

KAPITOLA 5

Rezultanty

1. Definícia a základná vlastnosť

LEMA 1.1. *Nech $f, g \in R[x]$, kde R je okruh s jednoznačným rozkladom. Potom f a g majú spoločného nekonštantného deliteľa práve vtedy, keď existujú $p, q \in R[x]$ také, že $pf + qg = 0$ a pre stupne p, q platí $\deg p < \deg g$, $\deg q < \deg f$.*

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

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

$$pf = -qg.$$

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

PRÍKLAD 1.2. Smerujeme k tomu, nájsť kritérium, kedy majú dva polynómy v $k[x]$ (alebo všeobecnejšie v $R[x]$, kde R je okruh s jednoznačným rozkladom) spoločný koreň. Najjednoduchší príklad dostaneme, keď si zoberieme dva lineárne polynómy:

$$f = f_1x + f_0, \quad g = g_1x + g_0, \quad \text{kde } f_1, g_1 \neq 0.$$

Lineárny polynóm má iba jeden koreň, a polynómy f a g budú mať tento koreň spoločný práve vtedy, keď f je konštantným násobkom polynómu g , čiže vtedy, keď

$$\det \begin{pmatrix} f_1 & f_0 \\ g_1 & g_0 \end{pmatrix} = 0.$$

DEFINÍCIA 1.3. Nech $f, g \in R[x]$ sú polynómy stupňov m a n nad okruhom s jednoznačným rozkladom:

$$\begin{aligned} f &= f_mx^m + \dots + f_1x + f_0, & f_m &\neq 0, \\ g &= g_nx^n + \dots + g_1x + g_0, & g_n &\neq 0. \end{aligned}$$

Štvorcová matica

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

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 1.4. Niekedy budeme označovať resultant polynómov f a g aj $\text{Res}_x(f, g)$, a to v prípade, keď budeme chcieť zdôrazniť, že f, g sú polynómy v premennej x .

VETA 1.5. *Polynómy $f, g \in R[x]$ majú netriviálneho spoločného deliteľa práve vtedy, keď $\text{Res}(f, g) = 0$.*

POZNÁMKA 1.6. Všimnite si, že Príklad 1.2 je vlastne dôkazom Vety 1.5 pre prípad $m = n = 1$.

Dôkaz Vety 1.5. Podľa Lemy 1.1 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 $\text{Res}(f, g) = 0$. $\square$

POZNÁMKA 1.7. Sylvestrovu maticu polynómov f a g môžeme chápať aj ako maticu zobrazenia lineárnych priestorov (v prípade, že $R = k$ je pole) či všeobecnejšie tzv. *modulov* (ak R je okruh). Ide o alternatívnu formuláciu dôkazu Vety 1.5, ktorá bude užitočná pre neskoršie úvahy.

Pre prehľadnosť uvažujme situáciu, keď $R = k$ je pole. Analogicky celá úvaha vyzerá aj v prípade, keď ide o moduly nad okruhom R .

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

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

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

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

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

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

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

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

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

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

Zobrazenie δ má nenulové jadro práve vtedy, keď existujú nenulové polynómy $p \in P_{n-1}$ a $q \in P_{m-1}$ také, že $pf + qg = 0$, čo je podľa Lemy 1.1 ekvivalentné tvrdeniu, že f a g sú súdeliteľné, a na druhej strane je to ekvivalentné faktu, že matica zobrazenia δ , teda Sylvestrova matica, je singulárna.

