Apunts d'Àlgebra Computacional

Facultat de Matemàtiques i Estadística
Departament de Matemàtica Aplicada II

Antonio Montes

Febrer 2012

Índex

CAPíTOL 1

Ideals, Polinomis, Factorització Única i Varietats afins

1. Anells, Ideals

Resumim breument definicions i conceptes que se suposen coneguts i que convé repassar per comprendre bé el curs.

DEFINICIÓ 1.1 (Anell). Un **anell** $\mathcal{R}$ és un grup additiu abelià amb una operació producte $(a, b) \mapsto ab$ i un "element identitat"1, que, per tot $a, b, c \in \mathcal{R}$ verifica

$$\begin{array}{rcll} a(bc) & = & (ab)c & \text{(associativa)} \\ a(b+c) & = & ab+ac & \\ (b+c)a & = & ba+ca & \text{(distributiva)} \\ 1\,a & = & a\,1 = a & \text{(identitat)} \end{array}$$

Si a més a més compleix que per tot $a, b \in \mathcal{R}$ és $ab = ba$, direm que $\mathcal{R}$ és un **anell commutatiu**. En aquest curs tots els anells que apareixeran seran commutatius.

DEFINICIÓ 1.2 (Unitat o element invertible). Una **unitat** d'un anell $\mathcal{R}$ és un element u pel qual existeix un element $v \in \mathcal{R}$, tal que $u\,v = 1$.

DEFINICIÓ 1.3 (Divisor). Donats $a, b \in \mathcal{R}$, diem que b **divideix** a (notació: $b \mid a$), si existeix $c \in \mathcal{R}$ tal que $a = b\,c$.

DEFINICIÓ 1.4 (Divisor de zero). Un **divisor de zero** és un element no nul $r \in \mathcal{R}$ tal que per algún $s \in \mathcal{R}$ no nul es verifica $r\,s = 0$.

DEFINICIÓ 1.5 (Domini). Un **domini** és un anell $\mathcal{R}$ sense divisors de zero.

PROPOSICIÓ 1.6. *Un anell $\mathcal{R}$ és un domini ssi*

$$((a \neq 0) \wedge (ab = ac)) \longrightarrow (a = b)$$

DEMOSTRACIÓ. Exercici 1.3. □

Un **cos** és un anell pel qual $1 \neq 0$, i tot element no nul és invertible. Denotem $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ per designar respectivament l'anell dels enters i els cossos dels racionals, reals i complexos.

Un **sub-anell** de $\mathcal{R}$ és un sub-conjunt tancat per suma, resta i multiplicació que conté la identitat de $\mathcal{R}$. Un exemple de sub-anell de $\mathbb{R}[x]$ és $\mathbb{Z}[x]$.

DEFINICIÓ 1.7 (Ideal). Un **ideal** d'un anell commutatiu $\mathcal{R}$ és un sub-anell $\mathcal{I}$ tal que per tot $r \in \mathcal{R}$ i $s \in \mathcal{I}$ es verifica $r\,s \in \mathcal{I}$

Direm que

$$\langle S\rangle = \left\{ \sum_1^n r_i\, s_i : \ r_i \in \mathcal{R},\ s_i \in S,\ n \geq 1 \right\}$$

és l'**ideal generat** per un sub-conjunt $S \subseteq \mathcal{R}$. Si S és un sub-conjunt finit $S = \{s_1, \ldots, s_n\}$, llavors escriurem $\langle S\rangle = \langle s_1, \ldots, s_n\rangle$. Convindrem que l'ideal generat pel conjunt buit és el l'ideal $\{0\}$.

Si $\mathcal{I} = \langle S\rangle$ direm que S és un **conjunt de generadors** o una **base** de $\mathcal{I}$.

DEFINICIÓ 1.8 (Ideal principal). Un ideal d'un anell és **principal** si té una base formada per un únic element: $\mathcal{I} = \langle h\rangle$.

DEFINICIÓ 1.9 (Anell quocient). Sigui $\mathcal{I}$ un ideal de $\mathcal{R}$. Definim

(i) la classe de $a \in \mathcal{R}$ per $\overline{a} = [a]_{\mathcal{I}} = \{b : \ b \in \mathcal{R},\ b - a \in \mathcal{I}\}$,
(ii) el conjunt quocient $\mathcal{R}/\mathcal{I}$ per $\mathcal{R}/\mathcal{I} = \{[a]_{\mathcal{I}} : \ a \in \mathcal{R}\}$,
(iii) la suma i producte d'elements de $\mathcal{R}/\mathcal{I}$ per

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a}\,\overline{b} &= \overline{ab} \end{aligned}$$

PROPOSICIÓ 1.10. . *El conjunt $\mathcal{R}/\mathcal{I}$ així definit amb les operacions associades és un anell.*

DEMOSTRACIÓ. Exercici 1.5. □

DEFINICIÓ 1.11 (Suma, producte i intersecció d'Ideals). Donats dos ideals $\mathcal{I}, \mathcal{J}$ d'un anell $\mathcal{R}$, definim les operacions **suma** i **producte** per

$$\begin{aligned} \mathcal{I} + \mathcal{J} &= \{a + b \ : \ a \in \mathcal{I}, b \in \mathcal{J}\} \\ \mathcal{I} \cdot \mathcal{J} &= \subseteq \sum_{k=1}^{n} a_k\, b_k : \ n \geq 1,\ a_k \in \mathcal{I},\ b_k \in \mathcal{J} \\ \mathcal{I} \cap \mathcal{J} &= \{a \ : \ (a \in \mathcal{I}) \wedge (a \in \mathcal{J})\} \end{aligned}$$

Més en general, si tenim una col·lecció d'ideals $\subseteq \mathcal{I}_i : i \in I$, definim la suma de tots ells

$$\sum_{i\in I} \mathcal{I}_i = \left\{ \sum_{j=1}^{n} a_j \ : \ n \geq 1,\ a_j \in \mathcal{I}_{i_j},\ i_j \in I \right\}$$

PROPOSICIÓ 1.12. *Si $\mathcal{I}$ i $\mathcal{J}$ són ideals de $\mathcal{R}$, llavors*

(1) *$\mathcal{I} + \mathcal{J}$, $\mathcal{I} \cdot \mathcal{J}$ i $\mathcal{I} \cap \mathcal{J}$ són ideals.*
(2) *$\mathcal{I} \cdot \mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$.*

DEMOSTRACIÓ.

(1) Exercici.
(2) Si $a \in \mathcal{I} \cdot \mathcal{J}$, llavors $a = \sum_i b_i\, c_i$, on $b_i \in \mathcal{I}$ i $c_i \in \mathcal{J}$. Per ser $\mathcal{I}, \mathcal{J}$ ideals, cada producte $b_i\, c_i$ pertany a $\mathcal{I}$ i a $\mathcal{J}$ i per tant a la intersecció $I \cap \mathcal{J}$. Per tant, $a = \sum_i b_i\, c_i$ també pertany a $I \cap \mathcal{J}$.

□

Proposició 1.13. *Si $\mathcal{I} = \langle a_1, \ldots, a_n \rangle$, i $\mathcal{J} = \langle b_1, \ldots, b_m \rangle$, llavors:*

(i) $\mathcal{I} + \mathcal{J} = \langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$
(ii) $\mathcal{I} \cdot \mathcal{J} = \langle \{a_r\, b_s : \ 1 \leq r \leq n, \ 1 \leq s \leq m\} \rangle$

En canvi no hi ha una expressió evident de la intersecció en termes dels generadors corresponents

Demostració. Exercici. □

Definició 1.14 (Ideal primer). Direm que un **ideal** $\mathcal{I}$ d'un anell commutatiu $\mathcal{R}$ és **primer** si $\mathcal{I} \neq \mathcal{R}$ (diem, llavors, que és un **ideal propi**) i si $a, b \in \mathcal{R}$ i $a\, b \in \mathcal{I}$ implica que $a \in \mathcal{I}$ o $b \in \mathcal{I}$.

Proposició 1.15. *Si un ideal $\mathcal{I}$ és primer i conté un producte d'ideals $\mathcal{J}_1\, \mathcal{J}_2 \ldots \mathcal{J}_n \subseteq \mathcal{I}$, llavors conté algún dels $\mathcal{J}_i$.*

Demostració. Exercicis 1.8 i 1.9. □

Definició 1.16 (Ideal maximal). Un **ideal** $\mathcal{P}$ de $\mathcal{R}$ és **maximal** si és un ideal propi no contingut estrictament en cap altre ideal propi.

Proposició 1.17. *$\mathcal{P} \subseteq \mathcal{R}$ és un ideal primer ssi $R/\mathcal{P}$ és un domini.*

Proposició 1.18. *$\mathcal{P} \subseteq \mathcal{R}$ és un ideal maximal ssi $\mathcal{R}/\mathcal{P}$ és un cos.*

Corol·lari 1.19. *Tot ideal maximal és primer.*

Demostració. Exercici 1.10 □

Definició 1.20 (Element primer). Un **element** $a \in \mathcal{R}$ no nul és **primer** si no és una unitat i si a divideix un producte $b\, c$ llavors a divideix a un dels factors b o c.

Definició 1.21 (Element irreductible). Un **element** $a \in \mathcal{R}$ és **irreductible** si no es pot descompondre en producte $b\, c$ d'elements b, c no unitaris.

Proposició 1.22. *Si $\mathcal{R}$ és un domini, tot primer $p \in \mathcal{R}$ és irreductible.*

Demostració. Si p és primer i $p = u\, v$, llavors $p \mid u$ o $p \mid v$. Ara bé,

$$p \mid u \quad \Rightarrow \quad \exists q \in \mathcal{R}, \ q\, p = u \Rightarrow pqv = uv = p \Rightarrow qv = 1 \Rightarrow v \text{ és una unitat.}$$

Anàlogament $p \mid v \Rightarrow u$ és una unitat. Per tant p és irreductible. □

2. Dominis Euclidians i PID's

DEFINICIÓ 2.1 (PID = Principal Ideal Domain). Un domini tal que tots els seus ideals són principals diem que és un **domini d'ideals principals** o PID.

DEFINICIÓ 2.2 (Domini euclidià). Un domini $\mathcal{R}$ és **euclidià** si existeix una aplicació de $g:\ \mathcal{R}\setminus\{0\}\to\mathbb{N}$, que anomenem norma, amb les propietats següents:

(i) Si $a,b\in\mathcal{R}$ i $a\neq 0$, $b\neq 0$, llavors $g(ab)\geq g(a)$.
(ii) Donats $a,b\in\mathcal{R}$, amb $b\neq 0$, existeix una expressió

$$a=bq+r$$

on, o bé $r=0$, o be $g(r)<g(b)$.

PROPOSICIÓ 2.3. *Tot domini euclidià $\mathcal{R}$ és un domini d'ideals principals.*

DEMOSTRACIÓ. Sigui $\mathcal{I}$ un ideal de $\mathcal{R}$, que podem suposar $\mathcal{I}\neq\{0\}$. Prenem $b\neq 0$ un element de $\mathcal{I}$ tal que $g(b)$ sigui mínim i veiem que $\mathcal{I}=\langle b\rangle$. Sigui $a\in\mathcal{I}$, $a\neq 0$. Per ser euclidià, $a=bq+r$ i, o bé $r=0$ o bé $g(r)<g(b)$. El segon és impossible perquè $r=a-bq\in\mathcal{I}$ i per l'elecció de b, $g(b)$ és mínim. Per tant $r=0$, i $a\in\langle b\rangle$. □

DEFINICIÓ 2.4 (Màxim comú divisor). Donats dos elements a,b d'un domini $\mathcal{R}$, definim un $\gcd(a,b)$ com un element $d\in\mathcal{R}$ tal que

(i) $d\mid a$ i $d\mid b$.
(ii) Si $p\in\mathcal{R}$ és tal que $p\mid a$ i $p\mid b$, llavors $p\mid d$

OBSERVACIÓ 2.5. El $\gcd(a,b)$ si existeix és únic tret de multiplicació per una unitat, ja que si n'hi hagués dos d_1,d_2 es tindria $d_1\mid d_2$ i $d_2\mid d_1$, i per tant $d_1=u\,d_2$ on u és una unitat. Quan el $\gcd(a,b)$ és una unitat, ho escriurem $\gcd(a,b)=1$.

PROPOSICIÓ 2.6 (Identitat de Bézout). *Si $\mathcal{R}$ és un* PID*, cada parell d'elements a,b té un* $\gcd(a,b)$*, i es verifica una identitat de Bézout de la forma*

$$Aa+Bb=\gcd(a,b),\quad amb\quad A,B\in\mathcal{R}$$

DEMOSTRACIÓ. Per ser $\mathcal{R}$ un PID és $\langle a,b\rangle=\langle h\rangle$, d'on resulta la identitat de Bézout si provem que $h=\gcd(a,b)$. En efecte: Com que $a\in\langle h\rangle$ i $b\in\langle h\rangle$ es compleix la condició (i) de gcd. Si $p\mid a$ i $p\mid b$, llavors $a,b\in\langle p\rangle$ i per tant $\langle h\rangle=\langle a,b\rangle\subseteq\langle p\rangle$. Així $h\in\langle p\rangle$ i $p\mid h$. Per tant $h=\gcd(a,b)$. □

OBSERVACIÓ 2.7. En un PID no tenim en general un algorisme per determinar el gcd, mentre que un anell euclidià tenim l'algorisme d'Euclides.

DEFINICIÓ 2.8 (Mínim comú múltiple). Donats dos elements a,b d'un domini $\mathcal{R}$, definim un $\operatorname{lcm}(a,b)$ com un element $m\in\mathcal{R}$ tal que

(i) $a\mid m$ i $b\mid m$.
(ii) Si $p\in\mathcal{R}$ és tal que $a\mid p$ i $b\mid p$, llavors $m\mid p$

OBSERVACIÓ 2.9. El $\text{lcm}(a, b)$ si existeix també és únic tret de multiplicació per una unitat.

PROPOSICIÓ 2.10. *Si $\mathcal{R}$ és un* PID*, cada parell d'elements a, b té un* $\text{lcm}(a, b)$*, i* $\langle \text{lcm}(a, b) \rangle = \langle a \rangle \cap \langle b \rangle$.

DEMOSTRACIÓ. Per ser $\mathcal{R}$ un PID, existeix m tal que $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$. Òbviament m verifica (i). Sigui ara M tal que $a \mid M$ i $b \mid M$. En conseqüència $M \in \langle a \rangle$ i $M \in \langle b \rangle$, i per tant $M \in \langle a \rangle \cap \langle b \rangle = \langle m \rangle$. Per tant $m \mid M$. □

3. Definició de polinomis sobre un anell commutatiu $\mathcal{R}$.

DEFINICIÓ 3.1. Donat un anell commutatiu $\mathcal{R}(+, \cdot)$, definim el conjunt de polinomis $\mathcal{R}[x_1, \ldots, x_n]$ en les variables $x_1, \ldots, x_n$ sobre $\mathcal{R}$, com el conjunt de totes les expressions que comportin un nombre d'operacions finit entre elements de $\mathcal{R}$ afegint les variables abstractes $x_1, \ldots, x_n$. Per definició, les variables x_i

(i) es comporten com nous elements de $\mathcal{R}$ respecte a les propietats d'anell, podent-se associar, commutar etc. amb els restants elements.
(ii) x_i i totes les seves potències i els productes amb diferents potències de les altres variables són elements diferents entre sí i diferents de tots els altres.
(iii) els elements x_i no tenen invers.

$\mathcal{R}[x_1, \ldots, x_n]$ és una extensió de $\mathcal{R}$ amb els elements $x_1, \ldots, x_n$. Donat un element de $f \in \mathcal{R}[x_1, \ldots, x_n]$, aplicant la propietat distributiva commutativa i associativa tantes vegades com calgui, i posant

$$\overbrace{x_i \cdot x_i \cdot x_i}^{n} = x_i^n$$

podem posar-lo sempre en la forma equivalent:

$$f = \sum_{\alpha_1 \ldots \alpha_n} a_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

PROPOSICIÓ 3.2. *Estenent les operacions de $\mathcal{R}$ a $\mathcal{R}[x_1, \ldots, x_n]$, tenint en compte la definició de polinomi, el conjunt de polinomis sobre $\mathcal{R}$ és un anell commutatiu.*

Farem servir la notació següent:

$$\begin{aligned} \overline{x} &= x_1, \ldots, x_n \\ \alpha &= (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n \\ c_\alpha &= c_{\alpha_1, \ldots, \alpha_n} \in \mathcal{R} \\ x^\alpha &= x_1^{\alpha_1} \ldots x_n^{\alpha_n} \\ f &= \sum_\alpha c_\alpha x^\alpha \end{aligned}$$

Posat f en la forma anterior, cada sumand $a_\alpha x^\alpha$ és un monomi, l'element a_α és el coeficient, i x^α és un producte de potències.

COROL·LARI 3.3. *Dos polinomis f, g de $K[\overline{x}]$ són iguals ssi posats en la forma $f = \sum_\alpha a_\alpha x^\alpha$ i $g = \sum_\beta b_\beta x^\beta$són tals que tenen els mateixos coeficients en correspondència amb els mateixos productes de potències.*

EXEMPLE 3.4. Sigui

$$f = (a + b \cdot x_1) \cdot (x_2 + c \cdot x_3) \cdot x_1 + (a \cdot x_2 + b) \cdot (c \cdot x_1 + x_2 + a)$$

Expandint tenim:

$$ba + bcx_1 + \left(b + a^2\right) x_2 + (a + ac)\, x_1x_2 + bx_1^2x_2 + ax_2^2 + acx_1x_3 + bcx_1^2x_3$$

que té la forma indicada.

Podríem també considerar f com un element de $(\mathcal{R}[x_1, x_3])[x_2]$, és a dir, com un polinomi en la variable x_2 a coeficients en l'anell $\mathcal{R}[x_1, x_3]$. Per això treiem factor comú les potències de x_2 així:

$$f = \left(ba + bcx_1 + acx_1x_3 + bcx_1^2x_3\right) + \left(b + a^2 + (a + ac)x_1 + bx_1^2\right) x_2 + ax_2^2$$

Degut a les propietats d'anell commutatiu, existeix un isomorfisme trivial entre els polinomis de n variables sobre un anell commutatiu, independentment de quines variables es considerin com a tals i quines formant part dels polinomis de l'anell de coeficients. Si representem per $\overline{y}_1, \overline{y}_2$ dos sub-conjunts de variables formant una partició qualsevol de les variables $\overline{x} = x_1, \ldots x_n$, tenim l'isomorfisme

$$(\mathcal{R}[\overline{y}_1])[\overline{y}_2] \approx (\mathcal{R}[\overline{y}_2])[\overline{y}_1] \approx \mathcal{R}[\overline{y}_1, \overline{y}_2] = \mathcal{R}[\overline{x}]$$

que correspon a treure factor comú els diferents productes de potències de $\overline{y}_2$, $\overline{y}_1$ o bé $\overline{x}$.

4. Anells Noetherians

NOTA HISTÒRICA 4.1. Es consideren fundadors de l'Àlgebra commutativa David Hilbert (Königsberg 1862 - Götingen 1943) i la matemàtica Emmy Noether (Erlangen 1882 - Bryn Mawr 1935), ambdós alemanys.

DEFINICIÓ 4.2 (Anell Noetherià). Direm que un anell $\mathcal{R}$ és **Noetherià**, si cada ideal de $\mathcal{R}$ és generat per un nombre finit d'elements.

OBSERVACIÓ 4.3. Els PID's són Noetherians, ja que cada ideal està generat per un únic element.

PROPOSICIÓ 4.4 (Condició de cadena ascendent ACC). *Un anell és Noetherià, ssi tota cadena ascendent d'ideals*

$$\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \ldots$$

estaciona, és a dir, existeix un N a partir del qual tots els $\mathcal{I}_k$ són iguals.

DEMOSTRACIÓ. $\Rightarrow$: Si $\mathcal{R}$ és Noetherià i $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \cdots$ és una cadena ascendent d'ideals, prenem $\mathcal{I} = \cup_{i=1}^{\infty} \mathcal{I}_i$. (**Ex:** Proveu que $\mathcal{I}$ és un ideal.) Per ser $\mathcal{R}$ Noetherià, $\mathcal{I}$ admet un conjunt finit de generadors: $\mathcal{I} = \langle a_1, \ldots, a_n \rangle$. Per la definició de $\mathcal{I}$, cada a_i pertany a algun $\mathcal{I}_{j(i)}$. Sigui N un cota superior dels indexos $j(i)$, $1 \leq i \leq n$. Òbviament $\mathcal{I} \subseteq \mathcal{I}_N$, i per tant, $\mathcal{I}_N = \mathcal{I}_{N+1} = \cdots = \mathcal{I}$.

$\Leftarrow$: Demostrem ara que si tota cadena ascendent estaciona, un ideal $\mathcal{I}$ qualsevol admet un conjunt finit de generadors. En efecte, sigui $a_1 \in \mathcal{I}$. Si $\mathcal{I} = \langle a_1 \rangle$, ja hem acabat. En cas contrari sigui $a_2 \in \mathcal{I} \setminus \langle a_1 \rangle$. Si $\mathcal{I} = \langle a_1, a_2 \rangle$ hem acabat, altrament prenem $a_3 \in \mathcal{I} \setminus \langle a_1, a_2 \rangle \ldots$ Aquest procediment acaba, ja que anem construint una cadena ascendent $\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \ldots$, que per hipòtesi estaciona. Concluïm que $\mathcal{I} = \langle a_1, a_2, \ldots, a_N \rangle$ i $\mathcal{I}$ és Noetherià. □

TEOREMA 4.5 (de la Base d'Hilbert). *Si $\mathcal{R}$ és Noetherià, llavors $\mathcal{R}[x]$ també ho és.*

DEMOSTRACIÓ. Sigui $\mathcal{I}$ un ideal de $\mathcal{R}[x]$ i $n \geq 0$. Notem

$$f = \sum_{i=0}^{n} a_i \, x^i, \quad a_n = \mathrm{lc}(f), \quad x^n = \mathrm{lpp}(f), \quad a_n \, x^n = \mathrm{lm}(f).$$

Direm que a_n és el coeficient principal, x^n la potència principal i $a_n \, x^n$ el monomi principal de $f \in \mathcal{R}[x]$.

A partir de $\mathcal{I}$ formem els conjunts

$$\mathcal{I}_n := \{\mathrm{lc}(f) \in \mathcal{R} \ : \ f \in \mathcal{I}, \ \mathrm{lpp}(f) = x^n\}.$$

Com que els $\mathcal{I}_n$ formen una cadena ascendent d'ideals de $\mathcal{R}$ (perquè?), estacionen en un cert índex N. Prenem $B_i \subseteq \mathcal{I}_i$ un sistema finit de generadors de $\mathcal{I}_i$ per a cada $0 \leq i \leq N$, i per cada element $a \in B_i$, un polinomi $f_a \in \mathcal{I}$ amb $\mathrm{lm}(f) = a \, x^i$. Sigui $B = B_0 \cup \cdots \cup B_N$. Anem a demostrar que $\mathcal{I} = \langle f_a \ : a \in B \rangle$. Provem per inducció sobre el grau i de f, que si $f \in \mathcal{I}$ llavors $f \in \langle f_a \ : a \in B \rangle$. Per $i = 0$ és clar. Si $0 < i \leq N$ sigui $\mathrm{lm}(f) = b \, x^i$, amb $b \in \mathcal{I}_i$. Llavors $b = \sum_{a \in B_i} r_a \, a$ i per tant $f - \sum_{a \in B_i} r_a \, f_a$ té grau menor que i (hem cancel·lat el terme de grau i) amb un polinomi de $\langle f_a : a \in B \rangle$. Per tant, per la hipòtesi d'inducció pertany a $\langle f_a \ : a \in B \rangle$, d'on resulta que també $f \in \langle f_a \ : a \in B \rangle$. Si $i > N$ llavors $b = \sum_{a \in B_N} r_a \, a$ i fem el mateix raonament amb el polinomi $f - \sum_{a \in B_N} r_a \, x^{i-N} f_a$. □

COROL·LARI 4.6. *L'anell dels polinomis $K[\overline{x}] = K[x_1, \ldots, x_n]$ de n variables sobre un cos (o un anell Noetherià) K és Noetherià.*

DEMOSTRACIÓ. Només cal aplicar inducció al teorema 4.5. □

PROPOSICIÓ 4.7. *En un anell Noetherià, de tot sistema generador d'un ideal s'en pot extreure un subsistema finit.*

DEMOSTRACIÓ. Si $S \subseteq \mathcal{R}$ i $\mathcal{I} = \langle S \rangle$, prenem $a_0 \in S$ qualsevol. Si $S \subseteq \langle a_0 \rangle$ ja hem acabat. Si no, prenem $a_1 \in S \setminus \langle a_0 \rangle$. Si $S \subseteq \langle a_0, a_1 \rangle$ ja hem acabat, altrament prenem $a_2 \in S \setminus \langle a_0, a_1 \rangle \ldots$ Aquest procés ha d'acabar

doncs altrament construiríem una cadena infinita estrictament ascendent d'ideals:

$$\langle a_0\rangle \subset \langle a_0, a_1\rangle \subset \langle a_0, a_1, a_2\rangle \subset \cdots$$

□

PROPOSICIÓ 4.8. *Si $\mathcal{R}$ és un domini Noetherià, tot element $a \in \mathcal{R}$ descomposa en producte d'irreductibles.*

DEMOSTRACIÓ. Si a és irreductible ja hem acabat. Si no, sigui $a = a_1a_2$ amb a_1, a_2 no unitaris. Òbviament, pels ideals generats tenim: $\langle a\rangle \subset \langle a_1\rangle$ i també $\langle a\rangle \subset \langle a_2\rangle$, on les inclusions són estrictes. Si algún dels factors (a_1 per exemple) no és irreductible, descomponem $a_1 = a_{11}a_{12}$ i així successivament. S'obté així un arbre de descomposicions i per cada branca apareix una cadena d'ideals estrictament ascendent:

$$\langle a\rangle \subset \langle a_{i_1}\rangle \subset \langle a_{i_1 i_2}\rangle \subset \ \ldots$$

Cal que les descomposicions acabin en producte d'irreductibles, altrament obtindríem una cadena estrictament ascendent d'ideals en contradicció amb el fet que $\mathcal{R}$ és Noetherià. Es forma així un arbre de descomposicions on cada branca és finita, i pel lema de König, l'arbre és finit. □

A fi d'il·lustrar la demostració no constructiva del teorema de la base de Hilbert, incluïm una construcció feta per tanteig en un quadern de treball de *Maple*.

Exemple de construcció heurística de les bases definides en la demostració del Teorema de la Base de Hilbert, emprant *Maple*.

```
> with(Groebner):     read(‘dpgb.mpl‘):     with(dpgb):
```

Exemple a Z[x].

La demostració donada del teorema de la base de Hilbert no és constructiva. No obstant, donat un ideal I de $R[x]$ defineix una successió d'ideals $[I_0, I_1..I_N]$ de R i uns conjunts de polinomis associats
$F_0 = [f_{0\,1}..f_{0\,k_0}],\ F_1 = [f_{1\,1}..f_{1\,k_I}],\ \ldots,\ F_N = [f_{N\,1}..f_{N\,k_N}]$

de $R[x]$ que, tots junts, formen una base finita de I. Posem un exemple i intentem construir els ideals descrits a la demostració del teorema.

Enunciat:

A fi d'il.lustrar el teorema, considerem l'deal de $Z[x]$ següent:

$I = [30\,x^2 + 2\,x,\ 44\,x^5 - 7\,x^3]$

a) Construïm els generadors de la família d'ideals $\{I_i\}$ de R i els conjunts $\{F_i\}$ de $R[x]$ associats que segons el teorema formen una base de I.

b) Seguim el procediment inductiu descrit en la demostració per comprovar que $g = 44\,x^5 - 7\,x^3$ es pot expressar en la base obtinguda de I i obtenim l'expressió corresponent.

Solució:

a) Sigui l'ideal de $Z[x]$ següent:

```
> H:=[30*x^2+2*x,44*x^5-7*x^3];
```

$$H := [30\,x^2 + 2\,x,\ 44\,x^5 - 7\,x^3]$$

Si el considerem a $Q[x]$, podem determinar la base anomenada de Gröbner mitjançant la comanda:

```
> GH:=gbasis(H,plex(x));
```

$$GH := [x]$$

Per tant, a $Q[x]$, l'ideal en qüestió conté tots els polinomis múltiples de x. Però a $Z[x]$ no es poden aconseguir tots, ni en particular tampoc x.

Per tal de construir els generadors dels ideals descrits, tractem d'eliminar els coeficients principals, i obtenir polinomis de H per cada potència de x amb coeficient principal tant petit com sigui possible:

```
> f1:=H[1]; f2:=H[2];
```

$$f1 := 30\,x^2 + 2\,x$$

$$f2 := 44\,x^5 - 7\,x^3$$

Definim el S-polinomi de f i g de la manera següent:

$$\mathrm{S}(f,\,g) = \frac{\mathrm{lcm}(\mathrm{lm}(f),\,\mathrm{lm}(g))\,f}{\mathrm{lm}(f)} - \frac{\mathrm{lcm}(\mathrm{lm}(f),\,\mathrm{lm}(g))\,g}{\mathrm{lm(g)}}$$

on $\mathrm{lm}(f)$ és el monomi principal (tant en coeficient com en variables). La definició de S-polinomi té per objecte cancel.lar els monomis principals d'ambdós polinomis.

```
> f3:=pspol(f1,f2,plex(x));
```

$$f3 := 44\,x^4 + 105\,x^3$$

```
> f4:=pspol(f3,f1,plex(x));
```

$$f4 := 1531\,x^3$$

```
> f5:=pspol(f1,f4,plex(x));
```

$$f5 := 3062\,x^2$$

```
> f6:=pspol(f1,f5,plex(x));
```

$$f6 := 3062\,x$$

```
> h1:=pspol(f1,f6,plex(x));
```

$$h1 := 3062\,x$$

```
> f7:=pspol(f6,f2,plex(x));
```

$$f7 := 10717\,x^3$$

```
> pspol(f7,f6,plex(x));
```

$$0$$

```
> h2:=pspol(f7,f2,plex(x));
```

$$h2 := 75019\,x^3$$

Hem obtingut dos polinomis de H de grau 2. A fi d'aconseguir un coeficient que pugui ser generador de I_2 emprem la identitat de Bézout pels coeficients. Així obtindrem un polinomi de I_2 que tindrà un coeficient que genera els coeficients dels dos polinomis obtinguts:

```
> igcdex(coeff(f1,x^2),coeff(f5,x^2),'A','B'), [A,B];
```

$$2,\ [-102,\ 1]$$

```
> f8:=expand(A*f1+B*f5);
```

$$f8 := 2\,x^2 - 204\,x$$

Ara busquem el generador de I_3

```
> igcdex(coeff(f4,x^3),coeff(f8,x^2),'A','B'), [A,B];
```

$$1,\ [1,\ -765]$$

```
> f9:=expand(A*f4+B*x*f8);
```

$$f9 := x^3 + 156060\,x^2$$

que tenint en compte f_6 i f_8 es pot reduir a

```
> b0:=iquo(156060,3062); h9:=f9-b0*x*f6;
```

$$b0 := 50$$

$$h9 := x^3 + 2960\,x^2$$

```
> h10:=h9-1480*f8;
```

$$h10 := x^3 + 301920\,x$$

```
> b1:=iquo(301920,3062); f10:=h10-b1*f6;
```

$$b1 := 98$$

$$f10 := x^3 + 1844\,x$$

La base dels S és:

```
> S:=[f6,f8,f10];
```

$$S := [3062\,x,\ 2\,x^2 - 204\,x,\ x^3 + 1844\,x]$$

en correspondència als ideals de Z:

```
> I0:=[]; I1:=[3062]; I2:=[2]; I3:=[1];
```

$$I0 := []$$

$$I1 := [3062]$$

$$I2 := [2]$$
$$I3 := [1]$$

b) Comprovem ara que *f2* es pot expressar per la via d'inducció de la demostració en termes de S:

```
> r1:=expand(f2-44*x^2*f10);
```
$$r1 := -81143\,x^3$$
```
> c1:=-coeff(r1,x^3); r2:=expand(r1+c1*f10);
```
$$c1 := 81143$$
$$r2 := 149627692\,x$$
```
> c2:=iquo(coeff(r2,x),coeff(f6,x));
```
$$c2 := 48866$$
```
> expand(44*x^2*f10-c1*f10+c2*f6);
```
$$44\,x^5 - 7\,x^3$$
```
> g:=collect(expand(44*x^2*F10-c1*F10+c2*F6),{F6,F8,F10
> },distributed);
```
$$g := (44\,x^2 - 81143)\,F10 + 48866\,F6$$

Aquesta és, doncs, una expressió de g en termes dels polinomis de S. Comprovem-ho:

```
> expand(subs(F6=f6,F8=f8,F10=f10,g));
```
$$44\,x^5 - 7\,x^3$$

5. Dominis factorials (UFD)

DEFINICIÓ 5.1 (UFD = Unique Factorization Domain). Direm que un domini $\mathcal{R}$ és un **domini de factorització única** o **domini factorial**, (UFD), si cada element es descompon en producte d'elements irreductibles de $\mathcal{R}$ de 'forma única', és a dir si $a = \prod_{i=1}^{r} p_i = \prod_{i=1}^{s} q_i$ on tots els p_i i q_i són irreductibles llavors $r = s$ i cada p_i és de la forma $q_i u_i$, amb u_i unitari.

LEMA 5.2. *Sigui $\mathcal{R}$ un domini on tot element admet una descomposició en producte d'irreductibles. Llavors són equivalents:*

(i) *$\mathcal{R}$ és un domini de factorització única.*
(ii) *En $\mathcal{R}$, tot element irreductible és primer.*

DEMOSTRACIÓ. .

(i) $\Rightarrow$ (ii): Sigui $\mathcal{R}$ un UFD i sigui $q \in \mathcal{R}$ irreductible. Si $q \mid bc$, siguin $b = p_1 \cdot \cdots \cdot p_r$ i $c = q_1 \cdot \cdots \cdot q_s$ les descomposicions en factors irreductibles de b i c respectivament. La descomposició de bc serà el producte de les dues anteriors. Per tant tindrem

$$qN = p_1 \cdot \cdots \cdot p_r \cdot q_1 \cdot \cdots \cdot q_s$$

i com la descomposició de bc és única i q és irreductible, q ha de coincidir amb algún dels factors anteriors. Per tant, o $q \mid b$ o $q \mid c$.

(ii) $\Rightarrow$ (i): Suposem que $a \in \mathcal{R}$ té dues descomposicions:

$$a = a_1 a_2 \dots a_n = b_1 b_2 \dots b_m,$$

on cada a_i i cada b_j són irreductibles i per tant, per hipòtesi, primers. Com que cada a_i divideix $\prod_j b_j$, ha de dividir a un d'ells, posem $b_{j(i)}$. Però com que $b_{j(i)}$ és irreductible, això implica que a_i i $b_{j(i)}$ són iguals tret de multiplicació per una unitat. Podem cancel·lar-los i continuar amb els altres factors. Finalment quan haurem cancel·lat tot els a_i s'han d'haver cancel·lat tots els b_j excepte unitats. Això demostra la unicitat de la descomposició.

□

Corol·lari 5.3. *Un domini Noetherià $\mathcal{R}$ és* UFD *sii en $\mathcal{R}$ tot irreductible és primer.*

Demostració. Per la proposició 4.8. □

Corol·lari 5.4 (PID $\Rightarrow$ UFD). *Tot domini d'ideals principals és factorial.*

Demostració. Tenint en compte el corol·lari 5.3, únicament caldrà provar que en un PID tot irreductible és primer.

Si a és irreductible i $a \mid bc$, si $a \nmid b$ llavors el $\gcd(a, b)$ és 1, ja que essent a irreductible l'únic divisor no unitari que admet és ell mateix llevat d'inversible. Per tant existeixen A, B tals que $Aa + Bb = 1$. Multiplicant per c resulta $Aac + Bbc = c$. Com a divideix els dos termes, necessàriament $a \mid c$ □

Proposició 5.5. *En un* UFD *sempre existeix el* gcd *i el* lcm. *A més:*

(i) *si les descomposicions en factors irreductibles (=primers) de a i b són*

$$a = \prod_i p_i^{\alpha_i}, \quad b = \prod_i p_i^{\beta_i},$$

llavors

$$\gcd(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)} \quad , \quad \operatorname{lcm}(a, b) = \prod_i p_i^{\max(\alpha_i, \beta_i)}.$$

(ii) $\gcd(a, b) \operatorname{lcm}(a, b) = a\, b$.

(iii) $\langle \operatorname{lcm}(a, b) \rangle = \langle a \rangle \cap \langle b \rangle$.

Observació 5.6. En un UFD no té perquè existir identitat de Bézout (tal com es pot observar en l'exercici 1.15); expressat en termes d'ideals, ja no és vàlida la fórmula $\langle a, b \rangle = \langle \gcd(a, b) \rangle$. En canvi si continua essent vàlida l'expressió corresponent pel lcm donada per (iii) de la proposició anterior, i a partir d'ella podem obtenir el gcd per l'apartat (ii).

