APUNTS D'ÀLGEBRA COMPUTACIONAL (CAPÍTOL 3):

TEORIA DE L'ELIMINACIÓ

A. MONTES

Date: 27 d'abril de 2001.

1. El teorema de l'eliminació

Abans d'enunciar-ho, posem un exemple de com funciona.

Exemple 1.1. Sigui l'ideal $\mathcal{I} = \langle f_1, f_2, f_3 \rangle$, on

$$\begin{aligned} f_1 &= x^2 + y + z - 1 \\ f_2 &= x + y^2 + z - 1 \\ f_3 &= x + y + z^2 - 1 \end{aligned}$$

Denotem $\mathrm{gb}(\mathcal{I}, \mathrm{lex}(x,y,z))$ la base de Gröbner reduïda de l'ideal $\mathcal{I}$ respecte a l'ordre lex amb $x \succ y \succ z$. Aquesta és: $\mathrm{gb}(\mathcal{I}, \mathrm{lex}(x,y,z)) = \{g_4, g_3, g_2, g_1\}$, on:

$$\begin{aligned} g_4 &= z^6 - 4\,z^4 + 4\,z^3 - z^2 \\ g_3 &= 2y\,z^2 + z^4 - z^2 \\ g_2 &= y^2 - y - z^2 + z \\ g_1 &= x + y + z^2 - 1 \end{aligned}$$

Les dues són bases de $\mathcal{I}$, i per tant representen la mateixa varietat. És a dir, tenen les mateixes solucions. Però en la base de Gröbner resulta molt més fàcil d'identificar-les. g_4 només depén de z i factoritza:

$$g_4 = z^2\,(z-1)^2\,(z^2 + 2\,z - 1)$$

i per tant, els possibles únics valors de z són $\{0, 1, -1+\sqrt{2}, -1-\sqrt{2}\}$. A partir d'aquí, una senzilla substitució ens permet obtenir els valors possibles de les altres variables:

$$\left\{\begin{array}{lcll} z = 0 & \to & \left\{\begin{array}{lcl} y = 0 & \to & x = 1 \\ y = 1 & \to & x = 0 \end{array}\right. & \\ z = 1 & \to & y = 0 & \to\ x = 1 \\ z = -1+\sqrt{2} & \to & y = -1+\sqrt{2} & \to\ x = -1+\sqrt{2} \\ z = -1-\sqrt{2} & \to & y = -1-\sqrt{2} & \to\ x = -1-\sqrt{2} \end{array}\right.$$

Les solucions obtingudes a partir de la base de Gröbner lex poden ser vistes en dos passos.

- Pas d'eliminació: g_4 només depén de z, i g_4, g_3, g_2 només depenen de z, y.
- Pas d'extensió: Una vegada resolta $g_4 = 0$ les solucions parcials en z estenen primer a solucions parcials en y, z, i després a solucions en x, y, z.

La idea bàsica de la teoria de l'eliminació és que ambdos passos es poden fer amb gran generalitat.

Definició 1.2. Posem $\overline{x}_j = x_{j+1}, \ldots, x_n$. Donat $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subset K[\overline{x}]$ anomenem j-èsim ideal d'eliminació a

$$\mathcal{I}_j = \mathcal{I} \cap K[\overline{x}_j].$$

Així doncs, $\mathcal{I}_j$ consisteix en totes les conseqüències de $f_1, \ldots, f_s$ que eliminen les variables $x_1, \ldots, x_j$. És immediat provar que $\mathcal{I}_j$ és un ideal de $K[\overline{x}_j]$. Amb aquesta notació $\mathcal{I} = \mathcal{I}_0$ i $\overline{x} = \overline{x}_0$.

Observeu que diferents ordres de les variables donen lloc a diferents ideals d'eliminació.

El pas d'eliminació es redueix a trobar bases de $\mathcal{I}_j$. Les bases de Gröbner lex ens les porporcionen.

Teorema 1.3 (d'eliminació). *Sigui $\mathcal{I}$ un ideal de $K[\overline{x}]$ i sigui $G = \mathrm{gb}(\mathcal{I}, \mathrm{lex}(\overline{x}))$. Llavors, per cada j amb $0 \leq j < n$, el conjunt*

$$G_j = G \cap K[\overline{x}_j]$$

és una base de Gröbner de $\mathcal{I}_j$.

Demostració. Sigui $G = \{g_1, \ldots, g_s\} = \mathrm{gb}(\mathcal{I}, \mathrm{lex}(\overline{x}))$, i ordenem els polinomis g_i de tal forma que $G_j = G \cap K[\overline{x}_j] = \{g_{r_j}, \ldots, g_s\}$. Amb aquesta ordenació és $1 = r_1 \leq r_2 \leq \cdots \leq r_{n-1}$. Per provar que $\mathcal{I}_j = \langle G_j \rangle$, sigui $f \in \mathcal{I}_j$. Dividim f per G en l'ordre $\mathrm{lex}(\overline{x})$. Per ser G una base de Gröbner de $\mathcal{I}$ i $\mathcal{I}_j \subset \mathcal{I}$, el residu és zero: $\overline{f}^G = 0$. Tindrem

$$f = \sum_{i=1}^{s} q_i(\overline{x})\, g_i + 0$$

Però cada un dels polinomis g_i amb $i < r_j$ conté alguna variable de $\overline{x}$ que no està a $\overline{x}_j$. Tractant-se de l'orde lex, el seu monomi principal també contindrà alguna d'aquestes variables que són més grans que les de $\overline{x}_j$. Com f no conté cap d'aquestes variables, cap dels seus monomis serà divisible per cap $\mathrm{lm}(g_i)$ per $i < r_j$, i l'expressió de f a la divisió es redueix a

$$f = \sum_{i=r_j}^{s} q_i(\overline{x})\, g_i$$

el que implica que $f \in \langle G_j \rangle$ i per tant, G_j és una base de $\mathcal{I}_j$.

Ara és immediat demostrar que també és base de Gröbner. En efecte, els S-polinomis dels polinomis de G_j pertanyen a $\mathcal{I}_j$ i pel que acabem de veure, el residu de dividir-los per G_j és zero. Per tant, G_j és base de Gröbner. □

De vegades no ens cal eliminar totes les variables sino únicament un grup de variables. En aquest cas no cal emprar ordre lex i podem emprar ordres producte tals que tot monomi que contingui les variables a eliminar sigui més gran que els monomis que no les contenen. Això evitarà emprar ordre lex respecte a totes les variables i els càlculs poden ser menors.

Abans de discutir el pas d'extensió, aprofundim una mica en l'estructura de les bases de Gröbner lex, per certs d'ideals de varietat.

Lema 1.4 (Shape lema)**.** *Sigui K un cos infinit i $\mathcal{I} = \mathbb{I}(V)$ l'ideal de varietat de d'una varietat zero-dimensional $V = \{P_1, \dots, P_s\}$ de K^n, i tal que els punts que conté estan en posició general respecte a la darrera variable x_n. Això significa que posant $P_i = (a_{i1}, \dots, a_{in})$, la darrera coordenada és diferent per cada punt: si $i \neq k$, llavors $a_{in} \neq a_{kn}$. Llavors, la base de Gröbner de l'ideal de varietat en ordre lex, $G = \mathrm{gb}(\mathbb{I}(V), \mathrm{lex}(\overline{x}))$, és $G = \{g_1, \dots, g_n\}$, on*

$$\begin{array}{lcl} g_n & = & p_n(x_n) = \prod_{i=1}^{s}(x_n - a_{in}) \\ g_{n-1} & = & x_{n-1} - p_{n-1}(x_n) \\ & & \dots \\ g_1 & = & x_1 - p_1(x_n) \end{array}$$

i els p_i per $1 \leq i < n$ són els polinomis interpoladors dels nusos $[(a_{1n}, a_{1i}), \dots, (a_{sn}, a_{si})]$,

$$p_i(x_n) = \sum_{k=1}^{s} a_{ki} \frac{\displaystyle\prod_{j \neq k}^{s}(x_n - a_{jn})}{\displaystyle\prod_{j \neq k}^{s}(a_{kn} - a_{jn})}$$

Demostració. Obviament els polinomis considerats pertanyen a $\mathbb{I}(V)$, ja que aquests s'anul·len a tots els punts de V. Provem que $\mathcal{I}_{n-1} = \langle g_n \rangle$. En efecte, sigui $f \in \mathcal{I}_{n-1}$. Dividim-ho per g_n. Tindrem

$$f = q(x_n)\, p_n(x_n) + r(x_n)$$

on $\deg(r) < \deg(p_n) = s$. Com r s'anul·la en, al menys els s punts P_i, i K és infinit, això implica que $r(x_n)$ és idènticament nul. Per tant $f \in \langle g_n \rangle$, i g_n és base de $\mathcal{I}_{n-1}$ i també lògicament base de Gröbner.

Sigui ara $f \in \mathcal{I}_{n-2}$ i dividim-ho per $[g_n, g_{n-1}]$. Tindrem

$$f = q_1(x_{n-1}, x_n)\,(x_{n-1} - p_{n-1}(x_n)) + q_2(x_{n-1}, x_n)\, p_n(x_n)) + r(x_n)$$

El residu r no pot contenir la variable x_{n-1} ja que és el monomi principal de g_{n-1}. Igual que abans també cal que $\deg(r) < \deg(p_n) = s$. Com s'anula pels punts P_i això implica que $r = 0$ idènticament i per tant $f \in \langle g_n, g_{n-1} \rangle = \mathcal{I}_{n-2}$, resultant que $\{g_n, g_{n-1}\}$ és base de Gröbnerde $\mathcal{I}_{n-2}$.

Per inducció deduïm que $\mathcal{I}_j = \langle g_{j+1}, \dots g_n \rangle$, i $\{g_{j+1}, \dots g_n\} = \mathrm{gb}(\mathcal{I}_j, \mathrm{lex}(\overline{x}_j))$.

Finalment resulta $G = G_0 = \mathrm{gb}(\mathbb{I}(V), \mathrm{lex}(\overline{x}))$. □

2. Descripció del teorema de l'extensió

Comentem ara el pas de l'extensió. Sigui ara un ideal $\mathcal{I} \subset K[\overline{x}]$ i considerem

$$\mathbb{V}(\mathcal{I}) = \{\overline{a} \in K^n : f(\overline{a}) = 0, \forall f \in \mathcal{I}\}$$

Per descriure els punts de $\mathbb{V}(\mathcal{I})$, la idea bàsica és de construir solucions coordenada per coordenada. Fixem j i anomenem $\overline{a}_j = (a_{j+1}, \dots, a_n) \in \mathbb{V}(\mathcal{I}_j)$

una *solució parcial* del sistema original. Per estendre-la a una solució completa de $\mathbb{V}(\mathcal{I})$ hem d'afegir, en primer lloc una nova coordenada a la solució parcial. Hem de trobar a_j tal que $(a_j, \overline{a}_j) \in \mathbb{V}(\mathcal{I}_{j-1})$. Més concretament, sigui

$$I_{j-1} = \langle g_{r_{j-1}}, \dots, g_s \rangle = \mathcal{I} \cap K[\overline{x}_{j-1}]$$

i volem trobar solucions $x_j = a_j$ de les equacions

$$g_{r_{j-1}}(x_j, \overline{a}_j) = \cdots = g_s(x_j, \overline{a}_j) = 0.$$

Per tant, estem considerant polinomis en una sola variable x_j i, en conseqüència, les possibles solucions a_j són les *arrels comunes* a tots els polinomis, o el que és el mateix, *les arrels del* gcd de tots els polinomis considerats en la variable x_j.