DÔSLEDOK. *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 $\text{Res}(f, g) = 0$.*

Dôkaz. Nech α je spoločný koreň polynómov f a g , $\alpha \in \bar{k}$. Čiže $k[\alpha]$ je okruh obsahujúci koreň a tiež obsahuje pole k . Definujme si zobrazenie

$$\varphi: k[x] \rightarrow k[\alpha], \quad x \mapsto \alpha,$$

čiže φ je dosadzovanie α za x . Takto definované zobrazenie φ je homomorfizmus okruhov, jeho jadrom je preto ideál okruhu $k[x]$. Navyše $k[x]$ je okruh hlavných ideálov, takže existuje $h \in k[x]$, že $\ker \varphi = (h)$. Pre polynómy f, g máme

$$\varphi(f) = f(\alpha) = 0, \quad \text{a tiež} \quad \varphi(g) = g(\alpha) = 0,$$

takže $f, g \in \ker \varphi$. Odtiaľ máme, že $h \mid f$ a $h \mid g$. Navyše, h je určite nekonštantný polynóm: ak by $h \in k$ (h je zrejme nenulové, lebo jadro φ je netriviálne), potom máme, že $1 = hh^{-1} \in (h)$ a teda $(h) = k[x]$, čo však nie je pravda, lebo napríklad $\varphi(1) = 1$ a teda $1 \notin \ker \varphi$. Našli sme tak nekonštantný spoločný deliteľ polynómov f a g , a teda $\text{Res}(f, g) = 0$.

Nech teraz $\text{Res}(f, g) = 0$, čiže podľa Vety 1.5 existuje spoločný deliteľ $h \in k[x]$ polynómov f, g , $\deg h \geq 1$. Môžeme predpokladať, že h je ireducibilný. Potom $k[x]/(h)$ je pole: nech $[a]$ označuje triedu $\varphi(a)$, kde φ je projekcia $k[x] \rightarrow k[x]/(h)$. Pre ľubovoľné nenulové $[a] \in k[x]/(h)$ potrebujeme nájsť k nemu inverzný prvok. Ak $a \in (h)$, potom $[a] = 0$. V opačnom prípade sú polynómy a a h nesúdeliteľné, a teda existujú $u, v \in k[x]$ také, že $ua + vh = 1$. Máme tak

$$[u][a] = \varphi(u)\varphi(a) = \varphi(ua) = \varphi(1 - vh) = \varphi(1) - \varphi(v)\varphi(h) = 1,$$

takže $[u]$ je inverzný ku $[a]$, čiže $k[x]/(h)$ je pole. Jadrom zobrazenia $\varphi: k[x] \rightarrow k[x]/(h)$ je ideál (h) . Keďže h je deliteľom f aj g , tieto dva polynómy patria do jadra. Na druhej strane máme, že

$$\varphi(f) = f_m \varphi(x)^m + \cdots + f_1 \varphi(x) + f_0,$$

takže $\varphi(x) \in k[x]/(h)$ je koreňom polynómu f . Analogicky ukážeme, že $\varphi(x)$ je koreňom g . Našli sme spoločný koreň polynómov f a g v rozšírení $k[x]/(h)$. $\square$

2. Diskriminant polynómu

TVRDENIE 2.1. *Polynóm $f \in k[x]$ má v $\bar{k}$ viacnásobný koreň práve vtedy, keď $\text{Res}(f, f') = 0$.*

Dôkaz. Nech $\alpha \in \bar{k}$ je aspoň dvojnásobný koreň, teda platí, že

$$f = (x - \alpha)^2 f_1, \quad \text{kde } f_1 \in \bar{k}[x].$$

Pre deriváciu f potom platí

$$f' = 2(x - \alpha)f_1 + (x - \alpha)^2 f_1' = (x - \alpha)(2f_1 + (x - \alpha)f_1'),$$

teda α je koreňom polynómu f' .

Naopak teraz predpokladajme, že $\alpha \in \bar{k}$ je spoločným koreňom polynómu f aj jeho derivácie f' . Z $f = (x - \alpha)f_2$ dostávame

$$f' = (x - \alpha)f_2' + f_2, \quad \text{čiže} \quad f_2 = f' - (x - \alpha)f_2'.$$

Keďže sme predpokladali, že $(x - \alpha) \mid f'$, platí, že $(x - \alpha) \mid f_2$, a teda $f_2 = (x - \alpha)f_3$ pre nejaký polynóm f_3 . Takže sme dostali

$$f = (x - \alpha)f_2 = (x - \alpha)^2 f_3,$$

a α je dvojnásobný koreň polynómu f . □

PRÍKLAD 2.2. Nech $f = ax^2 + bx + c$, $a \neq 0$. Zistíme, kedy má tento polynóm dvojnásobný koreň.