DEFINICIÓ 5.7 (Contingut d'un polinomi). Sigui $p = \sum_{i=0}^{n} a_i x^i$ un polinomi sobre un UFD. Definim el **contingut** de p així:

$$\operatorname{cont}(p) = \gcd(a_0, \ldots, a_n)$$

Amb aquesta definició, traient factor comú $\operatorname{cont}(p)$, resulta

$$p = \operatorname{cont}(p)\, p_1, \quad \text{on} \quad \operatorname{cont}(p_1) = 1.$$

Direm també que p_1 és la **part primitiva** de p:

$$p_1 = \operatorname{primpart}(p).$$

LEMA 5.8. *Sigui $\mathcal{R}$ un* UFD *i $f, g \in \mathcal{R}[x]$. Llavors*

$$\operatorname{cont}(f\, g) = \operatorname{cont}(f) \operatorname{cont}(g).$$

DEMOSTRACIÓ. Si expressem $f = \operatorname{cont}(f)\, f_1$, $g = \operatorname{cont}(g)\, g_1$ amb $\operatorname{cont}(f_1) = 1$ i $\operatorname{cont}(g_1) = 1$, llavors tindrem:

$$f g = \operatorname{cont}(f) \operatorname{cont}(g)\, f_1\, g_1.$$

Hem de provar que $\operatorname{cont}(f_1\, g_1) = 1$. Posant

$$f_1 = \sum_{i=0}^{n} a_i x^i, \quad g_1 = \sum_{j=0}^{m} b_j x^j, \quad f_1\, g_1 = \sum_{k=0}^{n+m} c_k x^k$$

tindrem

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Només cal provar que si $p \in \mathcal{R}$ és primer, llavors no divideix algun c_k. Com que p no pot dividir tots els a_i ni tots els b_j, siguin i, j els primers indexos tals que $p \nmid a_i$ i $p \nmid b_j$. El coeficient de x^{i+j} és:

$$c_{i+j} = a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0$$

Per hipòtesi $p \mid a_s$ per $0 \le s < i$ i $p \mid b_s$ per $0 \le s < j$. Per tant, p divideix a tots els termes del segon membre excepte potser $a_i b_j$. Com p és primer i no divideix ni a_i ni b_j, tampoc divideix al producte. Per tant $p \nmid c_{i+j}$. □

LEMA 5.9 (Gauss). *Siguin $\mathcal{R}$ un* UFD *i $f \in \mathcal{R}[x]$, amb $\operatorname{cont}(f) = 1$. Llavors f és irreductible en $\mathcal{R}[x]$ ssi ho és a l'anell $\operatorname{Quot}(\mathcal{R})[x]$, on $\operatorname{Quot}(\mathcal{R})$ és el cos de fraccions de $\mathcal{R}$.*

DEMOSTRACIÓ. $\Rightarrow$: Suposem que $f \in \mathcal{R}[x]$ és reductible a $\operatorname{Quot}(\mathcal{R})[x]$. Anem a provar que també ho és a $\mathcal{R}[x]$.

En efecte, si $f = \tilde{g}\, \tilde{h}$, i $\tilde{g}, \tilde{h} \in \operatorname{Quot}(\mathcal{R})[x]$ de grau positiu en x (en cas contrari serien unitats), llavors, multiplicant per un cert $d \in \mathcal{R}$, obtenim

$$d\, f = g\, h$$

amb $g, h \in \mathcal{R}[x]$ del mateix grau que $\tilde{g}$ i $\tilde{h}$ respectivament. Pel lema 5.8, $d = \operatorname{cont}(g) \operatorname{cont}(h)$. Dividint $d\, f = g\, h$ per d obtenim

$$f = \frac{g\, h}{d} = \left(\frac{g}{\operatorname{cont}(g)}\right) \left(\frac{h}{\operatorname{cont}(h)}\right),$$

on ara els dos factors de la dreta pertanyen a $\mathcal{R}[x]$. Com que s'obtenen respectivament a partir de $\tilde{g}$ i $\tilde{h}$ multiplicant i dividint per elements de $\mathcal{R}$, continuen tenint grau positiu en x i no són unitats de $\mathcal{R}[x]$. Així f és reductible a $\mathcal{R}[x]$.

$\Leftarrow$: Suposem que $f \in \mathcal{R}[x]$ és reductible a $\mathcal{R}[x]$. Anem a provar que també ho és a $\mathrm{Quot}(\mathcal{R})[x]$. En efecte, si $f = g\,h$ en $\mathcal{R}[x]$, on g i h no són unitats de $\mathcal{R}[x]$, aquesta descomposició també és vàlida a $\mathrm{Quot}(\mathcal{R})[x]$. L'únic que hem de veure és que els factors no són unitaris a $\mathrm{Quot}(\mathcal{R})[x]$. De $\mathrm{cont}(f) = 1$, pel lema 5.8, deduïm que $\mathrm{cont}(g)$ i $\mathrm{cont}(h)$ són unitats de $\mathcal{R}$. Com que g i h no són unitats de $\mathcal{R}[x]$, han de tenir grau positiu en x i per tant tampoc són unitats de $\mathrm{Quot}(\mathcal{R})[x]$. □

Teorema 5.10 (Gauss). *Si $\mathcal{R}$ és un* UFD*, llavors $\mathcal{R}[x]$ també ho és.*

Demostració. Tenint en compte el lema 5.2 i l'exercici 1.20, només cal provar que si $\mathcal{R}$ és UFD llavors tot element irreductible $f \in \mathcal{R}[x]$ és primer.

Distingirem dos casos:

Cas 1: $\deg(f) = 0$. En aquest cas $f \in \mathcal{R}$ i per tant f també és irreductible en $\mathcal{R}$. Pel lema 5.2 f és primer en $\mathcal{R}$. Suposem ara que $f \mid g\,h$ on $g, h \in \mathcal{R}[x]$. Pel lema 5.8 resulta que $f \mid \mathrm{cont}(g)\,\mathrm{cont}(h)$, per tant $f \mid \mathrm{cont}(g)$ o $f \mid \mathrm{cont}(h)$. Però si $f \mid \mathrm{cont}(g)$ llavors $f \mid g$ i anàlogament per h.

Cas 2: $\deg(f) > 0$. Observem primer que $\mathrm{cont}(f) = 1$, altrament podriem descompondre $f = \mathrm{cont}(f)\,f_1$, amb $\mathrm{cont}(f_1) = 1$. Suposem que $f \mid g\,h$ a $\mathcal{R}[x]$. Pel lema de Gauss 5.9 f és irreductible a $\mathrm{Quot}(\mathcal{R})[x]$, que és un PID. Per tant f és primer en aquest domini i f divideix g o h a $\mathrm{Quot}(\mathcal{R})[x]$. Anem a veure que f també divideix g o h a $\mathcal{R}[x]$. Si $f\tilde{q} = g$ amb $\tilde{q} \in \mathrm{Quot}(\mathcal{R})[x]$, veiem que $\tilde{q}$ pertany de fet a $\mathcal{R}[x]$. Multiplicant per un $d \in \mathcal{R}$ convenient $q := d\tilde{q} \in \mathcal{R}[x]$. Així $fq = dg$, d'on $\mathrm{cont}\,(q) = d\,\mathrm{cont}(g)$. Per tant $d \mid \mathrm{cont}(q)$, i finalment

$$\tilde{q} = \frac{\mathrm{cont}(q)}{d}\,\frac{q}{\mathrm{cont}(q)} \in \mathcal{R}[x].$$

□

Corol·lari 5.11. *Si $\mathcal{R}$ és* UFD*, llavors l'anell de polinomis de n variables $\mathcal{R}[x_1, \ldots, x_n]$ també ho és.*

Demostració. Aplicant inducció al teorema 5.10. □

En la figura 1 podem veure un esquema de les implicacions en l'estructura dels dominis.

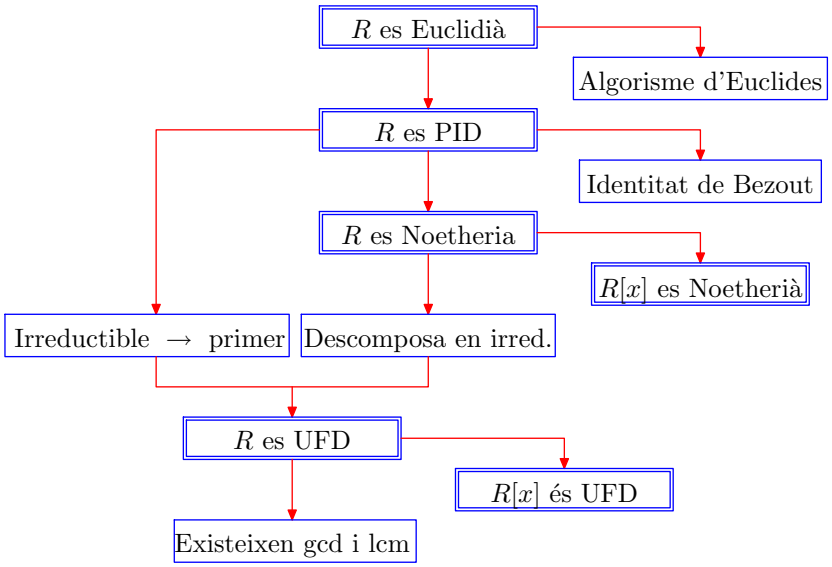


FIGURA 1. Dominis i implicacions

6. Espai afí

DEFINICIÓ 6.1 (Espai afí). Donat un cos K i un enter n, l'espai afí de dimensió n sobre K és

$$K^n = \{\overline{a} = (a_1, \ldots, a_n) : a_1, \ldots, a_n \in K\}.$$

Cada polinomi $f \in K[\overline{x}]$ defineix una funció polinòmica

$$\begin{array}{rccc} f: & K^n & \longrightarrow & K \\ & \overline{a} & \mapsto & f(\overline{a}), \end{array}$$

on $f(\overline{a})$ és el resultat de substituir $\overline{x}$ per $\overline{a}$ en l'expressió de f.

PROPOSICIÓ 6.2. *Si K és un cos infinit, i si $f \in K[\overline{x}]$, llavors $f = 0$ a $K[\overline{x}]$ ssi $f : K^n \to K$ és la funció nul·la.*

DEMOSTRACIÓ.

$\Rightarrow$: Obvi.

$\Leftarrow$: Ho provarem per inducció sobre el nombre de variables n.
Per $n = 1$, sabem que un polinomi de $K[x]$ no nul té un nombre finit de zeros, i per tant, si s'anul·la en infinits punts ha de ser el polinomi nul.
Sigui $f \in K[x_1, \ldots, x_n]$ un polinomi que s'anul·la sobre tot K^n. Podem escriure f en la forma

$$f = \sum_{i=0}^{N} g_i \, x_n^i$$

on cada $g_i \in K[x_1, \ldots, x_{n-1}]$. Anem a provar que cada g_i és el polinomi nul (de $n-1$ variables), el que implica que f és també el polinomi nul.
Fixem $(a_1, \ldots, a_{n-1}) \in K^{n-1}$. Per la hipòtesi sobre f, el polinomi

$$f(a_1, \ldots, a_{n-1}, x_n) \in K[x_n]$$

s'anul·la sobre tot K, per tant ha de ser el polinomi nul. Aquest fet implica que cada un dels coeficients de $f(a_1, \ldots, a_{n-1}, x_n)$ és nul, és a dir cada $g_i(a_1, \ldots, a_{n-1}) = 0$. Com que el punt $(a_1, \ldots, a_{n-1}) \in K^{n-1}$ era arbitrari, cada una de les funcions polinòmiques g_i s'anul·la idènticament sobre K^{n-1}. Per hipòtesi d'inducció cada g_i és el polinomi nul, i per tant també ho és f.

□

EXEMPLE 6.3. En canvi la proposició anterior no és certa en un cos finit. Posem per cas $K = \mathbb{F}_3$, i considerem el polinomi

$$f = x^3 - x = x(x-1)(x-2) \subset \mathbb{F}_3[x].$$

Òbviament f no és el polinomi nul, però la funció associada a f sí que és idènticament nul·la, ja que $f(0) = f(1) = f(2) = 0$.

7. Varietats Afins

DEFINICIÓ 7.1 (Varietats afins). Sigui $n \geq 1$, K un cos i B un subconjunt de $K[\overline{x}]$, on $\overline{x} = x_1, \ldots, x_n$. Definim

$$\mathbb{V}(B) := \{\overline{a} \in K^n \ : \ f(\overline{a}) = 0 \text{ per a tot } f \in B\}.$$

Els conjunts de la forma $\mathbb{V}(B)$, on $B \subseteq K[\overline{x}]$, reben el nom de *varietats afins*. Com que només parlarem de varietats afins ens estalviarem aquest adjectiu.

PROPOSICIÓ 7.2. *Si $\mathcal{I} = \langle B \rangle$ llavors $\mathbb{V}(\mathcal{I}) = \mathbb{V}(B)$, per tant, les varietats venen definides per ideals. En particular si $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ llavors $\mathbb{V}(\mathcal{I}) = \mathbb{V}(\{f_1, \ldots, f_m\})$, que per comoditat notarem $\mathbb{V}(f_1, \ldots, f_m)$.*

DEMOSTRACIÓ. Exercici. □

Pel teorema de la base de Hilbert, tot ideal de $K[\overline{x}]$ és finitament generat, per tant les varietats són sempre solucions d'un nombre finit d'equacions polinomials.

EXEMPLE 7.3. Els punts, les varietats lineals (les solucions d'un sistema lineal), les quàdriques i més en general les solucions d'una equació polinomial són varietats. La reunió de la paràbola $y = x^2$ amb la hipèrbola $xy = 1$ és una varietat. La cúbica guerxa definida per $V = \mathbb{V}(x^3 - z, x^2 - y)$ és una varietat de $\mathbb{R}^3$.

OBSERVACIÓ 7.4. Dos ideals diferents poden definir la mateixa varietat, per exemple $\langle x \rangle \neq \langle x^2 \rangle$ en canvi $\mathbb{V}(\langle x \rangle) = \mathbb{V}(\langle x^2 \rangle) = \{0\}$.

OBSERVACIÓ 7.5. Les varietats afins depenen del cos K. Exemple: $V = \mathbb{V}(x^2 + y^2)$.

(1) $V = \{(z, i\,z) : z \in \mathbb{C}\}$ a $\mathbb{C}^2$.
(2) $V = \{(0,0)\}$ a $\mathbb{R}^2$.
(3) $V = \{(0,0), (1,2), (2,1), (1,3), (3,1), (2,4), (4,2), (3,4), (4,3)\}$ a $\mathbb{Z}_5$.

PROPOSICIÓ 7.6. *Siguin $\mathcal{I}, \mathcal{J}$ ideals de $K[\overline{x}]$. Llavors:*

(i) $\mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I} \cdot \mathcal{J}) = \mathbb{V}(\mathcal{I}) \cup \mathbb{V}(\mathcal{J})$.
(ii) $\mathbb{V}(\mathcal{I} + \mathcal{J}) = \mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J})$.

DEMOSTRACIÓ. □

(i)$_a$ Provem que $\mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I} \cdot \mathcal{J})$.
- $\subseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I} \cap \mathcal{J})$ i $f \in \mathcal{I} \cdot \mathcal{J}$ és $f \in \mathcal{I} \cap \mathcal{J}$. Per tant $f(\overline{a}) = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{I} \cdot \mathcal{J})$.
- $\supseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I} \cdot \mathcal{J})$ i $f \in \mathcal{I} \cap \mathcal{J}$ és $f \in \mathcal{I}$ i $f \in \mathcal{J}$. Per tant $f^2 \in \mathcal{I} \cdot \mathcal{J}$ i $f^2(\overline{a}) = 0$. Per tant $f(\overline{a}) = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{I} \cap \mathcal{J})$.

(i)$_b$ Provem que $\mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I}) \cup \mathbb{V}(\mathcal{J})$.
- $\supseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I}) \cup \mathbb{V}(\mathcal{J})$ i $f \in \mathcal{I} \cap \mathcal{J}$ és $f \in \mathcal{I}$ i $f \in \mathcal{J}$. En conseqüència, tant si $\overline{a} \in \mathbb{V}(\mathcal{I})$ com si $\overline{a} \in \mathbb{V}(\mathcal{J})$ és $f(\overline{a}) = 0$ i, per tant, $\overline{a} \in \mathbb{V}(\mathcal{I} \cap \mathcal{J})$.
- $\subseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I} \cdot \mathcal{J})$ tal que $\overline{a} \notin \mathbb{V}(\mathcal{I})$ i $f \in \mathcal{J}$, podem trobar un $g \in \mathcal{I}$ tal que $g(\overline{a}) \neq 0$. Tindrem $fg \in \mathcal{I} \cdot \mathcal{J}$ i per tant $f(\overline{a})g(\overline{a}) = 0$. D'aquí resulta $f(\overline{a}) = 0$ i així $\overline{a} \in \mathbb{V}(\mathcal{J})$.

(ii)
- $\subseteq$: Si $\overline{a} \in \mathbb{V}(\mathcal{I} + \mathcal{J})$ llavors per tot $f \in \mathcal{I}$ és $f \in \mathcal{I} + \mathcal{J}$ i per tant $f(\overline{a}) = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{I})$. Anàlogament, per tot $g \in \mathcal{J}$ és $g \in \mathcal{I} + \mathcal{J}$ i per tant $g(\overline{a}) = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{J})$. Per tant resulta $\overline{a} \in \mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J})$.
- $\supseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J})$ és $\overline{a} \in \mathbb{V}(\mathcal{I})$ i $\overline{a} \in \mathbb{V}(\mathcal{J})$. Per tant, per tot $f \in \mathcal{I}$ i per tot $g \in \mathcal{J}$ és $f(\overline{a}) = 0$ i $g(\overline{a}) = 0$. Per tant, per tot $h = f + g \in \mathcal{I} + \mathcal{J}$ és $h(\overline{a}) = 0$. Resulta doncs que $\overline{a} \in \mathbb{V}(\mathcal{I} + \mathcal{J})$.

COROL·LARI 7.7. *Siguin $\mathcal{I} = \langle f_1, \ldots, f_r \rangle$ i $\mathcal{J} = \langle g_1, \ldots, g_s \rangle$. Tindrem $\mathbb{V}(\mathcal{I}) = \mathbb{V}(f_1, \ldots, f_s)$ i $\mathbb{V}(\mathcal{J}) = \mathbb{V}(g_1, \ldots, g_s)$. Per la proposició 1.13 resulta*

(i) $\mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J}) = \mathbb{V}(\mathcal{I} + \mathcal{J}) = \mathbb{V}(f_1, \ldots, f_r, g_1, \ldots, g_s)$.
(ii) $\mathbb{V}(\mathcal{I}) \cup \mathbb{V}(\mathcal{J}) = \mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I} \cdot \mathcal{J}) = \mathbb{V}(f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s)$,

EXEMPLE 7.8. Utilitzant el corol·lari anterior tenim

(1) $\mathbb{V}(x - x_1, y - y_1) = \mathbb{V}(x - x_1) \cap \mathbb{V}(y - y_1)$ que defineix un punt com intersecció de dues rectes.
(2) $\mathbb{V}(x^4 - xz, x^3 - xy) = \mathbb{V}(x(x^3 - z), x(x^2 - y)) = \mathbb{V}(x) \cup \mathbb{V}(x^3 - z, x^2 - y)$ que ens permet descompondre la varietat donada com unió del plá $x = 0$ i la cúbica guerxa.

8. La topologia de Zariski a K^n

Generalitzant la proposició 7.6 resulta la següent:

PROPOSICIÓ 8.1.

(i) *Si $\{\mathcal{I}_j : 1 \leq j \leq N\}$ és una col·lecció finita d'ideals de $K[\overline{x}]$, llavors*

$$\mathbb{V}\left(\bigcap_{j=1}^{N} \mathcal{I}_j\right) = \bigcup_{j=1}^{N} \mathbb{V}(\mathcal{I}_j).$$

(ii) *Si $\{\mathcal{I}_j \ : \ j \in J\}$ és una col·lecció d'ideals de $K[\overline{x}]$, llavors*

$$\mathbb{V}\left(\sum_{j\in J} \mathcal{I}_j\right) = \bigcap_{j\in J} \mathbb{V}(\mathcal{I}_j)$$

(iii) *Les varietats són tancades per unió finita i intersecció arbitrària.*

DEMOSTRACIÓ. .

(i) És la part (i) de la proposició 7.6. Cal fer notar, però, que la unió infinita de varietats no és en general una varietat. Considerem, per exemple, la sèrie d'ideals $I_j = \langle x - j\rangle$ per $j \in \mathbb{Z}$. Òbviament $\mathbb{V}(\bigcap_{j=1}^{N} I_j) = \langle (x-1)(x-2)\dots(x-N)\rangle$. Però no podem passar al límit ja que no hi ha cap polinomi que sigui producte d'infinits factors. La intersecció infinita dels ideals donarà l'ideal $\{0\}$. En canvi, la unió de varietats corresponents dona $\bigcup_{j=1}^{\infty} \mathbb{V}(I_j) = \{j \in \mathbb{Z} : j \geq 1\} \neq K$.

(ii) En canvi en la segona igualtat podem passar al límit, ja que $\sum_{j=1}^{1} \subseteq \dots \subseteq \sum_{j=1}^{N} \subseteq \dots$ formen una cadena ascendent d'ideals, que per ser $K[\overline{x}]$ Noetherià estaciona. Per tant, en el límit, tots dos membres estan ben definits i segueix complint-se la igualtat.

□

Recordem que una topologia sobre K^n es defineix donant els oberts, que han de ser una col·lecció de sub-conjunts de K^n tancats per intersecció finita, unió arbitrària i que continguin $\emptyset$ i K^n. Alternativament es pot definir a partir dels tancats (complementaris d'oberts).

Podem, doncs, definir una nova topologia a K^n donant una col·lecció de sub-conjunts de K^n, tancats per unió finita, intersecció arbitrària i que continguin $\emptyset$ i K^n.

COROL·LARI 8.2. *Les varietats de K^n són els tancats d'una topologia, que anomenarem* topologia de Zariski. *A la clausura topològica (adherència) d'un sub-conjunt A de K^n l'anomenarem* clausura de Zariski de A, *i la denotarem per $\overline{A}$.*

DEMOSTRACIÓ. Per la proposició anterior, només cal veure que $\emptyset$ i K^n són varietats: $\emptyset = \mathbb{V}(1)$ i $K^n = \mathbb{V}(0)$. □

Observem que, per definició, la clausura de Zariski de A és la mínima varietat que conté A.

PROPOSICIÓ 8.3. *Si K és $\mathbb{R}$ o $\mathbb{C}$, la topologia usual és més fina que la topologia de Zariski.*

DEMOSTRACIÓ. Exercici 1.23. □

9. Ideals de varietat. Correspondència Varietats - Ideals

DEFINICIÓ 9.1. Sigui $n \geq 1$, K un cos i A un sub-conjunt de K^n. Definim

$$\mathbb{I}(A) = \{f \in K[\overline{x}] : f(\overline{a}) = 0 \text{ per tot } \overline{a} \in A\}$$

Si $V \subset K^n$ és una varietat, a $\mathbb{I}(V)$ l'hi direm *l'ideal de varietat de V*.

PROPOSICIÓ 9.2. *Si $\mathcal{I}$ és un ideal de $K[\overline{x}]$ i V és una varietat de K^n, llavors*

(i) $\mathcal{I} \subseteq \mathbb{I}(\mathbb{V}(\mathcal{I}))$,
(ii) $V = \mathbb{V}(\mathbb{I}(V))$.

DEMOSTRACIÓ.

(i) Per tot $f \in \mathcal{I}$ i $\overline{a} \in \mathbb{V}(\mathcal{I})$ és $f(\overline{a}) = 0$, i per tant $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$.
(ii) $\subseteq$: Per tot $\overline{a} \in V$ i $f \in \mathbb{I}(V)$ és $f(\overline{a}) = 0$, i per tant $\overline{a} \in \mathbb{V}(\mathbb{I}(V))$.
$\supseteq$: Posem $V = \mathbb{V}(f_1, \ldots, f_s)$. Per tant, per cada i és $f_i \in \mathbb{I}(V)$. Així, per tot $\overline{a} \in \mathbb{V}(\mathbb{I}(V))$ i tot i tal que $1 \leq i \leq s$ és $f_i(\overline{a}) = 0$, resultant $\overline{a} \in V$.

□

OBSERVACIÓ 9.3. En canvi no és cert que si I és un ideal qualsevol, $\mathbb{I}(\mathbb{V}(I))$ sigui igual a I. Com assenyalàvem a l'observació 7.4, els ideals $\langle x^2 \rangle$ i $\langle x \rangle$ són diferents però defineixen la mateixa varietat $V = \{0\}$. Dels dos, $\langle x \rangle$ és l'ideal de la varietat V mentre que $\langle x^2 \rangle$ no ho és. No tots els ideals són ideals de varietat. L'apartat (i) de la proposició 9.2 ens diu que l'ideal de varietat és el màxim ideal que la defineix.

A les proposicions següents, considerem $\mathbb{I}$ i $\mathbb{V}$ com aplicacions, més exactament

$$\mathbb{I} : P(K^n) \to P(K[\overline{x}]),$$
$$\mathbb{V} : P(K[\overline{x}]) \to P(K^n),$$

on P indica les parts d'un conjunt.

PROPOSICIÓ 9.4. *Les aplicacions $\mathbb{I}$ i $\mathbb{V}$ són inverses respecte a la inclusió, és a dir, si $A', B' \subset K[x]$ i $A, B \subset K^n$ es verifica:*

(i) $A' \subseteq B' \Rightarrow \mathbb{V}(B') \subseteq \mathbb{V}(A')$
(ii) $A \subseteq B \Rightarrow \mathbb{I}(B) \subseteq \mathbb{I}(A)$

DEMOSTRACIÓ. □

(i) Per tot $b \in \mathbb{V}(B')$ i $f \in A'$, és $f \in B'$, i per tant $f(b) = 0$. Això implica que $b \in \mathbb{V}(A')$ i per tant $\mathbb{V}(B') \subseteq \mathbb{V}(A')$.

(ii) Per tot $f \in \mathbb{I}(B)$ i $a \in A$, és $a \in B$, i per tant $f(a) = 0$. Això implica que $f \in \mathbb{I}(A)$ i per tant $\mathbb{I}(B) \subseteq \mathbb{I}(A)$.

EXEMPLE 9.5.

(1) A R^3, $\mathbb{V}(x) \cap \mathbb{V}(y) \subset \mathbb{V}(x)$, és a dir la intersecció del pla $x = 0$ i el pla $y = 0$, que és l'eix z, está continguda en el pla $x = 0$. Pels ideals de varietat resulta

$$\langle x \rangle + \langle y \rangle = \langle x, y \rangle \supset \langle x \rangle.$$

(2) Anàlogament $\mathbb{V}(x) \cup \mathbb{V}(y) \supset \mathbb{V}(x)$, és a dir la unió del pla $x = 0$ i el pla $y = 0$ conté el plá $\mathbb{V}(x)$. Pels ideals de varietat resulta

$$\langle x \rangle \cap \langle y \rangle = \langle xy \rangle \subset \langle x \rangle.$$

LEMA 9.6. *Siguin $A \subseteq K^n$ i $B \subseteq K[\overline{x}]$. Es té*

(i) $A \subseteq \mathbb{V} \circ \mathbb{I}(A)$
(ii) $B \subseteq \mathbb{I} \circ \mathbb{V}(B)$.
(iii) $\mathbb{I} \circ \mathbb{V} \circ \mathbb{I} = \mathbb{I}$.
(iv) $\mathbb{V} \circ \mathbb{I} \circ \mathbb{V} = \mathbb{V}$.

DEMOSTRACIÓ.

(i) Per tot $a \in A$ i $f \in \mathbb{I}(A)$ és $f(a) = 0$. Això implica que $a \in \mathbb{V}(\mathbb{I}(A))$.
(ii) Per tot $f \in B$ i $a \in \mathbb{V}(B)$ és $f(a) = 0$. Això implica que $f \in \mathbb{I}(\mathbb{V}(B))$.
(iii) $\subseteq$: Aplicant $\mathbb{I}$ als dos membres de (i) i tenint en compte la proposició 9.4 resulta $\mathbb{I}(A) \supseteq \mathbb{I} \circ \mathbb{V} \circ \mathbb{I}(A)$.
$\supseteq$: Posant $B = \mathbb{I}(A)$ en (ii) resulta $\mathbb{I}(A) \subseteq \mathbb{I} \circ \mathbb{V} \circ \mathbb{I}(A)$.
(iv) $\subseteq$: Aplicant $\mathbb{V}$ als dos membres de (ii) i tenint en compte la proposició 9.4 resulta $\mathbb{V}(B) \supseteq \mathbb{V} \circ \mathbb{I} \circ \mathbb{V}(B)$.
$\subseteq$: Posant $A = \mathbb{V}(B)$ en (i) resulta $\mathbb{V}(B) \subseteq \mathbb{V} \circ \mathbb{I} \circ \mathbb{V}(B)$.

□

COROL·LARI 9.7.

(i) *Les varietats són la imatge de $\mathbb{V}$ i els ideals de varietat són la imatge de $\mathbb{I}$.*
(ii) *$\mathbb{I}$ i $\mathbb{V}$ són bijeccions, l'una inversa de l'altra, entre varietats de K^n i ideals de varietat de $K[\overline{x}]$. A més, inverteixen la inclusió, tal com veiem a la proposició 9.4*

Però cal recordar que no tots els ideals són ideals de varietat!

PROPOSICIÓ 9.8. *Si $A \subseteq K^n$, la varietat més petita que conté A és $\mathbb{V}(\mathbb{I}(A))$, que no és altre cosa que la clausura de Zariski de A:*

$$\overline{A} = \mathbb{V}(\mathbb{I}(A))$$

DEMOSTRACIÓ. Com que $\mathbb{V}(\mathbb{I}(A))$ és varietat, només cal provar que és la mínima que conté A: si $A \subseteq \mathbb{V}(\mathcal{I})$ llavors $\mathbb{I}(A) \supseteq \mathbb{I}(\mathbb{V}(\mathcal{I}))$ d'on $\mathbb{V}(\mathbb{I}(A)) \subseteq \mathbb{V}(\mathbb{I}(\mathbb{V}(\mathcal{I}))) = \mathbb{V}(\mathcal{I})$. □

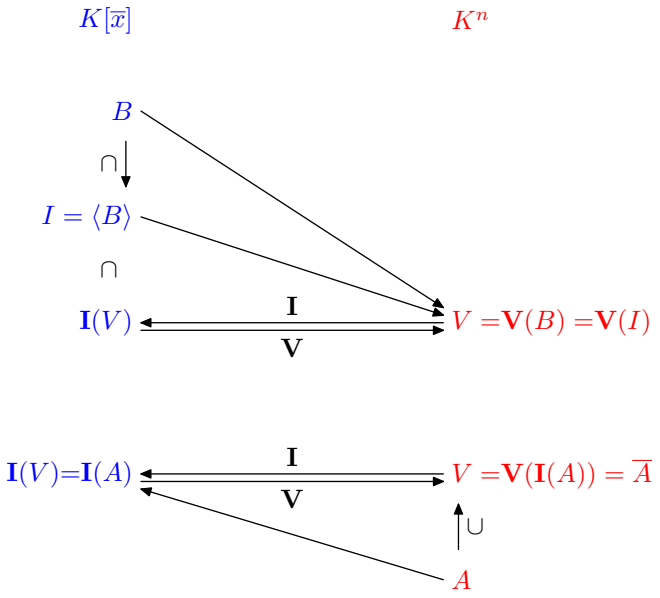


FIGURA 2. Correspondència Ideals - Varietats

Resumint, un conjunt $B \subseteq K[\overline{x}]$ determina una varietat $V = \mathbb{V}(B)$. Però aquesta varietat és la mateixa que la associada a l'ideal $\mathcal{I} = \langle B \rangle$. És a dir, $V = \mathbb{V}(\mathcal{I})$. V també està determinada per altres ideals.
Però a una varietat V li correspon un únic ideal de varietat $\mathbb{I}(V)$, que és el màxim ideal que la defineix. Recíprocament, a l'ideal de la varietat $\mathbb{I}(V)$ li correspon la varietat V. Les aplicacions $\mathbb{V}$ i $\mathbb{I}$ són bijeccions inversa la una de l'altre entre varietats i ideals de varietat.
D'altra banda, un conjunt de punts $A \subseteq K^n$ li correspon una varietat $\overline{A}$ que és la clausura de Zariski de A i que és la varietat més petita que conté A. La clausura $\overline{A}$ s'obté fent $\overline{A} = \mathbb{V}(\mathbb{I}(A))$.
L'esquema de la figura 2 ilustra les relacions.

PROPOSICIÓ 9.9. *Si V, W són varietats de K^n i $\mathcal{I}, \mathcal{J}$ són ideals de $K[\overline{x}]$, llavors:*

(i) $\mathbb{I}(V) \cap \mathbb{I}(W) = \mathbb{I}(V \cup W)$. *La intersecció d'ideals de varietat és ideal de varietat (de la unió).*
(ii) $\mathbb{I}(V) + \mathbb{I}(W) \subsetneq \mathbb{I}(V \cap W)$. *La suma d'ideals de varietat no sempre és ideal de varietat.*
(iii) $V = W$ *sii* $\mathbb{I}(V) = \mathbb{I}(W)$; $V \subseteq W$ *sii* $\mathbb{I}(W) \subseteq \mathbb{I}(V)$ *i* $V \subset W$ *sii* $\mathbb{I}(W) \subset \mathbb{I}(V)$.
(iv) $\mathcal{I}$ *i* $\mathcal{J}$ *defineixen la mateixa varietat sii* $\mathbb{IV}(\mathcal{I}) = \mathbb{IV}(\mathcal{J})$.

DEMOSTRACIÓ.

(i) Per tot $f \in \mathbb{I}(V \cup W)$ és $f \in \mathbb{I}(V)$ i $f \in \mathbb{I}(W)$. Per tant $f \in \mathbb{I}(V) \cap \mathbb{I}(W)$. El raonament és invertible.
(ii) Per tot $h \in \mathbb{I}(V) + \mathbb{I}(W)$ existeixen $f \in \mathbb{I}(V)$ i $g \in \mathbb{I}(W)$ tals que $h = f + g$. Per tant $f \in \mathbb{I}(V \cap W)$ i $g \in \mathbb{I}(V \cap W)$, resultant que també $h = f + g \in \mathbb{I}(V \cap W)$.
En canvi la inclusió en sentit contrari no és certa. Posem un contraexemple: Considerem les varietats de $\mathbb{C}^2$ següents: $V = \mathbb{V}(y)$ i $W = \mathbb{V}(y - x^2)$. Òbviament $\mathbb{I}(V) = \langle y \rangle$ i $\mathbb{I}(W) = \langle y - x^2 \rangle$. Tindrem

$$\mathbb{I}(V) + \mathbb{I}(W) = \langle y, x^2 \rangle \subsetneq \langle y, x \rangle = \mathbb{I}(V \cap W).$$

(iii) Siguin $V = \mathbb{V}(\mathcal{I})$ i $W = \mathbb{V}(\mathcal{J})$. Si $V = W$ clarament $\mathbb{I}(\mathbb{V}(\mathcal{I})) = \mathbb{I}(\mathbb{V}(\mathcal{J}))$, i per tant $\mathbb{I}(V) = \mathbb{I}(W)$. Recíprocament, si $\mathbb{I}(V) = \mathbb{I}(W)$ llavors $\mathbb{V}(\mathcal{I}) = \mathbb{V}\mathbb{I}\mathbb{V}(\mathcal{I}) = \mathbb{V}\mathbb{I}\mathbb{V}(\mathcal{J}) = \mathbb{V}(\mathcal{J})$ i per tant $V = W$.
La inclusió estricte i no estricte es demostren de la mateixa manera.
(iv) És immediat a partir de (iii) posant $V = \mathbb{V}(\mathcal{I})$ i $W = \mathbb{V}(\mathcal{J})$.

□

PROPOSICIÓ 9.10. *Sigui $P = (a_1, \ldots, a_n)$ un punt de $\mathbb{R}^n$. Llavors $\mathbb{I}(P) = \langle x_1 - a_1, \ldots, x_n - a_n \langle$. L'ideal de varietat d'un punt P està generat pels polinomis $x_i - a_i$ per $1 \leq i \leq n$.*

DEMOSTRACIÓ. En primer lloc, òbviament $x_i - a_i \in \mathbb{I}(P)$. Per altra banda sigui $f \in \mathbb{I}(P)$ qualsevol. Emprant la fórmula de Taylor per n variables tenim

$$f(\overline{x}) = f(\overline{a}) + \sum_{1 \leq i_1 + \cdots + i_n \leq N} c_{i_1 \ldots i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n},$$

on N és el grau del polinomi i les $c_{i_1 \ldots i_n}$ són els valors de les derivades parcials de f en el punt $\overline{a}$ afectades d'un coeficient numèric. Tenint en compte que si $f \in \mathbb{I}(P)$ és $f(\overline{a}) = 0$, resulta $f \in \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

10. Ideals i Radicals

DEFINICIÓ 10.1 (Ideal radical). Donat un ideal $\mathcal{I}$, diem que és radical, ssi

$$f^m \in \mathcal{I} \Longrightarrow f \in \mathcal{I}$$

DEFINICIÓ 10.2. (Radical d'un ideal) Donat un ideal $\mathcal{I}$ definim el *radical de $\mathcal{I}$* per:

$$\sqrt{\mathcal{I}} = \{f : \exists m \in \mathbb{N}, f^m \in \mathcal{I}\}$$

PROPOSICIÓ 10.3. *Donat un ideal $\mathcal{I}$ de l'anell $\mathcal{R}$, es té:*

(i) *$\sqrt{\mathcal{I}}$ és un ideal.*
(ii) *$\sqrt{\mathcal{I}}$ és un ideal radical.*

(iii) *Si $\mathcal{I} = \langle f \rangle \subset \mathcal{R}$, on $\mathcal{R}$ és un UFD, i la descomposició de f en factors irreductibles és $f = f_1^{a_1} \cdots f_s^{a_s}$, llavors*

$$\sqrt{\mathcal{I}} = \langle f_{red} \rangle \quad \text{on} \quad f_{red} = f_1 \cdots f_s$$

(iv) $\mathcal{I} \subseteq \sqrt{\mathcal{I}}$.

(v) *Si $\mathcal{I} \subset K[\overline{x}]$, on K és un cos qualsevol, llavors $\sqrt{\mathcal{I}} \subseteq \mathbb{I}(\mathbb{V}(\mathcal{I}))$.*

(vi) $\sqrt{\sqrt{\mathcal{I}}} = \sqrt{\mathcal{I}}$.

Nota: Més endavant veurem com el Nullstellensatz demostra que si K és algebraicament tancat, llavors (v) esdevé una igualtat.