El problema és que els mencionats polinomis poden no tenir arrels comunes. És a dir, poden existir solucions parcials que no estenguin a solucions completes. Considerem el següent

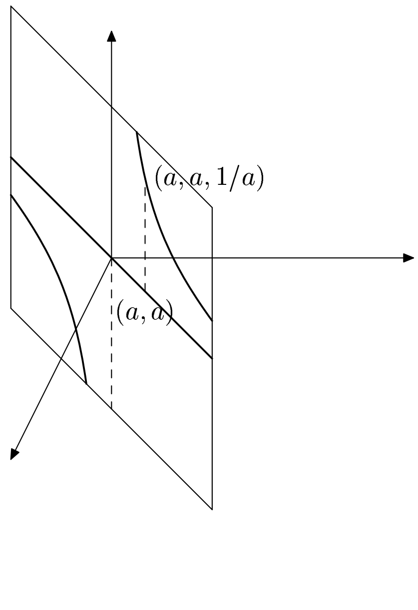
Exemple 2.1. Donat el sistema

$$\begin{cases} z\,y &= 1 \\ z\,x &= 1 \end{cases}$$

Considerem ordre $\operatorname{lex}(z, y, x)$. Resulta

$$\operatorname{gb}(\langle z\,y - 1, z\,x - 1\rangle, \operatorname{lex}(z, y, x)) = \{y - x, z\,y - 1, z\,x - 1\}$$

El primer ideal d'eliminació és $\mathcal{I}_1 = \langle y - x \rangle$, i el segon $\mathcal{I}_2 = \{0\}$. Per tant $\mathbb{V}(I_2) = \mathbb{C}$. La solució parcial $x = a$ a $\mathbb{V}(\mathcal{I}_2)$ estén per tot a a la solució parcial $x = a, y = a$ a $\mathbb{V}(\mathcal{I}_1)$. Ara en canvi aquestes solucions parcials estenen a $(a, a, \frac{1}{a})$ a $\mathbb{V}(\mathcal{I})$ per tot $a \neq 0$. Però la solució parcial $(0, 0)$ no estén. En el gràfic podem veure la interpretació geomètrica.



El nostre objectiu és poder determinar a priori quines solucions estenen i quines no.

Podem restringuir el problema al cas en que eliminem únicament la primera variable x_1. Volem saber si una solució parcial $(\overline{a_1}) \in \mathbb{V}(\mathcal{I}_1)$ estén o no a una solució $(\overline{a}) \in \mathbb{V}(\mathcal{I})$. Tenim el teorema següent:

Teorema 2.2 (de l'Extensió). *Sigui $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subset K[\overline{x}]$, on K és un cos algebraicament tancat, i sigui $\mathcal{I}_1$ el primer ideal d'eliminació de $\mathcal{I}$. Per cada $1 \leq i \leq s$ escribim f_i en la forma*

$$f_i = g_i(\overline{x_1})\, x_1^{N_i} + \textit{termes de grau inferior en } x_i$$

on $N_i \geq 0$ i $g_i \neq 0$. (Si $N_i = 0$ posem $g_i = 0$).

Si $(\overline{a_1}) \in \mathbb{V}(\mathcal{I}_1) \subseteq K^{n-1}$ és una solució parcial tal que $(\overline{a_1}) \notin \mathbb{V}(g_1, \ldots, g_s)$, llavors existeix $a_1 \in K$, tal que $(a_1, \overline{a_1}) \in \mathbb{V}(\mathcal{I})$ és solució.

La demostració del teorema utilitza resultants i la donem més endavant. Ara ens dedicarem a comentar i explotar les conseqüències del teorema.

Una *primera observació* és que el teorema s'aplica a un *cos K algebraicament tancat* com ara $\mathbb{C}$, però no a $\mathbb{R}$. Exemple: $\mathcal{I} = \langle x^2 - y, x^2 - z \rangle$. És facil comprovar que $y - z \in \mathcal{I}$ genera l'ideal d'eliminació $\mathcal{I}_1$, i que $(y = a, z = a)$ és solució parcial de $\mathbb{V}(\mathcal{I}_1)$ per tot a. Com que els monomis principals en x de la base donada de $\mathcal{I}$ tenen coeficient $g_1 = g_2 = 1$ i per tant no s'anul.len mai, el teorema de l'extensió assegura l'existència d'extensions per tot $a \in \mathbb{C}$. Però les solucions han de verificar $x^2 = a$. És cert que per tot $a \in C$ hi ha solució de $x^2 = a$ a $\mathbb{C}$. En canvi únicament hi ha solucions a $\mathbb{R}$ per $a \geq 0$.

Una *segona observació* és que el teorema *pot fracassar quan tots els $g_i(\overline{a_1})$ s'anul.len simultàniament* ($(\overline{a_1}) \in \mathbb{V}(g_1, \ldots, g_s)$). Aquest era el cas de l'exmeple 2.1. Alli teniem la solució parcial $y = a, z = a$ per tot a. La única solució parcial que no estenia era la corresponent a $a = 0$, que és precisament l'únic valor que anul.la simultàniament els coeficients del monomi principal en x dels polinomis de la base de $\mathcal{I}$. Aquests són precisament $g_1(a, a) = g_2(a, a) = a$. Així doncs, l'exigència en l'enunciat del teorema de que la solució parcial no anul.li simultàniament aquests coeficients del monomi principal en x no pot rebaixar-se, ja que efectivament, trobem exemples on realment no hi ha extensió possible quan la solució parcial els anul.la a tots simultàniament.

Finalment destaquem que $\mathbb{V}(g_1, \ldots, g_s)$ *depén de la base de $\mathcal{I}$*. Canviant de base, pot produïr canvis en $\mathbb{V}(g_1, \ldots, g_s)$. L'elecció de la base de $\mathcal{I}$ pot fer que $\mathbb{V}(g_1, \ldots, g_s)$ es redueixi. També cal destacar que *en l'espai projectiu, totes les solucions parcials estenen*, encara que pertanyin a $\mathbb{V}(g_1, \ldots, g_s)$.

Ara podem veure com actua el teorema quan l'emprem no únicament per la primera variable. La idea és que $\mathcal{I}_{j+1}$ és el primer ideal d'eliminació de $\mathcal{I}_j$, i podem estendre variable a variable.

Exemple 2.3. Sigui $B = \{x^2 + y^2 + z^2 - 1, xyz - 1\}$ una base de $\mathcal{I}$. Resulta que $\mathrm{gb}(\mathcal{I}, \mathrm{lex}(x, y, z)) = \{f_1, f_2\}$, on $f_1 = y^4z^2 + y^2z^4 - y^2z^2 + 1$ i $f_2 = x + y^3z + yz^3 - yz$.

Tindrem $\mathcal{I}_1 = \langle f_1 \rangle$ i $\mathcal{I}_2 = \{0\}$.

Per tant, $\mathbb{V}(\mathcal{I}_2) = \mathbb{C}$, i tot $c \in \mathbb{C}$ és una solució parcial de $\mathbb{V}(\mathcal{I}_2)$. La pregunta és quines solucions parcials $c \in \mathbb{V}(\mathcal{I}_2)$ estenen a $\mathbb{V}(\mathcal{I})$.

Estenem coordenada a coordenada. *La observació crucial* és que $\mathcal{I}_2$ és el primer ideal d'eliminació de $\mathcal{I}_1$. Així podem aplicar el teorema d'extensió per passar de $c \in \mathbb{V}(\mathcal{I}_2)$ a $(b, c) \in \mathbb{V}(\mathcal{I}_1)$. Per passar de $\mathcal{I}_2$ a $\mathcal{I}_1 = \langle f_1 \rangle$, el coeficient de y^4 a f_1 és z^2, que únicament s'anul.la per $c = 0$. Per tant c estén a al menys una solució $(b(c), c) \in \mathbb{V}(\mathcal{I}_1)$ per tot $c \neq 0$. Ara per passar a $\mathcal{I}$, els coeficients de la potència màxima de x en la base B de $\mathcal{I}$ són $g_1(b, c) = 1$ i $g_2(b, c) = bc$. Com un d'ells és constant i diferent de zero, el teorema d'extensió assegura que sempre podem estendre la solució anterior amb $c \neq 0$ a un conjunt finit de punts de la forma $(a(c), b(c), c) \in \mathbb{V}(\mathcal{I})$.

Corol·lari 2.4. *Sigui $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subset K[\overline{x}]$, i K algebraicament tancat i tal que per algún i f_i és de la forma*

$$f_i = cx_1^N + \textit{termer d'ordre inferior en } x_1$$

on $c \in K$ és una constant diferent de zero i $N > 0$. Si $\mathcal{I}_1$ és el primer ideal d'eliminació i $(\overline{a_1}) \in \mathbb{V}(\mathcal{I}_1)$, llavors existeix $a_1 \in K$ tal que $(a_1, \overline{a_1}) \in \mathbb{V}(\mathcal{I})$.

La demostració és immediata a partir del teorema de l'extensió.

Exercici 2.5. Sigui $\mathcal{I}$ un ideal de $\mathbb{C}[z, y, x]$ i $G = \mathrm{gb}(\mathcal{I}, \mathrm{lex}(z, y, x))$:

$$\begin{aligned} G \;=\; \{ & \, x(y+1)(xy^2 - 4x^3 - 4x^2 + 3x + 4), \\ & 2(x^2 - 1)z - x(y+1), \\ & (y+1)(\,2(y-1)z + x(y^2 - 4x^2 - 4x - 1)), \\ & (x-1)(y-1)z^2 - x(y+1) \, \} \end{aligned}$$

a) Doneu $\mathcal{I}_1 = \mathcal{I} \cap \mathbb{C}[y, x]$ Per quins punts de la solució parcial $\mathbb{V}(\mathcal{I}_1)$, el teorema d'extensió no garanteix que hi hagi solució completa a $\mathbb{V}(\mathcal{I})$ sobre $\mathbb{C}$?
b) Estudieu que passa en cada un dels punts determinats a a). Estèn la solució? Si per algún d'ells estén, quàntes solucions de $\mathbb{V}(\mathcal{I})$ li corresponen?
c) Pels restants punts de $\mathbb{V}(\mathcal{I}_1)$ discutiu també quàntes solucions de $\mathbb{V}(\mathcal{I})$ corresponen a cada punt.
d) Discutiu els apartats b) i c) a $\mathbb{R}[z, y, x]$
e) Describiu la varietat $\mathbb{V}(\mathcal{I})$. Feu un gràfic ilustrant també $\mathbb{V}(\mathcal{I}_1)$.