Derivácia $f' = 2ax + b$, takže rezultant $\text{Res}(f, f')$ je

$$\text{Res}(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a(4ac - b^2).$$

Platí, že f má dvojnásobný koreň práve vtedy, keď $\text{Res}(f, f') = a(4ac - b^2) = 0$.

Tento príklad nás motivuje k definícii

DEFINÍCIA 2.3. Nech $f \in k[x]$, $f = f_n x^n + \dots + f_1 x + f_0$, $f_n \neq 0$. *Diskriminant* polynómu f je

$$\text{Discr}(f) = \frac{(-1)^{\frac{n(n-1)}{2}}}{f_n} \text{Res}(f, f').$$

Nasledovné tvrdenie je len reformuláciou už dokázaného.

TVRDENIE 2.4. *Polynóm $f \in k[x]$ má viacnásobný koreň nad nejakým rozšírením k práve vtedy, keď $\text{Discr}(f) = 0$.*

3. Rezultant ako funkcia koreňov polynómov

PRÍKLAD 3.1. Nech $f, g \in k[x]$ sú polynómy s faktorizáciou nad vhodným rozšírením poľa k :

$$\begin{aligned} f &= f_1(x - \alpha) = f_1 x - f_1 \alpha, \\ g &= g_2(x - \beta_1)(x - \beta_2) = g_2 x^2 + g_2(-\beta_1 - \beta_2)x + g_2 \beta_1 \beta_2, \end{aligned}$$

teda α je koreňom polynómu f a β_1, β_2 sú korene polynómu g . Ich rezultant potom je

$$\text{Res}(f, g) = \begin{vmatrix} f_1 & -f_1 \alpha & 0 \\ 0 & f_1 & -f_1 \alpha \\ g_2 & g_2(-\beta_1 - \beta_2) & g_2 \beta_1 \beta_2 \end{vmatrix} = f_1^2 g_2 \begin{vmatrix} 1 & -\alpha & 0 \\ 0 & 1 & -\alpha \\ 1 & -\beta_1 - \beta_2 & \beta_1 \beta_2 \end{vmatrix} = f_1^2 g_2 (\alpha - \beta_1)(\alpha - \beta_2).$$

Toto pozorovanie teraz zovšeobecníme:

VETA 3.2. *Nech $f, g \in k[x]$ sú polynómy stupňov m a n . Nech*

$$\begin{aligned} f &= f_m(x - \alpha_1) \dots (x - \alpha_m), \\ g &= g_n(x - \beta_1) \dots (x - \beta_n) \end{aligned}$$

sú úplné faktorizácie nad rozšírením k . Potom

$$\text{Res}(f, g) = f_m^n g_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j).$$

Dôkaz. Označme si

$$\Theta(f, g) = f_m^n g_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j),$$

chceme ukázať, že $\text{Res}(f, g) = \Theta(f, g)$.

Ak f a g majú spoločný koreň, potom je tvrdenie pravdivé, na základe Vety 1.5. Predpokladajme teda, že f a g nemajú spoločný koreň a tiež bez ujmy na všeobecnosti predpokladajme, že $\deg f \geq \deg g$. Vetu ukážeme indukciou vzhľadom na dĺžku postupnosti nenulových zvyškov v euklidovom algoritme hľadania najväčšieho spoločného deliteľa f, g .