Demostració. .

(i) Si $f, g \in \sqrt{\mathcal{I}}$, llavors existeixen m, n tals que $f^m, g^n \in \mathcal{I}$. Per tant:

$$\begin{aligned}(f+g)^{m+n} &= \sum_{i=0}^{m+n} \binom{m+n}{i} f^i g^{m+n-i} \\ &= \sum_{i=0}^{m} \binom{m+n}{i} f^i g^n g^{m-i} \\ &+ \sum_{i=m+1}^{m+n} \binom{m+n}{i} f^m f^{i-m} g^{m+n-i} \in \mathcal{I}\end{aligned}$$

i per tant $f + g \in \sqrt{\mathcal{I}}$.

A més, si $f \in \sqrt{\mathcal{I}}$ i $h \in \mathcal{R}$, llavors existeix m tal que $f^m \in \mathcal{I}$ i per tant $(fh)^m = f^m h^m \in \mathcal{I}$. En conseqüència resulta que $fh \in \sqrt{\mathcal{I}}$.

(ii) Si $f^m \in \sqrt{\mathcal{I}}$, existeix n tal que $f^{mn} \in \mathcal{I}$ i per tant $f \in \sqrt{\mathcal{I}}$. Per tant, $\sqrt{\mathcal{I}}$ és radical.

(iii) Si $A = \sup_k(a_k)$, està clar que $f_{red}^A \in \langle f \rangle$ i per tant $f_{red} \in \sqrt{\mathcal{I}}$. Recíprocament, suposem que $g^B \in \mathcal{I}$. Això implica que $g^B = h\, f$ per algún h. Sigui $g = g_1^{b_1} \cdots g_r^{b_r}$ la factorització de g. Llavors s'ha de cumplir

$$g_1^{b_1 B} \cdots g_r^{b_r B} = h f_1^{a_1} \cdots f_s^{a_s}$$

Per la factorització única els factors irreductibles d'ambdós membres han de ser idèntics (excepte constants). Com els $f_1, \ldots, f_s$ són irreductibles, cada f_i, $1 \leq i \leq r$, ha de ser igual a algún g_j multiplicat per una unitat. En conseqüència g és un múltiple de f_{red} i g està contingut a $\langle f_{red} \rangle$, amb el que queda provada la igualtat $\sqrt{\mathcal{I}} = \langle f_{red} \rangle$.

(iv) Si $f \in \mathcal{I}$, llavors $f^1 \in \mathcal{I}$, i per tant $f \in \sqrt{\mathcal{I}}$.

(v) Si $f \in \sqrt{\mathcal{I}}$ llavors per un cert m és $f^m \in \mathcal{I}$, i f^m s'anul.la sobre $\mathbb{V}(\mathcal{I})$. Per tant, f s'anul.la sobre $\mathbb{V}(\mathcal{I})$ i $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$.

(vi) La inclusió $\supseteq$ és obvia per (iv). Recíprocament, si $f \in \sqrt{\sqrt{\mathcal{I}}}$, llavors existeix m tal que $f^m \in \sqrt{\mathcal{I}}$ i per tant $f \in \sqrt{\mathcal{I}}$ ja que $\sqrt{\mathcal{I}}$ és radical.

□

PROPOSICIÓ 10.4. *Siguin $\mathcal{I}$ i $\mathcal{J}$ ideals. Llavors*

$$\sqrt{\mathcal{I} \cap \mathcal{J}} = \sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}}$$

DEMOSTRACIÓ. .

⇒: Si $f \in \sqrt{\mathcal{I} \cap \mathcal{J}}$, llavors existeix un m tal que $f^m \in \mathcal{I} \cap \mathcal{J}$. Per tant $f^m \in \mathcal{I}$ i $f \in \sqrt{\mathcal{I}}$, i anàlogament per $\mathcal{J}$. Per tant $f \in \sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}}$.

⇐: Si $f \in \sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}}$, llavors existeixen enters positius n, m tals que $f^n \in \mathcal{I}$ i $f^m \in \mathcal{J}$. Per tant, $f^{\sup(n,m)} \in \mathcal{I} \cap \mathcal{J}$ i per tant $f \in \sqrt{\mathcal{I} \cap \mathcal{J}}$.

□

11. Quocient d'ideals i diferència de varietats

DEFINICIÓ 11.1. Es defineix el quocient d'ideals $\mathcal{I} : \mathcal{J}$ d'un anell $\mathcal{R}$ com

$$\mathcal{I} : \mathcal{J} = \{f \in \mathcal{R} \ : \ \text{per tot } g \in \mathcal{J}, \text{ és } fg \in \mathcal{I}\}.$$

és a dir, com el conjunt dels elements de l'anell que multiplicats per qualsevol element de $\mathcal{J}$ pertanyen a $\mathcal{I}$.

PROPOSICIÓ 11.2. *Siguin $\mathcal{I}$ i $\mathcal{J}$ ideals d'un anell $\mathcal{R}$. Es verifiquen*

(1) $\mathcal{I} : \mathcal{J}$ *és un ideal,*
(2) $\mathcal{I} \subseteq \mathcal{I} : \mathcal{J}$,
(3) $\mathcal{I} : \langle 1 \rangle = \mathcal{I}$,
(4) $\mathcal{I} : \mathcal{I} = \langle 1 \rangle$,
(5) $\mathcal{I} \cdot \mathcal{J} \subseteq (\mathcal{I} : \mathcal{J}) \cdot \mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$,
(6) $(\mathcal{I} \cdot \mathcal{J}) : \mathcal{J} \supseteq \mathcal{I}$,
(7) *Si $\mathcal{R}$ és un domini, llavors*

$$\langle p_1 q, \ldots, p_r q \rangle : \langle q \rangle = \langle p_1, \ldots, p_r \rangle.$$

Aquesta proposició figura com exercici 1.26 amb aclariments.

PROPOSICIÓ 11.3. *Si V i W són varietats de K^n es té:*

$$\mathbb{I}(V \setminus W) = \mathbb{I}(V) : \mathbb{I}(W).$$

DEMOSTRACIÓ.

⊆: Per tot $f \in \mathbb{I}(V \setminus W)$ i $g \in \mathbb{I}(W)$ i $\overline{a} \in V$ és $f(\overline{a})g(\overline{a}) = 0$, ja que si $\overline{a} \in V \setminus W$ és $f(\overline{a}) = 0$ i si $\overline{a} \in W$ és $g(\overline{a}) = 0$. Per tant és $fg \in \mathbb{I}(V)$, i així $f \in \mathbb{I}(V) : \mathbb{I}(W)$.

⊇: Per tot $f \in \mathbb{I}(V) : \mathbb{I}(W)$ i $\overline{a} \in V \setminus W$, prenem $g \in \mathbb{I}(W)$ tal que $g(\overline{a}) \neq 0$. Llavors $fg \in \mathbb{I}(V)$ i per tant s'anul·la en $\overline{a}$, d'on $f(\overline{a}) = 0$, i $f \in \mathbb{I}(V \setminus W)$.

□

12. Parametrització i descomposició de varietats en irreductibles

DEFINICIÓ 12.1 (Varietat irreductible). Una varietat V es diu irreductible si $V = V_1 \cup V_2$ on V_1 i V_2 són varietats, implica que o bé $V = V_1$ o bé $V = V_2$.

PROPOSICIÓ 12.2. *V és irreductible ssi $V \subseteq V_1 \cup \cdots \cup V_r$ implica que $V \subseteq V_i$ per algún $1 \leq i \leq r$.*

DEMOSTRACIÓ. Exercici 1.28 □

PROPOSICIÓ 12.3 (Descomposició d'una varietat en irreductibles). *Tota varietat descompon com a unió de varietats irreductibles. Si a més demanem que la descomposició sigui irredundant (és a dir, no n'hi hagi cap continguda en una altra) llavors la descomposició és única. És a dir, decompon de forma única com*

$$V = V_1 \cup V_2 \cup \cdots \cup V_k,$$

on cada V_i és irreductible i $V_i \nsubseteq V_j$ per $i \neq j$.

DEMOSTRACIÓ. L'existència de la descomposició és conseqüència de la Noetherianitat. Si V no és irreductible llavors $V = V_1 \cup V_2$, amb $V_i \subset V$ per $i = 1, 2$. Si V_1 i V_2 són irreductibles ja hem acabat, sinó descomponem les que no ho siguin iterativament. Així, si $V_{i_1,\ldots i_k}$ no és irreductible, tindrem $V_{i_1,\ldots i_k} = V_{i_1\ldots i_k 1} \cup V_{i_1\ldots i_k 2}$ amb $V_{i_1\ldots i_k j} \subset V_{i_1\ldots i_k}$ per $j = 1, 2$. Descomponem fins que totes les varietats finals siguin irreductibles. Ara provem que aquesta descomposició necessàriament acaba. Altrament tindríem cadenes infinites estrictament descendents de varietats seguint les branques $V \supset V_{i_1} \supset V_{i_1 i_2} \supset \cdots \supset V_{i_1 i_2 \ldots i_k} \supset \ldots$, que per la Noetherianitat de $K[\overline{x}]$ és impossible. Ara podem eliminar de la descomposició les varietats redundants (si alguna $V_i \subseteq V_j$ en la descomposició, podem eliminar V_i), i obtenir una descomposició irredundant. Per tal de veure la unicitat, suposem que existissin dues descomposicions irredundants. Tindríem $V_1 \cup \cdots \cup V_k = W_1 \cup \cdots \cup W_r$ cap d'elles irredundant, és a dir $V_i \nsubseteq V_j$ i $W_i \nsubseteq W_j$ per $i \neq j$. Per irreductibilitat, de $V_i \subseteq W_1 \cup \cdots \cup W_r$ deduïm que existeix $\varphi(i) \in \{1, \ldots, r\}$ de manera que $V_i \subseteq W_{\varphi(i)}$. Inversament, veiem que donat $j \in \{1, \ldots, r\}$ existeix $\rho(j) \in \{1, \ldots, k\}$ de manera que $W_j \subseteq V_{\rho(j)}$. Així $V_i \subseteq W_{\varphi(i)} \subseteq V_{\rho\circ\varphi(i)}$, i per irredundància deduïm $i = \rho \circ \varphi(i)$ i $V_i = W_{\varphi(i)}$. Deduïm $\varphi \circ \rho = \mathrm{Id}$, és a dir φ és una bijecció i $V_i = W_{\varphi(i)}$. □

TEOREMA 12.4. *V és irreductible sii $\mathbb{I}(V)$ és primer.*

DEMOSTRACIÓ.

- $\Rightarrow$: Si V és irreductible i $fg \in \mathbb{I}(V)$ llavors $V = \mathbb{V}\mathbb{I}(V) \subseteq \mathbb{V}(fg) = \mathbb{V}(f) \cup \mathbb{V}(g)$. Per ser V irreductible, la proposició 12.2 implica que $V \subseteq \mathbb{V}(f)$ o $V \subseteq \mathbb{V}(g)$, i per tant o $f \in \mathbb{I}(V)$ o $g \in \mathbb{I}(V)$.
- $\Leftarrow$: Recíprocament, si $\mathbb{I}(V)$ és primer i $V \subseteq V_1 \cup V_2$ llavors $\mathbb{I}(V) \supseteq \mathbb{I}(V_1 \cup V_2) = \mathbb{I}(V_1) \cap \mathbb{I}(V_2) \supseteq \mathbb{I}(V_1) \cdot \mathbb{I}(V_2)$. Per la primalitat de $\mathbb{I}(V)$ i l'exercici 1.8 o $\mathbb{I}(V_1) \subseteq \mathbb{I}(V)$ o $\mathbb{I}(V_2) \subseteq \mathbb{I}(V)$. Per tant, o $V \subseteq V_1$ o $V \subseteq V_2$, i V és irreductible.

□

PROPOSICIÓ 12.5. *Si K és un cos infinit i V és una varietat de K^n, llavors $\overline{K^n \setminus V} = K^n$.*

DEMOSTRACIÓ. Exercici 1.27 □

DEFINICIÓ 12.6. Una *parametrització* és una aplicació

$$\begin{array}{rccc} F: & A \subseteq K^m & \longrightarrow & K^n \\ & \bar{t} & \mapsto & F(\bar{t}) = (f_1(\bar{t}), \ldots, f_n(\bar{t})) \end{array}$$

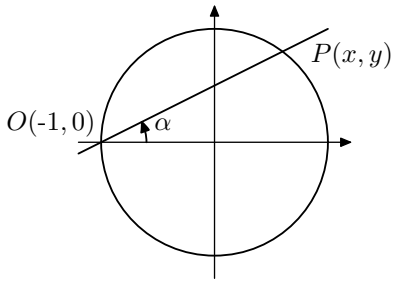
on, com és habitual, $\bar{t} = t_1, \ldots, t_m$. Entendrem que la *varietat V definida per la parametrització F* és la *clausura de Zariski de la imatge de F*, és a dir

$$V = \overline{F(A)} = \mathbb{VI}(F(A)).$$

Dos casos importants són les parametritzacions polinomials i les racionals. Una *parametrització polinomial* és aquella que ve definida component a component per funcions polinomials, és a dir, $f_1, \ldots, f_n \in K[\bar{t}]$. Observem que en aquest cas F está definida sobre tot K^m. Una *parametrització racional* és aquella que ve definida component a component per funcions racionals, és a dir, $f_1, \ldots, f_n \in K(\bar{t})$. Observem que si $f_i = f_i^N / f_i^D$ amb $f_i^N, f_i^D \in K[\bar{t}]$, llavors $F : K^m \setminus \mathbb{V}(f_1^D \cdots f_n^D) \to K^n$.

En general $\overline{F(A)}$ no té perquè coincidir amb $F(A)$, com es pot veure a l'exemple següent.

EXEMPLE 12.7. Parametrització de la circumferència $x^2 + y^2 = 1$. Considerem una recta de pendent m que passa pel punt $O(-1, 0)$.



Parametrització de la circumferència: $\tan \alpha = m$

El punt $P(x, y)$ de tall amb la circumferència verifica el sistema

$$\left.\begin{array}{l} y = m(x+1) \\ x^2 + y^2 = 1 \end{array}\right\}$$

d'on resulta $(x+1)(x-1) + m^2(x+1)) = 0$. Per tant, a les coordenades de P són:

$$\begin{array}{rcl} x & = & \dfrac{1 - m^2}{m^2 + 1} \\ y & = & \dfrac{2m}{m^2 + 1} \end{array}$$

que és una parametrització racional de la circumferència. Podem observar, que el punt $O(-1,0)$ no queda parametritzat (correspon a $m = \pm\infty$). Si anomenem $\mathcal{C}$ als punts de la circumferència i $(x,y) = F(m)$ a la parametrització tenim $F(\mathbb{R}) = \mathcal{C} \setminus \{O\}$ i $\overline{F(\mathbb{R})} = \mathcal{C}$. Per tant la varietat definida per la parametrització és la circumferència.

PROPOSICIÓ 12.8 (Irreductibilitat d'una parametrització). *Si K és infinit, tota varietat definida per una parametrització racional és irreductible.*

DEMOSTRACIÓ. Sigui la parametrització $F = (f_1, \ldots, f_n)$ on $f_i = f_i^N / f_i^D$, i $f_i^N, f_i^D \in K[\bar{t}]$. Sigui $W := \mathbb{V}(f_1^D \cdots f_n^D)$. La varietat definida per la paramterització és $V = \overline{F(K^m \setminus W)} = \mathbb{VI}(F(K^m \setminus W))$. Per tant, el seu ideal de varietat és $\mathbb{I}\left(\overline{F(K^m \setminus W)}\right) = \mathbb{IVI}(F(K^m \setminus W)) = \mathbb{I}(F(K^m \setminus W))$. Per provar que V és irreductible cal demostrar que $\mathbb{I}(F(K^m \setminus W))$ és primer. Si $g_0 = g_1 g_2 \in \mathbb{I}(F(K^m \setminus W))$, llavors la funció definida per la fracció racional $g_0(f_1, \ldots, f_n) \in K(\bar{t})$ s'anula idènticament sobre $K^m \setminus W$. Si escrivim $g_i(f_1, \ldots, f_n) = g_i^N / g_i^D$, amb $g_i^N, g_i^D \in K[\bar{t}]$ per $i = 1, 2$ llavors $g_0(f_1, \ldots, f_n) = \dfrac{g_1^N g_2^N}{g_1^D g_2^D}$. Així $g_1^N(\bar{t}) g_2^N(\bar{t})$ s'anul·la a $K^m \setminus W$. Com és un polinomi s'anul·la també a la clausura $\overline{K^m \setminus W}$, i per ser K infinit i l'exercici 1.27 deduïm que $g_1^N(\bar{t}) g_2^N(\bar{t}) = 0$ a K^m i per tant també és zero com a polinomi. Per tant $g_1^N = 0$ ó $g_2^N = 0$. Això implica que $g_1(\overline{x})$ ó $g_2(\overline{x})$ s'anul·len sobre tots els punts de $F(K^m \setminus W)$, i per tant, $g_1 \in \mathbb{I}(F(K^m \setminus W))$ ó $g_2 \in \mathbb{I}(F(K^m \setminus W))$ i l'ideal és primer. □

EXEMPLE 12.9. Considerem la varietat $V = \mathbb{V}(y^3 - x^2) \subset \mathbb{C}^2$. Ens preguntem si és irreductible.

Podem parametritzar-la per $(x = t^3, y = t^2)$. Comprovem, en primer lloc que els punts que parametritza estan a V: $y^3(t) - x^2(t) = t^6 - t^6 = 0$. Provem ara que parametritza tots els punts (o alternativament que la clausura del conjunt parametritzat és tota V). Per això, per tot y, determinem els punts de V. Tindrem

$$\begin{aligned} x^2 &= y^3 \\ x &= |y|^{\frac{3}{2}}\, \mathbf{e}^{i\frac{3}{2}\arg(y)} \mathbf{e}^{ik\pi}, \quad k = 0, 1 \end{aligned}$$

Ara, per tot y, determinem els punts parametritzats.

$$\begin{aligned} y &= t^2 \\ t &= |y|^{\frac{1}{2}}\, \mathbf{e}^{i\frac{1}{2}\arg(y)} \mathbf{e}^{ik'\pi} \quad k' = 0, 1 \\ x &= |y|^{\frac{3}{2}}\, \mathbf{e}^{i\frac{3}{2}\arg(y)} \mathbf{e}^{ik'\pi} \end{aligned}$$

i tots els punts estan parametritzats.

EXEMPLE 12.10. Per comprovar que cal anar amb compte, considerem ara la varietat $V = \mathbb{V}(z^3 - x^5, y^3 - x^2) \subset \mathbb{C}^3$. Ens preguntem també si és irreductible.

A primera vista trobem fàcilment una parametrització $x = t^3, y = t^2, z = t^5$, que podem anomenar $F_0(t)$. Òbviament tots els punts parametritzats

estan a V: $z^3(t) - x^5(t) = t^{15} - t^{15} = 0$ i $y^3(t) - x^2(t) = t^6 - t^6 = 0$. Però comprovem ara que no tots els punts de V estan parametritzats.

En primer lloc $V = \mathbb{V}(z^3 - x^5, y^3 - x^2) = \mathbb{V}(z^3 - x^3y^3, y^3 - x^2)$. A partir de la descomposició $z^3 - x^3y^3 = (z - xy)(z - xy\mathbf{e}^{i\frac{2}{3}\pi})(z - xy\mathbf{e}^{i\frac{4}{3}\pi})$, es pot descompondre V en unió de tres varietats $V_0 = \mathbb{V}(z - xy, y^3 - x^2)$, $V_1 = \mathbb{V}(z - xy\mathbf{e}^{i\frac{2}{3}\pi}, y^3 - x^2)$, $V_2 = \mathbb{V}(z - xy\mathbf{e}^{i\frac{4}{3}\pi}, y^3 - x^2)$, i la parametrització F_0 únicament parametritza V_0 com pot comprovar-se, però no les altres dues, que tenen també parametritzacions obvies.

13. Exercicis

Secció 1.

EXERCICI 1.1. Sigui $\mathcal{R}$ un anell. Proveu que

a) $0\,a = 0$
b) $(-1)\,a = -a$.

EXERCICI 1.2. Proveu que, en un domini $\mathcal{R}$,

a) si un element $u \in \mathcal{R}$ té invers multiplicatiu, llavors és únic; es denota $v = u^{-1}$, i s'anomena **invers** de u; (Els elements que tenen invers s'anomenen **unitats** del domini.)
b) el conjunt de les unitats de $\mathcal{R}$ és un grup multiplicatiu.

EXERCICI 1.3. Proveu que $\mathcal{R}$ és un domini ssi $a\,b = a\,c$, $a \neq 0 \Longrightarrow b = c$.

EXERCICI 1.4. Sigui $S = \{s_1, \ldots, s_n\}$. Proveu que $\langle S \rangle$ és el mínim ideal que conté S.

EXERCICI 1.5. Donats un anell commutatiu $\mathcal{R}$ i un ideal $\mathcal{I} \subseteq \mathcal{R}$, proveu que si en el grup quocient $\mathcal{R}/\mathcal{I}$ definit per

$$\begin{aligned} [a]_{\mathcal{I}} &= \{b :\ b \in \mathcal{R},\ b - a \in \mathcal{I}\} \\ \mathcal{R}/\mathcal{I} &= \{[a]_{\mathcal{I}} :\ a \in \mathcal{R}\} \\ [a]_{\mathcal{I}} + [b]_{\mathcal{I}} &= [a+b]_{\mathcal{I}} \end{aligned}$$

afegim la multiplicació definida de forma natural per

$$[a]_{\mathcal{I}} \cdot [b]_{\mathcal{I}} = [a\,b]_{\mathcal{I}}$$

llavors

(i) si $a, b \in \mathcal{R}$, llavors o be $[a]_{\mathcal{I}} = [b]_{\mathcal{I}}$, o be $[a]_{\mathcal{I}} \cap [b]_{\mathcal{I}} = \phi$, (són classes d'equivalència);
(ii) la suma i el producte estan ben definits;
(iii) la suma i el producte donen estructura d'anell a $\mathcal{R}/\mathcal{I}$ (que anomenem anell quocient).

EXERCICI 1.6. Proveu les afirmacions següents: La suma, el producte i la intersecció de dos ideals és un ideal. La intersecció (finita o infinita) d'ideals és ideal i el producte finit d'ideals és ideal. La suma (finita o infinita) d'ideals és el mínim ideal que els conté a tots ells. La reunió d'ideals és ideal en general?

EXERCICI 1.7. (*) Donats tres ideals $\mathcal{I}_1, \mathcal{I}_2, \mathcal{J}$ d'un anell $\mathcal{R}$, proveu que

$$(\mathcal{I}_1 + \mathcal{I}_2)\mathcal{J} = \mathcal{I}_1\mathcal{J} + \mathcal{I}_2\mathcal{J}.$$

EXERCICI 1.8. (**) Proveu que un ideal $\mathcal{I}$ de un anell commutatiu $\mathcal{R}$ és primer ssi $\mathcal{J}\mathcal{K} \subseteq \mathcal{I}$ implica que $\mathcal{J} \subseteq \mathcal{I}$ o $\mathcal{K} \subseteq \mathcal{I}$.

EXERCICI 1.9. (*) Proveu, per inducció sobre n que si $\mathcal{I}$ és primer i conté un producte d'ideals $\mathcal{J}_1\,\mathcal{J}_2 \ldots \mathcal{J}_n \subseteq \mathcal{I}$, llavors conté algún dels $\mathcal{J}_i$.

EXERCICI 1.10. (**) Proveu les proposicions 1.17 i 1.18 i el corol·lari 1.19:

(i) $\mathcal{P} \subseteq \mathcal{R}$ és un ideal primer ssi $R/\mathcal{P}$ és un domini.
(ii) $\mathcal{P} \subseteq \mathcal{R}$ és un ideal maximal ssi $\mathcal{R}/\mathcal{P}$ és un cos.
(iii) Tot ideal maximal és primer.

EXERCICI 1.11. (*) Proveu que $a \neq 0$ és primer ssi genera un ideal primer.

Secció 2.

EXERCICI 1.12. Proveu que en un anell euclidià l'aplicació g té les propietats següents:

(i) Si u és una unitat, llavors $g(u) \leq 1$, i per tant o be $g(u) = 0$ o $g(u) = 1$.
(ii) Si u_1 i u_2 són unitats, llavors $g(u_1) = g(u_2)$.
(iii) Si u és una unitat i a no, llavors $g(u) \leq g(a)$.

EXERCICI 1.13. Proveu que l'anell $\mathbb{Z}$ dels enters amb la norma donada pel valor absolut i la divisió és un domini Euclidià on $g(ab) = g(a)g(b)$. és única la divisió? O hem d'afegir alguna condició per que la divisió sigui única?

EXERCICI 1.14. Proveu que l'anell $K[x]$ dels polinomis d'una variable sobre un cos K també és euclidià amb la la divisió ordinària i la norma donada pel grau del polinomi, que verifica $g(ab) = g(a) + g(b)$.
Pista: Doneu l'algorisme i proveu que acaba i amb el resultat esperat.

EXERCICI 1.15. En canvi $K[x, y]$ no és Euclidià. Observem que si volguéssim emprar la mateixa forma de divisió que a $K[x]$ en intentar dividir $a = xy^3$ per $b = x^2y$, sigui quin sigui el quocient, no és possible cancel·lar el terme xy^3, i així el residu tindria grau total més gran que el de b. Proveu que $K[x, y]$ no és un PID ja que l'ideal $\langle x, y\rangle$ no admet un únic generador.

Secció 4.

EXERCICI 1.16. (*) Demostreu que si $\mathcal{R}[x]$ és Noetherià també ho és $\mathcal{R}$.

Secció 5.

EXERCICI 1.17. Proveu la proposició 5.5.

EXERCICI 1.18. (**) [Anells de Dedekind]. Sigui $d \in \mathbb{Z}$, $d \neq 1$, no divisible pel quadrat de cap primer. Sigui

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z}[x]/\left\langle x^2 - d\right\rangle = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Z}\}.$$

Es defineix el conjugat de $z = a + b\sqrt{d}$ per $\overline{z} = a - b\sqrt{d}$ i la norma de z per $N(z) = |z\overline{z}| = |a^2 - db^2| \in \mathbb{Z}_{\geq 0}$. Proveu que a $\mathbb{Z}[\sqrt{d}]$,

(1) $N(z) \geq 0$, i $N(z) = 0$ si i només si $z = 0$;
(2) $N(z_1z_2) = N(z_1)N(z_2)$;

(3) $\mathbb{Z}[\sqrt{d}]$ és un domini d'integritat
(4) $N(z) = 1$ ssi z és una unitat;
(5) $\langle x^2 - d \rangle$ és primer però no és maximal a $\mathbb{Z}[x]$ (doneu demostració directe);
(6) Si $N(z)$ és un enter primer, llavors z és irreductible a $\mathbb{Z}[\sqrt{d}]$;
(7) $1 + \sqrt{-3}$ és irreductible però no és primer a $\mathbb{Z}[\sqrt{-3}]$;
(8) $\mathbb{Z}[\sqrt{-3}]$ no és un UFD.
(9) Determineu les unitats de $\mathbb{Z}[\sqrt{3}]$.
(10) Proveu que $\mathbb{Z}[\sqrt{d}]$ és euclidià per $d = 2, 3, -1, -2$. Per això siguin $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ i $\gamma, \delta \in \mathbb{Z}[\sqrt{d}]$ respectivament el quocient i residu de la divisió entera de α i β. Perquè sigui euclidià s'ha de complir $\alpha = \beta\gamma + \delta$ i $N(\delta) < N(\beta)$. Determineu γ com l'element de $\mathbb{Z}[\sqrt{d}]$ que té components més properes a $\alpha/\beta \in \mathbb{Q}[\sqrt{d}]$.
(11) $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ és el domini dels enters Gaussians. Resumiu les seves propietats. Doneu la definició de la divisió entera i afegiu condicions perquè sigui única.

EXERCICI 1.19. $k[x, y]$ és un UFD, (veure el corol·lari 5.11). Comproveu que

a) $\gcd(x, y) = 1$.
b) en canvi $1 \notin \langle x, y \rangle$.

EXERCICI 1.20. Proveu que si $\mathcal{R}$ és UFD, llavors tot element de $\mathcal{R}[x]$ admet una descomposció en irreductibles. Com són els irreductibles de $\mathcal{R}[x]$?

EXERCICI 1.21. Utilitzant el lema de Gauss i emprant algorismes (p.e. en Maple) per trobar el gcd en varies variables, proveu de factoritzar el següent polinomi a $\mathbb{Q}[x, y, z]$. La factorització feta val també a $\mathbb{C}[x, y, z]$? (*Indicació: Considereu $f \in \mathbb{Q}[x, y, z] \subseteq \mathbb{Q}(x, y)[z]$ i factoritzeu en el segon anell*)

$$\begin{aligned} f \;:=\; & x^6yz^3 - 2\,x^5y^2z^2 + x^4y^3z - 3\,x^5yz^3 + 6\,x^4y^2z^2 - 3\,x^3y^3z + 2\,x^4yz^3 \\ & -4\,x^3y^2z^2 + 2\,x^2y^3z - y^5x^4z^3 + 2\,y^6x^3z^2 - y^7x^2z + 3\,y^5x^3z^3 \\ & -6\,y^6x^2z^2 + 3\,y^7xz - 2\,y^5x^2z^3 + 4\,y^6xz^2 - 2\,y^7z. \end{aligned}$$

Secció 6.

EXERCICI 1.22. Demostreu que el resultat de la proposició 6.2 es pot millorar de la manera següent. Sigui $f \in K[\overline{x}]$ i $A_i \subseteq K$ $i = 1, \ldots, n$ tals que $|A_i| > \deg(f, x_i)$, on $\deg(f, x_i)$ indica el grau de f en x_i (mirat com a polinomi en la variable x_i sobre l'anell $K[x_1, \ldots, \widehat{x_i}, \ldots x_n]$). Si f s'anul·la sobre $A_1 \times \cdots \times A_n$ llavors $f = 0$.

Secció 8.

EXERCICI 1.23. (*) Proveu que si K és $\mathbb{R}$ o $\mathbb{C}$, la topologia usual és més fina que la topologia de Zariski, és a dir: els tancats de Zariski són també

tancats per la topologia usual, i en canvi no tots els tancats per la topologia ordinària són tancats de Zariski.

Secció 9.

EXERCICI 1.24. (*) Sigui A un sub-conjunt de K^n. Demostreu que $\mathbb{I}(A)$ és un ideal de $K[\overline{x}]$.

EXERCICI 1.25. (**) Proveu que $\mathbb{I}(V \cap W) = \mathbb{IV}(\mathbb{I}(V) + \mathbb{I}(W))$.

Secció 11.

EXERCICI 1.26. Siguin $\mathcal{I}$ i $\mathcal{J}$ ideals d'un anell $\mathcal{R}$.

(1) Demostreu que $\mathcal{I} : \mathcal{J}$ és un ideal.
(2) Proveu que $\mathcal{I} \subseteq \mathcal{I} : \mathcal{J}$.
(3) Proveu que $\mathcal{I} : \langle 1 \rangle = \mathcal{I}$.
(4) Proveu que $\mathcal{I} : \mathcal{I} = \langle 1 \rangle$
(5) Proveu que $\mathcal{I} \cdot \mathcal{J} \subseteq (\mathcal{I} : \mathcal{J}) \cdot \mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$.
(6) Proveu que $(\mathcal{I} \cdot \mathcal{J}) : \mathcal{J} \supseteq \mathcal{I}$.
(7) Proveu que si $\mathcal{R}$ és un domini, llavors
$$\langle p_1 q, \ldots, p_r q \rangle : \langle q \rangle = \langle p_1, \ldots, p_r \rangle .$$
(8) Comproveu que si prenem $\mathcal{I} = \langle 2x^3, 10x^2 \rangle$ i $\mathcal{J} = \langle 4x^2, 24x \rangle$ a $\mathbb{Z}[x]$ les dues inclusions (5) són estrictes.
(9) Comproveu que l'exemple (8) no dona contre-exemple de la inclusió estricta per (6).
Nota: En el capítol 3 es donen propietats que permeten determinar quocients d'ideals a partir de la intersecció. Utilitzeu-les en els apartats (8) i (9). També es dona en el capítol 3 un algorisme per determinar la intersecció d'ideals de $K[\overline{x}]$. Aquest no resulta útil aquí ja que $\mathbb{Z}$ no és un cos. Per determinar la intersecció d'ideals de monomis de $\mathbb{Z}[x]$, podeu determinar els gcd's dels generadors agafats de dos en dos. La inclusió (6) no és sempre una igualtat. Trobarem contre-exemples a $K[\overline{x}]$ amb les tècniques del capítol 3.

Secció 12.

EXERCICI 1.27. (**)

(1) Demostreu que si V i W són varietats de K^n,
   a) si $W \subset V$, llavors $V = W \cup (\overline{V \setminus W})$;
   b) si $W \subsetneq V$ i V és irreductible, llavors $\overline{V \setminus W} = V$.
   c) Doneu exemples on es vegi que la hipòtesi V *irreductible* és necessària per la conclusió de l'apartat b).
(2) Demostreu que si K és infinit, l'espai afí K^n és irreductible.
(3) Utilitzant els resultats dels exercicis anteriors, proveu que si K és infinit, V és una varietat i $V \subset K^n$, llavors $\overline{K^n \setminus V} = K^n$.
(4) Demostreu que la clausura de Zariski d'un sub-conjunt infinit de K és tot K. Què passa en el cas finit?

EXERCICI 1.28. (**)

(1) Demostreu que V és irreductible sii $V \subseteq V_1 \cup \cdots \cup V_r$ implica $V \subseteq V_i$ per algún $1 \leq i \leq r$.
(2) Demostreu que si V és finit, llavors V és irreductible sii té un sol element.
(3) Demostreu que si K és finit, les úniques varietats irreductibles de K^n són els punts.

EXERCICI 1.29. (**) $\mathbb{R}$ no és un cos algebraicament tancat. En aquest cas no són equivalents $p(x)$ és irreductible i $\mathbb{V}(p)$ és irreductible.

a) Trobeu un contre-exemple a $\mathbb{R}[\overline{x}]$ on $p(\overline{x}) \in K[\overline{x}]$ sigui irreductible sobre K, i $\mathbb{V}(p)$ sigui una varietat reductible.
b) Trobeu un contre-exemple on $p(\overline{x})$ sigui reductible i en canvi $\mathbb{V}(p)$ sigui irreductible.

EXERCICI 1.30.

(1) La cúbica guerxa (a K) és la varietat definida per la parametrització polinomial $F : K \to K^3$, $F(a) = (a, a^2, a^3)$. Trobeu polinomis que defineixin la cúbica guerxa i demostreu que F cobreix tota la cúbica guerxa.
(2) Trobeu la varietat definida per la parametrització $F : \mathbb{R} \to \mathbb{R}^2$, $F(a) = (\cos a, \cos 2a)$. F cobreix tota la varietat?

EXERCICI 1.31. (**) En aquests exercicis K és infinit.

a) Proveu que tota varietat lineal és irreductible. És cert també per un cos finit?
b) Proveu que tota varietat de K^2 definida per $V = \mathbb{V}(y - f(x))$ és irreductible ($f \in K[x]$). Proveu també que $\langle y - f(x) \rangle$ és ideal de varietat.
c) Proveu que si $\mathcal{I} = \langle yg_1(x) - f_1(x), zg_2(x) - f_2(x) \rangle$, on $f_1, f_2, g_1, g_2 \in K[x]$ i g_1, g_2 són polinomis no nuls, i $(f_i, g_i) = 1$ per $1 \leq i \leq 2$, llavors $\mathbb{V}(\mathcal{I})$ és irreductible.
d) Proveu que la hipèrbola $xy - 1 = 0$ és irreductible, tot i que el seu gràfic té dues branques a $\mathbb{R}^2$.
e) Proveu que si $f \in K[\overline{x}]$ és irreductible, i $\langle f \rangle = \mathbb{I}(\mathbb{V}(f))$, llavors $\mathbb{V}(f)$ és irreductible.
f) Més endavant veurem que si K és algebraicament tancat i $f \in K[\overline{x}]$, llavors $\mathbb{V}(f)$ és irreductible ssi f és potència d'irreductible. Això no és cert si K no és algebraicament tancat, com podem veure en els exemples següents:
   (1) Comproveu que a $\mathbb{R}[x, y]$, $f = (x^2 + y^2)(x - y) = x^3 + xy^2 - x^2y - y^3$ no és irreductible i en canvi $\mathbb{V}(f)$ és irreductible. Què passa a $\mathbb{C}$?

(2) Demostreu que $f = (y - x^2)^2 + (y - x)^2 = x^4 - 2x^2y + x^2 + 2y^2 - 2xy$ és irreductible, però $\mathbb{V}(f)$ no ho és a $\mathbb{R}$ ni a $\mathbb{Q}$. Què passa a $\mathbb{C}$?

EXERCICI 1.32. (**) Trobeu la descomposició en varietats irreductibles a $\mathbb{C}$ i a $\mathbb{R}$ de

(1) $V_1 = \mathbb{V}\left(x - 1, x - y^2\right)$.
(2) $V_2 = \mathbb{V}\left((x - 3)(yx - 1)(x^2 - y), (y - 3)(yx - 1)\right)$.
(3) $V_3 = \mathbb{V}\left(xy(y - x^2), zy(y - z)(y - x^2)\right)$

EXERCICI 1.33. Sigui la parametrització següent

$$\begin{aligned} x &= \frac{t}{1+t} \\ y &= 1 - \frac{1}{t^2} \end{aligned}$$

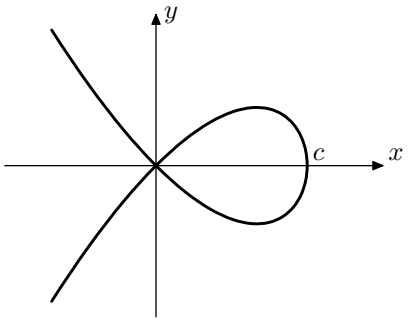
a) Trobeu l'equació de la varietat afí que determina.
b) Proveu que parametritza tots els punts de la varietat trobada excepte un punt.
c) Trobeu una parametrització de la corba que parametritzi tots els punts.
Nota: No disposant encara de bases de Gröbner cal anar en compte amb l'eliminació.