3. Geometria de l'eliminació

Definició 3.1 (Projecció d'una varietat afí). Donada $V = \mathbb{V}(f_1, \ldots, f_s) \subseteq K^n$ anomenem j-èsima projecció a

$$\begin{array}{rccc} \pi_j: & K^n & \longrightarrow & K^{n-j} \\ & (\overline{a}) & \mapsto & (\overline{a_j}) \end{array}$$

Tindrem $\pi_j(V) \subseteq K^{n-j}$ i ho podem relacionar amb el j-èsim ideal d'eliminació.

Lema 3.2. *Amb la notació anterior, sigui* $\mathcal{I}_j = \langle f_1, \ldots, f_s \rangle \cap K[\overline{x_j}]$ *el* j*-èsim ideal d'eliminació. Llavors, a* K^{n-j} *tenim*

$$\pi_j(V) \subseteq \mathbb{V}(\mathcal{I}_j)$$

Demostració. Si $f \in \mathcal{I}_j$ i $(\overline{a}) \in V$, llavors f s'anul.la a $(\overline{a})$. Però tenint en compte que f no més depén de $\overline{x_j}$, resulta $f(\overline{a_j}) = 0$,

$$f(\overline{a_j}) = f(\pi_j(\overline{a})) = 0$$

el que prova que f s'anul.la a cada punt de $\pi_j(V)$. □

Amb ajut d'aquest lema podem escriure els punts de $\pi_j(V)$ així:

$$\pi_j(V) = \{(\overline{a_j}) \in \mathbb{V}(\mathcal{I}_j) \ : \ \exists (a_1, \ldots, a_j) \in K^j, (a_1, \ldots, a_j, \overline{a_j}) \in V\}$$

és a dir, $\pi_j(V)$ consta exactament de les solucions parcials que es poden estendre a V.

En l'exemple 2.1, tenim

$$\pi_1(V) = \{(a, a) \in \mathbb{C}^2 \ : \ a \neq 0\} = \mathbb{V}(\mathcal{I}_1) - \{(0, 0)\}$$

Teorema 3.3 (Enunciat geomètric del teorema de l'extensió)**.** *Donada* $V = \mathbb{V}(f_1, \ldots, f_s) \subseteq K^n$ *on* K *és algebraicament tancat i els* g_i*'s són els definits en l'enucnciats del teorema de l'extensió 2.2. Si* $\mathcal{I}_1$ *és el primer ideal d'elimincació tenim la igualtat següent a* K^{n-1}*:*

$$\mathbb{V}(\mathcal{I}_1) = \pi_1(V) \cup (\mathbb{V}(g_1, \ldots, g_s) \cap \mathbb{V}(\mathcal{I}_1)) \tag{3.1}$$

Demostració. Resulta del lema 3.2 i el teorema de l'extensió 2.2. □

El teorema afirma que $\pi_1(V)$ omple la varietat afi $\mathbb{V}(\mathcal{I}_1)$ excepte pot ser una part que està a $\mathbb{V}(g_1, \ldots, g_s)$. Malhauradament, no dona indicacions del tamany d'aquesta part. I en ocasions, és inusualment gran.

Exemple 3.4. Sigui l'ideal $\mathcal{I} = \langle f_1, f_2 \rangle$ on

$$\begin{aligned} f_1 = &\quad (y - z)x^2 + xy - 1 \\ f_2 = &\quad (y - z)x^2 + xz - 1 \end{aligned}$$

Determinem el seu ideal d'eliminació (calculant $\text{gb}(\mathcal{I}, \text{lex}(x, y, z))$. Obtenim $G = \{xy - 1, xz - 1, y - z\}$ i per tant $\mathcal{I}_1 = \langle y - z \rangle$.

Donat que, per la base donada de $\mathcal{I}$ és $g_1 = g_2 = y - z$, resulta clar que les g_i's s'anul.len a tot $\mathbb{V}(\mathcal{I}_1)$. Així, el teorema 2.2 no ens dona cap informació sobre el tamany de $\pi_1(V)$ en aquest cas. (En canvi sí que ens dona informació si emprem la base de Gröbner G).

Existeix una relació forta entre $\pi_j(V)$ i $\mathcal{I}_j$, donada pel següent

Teorema 3.5 (Clausura)**.** *Sigui* $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subseteq K[\overline{x}]$ *amb* K *algebraicament tancat i sigui* $V = \mathbb{V}(\mathcal{I})$*. Llavors*

(i) $\mathbb{V}(\mathcal{I}_j)$ *és la clasura de Zariski de* $\pi_j(V) \subseteq K^{n-j}$*:*

$$\mathbb{V}(\mathcal{I}_j) = \overline{\pi_j(V)}$$

(ii) *Si* $V \neq \phi$*, existeix una varietat afí* $W \subset \mathbb{V}(\mathcal{I}_j)$ *estrictament, tal que*

$$\mathbb{V}(\mathcal{I}_j) - W \subseteq \pi_j(V).$$

Demostració. El punt (i) del teorema es provarà en el capítol 4, ja que requereix el Nullstellensatz. Aquí únicament provarem (ii) per $j = 1$.

(ii) ens diu que, si be $\pi_j(V)$ pot no ser igual a $\mathbb{V}(\mathcal{I}_j)$, omple la major part de $\mathbb{V}(\mathcal{I}_j)$, en el sentit de que el que falta està dins d'una varietat estrictament continguda en $\mathbb{V}(\mathcal{I}_j)$. Ho provarem per $j = 1$. La demostració per j més gran és més difícil.

Farem servir la descomposició (3.1).

Sigui W la varietat definida per $W = \mathbb{V}(g_1, \dots, g_s) \cap \mathbb{V}(\mathcal{I}_1)$. La descomposició (3.1) implica que $\mathbb{V}(\mathcal{I}_1) - W \subseteq \pi_1(V)$ i $W \subseteq \mathbb{V}(\mathcal{I}_1)$. Si provem que $W \neq \mathbb{V}(\mathcal{I}_1)$, haurem acabat. Però pot passar, com hem vist a l'exemple 3.4, que $W = \mathbb{V}(\mathcal{I})$.

En aquest cas fem un canvi en les equacions que defineixen V, de manera que W esdevingui més petita. La clau està en veure que si $W = \mathbb{V}(\mathcal{I}_1)$, llavors $V = \mathbb{V}(f_1, \dots, f_s, g_1, \dots, g_s)$. La inclusió $\supseteq$ és obvia. Per provar la inclusió $\subseteq$, sigui $(\overline{a}) \in V$. Llavors, cada f_i s'anul.la en $(\overline{a_1})$, i com que $(\overline{a_1}) \in \pi_1(V) \subseteq \mathbb{V}(\mathcal{I}_1) = W$, resulta que les g_i també s'anul.len. Per tant $(\overline{a}) \in \mathbb{V}(f_1, \dots, f_s, g_1, \dots, g_s)$, el que prova la igualtat.

Sigui ara $\tilde{\mathcal{I}} = \langle f_1, \dots, f_s, g_1, \dots, g_s \rangle$. Observis que $\mathcal{I}$ i $\tilde{\mathcal{I}}$ poden no ser iguals, encara que les varietats associades siguin la mateixa. Per tant, els ideals d'eliminació respectius $\mathcal{I}_1$ i $\tilde{\mathcal{I}_1}$ poden ser diferents. Però com que $\mathbb{V}(\mathcal{I}_1)$ i $\mathbb{V}(\tilde{\mathcal{I}_1})$ són ambdues la clausra de Zarisky de $\pi_1(V)$ (per la part (i) del teorema), resulta que $\mathbb{V}(\mathcal{I}_1) = \mathbb{V}(\tilde{\mathcal{I}_1})$.

El següent pas és trobar una millor base per $\tilde{\mathcal{I}}$. Posem

$$\tilde{f}_i = f_i - g_i x_1^{N_i}$$

el que elimina el terme de grau més gran en x_1 de cada f_i. Per cada i, o be $\tilde{f}_i = 0$, o be té grau estrictament més petit que f_i en x_1. Es obvi que

$$\tilde{\mathcal{I}} = \langle \tilde{f}_1, \dots, \tilde{f}_s, g_1, \dots, g_s \rangle.$$

Apliquem novament el teorema 3.3 a $V = \mathbb{V}(\tilde{f}_1, \dots, \tilde{f}_s, g_1, \dots, g_s)$. Ara els coeficients principals en x_1 dels generadors són diferents, de manera que tenim una nova descomposició

$$\mathbb{V}(\mathcal{I}_1) = \mathbb{V}(\tilde{\mathcal{I}_1}) = \pi_1(V) \cup \tilde{W}$$

on $\tilde{W} = \mathbb{V}(\tilde{\mathcal{I}_1}) \cap \mathbb{V}(\tilde{f}_1, \dots, \tilde{f}_s, g_1, \dots, g_s)$, consisteix en aquelles solucions parcials per les quals els coeficients principals en x_1 de $\tilde{f}_1, \dots, \tilde{f}_s$ s'anul.len.

Abans de continuar ilustrem amb l'exemple 3.4 per què $\tilde{W}$ pot ser més petita que W. Teniem $\mathcal{I}_1 = \langle y - z \rangle$ i $g_1 = g_2 = y - z$, de manera que

$W = \mathbb{V}(\mathcal{I}_1)$. El procés descrit porta a l'ideal

$$\tilde{\mathcal{I}} = \langle (y-z)x^2 + xy - 1, (y-z)x^2 + xz - 1, y - z\rangle$$

i a la nova base de $\tilde{\mathcal{I}}$

$$\tilde{\mathcal{I}} = \langle xy - 1, xz - 1, y - z\rangle = \mathcal{I}$$

Aplicant ara el teorema 3.3 obtenim que $\tilde{W}$ consisteix en les solucions parcials on y i z s'anul.len, és a dir $\tilde{W} = \{(0,0)\}$, que és evidentment més petita que W.

Però no hi ha garantia que fent aquest procés necessàriament $\tilde{W}$ sigui sempre més petita que W. En aquest cas tornem a repetir el procés. En quand aconseguim una $\tilde{W} \subset W$ estrictament, haurem acabat.