Nech zvyšok po delení polynómu f polynómom g je 0. Z toho vyplýva, že $\deg g = 0$, keďže podľa predpokladu sú polynómy f a g nesúdeliteľné. Polynóm g pozostáva len z absolútneho člena g_0 , matica $\text{Syl}(f, g) = g_0 \mathbf{I}_m$, a platí

$$\text{Res}(f, g) = g_0^m = g_0^m f_n^0 = \Theta(f, g).$$

(Indukčný krok.) Nech teraz

$$f = qg + r, \quad \text{kde} \quad r \neq 0, \deg r = d < \deg g, \quad r = r_d x^d + \dots + r_0.$$

Postupovať budeme tak, že nájdeme predpis pre výpočet $\text{Res}(f, g)$ pomocou $\text{Res}(g, r)$, podobne predpis pre výpočet $\Theta(f, g)$ pomocou $\Theta(g, r)$, a uvidíme, že oba vyzerajú rovnako.

Zo vzťahu $r = f - qg = f - (\sum_{i=0}^{m-n} q_i x^i)g$ dostávame, že $\text{Res}(f, g)$ je determinant

$$\begin{vmatrix} f_m & f_{m-1} & \dots & f_0 & 0 & \dots & 0 \\ 0 & f_m & \dots & f_1 & f_0 & & 0 \\ & & \ddots & & & \ddots & \\ 0 & \dots & 0 & f_m & \dots & f_1 & f_0 \\ g_n & g_{n-1} & \dots & g_0 & 0 & \dots & 0 \\ 0 & g_n & \dots & g_1 & g_0 & & 0 \\ & & \ddots & & & \ddots & \\ 0 & \dots & 0 & g_n & \dots & g_1 & g_0 \end{vmatrix} = \begin{vmatrix} 0 & \dots & 0 & r_d & \dots & r_0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & r_d & \dots & r_0 & & 0 \\ & & & & & \ddots & & \ddots & \\ 0 & \dots & 0 & 0 & \dots & 0 & r_d & \dots & r_0 \\ g_n & g_{n-1} & & \dots & & g_0 & 0 & \dots & 0 \\ 0 & g_n & & \dots & & g_1 & g_0 & & 0 \\ & & \ddots & & & & & \ddots & \\ 0 & \dots & 0 & g_n & & \dots & & g_1 & g_0 \end{vmatrix}.$$

Rovnosť platí, lebo maticu sme modifikovali tak, že k riadkom s koeficientami polynómu f sme pripočítali násobky riadkov s koeficientami g , čo je operácia nemeniaca hodnotu determinantu. Ďalej v tejto matici poprehadzujeme riadky (operácia mení znamienko

determinantu) a dostávame, že predchádzajúci determinant je rovný

$$(-1)^{nm} \begin{vmatrix} g_n & g_{n-1} & \dots & g_0 & 0 & \dots & 0 \\ 0 & g_n & \dots & g_1 & g_0 & \dots & 0 \\ & & \ddots & & & \ddots & \\ 0 & \dots & 0 & g_n & \dots & g_1 & g_0 \\ 0 & \dots & 0 & r_d & \dots & r_0 & 0 \\ & & & 0 & r_d & \dots & r_0 \\ & & & & \ddots & \ddots & \\ 0 & \dots & 0 & 0 & \dots & 0 & r_d & \dots & r_0 \end{vmatrix} = (-1)^{nm} g_n^{m-d} \text{Res}(g, r),$$

kde poslednú rovnosť sme získali niekoľkonásobným rozvojom determinantu podľa prvého stĺpca. Máme teda vzťah

$$\text{Res}(f, g) = (-1)^{nm} g_n^{m-d} \text{Res}(g, r).$$

Pre nájdenie analogického predpisu pre $\Theta(f, g)$ si najprv všimnime, že z $f = qg + r$ vyplýva, že $f(\beta_i) = r(\beta_i)$ pre všetky korene β_i polynómu g . Počítajme:

$$\begin{aligned} \Theta(f, g) &= f_m^n g_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j) = (-1)^{mn} f_m^n g_n^m \prod_{i=1}^m \prod_{j=1}^n (\beta_j - \alpha_i) \\ &= (-1)^{mn} g_n^m \prod_{j=1}^n (f_m \prod_{i=1}^m (\beta_j - \alpha_i)) = (-1)^{mn} g_n^m \prod_{j=1}^n f(\beta_j) = (-1)^{mn} g_n^m \prod_{j=1}^n r(\beta_j) \\ &= (-1)^{mn} g_n^m \prod_{j=1}^n (r_d \prod_{i=1}^d (\beta_j - \gamma_i)) = (-1)^{nm} g_n^{m-d} \Theta(g, r). \end{aligned}$$