EXERCICI 1.34. (*) Volem trobar una parametrització de l'esfera $x^2 + y^2 + z^2 - 1 = 0$ a $\mathbb{R}^3$.

a) Donat un punt $(u, v, 0)$ del plá (x, y), traceu una línia cap el pol nord $(0, 0, 1)$. Sigui (x, y, z) l'altre punt en que la recta talla a l'esfera. Feu un gràfic per ilustrar-ho, i argumenteu geomètricament que el mapeig (u, v) versus (x, y, z) determina una parametrització de l'esfera a excepció del pol nord.
b) Trobeu la parametritció de l'esfera.

EXERCICI 1.35. Adapteu l'argumentació del exercici anterior per parametritzar l'esfera n-dimensional $x_1^2 + \cdots + x_n^2 = 1$ de $\mathbb{R}^n$.

EXERCICI 1.36. Sigui la corba d'equació $y^2 = cx^2 - x^3$, on c és una constant. Heus aquí un gràfic de la corba per $c > 0$:



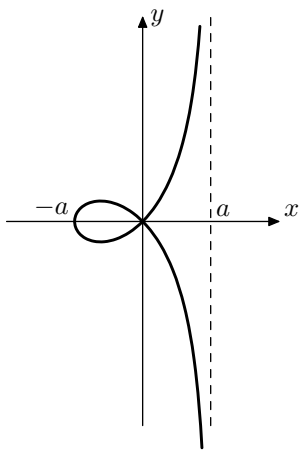


FIGURA 3. Strofoide

Volem parametritzar-la.

a) Proveu que una recta talla la corba en 0, 1, 2 ó 3 punts. Il·lustreu el resultat sobre el gràfic.
b) Proveu que una recta de pendent m no-vertical que passi per l'origen talla la corba exactament en un punt si $m^2 \neq c$.
c) Considereu ara la recta vertical $x = 1$. Donat un punt $(1, t)$ d'aquesta recta, dibuixeu la recta que el connecta a l'origen. Aquesta recta tallarà a la corba en un punt (x, y). Dibuixeu la construcció, i argumenteu geomètricament per què aquest fet dóna lloc a una parametrització de la corba sencera. Quina és la parametrització que s'obté?

EXERCICI 1.37. La *strofoide* és una corba que ha estat estudiada per diversos matemàtics, entre els quals destaquen Isaac Barrow (1630-1677), Jean Bernouilli (1667-1748) i Maria Agnesi (1718-1799). Admet una parametrització trigonomètrica, que és la següent:

$$\begin{aligned} x &= a\sin(t) \\ y &= a\tan(t)(1+\sin(t)) \end{aligned}$$

on a és una constant. Si variem $-4.2 \leq t \leq 1.0$ obtenim el següent gràfic de la figura 3:

a) Trobeu l'equació en x, y que descriu la strofoide. Aneu amb compte, i comproveu que no és exacte si el resultat obtingut és $(a^2-x^2)y^2 = x^2(a+x)^2$. Què passa per $x = -a$?
b) Trobeu una parametrització algebraica de la strofoide.

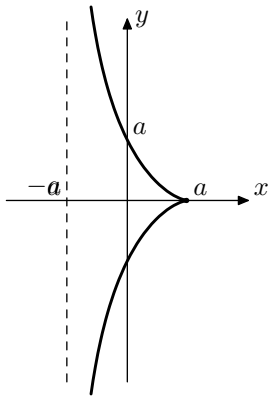


FIGURA 4. Cisoide

EXERCICI 1.38. Cap el 180 A.C. Diocles va escriure el llibre *Sobre els miralls*, i en ell va considerar la corba anomenada *cisoide*. La va utilitzar per resoldre el problema de la duplicació del cub. La cisoide té com a equació $y^2(a+x) = (a-x)^3$, on a és una constant. (Veure gràfica de la figura 4).

a) Trobeu una parametrització algebraica de la cisoide.
b) Diocles descriu la cisoide emprant la construcció geomètrica de la següent. (Veure figura 5). Donat un cercle de radi a (que prendrem centrat a l'origen) prenem x en l'interval $(-a, a]$, i considerem la línia L que uneix el punt $(a, 0)$ al punt del cercle $P = (-x, \sqrt{a^2 - x^2})$. Així queda determinat un punt $Q = (x, y)$ sobre L. Proveu que la cisoide és el lloc geomètric de tots els punts Q.
c) La duplicació del cub és el problema grec classic d'intentar construir $2^{1/3}$ amb regle i compàs. Sabem que no té solució emprant únicament regle i compàs. Diocles va mostrar que si es permet emprar també la cisoide, llavors sí que podem construir $2^{1/3}$. Vegem com funciona. Dibuixeu una línia enllaçant $(-a, 0)$ i $(0, a/2)$. Aquesta línia tallarà la cisoide en un punt (x, y). Proveu que

$$2 = \left(\frac{a-x}{y}\right)^3,$$

el que demostra que es pot construir $2^{1/3}$ amb l'ajut de regle compàs i cisoide.

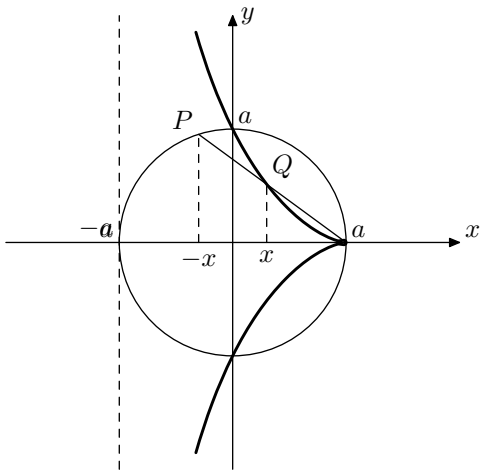


FIGURA 5. Construcció de la cisoide

EXERCICI 1.39. Anem a deduir la següent parametrització de la superfície $x^2 - y^2z^2 + z^3 = 0$:

$$\begin{aligned} x &= t(u^2 - t^2) \\ y &= u \\ z &= u^2 - t^2 \end{aligned}$$

a) Proveu que la corba $x^2 = cz^2 - z^3$ pot ser parametritzada per

$$\begin{aligned} z &= c - t^2 \\ x &= t(c - t^2) \end{aligned}$$

b) Substituïu c per y^2 en l'apartat anterior i proveu la parametrització desitjada.
c) Expliqueu per què aquesta parametrització recorre enterament la superfície $\mathbf{V}(x^2 - y^2z^2 + z^3)$.

EXERCICI 1.40. Sigui la varietat $V = \mathbb{V}(y - x^2, z - x^4) \subset \mathbb{R}^3$

a) Feu una gràfica.
b) Trobeu una parametrització.
c) Parametritzeu la superfície tangent a V.

EXERCICI 1.41. Aquest problema tracta de conjunts convexos i serà emprat en el proper per mostrar que una corba de Bézier queda a l'interior del seu polígon de control. Un sub-conjunt $C \subset \mathbb{R}^2$ és *convex* si per cada $P, Q \in C$ el segment que uneix $P = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ i $Q = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$ està íntegrament

a l'interior de C. El segment PQ ve donat per

$$S:\ t\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + (1-t)\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

on $0 \leq t \leq 1$.

Si $P_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix}$ estan dins d'un conjunt convex C per $i \leq i \leq n$, proveu que

$$\sum_{i=1}^{n} t_i \begin{pmatrix} x_i \\ y_i \end{pmatrix} \in C$$

si $t_1, \ldots t_n$ són nombres no-negatius tals que $\sum_{i=1}^{n} t_i = 1$. (Nota: Demostreu-ho per inducció sobre n).

EXERCICI 1.42. (**) Una cúbica de Bézier ve donada per

$$\begin{aligned} x &= (1-t)^3 x_0 + 3t(1-t)^2 x_1 + 3t^2(1-t)x_2 + t^3 x_3 \\ y &= (1-t)^3 y_0 + 3t(1-t)^2 y_1 + 3t^2(1-t)y_2 + t^3 y_3 \end{aligned}$$

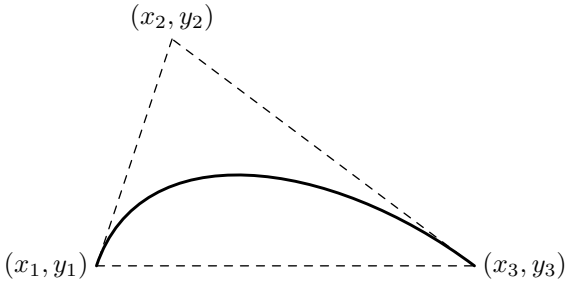
a) Escriviu l'expressió anterior de la cúbica de Bézier en forma vectorial i amb un sumatori i generalitzeu-la per una corba de Bézier de grau n determinada per $n+1$ punts.
b) Utilitzant el resultat de l'exercici 1.41 proveu que les corbes de Bézier sempre queden a dins del seu polígon de control.
c) Proveu que passa sempre pels punts P_0 i P_n.
d) Proveu que les direccions de la corba en els punts P_0 i P_n són $P_1 - P_0$ i $P_n - P_{n-1}$ respectivament.
e) Es poden invertir l'ordre dels punts de control? Quin efecte tindrà sobre la corba?
f) Es poden repetir punts? Quin efecte tindrà sobre la corba?

EXERCICI 1.43. Un inconvenient de les cúbiques de Bézier és que corbes com hipèrboles o circumferències no poden ser exactament descrites per elles. Ara veurem un mètode per parametritzar seccions còniques. Una secció cònica és una corba en el pla definida per una equació de segon grau de la forma $ax^2 + bxy + cy^2 + dx + ey + f = 0$. Exemples clàssics de còniques són circumferències, el·lipses, paràboles, e hipèrboles. Considerem la corba parametritzada per

$$\begin{aligned} x &= \frac{(1-t)^2 x_1 + 2t(1-t)wx_2 + t^2 x_3}{(1-t)^2 + 2t(1-t)w + t^2} \\ y &= \frac{(1-t)^2 y_1 + 2t(1-t)wy_2 + t^2 y_3}{(1-t)^2 + 2t(1-t)w + t^2} \end{aligned}$$

on $0 \leq t \leq 1$. Les constants $w, x_1, y_1, x_2, y_2, x_3, y_3$ ja venen donades i suposarem també que $w \geq 0$. L'objectiu d'aquest problema ès donar una interpretació geomètrica a les constants $w, x_1, y_1, x_2, y_2, x_3, y_3$.

a) Proveu que la suposició de que $w > 0$ implica que els denominadors de les corbes mai s'anul·len.
b) Avalueu les equacions per $t = 0$ i $t = 1$. Amb això podreu entendre el significat de x_1, y_1, x_3, y_3.
c) Ara avalueu $(x'(0), y'(0))$ i $(x'(1), y'(1))$. Utilitzeu-ho per provar que (x_2, y_2) és la intersecció entre les tangents que formen l'inici i el final de la corba. Expliqueu perquè $(x_1, y_1), (x_2, y_2)$ i (x_3, y_3) són anomenats els punts de control de la corba.
d) Definiu el seu polígon de control (en el nostre cas un triangle), i proveu que la corba definida per les equacions sempre queda dins del seu polígon de control. Pista: Adapteu l'argumentació del problema anterior.

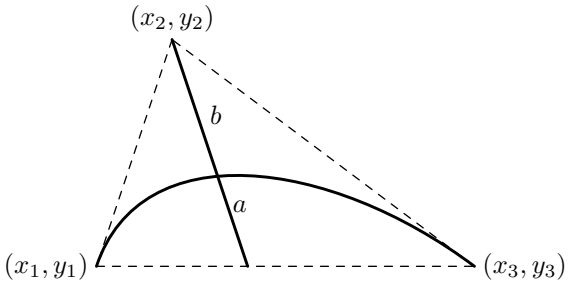


El dibuix intenta explicar el significat de la constant w, (shape factor). Una pista pot ser la resposta de l'apartat c). Noteu que w apareix en les fórmules dels vectors tangents quan $t = 0, 1$. Així w controla la velocitat ja que un valor molt gran per w faria que la corba es tanqués a (x_2, y_2). En els dos darrers apartats veurem exactament quin paper juga w.

e) Demostreu que

$$\begin{pmatrix} x\left(\frac{1}{2}\right) \\ y\left(\frac{1}{2}\right) \end{pmatrix} = \frac{1}{1+w}\left(\frac{1}{2}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} x_3 \\ y_3 \end{pmatrix}\right) + \frac{w}{1+w}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

Feu servir aquesta equació per demostrar que $\left(x\left(\frac{1}{2}\right), y\left(\frac{1}{2}\right)\right)$ està sobre el segment que connecta (x_2, y_2) al punt mig entre (x_1, y_1) i (x_3, y_3).



f) Noteu que $(x\left(\frac{1}{2}\right), y\left(\frac{1}{2}\right))$ parteix el segment en dos parts de longitud a i b tal com indica el dibuix. Demostreu que

$$w = \frac{a}{b}$$

Observeu doncs que w ens indica exactament si la corba talla el segment. Pista: Utilitzeu la fórmula de la distància.

g) Proveu que la parametrització donada determina una cònica i decidiu de quin tipus és en funció del paràmetre w.

CAPíTOL 2

Bases de Gröbner

1. Problemes a resoldre

A partir d'aquest moment ens interessem bàsicament en l'anell $K[\overline{x}] = K[x_1, \ldots, x_n]$ de polinomis de n variables sobre un cos K. Sabem, pel capítol anterior que és un UFD Noetherià.

La teoria exposada fins aquí dona pocs recursos de càlcul a l'hora de resoldre tot un seguit de problemes. Citem-ne alguns:

(1) Descripció d'un ideal, comparació d'ideals.
(2) Pertinença d'un polinomi $f \in K[\overline{x}]$ a un ideal $\mathcal{I} \subseteq K[\overline{x}]$.
(3) Determinació del gcd i el lcm.
(4) Solució d'un sistema d'equacions polinòmiques.
(5) Varietats irreductibles i ideals primers. Descomposició minimal d'una varietat en irreductibles.
(6) Determinació de la varietat definida per una parametrització polinòmica o racional.
(7) Trobar la clausura de Zariski d'un conjunt de K^n.
(8) Determinació de l'ideal d'una varietat.
(9) Determinació de la intersecció d'ideals.
(10) Determinació de l'ideal de varietat d'un ideal.

Tots aquests problemes són fàcils de resoldre a $K[x]$, amb una sola variable. La raó és que $K[x]$ és un domini euclidià on existeix la divisió, i per tant és també un PID. En alguns problemes el resultat depèn del cos (p.e. $\mathbb{Q}$ $\mathbb{R}$, $\mathbb{C}$). Recordem com es resolen aquests problemes a $K[x]$ (quan calgui diferenciarem entre els casos esmentats).

(1) Per ser $K[x]$ un PID, tot ideal $\mathcal{I} \subseteq K[x]$ està generat per un únic polinomi generador, que és a més a més el gcd de tots els polinomis de $\mathcal{I}$. Es verifica que $\langle f \rangle \subseteq \langle g \rangle$ ssi $g \mid f$.
(2) Si $\mathcal{I} = \langle g \rangle$, llavors $f \in \mathcal{I}$ ssi el residu de dividir f per g és 0.
(3) El $\gcd(f, g)$ es calcula per l'algorisme d'Euclides, i existeixen identitats de Bézout, etc.
(4) Tot conjunt d'equacions polinòmiques és equivalent a una única equació. En un cos algebraicament tancat tot polinomi de grau n descompon com a producte de n arrels, que poden ser múltiples. L'exemple emblemàtic és $\mathbb{C}[x]$ (teorema fonamental de l'àlgebra).

En canvi a $\mathbb{Q}[x]$ podem tenir polinomis de grau arbitrari que corresponen a la varietat buida.

(5) Els ideals primers són els generats per un polinomi irreductible. A $\mathbb{C}[x]$, els únics polinomis irreductibles són lineals, i per tant, els ideals primers són de la forma $\langle x-a\rangle$. A $\mathbb{Q}[x]$ hi ha també polinomis irreductibles de grau qualsevol. Els corresponents ideals generats són primers, i la varietat associada és buida. Les úniques varietats irreductibles no buides, en ambdós casos, estan formades per un únic punt. Les varietats són ϕ, K i conjunts finits de punts. La descomposició d'una varietat en irreductibles és trivial.
(6) Com sabem, les varietats parametritzables són irreductibles i per tant les úniques varietats de $K[x]$ parametritzables són de la forma $x=a$, amb a fixat o $x=t$ per tot $t\in K$, que és tot K.
(7) Si K és infinit i el conjunt S té infinits punts, la clausura de Zariski de S és tot K.
(8) Si $V=\{a_1,a_2,\ldots,a_s\}$, llavors $\mathbb{I}(V)=\langle(x-a_1)(x-a_2)\ldots(x-a_s)\rangle$.
(9) La intersecció dels ideals $\langle f\rangle$ i $\langle g\rangle$ és $\langle \operatorname{lcm}(f,g)\rangle$.
(10) A $\mathbb{C}[x]$, si $\mathcal{I}=\langle f\rangle$, llavors $\mathbb{IV}(\mathcal{I})=\langle g\rangle$ on g és el polinomi lliure de quadrats que s'obté com a producte sense multiplicitat de les arrels de f. Per tant coincideix amb l'ideal radical.

A $\mathbb{Q}[x]$ el polinomi lliure de quadrats pot tenir factors sense arrels i per tant no figuren en el generador de l'ideal de la varietat de l'ideal.

A $K[x_1,\ldots,x_n]$ les coses són més complicades. La teoria de les bases de Gröbner donarà eines per abordar alguns d'aquests problemes.

NOTA HISTÒRICA 1.1. La teoría de les bases de Gröbner va ser introduïda simultàniament i per separat per H. Hironaka (Japó) i per Bruno Buchberger (Linz, Austria). El primer les anomenà bases estandard, nom que és poc utilitzat actualment. El segon les va denominar bases de Gröbner en honor al seu director de tesi W. Gröbner (1899-1980), i és el nom que reben generalment.

El fet de l'aparició tan tardana d'aquesta teoria prové de la dificultat que comporta l'absència de divisió Euclidiana en els polinomis de n variables.

Per entrar en matèria, intentem resoldre el següent exemple.

EXEMPLE 1.2. Donats els polinomis de $\mathbb{Q}[x,y]$

$$f=x^2\,y-3\,x\,y+x,\qquad \text{i}\qquad g=x\,y+y$$

(1) És cert que $\langle f,g\rangle=\left\langle x+4\,y,4\,y^2-y\right\rangle$?
(2) És cert que $x-4\,x\,y\in\langle f,g\rangle$?
(3) Determinem $\mathbb{V}(\mathcal{I})$.
(4) La varietat determinada no es pot parametritzar. Per què?
(5) Quin és l'ideal de la varietat $\mathbb{V}(\mathcal{I})$?

(1) $\mathbb{Q}[x,y]$ no és un PID i per tant no és euclidià. No podem esperar trobar una divisió euclidiana. Tenim

$$\begin{aligned} f_1 &= x\,g - f = 4\,x\,y - x \\ f_2 &= 4\,g - f_1 = x + 4\,y \\ f_3 &= y\,f_2 - g = 4\,y^2 - y \end{aligned}$$

d'on resulta

$$\begin{aligned} f_2 &= 4\,g - f_1 = 4\,g - (x\,g - f) = f + (4-x)\,g \\ f_3 &= y\,f_2 - g = y\,(x\,f + (4-x)\,g) - g \\ &= y\,f + (-x\,y + 4\,y - 1)\,g \\ g &= y\,f_2 - f_3 \\ f &= x\,g - f_1 = xg - (4g - f_2) = (x-4)g + f_2 \\ &= (x-4)(y\,f_2 - f_3) + f_2 = (x\,y - 4\,y + 1)f_2 + (4-x)f_3 \end{aligned}$$

i en conseqüència $\langle f, g\rangle = \langle f_2, f_3\rangle$.

(2) $x - 4\,x\,y = f - x\,g \in \langle f, g\rangle$.
(3) $V = \mathbb{V}(\mathcal{I}) = \mathbb{V}(f_2, f_3) = \{(0,0), (-1, 1/4)\}$
(4) V no es pot parametritzar perquè no és irreductible.
(5) Més difícil és demostrar que en aquest exemple $\mathbb{IV}(\mathcal{I}) = \mathcal{I}$.

Comprovem que no disposem de mètode general per respondre en aquestes preguntes. Cal una teoria més elaborada.

2. Polinomis, notacions.

Precisem les notacions que fem servir per a polinomis.

Definició 2.1 (Anell de polinomis de n variables sobre un cos (o UFD) K). El denotem $K[x_1, \ldots, x_n] = K[\overline{x}]$.

Multigrau: (multideg)	$\alpha = (\alpha_1, \alpha_2 \ldots, \alpha_n)$, on $\alpha \in \mathbb{Z}^n_{\geq 0}$
Producte de potències:	$x^\alpha = x_1^{\alpha_1}\, x_2^{\alpha_2} \ldots x_n^{\alpha_n}$
Monomi:	$a\,x^\alpha$, on $a \in K$ és el coeficient
Grau total d'un producte de potències x^α:	$\lvert\,\alpha\,\rvert = \alpha_1 + \alpha_2 + \cdots + \alpha_n$
Polinomi:	$f = \sum_\alpha a_\alpha\, x^\alpha$, on $a_\alpha \in K$
Grau total d'un polinomi f:	$\deg(f) = \max\{\lvert\,\alpha\,\rvert : f = \sum a_\alpha\, x^\alpha, a_\alpha \neq 0\}$

3. Ordres monomials

Per avançar en la resolució dels problemes esmentats en la secció 1 cal introduir algún algorisme de divisió que donats un polinomi $f \in K[\overline{x}]$ i un ideal $\langle g_1, \dots, g_s \rangle$ expressi f en una forma del tipus $f = \sum_i h_i\, g_i + r$, on $h_i \in K[\overline{x}]$ amb certes bones propietats del residu i quocients. L'algorisme de la divisió funciona a $K[x]$ perquè existeix un ordre natural dels monomis $a\, x^i$, i resulta obvi determinar el monomi principal. A fi d'introduir una divisió cal doncs definir ordres monomials a $K[\overline{x}]$.

Definició 3.1 (Ordre monomial). A $K[\overline{x}]$ un **ordre monomial** és una relació $\succ$ sobre $\mathbb{Z}^n_{\geq 0}$, o de manera equivalent entre productes de potències $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$, o encara entre monomis $a\, x^\alpha$, que verifica

(i) $\succ$ és un ordre total sobre $\mathbb{Z}^n_{\geq 0}$.
(ii) Si $\alpha \succ \beta$ i $\gamma \in \mathbb{Z}^n_{\geq 0}$, llavors $\alpha + \gamma \succ \beta + \gamma$.
(iii) $\succ$ és una bona ordenació de $\mathbb{Z}^n_{\geq 0}$. Això vol dir que tot sub-conjunt no buit de $\mathbb{Z}^n_{\geq 0}$ té un element mínim.

Lema 3.2. *Una relació d'ordre $\succ$ a $\mathbb{Z}^n_{\geq 0}$ és una bona ordenació ssi tota seqüència de $\mathbb{Z}^n_{\geq 0}$ estrictament decreixent, $\alpha(1) \succ \alpha(2) \succ \alpha(3) \dots$ estaciona.*

Demostració. Ho provarem per reducció a l'absurd.

$\Rightarrow$: Suposem que $\succ$ és un bon ordre i que en canvi a $\mathbb{Z}^n_{\geq 0}$ existeix una seqüència infinita estrictament decreixent: $\alpha_1 \succ \alpha_2 \succ \dots$. Llavors el conjunt $S = \{\alpha_1, \alpha_2, \dots\} \subset \mathbb{Z}^n_{\geq 0}$, no tindria mínim i per tant $\succ$ no seria un bon ordre.

$\Leftarrow$ Suposem ara que tota successió estrictament decreixent estabilitza i que en canvi $\succ$ no és un bon ordre. Si $\succ$ no és una bona ordenació, existeix un sub-conjunt $S \subset \mathbb{Z}^n_{\geq 0}$ que no té element mínim. Triem $\alpha(1) \in S$. Com que no és l'element més petit, podem trobar $\alpha(1) \succ \alpha(2)$ i així successivament. Obtindrem una seqüència infinita estrictament decreixent $\alpha(1) \succ \alpha(2) \succ \dots$, que no estabilitza.

□

Definició 3.3. **Ordre lexicogràfic (lex)**. Donats $\alpha = (\alpha_1, \dots, \alpha_n)$ i $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, direm que $\alpha \succ_{\text{lex}} \beta$ si en el vector $\alpha - \beta \in \mathbb{Z}^n$, la primera component per l'esquerra no nul.la és positiva. Si $\alpha \succ_{\text{lex}} \beta$ escriurem $x^\alpha \succ_{\text{lex}} x^\beta$.

Amb l'ordre donat, les variables estan en l'ordre habitual:

$$x_1 \succ_{\text{lex}} x_2 \succ_{\text{lex}} \cdots \succ_{\text{lex}} x_n$$

ja que

$$(1, 0, \dots, 0) \succ_{\text{lex}} (0, 1, \dots, 0) \succ_{\text{lex}} \cdots \succ_{\text{lex}} (0, 0, \dots, 1)$$

Per donar completament un ordre lex, cal precisar en quin ordre considerem les variables (és a dir quina component correspon a cada variable).

Per tant, existeixen $n!$ ordres lex diferents, un per cada permutació dels indexos.

DEFINICIÓ 3.4. **Ordre total + invers lexicogràfic (grevlex)**. Donats $\alpha = (\alpha_1, \ldots, \alpha_n)$ i $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, direm que $\alpha \succ_{\text{grevlex}} \beta$ si

$$|\alpha| = \sum_{i=1}^{n} \alpha_i \ > \ |\beta| = \sum_{i=1}^{n} \beta_i,$$

o be $|\alpha| = |\beta|$ i en el vector $\alpha - \beta \in \mathbb{Z}^n$, la primera component per la dreta no nul.la és negativa.

DEFINICIÓ 3.5. **Ordre total +lexicogràfic (grlex)**. Donats $\alpha = (\alpha_1, \ldots, \alpha_n)$ i $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, direm que $\alpha \succ_{\text{grlex}} \beta$ si

$$|\alpha| = \sum_{i=1}^{n} \alpha_i \ > \ |\beta| = \sum_{i=1}^{n} \beta_i,$$

o be $|\alpha| = |\beta|$ i $\alpha \succ_{\text{lex}} \beta$.

PROPOSICIÓ 3.6. *Els ordres* lex, grevlex *i* grlex *a* $\mathbb{Z}^n_{\geq 0}$ *són ordres monomials.*

DEMOSTRACIÓ. Exercici 2.1. □

EXEMPLE 3.7. Ordenem els monomis del polinomi $f = x^3\,y\,z^2 + x^2\,z^5 + x^2\,y^3\,z$ en ordre monomial decreixent pels diferents ordres amb $x \succ y \succ z$. Tenim

$$\begin{aligned} f &= x^3\,y\,z^2 + x^2\,y^3\,z + x^2\,z^5 \quad \text{en ordre } \succ_{\text{lex}}. \\ f &= x^2\,z^5 + x^2\,y^3\,z + x^3\,y\,z^2 \quad \text{en ordre } \succ_{\text{grevlex}}. \\ f &= x^2\,z^5 + x^3\,y\,z^2 + x^2\,y^3\,z \quad \text{en ordre } \succ_{\text{grlex}}. \end{aligned}$$

DEFINICIÓ 3.8. Sigui $f = \sum_\alpha a_\alpha\,x^\alpha$ un polinomi no nul de $K[\overline{x}]$ i sigui $\succ$ un ordre monomial. Definim:

(i) **Multigrau (multideg)** de f

$$\text{multideg}(f) = \max_{\succ}(\alpha \in \mathbb{Z}^n_{\geq 0} \ : \ a_\alpha \neq 0).$$

(ii) **Coeficient principal, (leading coefficient)** de f

$$\text{lc}(f) = a_{\text{multideg}(f)} \in K.$$

(iii) **Producte de potències principal (leading power product)** de f

$$\text{lpp}(f) = x^{\text{multideg}(f)}.$$

(iv) **Monomi principal (leading monomial)** de f

$$\text{lm}(f) = \text{lc}(f)\ \text{lpp}(f)$$

LEMA 3.9. *Siguin $f, g \in K[\overline{x}]$ polinomis no nuls. Tenim:*

(i) $\text{multideg}(f\,g) = \text{multideg}(f) + \text{multideg}(g)$.

(ii) *Si $f+g \neq 0$, llavors* $\text{multideg}(f+g) \preceq \max(\text{multideg}(f), \text{multideg}(g))$. *Si a més a més,* $\text{multideg}(f) \neq \text{multideg}(g)$, *llavors hi ha igualtat.*

4. Algorisme de divisió a $K[\overline{x}]$

Input: $f \in K[\overline{x}]$ i $F = [f_1, \ldots, f_s] \subset K[\overline{x}]$,
$\succ$: un $\overline{x}$-ordre monomial.

Output: $r \in K[\overline{x}]$ i $Q = \{q_1, \ldots, q_s\} \subset K[\overline{x}]$ tals que $f = \sum_{i=1}^{s} q_i\, f_i + r$

$q_1 := 0;\ \ldots\ q_s := 0;\quad r := 0$
$p := f$
MENTRE $p \neq 0$ FER
  $i := 1$
  dividit:=fals
  MENTRE $i \leq s$ I dividit=fals FER
    SI $\text{lm}(f_i)$ divideix $\text{lm}(p)$ LLAVORS
      $q_i := q_i + \text{lm}(p)/\,\text{lm}(f_i)$
      $p := p - (\text{lm}(p)/\,\text{lm}(f_i))\, f_i$
      dividit:=cert
    ALTRAMENT
      $i := i + 1$
    FI SI
  FI MENTRE
  SI dividit=fals LLAVORS
    $r := r + \text{lm}(p)$
    $p := p - \text{lm}(p)$
  FI SI
FI MENTRE

L'algorisme de divisió, tot i no tenint les mateixes propietats que a $K[x]$, permet fonamentar la teoria de les bases de Gröbner.

EXEMPLE 4.1. Fem la divisió de $f = x^2\,y + x\,y^2 + y^2$ entre $f_1 = x\,y - 1$ i $f_2 = y^2 - 1$ en ordre lex amb $x \succ y$.

Ho disposem en la forma següent:

$$f_1 = x\,y - 1 :$$
$$f_2 = y^2 - 1 :$$

$$\sqrt{x^2\,y + x\,y^2 + y^2}$$

i anem fent quocients i separant els residus que no caben. El resultat serà:

$$\begin{array}{l} f_1 = x\,y - 1 : x + y \\ f_2 = y^2 - 1 \ : 1 \end{array}$$

$$\begin{array}{l|ll} \sqrt{x^2\,y + x\,y^2 + y^2} & & \\ \hline -x^2\,y + x & & \\ \hline \quad x\,y^2 + x + y^2 & & \\ \hline -x\,y^2 + y & & \\ \hline \quad x + y^2 + y & & \\ \hline -x & & x \\ \hline \quad y^2 + y & & \\ \hline -y^2 + 1 & & \\ \hline \quad y + 1 & & \\ \hline -y - 1 & & \underline{\quad y + 1 \quad} \\ \hline \quad 0 & & x + y + 1 \end{array}$$

On hem anat col.locant, per ordre, els quocients parcials x per f_1, y per f_1; després el proper monomi principal x no és divisible i passa al residu; a continuació el quocient parcial és 1 per f_2. Finalment passen al residu, ja que no són divisibles y i 1. El residu de la divisió és en total $x + y + 1$, i resultat de la divisió és:

$$f = x^2\,y + x\,y^2 + y^2 = (x + y) \cdot f_1 + 1 \cdot f_2 + (x + y + 1)$$

Si ara fem la divisió anterior considerant f_2 com a primer divisor i f_1 com a segon, el resultat és (exercici 2.4)

$$f = x^2\,y + x\,y^2 + y^2 = (x + 1)f_2 + x f_1 + (2x + 1).$$

Observem, doncs, que la divisió no dona un residu idèntic segons l'ordre en que s'agafen els divisors i ni tan sols conserva el residu. Òbviament, si al dividir f entre $f_1, \ldots, f_s$ en algun ordre el residu val zero, podem afirmar que $f \in \langle f_1, \ldots, f_s \rangle$. Però no podem esperar, sense més, que el recíproc sigui cert. El teorema que caracteritza la divisió que hem descrit és el següent:

TEOREMA 4.2. *Donat un ordre monomial $\succ$ a $\mathbb{Z}^n_{\geq 0}$ i una s-tupla de polinomis $F = [f_1, \ldots, f_s] \subset K[\overline{x}]$,*

(i) *tot $f \in K[\overline{x}]$ pot expressar-se en la forma*

$$f = \sum_{i=1}^{s} q_i\,f_i + r$$

on $q_i, r \in K[\overline{x}]$, i

(ii) *o be* $r = 0$ *o be* r *és una* K *combinació lineal de productes de potències, tals que cap d'elles és divisible per cap* $\mathrm{lpp}(f_i)$ *per* $1 \leq i \leq s$. *Direm que* r *és un* **residu** *de la divisió de* f *per* F.

(iii) *Es compleix que, si* $q_i\, f_i \neq 0$, *llavors*

$$\mathrm{multideg}(f) \succeq \mathrm{multideg}(q_i\, f_i)$$

(iv) *L'algorisme de divisió donat produeix els resultats* (i), (ii), (iii).

Demostració. En l'algorisme de la divisió, la variable p representa el residu parcial a cada pas de divisió. Els q_i's i r són els respectius quocients i residu parcials. La variable "dividit" indica si en el bucle corresponent hi ha hagut divisió parcial o no. En cas que no hi hagi, el corresponent monomi principal de p passa al residu.

(i) A cada nou bucle es compleix que

$$f = \sum_{i=1}^{s} q_i\, f_i + p + r.$$

És cert inicialment. A cada bucle, part del contingut de p passa a r o a la suma, de manera que l'equació es conserva. Si provem que l'algorisme acaba, com que finalment $p = 0$ quedarà provat que es verifica (i).

Per veure que l'algorisme acaba tinguem en compte que a cada bucle redefinim p de tal manera que el seu monomi principal és eliminat i $\mathrm{multideg}(p)$ decreix estrictament (per la propietat (ii) d'ordre monomial). Per ser $\succ$ una bona ordenació, l'algorisme acaba.

(ii) Cada monomi que ha passat a r durant l'algorisme no és divisible per cap $\mathrm{lpp}(f_i)$ per $1 \leq i \leq s$. Per tant, quan l'algorisme acabi es seguirà complint (ii).

(iii) Cada monomi de q_i és tal que $\mathrm{lm}(p) = \mathrm{lm}(q)\,\mathrm{lm}(f_i)$ per algun p intermedi. L'algorisme comença amb $p = f$ i a (i) hem vist que $\mathrm{multideg}(p)$ decreix. Utilitzant el lema 3.9 resulta immediatament la condició (iii).

□

Definició 4.3. Denotem $\overline{f}^F$ el residu de la divisió de f per la s-tupla $F = [f_1, \ldots, f_s]$.

5. Ideals de monomis i lema de Dickson

Definició 5.1 (Ideal de monomis). Direm que $\mathcal{I} \subset K[\overline{x}]$ és un ideal de monomis si existeix un conjunt A (finit o infinit) de productes de potències que el genera:

$$\mathcal{I} = \langle x^\alpha \ : \ \alpha \in A \rangle = \left\{ \sum_\alpha h_\alpha\, x^\alpha \ : \ h_\alpha \in K[\overline{x}],\ \alpha \in A \right\}$$

Observis que fora equivalent parlar de conjunt de monomis, ja que K és un cos, i si $c \neq 0$, dir que $c\,x^\alpha$ és un generador és equivalent a dir que ho és x^α.

EXEMPLE 5.2. $\mathcal{I} = \langle x^3\,y^2\,z, x\,y^5\,z^3, y^3\,z^2\rangle \subset K[x,y,z]$.

LEMA 5.3. *Sigui $\mathcal{I} = \langle x^\alpha \,:\, \alpha \in A\rangle$ un ideal de monomis. Llavors un producte de potències $x^\beta \in \mathcal{I}$ ssi x^β és divisible per algún producte de potències x^α, $\alpha \in A$.*

DEMOSTRACIÓ. $\Rightarrow$: Òbviament si x^β és múltiple d'algún x^α per algún $\alpha \in A$, llavors $x^\beta \in \mathcal{I}$.

$\Leftarrow$: Si $x^\beta \in \mathcal{I}$, llavors $x^\beta = \sum_{i=1}^s h_i\,x^{\alpha(i)}$, per certs $h_i \in K[\overline{x}]$ i $\alpha(i) \in A$. Expandint el producte tindrem

$$x^\beta = \sum_{i=1}^{s} h_i\,x^{\alpha(i)} = \sum_{i=1}^{s}\sum_{j=1}^{t_i} c_{ij}x^{\gamma_{ij}+\alpha(i)} = x^\beta \sum_{\gamma_{ij}+\alpha(i)=\beta} c_{ij}$$

on $c_{ij} \in K$. Un cop expandit el producte, únicament no es cancel.len els productes de potències amb exponent β. Per cada un dels productes de potències restants és $\gamma_{ij} + \alpha(i) = \beta$. Per tant x^β és divisible per cada un dels productes de potències $x^{\alpha(i)}$ que no s'hagin cancel.lat. □

Els productes de potències x^β que són divisibles per x^α corresponen a

$$\alpha + \mathbb{Z}^n_{\geq 0} = \left\{\alpha + \gamma \;:\; \gamma \in \mathbb{Z}^n_{\geq 0}\right\}$$

Així, els productes de potències de l'ideal de l'exemple anterior seran:

$$\left((3,2,1) + \mathbb{Z}^3_{\geq 0}\right) \cup \left((1,5,3) + \mathbb{Z}^3_{\geq 0}\right) \cup \left((0,3,2) + \mathbb{Z}^3_{\geq 0}\right)$$

EXEMPLE 5.4. Podem representar gràficament els monomis d'un ideal de monomis. Per exemple, per l'ideal $\mathcal{I} = \langle x\,y^3, x^3\,y^2, x^4\,y\rangle \subset K[x,y]$, els monomis de $\mathcal{I}$ venen representats a la figura 1.