No més falta per considerar el cas en que aquest procés sempre porta a una $\tilde{W} = \mathbb{V}(\mathcal{I}_1)$. A cada pas del procés, els graus dels generadors $\tilde{f}_i$'s en x_1 disminueixen (o són zero), de tal manera que en aquest cas arribariem a que tots els generadors tindriem grau 0 en x_1. Això implicaria que V pot ser definit per polinomis de $K[\overline{x_1}]$. Així, doncs, si $(\overline{a_1})$ és una solució parcial, estén per tot valor a_1 a $(a_1, \overline{a_1}) \in V$, i x_1 no apareix en les equacions de definició de V. En aquest cas $\pi_1(V) = \mathbb{V}(\mathcal{I}_1)$ i la part (ii) del teorema es verifica per $W = \phi$. (És aquí on fem servir la hipòtesi de que $V \neq \phi$). ☐

El teorema de la clausura ens dons una descripció parcial de $\pi_j(V)$ ja que ens diu que omple $\mathbb{V}(\mathcal{I}_j)$ a excepció d'un conjunt de punts que estan estrictment continguts en una varietat menor que $\mathbb{V}(\mathcal{I}_j)$. Però els punts no inclosos poden no omplir la varietat menor. L'estructura precisa de $\pi_j(V)$ pot ser descrita de la següent manera. Existeixen varietats $Z_i \subset W_i \subset K^{n-j}$ per $1 \leq i \leq l$ tals que

$$\pi_j(V) = \cup_{i=1}^{l} (W_i - Z_i)$$

Un conjunt amb aquesta característica es diu que és constructible.

En correspondència al corol.lari 2.4 tenim la següent versió geomètrica.

Corol·lari 3.6. *Sigui $V = \mathbb{V}(f_1, \ldots, f_s) \subset K^n$, amb K algebraicament tancat, tal que algun dels f_i's sigui de la forma*

$$f_i = c\,x_1^N + \textit{termes de grau menor en } x_1$$

on $c \in K$ és una constant no nul.la i $N > 0$. Si $\mathcal{I}_1$ és el primer ideal d'eliminació, llavors

$$\pi_1(V) = \mathbb{V}(\mathcal{I}_1).$$

4. Implicitació

Una parametrització és una aplicació:

$$(4.1) \qquad \begin{array}{rccc} F: & S \subseteq K^m & \longrightarrow & K^n \\ & \overline{t} & \mapsto & F(\overline{t}) \end{array}$$

amb la notació habitual $\overline{t} = t_1, \ldots, t_m$. Més detalladament la parametrització F s'escriu:

$$x_1 = f_1(\overline{t}),\ \ldots,\ x_n = f_n(\overline{t}) \tag{4.2}$$

Ens interessem fonamentalment en les parametritzacions polinòmiques, on F és una funció polinòmica i en les racionals. No obstant, altres parameteritzacions, com ara les trigonomètriques, poden transformar-se en racionals fent un canvi de variables. En les parametritzacions polinòmiques $S = K^m$.

El conjunt $F(S)$ és el conjunt de punts parametritzats. En les parametritzacions polinòmiques i en les racionals, té sentit el problema de la implicitació, que consiteix en trobar la clausura de Zarisky $\overline{F(S)}$ de $F(S)$, és a dir, la varietat més petita que conté els punts parametritzats.

El segon problema relacionat, donada una parametrització polinòmica, és saber si tots els punts de la varietat $\overline{F(S)}$ estan o no parametritzats, és a dir si pertanyen o no a $F(S)$.

Les bases de Gröbner lex ens proporcionen el mètode per obtenir la implicitació de les parametritzacions polinòmiques i racionals. Essencialment és un problema d'eliminació de variables.

4.1. **Implicitació polinòmica.** Donada la parametrització polinòmica (4.1), on F és polinòmica i $S = K^m$, a fi d'estudiar com actua el mètode d'eliminació, introduïm les funcions següents

$$\begin{array}{rccc} i: & K^m & \longrightarrow & K^{m+n} \\ & (\overline{t}) & \mapsto & (\overline{t}, F(\overline{t})) \end{array} \qquad \begin{array}{rccc} \pi_m: & K^{n+m} & \longrightarrow & K^n \\ & (\overline{t}, \overline{x}) & \mapsto & (\overline{x}), \end{array}$$

l'ideal de $\mathcal{I} \subseteq K[\overline{t}, \overline{x}]$

$$\mathcal{I} = \langle x_1 - f_1(\overline{t}), \ldots, x_n - f_n(\overline{t}) \rangle,$$

i la seva varietat d'ideal $V = \mathbb{V}(\mathcal{I}) \subseteq K^{m+n}$.

Fem un esquema de com actuen les funcions descrites:

$$\begin{tikzcd} & K^{m+n} \arrow[dr, "\pi_m"] & \\ K^m \arrow[ur, "i"] \arrow[rr, "F"] & & K^n \end{tikzcd}$$

Tenim $F = \pi_m \circ i$. És facil veure que

$$i(K^m) = V$$

ja que per tot $(\overline{t}) \in K^m$, els punts $i(\overline{t}) = (\overline{t}, F(\overline{t}))$ verifiquen les equacions que defineixen V, i recíprocament, si $(\overline{t}, \overline{x}) \in V$, llavors $i(\overline{t}) = (\overline{t}, F(\overline{t})) \in V$. Per tant tenim:

$$F(K^m) = (\pi_m \circ i)(K^m) = \pi_m(i(K^m)) = \pi_m(V)$$

Si K és un cos algebraicament tancat, el teorema de la clausura 3.5 ens assegura que la clausura de Zarisky de la parametrització és $\mathbb{V}(\mathcal{I}_m)$:

$$\overline{F(K^m)} = \mathbb{V}(I_m)$$

on $\mathcal{I}_m = \mathcal{I} \cap K[\overline{x}]$ és el m-èsim ideal d'eliminació. Però el teorema pot generalitzar-se per tot cos infinit:

Teorema 4.1 (Implicitació polinòmica)**.** *Sigui K un cos infinit, i sigui (4.2) l'expressió detallada d'una parametrització polinòmica $F : K^m \longrightarrow K^n$. Sigui $\mathcal{I}$ l'ideal de $K[\overline{t}, \overline{x}]$, definit per $\mathcal{I} = \langle x_1 - f_1(\overline{t}), \dots, x_n - f_n(\overline{t})\rangle$, i $\mathcal{I}_m = \mathcal{I} \cap K[\overline{x}]$ l'm-èsim ideal d'eliminació. Llavors la clausura de Zarisky dels punts parametritzats és:*

$$\overline{F(K^m)} = \mathbb{V}(\mathcal{I}_m)$$

Demostració. Posem $V = \mathbb{V}(\mathcal{I})$. Hem provat el teorema en la discusió anterior quan el cos és algebraicament tancat. Suposem ara que K és un cos infinit qualsevol. Obviament $\mathbb{Z} \subset \mathbb{Q} \subseteq K \subset \overline{K}$, on $\overline{K}$ és el cos clausura algebraica de K. (Veure cap VII, §2, LANG (1965)).

Per provar el teorema a K utilitzarem una tècnica característica que consiteix en passar convenientment de K a $\overline{K}$ i viceversa. Utilitzarem el subindex K o $\overline{K}$ per diferenciar les varietats definides sobre K o sobre $\overline{K}$. Així $\mathbb{V}_K(\mathcal{I}_m)$ és la varietat definida sobre K^n continguda en la varietat més àmplia $\mathbb{V}_{\overline{K}}(\mathcal{I}_m)$. Hem de provar que $\mathbb{V}_K(\mathcal{I}_m) = \overline{F(K^m)}$.

Pel lema 3.2 sabem que $F(K^m) = \pi_m(V_K) \subseteq \mathbb{V}_K(\mathcal{I}_m)$. Sigui ara $Z_K = \mathbb{V}(h_1, \dots, h_s) \subseteq K^n$ una varietat qualsevol de K^n tal que $F(K^m) \subseteq Z_K$. Hem de provar que $\mathbb{V}_K(\mathcal{I}_m) \subseteq Z_K$.

Comencem per observar que $h_i = 0$ a Z_K per tot i, i per tant també $h_i = 0$ sobre el subconjunt més petit $F(K^m)$. Això prova que $h_i \circ F$ s'anul.la a tot K^m. Tenint en compte que $h_i \in K[\overline{x}]$ i F està format per polinomis $f_j \in K[\overline{t}]$, resulta que $h_i \circ F \in K[\overline{t}]$. Per tant, $h_i \circ F$ és un polinomi que s'anul.la sobre K^m. Com K és infinit, això implica (per un teorema que vem veure al capítol 1) que és el polinomi idènticament nul. Per tant, $h_i \circ F$ també són nuls a $\overline{K}^m$ i per tant els h_i s'anul.len a tot $F(\overline{K}^m)$. Així doncs, $Z_{\overline{K}} = \mathbb{V}_{\overline{K}}(h_1, \dots, h_s)$ és una varietat de $\overline{K}^n$ que conté $F(\overline{K}^m)$. Ara podem aplicar el teorema de la clausura 3.5 resultant que $\mathbb{V}_{\overline{K}}(\mathcal{I}_m) \subseteq Z_{\overline{K}}$.

Si en l'expressió anterior ens restiringim a les solucions que estan a K^n resulta immediatament que $\mathbb{V}_K(\mathcal{I}_m) \subseteq Z_K$. □

Algorisme. La utilització pràctica del teorema anterior és la següent. Donada una parametrització polinòmica definida per (4.1), (4.2), considerenm l'ideal

$$\mathcal{I} = \langle x_1 - f_1(\overline{t}), \dots, x_n - f_n(\overline{t})\rangle.$$

Per determinar l'm-èsim ideal d'eliminació, calculem

$$\mathcal{I}_m = \langle \mathrm{gb}(\mathcal{I}, \mathrm{lex}(\overline{t}, \overline{x})) \cap K[\overline{x}]\rangle$$

Llavors $\mathbb{V}(\mathcal{I}_m)$ és la implicitació de la parametrització, o el que és equivalent, la clausura de Zarisky dels punts parametritzats.

Per determinar quins punts de la varietat estan parametritzats i quins no emprem el teorema de l'extensió. Però ara la discusió s'ha de fer cas per cas amb detall. Posem un exemple.

Exemple 4.2. Sigui la següent parametrització:

$$x = -u^2, \quad y = u\,v, \quad z = v^4.$$

La base de Gröbner lex $G = \mathrm{gb}(\langle x + u^2, y - u\,v, z - v^4\rangle, \mathrm{lex}(v, u, x, y, z))$ és:

$$G = \{zx^2 - y^4, u^2 + x, vy^3 + zxu, vx + uy, uv - y, v^2y^2 + zx, v^3y - uz, v^4 - z\}$$

Per tant, la varietat clausura de Zarisky és

$$V = \mathbb{V}(zx^2 - y^4)$$

Ara volem determinar quins punts estan parametritzats i quins no. Per poder aplicar el teorema de l'extensió, hem de treballar a $\mathbb{C}$. Després utilitzarem els resultats per fer la discusió a $\mathbb{R}$ que és on realment sol interessar.