Takže pre výpočet $\Theta(f, g)$ máme ten istý predpis ako pre výpočet $\text{Res}(f, g)$, a z indukčného predpokladu tak dostávame, že $\text{Res}(f, g) = \Theta(f, g)$. $\square$

4. Rezultanty a eliminácia

PRÍKLAD 4.1. 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 1.5 je to práve vtedy, keď $\text{Res}_x(f, g) = 0$. Polynóm f je lineárny v x , polynóm g zas kvadratický. Máme

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

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

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

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

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.

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

VEŤA 4.3. *Nech $f, g \in k[x_1, \dots, x_n]$. Potom*

$$\text{Res}_{x_1}(f, g) \in (f, g) \cap k[x_2, \dots, x_n].$$

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

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

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

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

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

Aplikovaním tohto pravidla na Sylvestrovu maticu dostávame

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

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

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

V Poznámke 1.7 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 $\text{Res}_{x_1}(f, g) = pf + qg$, a preto $\text{Res}_{x_1}(f, g) \in (f, g)$. $\square$

DÔSLEDOK.

$$(9) \quad V((f, g) \cap k[x_2, \dots, x_n]) \subseteq V(\text{Res}_{x_1}(f, g)),$$

kde na oboch stranách inklúzie sú variety priestoru $\mathbb{A}^{n-1}$.

Z Tvrdenia 6.6 v kapitole o Gröbnerových bázach pre premietanie

$$\pi: (a_1, a_2, \dots, a_n) \mapsto (a_2, \dots, a_n)$$

máme, že

$$\overline{\pi(V(f, g))} \subseteq V((f, g) \cap k[x_2, \dots, x_n]),$$

Spolu s (9) tak dostávame

$$\overline{\pi(V(f, g))} \subseteq V(\text{Res}_{x_1}(f, g)).$$

Používať rezultanty pri hľadaní spoločných bodov dvoch kriviek je teda korektný postup: v Príklade 4.1 polynóm $\text{Res}_x(f, g)$ popisuje varietu, ktorá určite obsahuje všetky body

priemetu prieniku $V(f)$ a $V(g)$ na y -os. Potom x -súradnicu môžeme dopočítať buď dosadením konkrétnej y -súradnice do f a g , alebo ešte nájdeme rezultant

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

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

Príklad 4.2 zas ukazuje, že $V((f, g) \cap k[x_2, \dots, x_n])$ naozaj môže byť vlastnou podmnožinou $V(\text{Res}_{x_1}(f, g))$, dokonca aj nad algebraicky uzavretým poľom, t.j. inklúzia v (9) sa nedá nahradiť rovnosťou. Pre porovnanie môžeme skúsiť nájsť Gröbnerovu bázu ideálu (f, g) , a zistíme, že obsahuje polynóm $y^3 - 4y + 1$.

PRÍKLAD 4.4. Nájdime všetky racionálne body (t.j. body, ktorých súradnice sú racionálne čísla) algebraickej variety $V(f, g)$, 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 variety $V(f, g)$ na y -os teda obsahuje najviac 2 racionálne body. Podobne nájdeme množinu obsahujúcu priemet $V(f, g)$ 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 . Varieta $V(f, g)$ teda obsahuje priamku $V(y + 1)$.

