

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

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

Príklad 7.2. Nájdime prienik kriviek $V(f), V(g) \subset \mathbb{A}^2(\mathbb{C})$, kde

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

Rezultant polynómov f, g vzhľadom na premennú x je

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

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

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

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

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

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

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

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

Oba priestory, $P_{n-1} \oplus P_{m-1}$ aj P_{m+n-1} sú vektorovými priestormi dimenzie $m+n$ a pre zobrazenie δ platí

- $\delta(c \cdot (p, q)) = c \cdot \delta((p, q)) \quad \forall c \in k, \quad \forall (p, q) \in P_{n-1} \oplus P_{m-1},$
- $\delta((p_1, q_1) + (p_2, q_2)) = \delta((p_1, q_1)) + \delta((p_2, q_2)) \quad \forall (p_1, q_1), (p_2, q_2) \in P_{n-1} \oplus P_{m-1},$

čiže δ je lineárnym zobrazením. Preto po zvolení báz v oboch priestoroch sa dá takéto zobrazenie popísať štvorcovou maticou stupňa $m+n$.

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

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

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

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

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

Veta 7.3. *Nech $f, g \in k[x_1, \dots, x_n]$. Potom existujú polynómy $p, q \in k[x_1, \dots, x_n]$ také, že*

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

Dôkaz. Z definície rezultantu je zrejmé, že $\text{Res}_{x_1}(f, g)$ je polynóm, presnejšie $\text{Res}_{x_1}(f, g) \in k[x_2, \dots, x_n]$. Cramerovým pravidlom ukážeme, že $\text{Res}_{x_1}(f, g)$ sa dá napísať ako kombinácia f a g .

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

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

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

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

Aplikovaním tohto pravidla na Sylvestrovu maticu dostávame

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

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

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

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

Dôsledok 7.4. *Ak $(a_1, a_2, \dots, a_n)$ je spoločným koreňom f a g , potom jeho priemet*

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

je koreňom $\text{Res}_{x_1}(f, g)$.

Používať rezultanty pri hľadaní spoločných bodov dvoch kriviek je teda korektný postup: v Príklade 7.1 polynóm $\text{Res}_x(f, g)$ popisuje varietu, ktorá určite obsahuje všetky body priemetu prieniku $V(f)$ a $V(g)$ na y -os. Potom x -súradnicu môžeme dopočítať buď dosadením konkrétnej y -súradnice do f a g , alebo ešte nájdeme rezultant

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

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

Príklad 7.2 zas ukazuje, že priemet množiny spoločných koreňov f a g na posledných $n - 1$ súradníc naozaj môže byť vlastnou podmnožinou $V(\text{Res}_{x_1}(f, g))$.

Príklad 7.5. Nájdime všetky racionálne body (t.j. body, ktorých súradnice sú racionálne čísla) ležiace na krivkách $V(f)$ a $V(g)$, ak

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

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

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

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

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

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

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

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

Síce je rezultant definovaný len pre dva polynómy, možno ho použiť aj na hľadanie spoločných koreňov viacerých polynomických rovníc. Napríklad, ak chceme nájsť spoločné korene polynómov $f, g, h \in k[x, y, z]$, môžeme konštruovať priemety postupne: $V(\text{Res}_z(f, g)) \subset \mathbb{A}^2$ obsahuje priemety koreňov $f = 0, g = 0$ do xy -roviny, podobne $V(\text{Res}_z(f, h)) \subset \mathbb{A}^2$ obsahuje priemety koreňov $f = 0, h = 0$, takže $V(\text{Res}_z(f, g), \text{Res}_z(f, h))$ obsahuje priemety koreňov $f = 0, g = 0, h = 0$ do xy -roviny. Pomocou rezultantov nájdeme potenciálne priemety na x -os, podobne potenciálne priemety na y -os. Potom ešte analogickým postupom nájdeme potenciálne priemety na z -os. Ak dostaneme len konečne veľa možností pre hodnotu každej súradnice, jednoducho dosadíme všetky možnosti do pôvodných rovníc $f = g = h = 0$, a tak nájdeme všetky korene polynómov $f, g, h \in k[x, y, z]$.