Considerem l'ideal $\mathcal{I}_1 = \langle zx^2 - y^4, u^2 + x\rangle$. Tenint en compte que el coeficient de u^2 és 1, tots els punts de V estenen en $\mathbb{C}$ a valors de u. De fet, per un valor de x corresponen dos valors de $u = \pm\sqrt{-x}$, excepte per $x = 0$ que correspon $u = 0$.

Considerem ara l'extensió a v. Els coeficients principals en v de la base de $\mathcal{I}$ són: $\{y^3, x, u, y^2, y, 1\}$. Per tant, tots els punts estenen en $\mathbb{C}$ a v. A més, per $x \neq 0$ o $y \neq 0$ hi ha alguna equació lineal amb coeficient no nul per aillar v. Per tant, hi ha un sol valor de v que corespon a un punt (u, x, y, z) parametritzat, excepte els punts de l'eix de les z que estan parametritzats quatre vegades ($u = 0$ i $v = z^{1/4}$, les quatre arrels quartes de z).

Passem ara a discutir la parametrització a $\mathbb{R}$. L'argumentació anterior ens mostra que per tot $x \leq 0, y \neq 0$ hi ha extensió real a dos parametritzacions de cada punt. N'hi ha prou en considerar $u \geq 0$. En canvi, la branca de la varietat que correspón a punts positius de x està parametritzada per valors imaginaris de u, i per tant no estén en $\mathbb{R}$. Pel que fa a l'eix de les z, únicament estan parametritzats a $\mathbb{R}$ els que corresponen a $z \geq 0$, ja que els altres corresponen també a valors de v complexos.

4.2. **Implicitació racional.** En el cas d'una parametrització racional les equacions que la defineixen són de la forma:

$$x_1 = \frac{f_1(\bar{t})}{g_1(\bar{t})}, \; \ldots, \; x_n = \frac{f_n(\bar{t})}{g_n(\bar{t})} \tag{4.3}$$

Posem

$$F = \left(\frac{f_1(\bar{t})}{g_1(\bar{t})}, \; \ldots, \; \frac{f_n(\bar{t})}{g_n(\bar{t})}\right).$$

Com que els denominadors es poden anul.lar per punts de K^m, definim $g = g_1 \ldots g_n$ i $W = \mathbb{V}(g)$. Fora de la varietat W no s'anul.len mai els denominadors. Per tant, definim la parametrització així:

$$
\begin{array}{rccc}
F: & K^m - W & \longrightarrow & K^n \\
 & \bar{t} & \mapsto & F(\bar{t})
\end{array}
\tag{4.4}
$$

El problema consisteix, com abans en trobar $\overline{F(K^m)}$.

La idea inicial és considerar l'ideal de K^{n+m}

$$\mathcal{I} = \langle x_1 g_1(\bar{t}) - f_1(\bar{t}), \ldots, x_n g_n(\bar{t}) - f_n(\bar{t}) \rangle$$

i procedir com abans. La sorpresa és que actuant així no sempre obtenim la varietat més petita que conté els punts parametritzats.

Exemple 4.3. Considerem la parametrització racional següent:

$$x = \frac{u^2}{v},\ y = \frac{v^2}{u},\ z = u$$

Si apliquem la tècnica d'eliminació a l'ideal $\mathcal{I} = \langle xv - u^2, uy - v^2, u - z \rangle$ el resultat és

$$\mathbb{V}(\mathcal{I}_2) = \mathbb{V}(z(x^2y - z^3)) = \mathbb{V}(x^2y - z^3) \cup \mathbb{V}(z)$$

que és unió de dos varietats amb parts no comunes. Però és facil comprovar que tots els punts parametritzats estan a $\mathbb{V}(x^2y - z^3)$. Per tant el mètode inicial no obté la varietat més petita que conté la paramtrització.

Podem aconseguir el propòsit introduint una nova variable y i un nou polinomi $g = (g_1 g_2 \cdots g_n)_{red}$ per definir l'ideal $J \subset K[y, \bar{t}, \bar{x}]$

$$\mathcal{J} = \langle x_1 g_1(\bar{t}) - f_1(\bar{t}), \ldots, x_n g_n(\bar{t}) - f_n(\bar{t}), 1 - y\, g \rangle$$

i la seva varietat d'ideal $V = \mathbb{V}(\mathcal{J}) \subseteq K^{n+m+1}$. Posem $W = \mathbb{V}(g)$, que determina els punts on la parametrització no està definida. De forma similar a com hem fet en el cas de la parametrització polinòmica ara tenim les funcions:

$$
\begin{array}{rccc}
j: & K^m - W & \longrightarrow & K^{n+m+1} \\
 & (\bar{t}) & \mapsto & (\frac{1}{g}, \bar{t}, F(\bar{t}))
\end{array}
\qquad
\begin{array}{rccc}
\pi_{m+1}: & K^{n+m+1} & \longrightarrow & K^n \\
 & (y, \bar{t}, \bar{x}) & \mapsto & (\bar{x}),
\end{array}
$$

L'esquema de com actuen aquestes funcions és:

$$
\begin{tikzcd}
 & K^{m+n+1} \arrow[dr, "\pi_{m+1}"] & \\
K^m - W \arrow[ur, "j"] \arrow[rr, "F"] & & K^n
\end{tikzcd}
$$

Tenim $F = \pi_{m+1} \circ j$. La gràcia està en el fet que ara també

$$j(K^m - W) = \mathbb{V}(\mathcal{J}) = V$$

mentre que si empressim la funció $i : K^m - W \longrightarrow K^{m+n}$, llavors tindriem $i(K^m - W) \subseteq \mathbb{V}(\mathcal{I})$, però no podem assegurar la igualtat.

Provem la igualtat anterior.

$\subseteq$: Sigui $\overline{t} \in K^m - W$. Llavors els denominadors no s'anul.len i $g \neq 0$. Es verifiquen totes les equacions que defineixen V incloent la darrera, ja que $1 - g\frac{1}{g} = 0$.

$\supseteq$: Si $(y, \overline{t}, \overline{x}) \in V$, llavors $g \neq 0$, ja que en cas contrari no es verifica la darrera equació que defineix V. Es poden aillar totes les x_i en les equacions que defineixen V i per tant el punt $(\overline{t}) \in K^m - W$, i $(y, \overline{t}, \overline{x}) \in j(K^m - W)$.

Tenint en compte aquesta igualtat resulta ara

$$F(K^m - W) = (\pi_{m+1} \circ j)(K^m - W) = \pi_{m+1}(j(K^m - W)) = \pi_{m+1}(V).$$

Ara el teorema de la clausura assegura que si K és algebraicament tancat, llavors

$$\overline{F(K^m - W)} = \overline{\pi_{m+1}(V)} = \mathbb{V}(\mathcal{J}_{m+1})$$

Tenim el següent teorema, que com abans es pot generalitzar a un cos infinit

Teorema 4.4 (Implicitació racional). *Sigui K un cos infinit, i sigui (4.3) una parametrització racional. Posem $g = g_1 \dots g_n$ i $W = \mathbb{V}(g)$. La parametrització estarà definida a $F : K^m - W \longrightarrow K^n$. Sigui $\mathcal{J}$ l'ideal de $K[y, \overline{t}, \overline{x}]$, definit per $\mathcal{J} = \langle x_1 - f_1(\overline{t}), \dots, x_n - f_n(\overline{t}), y - g\,y \rangle$, i $\mathcal{J}_{m+1} = \mathcal{J} \cap K[\overline{x}]$ l'$(m+1)$-èsim ideal d'eliminació. Llavors la clausura de Zarisky dels punts parametritzats és:*

$$\overline{F(K^m - W)} = \mathbb{V}(\mathcal{J}_{m+1})$$

Acabem de veure la demostració per un cos algebraicament tancat. Per un cos infinit, la tècnica és la mateixa que abans i la única dificultat afegida és que ara enlloc de K^m hem de treballar a $K^m - W$ i cal justificar que els polinomis que s'anul.len a tot $K^m - W$ s'anul.len idènticament. Ho deixem com exercici.

Algorisme. La utilització pràctica del teorema anterior és la següent. Donada una parametrització racional definida per (4.3), definim $g = g_1 \dots g_n$ i considerenm l'ideal

$$\mathcal{J} = \langle x_1 - f_1(\overline{t}), \dots, x_n - f_n(\overline{t}), 1 - yg \rangle.$$

Determinem l'$(m+1)$-èsim ideal d'eliminació, calculant

$$\mathcal{J}_{m+1} = \langle \mathrm{gb}(\mathcal{J}, \mathrm{lex}(y, \overline{t}, \overline{x})) \cap K[\overline{x}] \rangle$$

Llavors $\mathbb{V}(\mathcal{J}_{m+1})$ és la implicitació de la parametrització, o el que és equivalent, la clausura de Zarisky dels punts parametritzats.

Anàlogament al cas de la parametrització polinòmica, el teorema de l'extensió ens permet discutir quins punts estan parametritzats i quins no.

Exemple 4.5. Sigui la parametrització racional

$$x = \frac{1 + t^2}{1 - t^2}, \; y = \frac{2t}{1 - t^2}$$

Considerem l'ideal de $K[w, t, x, y]$ següent:

$$\mathcal{J} = \langle x(1 - t^2) - (1 + t^2), \; y(1 - t^2) - 2t, 1 - w(1 - t^2) \rangle$$

i determinem $G = \text{gb}(\mathcal{J}, \text{lex}(w,t,x,y))$. Obtenim:

$$G = \{x^2 - y^2 - 1, yt - x + 1, (1+x)t - y, 2w - x - 1\}$$

Per tant la implicitació ve donada per la varietat

$$V = \mathbb{V}(x^2 - y^2 - 1)$$

que és una hipèrbola.

Estudiem ara quins punts estan parametritzats a $\mathbb{C}$. Tenim $\mathcal{J}_1 = \langle x^2 - y^2 - 1, yt - x + 1, (1+x)t - y\rangle$, i els únics punts problemàtics pel teorema de l'extensió són els punts de la hipèrbola que anul.len simultàniament els coeficients de grau màxim en t. Hi ha un únic punt que és $P = (-1, 0)$. Per tant, els altres punts estenen, i donat que fora de P alguna de les dues equacions lineals permeten aillar t, el valor de t és únic. Això finalitza la discusió a $\mathbb{C}$. Però el mateix argument que assegura l'existència d'un sol valor de t per cada punt parametritzat, serveix per veure que a cada punt real de V li correspon un valor real de t. Per tant, tots els punts de la varietat V a R^2 excepte el punt $P(-1,0)$ estan parametritzats per un valor real i únic de R. El punt no parametritzat correspondria a $t = \infty$.

Si fem un gràfic paramètric entre $t = -M..M$, quedaran per representar no únicament el punt P, sino també els del seu voltant.

5. Resultants

La resultant de dos polinomis té moltes aplicacions. En particular té també importància en la teoria de l'eliminació.