LEMA 5.5. *Sigui $\mathcal{I}$ un ideal de monomis i $f \in K[\overline{x}]$. Són equivalents les afirmacions següents:*

(i) *$f \in \mathcal{I}$.*
(ii) *Cada monomi de f pertany a $\mathcal{I}$.*
(iii) *f és una K-combinació lineal de productes de potències de $\mathcal{I}$.*

DEMOSTRACIÓ. Òbviament (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i). Només cal provar que (i) implica (iii). La demostració és anàloga a la del lema anterior. Sigui $f \in \mathcal{I} = \langle x^\alpha : \alpha \in A\rangle$. Llavors, existeixen certs $h_i \in K[\overline{x}]$ i $\alpha(i) \in A$, tals que

$$f = \sum_{i=1}^{s} h_i\,x^{\alpha(i)} = \sum_{i=1}^{s}\sum_{j=1}^{t_i} c_{ij}\,x^{\gamma_{ij}+\alpha(i)}$$

on $c_{ij} \in K$. Per tant, cada producte de potències de f és de la forma $x^{\gamma_{ij}+\alpha(i)}$, i per tant és divisible per algún $x^{\alpha(i)}$ i, pel lema 5.3, pertany a $\mathcal{I}$. □

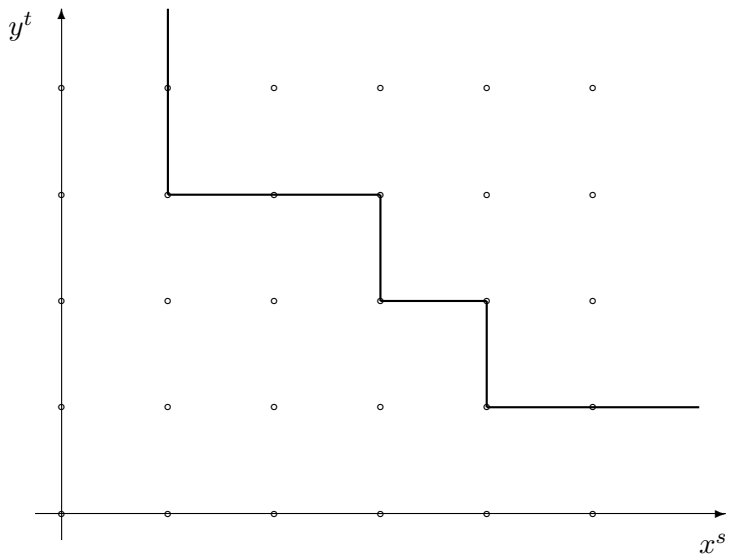


FIGURA 1. Monomis de l'ideal $\mathcal{I} = \langle x\,y^3, x^3\,y^2, x^4\,y\rangle$

COROL·LARI 5.6. *Dos ideals de monomis són iguals ssi tenen els mateixos productes de potències.*

TEOREMA 5.7 (**Lema de Dickson**). *Si $\mathcal{I} \subset K[\overline{x}]$ és un ideal de monomis $\mathcal{I} = \langle x^\alpha \,:\, \alpha \in A\rangle$ llavors podem extreure $B = \{\alpha(1), \ldots, \alpha(s)\} \subset A$, subconjunt finit de A, tal que*

$$\mathcal{I} = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle.$$

DEMOSTRACIÓ. Havent demostrat el teorema de la base d'Hilbert al capítol 1, ara el lema de Dickson és un corol·lari.

Per la proposició demostrada al capítol 1 que segueix al teorema de la base d'Hilbert, de tota base d'un ideal podem extreure una base finita. Per tant, donat $\mathcal{I} = \langle x^\alpha \,:\, \alpha \in A\rangle$ podem extreure una base finita $\{\alpha(1), \ldots, \alpha(s)\} \subset A$. □

COROL·LARI 5.8. *Sigui $\succ$ una relació a $\mathbb{Z}^n_{\geq 0}$ que verifica*

(i) *$\succ$ és una relació d'ordre total a $\mathbb{Z}^n_{\geq 0}$.*
(ii) *Si $\alpha \succ \beta$ i $\gamma \in \mathbb{Z}^n_{\geq 0}$, llavors $\alpha + \gamma \succ \beta + \gamma$.*

Llavors $\succ$ és un bon ordre ssi $\alpha \succeq 0$ per tot $\alpha \in \mathbb{Z}^n_{\geq 0}$.

DEMOSTRACIÓ. $\Leftarrow$: Si existeix $0 \succ \alpha_0$ diferent de 0, afegint repetidament α_0 a cada banda, emprant (ii), tindríem una successió

$$\alpha_0 \succ 2\,\alpha_0 \succ \ldots n\,\alpha_0 \succ \ldots$$

estrictament decreixent que no estacionaria, i per tant $\prec$ no seria un bon ordre.

$\Rightarrow$: Suposem ara que tot $\alpha \in \mathbb{Z}^n_{\geq 0}$ és $\alpha \succeq 0$. Llavors si $A \subset \mathbb{Z}^n_{\geq 0}$ qualsevol demostrem que té un element mínim. En efecte, sigui $\mathcal{I} = \langle x^\alpha \ : \ \alpha \in A\rangle$. Pel lema de Dickson existeixen elements de A tals que $\mathcal{I} = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\right\rangle$. Sigui, reordenant si cal, $\alpha(1) \preceq \alpha(i)$. Anem a veure que $\alpha(1)$ és el mínim dels elements de A. En efecte, en primer lloc $x^{\alpha(1)} \in A$ per construcció. En segon lloc, si $\beta \in A$, llavors $x^\beta \in \mathcal{I}$, i pel lema 5.3 és divisible per algún $x^{\alpha(i)}$. Això implica $\beta = \gamma + \alpha(i)$. Per (ii) tindrem

$$\beta = \gamma + \alpha(i) \succeq \alpha(i) \succeq \alpha(1)$$

tal com volíem demostrar. □

6. Teorema de les bases de Gröbner

Les bases de Gröbner van ser introduïdes a mitjans dels anys 60 per H. Hironaka (que les anomenà bases estandard). Paral·lelament i independent, les va trobar B. Buchberger en la seva tesi doctoral al 1965, i les va anomenar així en honor al seu director de tesi W. Gröbner.

Definició 6.1. Donat un ideal $\mathcal{I} \subset K[\overline{x}]$ diferent de $\{0\}$ i un ordre monomial $\succ$, denotem $\mathrm{lm}(\mathcal{I})$ al conjunt dels monomis principals de tots els elements de $\mathcal{I}$:

$$\mathrm{lm}(\mathcal{I}) = \{c\, x^\alpha \ : \ c\, x^\alpha = \mathrm{lm}(f),\ f \in \mathcal{I}\},$$

i per $\langle \mathrm{lm}(\mathcal{I})\rangle$ a l'ideal de monomis generat per $\mathrm{lm}(\mathcal{I})$.

Teorema 6.2 (Base de Gröbner). *Sigui $\mathcal{I} \subset K[\overline{x}]$ un ideal diferent de $\{0\}$ i $\succ$ un ordre monomial. Llavors*

(i) *Existeix un conjunt finit $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$, tal que*

$$\langle \mathrm{lm}(\mathcal{I})\rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\rangle . \tag{6.1}$$

(ii) *Tot sub-conjunt $G \subset \mathcal{I}$ que verifiqui (6.1) és una base de $\mathcal{I}$*

$$\mathcal{I} = \langle g_1, \ldots, g_s\rangle .$$

Direm que G és una **base de Gröbner** *de $\mathcal{I}$.*

Demostració. .

(i) Pel lema de Dickson, existeix un sub-conjunt finit d'elements de $\mathrm{lm}(\mathcal{I})$ que genera $\langle \mathrm{lm}(\mathcal{I})\rangle$. Però els elements de $\mathrm{lm}(I)$ són de la forma $\mathrm{lm}(f)$, on $f \in \mathcal{I}$. Per tant, existeix $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$ tal que $\langle \mathrm{lm}(\mathcal{I})\rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\rangle$.

(ii) Demostrem que el conjunt G de (i) verifica també $\mathcal{I} = \langle g_1, \ldots, g_s\rangle$. És evident que $\langle g_1, \ldots, g_s\rangle \subseteq \mathcal{I}$, ja que cada $g_i \in \mathcal{I}$. Recíprocament, si $f \in \mathcal{I}$ l'algorisme de la divisió expressa f en la forma

$$f = a_1\, g_1 + \cdots + a_s\, g_s + r$$

on $a_1, \ldots, a_s, r \in K[\overline{x}]$ i cap monomi de r és divisible per cap dels $\mathrm{lm}(g_i)$, $1 \leq i \leq s$. Demostrarem que $r = 0$. En efecte, de l'expressió anterior en deduïm que

$$r = f - a_1\, g_1 - \cdots - a_s\, g_s \in \mathcal{I}.$$

Per tant, si $r \neq 0$ és

$$\mathrm{lm}(r) \in \langle \mathrm{lm}(\mathcal{I}) \rangle = \langle \mathrm{lm}(g_1, \ldots, \mathrm{lm}(g_s) \rangle\,.$$

Com per construcció cap monomi de r és divisible per cap $\mathrm{lm}(g_i)$ (és el residu de dividir pels g_i's), pel lema 5.3 ha de ser $r = 0$. En conseqüència $f \in \langle g_1, \ldots, g_s \rangle$, el que prova que $\mathcal{I} \subseteq \langle g_1, \ldots, g_s \rangle$. Per tant $\mathcal{I} = \langle g_1, \ldots, g_s \rangle$ i tot conjunt que verifiqui (6.1) és una base de Gröbner de $\mathcal{I}$. □

7. Propietats de les bases de Gröbner

Proposició 7.1. *Sigui $f \in K[\overline{x}]$, i $G = \langle g_1, \ldots, g_s \rangle \subset K[\overline{x}]$ una base de Gröbner d'un ideal $\mathcal{I}$. Llavors el residu $r \in K[\overline{x}]$ de la divisió de f entre G té les quatre propietats següents:*

(i) *Cap monomi de r és divisible per cap* $\mathrm{lm}(g_i)$, $1 \leq i \leq s$.
(ii) *Existeix $g \in \mathcal{I}$ tal que $f = g + r$.*
(iii) *r és únic. És a dir, no existeix cap altre r' amb les propietats* (i) *i* (ii). *En particular, el residu és independent de l'ordre en que considerem els elements de G en la divisió.*
(iv) *El residu r és zero ssi $f \in \mathcal{I}$.*

Demostració.

(i) L'algorisme de la divisió de f entre G dona

$$f = q_1\, g_1 + \cdots + q_s\, g_s + r$$

i ens mostra l'existència d'un r que verifica (i).

(ii) Tenim $g = q_1\, g_1 + \cdots + q_s\, g_s$ que verifica (ii).

(iii) Suposem que existissin dos parells (r, g) i (r', g') que complissin (i) i (ii). Tindríem $f = g + r = g' + r'$. Per tant, $r' - r = g - g' \in \mathcal{I}$. Per tant, si $r' - r \neq 0$ seria

$$\mathrm{lm}(r' - r) \in \langle \mathrm{lm}(\mathcal{I}) \rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle\,.$$

Pel lema 5.3, $\mathrm{lm}(r' - r)$ hauria de ser divisible per algún $\mathrm{lm}(g_i)$, $1 \leq i \leq s$. Però això és impossible ja que cap monomi de r ni de r' ho és. Per tant $r' - r = 0$.

(iv) És conseqüència immediata de (i), (ii) i (iii).

□

De vegades s'utilitza la caracterització que dona la proposició 7.1 per definir les bases de Gröbner. La definició de base de Gröbner per la condició (6.1) és equivalent a que per tot $f \in \mathcal{I}$ el residu de dividir f per G és zero.

La proposició 7.1 resol el problema de la pertinença a un ideal: f pertany a $\mathcal{I}$ ssi el residu de dividir f per una base de Gröbner de $\mathcal{I}$ és zero.

LEMA 7.2. *Sigui G una base de Gröbner de l'ideal $\mathcal{I} \subset K[\overline{x}]$. Sigui $p \in G$ tal que $\mathrm{lm}(p) \in \langle \mathrm{lm}(G \setminus \{p\})\rangle$. Llavors $G \setminus \{p\}$ també és una base de Gröbner de $\mathcal{I}$.*

DEMOSTRACIÓ. Sabem que $\langle \mathrm{lm}(\mathcal{I})\rangle = \langle \mathrm{lm}(G)\rangle$. Si $\mathrm{lm}(p) \in \langle \mathrm{lm}(G \setminus \{p\})\rangle$, llavors $\langle \mathrm{lm}(G \setminus \{p\})\rangle = \langle \mathrm{lm}(G)\rangle$. Per tant, $G \setminus \{p\}$ també és una base de Gröbner de $\mathcal{I}$. □

Eliminant tots els polinomis que compleixen el lema anterior un darrera de l'altre i normalitzant després, arribem a una base de Gröbner minimal.

DEFINICIÓ 7.3 (Base de Gröbner minimal). Direm que G és una base de Gröbner minimal de $\mathcal{I} \subset K[\overline{x}]$, si és una base de Gröbner tal que

(i) Per cada $p \in G$, $\mathrm{lm}(p) \notin \langle \mathrm{lm}(G \setminus \{p\})\rangle$.
(ii) Per cada $p \in G$, $\mathrm{lc}(p) = 1$.

PROPOSICIÓ 7.4. *Donades dues bases minimals G i G' del mateix ideal $\mathcal{I} \subset K[\overline{x}]$, aquestes tenen el mateix nombre de polinomis i estan en correspondència bijectiva. Els associats en la correspondència tenen el mateix monomi principal.*

DEMOSTRACIÓ. Exercici 2.16 □

EXEMPLE 7.5. Donat $F = \langle f_1, f_2\rangle$, on $f_1 = x^3 - 2\,x\,y$, i $f_2 = x^2\,y + x - 2\,y^2$ aplicant l'algorisme de Buchberger que veurem a la secció 9, calculem una base de Gröbner de F en ordre lex amb $x \succ y$. Obtenim

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

on $f_3 = x^2$, $f_4 = 2xy^2 - x^2$, $f_5 = 2xy - x^3$, $f_6 = x - 2y^2$. Per obtenir una base de Gröbner minimal, podem eliminar f_1, f_2, f_4, ja que tenen monomi principal divisible pels de f_3, f_5, f_6. Normalitzant tenim

$$G_M = [x^2, x\,y - \frac{1}{2}x^3, x - 2y^2]$$

Però un ideal admet diferents bases de Gröbner minimals. Enlloc del polinomi $x\,y - \frac{1}{2}x^3$, podem posar $x\,y$, ja que aquest darrer té el mateix monomi principal que l'anterior i també pertany a F. A fi d'obtenir una base única introduïm el concepte de base de Gröbner reduïda.

DEFINICIÓ 7.6 (Base de Gröbner reduïda). Direm que G és una base de Gröbner reduïda de $\mathcal{I} \subset K[\overline{x}]$, si és una base de Gröbner minimal tal que

(i) Per cada $p \in G$, cap monomi de p pertany a $\langle \mathrm{lm}(G \setminus \{p\})\rangle$.
(ii) Per cada $p \in G$, $\mathrm{lc}(p) = 1$.

Observis que de la base minimal de l'exemple anterior obtenim la única base reduida $G = [x^2, x\,y, x - 2y^2]$. En general, tenim la proposició següent:

PROPOSICIÓ 7.7. *Sigui $\mathcal{I} \subset K[\overline{x}]$ un ideal no nul. Llavors, fixat un ordre monomial $\succ$, $\mathcal{I}$ admet una i una sola base de Gröbner reduïda.*

DEMOSTRACIÓ. Ho provarem de forma constructiva.

Sigui G una base minimal. Per cada $g \in G$ determinem $g' = \overline{g}^{G\setminus\{g\}}$. i posem $G' = (G \setminus \{g\}) \cup \{g'\}$. És immediat comprovar que G' segueix sent una base minimal, ja que el monomi principal no ha canviat. Però g' compleix la condició (i). Fent el mateix per tots els polinomis de G, anem reduint cada polinomi de la G inicial. Observis que en fer-ho, els polinomis que ja hem reduït prèviament, continuen estant reduïts, ja que per això únicament compten els monomis principals, i aquests no canvien en el procés. El resultat és una base de Gröbner reduïda.

No més cal provar que aquesta és única. Si existissin dues G i G', ambdues serien minimals. No més cal provar que els polinomis $g \in G$ i $g' \in G'$ que es corresponen per tenir el mateix monomi principal són iguals. En efecte, $r = g - g' \in \mathcal{I}$ i per tant, el residu de dividir-lo per G és zero. Però cap monomi de g ni de g' és divisible per cap monomi principal de G, i per tant passen directament al residu. Com que aquest és nul, això implica que $g - g' = \overline{g - g'}^{G} = 0$. □

COROL·LARI 7.8 (Igualtat d'ideals). *Dos ideals són iguals ssi tenen la mateixa base de Gröbner reduïda per un ordre monomial $\succ$.*

L'ideal $\mathcal{I}_1$ està contingut en $\mathcal{I}_2$, $\mathcal{I}_1 \subset \mathcal{I}_2$, si tots els generadors d'una base del segon redueixen a zero al ser dividits per una base de Gröbner del primer.

L'existència d'una base de Gröbner reduïda única per cada ordre monomial resol el problema de la descripció dels ideals.

El problema és ara saber detectar quan un conjunt de generadors d'un ideal $\mathcal{I}$ és una base de Gröbner i saber construir-ne una a partir d'un conjunt donat de generadors. Això serà l'objecte de la secció següent. Veiem, però un exemple.

8. Determinació de les bases de Gröbner

Demostrada l'existència de bases de Gröbner, ara ens cal saber reconèixer si una base donada ho és i saber completar una base donada d'un ideal fins a obtenir una base de Gröbner.

En tot el que segueix, suposarem fixat un ordre monomial $\succ$, i tots els càlculs seran relatius a l'ordre donat.

Hem vist que el residu de dividir un polinomi per una base de Gröbner és únic. Per tant, si F és una base de Gröbner de $\mathcal{I} = \langle f_1, \ldots, f_s\rangle$, llavors al fer la divisió, l'ordre en els f_i no importa, i a més a més, $\overline{f}^{F}$ és el representant canònic de $K[\overline{x}]/\mathcal{I}$ equivalent a f tal que cap monomi és divisible per cap $\mathrm{lm}(g_i)$, per $1 \leq i \leq s$.

A fi de determinar una base de Gröbner, ens interessa generalitzar el mètode d'eliminació de Gauss. El S-polinomi, que introduïm a continuació, juga aquest paper:

DEFINICIÓ 8.1 (S-polinomi). Siguin $f, g \in K[\overline{x}]$, no nuls. Siguin

$$\begin{array}{rcl} \alpha & = & \text{multideg}(f), \\ \beta & = & \text{multideg}(g), \\ x^\gamma & = & \text{lcm}(x^\alpha, x^\beta) \end{array}$$

Definim el S-polinomi de f i g per

$$S(f,g) = \frac{x^\gamma}{\text{lm}(f)}\, f - \frac{x^\gamma}{\text{lm}(g)}\, g$$

Els S-polinomis produeixen cancel·lació de monomis principals. En conseqüència, és evident que

$$\text{multideg}(S) \prec \gamma$$

A fi de provar el teorema de reconeixement d'una base de Gröbner, necessitem un lema tècnic:

LEMA 8.2. *Sigui una suma de la forma* $S = \sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i$, *on*

$\text{lm}(g_i) = d_i\, x^{\beta(i)}$
$c_i \in K$ *per* $1 \le i \le t$,
$\alpha(i) + \beta(i) = \delta \in \mathbb{Z}^n_{\ge 0}$ *si* $c_i \neq 0$.

Si $\text{multideg}(S) \prec \delta$, *és a dir, si hi ha cancel·lació de monomis principals, llavors*

(i) *existeixen constants* $c_{jk} \in K$ *tals que*

$$\sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i = \sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}}\, S(g_j, g_k),$$

on

$$x^{\gamma_{jk}} = \text{lcm}(\text{lpp}(g_j), \text{lpp}(g_k)); \tag{8.1}$$

(ii) *cada sumand* $c_{jk}\, x^{\delta-\gamma_{jk}}\, S(g_j, g_k)$ *té multigrau estrictament inferior a* δ.

OBSERVACIÓ 8.3. La importància del lema radica en que a la fórmula del lema, cada sumand del primer membre té el mateix monomi principal x^δ, i es produeix la cancel·lació de monomi principal un cop efectuada tota la suma. En canvi, en el segon membre, cada terme ja te un monomi principal de multigrau menor que δ.

En altres paraules, el lema expressa que tota cancel·lació de monomis principals pot expressar-se en termes de S-polinomis, on cada terme té multigrau estrictament menor que el monomi principal cancel·lat.

DEMOSTRACIÓ. Amb la notació de l'enunciat, el coeficient principal de $c_i\, x^{\alpha(i)}\, g_i$ serà $c_i\, d_i$. Tenint en compte que cada un d'aquests sumands té el

mateix multigrau δ i que la suma té multigrau estrictament inferior, resulta que $\sum_{i=1}^{t} c_i\, d_i = 0$.

Posem $p_i = x^{\alpha(i)}\, g_i/d_i$. Observem que el coeficient principal de p_i és 1. Ara considerarem un desenvolupament telescòpic de la suma. Però abans hem de comentar, que hi poden haver termes i que no hi figurin en la suma, de manera, que al considerar el desenvolupament telescòpic, cal entendre que parlem dels indexos correlatius presents en la suma, que no són necessàriament tots els i. Amb aquesta observació, considerem el desenvolupament telescòpic següent

$$\begin{aligned}\sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i &= \sum_{i=1}^{t} c_i\, d_i\, p_i = c_1\, d_1\, (p_1 - p_2) + (c_1\, d_1 + c_2\, d_2)(p_2 - p_3) + \dots \\ &\quad + (c_1\, d_1 + \cdots + c_{t-1}\, d_{t-1})(p_{t-1} - p_t) + p_i \sum_{i=1}^{t} c_i\, d_i\end{aligned}$$

Per hipòtesi $\alpha(i) + \beta(i) = \delta$. Per tant $\mathrm{lpp}(g_i) \mid x^{\delta}$ per $1 \leq i \leq t$. En conseqüència $x^{\gamma_{jk}} \mid x^{\delta}$, i per tant, $x^{\delta - \gamma_{jk}} \in \mathbb{Z}^n_{\geq 0}$. Anàlogament $x^{\gamma_{jk} - \beta(i)} \in \mathbb{Z}^n_{\geq 0}$. Per tant,

$$\begin{aligned}x^{\delta - \gamma_{jk}}\, S(g_j, g_k) &= x^{\delta - \gamma_{jk}} \left(\frac{x^{\gamma_{jk}}}{\mathrm{lm}(g_j)}\, g_j - \frac{x^{\gamma_{jk}}}{\mathrm{lm}(g_k)}\, g_k \right) \\ &= \frac{x^{\delta}}{d_j\, x^{\beta(j)}}\, g_j - \frac{x^{\delta}}{d_k\, x^{\beta(k)}}\, g_k \\ &= \frac{x^{\alpha(j)}}{d_j}\, g_j - \frac{x^{\alpha(k)}}{d_k}\, g_k = p_j - p_k.\end{aligned}$$

Substituint a la suma anterior, i tenint en compte que el darrer sumand es cancel·la, resulta

$$\sum_{i=1}^{t} c_i\, x^{\alpha(i)}\, g_i = \sum_{j,k} c_{jk}\, x^{\delta - \gamma_{j,k}}\, S(g_j, g_k).$$

Cal recordar, segons el comentari fet més amunt, que a la suma, únicament figuren els indexos j, k de la forma i_k, i_{k+1}, on $i_1 < \cdots < i_t$ és el conjunt de indexos pels que figuraven g_{i_k}, en la suma del primer membre del lema. En conseqüència, no podem considerar únicament els $S(g_j, g_k)$ d'indexos correlatius, quedant provada la part (i) del lema.

Pel que fa a la part (ii), només cal tenir en compte que $\mathrm{multideg}(S(g_j, g_k)) \prec \gamma_{jk}$. □

TEOREMA 8.4 (Reconeixement d'una base de Gröbner). *Sigui $\mathcal{I} \subset K[\overline{x}]$ un ideal. Llavors $G = \{g_1, \dots, g_s\} \subset \mathcal{I}$ és una base de Gröbner de $\mathcal{I}$ per*

un ordre monomial $\succ$ donat, ssi per cada parell $i \neq j$, el residu de dividir $S(g_i, g_j)$ per G, (amb la s-tupla en un ordre fixat) és zero.

DEMOSTRACIÓ. $\Rightarrow$: Òbviament, Si G és una base de Gröbner com que cada S-polinomi pertany a $\langle G\rangle$, la proposició 7.1 assegura que el residu és zero.

$\Leftarrow$: Hem de provar que si $f \in \mathcal{I}$, i tots els S-polinomis tenen residu zero, llavors $\mathrm{lm}(f) \in \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\rangle$. Abans de provar-ho, anem a donar l'estratègia de la prova.

Donat $f \in \langle g_1, \ldots, g_s\rangle$ existeixen polinomis $h_i \in K[\overline{x}]$ tals que

$$f = \sum_{i=1}^{s} h_i\, g_i$$

Posem

$$m(i) = \mathrm{multideg}(h_i\, g_i), \quad \text{i} \quad \delta = \max_i \{m(1), \ldots, m(s)\}\,.$$

Pel lema 3.9 es verifica $\mathrm{multideg}(f) \preceq \delta$. Si no hi ha igualtat, és que es produeix alguna cancel·lació de monomis principals al segon membre. Entre les expressions de f en termes dels g_i n'hi poden haver moltes. Com que $\succ$ és un bon ordre, existeix alguna expressió que correspon a una δ mínima.

L'estratègia consistirà en provar que un cop triada una expressió amb δ mínima, si tots els residus dels S-polinomis són nuls, llavors $\mathrm{multideg}(f) = \delta$, i per tant existeix algún i amb $m(i) = \delta = \mathrm{multideg}(f)$. Això implica que $\mathrm{lpp}(g_i) \mid \mathrm{lpp}(f)$, i per tant que $\mathrm{lm}(f) \in \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\rangle$, tal com volem provar.

Queda per provar, que si tots els $\overline{S(g_i, g_j)}^{G} = 0$, llavors $\mathrm{multideg}(f) = \delta$. Ho provarem per reducció a l'absurd. Suposarem que δ és mínima i que en canvi $\mathrm{multideg}(f) \prec \delta$. Utilitzant la condició sobre els S-polinomis i el lema anterior 8.2 aconseguirem una nova expressió de f en termes dels g_i amb un $\delta' \prec \delta$, arribant a una contradicció. Veiem els detalls.

L'expressió de f amb δ mínima pot posar-se en la forma següent:

$$\begin{aligned} f &= \sum_{i=1}^{s} h_i\, g_i = \sum_{m(i)=\delta} h_i\, g_i + \sum_{m(i)\prec\delta} h_i\, g_i \\ &= \sum_{m(i)=\delta} \mathrm{lm}(h_i)\, g_i + \sum_{m(i)=\delta} (h_i - \mathrm{lm}(h_i))g_i + \sum_{m(i)\prec\delta} h_i\, g_i \end{aligned}$$

Únicament els productes de potències de la primera suma de la segona linea tenen multigrau igual a δ.

Posem $\mathrm{lm}(h_i) = c_i\, x^{\alpha(i)}$. Llavors la suma esmentada

$$S_\delta = \sum_{m(i)=\delta} \mathrm{lm}(h_i)\, g_i = \sum_{m(i)=\delta} c_i\, x^{\alpha(i)}\, g_i$$

té exactament la forma i les condicions del primer membre de l'equació del lema 8.2, ja que hem suposat que $\mathrm{multideg}(f) \prec \delta$. L'esmentat lema permet,

llavors expressar aquesta suma així:

$$S_\delta = \sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}}\, S(g_i, g_j),$$

on $c_{jk} \in K$, i $x^{\gamma_{jk}}$ donat per la fórmula (8.1).

Ara utilitzem la hipòtesi $\overline{S(g_i, g_j)}^G = 0$, per $1 \leq i < j \leq s$. Per l'algorisme de la divisió, aquesta hipòtesi implica que existeix una expressió de cada S-polinomi de la forma

$$S(g_i, g_j) = \sum_{i=1}^{t} a_{ijk}\, g_i$$

on $a_{ijk} \in K[\overline{x}]$ i

$$\text{multideg}(a_{ijk}\, g_i) \preceq \text{multideg}(S(g_j, g_k)) \prec \gamma_{jk}$$

per cada i, j, k. Aquest resultat el podem interpretar dient que la hipòtesi sobre els S-polinomis ens permet expressar cada S-polinomi en termes dels g_i's sense que hi hagi cancel·lació.

El resultat obtingut ens permet reescriure ara la suma S_δ així:

$$S_\delta = \sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}} \left(\sum_i a_{ijk}\, g_i \right) = \sum_i \left(\sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}}\, a_{ijk} \right) g_i$$

on, per cada i, $1 \leq i \leq s$ és

$$\text{multideg} \left((\sum_{j,k} c_{jk}\, x^{\delta-\gamma_{jk}}\, a_{ijk})\, g_i \right) \prec \delta$$

Substituint ara aquesta expressió de S_δ en l'expressió completa de f, arribem a una expressió de la forma $f = \sum_i \tilde{h}_i\, g_i$ que correspondria a una δ inferior a la mínima precedent. Tenim, doncs, la contradicció esperada, i per tant, si l'expressió de f en termes dels g_i correspon a δ mínim, llavors

$$\text{multideg}(f) = \delta$$

el que implica que $\text{lm}(f) \in \langle \text{lm}(g_1), \ldots, \text{lm}(g_s) \rangle$, tal com volíem demostrar. □

9. Algorisme de Buchberger

TEOREMA 9.1. *Sigui $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ un ideal de $K[\overline{x}]$. Llavors, l'algorisme següent construeix una base de Gröbner en un nombre finit de passos:*

Algorisme de Buchberger

Input: $F = [f_1, \ldots, f_s]$. Un ordre monomial $\succ$.
Output: $G = [g_1, \ldots, g_m]$, base de Gröbner de $\mathcal{I}$, amb $F \subset G$.

$G := F$
REPETIR
  $G' := G$
  PER cada parell $\{p, q\} \in G'$, $p \neq q$ FER
    $S := \overline{S(p,q)}^{G'}$
    SI $S \neq 0$ LLAVORS $G := G \cup \{S\}$ FI SI
  FI PER
FINSQUE $G = G'$.

DEMOSTRACIÓ. En primer lloc, $G \subset \mathcal{I}$, ja que ho és inicialment, i durant l'algorisme, únicament s'afegeixen a G polinomis de $\mathcal{I}$. Per construcció, també $F \subset G$.

En segon lloc, l'algorisme acaba quan $G = G'$, es a dir quan tots els $\overline{S(p,q)}^{G} = 0$ per cada $(p, q) \in G$. Pel teorema 8.4, això implica que G és una base de Gröbner de $\langle G \rangle = \mathcal{I}$.

Només cal provar que l'algorisme acaba. Però observem que passa al final de cada pas del bucle principal. Tindrem

$$\langle \mathrm{lm}(G') \rangle \subset \langle \mathrm{lm}(G) \rangle$$

ja que $G' \subset G$. Però si $G \neq G'$ demostrarem que $\langle \mathrm{lm}(G') \rangle$ és estrictament menor que $\langle \mathrm{lm}(G) \rangle$. En efecte, si $G \neq G'$, és que, abans d'acabar el bucle, s'ha afegit algun residu r no nul d'un S-polinomi dividit per G'. Per tant, cap monomi de r és divisible per cap monomi principal de G'. Per tant, $\mathrm{lm}(r) \notin \langle \mathrm{lm}(G') \rangle$. En canvi $\mathrm{lm}(r) \in \langle \mathrm{lm}(G) \rangle$, i per tant la inclusió és estricta.

Si considerem la successió de $\langle \mathrm{lm}(G) \rangle$'s de cada pas del bucle, és una cadena d'ideals estrictament ascendent. Per ser $K[\overline{x}]$ un anell Noetherià, la cadena estabilitza. Arribarà un moment en que $\langle \mathrm{lm}(G') \rangle = \langle \mathrm{lm}(G) \rangle$. Com que la successió és estrictament creixent, això s'ha de produir en un nombre finit de passos de l'algorisme. Per tant, l'algorisme acaba. □

Cal observar que la versió donada de l'algorisme de Buchberger és molt ineficient, ja que verifica moltes més coses de les necessàries. Més endavant donarem una versió més pràctica.

10. Millores de l'algorisme de Buchberger

L'algorisme de Buchberger té una complexitat intrínseca elevada. Quan volem implementar un algorisme matemàtic, a més de posar atenció en la seva correcció, hem de posar èmfasi en altres qüestions i en particular en la seva eficiència. Hem d'intentar minimitzar els càlculs que fem. La versió donada en la secció anterior és exclusivament teòrica, ja que verifica a cada

pas tots els residus dels S-polinomis. Anem a veure algunes millores que el fan més pràctic.

DEFINICIÓ 10.1. Donats un conjunt $G = \{g_1, \ldots, g_s\} \subset K[\overline{x}]$ i un ordre monomial $\succ$, direm que $f \in K[\overline{x}]$ **redueix a zero mòdul** G i posarem $f \to_G 0$, si

(i) existeix una expressió de la forma

$$f = q_1\, g_1 + \cdots + q_s\, g_s$$

(ii) tal que si $q_i\, g_i \neq 0$, llavors

$$\text{multideg}(f) \succeq \text{multideg}(q_i\, g_i)$$

Òbviament, si $\overline{f}^G = 0$ llavors $f \to_G 0$. En canvi el recíproc no és cert en general.

EXEMPLE 10.2. Si posem $f = 2\,x^2\,y^2 - x\,y$, $g_1 = x^2 + y^2$, $g_2 = 2\,x\,y - 1$, el resultat de dividir f entre $[g_1, g_2]$ és

$$f = (2\,y^2)\,g_1 + (-\frac{1}{2})\,g_2 + (-2\,y^4 - \frac{1}{2})$$

i per tant $\overline{f}^G = -2\,y^4 - \frac{1}{2} \neq 0$. En canvi si dividim f entre $[g_2, g_1]$ el resultat és

$$f = (x\,y)\,g_1 + 0\,g_2$$

i per tant $f \to_G 0$.

Aquesta definició permet rebaixar la hipòtesi del teorema 8.4 substituint divisió per reducció, ja que de fet, és la única cosa que hem utilitzat en la demostració. Tenim doncs

TEOREMA 10.3. *Sigui $\mathcal{I} \subset K[\overline{x}]$ un ideal. Llavors $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$ és una base de Gröbner de $\mathcal{I}$ per un ordre monomial $\succ$ donat, ssi per cada parell $i \neq j$, $S(g_i, g_j) \to_G 0$.*

La següent proposició ens evitarà calcular alguns residus de S-polinomis.

PROPOSICIÓ 10.4. *Donat un conjunt $G \subset K[\overline{x}]$ i un ordre monomial, siguin $f, g \in G$. Si $\text{lpp}(f)$ i $\text{lpp}(g)$ no tenen variables en comú (és a dir, si $\text{lcm}(\text{lpp}(f), \text{lpp}(g)) = \text{lpp}(f) \cdot \text{lpp}(g)$), llavors $S(f, g) \to_G 0$.*

DEMOSTRACIÓ. Siguin

$$f = a\,x^\alpha + f_r, \quad g = b\,x^\beta + g_r$$

on $\text{multideg}(f_r) \prec \text{multideg}(f)$ i $\text{multideg}(g_r) \prec \text{multideg}(g)$. Si es compleix la hipòtesi tenim

$$\begin{aligned} S(f,g) &= \frac{b\,x^\beta}{a\,b} f - \frac{a\,x^\alpha}{a\,b} g \\ &= \frac{1}{a\,b}\left((g - g_r)f - (f - f_r)g\right) = \frac{1}{a\,b}\left(f_r\,g - g_r\,f\right) \end{aligned}$$

i a més a més

$$\text{multideg}(S(f,g)) = \max\left(\text{multideg}(f_r\, g), \text{multideg}(g_r\, f)\right),$$

ja que si hagués cancel.lació de monomis principals això implicaria la igualtat $x^\beta\ \text{lpp}(f_r) = x^\alpha\ \text{lpp}(g_r)$. Però tenint en compte que x^α i x^β són primers entre si, caldria que $x^\beta \mid \text{lpp}(g_r)$, el que és impossible. □

EXEMPLE 10.5. Amb aquesta proposició és immediat comprovar que

$$G = \left\{x^3 - y\,z^2 + 3, y\,z^2 - z^5, u^3 + 2\,u^2 + u\right\}$$

és una base de Gröbner respecte a l'ordre lex $x \succ y \succ z \succ u$.

En efecte, com que els monomis principals són primers entre si dos a dos, els tres S-polinomis redueixen a zero, i el teorema 10.3 assegura que G és una base de Gröbner.

EXEMPLE 10.6. Anàlogament, aquesta proposició assegura immediatament que la base produïda per eliminació gaussiana en un sistema lineal, és una base de Gröbner minimal, ja que els monomis principals tenen variables disjuntes.

La següent definició generalitza el concepte de S-polinomi.