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 bodom $V(f, g)$ 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 body variety $V(f, g, h)$, kde $f, g, h \in k[x, y, z]$, môžeme konštruovať priemety postupne: $V(\text{Res}_z(f, g)) \subset \mathbb{A}^2$ obsahuje body priemetu variety $V(f, g)$ do xy -roviny, podobne $V(\text{Res}_z(f, h)) \subset \mathbb{A}^2$ obsahuje body priemetu $V(f, h)$, takže $V(\text{Res}_z(f, g), \text{Res}_z(f, h))$ obsahuje priemet $V(f, g, h)$ do xy -roviny. Pomocou rezultantov nájdeme varietu obsahujúcu priemet na x -os, podobne priemet na y -os. Potom ešte analogickým postupom nájdeme varietu obsahujúcu priemet 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 body variety $V(f, g, h)$.

5. Eliminácia pomocou rezultantov a Gröbnerových báz – zhrnutie

Na prvý pohľad sa metóda používajúca rezultanty môže javiť ako menej atraktívna. Teória spojená s nimi vyzerá omnoho komplikovanejšie, a navyše so slabšími tvrdeniami

– uzáver priemetu algebraickej variety je Gröbnerovými bázami popísaný presne, no pomocou rezultantov nájdeme len varietu obsahujúcu uzáver priemetu. Tiež sa môže zdať, že pomocou rezultantov nevieme dobre uchopiť algebraické variety, ktoré majú nekonečne veľa bodov: že sa nám poradilo vyriešiť Príklad 4.4, bolo tak trochu šťastie: išlo o špeciálnu varietu so špeciálnou polohou. Napriek tomu sa pri mnohých príležitostiach veľmi často používajú práve rezultanty. Dôvodov je na to niekoľko:

Postupy využívajúce rezultanty sú podstatne jednoduchšie než používanie Gröbnerových báz. Pomocou Gröbnerových báz síce jednoducho nájdeme priemet na jednu súradnicovú os, vyriešime príslušnú rovnicu, ale rozširovanie čiastočných riešení na úplné si vyžaduje dosť podrobnú analýzu jednotlivých eliminačných ideálov – ak by sme túto metódu chceli naprogramovať, program by bol pomerne komplikovaný.

Ďalej u rezultantov máme lepšiu kontrolu nad zložitou (časovou aj pamäťovou) výpočtu. Pre dané dva polynómy totiž vieme, ako sa konštruje rezultant, a tak vieme odhadnúť, s akými veľkými polynómami sa bude počas výpočtu manipulovať. Naproti tomu pri hľadaní Gröbnerovej bázy je ťažko povedať, ako veľké S-polynómy sa budú musieť vypočítať. Nie je zriedkavosťou, že priebežné S-polynómy sú podstatne komplikovanejšie než vstupné polynómy (tie, ktorými ideál definujeme) a výsledná Gröbnerova báza. Preto ak by sme sa chceli vyhnúť rozširovaniu čiastočných riešení (a teda komplikovanej analýze eliminačných ideálov) tak, že by sme hľadali Gröbnerovu bázu viackrát (t.j. hľadali by sme Gröbnerovými bázami priemety na ostatné súradnicové osi), z hľadiska výpočtovej zložitosti to rozhodne nie je dobrý nápad.

Ak hľadáme približné riešenia sústavy, pri použití rezultantov máme lepšiu kontrolu nad chybou: v každej súradnici nájdeme dostatočne presnú aproximáciu, a tak vieme aká je maximálna výsledná chyba. Ak by sme použili Gröbnerove bázy a jednu súradnicu vypočítame s chybou, táto chyba vo všeobecnosti výrazne narastá v každej ďalšej súradnici, keď riešenie rozširujeme.

Teória rezultantov je omnoho rozvinutejšia než sme si uviedli a tento nástroj je omnoho mocnejší než sa môže zdať na základe tejto prednášky. Mnohé tvrdenia, ktoré hovoria o rozširovaní čiastočných riešení nájdených cez Gröbnerove bázy, sú dokazované práve pomocou rezultantov.