La resultant de dos polinomis d'una variable $f, g \in K[x]$ respón a la pregunta de si f i g tenen algún factor comú (un polinomi $h(x)$ de grau positiu que els divideix tots dos). Per averiguar-ho tenim mètodes alternatius com ara factoritzar els dos (molt costós) o calcular el gcd per l'algorisme d'Euclides. Però el càlcul del $\text{gcd}(f, g, x)$ comporta divisions en K, mentre, com veurem, la resultant ho evita, i això interessa de cara a l'eliminació.

Lema 5.1. *Siguin $f, g \in K[x]$ de graus $l > 0$ i $m > 0$ respectivament. Llavors f, g tenen un factor comú de grau positiu en x ssi existeixen polinomis $A, B \in K[x]$ tals que*

(i) *A, B no són ambdós nuls.*
(ii) *A té com a màxim grau $m - 1$ i B com a màxim grau $l - 1$.*
(iii) *$Af + Bg = 0$.*

Demostració. Suposem, en primer lloc, que f i g tenen un factor comú $h \in K[x]$ de grau positiu. Sigui $f = h\, f_1$ i $g = h\, g_1$. Obviament f_1 té grau com a màxim $l - 1$ i g_1 grau $m - 1$. Llavors

$$g_1\, f + (-f_1)\, g = g_1\, h\, f_1 - f_1\, h\, g_1 = 0$$

i $A = g_1$ i $B = f_1$ tenen les propietats requerides.

Recíprocament, suposem que existeixen A i B amb les propietats anteriors. Per (i) podem suposar que $B \neq 0$. Si f i g no tinguessin cap factor comú, el seu gcd fora 1. Això implicaria que existirien $\tilde{A}$ i $\tilde{B}$ tals que $\tilde{A}f+\tilde{B}g=1$. Ara multipliquem per B i emprem (iii)

$$B=(\tilde{A}\,f+\tilde{B}\,g)\,B=\tilde{A}\,B\,f+\tilde{B}\,B\,g=\tilde{A}\,Bf-\tilde{B}\,A\,f=(\tilde{A}\,B-\tilde{B}\,A)\,f.$$

Com que $B\neq 0$, això prova que B té grau com a mínim l, el que contradiu (ii). Això demostra que té que existir un factor comú de f i g de grau positiu. □

La resposta que dona el lema no és encara prou satisfactòria, ja que hem de decidir si existeixen A i B amb les propietats (i), (ii) i (iii). Però això és un problema d'àlgebra lineal. En efecte, posem

$$\begin{array}{ll} f=\displaystyle\sum_{i=0}^{l}a_i\,x^{l-i} & g=\displaystyle\sum_{i=0}^{m}b_i\,x^{m-i} \\ A=\displaystyle\sum_{j=0}^{m-1}c_j\,x^{m-1-j} & B=\displaystyle\sum_{j=0}^{l-1}d_j\,x^{l-1-j}. \end{array}$$

f,g són les dades, és a dir, els seus coeficients $\{a_i:0\leq i\leq l\}$ i $\{b_j:0\leq j\leq m\}$ són coneguts. Substituïm en (iii) i busquem $\{c_j:0\leq j\leq m-1\}$ i $\{d_i:0\leq i\leq l-1\}$ que són les incògnites. Tenim:

$$\begin{aligned} 0 \;=\; & Af+Bg=\sum_{i=0}^{l}\sum_{j=0}^{m-1}a_ic_jx^{l+m-1-i-j}+\sum_{i=0}^{m}\sum_{j=0}^{l-1}b_id_jx^{m+l-1-i-j} \\ & \sum_{k=0}^{l+m-1}x^{m+l-1-k}\left(\sum_{i=\max(0,k-m+1)}^{\min(l,k)}a_ic_{k-i}+\sum_{i=\max(0,k-l+1)}^{\min(m,k)}b_id_{k-i}\right)=0 \end{aligned}$$

Per que es verifiqui idènticament (iii) cal que els coeficients de cada potència de x siguin zero. Les equacions resultants són:

(5.1)
$$\left\{\begin{array}{llllllll}
a_0c_0+ & & & b_0d_0 & & & = & 0 \quad : x^{l+m-1}\\
a_1c_0+a_0c_1+ & & & \vdots & \ddots & & = & 0 \quad : x^{l+m-2}\\
\vdots & \ddots & & \vdots & & b_0d_{l-1} & = & 0\\
\vdots & & a_0c_{m-1}+ & \vdots & & \vdots & = & 0\\
\vdots & & \vdots & \vdots & & \vdots & = & 0\\
a_lc_0+ & & \vdots & \vdots & & \vdots & = & 0\\
\ddots & & \vdots & \vdots & & \vdots & = & 0\\
\quad\ddots & & \vdots & b_md_0 & & \vdots & = & 0\\
 & \ddots & \vdots & & \ddots & \vdots & = & 0\\
 & & a_lc_{m-1} & & & b_md_{l-1} & = & 0 \quad : x^0
\end{array}\right.$$

Hi han $l+m$ equacions amb $l+m$ incògnites. El sistema homogeni tindrà solució no trivial si els coeficients de la matriu tenen determinant nul.

Això ens porta a la següent definició:

Definició 5.2 (Matriu de Sylvester, Resultant)**.** Donats dos polinomis $f, g \in K[x]$ de grau positiu en x els escrivim en la forma:

$$\begin{array}{rcl} f & = & a_0x^l+\cdots+a_l\\ g & = & b_0x^m+\cdots+b_m \end{array}$$

Anomenem *matriu de Sylverster* de f i g respecte x a la matriu del sistema anterior. És a dir,

$$\mathrm{Syl}(f,g,x)=\begin{pmatrix}
a_0 & & & & & b_0 & & & \\
a_1 & a_0 & & & & b_1 & b_0 & & \\
\vdots & a_1 & a_0 & & & \vdots & b_1 & \ddots & \\
\vdots & & a_1 & \ddots & & & & & b_0\\
\vdots & & & & a_0 & \vdots & & & b_1\\
a_l & & & & a_1 & \vdots & & & \vdots\\
 & a_l & & & \vdots & b_m & & & \vdots\\
 & & a_l & & \vdots & & b_m & & \vdots\\
 & & & \ddots & \vdots & & & \ddots & \vdots\\
 & & & & a_l & & & & b_m
\end{pmatrix}$$

on els elements exteriors als parl.lelògrams són nuls.

Es defineix la *resultant* de f i g respecte a x com el determinant

$$\mathrm{Res}(f,g,x)=\det(\mathrm{Syl}(f,g,x))$$

Tenint en compte la definició resulten les següents propietats de la resultant:

Proposició 5.3. *Donats $f, g \in K[x]$ de grau positiu en x,*

(i) *la resultant* $\mathrm{Res}(f, g, x) \in K$ *és un polinomi enter en els coeficients de f i g (polinomi a coeficients enters en els coeficients considerats com a variables),*

(ii) *Els polinomis f i g tenen un factor comú a $K[x]$ de grau positiu ssi* $\mathrm{Res}(f, g, x) = 0$.

Demostració. (i) Resulta de la definició de determinant. (ii) La resultant és el determinant del sistema (5.1). Per tant, si és zero, el sistema (5.1) té solució no tirivial i recíprocament. I si el sistema té solució, els polinomis A i B verifiquen (i), (ii) i (iii) del lema 5.1. □

Exemple 5.4. Siguin $f = 2x^3 - 9x^2 + 13x + 6$ i $g = 10x^2 - 9x - 9$. La resultant és

$$\mathrm{Res}(f, g, x) = \begin{vmatrix} 2 & & 10 & & \\ -9 & 2 & -9 & 10 & \\ 13 & -9 & -9 & -9 & 10 \\ 6 & 13 & & -9 & -9 \\ & 6 & & & -9 \end{vmatrix} = 0$$

Per tant f i g tenen un factor comú de grau positiu en x.

Un inconvenient de la resultant és que els determinants costen de calcular. No obstant, les resultants no són determinants qualsevol i existeix algorisme alternatiu per calcular-les que molts sistemes CAS tenen implementat.

Per lligar les resultants a l'eliminació, calculem la resultant de dos polinomis de dues variables $f = xy - 1$ i $g = x^2 + y^2 - 4$, com polinomis en x amb coeficients a $K[y]$.

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

Més en general, si $f, g \in K[x, y]$ són de grau positiu en x, té sentit calcular $\mathrm{Res}(f, g, x)$. Com els coeficients són polinomis en y, la proposició 5.3 assegura que $\mathrm{Res}(f, g, x)$ és un polinomi en y. Per tant, la resultant permet d'eliminar la x. Per que tingui interés cal veure que la resultant obtinguda pertany al primer ideal d'eliminació $\langle f, g\rangle \cap K[y]$. Considerem ara polinomis de n variables $x, \overline{y}$. La definició 5.2 de la resultant, pot ampliar-se als pòlinomis de $K[x, \overline{y}]$. Tenim la següent proposició:

Proposició 5.5. *Donats $f, g \in K[x, \overline{y}]$ de grau positiu en x, existeixen polinomis $A, B \in K[x, \overline{y}]$ únics tals que*

(i) $Af + Bg = \mathrm{Res}(f, g, x)$,

(ii) $A, B \in K[x, \overline{y}]$ *són polinomis enters en els coeficients de f i g, considerats com polinomis de x amb coeficients en $K[\overline{y}]$*

(iii) $deg_x(A) < deg_x(g)$ *i* $deg_x(B) < deg_x(f)$, *o be* $A = B = 0$ *si la resultant és nul.la.*
(iv) $\mathrm{Res}(f, g, x)$ *pertany a l'ideal d'eliminació* $\langle f, g\rangle \cap K[\overline{y}]$.
(v) f, g *tenen un factor comú de grau positiu en* x *ssi* $\mathrm{Res}(f, g, x) = 0$.

Demostració. La definició de la resultant està basada en l'equació $Af+Bg = 0$. Podem emprar els mateixos mètodes que hem emprat a la demostració de la proposició 5.3 per aplicar-los a l'equació

$$\tilde{A}f + \tilde{B}g = 1 \tag{5.2}$$

on $\tilde{A}, \tilde{B} \in K(\overline{y})[x]$. La raó d'utilitzar $\tilde{A}, \tilde{B}$ enlloc de A, B quedarà clara més endavant.