DEFINICIÓ 10.7 (Syzygies). Sigui $F = [f_1, \ldots, f_s] \in (K[\overline{x}])^s$. Una syzygia sobre els monomis principals dels polinomis de F és una s-tupla de polinomis $S = [h_1, \ldots, h_s] \in (K[\overline{x}])^s$ tal que

$$\sum_{i=1}^{s} h_i\ \text{lm}(f_i) = 0.$$

Anomenarem $S(F)$ al sub-conjunt d'elements de $(K[\overline{x}])^s$ format per totes les syzygies sobre els monomis principals de F.

Podem considerar una syzygia com un vector de $(K[\overline{x}])^s$. Si denotem $\mathbf{e}_i = [0, \ldots, 0, 1, 0, \ldots, 0]$ els elements de la base canònica de K^s, llavors la syzygia de la definició pot expressar-se en la forma $S = \sum_{i=1}^{s} h_i\, \mathbf{e}_i$.

En particular, els S-polinomis són syzygies relatives a dos polinomis (d'aquí el seu nom de Syzygia-polinomi):

$$S_{ij} = \frac{x^{\gamma_{ij}}}{\text{lm}(f_i)}\mathbf{e}_i - \frac{x^{\gamma_{ij}}}{\text{lm}(f_j)}\mathbf{e}_j$$

La relació amb l'S-polinomi és:

$$S(g_i, g_j) = S_{ij} \cdot G$$

És immediat veure que $S(F)$ és tancat per suma (de vectors) i per multiplicació per polinomis (escalars). Per tant formen l'anàleg d'un espai vectorial, però sobre l'anell $K[\overline{x}]$. Aquesta estructura s'anomena mòdul. Les syzygies formen, doncs un $K[\overline{x}]$-mòdul.

Una particularitat essencial de $S(F)$ és que admet una base finita. Abans de demostrar-ho ens cal aprofundir un xic més sobre les syzygies.

En primer lloc, definim el concepte de syzygia homogènia.

DEFINICIÓ 10.8. Un element de $S(F)$ és **homogènia de multigrau** $\delta \in \mathbb{Z}^n_{\geq 0}$, si és de la forma

$$S = [c_1\, x^{\alpha_1}, \ldots, c_s\, x^{\alpha_s}],$$

on $c_i \in K$ i $\alpha_i + \text{multideg}(f_i) = \delta$ si $c_i \neq 0$.

En particular, la syzygia S_{ij}, associada al S-polinomi $S(g_i, g_j)$, és una syzygia homogènia de multigrau γ_{ij}.

LEMA 10.9. *Tot element de $S(F)$ pot expressar-se de forma única com a suma de syzygies homogènies de $S(F)$.*

DEMOSTRACIÓ. Sigui $S = [h_1, \ldots, h_s] \in S(F)$. Fixat un exponent δ, sigui $h_{i\delta}$ el monomi de h_i, si existeix, tal que $h_{i\delta}\,\text{lm}(f_i)$ té multigrau δ. S'ha de cumplir que $\sum_{i=1}^s h_{i\delta}\,\text{lm}(f_i) = 0$. Per tant, $S_\delta = [h_{1\delta}, \ldots, h_{s\delta}]$ és una syzygia homogènia de $S(F)$. Òbviament, $S = \sum_\delta S_\delta$.

Com el component $h_{i\delta}$ és un monomi $c_i x^{\alpha(i)}$ de h_i, i és l'únic component de h_i de multigrau igual a $\delta - \text{multideg}(f_i)$, està unívocament determinat. □

PROPOSICIÓ 10.10. *Donat $F = [f_1, \ldots, f_s]$.*

(i) *Cada element $S \in S(F)$ pot posar-se en la forma*

$$S = \sum_{ij} u_{ij}\, S_{ij}$$

on $u_{ij} \in K[\overline{x}]$ i S_{ij} són les syzygies corresponents als S-polinomis.

(ii) *En la descomposició anterior, si S és homogènia, es manté el multigrau δ d'homogeneïtat.*

DEMOSTRACIÓ. Pel lema anterior, podem suposar que S és homogènia de multigrau δ. Siguin i, j dues components no nules de S amb $i < j$ (necessàriament n'ha de tenir al menys dues). Siguin aquestes $c_i\, x^{\alpha_i}$ i $c_j\, x^{\alpha_j}$. Llavors $\alpha_i + \text{multideg}(f_i) = \alpha_j + \text{multideg}(f_j) = \delta$. Per tant $x^{\alpha_i} \mid x^\delta$ i $x^{\alpha_j} \mid x^\delta$. En conseqüència $x^{\gamma_{ij}} \mid x^\delta$, on $x^{\gamma_{ij}} = \text{lcm}(x^{\alpha_i}, x^{\alpha_j})$. Llavors

$$S' = S - c_i\ \text{lc}(f_i) x^{\delta - \gamma_{ij}} S_{ij}$$

té la seva component i-èsima nula. Apart de la component i, l'única altra component de S' diferent de S és la j que haurà variat en el seu coeficient de K. Hem obtingut una nova syzygia S' de multigrau δ, amb una component menys que S i sense alterar el multigrau δ d'homogeneïtat. Continuant el procediment amb la component j i la següent component no nul.la de S' acabarem expressant S com a combinació de les S_{ij}. □

Aquesta proposició precisa la idea de que tota cancel·lació de monomis principals pot expresar-se en termes de S-polinomis.

Hem demostrat que les S_{ij} per $i < j$ formen una base de totes les syzygies de $S(F)$. Però observem que no sempre són independents.

EXEMPLE 10.11. Sigui $F = [x^2\,y^2 + z^2, x\,y^2 + y^2, x^2\,y + y\,z]$ i considerem l'ordre lex amb $x \succ y \succ z$. Les tres syzygies corresponents als tres S-polinomis són:

$$S_{12} = [1, -x, 0], \quad S_{13} = [1, 0, -y], \quad S_{23} = [0, x, -y].$$

Observem que $S_{23} = S_{13} - S_{12}$. Per tant, S_{23} és combinació de les altres dues i pot eliminar-se de la base.

EXEMPLE 10.12. Sigui $G = [x^2yz - y^2, xy^2z - x + y^3, xyz^2 - xz - y, x^2y^2 + z^2]$. Considerem ordre lex amb $x \succ y \succ z$.

a) Determinem totes les syzygies corresponents a S-polinomis.
b) Expressem la syzygia $S = [2xyz, -x^2z, 3x^2y, -4xz^2]$ en termes de les anteriors.
c) Trobem una base mínima de syzygies.

a) Les syzygies corresponents als S-polinomis són:

$$\begin{array}{rcl}
S_{12} & = & [\ y, \ -x, \ 0, \ 0\ ] \\
S_{13} & = & [\ z, \ 0, \ -x, \ 0\ ] \\
S_{14} & = & [\ y, \ 0, \ 0, \ -z\ ] \\
S_{23} & = & [\ 0, \ z, \ -y, \ 0\ ] \\
S_{24} & = & [\ 0, \ x, \ 0, \ -z\ ] \\
S_{34} & = & [\ 0, \ 0, \ xy, \ -z^2\ ]
\end{array}$$

b) Per determinar S en termes de les syzygies corresponents als S-polinomis, fem

$$\begin{array}{rcl}
S_1 = S - 2xzS_{12} & = & [\ 0, \ x^2z, \ 3x^2y, \ -4xz^2\ ] \\
S_2 = S_1 - x^2S_{23} & = & [\ 0, \ 0, \ 4x^2y, \ -4xz^2\ ] \\
S_3 = S_2 - 4xS_{34} & = & [\ 0, \ 0, \ 0, \ 0\ ]
\end{array}$$

Finalment, doncs,

$$S = 2xzS_{12} + x^2S_{23} + 4xS_{34}$$

c) Observem ara que aquest mateix procés el podem fer per expressar algunes de les syzygies corresponents a S-polinomis en termes de les altres. Així:

$$\begin{array}{rcl}
S_{14} - S_{24} & = & [\ y, \ -x, \ 0, \ 0\ ] \ = \ S_{12} \\
S_{34} - zS_{24} & = & [\ 0, \ -zx, \ xy, \ 0\ ] \\
& = x & [\ 0, \ -z, \ y, \ 0\ ] \ = \ -xS_{23}
\end{array}$$

TEOREMA 10.13. *Un conjunt $G = \{g_1, \ldots, g_s\} \subset \mathcal{I}$ és una base de Gröbner de l'ideal $\mathcal{I} \subset K[\overline{x}]$ per un ordre monomial donat, si per cada element $S = [h_1, \ldots, h_s]$ d'una base homogènia de syzygies de $S(G)$ es verifica*

$$S \cdot G = \sum_{i=1}^{s} h_i\, g_i \to_G 0.$$

DEMOSTRACIÓ. Pel teorema 8.4, G és una base de Gröbner si totes les syzygies redueixen a zero. Tenint en compte que en la descomposició d'una syzygia homogènia en una base de syzygies el multigrau d'homogeneïtat es manté, és obvi que si les syzygies d'una base redueixen a zero, les restants syzygies també redueixen a zero mòdul G. □

Ara hem de saber com fer més petita una base de syzygies. Hi ha manera d'obtenir bases minimals, però una forma general de reduir-les es basa en la proposició següent

PROPOSICIÓ 10.14. *Sigui $G = \{g_1, \ldots, g_s\}$ una base de $\mathcal{I}$, i sigui*

$$S \subset \{S_{ij} \ : \ 1 \leq i < j \leq s\}$$

una base de les syzygies $S(G)$. Si existeixen elements diferents $g_i, g_j, g_k \in G$ tals que

$$\mathrm{lpp}(g_k) \mid \mathrm{lcm}(\mathrm{lpp}(g_i), \mathrm{lpp}(g_j)),$$

i $S_{ik}, S_{jk} \in S$, llavors $S \setminus \{S_{ij}\}$ també és una base de $S(G)$.

DEMOSTRACIÓ. Suposem, per simplificar que $i < j < k$ i siguin $x^{\gamma_{ij}}, x^{\gamma_{ik}}, x^{\gamma_{jk}}$ els habituals lcm's. La hipòtesi implica que $x^{\gamma_{ik}} \mid x^{\gamma_{ij}}$ i $x^{\gamma_{jk}} \mid x^{\gamma_{ij}}$. Per tant resulta

$$\begin{aligned} S_{ij} &= \frac{x^{\gamma_{ij}}}{x^{\gamma_{ik}}}\left(\frac{x^{\gamma_{ik}}}{\mathrm{lm}(g_i)}\mathbf{e}_i - \frac{x^{\gamma_{ik}}}{\mathrm{lm}(g_k)}\mathbf{e}_k\right) + \frac{x^{\gamma_{ij}}}{x^{\gamma_{jk}}}\left(\frac{x^{\gamma_{jk}}}{\mathrm{lm}(g_k)}\mathbf{e}_k - \frac{x^{\gamma_{jk}}}{\mathrm{lm}(g_j)}\mathbf{e}_j\right) \\ &= \frac{x^{\gamma_{ij}}}{x^{\gamma_{ik}}}S_{ik} - \frac{x^{\gamma_{ij}}}{x^{\gamma_{jk}}}S_{jk} \end{aligned}$$

amb multideg homogeni γ_{ij}, quedant demostrada la proposició. □

Algorisme de Buchberger millorat

Input: $F = \{f_1, \ldots, f_s\}$. Un ordre monomial $\succ$.
Output: $G = \{g_1, \ldots, g_m\}$, base de Gröbner de $\mathcal{I}$, amb $F \subset G$.

$B := \{\{i, j\} \ : \ 1 \leq i < j \leq s\}$
$G := F$; $m := s$
MENTRE $B \neq \phi$ FER
  Seleccionar un element $\{i, j\} \in B$
  $B := B \setminus \{\{i, j\}\}$
  SI variables(lpp(f_i)) $\cap$ variables(lpp(f_j)) $\neq \phi$
    SI Criteri(f_i, f_j, B, G) és fals LLAVORS
      $S := \overline{S(f_i, f_j)}^G$
      SI $S \neq 0$ LLAVORS
        $m := m + 1$
        $f_m := S$
        $G := G \cup \{f_m\}$
        $B := B \cup \{\{n, m\} \ : \ 1 \leq n < m\}$
      FI SI
    FI SI
  FI SI
FI MENTRE

S'han incorporat les proposicions 10.4 i 10.14 en l'algorisme de Buchberger millorat que el fan més eficient que l'emprat per la demostració. Fem servir els parells ordenats $[i, j]$ amb $i < j$ per identificar les syzygies corresponents.

La funció Criteri(f_i, f_j, B) retorna cert si existeix algún $k \notin \{i, j\}$ pel qual $\{i, k\}$ i $\{j, k\}$ no estan a B i tal que lpp(f_k) | lcm(lpp(f_i), lpp(f_j)).

La funció Criteri està basada en la proposició 10.14, i el primer criteri per evitar calcular residus de S-polinomis en la proposició 10.4.

L'algorisme donat pot millorar-se. Per una discussió més detallada consultar [1] [2].

Normalment, després de calcular una base de Gröbner, s'acaba determinant primer una base minimal i finalment una base reduïda. Els programes de càlcul simbòlic determinen, en general, la base reduïda.

---

[1](1985) B. Buchberger, "Gröbner bases: an algorithmic method in polynomial ideal theory"a "Multidimensional Systems Theory", ed. N.K. Bose, D. Reidel, Publishing Company, Dordrecht, 184-232.

[2](1988) R. Gebauer & H.M. Möller, "On an installation of Buchberger's algorithm"a "Computational Aspects of Commutative Algebra", ed. L.Robbiano, Academic Press, New-York, 15-33.

Acabem comentant una mica la complexitat de l'algorisme. A pesar de les millores actuals de l'algorisme, resulta fàcil donar exemples de bases per les quals l'algorisme queda col·lapsat en temps i memòria.

Entre d'altres problemes el grau dels polinomis intermedis que es produeixen durant l'evolució de l'algorisme pot créixer molt. També solen créixer molt la grandària dels coeficients.

En general, l'ordre monomial que sol donar menor grau dels polinomis intermedis és grevlex, mentre que lex sol donar una major complexitat [3] [4].

Actualment hi han noves millores de l'algorisme i hi ha molt treball de recerca sobre el tema.

[3](1987) D. Bayer & M. Stillman, "A criterion for detecting m-regularity", Invent. Math. **87**, 1-11.

[4](1987) D. Bayer & M. Stillman, "A theorem on refining division orders by the reverse lexicographic order", Duke J. Math. **55**, 321-328.

11. Exercicis

Secció 3.

EXERCICI 2.1. Demostreu la proposició 3.6.

EXERCICI 2.2. (*)

(1) Quants productes de potències diferents de grau total m amb n variables hi ha?
(2) Proveu que pels ordres grevlex i grlex tot producte de potències x^α té un anterior $A(x^\alpha) = x^{\alpha'}$ tal que $x^\alpha \succ x^{\alpha'}$ i no hi ha cap altre entre ambdós. Escriviu 10 multigraus en ordre grevlex descendent a partir de $(2, 1, 3, 4)$.
(3) Quina és la distància grevlex entre $(2, 1, 3, 4)$ i $(6, 2, 1, 3)$?
(4) Determineu el monomi anterior a $(\alpha_1, \ldots, \alpha_n)$ en ordre grevlex i proveu que ho és.
(5) Existeix l'anterior per l'ordre lex? Té sentit la pregunta de la distància per l'ordre lex? Quin seria el multigrau anterior a $(3, 2, 0, 5)$ en odre lex? I l'anterior a $(3, 2, 0, 0)$?

EXERCICI 2.3. Proveu el lema 3.9.

Secció 4.

EXERCICI 2.4. Comproveu que fent la divisió de l'exemple 4.1 amb els divisors en l'ordre f_2, f_1, el residu de la divisió és $2\,x + 1$ i resultat de la divisió és:

$$f = x^2\,y + x\,y^2 + y^2 = (x + 1) \cdot f_2 + x \cdot f_1 + (2\,x + 1)$$

EXERCICI 2.5. Calculeu el residu de la divisió en ordre lex(x, y, z) de

a) $f = xy^2z^2 + xy - yz$ entre $F = (x - y^2, y - z^3, z^2 - 1)$.
b) Repetiu-ho fent permutacions cícliques a F.
c) Repetiu-ho en ordre grevlex(x, y, z). Comenteu les diferències.

EXERCICI 2.6. (*) Ara estudiarem la divisió de $f = x^3 - x^2y - x^2z + x$ per $f_1 = x^2y - z$ i $f_2 = xy - 1$

a) Calculeu utilitzant l'ordre grlex :

$$\begin{aligned} r_1 &= \text{residu de dividir } f \text{ per } (f_1, f_2) \\ r_2 &= \text{residu de dividir } f \text{ per } (f_2, f_1) \end{aligned}$$

Els resultats haurien de ser diferents. En quin pas de l'algorisme radica la diferència?. (Cal que feu uns quants passos a mà)
b) és $r = r_1 - r_2$ a l'ideal $\langle f_1, f_2 \rangle$? Si la resposta és positiva trobeu una expressió explícita de $r = Af_1 + Bf_2$, i si no digueu el perquè.
c) Calculeu el residu de la divisió de r per (f_1, f_2). Perquè podríem haver previst el resultat abans de fer la divisió?

d) Trobeu un altre polinomi $g \in \langle f_1, f_2\rangle$ tal que el residu de la divisió de g per (f_1, f_2) sigui diferent de zero. Pista: $(xy+1)\cdot f_2 = x^2y^2-1$, mentre que $y \cdot f_1 = x^2y^2 - yz$.
e) Dieu si l'algorisme de la divisió dona per si sol una solució pel problema de la pertinença a un ideal. Considereu l'ideal $\langle f_1, f_2\rangle$.

EXERCICI 2.7. Utilitzant l'ordre grlex, trobeu un element g de

$$\langle f_1, f_2\rangle = \left\langle 2xy^2 - x, 3x^2y - y - 1\right\rangle \subset \mathbb{R}[x, y]$$

tal que el residu de dividir-l'ho per (f_1, f_2) sigui diferent de zero.

Secció 5.

EXERCICI 2.8. (*) En aquest problema estudiarem un cas especial d'*ordre amb pes*. Sigui $\mathbf{u} = (u_1, \ldots, u_n)$ un vector de $\mathbb{R}^n$ tal que $u_1, \ldots, u_n$ són positius i linealment independents sobre $\mathbb{Q}$. Direm que $\mathbf{u}$ és un *vector de pes independent*. Per tot $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, definim

$$\alpha \succ_{\mathbf{u}} \beta \Longleftrightarrow \mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta$$

on el punt representa el producte escalar de vectors. Anomenarem $\succ_{\mathbf{u}}$ *ordre amb pes* determinat per $\mathbf{u}$.

a) Demostreu que $\succ_{\mathbf{u}}$ és un ordre monomial. Pista : En quin punt de la demostració, utilitzeu la independència lineal de $u_1, \ldots, u_n$?
b) Demostreu que $\mathbf{u} = (1, \sqrt{2})$ és un vector de pes independent i que $\succ_{\mathbf{u}}$ és un ordre amb pes a $\mathbb{Z}^2_{\geq 0}$.
c) Demostreu que $\mathbf{u} = (1, \sqrt{2}, \sqrt{3})$ és un vector de pes independent i que $\succ_{\mathbf{u}}$ és un ordre amb pes a $\mathbb{Z}^3_{\geq 0}$.

EXERCICI 2.9. (*) Un altre ordre amb pes que té interés es construeix de la següent manera. Sigui $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n_{\geq 0}$, i $\succ_\sigma$ un ordre monomial (com per exemple $\succ_{\text{lex}}$ o $\succ_{\text{grlex}}$) de $\mathbb{Z}^n_{\geq 0}$. Per tot $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, definim $\alpha \succ_{\mathbf{u},\sigma} \beta$ si i només si

$$\mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta \text{ o bé } \mathbf{u} \cdot \alpha = \mathbf{u} \cdot \beta \text{ i } \alpha \succ_\sigma \beta$$

Anomenem $\succ_{\mathbf{u},\sigma}$ l'ordre amb pes determinat per $\mathbf{u}$ i $\succ_\sigma$.

a) Demostreu que $\succ_{\mathbf{u},\sigma}$ és un ordre monomial.
b) Trobeu un $\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$ tal que l'ordre $\succ_{\mathbf{u},\sigma}$ sigui exactament l'ordre $\succ_{\text{grevlex}}$.
c) Un exemple útil de pes amb ordre és l'*ordre d'eliminació* introduït per BAYER i STILLMAN (1987). Fixem un enter $1 \leq j \leq n$ i sigui $\mathbf{u} = (1, \ldots, 1, 0, \ldots, 0)$ amb j uns i $n - j$ zeros. S'anomena *j-èsim ordre d'eliminació* $\succ_j$ a l'ordre amb pes $\succ_{\mathbf{u},\text{grevlex}}$. Proveu que $\succ_j$ té la propietat següent: Si x^α és un monomi qualsevol en el que apareix alguna de les variables $x_1, \ldots, x_j$, llavors $x^\alpha \succ x^\beta$ per tot monomi que únicament conté les variables $x_{j+1}, \ldots, x_n$. Els ordres d'eliminació juguen un paper important en la teoria de l'eliminació.

Nota: Correspon a l'ordre lexdeg($[x_1, \ldots, x_j], [x_{j+1}, \ldots, x_n]$) en *Maple*.

EXERCICI 2.10. Separem les variables $\overline{x}$ en un grup $\overline{y}$ amb j variables i un grup $\overline{z}$ amb $n-j$ variables. Posem $\overline{x}=\overline{y},\overline{z}$, i siguin $\succ_{\overline{y}}$ i $\succ_{\overline{z}}$ ordres monomials respecte a les variables $\overline{y}$ i $\overline{z}$ respectivament. Anomenem ordre producte $\succ_{\overline{y},\overline{z}}$ al que compleix el següent:

Donats $\alpha=(\alpha_1,\ldots,\ldots\alpha_n),\ \beta=(\beta_1,\ldots,\beta_n)\in\mathbb{Z}^n_{\geq 0}$, direm que $\alpha\succ_{\overline{yz}}\beta$

$$\begin{array}{ll}\text{si} & (\alpha_1,\ldots,\alpha_j)\succ_{\overline{y}}(\beta_1,\ldots,\beta_j),\\ \text{o be} & (\alpha_1,\ldots,\alpha_j)=(\beta_1,\ldots,\beta_j)\\ & \text{i}\ \ (\alpha_{j+1},\ldots,\alpha_n)\succ_{\overline{z}}(\beta_{j+1},\ldots,\beta_n).\end{array}$$

Proveu que és un ordre monomial i que tot monomi que contingui alguna de les variables $\overline{y}$ és més gran que qualsevol monomi que només contingui les variables $\overline{z}$.

EXERCICI 2.11. (*) Demostreu que si $\overline{a}=(a_1,\ldots,a_n)\in K^n$, llavors

$$\mathbb{I}(\{\overline{a}\})=\langle x_1-a_1,\ldots,x_n-a_n\rangle$$

EXERCICI 2.12. (*) Determineu la clausura de Zariski a $\mathbb{R}^2$ i a $\mathbb{C}^2$ dels conjunts següents:

a) $S_1=\{(x,y)\in\mathbb{R}^2\ :\ y=x^2,\ x>0\}$.
b) $S_2=\{(t^2,t^3)\in\mathbb{R}^2\ :\ t\in T\}$ on $T\subset\mathbb{R}$ és un subconjunt infinit.

EXERCICI 2.13. (*) Descomponeu $\mathbb{V}(z^3-x^5,y^3-x^2)$ en varietats irreductibles a $\mathbb{C}^3$ i a $\mathbb{R}^3$.

Nota: Empreu parametritzacions adients, el teorema de la parametrització, i estudieu la seva bijectivitat o no.

EXERCICI 2.14. (*) Descomponeu $V=\mathbb{V}(y^m-x^n)$ en varietats irreductibles a $\mathbb{C}^2$ i a $\mathbb{R}^2$ emprant parametritzacions adients. Suposeu que $(n,m)=d$.

Nota: Empreu parametritzacions adients, el teorema de la parametrització, i estudieu la bijectivitat o no de les parametritzacions que feu servir.

EXERCICI 2.15. Descomponeu $V=\mathbb{V}(x^m-y^n,x^n-z^m)$ en varietats irreductibles a $\mathbb{C}^3$ i a $\mathbb{R}^3$ emprant parametritzacions adients. Suposeu que $(n,m)=d$.

Nota: Empreu parametritzacions adients, el teorema de la parametrització, i estudieu la bijectivitat o no de les parametritzacions que feu servir.

Secció 7.

EXERCICI 2.16. (*) Proveu la proposició 7.4:

Donades dues bases minimals G i G' del mateix ideal $\mathcal{I}\subset K[\overline{x}]$, aquestes tenen el mateix nombre de polinomis i estan en correspondència bijectiva. Els associats en la correspondència tenen el mateix monomi principal.

EXERCICI 2.17. (*) Proveu que si $B=\{g_1,\ldots,g_s\}$ és una base d'un ideal $\mathcal{I}\subset K[\overline{x}]$ i té la propietat de que, donat un ordre monomial, per tot $f\in\mathcal{I}$ és $\overline{f}^B=0$, llavors B és base de Gröbner de $\mathcal{I}$.

Secció 10.

EXERCICI 2.18. (*) Sigui

$$G = [x^3y\,z - y^2\,z, x\,y^2\,z - x + x\,y, x\,y\,z^2 - x\,z - y, x\,y^2\,z^2 + z^2]$$

i considerem ordre grevlex(x, y, z).

a) Construïu una base de les syzygies S_{ij} sobre els monomis principals de G corresponents als S-polinomis.
b) Trobeu una base mínima d'entre aquestes syzygies.
c) Comproveu que

$$S = [-xy^3z - y, x^3y^2z + x^2, -x^3y^3 + y, x^3y^2 - 1]$$

és una syzygia (no homogènia) sobre els monomis principals de G, i descomponeu-la en suma de syzygies homogènies.
d) Expresseu S en termes de la base mínima obtinguda a l'apartat anterior.

EXERCICI 2.19. (*)
Proveu que en un ideal lineal $\mathcal{I}$

a) per eliminació Gaussiana obtenim una base de Gröbner minimal per qualsevol ordre monomial tal que $x_1 \succ x_2 \succ \cdots \succ x_n$.
b) Com s'obté la base reduïda?
c) Proveu que és ideal de varietat.

EXERCICI 2.20. (*) Demostreu que $\{y - x^2, z - x^3\}$

a) és una base de Gröbner per ordre lex(z, y, x);
b) no és una base de Gröbner per ordre lex(x, y, z). Trobeu-la.

CAPíTOL 3

Teoria de l'Eliminació

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:

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

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, 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:

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

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

- Pas d'eliminació: g_4 només depèn 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 ambdós 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 proporcionen.

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 $1 = r_0 \leq r_1 \leq \cdots \leq r_n \leq s$. 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 d'una varietat zero-dimensional $V = \{P_1, \ldots, P_s\}$ 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 $P_i = (a_{i1}, \ldots, a_{in})$, 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 $G = \{g_1, \ldots, g_n\}$, on*

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

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

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

DEMOSTRACIÓ. En primer lloc tots els g_i's s'anul·len a tots els punts de V, i per tant pertanyen a $\mathbb{I}(V)$. A més $G = \{g_1, \ldots, g_n\}$ és la base de Gröbner reduïda d'un ideal $I \supseteq \mathbb{I}(V)$, ja que tots els S-polinomis redueixen a zero per la proposició 10.4 i a més estan reduïts. Només cal provar que tot $f \in \mathbb{I}(V)$ redueix a zero al dividir-lo per G. Fent la divisió tindrem

$$f = q_n(\overline{x})p_n(x_n) + \sum_{i=1}^{n-1} q_i(\overline{x})(x_i - p_i(x_n)) + r(x_n)$$

on el residu no pot contenir cap de les variables $x_1, \ldots, x_{n-1}$ ja que aquestes figuren com a monomis principals dels divisors. A més $r(x_n)$ ha de tenir grau menor que s, ja que p_n te grau s i és el polinomi de I_{n-1} de grau mínim. Com s'anul·la per s valors de x_n, ha de ser idènticament 0. Per tant resulta $f \in \langle G \rangle$ i per tant $G = \mathrm{gb}(\mathbb{I}(V), \mathrm{lex}(\overline{x}))$. □

El teorema de l'eliminació ens proporciona algorismes per determinar la intersecció d'ideals, el quocient d'ideals i la pertinença a l'ideal radical. En les seccions següents descrivim aquests algorismes.

2. Intersecció d'ideals

Una de les operacions entre ideals importants és la intersecció. Ja vam observar que donats els generadors de $\mathcal{I}$ i de $\mathcal{J}$ és immediat trobar generadors de $\mathcal{I} \cdot \mathcal{J}$, però no de $\mathcal{I} \cap \mathcal{J}$. Si sabem determinar els generadors de la

intersecció, podrem, per exemple, calcular el mínim comú múltiple (lcm) d'un conjunt de polinomis, o l'ideal de varietat d'una unió de varietats de les quals coneixem els seus ideals de varietat, o el quocient d'ideals, entre d'altres aplicacions. Anem a veure com determinar-la.

LEMA 2.1. *Sigui* $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subset K[\overline{x}]$ *un ideal. Definim*

$$g(t) \cdot \mathcal{I} = \langle g(t)h(\overline{x}) : h(\overline{x}) \in \mathcal{I} \rangle$$

Llavors

(i) $g(t) \cdot \mathcal{I}$ *és un ideal de* $K[\overline{x}, t]$, *i*

$$g(t) \cdot \mathcal{I} = \langle g(t)f_1, \ldots, g(t)f_s \rangle .$$

(ii) *Si* $h(\overline{x}, t) \in g(t) \cdot \mathcal{I}$ *i* $t_0 \in K$ *és qualsevol, llavors* $h(\overline{x}, t_0) \in \mathcal{I}$.

DEMOSTRACIÓ. .

(i) Sigui $h(\overline{x}, t)$ un polinomi qualsevol de $g(t) \cdot \mathcal{I}$. Podrà expressar-se en la forma

$$h(\overline{x}, t) = \sum_i q_i(\overline{x}, t)g(t)p_i(\overline{x})$$

on $q_i(\overline{x}, t)$ són arbitraris i $p_i(\overline{x}) \in \mathcal{I}$. Expressant cada $p_i(\overline{x})$ en termes dels generadors de $\mathcal{I}$ tindrem

$$h(\overline{x}, t) = \sum_{i,j} q_i(\overline{x}, t)g(t)u_{ij}(\overline{x})f_j(\overline{x}) = \sum_j v_j(\overline{x}, t)g(t)f_j(\overline{x})$$

per tant $h(\overline{x}, t)$ pertany a l'ideal $\langle g(t)f_1(\overline{x}), \ldots, g(t)f_s(\overline{x}) \rangle$. En sentit contrari, òbviament, tot element d'aquest ideal pertany a $g(t) \cdot \mathcal{I}$, quedant així provat tot l'apartat (i).

(ii) És conseqüència immediata de l'expressió de $h(\overline{x}, t)$ anterior substituint t per t_0.

□

TEOREMA 2.2 (Intersecció d'ideals). *Siguin* $\mathcal{I}$ *i* $\mathcal{J}$ *ideals de* $K[\overline{x}]$. *Llavors*

$$\mathcal{I} \cap \mathcal{J} = (t \cdot \mathcal{I} + (1 - t) \cdot \mathcal{J}) \cap K[\overline{x}]$$

DEMOSTRACIÓ. Pel lema anterior, $t \cdot \mathcal{I} + (1-t) \cdot \mathcal{J}$ és un ideal de $K[\overline{x}, t]$.

$\subseteq$: Sigui $f(\overline{x}) \in \mathcal{I} \cap \mathcal{J}$. Llavors $tf \in t \cdot \mathcal{I}$, i $(1 - t)f \in (1 - t) \cdot \mathcal{J}$. Per tant,

$$f(\overline{x}) = tf + (1 - t)f \in t \cdot \mathcal{I} + (1 - t) \cdot \mathcal{J}.$$

Tenint en compte que $\mathcal{I} \cap \mathcal{J} \subset K[\overline{x}]$ resulta que

$$f \in (t \cdot \mathcal{I} + (1 - t) \cdot \mathcal{J}) \cap K[\overline{x}].$$

$\supseteq$: Sigui ara $f(\overline{x}) \in (t \cdot \mathcal{I} + (1-t) \cdot \mathcal{J}) \cap K[\overline{x}]$. Llavors $f(\overline{x}) = g(\overline{x}, t) + h(\overline{x}, t)$ on $g(\overline{x}, t) \in t \cdot \mathcal{I}$ i $h(\overline{x}, t) \in (1-t) \cdot \mathcal{J}$. Posem $t = 0$. Tindrem $g(\overline{x}, 0) = 0$ i $f(\overline{x}) = h(\overline{x}, 0)$, i per tant, pel lema 2.1 és $f(\overline{x}) \in \mathcal{J}$. Anàlogament posant $t = 1$ resulta $f(\overline{x}) \in \mathcal{I}$. Per tant $f \in \mathcal{I} \cap \mathcal{J}$.

□

El teorema anterior ens dona un algorisme per determinar la intersecció de dos (o més) ideals qualsevulla.

Algorisme per determinar la intersecció d'ideals. Siguin

$$\mathcal{I} = \langle f_1, \ldots, f_s \rangle, \quad \mathcal{J} = \langle g_1, \ldots, g_r \rangle$$

dos ideals de $K[\overline{x}]$. Llavors, per determinar $\mathcal{I} \cap \mathcal{J}$ considerem l'ideal de $K[\overline{x}, t]$ següent:

$$\mathcal{K} = \langle tf_1, \ldots, tf_s, (1-t)g_1, \ldots, (1-t)g_r \rangle$$

i procedim a eliminar la variable t determinant la base de Gröbner G de $\mathcal{K}$ respecte un ordre d'eliminació de la t (per exemple $\mathrm{lex}(t, \overline{x})$. Llavors $G \cap K[\overline{x}]$ és base de Gröbner de $\mathcal{I} \cap \mathcal{J}$.

EXEMPLE 2.3. Siguin $\mathcal{I} = \langle xy^3, x+y \rangle$ i $\mathcal{J} = \langle x^2y, x^2-y^2 \rangle$. Tenim

$$\begin{array}{rcl} G & = & \mathrm{gb}([txy^3, t(x+y), (1-t)x^2y, (1-t)(x^2-y^2)], \mathrm{lex}(t,x,y)) \\ & = & \{y^4, xy^3, x^2-y^2, -y^3+ty^3, tx+ty\} \end{array}$$

i per tant $\mathcal{I} \cap \mathcal{J} = G \cap K[x,y] = \langle y^4, xy^3, x^2-y^2 \rangle$.

Podem comprovar, dividint cada polinomi de l'ideal intersecció trobat per les bases de Gröbner de $\mathcal{I}$ i de $\mathcal{J}$, que pertanyen a ambdós ideals.

Abans de posar més exemples, considerem dos aplicacions importants de la intersecció d'ideals: la determinació del lcm de dos polinomis i del seu gcd, i de l'ideal de varietat de la unió de varietats de les quals coneixem els seus ideals de varietat.

PROPOSICIÓ 2.4. .

(i) *La intersecció $\mathcal{I} \cap \mathcal{J}$ de dos ideals principals de $K[\overline{x}]$ és principal.*
(ii) *Si $\mathcal{I} = \langle f \rangle$ i $\mathcal{J} = \langle g \rangle$ i $\mathcal{I} \cap \mathcal{J} = \langle h \rangle$, llavors*

$$h = \mathrm{lcm}(f, g)$$

DEMOSTRACIÓ. N'hi ha prou en provar (ii) directament. $\mathcal{I}$ consisteix en tots els polinomis múltiples de f, i $\mathcal{J}$ en els múltiples de g. Per tant $\mathcal{I} \cap \mathcal{J}$ contindrà els múltiples comuns de f i g. Emprant la descomposició en factors única a $K[\overline{x}]$ és obvi que l'ideal intersecció estarà generat pel polinomi $\mathrm{lcm}(f, g)$. □

Ara ja podem determinar el $\mathrm{lcm}(f, g)$ i el $\gcd(f, g)$.

EXEMPLE 2.5. Siguin

$$\begin{aligned} f &= x^3 - x^2y + x^2z + 2zx^2y - 2zxy^2 + 2z^2xy + z^2y^2x - y^3z^2 + z^3y^2 \\ g &= x^3 - 2x^2y + 2x^2z + xy^2 - 2zxy + xz^2 + zx^2y - 2zxy^2 + 2z^2xy \\ &\quad + y^3z - 2z^2y^2 + yz^3 \end{aligned}$$

Determinem $\operatorname{lcm}(f,g)$ i $\gcd(f,g)$. Calculant $\operatorname{gb}([tf,(1-t)g],\operatorname{lex}(t,x,y))$ resulta:

$$\begin{aligned} G \cap K[x,y] &= [2xz^3y^2 - 4x^2y^2z + x^2z^2y^2 - 2y^3z^3 - 2xy^3z^2 + 2yzx^3 \\ &\quad + 2yz^3x + 4yz^2x^2 + 2y^3zx - 4z^2y^2x - 2zx^2y + z^4y^2 \\ &\quad + y^4z^2 + 2x^3z + x^2z^2 - 2x^3y + x^2y^2 + x^4] \end{aligned}$$

que ens dona el $\operatorname{lcm}(f,g)$. Ara per determinar el $\gcd(f,g)$ tenim en compte que

$$\gcd(f,g) = \frac{fg}{\operatorname{lcm}(f,g)}.$$

Per tant, multiplicant f i g i dividint el resultat pel $\operatorname{lcm}(f,g)$, respecte a qualsevol de les variables, el resultat ha de ser un quocient enter i un residu 0. En l'exemple obtenim:

$$\gcd(f,g) = x^2 + (-y + yz + z)x - y^2z + yz^2.$$

PROPOSICIÓ 2.6. *La intersecció de m ideals $\mathcal{I}_1,\ldots,\mathcal{I}_n$ de $K[\overline{x}]$ es pot determinar per*

$$\bigcap_{i=1}^{m} \mathcal{I}_i = \left(\sum_{i=1}^{m} t_i \cdot \mathcal{I}_i + (1 - \sum_{i=1}^{m} t_i) \cdot 1\right) K[\overline{x}]$$

Es tracta d'una generalització immediata del teorema 2.2.