El punt (i) de la proposició és obvi si $\mathrm{Res}(f, g, x) = 0$ (simplement posem $A = B = 0$). Suposem ara que $\mathrm{Res}(f, g, x) \neq 0$ Sigui ara

$$\begin{array}{rcl} f & = & a_0x^l + \cdots + a_l \\ g & = & b_0x^m + \cdots + b_m \\ \tilde{A} & = & \tilde{c}_o x^{m-1} + \cdots + \tilde{c}_{m-1} \\ \tilde{B} & = & \tilde{d}_0 x^{l-1} + \cdots + \tilde{d}_{l-1} \end{array}$$

on els coeficients $\tilde{c}_i, \tilde{d}_i \in K(\overline{y}) = \mathrm{Quot}(\mathrm{K}[\overline{\mathrm{y}}])$ són les incògnites. Subsituint les expressions anteriors en (5.2) tenim un sistema similar al (5.1) canviant la darrera equació per

$$a_l\tilde{c}_{m-1} + b_m\tilde{d}_{l-1} = 1$$

que és el coeficient de x^0 o terme independent de x. Únicament canvia el segon membre que passa de ser 0 a ser 1. El sistema deixa de ser homogeni. Ara, per que sigui un sistema de Cramer amb solució única cal que el determinant del sistema sigui diferent de zero. Però el determinant del sistema és precisament la resultant $\mathrm{Res}(f, g, x)$, que hem suposat diferent de zero. Per tant, el sistema té solució única a $K(\overline{y})$. Al resoldre per Cramer, el denominador és precisamant la resultant. Per tant, els coeficients $\tilde{c}_i, \tilde{d}_i$ tenen denominador comú que és la resultant. Així tindrem

$$\tilde{A} = \frac{A}{\mathrm{Res}(f, g, x)} \quad \tilde{B} = \frac{B}{\mathrm{Res}(f, g, x)}$$

on A, B són polinomis de $K[\overline{y}]$, calculables com a determinants amb coeficients que estan entre els a_i, b_i. Són, per tant, polinomis enters dels coeficients a_i, b_i. Tenint en compte que $\tilde{A}, \tilde{B}$ verifiquen l'equació (5.2), multiplicant per la resultant tindrem:

$$Af + Bg = \mathrm{Res}(f, g, x)$$

Queden provats, doncs, els punts (i), (ii), (iii) i (iv) de la proposició.

Provem ara el punt (v). La demostració de la proposició 5.3 es pot estendre al cas de n variables si treballem a $K(\overline{y})[x]$, ja que $K(\overline{y})$ és un cos. Per tant f i g tenen un factor comú de grau positiu en x a $K(\overline{y})[x]$ ssi

$\operatorname{Res}(f,g,x) = 0$. Però el lema de Gauss vist en el capítol 1, afirma que $f \in K[\overline{y}][x]$ de $\operatorname{cont}(f) = 1$ és irreductible a $K[\overline{y}][x]$ ssi ho és a $K(\overline{y})[x]$. Aplicant-ho aqui, acaba de provar el punt (v) de la proposició. □

La proposició anterior posa de manifest la relació que hi ha entre resultants i eliminació.

Exemple 5.6. Podem ara reprendre l'exemple 5.4. Per la proposició 5.5, està clar que $f = 2x^3 - 9x^2 + 13x + 6$ i $g = 10x^2 - 9x - 9$ no tenen cap factor comú de grau positiu en x, ja que la seva resultant respecte x és diferent de zero. Com a polinomis a $K(y)[x]$ el seu gcd és 1. La identitat de Bézout aplicada a f i g dona:

$$-\frac{yx+1}{y^4-4x^2+1}f + \frac{y^2}{y^4-4x^2+1}g = 1$$

Multiplicant pel denominador, que no és altre que la resultant de f i g, resulta

$$-(yx+1)f + y^2 g = y^4 - 4x^2 + 1 = \operatorname{Res}(f,g,x)$$

que és la versió sense denominadors de la identitat de Bézout, i que expressa la resultant com element de l'ideal d'eliminació $\langle f,g\rangle \cap K[y]$.

6. Resultants i teorema de l'extensió

Com a conseqüencia immediata de la proposició 5.3 resulta el següent

Corol·lari 6.1. *Si K és un cos algebraicament tancat (p.e. $\mathbb{C}$), i $f,g \in K[x]$, llavors f,g tenen una arrel comú a K ssi* $\operatorname{Res}(f,g,x) = 0$.

Amb aquest corol.lari disposem de tots els ingredients per provar el teorema de l'extensió. Provem en primer lloc el següent cas especial.

Teorema 6.2. *Donats $f,g \in K[\overline{y}][x]$ on K és algebraicament tancat, sigui*

$$f = a_0x^l + \cdots + a_l, \quad g = b_0x^m + \cdots + b_m$$

així que $a_0, b_0 \in K[\overline{y}]$ són els coeficients de grau màxim en x de f,g. Sigui $\mathcal{I}_1 = \langle f,g\rangle \cap K[\overline{y}]$ el primer ideal d'eliminació. Si $(\overline{c}) \in \mathbb{V}(\mathcal{I}_1) - \mathbb{V}(a_0,b_0)$, llavors existeix $c \in K$ tal que $(\overline{c},c) \in \mathbb{V}(f,g)$.

Nota: Es tracta de la versió del teorema de l'extensió pel cas en que l'ideal està format per dos polinomis.

Demostració. El nostre objectiu és provar que $f(\overline{c},x)$ i $g(\overline{c},x)$ tenen una arrel comú $c \in K$. Això ens donarà el punt $(\overline{c},c) \in \mathbb{V}(f,g)$.

Suposem en primer lloc que $a_0(\overline{c}) \neq 0$ i $b_0(\overline{c}) \neq 0$. És a dir, que tots dos són no nuls. Tenim

$$\begin{aligned} f(\overline{c},x) &= a_0(\overline{c})x^l + \cdots + a_l(\overline{c}), \quad \text{amb } a_0(\overline{c}) \neq 0 \\ g(\overline{c},x) &= b_0(\overline{c})x^m + \cdots + b_m(\overline{c}), \quad \text{amb } b_0(\overline{c}) \neq 0 \end{aligned}$$

Per la proposició 5.5 sabem que $h = \mathrm{Res}(f,g,x) \in \mathcal{I}_1$, i pel fet que $(\overline{c}) \in \mathbb{V}(\mathcal{I}_1)$ això implica que $h(\overline{c}) = 0$. Avaluem el determinant que dona h en el punt $(\overline{c})$:

$$h(\overline{c}) = \begin{vmatrix}
a_0(\overline{c}) & & & & & b_0(\overline{c}) & & & \\
a_1(\overline{c}) & a_0(\overline{c}) & & & & b_1(\overline{c}) & b_0(\overline{c}) & & \\
\vdots & a_1(\overline{c}) & a_0(\overline{c}) & & & \vdots & b_1(\overline{c}) & \ddots & \\
\vdots & & a_1(\overline{c}) & \ddots & & & & & b_0(\overline{c}) \\
\vdots & & & & a_0(\overline{c}) & \vdots & & & b_1(\overline{c}) \\
a_l(\overline{c}) & & & & a_1(\overline{c}) & \vdots & & & \vdots \\
& a_l(\overline{c}) & & & \vdots & b_m(\overline{c}) & & & \vdots \\
& & a_l(\overline{c}) & & \vdots & & b_m(\overline{c}) & & \vdots \\
& & & \ddots & \vdots & & & \ddots & \vdots \\
& & & & a_l(\overline{c}) & & & & b_m(\overline{c})
\end{vmatrix}$$

Tenint en compte que $a_0(\overline{c}) \neq 0$ i $b_0(\overline{c}) \neq 0$, resulta que és també el determinant que dona la resultant de $f(\overline{c},x)$ i $g(\overline{c},x)$respecte a x. Resulta:

$$0 = h(\overline{c}) = \mathrm{Res}(f(\overline{c},x), g(\overline{c},x), x).$$

En conseqüència, el corol.lari 6.1 implica que $f(\overline{c},x)$ i $g(\overline{c},x)$ tenen una arrel comú, $c \in K$ tal com voliem demostrar.

Ara falta considerar el cas en que no tots dos $a_0(\overline{c})$ i $b_0(\overline{c})$ són diferents de zero. Suposem que únicament és diferent de zero $a_0(\overline{c}) \neq 0$, mentre que $b_0(\overline{c}) = 0$. En aques cas, $g(\overline{c},x)$ té grau estrictament inferior a $m = \deg_x g(\overline{y},x)$. En aquest cas, el determinant anterior de valor $h(\overline{c})$ que té $l+m$ files i $l+m$ columnes no és ja la resultant de $f(\overline{c},x)$ i $g(\overline{c},x)$, que seria un determinant amb menys files i columnes. Podriem estudiar la relació que té amb la resultant. Però seguirem una altra via més simple.

La idea és que com que $\mathbb{V}(f,g)$ està associada a l'ideal $\langle f,g\rangle$, podem utilitzar una altra base de l'ideal en el cas que ens ocupa $a_0(\overline{c}) \neq 0$, $b_0(\overline{c}) = 0$. Si N és un enter positiu, obviament

$$\langle f,g\rangle = \langle f, g + x^N f\rangle$$

Triant N suficientment gran per tal que $\deg_x(x^N f) > \deg_x(g)$, el coeficient principal de $g + x^N f$ respecte a x és a_0, que sabem que és diferent de zero en $(\overline{c})$. Això ens permet utilitzar el raonament anterior amb la nova base $\{f, g + x^N f\}$ i deduir que existeix $c \in K$ tal que $(\overline{c}, c) \in \mathbb{V}(f, g + x^N f) = \mathbb{V}(f,g)$. □

Observem que la prova anterior falla si $a_0(\overline{c}) = b_0(\overline{c}) = 0$ simultàniament per la solució parcial $(\overline{c})$. La raó de fons és que aquesta solució parcial *pot no estendre* efectivament com hem vist en els contraexemples del teorema de l'extensió.

Comparem ara la diferent i complementària informació que donen les bases de Gröbner lex i la resultant respecte a l'ideal d'eliminació $\mathcal{I}_1$. La $\mathrm{gb}(\mathcal{I}, \mathrm{lex}(x, \overline{y}))$ dona una base de $\mathcal{I}_1 = \mathcal{I} \cap K[\overline{y}]$, però no ens assegura que les solucions parcials estenguin. En canvi, la resultant de dos polinomis *crea* un polinomi de l'ideal $\mathcal{I}_1$ que està directament relacionat amb el fet que les soluciions parcials estenguin. Aquesta és la raó de la seva utilitat en el teorema de l'extensió.

Hem demostrat el teorema de l'extensió en el cas d'ideals formats per una base de dos polinomis. Ara hem de generalitzar la demostració per ideals que tenen bases amb un nombre arbitrari de polinomis. La dificultat és que únicament hem definit la resultant de dos polinomis i ens cal un concepte més general de resultant.