EXEMPLE 2.7. Determinem l'*ideal de varietat* de la varietat formada pels tres punts $V = \{(0,0),(1,0),(1,1)\}$.

Recordant que

$$\mathbb{I}(\bigcup_{i=1}^{m} V_i) = \bigcap_{i=1}^{m} \mathbb{I}(V_i)$$

els ideals de cada un dels punts de V són

$$\mathcal{I}_1 = \langle x, y\rangle, \quad \mathcal{I}_2 = \langle x-1, y\rangle, \quad \mathcal{I}_3 = \langle x-1, y-1\rangle.$$

Per tant hem de determinar l'ideal de $K[t_1,t_2,x,y]$ següent:

$$\mathcal{I} = \langle t_1x, t_1y, t_2(x-1), t_2y, (1-t_1-t_2)(x-1), (1-t_1-t_2)(y-1)\rangle \cap K[\overline{x}]$$

Resulta:

$$\operatorname{gb}(\mathcal{I}, \operatorname{lex}(t_1,t_2,x,y)) = \{y^2 - y, yx - y, x^2 - x, -x + y + t_2, t_1 + x - 1\}$$

i finalment

$$\mathbb{I}(V) = \left\langle y^2 - y, yx - y, x^2 - x\right\rangle$$

3. Quocient d'ideals

Considerarem ara noves proposicions relatives al quocient i a la intersecció que no vam considerar en el capítol 1 i que ens serviran ara per obtenir un algorisme pel càlcul del quocient d'ideals.

PROPOSICIÓ 3.1. *Siguin $\mathcal{I}, \mathcal{I}_i, \mathcal{J}, \mathcal{J}_i$ ideals de $K\overline{x}]$ per $1 \leq i \leq r$. Llavors*

(i)
$$\left(\bigcap_{i=1}^{r} \mathcal{I}_i\right) : \mathcal{J} = \bigcap_{i=1}^{r} (\mathcal{I}_i : \mathcal{J})$$

(ii)
$$\mathcal{I} : \left(\sum_{i=1}^{r} \mathcal{J}_i\right) = \bigcap_{i=1}^{r} (\mathcal{I} : \mathcal{J}_i)$$

(iii)
$$\mathcal{I} : \langle f_1, \ldots, f_r \rangle = \bigcap_{i=1}^{r} (I : \langle f_i \rangle).$$

DEMOSTRACIÓ. Tenim les implicacions següents:

(i)
$$\begin{aligned} f \in \left(\bigcap_{i=1}^{r} \mathcal{I}_i\right) : \mathcal{J} &\iff \forall g \in \mathcal{J} \text{ és } fg \in \bigcap_{i=1}^{r} \mathcal{I}_i \\ &\iff \forall g \in \mathcal{J} \text{ i } 1 \leq i \leq r \text{ és } fg \in \mathcal{I}_i \\ &\iff \text{per } 1 \leq i \leq r \text{ és } f \in (\mathcal{I}_i : \mathcal{J}) \\ &\iff f \in \bigcap_{i=1}^{r} (\mathcal{I}_i : \mathcal{J}) \end{aligned}$$

(ii)
$$\begin{aligned} \mathcal{I} : \left(\sum_{i=1}^{r} \mathcal{J}_i\right) &\iff \forall g \in \sum_{i=1}^{r} \mathcal{J}_i \text{ és } fg \in \mathcal{I} \\ &\iff \text{per } 1 \leq i \leq r \text{ i } \forall g_i \in \mathcal{J}_i \text{ és } fg_i \in \mathcal{I} \\ &\iff \text{per } 1 \leq i \leq r \text{ és } f \in \mathcal{I} : \mathcal{J}_i \\ &\iff f \in \bigcap_{i=1}^{r} (\mathcal{I} : \mathcal{J}_i) \end{aligned}$$

(iii) És una conseqüència immediata de (ii).

□

TEOREMA 3.2. *Sigui $\mathcal{I}$ un ideal i g un polinomi de $K[\overline{x}]$. Si $\{h_1, \ldots, h_s\}$ és una base de l'ideal $\mathcal{I} \cap \langle g \rangle$, llavors $\{h_1/g, \ldots, h_s/g\}$ és una base de $\mathcal{I} : \langle g \rangle$.*

DEMOSTRACIÓ. .

$\subseteq$: Sigui $f \in \mathcal{I} : \langle g \rangle$. Llavors $fg \in \mathcal{I}$. Com a més a més $fg \in \langle g \rangle$, llavors $fg \in \mathcal{I} \cap \langle g \rangle$. Si $\mathcal{I} \cap \langle g \rangle = \langle h_1, \ldots, h_s \rangle$ tindrem $fg = \sum_i A_i h_i$ per certs polinomis A_i. Tenint en compte que cada $h_i \in \langle g \rangle$, cada h_i/g és un polinomi, i resulta que $f = \sum_i A_i(h_i/g)$, i en conseqüència $f \in \langle h_1/g, \ldots, h_s/g \rangle$.

$\supseteq$: Sigui $f \in \langle h_1/g, \ldots, h_s/g \rangle$ i $u \in \langle g \rangle$. Per la primera tindrem $f = \sum_i A_i(h_i/g)$, i per la segona $u = wg$. Per tant tindrem

$$uf = wgf = \sum_i wA_i h_i \in \mathcal{I} \cap \langle g \rangle \in \mathcal{I}$$

Per tant $f \in \mathcal{I} : \langle g \rangle$.

□

Amb aquest teorema i la proposició 3.1, junt amb l'algorisme per determinar interseccions, tenim les eines per donar un algorisme per determinar quocients d'ideals:

Algorisme per determinar el quocient de dos ideals

Input: $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$
$\mathcal{J} = \langle g_1, \ldots, g_r \rangle$
Output: $B =$ base de $\mathcal{I} : \mathcal{J}$

PER $1 \leq i \leq r$ FER
$G_i = \langle f_1, \ldots, f_s \rangle \cap \langle g_i \rangle$ (algorisme intersecció)
$H_i = G_i/g_i$ (dividim cada element de G_i per g_i)
$B = \bigcap_{i=1}^{r} H_i$ (algorisme intersecció)

Exemple 3.3. Donats

$$\mathcal{I} = \left\langle x^2 + xy, x^3 + x^2 \right\rangle, \quad \mathcal{J} = \left\langle x^2, xy, y^2 \right\rangle$$

Determinem les interseccions $\mathcal{I} \cap \mathcal{J}_i$ per $1 \leq i \leq 3$ i els $\mathcal{I} : \mathcal{J}_i$, dividint cada polinomi per $\mathcal{J}_i$:

$$\begin{array}{ll} \mathcal{I} \cap \left\langle x^2 \right\rangle = \left\langle x^2 y - x^2, x^3 + x^2 \right\rangle, & \mathcal{I} : \left\langle x^2 \right\rangle = \langle y - 1, x + 1 \rangle \\ \mathcal{I} \cap \langle xy \rangle = \left\langle xy^2 - xy, x^2 y + xy \right\rangle, & \mathcal{I} : \langle xy \rangle = \langle y - 1, x + 1 \rangle \\ \mathcal{I} \cap \left\langle y^2 \right\rangle = \left\langle xy^3 - xy^2, x^2 y^2 + xy^2 \right\rangle, & \mathcal{I} : \left\langle y^2 \right\rangle = \left\langle xy - x, x^2 + x \right\rangle \end{array}$$

Finalment determinem el quocient de $\mathcal{I} : \mathcal{J}$ fent la intersecció $\bigcap_{i=1}^{3} \mathcal{I} : \mathcal{J}_i$.

$$\mathcal{I} : \mathcal{J} = (\mathcal{I} : \left\langle x^2 \right\rangle) \cap (\mathcal{I} \cap \langle xy \rangle) \cap (\mathcal{I} \cap \left\langle y^2 \right\rangle) = \left\langle xy - x, x^2 + x \right\rangle$$

4. Pertinença a l'ideal radical

PROPOSICIÓ 4.1 (Pertinença a l'ideal radical). *Sigui K un cos arbitrari i $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ un ideal de $K[\overline{x}]$. Llavors $f \in K[\overline{x}]$ pertany a $\sqrt{\mathcal{I}}$ ssi el polinomi constant 1 pertany a l'ideal $\tilde{\mathcal{I}} \subseteq K[\overline{x}, y]$ donat per*

$$\tilde{\mathcal{I}} = \langle f_1, \ldots, f_s, 1 - y\, f \rangle$$

DEMOSTRACIÓ. .

$\Rightarrow$: Si $f \in \sqrt{\mathcal{I}}$, existeix m tal que $f^m \in \mathcal{I}$ i per tant també $f^m \in \tilde{\mathcal{I}}$. A més, també $1 - yf \in \tilde{\mathcal{I}}$. Tindrem

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + \cdots + y^{m-1} f^{m-1})$$

i per tant el polinomi 1 pertany a $\tilde{\mathcal{I}}$.

$\Leftarrow$: Si el polinomi constant 1 pertany a $\tilde{\mathcal{I}}$ tindrem

$$1 = \sum_i p_i(\overline{x}, y) f_i + q(\overline{x}, y)(1 - yf)$$

Posant $y = 1/f(\overline{x})$ resulta

$$1 = \sum_i p_i(\overline{x}, 1/f) f_i$$

Multiplicant per una potència convenient de f a fi d'eliminar denominadors polinòmics en l'expressió anterior, resultarà

$$f^m = \sum_i A_i(\overline{x}) f_i$$

i per tant $f \in \sqrt{\mathcal{I}}$.

□

Algorisme per determinar la pertinença a l'ideal radical. La proposició anterior complementada amb la teoria de les bases de Gröbner ens proporciona el següent algorisme per determinar si donat un polinomi f i un ideal $\mathcal{I}$, el primer pertany o no al radical de $\mathcal{I}$.

Input: $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subset K[\overline{x}]$
$f \in K[\overline{x}]$
Output: *pertany* = cert si $f \in \sqrt{\mathcal{I}}$ i false en cas contrari

$G = \mathrm{gb}([f_1, \ldots, f_s, 1 - yf], \succ_{y,\overline{x}})$
SI $G = \{1\}$ LLAVORS cert ALTRAMENT fals

EXEMPLE 4.2. Sigui l'ideal $\mathcal{I} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$. Volem esbrinar si el polinomi $f = y - x^2 + 1$ pertany o no a $\sqrt{\mathcal{I}}$. L'algorisme consisteix a considerar l'ideal

$$\tilde{\mathcal{I}} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1) \rangle \subset K[x, y, z]$$

i determinar una base de Gröbner reduïda per saber si $\mathcal{I} = \langle 1 \rangle$ o no. Calculant-la obtenim

$$\mathrm{gb}(\tilde{\mathcal{I}}, \mathrm{grevlex}(x, y, z)) = \{1\}$$

i en conseqüència deduïm que $f \in \sqrt{\mathcal{I}}$.

Un camí alternatiu seria anar calculant potències de f dividides per la base de Gröbner G de $\mathcal{I}$ per veure si hi ha alguna potència que pertany a $\mathcal{I}$. El problema és que no sabem quan hem d'aturar-nos. Així, en l'exemple, tenim:

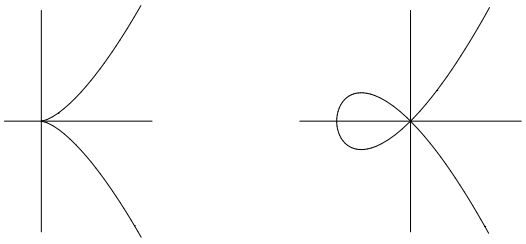
$$\begin{aligned} \overline{f}^G &= y - x^2 + 1 \\ \overline{f^2}^G &= -2x^2y + 2y \\ \overline{f^3}^G &= 0 \end{aligned}$$

5. Aplicacions: Punts singulars de corbes

La geometria proporciona interessants conjunts d'equacions que poden ésser abordades amb les tècniques descrites. Entre aquestes figuren la determinació dels punts singulars de les corbes i l'estudi de les tangents en ells.

Sigui una corba del pla K^2 d'equació $f(x, y) = 0$, on $f \in K[x, y]$. És d'esperar que la corba tingui una recta tangent ben definida en la major part de punts, si be pot no ser cert en aquells punts en que la corba es talla a sí mateixa o en punts de retrocès.

Exemples:



$y^2 - x^3 = 0$ $\qquad$ $y^2 - (x+1)\,x^2 = 0$

Intuïtivament, un punt singular de $\mathbb{V}(f)$ és un punt com els dels gràfics, on la tangent té problemes. Per precisar la noció donarem una definició algebraica.

Donat un punt $(x_0, y_0) \in \mathbb{V}(f)$, una recta que passa per ell té una equació paramètrica de la forma:

$$\begin{cases} x = x_0 + at \\ y = y_0 + bt \end{cases} \tag{5.1}$$

La recta passa per (x_0, y_0) per $t = 0$, i $(a, b) \neq (0, 0)$ és un vector director de la recta. Variant (a, b) obtenim un feix de rectes que passen per (x_0, y_0). Posem

$$g(t) = f(x_0 + at, y_0 + bt),$$

Per $t = 0$ tindrem $g(0) = 0$, ja que (x_0, y_0) és de la corba. Les arrels de $g(t)$ determinen els punts on la recta (5.1) talla a la corba.

DEFINICIÓ 5.1. Direm que la recta (5.1) talla a la corba $f(x, y) = 0$ en el punt (x_0, y_0) amb *multiplicitat* k (on k és un enter positiu) si

$$g(t) = f(x_0 + at, y_0 + bt) = t^k\, h(t)$$

i $h(0) \neq 0$, és a dir, si g té l'arrel 0 amb multiplicitat k.

EXEMPLE 5.2. Considerem la cúbica

$$f(x, y) = y^2 - (x + 1)\, x^2$$

i el punt de la corba $(0, 0)$. Considerem

$$g(t) = f(0 + at, 0 + bt) = b^2t^2 - (at + 1)a^2t^2 = (b^2 - a^2)t^2 - a^3t^3$$

La màxima multiplicitat de contacte l'obtindrem quan $b^2 - a^2 = 0$. Això dóna dues solucions $a = b = 1$ i $a = -b = 1$, que corresponen a les dues tangents $(x = t, y = t)$ i $(x = t, y = -t)$ en el punt singular $(0, 0)$. En aquest cas, la *multiplicitat de l'arrel* és 3, i seria únicament 2 per les altres rectes. Es tracta d'un punt singular.

Sigui M el grau de f. Desenvolupant per Taylor tindrem

$$\begin{aligned} g(t) &= \sum_{n=0}^{M} \frac{g^{(n)}(0)}{n!} t^n = \left(\frac{\partial f}{\partial x} a + \frac{\partial f}{\partial y} b \right)_{(x_0,y_0)} t \\ &\quad + \sum_{n=2}^{M} \frac{t^n}{n!} \sum_{i=0}^{n} \binom{n}{i} \frac{\partial^n f}{\partial^i x \partial^{n-i} y}_{(x_0,y_0)} a^i b^{n-i} \end{aligned} \tag{5.2}$$

PROPOSICIÓ 5.3. *Donada la corba $f(x, y) = 0$ i un punt de la corba $P(x_0, y_0)$,*

(i) *Si $(\nabla f)_{(x_0,y_0)} = \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \right)_{(x_0,y_0)} \neq (0, 0)$, llavors existeix una direcció única (a, b), perpendicular al vector gradient, per la qual la recta (5.1) talla f amb multiplicitat més gran o igual a 2. L'anomenem recta tangent, i el punt és un punt ordinari de f.*

(ii) *Si $(\nabla f)_{(x_0,y_0)} = \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \right)_{(x_0,y_0)} = (0, 0)$, llavors totes les rectes que passen per (x_0, y_0) tallen a f amb multiplicitat més gran o igual a 2. Direm que és un punt singular. Anul·lant el primer coeficient del desenvolupament de $g(t)$ no idènticament nul, obtenim les rectes que tallen f amb multiplicitat màxima en el punt (x_0, y_0) i representen les rectes tangents en el punt singular. Ens donen informació sobre l'estructura del punt singular.*

DEMOSTRACIÓ. La proposició és conseqüència immediata de (5.2). □

Òbviament, la solució del sistema d'equacions que determina els punts singulars, així com els coeficients de les rectes tangents en els punts singulars, poden ser resolts emprant les tècniques apreses de les bases de Gröbner.

EXEMPLE 5.4. Ara trobarem els punts singulars i les tangents a una corba emprant *Maple*.

```
> with(Groebner):
```

Carreguem la llibreria "geomplot"

```
> read(‘c:/maple/geomplot4/geomplot.m‘):
> with(geomplot):
```

Donada la corba

```
> f:=y^4-2*y^3+y^2-3*x^2*y+2*x^4;
```

$$f := y^4 - 2\,y^3 + y^2 - 3\,x^2\,y + 2\,x^4$$

El sistema per determinar els seus punts singulars és:

```
> F:=[diff(f,x),diff(f,y),f];
```

$$F := [-6\,x\,y + 8\,x^3,\ 4\,y^3 - 6\,y^2 + 2\,y - 3\,x^2,\ y^4 - 2\,y^3 + y^2 - 3\,x^2\,y + 2\,x^4]$$

Resolem el sistema emprant bases de Gröbner:

```
> G:=gbasis(F,plex(x,y));
```

$$G := [y^3 - y^2,\ x\,y,\ 3\,x^2 + 2\,y^2 - 2\,y]$$

```
> S:=gsolve(G,[x,y]);
```

$$S := \{[[x,\ y],\ \mathrm{plex}(y,\ x),\ \{\}],\ [[x,\ y - 1],\ \mathrm{plex}(y,\ x),\ \{\}]\}$$

Expressem $\mathrm{g}(t) = \mathrm{f}(x_0 + a\,t,\ y_0 + b\,t)$ en els dos punts singulars [0, 1] i [0, 0]

```
> g1:=collect(subs(x=a*t,y=1+b*t,f),t);
```

$$g1 := (b^4 + 2\,a^4)\,t^4 + (2\,b^3 - 3\,a^2\,b)\,t^3 + (b^2 - 3\,a^2)\,t^2$$

i imposem que el coeficient de t^2 sigui 0. Obtenim les dues rectes tangents en [0, 1] que són

```
> s1:=[solve(coeff(g1,t^2)=0,{b})];
```

$$s1 := [\{b = \sqrt{3}\,a\},\ \{b = -\sqrt{3}\,a\}]$$

```
> t1:=[t,1+subs(a=1,op(2,op(op(1,s1))))*t];
> t2:=[t,1+subs(a=1,op(2,op(op(2,s1))))*t];
```

$$t1 := [t,\ 1 + \sqrt{3}\,t]$$

$$t2 := [t,\ 1 - \sqrt{3}\,t]$$

Per les quals resulta una multiplicitat igual a 3. Resulta natural, ja que el punt singular correspon a dues branques que es tallen. La recta tangent a una de les branques té triple contacte amb la corba: d'una banda és tangent a una branca (multiplicitat 2), i del'altra talla a la segona branca (multiplicitat 1, total 3).

```
> expand(subs(x=t1[1],y=t1[2],f)); expand(subs(x=t2[1],y=t2[2],f));
```

$$3\,\sqrt{3}\,t^3 + 11\,t^4$$

$$-3\,\sqrt{3}\,t^3 + 11\,t^4$$

Procedint de forma anàloga pel punt [0, 0] obtenim:

```
> g2:=collect(subs(x=a*t,y=b*t,f),t);
```

$$g2 := (b^4 + 2\,a^4)\,t^4 + (-2\,b^3 - 3\,a^2\,b)\,t^3 + b^2\,t^2$$

```
> s1:=[solve(coeff(g2,t^2)=0,{b})];
```

$$s1 := [\{b = 0\}]$$

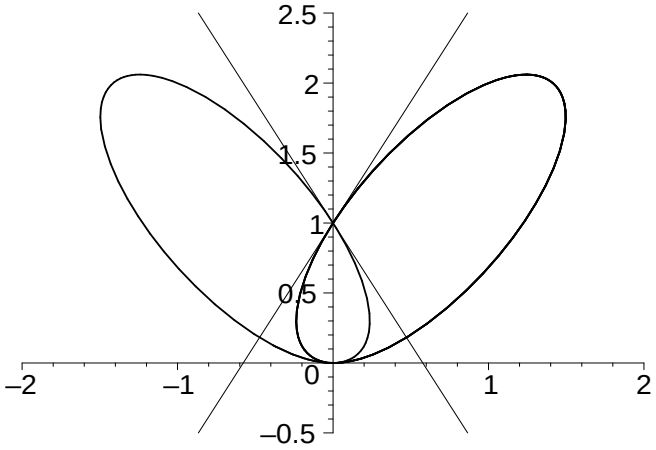
La multiplicitat de la tangència és 4, ja que també s'anul·la el coeficient de t^3.

```
> t3:=[t,subs(a=1,op(2,op(op(1,s1))))*t];
```

$$t3 := [t,\ 0]$$

```
> gmplot([y-1-sqrt(3)*x,y-1+sqrt(3)*x,size=1/20,f],x=-2..2,y=-.5..2.5);
```

LINE
LINE
IMPLICIT CURVE
$branchpoint = [-0.3842105301,\ 0.1256757296]$
$critpoint = [0.,\ 1.000000000]$



6. Aplicacions: Envolupant d'una família de corbes

Un altre sistema d'equacions interessant geomètricament és l'envolupant d'una família de corbes. Considerarem únicament famílies polinòmiques.

Definició 6.1. Una família polinòmica de corbes de $\mathbb{R}^2$ ve determinada per una funció $F(x, y, t) \in \mathbb{R}[x, y, t]$ que representa, per cada $t \in \mathbb{R}$ fixat, una varietat $\mathbb{V}(F_t)$, que són les corbes de la família.

DEFINICIÓ 6.2. Donada una família de corbes determinada per $F(x, y, t)$, la seva envolupant es defineix com el conjunt de punts $(x, y) \in \mathbb{R}^2$ que verifiquen el sistema d'equacions següent:

$$\begin{aligned} F(x, y, t) &= 0 \\ \frac{\partial F}{\partial t}(x, y, t) &= 0 \end{aligned}$$

Podem justificar la definició de forma heurística. La corba C, envolupant de la família $F(x, y, t)$, ha de cumplir que cada punt de C pertany a alguna corba de la família, i per tant verifica $F(x, y, t) = 0$, i que és tangent en aquest punt a la mateixa corba de la família. Per simplificar el raonament, suposem que l'envolupant C es pot parametritzar pel mateix paràmetre t que identifica la corba de la família a la qual és tangent per

$$\begin{cases} x = x(t) \\ y = y(t). \end{cases}$$

El punt $(x(t), y(t))$ està sobre C i sobre la varietat $\mathbb{V}(F_t)$, i ambdues són tangents. El vector tangent a C serà $(x'(t), y'(t))$, i el vector perpendicular al vector tangent a $\mathbb{V}(F_t)$ és $\nabla F = \left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}\right)$. Per tant s'ha de cumplir

$$\frac{\partial F}{\partial x} x'(t) + \frac{\partial F}{\partial y} y'(t) = 0$$

Per altra banda s'ha de cumplir idènticament

$$F(x(t), y(t), t) = 0$$

i per tant la derivada total de $F(x(t), t(t), t$ respecte a t ha de ser també nul·la. Per tant també

$$\frac{\partial F}{\partial x} x'(t) + \frac{\partial F}{\partial y} y'(t) + \frac{\partial F}{\partial t} = 0$$

Restant les dues s'obté

$$\frac{\partial F}{\partial t} = 0.$$

Igualment, les equacions que determinen l'envolupant d'una família de corbes poden ser resoltes amb les tècniques de resolució i eliminació que ens proporcionen les bases de Gröbner.

EXEMPLE 6.3. Utilitzem *Maple* per determinar l'envolupant d'una família de corbes.

```
> with(Groebner):
```

Carreguem la llibreria "geomplot"

```
> read(‘c:/maple/geomplot4/geomplot.m‘):
> with(geomplot):
```

Donada la família de cercles:

```
> Fu:=(x-u^3/2-2*u)^2+y^2-(u^2/2+1)^2*(1+u^2);
```

$$Fu := (x - \frac{1}{2}\,u^3 - 2\,u)^2 + y^2 - (\frac{u^2}{2} + 1)^2\,(1 + u^2)$$

Determinem el sistema d'equacions de l'envolupant:

```
> Hu:=[Fu,diff(Fu,u)];
```

$$Hu := [(x - \frac{1}{2}\,u^3 - 2\,u)^2 + y^2 - (\frac{u^2}{2} + 1)^2\,(1 + u^2),$$
$$2\,(x - \frac{1}{2}\,u^3 - 2\,u)\,(-\frac{3\,u^2}{2} - 2) - 2\,(\frac{u^2}{2} + 1)\,(1 + u^2)\,u - 2\,(\frac{u^2}{2} + 1)^2\,u]$$

Resolem per Gröbner:

```
> Gu:=gbasis(Hu,plex(u,x,y));
```

$$Gu := [588 + 54\,x^6\,y^2 + 27\,x^4\,y^4 + 27\,x^8 + 1108\,x^2 + 775\,x^4 - 808\,x^2\,y^2 + 238\,x^6 - 18\,x^4\,y^2$$
$$- 108\,x^2\,y^4 - 108\,y^6 - 1092\,y^2 + 612\,y^4, 5832\,y^8\,u - 160704\,y^6\,u + 375696\,y^4\,u$$
$$- 77568\,u\,y^2 + 4200\,u + 13851\,y^2\,x^7 + 13581\,x^7 + 19683\,y^4\,x^5 + 177930\,x^5\,y^2$$
$$+ 96467\,x^5 + 23328\,x^3\,y^4 + 491184\,x^3\,y^2 + 222896\,x^3 - 5832\,x\,y^8 + 81972\,y^6\,x$$
$$- 787068\,y^4\,x + 399100\,x\,y^2 + 164372\,x, 648\,y^6\,x\,u - 16344\,y^4\,x\,u + 3608\,x\,u\,y^2$$
$$- 200\,x\,u - 891\,x^6\,y^2 + 1107\,x^6 - 1539\,x^4\,y^4 - 1482\,x^4\,y^2 + 7949\,x^4 - 648\,y^6\,x^2$$
$$+ 13752\,x^2\,y^4 - 3272\,x^2\,y^2 + 18712\,x^2 + 6156\,y^6 - 14484\,y^4 - 5756\,y^2 + 14084,$$
$$2665600\,x^2\,u - 110808\,y^6\,u + 3162024\,y^4\,u - 8695368\,u\,y^2 + 4481400\,u$$
$$- 263169\,x^7 - 373977\,x^5\,y^2 - 3013983\,x^5 - 443232\,x^3\,y^2 - 11563504\,x^3$$
$$+ 110808\,y^6\,x - 1666116\,y^4\,x + 15044688\,x\,y^2 - 12326628\,x, 150528\,u^2$$
$$+ 7128\,y^4\,x\,u - 170928\,x\,u\,y^2 - 282152\,x\,u - 9801\,x^6 - 16929\,x^4\,y^2 - 37335\,x^4$$
$$- 7128\,x^2\,y^4 + 142416\,x^2\,y^2 + 99896\,x^2 + 67716\,y^4 - 75192\,y^2 + 7476]$$

Seleccionem l'envolupant retenint l'ideal d'eliminació:

```
> env:=select(v->indets(v) subset {x,y},Gu);
```

$$env := [588 + 54\,x^6\,y^2 + 27\,x^4\,y^4 + 27\,x^8 + 1108\,x^2 + 775\,x^4 - 808\,x^2\,y^2 + 238\,x^6 - 18\,x^4\,y^2$$
$$- 108\,x^2\,y^4 - 108\,y^6 - 1092\,y^2 + 612\,y^4]$$

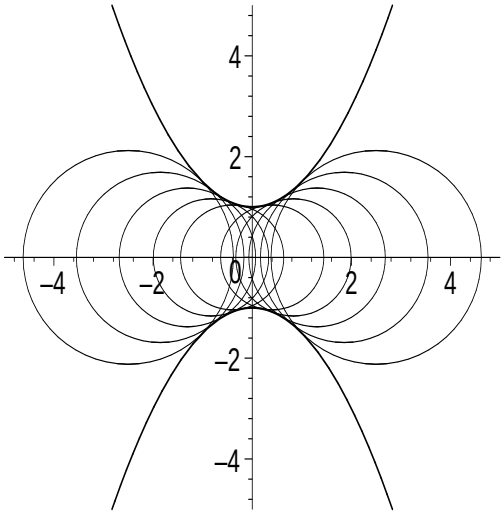
Factoritzem:

```
> cu:=factor(op(env));
```

$$cu := (2\,y + 2 + x^2)\,(-2\,y + 2 + x^2)\,(27\,x^4 + 130\,x^2 + 54\,x^2\,y^2 + 147 + 27\,y^4 - 126\,y^2)$$

```
> gmplot(['subs(u=i/5,Fu)' $ 'i'=-5..-1,'subs(u=i/5,Fu)' $
> 'i'=1..5,size=1/20,op(env)],x=-5..5,y=-5..5,comments=0);
```

Wait for the graphic please..



7. Descripció del teorema de l'extensió

El teorema de l'eliminació es complementa amb el teorema de l'extensió. A més de la seva pròpia utilitat, aquest teorema porta al Nullstellensatz, al teorema de la clausura de Zariski i als teoremes d'implicitació.

A fi d'aproximar-nos, comentem el pas d'extensió en l'exemple 1.1. Allí teníem $g_4(z) = z^2(z-1)^2(z^2+2z-1) = 0$. La pregunta de l'extensió és: sota quines condicions per cada valor de $z \in \mathbb{V}(\mathcal{I} \cap K[z])$ existeix algún valor de y, i per cada valor de $(z,y) \in \mathbb{V}(\mathcal{I} \cap K[z,y])$ algún valor de x tal que $(z,y,x) \in V(\mathcal{I})$?

Més en general, sigui 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 construir solucions coordenada per coordenada. Fixem j i anomenem $\overline{a}_j = (a_{j+1}, \ldots, a_n) \in \mathbb{V}(\mathcal{I}_j)$ 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

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

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

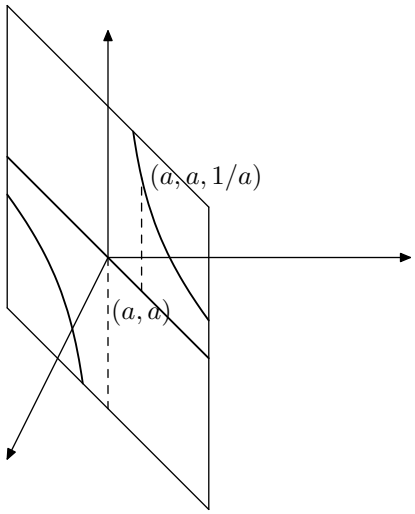
EXEMPLE 7.1. Donat el sistema

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

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

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

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.



En aquest exemple tenim:

$$\pi_1(V) = \mathbb{V}(\mathcal{I}_1) \setminus \{(0, 0)\},$$

on $\pi_1(V)$ és la projecció de V sobre $\mathbb{V}(\mathcal{I}_1)$. El nostre objectiu és poder determinar a priori quines solucions estenen i quines no.

Podem restringir 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 7.2 (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 $1 \leq i \leq s$ sigui*

$$\mathrm{lm}(f_i, \succ_{x_1}) = g_i(\overline{x_1})\, x_1^{N_i}$$

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 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 fàcil 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 $a \in \mathbb{C}$ 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'exemple 7.1. Alli teníem la solució parcial $x = a, y = a$ 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 z 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 z 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 $\mathbb{V}(g_1, \ldots, g_s)$ *depèn de la base de* $\mathcal{I}$. Canviant de base, es poden produir 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, el corresponent teorema de l'extensió afirma que 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 7.3. 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 $z = c \in \mathbb{V}(\mathcal{I}_2)$ 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

$g_1(b,c) = 0$ i $g_2(b,c) = 1$. 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 7.4. *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 i sigui*

$$\operatorname{lm}(f_i, \succ_{x_1}) = cx_1^N$$

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.

8. Geometria de l'eliminació

DEFINICIÓ 8.1 (Projecció). A l'espai afí $\overline{K}^m$, anomenem j-èsima projecció a

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

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

LEMA 8.2. *Donat un ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ i $V = \mathbb{V}(\mathcal{I})$, sigui $\mathcal{I}_j = \mathcal{I} \cap K[\overline{x_j}]$ 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 depèn de $\overline{x_j}$, resulta

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

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:

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

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

En l'exemple 7.1, tenim

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

TEOREMA 8.3 (Enunciat geomètric del teorema de l'extensió). *Donat un ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subseteq K[\overline{x}]$ on $\overline{K}$ és algebraicament tancat, sigui $V = \mathbb{V}(\mathcal{I})$ i*

$$\operatorname{lm}(f_i, \succ_{x_1}) = g_i(\overline{x}_1) x_1^{N_i}$$

Si $\mathcal{I}_1 = \mathcal{I} \cap K[\overline{x}_1]$ és el primer ideal d'eliminació tenim la igualtat següent a $\overline{K}^{n-1}$:

$$\mathbb{V}(\mathcal{I}_1) = \pi_1(V) \cup (\mathbb{V}(g_1, \ldots, g_s) \cap \mathbb{V}(\mathcal{I}_1)) \tag{8.1}$$

DEMOSTRACIÓ. Resulta del lema 8.2 i el teorema de l'extensió 7.2. □

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

EXEMPLE 8.4. Sigui l'ideal $\mathcal{I}=\langle f_1,f_2\rangle$ on

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

Determinem el seu ideal d'eliminació (calculant $\mathrm{gb}(\mathcal{I},\mathrm{lex}(x,y,z))$. Obtenim $G=\{y-z,xz-1,xy-z\}$ 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 7.2 no ens dona cap informació sobre la grandària 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 $\mathbb{V}(\mathcal{I}_j)$, donada pel teorema de la clausura que veurem al capítol 4 paragraph 2.1.

9. 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 $f,g\in K[x]$ respon 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 $\gcd(f,g,x)$ comporta divisions en K, mentre, com veurem, la resultant ho evita, i això interessa de cara a l'eliminació.

LEMA 9.1. *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) *$\deg_x(A)<m$ i $\deg_x(B)<l$.*
(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 $g=h\,g_1$. Òbviament f_1 té com a màxim grau $l-1$ 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 A' i B' tals que $A'f + B'g = 1$. Ara multipliquem per B i emprem (iii)

$$B = (A'\,f + B'\,g)\,B = A'\,B\,f + B'\,B\,g = A'\,Bf - A\,B'\,A\,f = (A'\,B - B'\,A)\,f.$$

Com que $B \neq 0$, això prova que B té com a mínim grau 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

$$f = \sum_{i=0}^{l} a_i\,x^i \qquad g = \sum_{i=0}^{m} b_i\,x^i$$
$$A = \sum_{j=0}^{m-1} c_j\,x^j \qquad B = \sum_{j=0}^{l-1} d_j\,x^j.$$

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:

$$\begin{aligned} 0 \;=\; Af + Bg &= \sum_{i=0}^{l}\sum_{j=0}^{m-1} a_i c_j x^{i+j} + \sum_{i=0}^{m}\sum_{j=0}^{l-1} b_i d_j x^{i+j} \\ &\sum_{k=0}^{l+m-1} x^k \left(\sum_{i=\max(0,k-m+1)}^{\min(l,k)} a_i c_{k-i} + \sum_{i=\max(0,k-l+1)}^{\min(m,k)} b_i d_{k-i} \right) = 0 \end{aligned}$$

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

(9.1)

$$\left\{\begin{array}{lllll} a_l c_{m-1} & & b_m d_{l-1} & = 0 & : x^{l+m-1} \\ a_{l-1}c_{m-1} + a_l c_{m-2} & & b_{m-1}d_{l-1} + b_m d_{l-2} & = 0 & : x^{l+m-2} \\ \vdots \quad \ddots & & \vdots & b_m d_0 = 0 & \\ \vdots & a_l c_0 + & \vdots & = 0 & \\ \vdots & \vdots & \vdots & = 0 & \\ a_0 c_{m-1} + & \vdots & \vdots & = 0 & \\ \quad \ddots & \vdots & \vdots & = 0 & \\ \quad\quad \ddots & \vdots & b_0 d_{l-1} & = 0 & \\ \quad\quad\quad \ddots & \vdots & & = 0 & \\ & a_0 c_0 + & & b_0 d_0 = 0 & : x^0 \end{array}\right.$$

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

$$\begin{aligned} f &= a_l x^l + \cdots + a_0 \\ g &= b_m x^m + \cdots + b_0 \end{aligned}$$

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

$$\mathrm{Syl}(f,g,x) = \begin{pmatrix} a_l & & & & & b_m & & & \\ a_{l-1} & a_l & & & & b_{m-1} & b_m & & \\ \vdots & a_{l-1} & a_l & & & \vdots & b_{m-1} & \ddots & \\ \vdots & & a_{l-1} & \ddots & & & & & b_m \\ \vdots & & & & a_l & \vdots & & & b_{m-1} \\ a_0 & & & & a_{l-1} & \vdots & & & \vdots \\ & a_0 & & & \vdots & b_0 & & & \vdots \\ & & a_0 & & \vdots & & b_0 & & \vdots \\ & & & \ddots & \vdots & & & \ddots & \vdots \\ & & & & a_0 & & & & b_0 \end{pmatrix}$$

on els elements exteriors als parl.lelògrams són nuls. És una matriu quadrada de $l+m$ files i columnes.