7. Resultants generalitzades i teorema de l'extensió

Definició 7.1 (Resultants generalitzades)**.** Donat un conjunt de polinomis $F = \{f_1, \ldots, f_s\} \subset K[\overline{y}, x]$, considerem el polinomi

$$f = u_2 f_2 + \cdots + u_s f_s \in K[\overline{u}, \overline{y}, x]$$

Podem considerar també f_1 com un polinomi de $K[\overline{u}, \overline{y}, x]$. Per la proposició 5.5, la resultant $\mathrm{Res}(f_1, f, x)$ està en $K[\overline{u}, \overline{y}]$. A fi d'obtenir polinomis en $K[\overline{y}]$, desenvolupem la resultant anterior en potències de $\overline{u}$. Ho podem escriure així:

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x) = \sum_\alpha h_\alpha(\overline{y})\, u^\alpha$$

on $u^\alpha = u_2^{\alpha_2} \ldots u_s^{\alpha_s}$ són els momomis en $\overline{u}$ que apareixen al fer el desenvolupament, i $h_\alpha \in K[\overline{y}]$. Anomenem *resultants generalitzades* de $f_1, f_2, \ldots, f_n$ al conjunt dels polinomis h_α descrits.

Exemple 7.2. Determinem les resultant generalitzades dels polinomis

$$f_1 = x^2 + y + z - 1,\ f_2 = x + y^2 + z - 1,\ f_3 = x + y + z^2 - 1$$

Tenim:

$$\begin{aligned}
\mathrm{Res}(f_1, u_2 f_2 + u_3 f_3, x) &= (y^4 + 2y^2 z - 2y^2 + z^2 + y - z)u_2^2 \\
&+ 2(y^2 z^2 + y^3 + z^3 - y^2 - z^2 + yz)u_2 u_3 \\
&+ (z^4 + 2yz^2 + y^2 - 2z^2 + y^2 - 2z^2 - y + z)u_3^2
\end{aligned}$$

Proposició 7.3. *Sigui $\mathcal{I} = \langle f_1, f_2, \ldots, f_s\rangle \subset K[\overline{y}, x]$, i siguin $h_\alpha(\overline{y})$ les resultants generalitzades*

$$h = \mathrm{Res}(f_1, f_2 u_2 + f_s u_s, x) = \sum_\alpha h_\alpha u^\alpha \subset K[\overline{u}, \overline{y}]$$

on $h_\alpha \in K[\overline{y}]$. Llavors, per tot α és $h_\alpha \in \mathcal{I}_1 = \mathcal{I} \cap K[\overline{y}]$, és a dir, les resultants generalitzades pertanyen a l'ideal d'eliminació.

Demostració. Per la proposició 5.5 aplicada a l'anell $K[\overline{u},\overline{y},x]$, existeixen dos polinomis $A, B \in K[\overline{u},\overline{y},x]$ tals que

$$A\,f_1 + B\,(u_2f_2 + \cdots + u_sf_s) = \mathrm{Res}(f_1, u_2f_2 + \cdots + u_sf_s, x) \subset K[\overline{u},\overline{y}]$$

Ara posem

$$A = \sum_\alpha A_\alpha u^\alpha, \quad B = \sum_\beta B_\beta u^\beta$$

on $A_\alpha, B_\beta \in K[\overline{y},x]$.

Provarem que $h_\alpha \in \langle f_1, f_2, \ldots, f_s\rangle = \mathcal{I}$ comparant coeficients de u^α en les dues expressions anteriors que ens donen la resultant. Com ja sabem que $h_\alpha \in K[\overline{y}]$ això implicarà que $h_\alpha \in \mathcal{I}_1$.

Per comparar monomis en $\overline{u}$ posem $\mathbf{e}_2 = (1,0,\ldots,0)$, ... , $\mathbf{e}_s = (0,0,\ldots,1)$, de forma que

$$u_2f_2 + \cdots + u_sf_s = \sum_{i=2}^{s} u^{\mathbf{e}_i} f_i$$

Així tindrem:

$$\begin{aligned}
\sum_\alpha h_\alpha u^\alpha &= \left(\sum_\alpha A_\alpha u^\alpha\right) f_1 + \left(\sum_\beta B_\beta u^\beta\right)\left(\sum_{i=2}^{s} u^{\mathbf{e}_i} f_i\right)\\
&= \sum_\alpha (A_\alpha)\, u^\alpha + \sum_{\beta, i\geq 2} (B_\beta f_i)\, u^{\beta+\mathbf{e}_i}\\
&= \sum_\alpha (A_\alpha)\, u^\alpha + \sum_\alpha \left(\sum_{\beta, i\geq 2, \beta+\mathbf{e}_i=\alpha} B_\beta f_i\right) u^\alpha\\
&= \sum_\alpha \left(A_\alpha f_1 + \sum_{\beta, i\geq 2, \beta+\mathbf{e}_i=\alpha} B_\beta f_i\right) u^\alpha
\end{aligned}$$

Igualant coeficients resulta finalment

$$h_\alpha = A_\alpha f_1 + \sum_{\beta, i\geq 2, \beta+\mathbf{e}_i=\alpha} B_\beta f_i$$

que prova que $h_\alpha \in \mathcal{I}$. Per tant $h_\alpha \in \mathcal{I}_1$. □

Teorema 7.4 (de l'extensió)**.** *Sigui K un cos algebraicament tancat. Sigui $\mathcal{I} = \langle f_1, \ldots, f_s\rangle \subset K[\overline{y},x]$, i sigui $\mathcal{I}_1 = \mathcal{I} \cap K[\overline{y}]$ el primer ideal d'eliminació de $\mathcal{I}$. Per cada $1 \leq i \leq s$ posem*

$$f_i = g_i(\overline{y})x^{N_i} + \text{ termes de grau menor que } N_i \text{ en } x$$

on $N_i \geq 0$ i $g_i \in K[\overline{y}]$ no són nuls. (Posem $g_i = 0$ si $N_i = 0$). Sigui $(\overline{c}) \in \mathbb{V}(\mathcal{I}_1)$ una solució parcial.

Llavors, si $(\overline{c}) \notin \mathbb{V}(g_i, \ldots, g_s)$, existeix $c \in K$ tal que $(\overline{c}, c) \in \mathbb{V}(\mathcal{I})$.

Demostració. Busquem si existeix una arrel $c \in K$ comú a $f_1(\overline{c}, x), \ldots, f_s(\overline{c}, x)$. El cas $s = 2$ l'hem tractat i resolt en el paragraf anterior i està resumit en el teorema 6.2, que cubreix també el cas $s = 1$ ja que $\mathbb{V}(f_1) = \mathbb{V}(f_1, f_1)$. Queda per provar el teorema per $s \geq 3$.

Com $c \notin \mathbb{V}(g_1, \ldots, g_s)$ podem suposar, reordenant si cal, que $g_1(\overline{c}) \neq 0$. Siguin $h_\alpha \in K[\overline{y}]$ les resultants generalitzades

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x) = \sum_\alpha h_\alpha u^\alpha \tag{7.1}$$

Per la proposició anterior 7.3, això implica que $h_\alpha \in \mathcal{I}_1$ per tot α.

Tenint en compte que $(\overline{c}) \in \mathbb{V}(\mathcal{I}_1)$ resulta que $h_\alpha(\overline{c}) = 0$ per tot α. Ara l'equació (7.1) mostra que la resultant

$$h(\overline{u}, \overline{y}) = \mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x) \tag{7.2}$$

s'anul.la idénticament a $(\overline{c})$:

$$h(\overline{u}, \overline{c}) \equiv 0 \tag{7.3}$$

com a polinomi de $K[\overline{u}]$.

Fem ara la hipòtesi següent sobre f_2:

$$g_2(\overline{c}) \neq 0, \quad \text{i } f_2 \text{ té grau en } x \text{ més gran que } f_3, \ldots, f_s \tag{7.4}$$

La conjectura és que això implica

$$h(\overline{u}, \overline{c}) = \mathrm{Res}(f_1(\overline{c}, x), u_2 f_2(\overline{c}, x) + \cdots + u_s f_s(\overline{c}, x), x) \tag{7.5}$$

és a dir a la resultant generalitada dels polinomis $f_1(\overline{c}, x), \ldots f_s(\overline{c}, x)$ respecte a la única variable x.

L'argumentació és anàloga a la que hem fet en la demostració del teorema 6.2. És a dir, quan avaluem el determinant (7.2) en $\overline{y} = \overline{c}$, resulta que $h(\overline{u}, \overline{c})$ be donat per cert determinant. I si els coeficients principals de f_1 i de $u_2 f_2 + \ldots u_s f_s$ no s'anul.len en $\overline{c}$, aquest determinant és precisament el segon membre de (7.5), que és el que hem conjecturat.

Però en el cas de f_1 és cert, ja que per hipòtesi $g_1(\overline{c}) \neq 0$. Pel polinomi $u_2 f_2 + \ldots u_s f_s$ també és cert en el cas de les hipòtesis (7.4), ja que amb aquestes hipòtesis el coeficient principal és $g_2(\overline{c}) \neq 0$.

Combinant (7.3) i (7.5), resulta

$$\mathrm{Res}(f_1(\overline{c}, x), u_2 f_2(\overline{c}, x) + \cdots + u_s f_s(\overline{c}, x), x) = 0$$

Els polinomis $f_1(\overline{c}, x)$ i $u_2 f_2(\overline{c}, x) + \cdots + u_s f_s(\overline{c}, x)$ estan a $K[\overline{u}, x]$, i per tant, el fet que la seva resultant s'anul.li imlica que tenen un factor comú F de grau positiu en x. Tenint en compte que $F \mid f_1(\overline{c}, x)$ resulta que F és un polinomi de $K[x]$. Com que també $F \mid u_2 f_2(\overline{c}, x) + \cdots + u_s f_s(\overline{c}, x)$, un raonament senzill prova que $F \mid f_i(\overline{c}, x)$ per cada i. Per tant F és un factor comú de grau positiu en x de tots els $f_i(\overline{c}, x)$. Sigui ara $c \in K$ una arrel de F (sabem que existeix ja que K és algebraicament tancat). Llavors c és una arrel de tots els $f_i(\overline{c}, x)$, el que acaba de provar el teorema de l'extensió quan es cumpleixen les hipòtesis (7.4).

Només queda provar-lo si no es verifiquen les hipòtesis (7.4). El procediment és el mateix que hem fet servir en el cas del teorema 6.2, és a dir un canvi de base de l'ideal. És obvi que

$$\mathcal{I} = \langle f_1, f_2 + x^N f_1, f_3, \dots, f_s \rangle$$

Si N és suficientment gran el coeficient principal de $f_2 + x^N f_1$ respecte a x serà $g_1(\overline{y})$, que per hipòtesi no s'anul.la per $\overline{y} = \overline{c}$. Fent N més gran si cal, podem fer que $f_2 + x^N f_1$ tingui grau més gran en x que qualsevol dels altres $f_3, \dots, f_s$. La nova base ara ja cumpleix les hipòtesis (7.4), i l'argument anterior ens dona una arrel comú c de cada polinomi de la nova base en $\overline{y} = \overline{c}$. És obvi que és també arrel de $f_2(\overline{c}, x)$. Això completa la demostració. $\square$