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 propietats de la resultant següents:

PROPOSICIÓ 9.3 (Propietats). *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 (9.1). Per tant, si és zero, el sistema (9.1) té solució no trivial i recíprocament. I si el sistema té solució, els polinomis A i B verifiquen (i), (ii) i (iii) del lema 9.1. □

EXEMPLE 9.4. Siguin $f = 2x^3 - 11x^2 + 8x + 6$ i $g = 10x^2 - 9x - 9$. La resultant és

$$\operatorname{Res}(f,g,x) = \begin{vmatrix} 2 & & 10 & & \\ -11 & 2 & -9 & 10 & \\ 8 & -11 & -9 & -9 & 10 \\ 6 & 8 & & -9 & -9 \\ & 6 & & & -9 \end{vmatrix} = 0$$

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

PROPOSICIÓ 9.5 (Propietats). *Donats $f, g \in K[x]$ de graus en x respectius l, m, es verifiquen les propietats següents:*

(i) $\operatorname{Res}(f,g,x) = (-1)^{lm} \operatorname{Res}(g,f,x)$.
(ii) $\operatorname{Res}(f,b_0,x) = b_0^l$, $\operatorname{Res}(a_0,g,x) = a_0^m$, $\operatorname{Res}(a_0,b_0,x) = 1$, $\operatorname{Res}(f,0,x) = \operatorname{Res}(0,g,x) = 0$.
(iii) *Siguin q, r el quocient i residu de dividir f entre g: $f = qg + r$. Llavors es té:*

$$\operatorname{Res}(f,g,x) = (-1)^{lm} b_m^{l-\deg(r)} \operatorname{Res}(g,r,x).$$

DEMOSTRACIÓ. Exercici 3.11 □

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

Algorisme pel càlcul de resultants

Input: $f, g \in K[\overline{x}]$
x: la variable respecte de la qual es calcula la resultant.
Output: $\operatorname{Res}(f,g,x)$

SI $g = 0$ ó $f = 0$ LLAVORS RETORNA 0
ALTRAMENT
  SI $f = a_0 = cte.$ LLAVORS RETORNA $a_0^{\deg(g,x)}$
  ALTRAMENT
    SI $g = b_0 = cte.$ LLAVORS RETORNA $b_0^{\deg(f,x)}$
    ALTRAMENT
      $r := \operatorname{rem}(f,g,x)$
      $(-1)^{\deg(f,x)\deg(g,x)} \operatorname{lcoeff}(g,x)^{\deg(f,x)-\deg(r,x)} \operatorname{Res}(g,r,x)$
    FI SI
  FI SI
FI SI

DEFINICIÓ 9.6. Donats els polinomis de $K[x]$

$$f = \sum_{i=0}^{l} a_i x^i, \quad g = \sum_{j=0}^{m} b_j x^j,$$

expressem-los en termes de les seves arrels ξ_i, η_j així:

$$f = a_l \prod_{i=1}^{l} (x - \xi_i), \quad g = b_m \prod_{j=1}^{m} (x - \eta_j).$$

Definim

$$\operatorname{res}(f, g, x) = a_l^m \prod_{i=1}^{l} g(\xi_i) = a_l^m b_m^l \prod_{i=1}^{l} \prod_{j=1}^{m} (\xi_i - \eta_j) = (-1)^{lm} b_m^l \prod_{j=1}^{m} f(\eta_j)$$

La igualtat de les tres definicions és obvia, emprant la descomposició dels polinomis en producte de les arrels.

PROPOSICIÓ 9.7. *Es compleix que* $\operatorname{res}(f, g, x) = \operatorname{Res}(f, g, x)$*, i per tant, la fórmula de la definició anterior de resultant es converteix en una nova propietat de la resultant.*

$$\operatorname{Res}(f, g, x) = a_l^m \prod_{i=1}^{l} g(\xi_i) = a_l^m b_m^l \prod_{i=1}^{l} \prod_{j=1}^{m} (\xi_i - \eta_j) = (-1)^{lm} b_m^l \prod_{j=1}^{m} f(\eta_j)$$

DEMOSTRACIÓ. La demostració consisteix en provar que l'algorisme per determinar la resultant donada per la definició anterior és el mateix que l'algorisme per determinar la resultant definida per la matriu de Sylvester. Cal provar, doncs, que amb la definició anterior, valen també les propietats 9.5, que determinen l'algorisme de la resultant. Exercici 3.12. □

EXEMPLE 9.8. 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 $K[y]$.

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

Més en general, si $f, g \in K[x, y]$ són de grau positiu en x, té sentit calcular $\operatorname{Res}(f, g, x)$. Com els coeficients són polinomis en y, la proposició 9.3 assegura que $\operatorname{Res}(f, g, x)$ 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 9.2 de la resultant, pot ampliar-se als polinomis de $K[x, \overline{y}]$. Tenim la següent proposició:

PROPOSICIÓ 9.9. *Donats* $f, g \in K[x, \overline{y}]$ *de grau positiu en* x*, existeixen polinomis* $A, B \in K[x, \overline{y}]$ (*únics si la resultant és diferent de zero*)*, tals que*

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

(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* $\deg_x(B) < \deg_x(f)$.
(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 9.3 per aplicar-los a l'equació

$$\tilde{A}f + \tilde{B}g = 1 \tag{9.2}$$

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.

Suposem, en primer lloc, que $\mathrm{Res}(f, g, x) \neq 0$. Posem

$$\begin{aligned} f &= a_l x^l + \cdots + a_0 \\ g &= b_m x^m + \cdots + b_0 \\ \tilde{A} &= \tilde{c}_{m-1} x^{m-1} + \cdots + \tilde{c}_0 \\ \tilde{B} &= \tilde{d}_{l-1} x^{l-1} + \cdots + \tilde{d}_0 \end{aligned}$$

on els coeficients $\tilde{c}_i, \tilde{d}_i \in K(\overline{y}) = \mathrm{Quot}(K[\overline{y}])$ són les incògnites. Substituint les expressions anteriors en (9.2) tenim un sistema similar al (9.1) canviant la darrera equació per

$$a_0\tilde{c}_0 + b_0\tilde{d}_0 = 1$$

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 precisament 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 (9.2), multiplicant per la resultant tindrem:

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

Si la resultant és igual a zero, llavors el sistema homogeni té solució (no única) i també podem multiplicar pel denominador per obtenir l'expressió $Af + Bg = 0$. Queden provats, doncs, els punts (i), (ii), (iii) i (iv) de la proposició.

Provem ara el punt (v). La demostració de la proposició 9.3 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 $\mathrm{Res}(f,g,x)=0$. Però el lema de Gauss vist en el capítol 1, afirma que $f\in K[\overline{y}][x]$ de $\mathrm{cont}(f)=1$ és irreductible a $K[\overline{y}][x]$ ssi ho és a $K(\overline{y})[x]$. Aplicant-ho aquí, 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 9.10. Podem ara reprendre l'exemple 9.8. Per la proposició 9.9, està clar que $f=xy-1$ i $g=x^2+y^2-4$ 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:

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

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

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

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

EXEMPLE 9.11. Si considerem els polinomis

$$f=(xy-z)(xy+z)=x^2y^2-z^2$$
$$g=(xy+z)(x+y+z)=x^2y+x(y^2+yz+z)+z(y+z)$$

tindrem $\mathrm{Res}(f,g,x)=0$. Anàlogament també tindríem $\mathrm{Res}(f,g,y)=0$ i $\mathrm{Res}(f,g,z)=0$.

10. Resultants i teorema de l'extensió

Com a conseqüencia immediata de la proposició 9.3 resulta el següent

COROL·LARI 10.1. *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* $\mathrm{Res}(f,g,x)=0$.

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

$$f=a_lx^l+\cdots+a_0,\quad g=b_mx^m+\cdots+b_0$$

així que $a_l,b_m\in K[\overline{y}]$ 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 $(\overline{c})\in\mathbb{V}(\mathcal{I}_1)\setminus\mathbb{V}(a_m,b_l)$, 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 $a_l(\overline{c})\neq 0$ i $b_m(\overline{c})\neq 0$. És a dir, que tots dos són no nuls. Tenim

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

Per la proposició 9.9 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 $(\overline{c})$:

$$h(\overline{c})=\begin{vmatrix} a_l(\overline{c}) & & & & b_m(\overline{c}) & & \\ a_{l-1}(\overline{c}) & & & & b_{m-1}(\overline{c}) & & \\ \vdots & a_l(\overline{c}) & & & \vdots & \ddots & \\ \vdots & a_{l-1}(\overline{c}) & \ddots & & & & b_m(\overline{c}) \\ \vdots & & & a_l(\overline{c}) & \vdots & & b_{m-1}(\overline{c}) \\ a_0(\overline{c}) & & & a_{l-1}(\overline{c}) & \vdots & & \vdots \\ & & & \vdots & b_0(\overline{c}) & & \vdots \\ & a_0(\overline{c}) & & \vdots & & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_0(\overline{c}) & & & b_0(\overline{c}) \end{vmatrix}$$

Tenint en compte que $a_l(\overline{c})\neq 0$ i $b_m(\overline{c})\neq 0$, 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 10.1 implica que $f(\overline{c},x)$ i $g(\overline{c},x)$ tenen una arrel comú, $c\in K$ tal com volíem demostrar.

Ara falta considerar el cas en que no tots dos $a_l(\overline{c})$ i $b_m(\overline{c})$ són diferents de zero. Suposem que únicament és diferent de zero $a_l(\overline{c})\neq 0$, mentre que $b_m(\overline{c})=0$. En aquest cas, $g(\overline{c},x)$ té grau estrictament inferior a $m=\deg_x g(\overline{y},x)$ i 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. Podríem 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 $a_l(\overline{c})\neq 0$, $b_m(\overline{c})=0$. Si N és un enter positiu, òbviament

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

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_l, 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 $a_l(\overline{c}) = b_m(\overline{c}) = 0$ 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 contra-exemples 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 solucions 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.

11. Resultants generalitzades i teorema de l'extensió

Definició 11.1 (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 9.9, 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 11.2. 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:

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

PROPOSICIÓ 11.3. *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*

$$h = \mathrm{Res}(f_1, f_2u_2 + \cdots + f_su_s, x) = \sum_\alpha h_\alpha(\overline{y})u^\alpha \subset K[\overline{u}, \overline{y}]$$

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 9.9 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:

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

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 11.4 (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 $1 \leq i \leq s$ i sigui*

$$\operatorname{lm}(f_i, \succ_x) = g_i(\overline{y}) x^{N_i}$$

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. Volem saber $f_1(\overline{c}, x), \ldots, f_s(\overline{c}, x)$ tenen una arrel $c \in K$ comú. El cas $s = 2$ l'hem tractat i resolt en el paragraph anterior i està resumit en el teorema 10.2, que cobreix 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 $\overline{c} \notin \mathbb{V}(g_1, \ldots, g_s)$ podem suposar, reordenant si cal, que $g_1(\overline{c}) \neq 0$. Siguin $h_\alpha \in K[\overline{y}]$ les resultants generalitzades

$$\operatorname{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x) = \sum_\alpha h_\alpha u^\alpha \tag{11.1}$$

Per la proposició anterior 11.3, 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 (11.1) mostra que la resultant

$$h(\overline{u}, \overline{y}) = \operatorname{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x) \tag{11.2}$$

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

$$h(\overline{u}, \overline{c}) \equiv 0 \tag{11.3}$$

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

Fem ara la hipòtesi següent sobre f_2:

$$g_2(\overline{c}) \neq 0, \quad \text{i } f_2 \text{ té grau en } x \text{ més gran que } f_3, \ldots, f_s \tag{11.4}$$

La conjectura és que això implica

$$h(\overline{u}, \overline{c}) = \operatorname{Res}(f_1(\overline{c}, x), u_2 f_2(\overline{c}, x) + \cdots + u_s f_s(\overline{c}, x), x) \tag{11.5}$$

és a dir a la resultant dels polinomis $f_1(\overline{c}, x)$ i $\sum_{i=2}^s u_i\, f_i(\overline{c}, x)$ respecte a la variable x.

L'argumentació és anàloga a la que hem fet en la demostració del teorema 10.2. És a dir, quan avaluem el determinant (11.2) 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 (11.5), 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 (11.4), ja que amb aquestes hipòtesis el coeficient principal és $g_2(\overline{c}) \neq 0$.

Combinant (11.3) i (11.5), resulta

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

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 implica 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 $F \mid u_2 f_2(\overline{c}, x) + \cdots + u_s f_s(\overline{c}, x)$, posant $u_j = 0$ per $j \neq i$ i $u_i = 1$ resulta 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 compleixen les hipòtesis (11.4).

Només queda provar-lo si no es verifiquen les hipòtesis (11.4). El procediment és el mateix que hem fet servir en el cas del teorema 10.2, és a dir un canvi de base de l'ideal. És obvi que

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

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 $f_3, \ldots, f_s$. La nova base ara ja compleix les hipòtesis (11.4), 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. □

Recordem aquí, per la seva importància, el corol·lari 7.4 d'aquest teorema, ja enunciat al principi del capítol.

12. Exercicis

Secció 1.

EXERCICI 3.1. Proveu que l'ordre de Bayer-Stillman definit a l'exercici 2.9 c) és un ordre d'eliminació per les variables $x_1, \ldots, x_j$.

EXERCICI 3.2. Trobeu l'ideal de varietat de $V = \{(0,0),(1,0)\}$ a $\mathbb{C}^2$.

EXERCICI 3.3. Proveu que $B = \{x+4y, 4y^2-y\}$ és una base de Gröbner d'un ideal $\mathcal{I}$ per un cert ordre monomial. Proveu també que $\mathcal{I}$ és ideal de varietat. De quina varietat?

EXERCICI 3.4. Proveu que l'ideal de varietat de la cúbica guerxa és $\langle y - x^2, z - x^3\rangle$.

EXERCICI 3.5. A $\mathbb{F}_2[x,y]$ considerem el conjunt $\mathcal{I}$ de polinomis que s'anul·len per tot punt de $\mathbb{F}_2^2$.

a) Proveu que $\mathcal{I}$ és un ideal de $\mathbb{F}[x,y]$.
b) Proveu que $F = \{x^2 - x, y^2 - y\}$ és una base de $\mathcal{I}$. És una base de Gröbner per algún ordre? És l'ideal d'una varietat? De quina varietat? Compareu-ho amb el cas d'un cos infinit.
c) Trobeu una base de l'ideal de polinomis de $\mathbb{F}_p[x_1, \ldots, x_n]$ que s'anul·len a $\mathbb{F}_p^n$, demostrant que ho és.
d) Comenteu si és base de Gröbner i per quins ordres.

EXERCICI 3.6. Trobeu la base de Gröbner en l'ordre $\text{lex}(x,y,z)$ de l'ideal de varietat de

$$V = \{(1,-1,0),(0,1,1),(2,1,2)\}$$

EXERCICI 3.7. Trobeu l'ideal de varietat de la varietat de $\mathbb{R}^3$ següent:

$$V = \{(0,0,0),(1,0,0),(0,1,0),(0,1,1),(1,0,1)$$

EXERCICI 3.8. Determineu la base de Gröbner reduïda en l'ordre $\text{lex}(x,y)$ de l'ideal de varietat de

$$V = \{(a_1,b_1),(a_1,b_2),(a_2,b_2)\},$$

on $a_1 \neq a_2$ i $b_1 \neq b_2$.

EXERCICI 3.9. Determineu la base de Gröbner reduïda $\text{gb}(\mathbb{I}(V), \text{lex}(x,y,z))$ de l'ideal de varietat de V, on

$$V = \{(x_0,y_1,z_1),(x_1,y_0,z_1),(x_1,y_1,z_0)\},$$

i $x_0 \neq x_1$, $y_0 \neq y_1$, $z_0 \neq z_1$.

Secció 4.

EXERCICI 3.10. 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) Descriviu la varietat $\mathbb{V}(\mathcal{I})$. Feu un gràfic il·lustrant també $\mathbb{V}(\mathcal{I}_1)$.

Secció 9.

EXERCICI 3.11. La proposició 9.5 diu:

Donats $f, g \in K[x]$ de graus en x respectius l, m, es verifiquen les propietats següents:

(i) $\mathrm{Res}(f,g,x) = (-1)^{lm}\,\mathrm{Res}(g,f,x)$.
(ii) $\mathrm{Res}(f,b_0,x) = b_0^l$, $\mathrm{Res}(a_0,g,x) = a_0^m$, $\mathrm{Res}(a_0,b_0,x) = 1$, $\mathrm{Res}(f,0,x) = \mathrm{Res}(0,g,x) = 0$.
(iii) Siguin q, r el quocient i residu de dividir f entre g: $f = qg + r$. Llavors es té:

$$\mathrm{Res}(f,g,x) = (-1)^{lm} b_m^{l-\deg(r)}\,\mathrm{Res}(g,r,x).$$

A fi de provar-la, procediu de la manera següent: Siguin $f = \sum_{i=0}^{l} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$, i suposeu $l \geq m$.

a) Sigui $\tilde{f} = f - (a_l/b_m)x^{l-m}g$, és a dir el primer residu parcial de la divisió de f entre g. Proveu que si $\deg \tilde{f} = l-1$, llavors

$$\mathrm{Res}(f,g,x) = (-1)^m\, b_m\, \mathrm{Res}(\tilde{f},g,x).$$

b) Si ara admetem que el grau de $\tilde{f}$ pugui ser inferior a $l-1$, proveu que

$$\mathrm{Res}(f,g,x) = (-1)^{m(l-\deg\tilde{f})}\, b_m^{l-\deg\tilde{f}}\, \mathrm{Res}(\tilde{f},g,x).$$

c) Utilitzeu l'algorisme de la divisió per provar que

$$\mathrm{Res}(f,g,x) = (-1)^{ml}\, b_m^{l-\deg r}\, \mathrm{Res}(g,r,x).$$

EXERCICI 3.12. A fi de provar la proposició 9.7, recordem les definicions: Donats els polinomis de $K[x]$

$$f = \sum_{i=0}^{l} a_i x^i, \quad g = \sum_{j=0}^{m} b_j x^j,$$

els expressem en termes de les seves arrels ξ_i, η_j així:

$$f = a_l \prod_{i=1}^{l} (x - \xi_i), \quad g = b_m \prod_{j=1}^{m} (x - \eta_j).$$

Definim

$$\operatorname{res}(f, g, x) = a_l^m \prod_{i=1}^{l} g(\xi_i).$$

a) Proveu que

$$\operatorname{res}(f, g, x) = a_l^m \prod_{i=1}^{l} g(\xi_i) = a_l^m b_m^l \prod_{i=1}^{l} \prod_{j=1}^{m} (\xi_i - \eta_j) = (-1)^{lm} b_m^l \prod_{j=1}^{m} f(\eta_j)$$

b) Proveu les propietats (i), (ii) i (iii) de l'exercici 3.11, però ara relatives a la definició de $\operatorname{res}(f, g, x)$.
c) Deduïu que $\operatorname{Res}(f, g, x) = \operatorname{res}(f, g, x)$.

EXERCICI 3.13. Es defineix el discriminant d'un polinomi $f(x)$ per

$$\operatorname{disc}(f) = a_n^{2n-2} \prod_{i<j} (\xi_i - \xi_j)^2.$$

Proveu que

(i) $\operatorname{disc}(fg) = \operatorname{disc}(f) \operatorname{disc}(g) \operatorname{Res}(f, g, x)^2$,
(ii) Si $f \neq 0$, $\operatorname{Res}(f, f', x) = (-1)^{n(n-1)/2} a_n \operatorname{disc}(f)$.
(iii) Sigui p un primer senar. Considerem el polinomi ciclotòmic

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

Llavors és

$$\operatorname{disc}(\Phi_p) = (-1)^{(p-1)/2} p^{p-2}.$$

Secció 10.

EXERCICI 3.14. Sigui $H = \langle h_1, h_2 \rangle$ un ideal de $\mathbb{Q}[x, y]$ i $G_H = \{g_1, \ldots, g_s\}$ la base de Gröbner lex $x \succ y$ de H.

Estudieu com són les solucions $\mathbb{V}(H)$ segons com siguin $\operatorname{Res}(h_1, h_2, x)$ i $\operatorname{Res}(h_1, h_2, y)$. (Digueu si és 0-dimensional o no.)

Secció 11.

EXERCICI 3.15. Sigui $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ un ideal de $K[\overline{y}, x]$. Proveu que $\mathcal{I} \cap K[\overline{y}] = \{0\}$ ssi tots els polinomis de $\mathcal{I}$ tenen un factor comú de grau positiu en x.

Nota: Utilitzeu les resultants generalitzades.

CAPíTOL 4

Nullstellensatz i Conseqüències

1. Nullstellensatz d'Hilbert

El teorema dels zeros d'Hilbert va ser un teorema tan cel·lebrat que s'acostuma a nomenar pel nom en alemany amb que va ser batejat. (En alemany Null = zero, Stelle = posició, Satz = teorema; Nullstellensatz = Teorema de la posició dels zeros). La seva importància radica en el fet que generalitza el teorema fonamental de l'àlgebra per n variables.

1.1. Nullstellensatz feble.

TEOREMA 1.1 (Nullstellensatz feble). *Sigui K un cos algebraicament tancat i $\mathcal{I} \subset K[\overline{x}]$ un ideal tal que $\mathbb{V}(\mathcal{I}) = \phi$. Llavors $\mathcal{I} = \langle 1 \rangle = K[\overline{x}]$.*

El Nullstellensatz generalitza el teorema fonamental de l'àlgebra. En efecte, $\mathbb{C}[x]$ és un PID, i per tant tot ideal de $\mathbb{C}[x]$ és generat per un únic polinomi $p(x)$. Tenim $\mathcal{I} = \langle p(x) \rangle$ i $\mathbb{V}(\mathcal{I}) = \mathbb{V}(p(x))$. El teorema fonamental de l'àlgebra afirma que tot polinomi no constant sobre $\mathbb{C}[x]$ té al menys una arrel. Per tant, si $\mathbb{V}(p(x)) = \phi$ implica que $p(x)$ és un polinomi constant, i per tant $\langle p(x) \rangle = \mathbb{C}[x]$, que és l'enunciat del Nullstellensatz feble en aquest cas.

En realitat, el teorema fonamental de l'àlgebra el que afirma pròpiament és que $\mathbb{C}$ és un cos algebraicament tancat.

DEMOSTRACIÓ. Anem a provar-ho per inducció sobre el nombre de variables n. El cas d'una sola variable ja l'hem discutit més amunt.

Suposem ara cert el teorema per n variables i provem-ho per $n+1$. Considerem un ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subset K[\overline{x}, y]$. Per hipòtesi d'inducció el teorema és cert a $K[\overline{x}]$. Podem suposar que f_1 no és una constant, ja que si no no hi ha res a provar. Sigui $N \geq 1$ el grau total de f_1. Anem a veure que podem considerar que f_1 és de la forma

$$f_1(\overline{x}, y) = cy^N + \text{termes de grau menor que } N \text{ en } y \tag{1.1}$$

on c és una constant.

En efecte, considerem un canvi de coordenades

$$\begin{aligned} y &= \tilde{y} \\ x_1 &= \tilde{x_1} + a_1\tilde{y} \\ &\cdots \\ x_n &= \tilde{x_n} + a_n\tilde{y} \end{aligned}$$

on les a_i's són constants no nul.les a determinar. Llavors

$$f_1(\overline{x},y)=\sum_{\alpha,i}c_{\alpha i}\overline{x}^{\alpha}y^i=\sum_{|\alpha|+i=N}c_{\alpha i}\overline{x}^{\alpha}y^i+\sum_{|\alpha|+i<N}c_{\alpha i}\overline{x}^{\alpha}y^i$$

Denotem S el conjunt de monomis de f_1 de grau total N màxim. Tenint en compte que els a_i's són no nuls, els monomis de grau màxim N en $\tilde{y}$ seran aquells que provinguin del desenvolupament dels anteriors on $|\alpha|+i=N$:

$$\begin{aligned}\overline{x}^{\alpha}y^i &= x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}y^i=(\tilde{x_1}+a_1\tilde{y})^{\alpha_1}(\tilde{x_2}+a_2\tilde{y})^{\alpha_2}\dots(\tilde{x_n}+a_n\tilde{y}^{\alpha_n})y^i\\ &= a_1^{\alpha_1}\dots a_n^{\alpha_n}\,\tilde{y}^{|\alpha|+i}+\text{termes de grau en }\tilde{y}\text{ menors que }|\alpha|+i\end{aligned}$$

i per tant seran de la forma $\overline{a}^{\alpha}\tilde{y}^N$. En definitiva, aquests termes de grau N de f_1 seran

$$\tilde{y}^N\sum_{|\alpha|+i=N}c_{\alpha i}\overline{a}^{\alpha}=h(\overline{a})\,\tilde{y}^N$$

on $h(\overline{a})$ és un polinomi en les $\overline{a}$. Tenint en compte que el cos és algebraicament tancat, i per tant infinit, podem trobar valors de les a_i's pels quals $c=h(\overline{a}^{(0)})\neq 0$.

Amb el canvi de variables, cada polinomi en les x_i's i y es transforma en un altre polinomi en les $\tilde{x_i}$'s i $\tilde{y}$, i òbviament $\tilde{\mathcal{I}}=\{\tilde{f}:f\in\mathcal{I}\}$ és un ideal de $K[\tilde{\overline{x}},\tilde{y}]$. Observem que també $\mathbb{V}(\tilde{\mathcal{I}})=\phi$ ja que si les equacions transformades tenen solucions, les inicials també pel canvi de coordenades. Per tant queda provat que podem considerar que f_1 és de la forma assenyalada (1.1) i té com a coeficient de grau màxim en y una constant.

Ara podem aplicar el teorema de l'extensió i el seu corol·lari quan hi ha algún coeficient constant. Sigui $\mathcal{I}_1=\mathcal{I}\cap K[\overline{x}]$ l'ideal d'eliminació. Tota solució parcial $\overline{b}\in\mathbb{V}(\mathcal{I}_1)$ estén a alguna solució $(\overline{b},b)\in\mathbb{V}(\mathcal{I})$. Per tant, si $\mathbb{V}(\mathcal{I})=\phi$, també

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

Ara la hipòtesi d'inducció implica que $\mathcal{I}_1=\langle 1\rangle$, i per tant $1\in\mathcal{I}_1\subset\mathcal{I}$. □

Aquest teorema resol el problema de la consistència d'un sistema d'equacions sobre $\mathbb{C}[\overline{x}]$. El sistema

$$f_1(\overline{x})=0,\dots,\ f_s(\overline{x})=0$$

tindrà solució ssi $1\notin\langle f_1,\dots,f_s\rangle$. En termes de bases de Gröbner només caldrà trobar la base de Gröbner reduïda de l'ideal en qualsevol ordre monomial, i si és diferent de $\{1\}$ el sistema és compatible. Aquest serà *l'algorisme de consistència*.

Si el cos en qüestió no és algebraicament tancat, l'algorisme funciona en un sentit: si la base de Gröbner és $\{1\}$, el sistema és incompatible. Però no podem afirmar que sigui compatible en cas contrari, com es fàcil comprovar (Ex.: $\mathcal{I}=\langle x^2+1\rangle$ a $\mathbb{R}[x]$).

Existeixen dues versions més fortes del teorema que expliquen amb més detall la relació entre ideal i ideal de varietat per un cos algebraicament tancat. En particular, provem que la única raó per la qual un ideal no és

ideal de varietat és perquè conté algún factor múltiple f^m d'un polinomi f i en canvi no conté f. Més concretament tenim:

TEOREMA 1.2 (Nullstellensatz). *Sigui K un cos algebraicament tancat. Si $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ i $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$, llavors existeix un enter m tal que $f^m \in \mathcal{I}$ i recíprocament.*

DEMOSTRACIÓ. Hem de provar, que donat un polinomi $f \in K[\overline{x}]$ que s'anul·la sobre tot $\mathbb{V}(\mathcal{I})$, existeix un $m \in \mathbb{N}$ i uns $A_i(\overline{x}) \in K[\overline{x}]$ tal que

$$f^m = \sum_{i=1}^{s} A_i f_i$$

Considerem l'ideal de $K[\overline{x}, y]$

$$\tilde{\mathcal{I}} = \langle f_1, \ldots, f_s, 1 - yf \rangle$$

Primer provem que

$$\mathbb{V}(\tilde{\mathcal{I}}) = \phi.$$

Per provar-ho demostrarem que cap punt $(\overline{a}, a) \in K^{n+1}$ és solució del sistema $\mathbb{V}(\tilde{\mathcal{I}})$. En efecte, poden passar dues coses:

(i) $(\overline{a}) \in \mathbb{V}(f_1, \ldots, f_s)$. Llavors $f(\overline{a}) = 0$ i per tant $1 - af(\overline{a}) = 1 \neq 0$ i per tant $(\overline{a}, a) \notin \mathbb{V}(\tilde{\mathcal{I}})$.

(ii) $(\overline{a}) \notin \mathbb{V}(f_1, \ldots, f_s)$. Llavors existeix algún f_i tal que $f_i(\overline{a}) \neq 0$, i per tant $(\overline{a}, a) \notin \mathbb{V}(\tilde{\mathcal{I}})$.

Aplicant ara el Nullstellensatz feble, resulta que $1 \in \tilde{\mathcal{I}}$. Per tant, existeixen polinomis C_i, per $1 \leq i \leq s$, i B tal que

$$1 = \sum_{i=1}^{s} C_i(\overline{x}, y) f_i + B(\overline{x}, y)(1 - yf) \tag{1.2}$$

Posem $y = 1/f(\overline{x})$. L'expressió anterior es converteix en

$$1 = \sum_{i=1}^{s} C_i(\overline{x}, 1/f(\overline{x})) f_i \tag{1.3}$$

Multiplicant ambdós costats de la igualtat anterior per una potència convenient de f, eliminarem els denominadors del segon membre, resultant

$$f^m = \sum_{i=1}^{s} A_i(\overline{x}) f_i(\overline{x}) \tag{1.4}$$

per certs polinomis $A_i \in K[\overline{x}]$, tal com volíem provar. □

Amb aquest teorema queda clara la relació entre ideals i ideals de varietat per cossos algebraicament tancats, que podem concretar en el següent teorema de Hilbert:

TEOREMA 1.3 (Nullstellensatz fort). *Sigui K un cos algebraicament tancat i $\mathcal{I}$ un ideal qualsevol de $K[\overline{x}]$. Llavors*

$$\mathbb{I}(\mathbb{V}(\mathcal{I})) = \sqrt{\mathcal{I}}$$

DEMOSTRACIÓ. Ja sabem que sempre $\sqrt{\mathcal{I}} \subseteq \mathbb{I}(\mathbb{V}(\mathcal{I}))$, ja que si $f \in \sqrt{\mathcal{I}}$, per definició existeix un m tal que $f^m \in \mathcal{I}$, i per tant f s'anul·la sobre $\mathbb{V}(\mathcal{I})$ i $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$.

Ara, en el cas que el cos sigui algebraicament tancat, el Hilbert Nullstellensatz (1.2) permet provar la inclusió recíproca. En efecte, si $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$, llavors per (1.2) existeix un m tal que $f^m \in \mathcal{I}$. Per tant, $f \in \sqrt{\mathcal{I}}$, quedant completat el resultat. □

Al capítol 3 vàrem donar un algorisme per determinar si un polinomi f pertany a $\sqrt{\mathcal{I}}$. Consisteix en determinar si la base de Gröbner de l'ideal $\tilde{\mathcal{I}} = \langle \mathcal{I}, 1 - y\, f \rangle \subseteq K[\overline{x}, y]$ en un ordre monomial qualsevol és igual a $\langle 1 \rangle$. Si el cos és algebraicament tancat és $\mathbb{I}(\mathbb{V}(\mathcal{I})) = \sqrt{\mathcal{I}}$ i per tant, l'algorisme de pertinença és el mateix.

2. Teorema de la Clausura

TEOREMA 2.1 (Clausura de Zariski). *Sigui K un cos algebraicament tancat, $\mathcal{I} = \langle f_1, \ldots, f_s \rangle \subset K[\overline{x}]$ i $V = \mathbb{V}(\mathcal{I}) \subset K^n$. Sigui $\pi_j : K^n \to K^{n-j}$ la j-èsima projecció i $\mathcal{I}_j = \mathcal{I} \cap K[\overline{x}_j]$. Llavors*

(i) *$\mathbb{V}(\mathcal{I}_j)$ és la clausura 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*

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

DEMOSTRACIÓ.

(i) Donat un conjunt S, la seva clausura de Zariski $\overline{S}$ és la varietat més petita que el conté i ve donada per: $\overline{S} = \mathbb{V}(\mathbb{I}(S))$. Per tant, el que hem de provar és que

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

$\subseteq$: Obvi, ja que $\pi_j(V) \subseteq \mathbb{V}(\mathcal{I}_j)$ i $\mathbb{V}(\mathcal{I}_j)$ és una varietat.

$\supseteq$: Hem de provar que $\mathbb{V}(\mathbb{I}(\pi_j(V))) \supseteq \mathbb{V}(\mathcal{I}_j)$ que és equivalent a $\mathbb{I}(\pi_j(V)) \subseteq \mathbb{I}(\mathbb{V}(\mathcal{I}_j) = \sqrt{\mathcal{I}_j}$ pel Nullstellensatz.
Prenem $f \in \mathbb{I}(\pi_j(V))$ i $\overline{a}_j \in \pi_j(V)$. Tindrem $f(\overline{a}_j) = 0$, i com f no depèn de les primeres j variables, per tot $a_1, \ldots, a_j$ tindrem $f(a_1, \ldots, a_j, \overline{a}_j) = 0$. Per tant, per tot $\overline{a} \in \mathbb{V}(\mathcal{I})$ serà $f(\overline{a}) = 0$, el que assegura que $f \in \mathbb{I}(V(\mathcal{I}))$. Pel Nullstellensatz

existeix N tal que $f^N \in \mathcal{I}$. Però com $f \in K[\overline{x}]$ serà $f^N \in \mathcal{I}_j$ i per tant $f \in \sqrt{\mathcal{I}_j}$ tal com volíem provar.

(ii) Ho provarem per $j = 1$.

Farem servir la descomposició donada per la fórmula (8.1), relativa al teorema 8.3 del capítol 3. Donat l'ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$, i $V = \mathbb{V}(\mathcal{I})$, posàvem

$$f_i(\overline{x}) = g(\overline{x}_1)x_1^{N_i} + \text{ termes de grau menor que } N_i \text{ en } x_1$$

on $\overline{x}_1 = x_2, \ldots, x_n$. Llavors teníem

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

on

$$W = \mathbb{V}(g_1, \ldots, g_s) \cap \mathbb{V}(\mathcal{I}_1)$$

Aquesta descomposició (8.1) implica que $\mathbb{V}(\mathcal{I}_1) \setminus W \subseteq \pi_1(V)$ i $W \subseteq \mathbb{V}(\mathcal{I}_1)$. Si provem que $W \neq \mathbb{V}(\mathcal{I}_1)$, haurem acabat. Però pot passar, com a l'exemple 8.4 del capítol 3, 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 $V = \mathbb{V}(f_1, \ldots, f_s, g_1, \ldots, g_s)$. La inclusió $\supseteq$ és obvia. Per provar la inclusió $\subseteq$, sigui $\overline{a} \in V$. Llavors, cada f_i s'anul.la en $\overline{a}$, 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 $\overline{a} \in \mathbb{V}(f_1, \ldots, f_s, g_1, \ldots, g_s)$, el que prova la igualtat.

Sigui ara $\tilde{\mathcal{I}} = \langle f_1, \ldots, f_s, g_1, \ldots, g_s \rangle$. 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 clausura de Zariski 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

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

Apliquem novament el teorema 8.3 a $V = \mathbb{V}(\tilde{f}_1, \ldots, \tilde{f}_s, g_1, \ldots, g_s)$. 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 $\tilde{W} = \mathbb{V}(\tilde{\mathcal{I}}_1) \cap \mathbb{V}(\tilde{f}_1, \ldots, \tilde{f}_s, g_1, \ldots, g_s)$, consisteix en aquelles solucions parcials per les quals els coeficients principals en x_1 de $\tilde{f}_1, \ldots, \tilde{f}_s$ s'anul.len.

Abans de continuar il·lustrem amb l'exemple 8.4 per què $\tilde{W}$ pot ser més petita que W. La base de I és

$$B = \{(y-z)x^2 + xy - 1, (y-z)x^2 + xz - 1\}$$

i $\mathcal{I}_1 = \langle y - z\rangle$. Per tant tenim $g_1 = g_2 = y - z$, 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 8.3 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 arribaríem a que tots els generadors tindrien 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 $V \neq \phi$).

□

L'enunciat de (i) afirma que el conjunt de punts de $\pi_j(V)$ que estenen formen un conjunt *obert* i *dens* a $\mathbb{V}(\mathcal{I}_j)$. Únicament en un conjunt de punts que no afecta a la clausura poden no estendre les solucions parcials. Si la descomposició de $\mathbb{V}(\mathcal{I}_j)$ en varietats irreductibles és $\mathbb{V}(\mathcal{I}_j) = \bigcup_i V_{ji}$, i el subconjunt de punts que no estenen és S, tenim

$$\pi_j(V) = \mathbb{V}(\mathcal{I}_j) \setminus S = \bigcup_i V_{ji} \setminus S_i$$

on $S_i = S \cap V_{ji}$. (i) afirma doncs que $\overline{V_{ji} \setminus S_i} = V_{ij}$ i per tant no solament $\pi_j(V)$ és obert en $\mathbb{V}(\mathcal{I}_j)$ sino que també és obert dins de cada component i és per tant dens.

L'enunciat de (ii) afirma 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 $\mathbb{V}(\mathcal{I}_j)$.

El teorema de la clausura ens dona 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 estrictament continguts en una varietat menor que $\mathbb{V}(\mathcal{I}_j)$ i que és dens.

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

$$\pi_j(V) = \bigcup_{i=1}^{l} (W_i \setminus Z_i)$$

Un conjunt amb aquesta característica es diu que és constructible.

En correspondència al corol.lari 7.4 tenim la següent versió geomètrica.

COROL·LARI 2.2. *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

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

DEMOSTRACIÓ. És conseqüència immediata del teorema de l'extensió. □

3. Implicitació

Recordem (veure apartat 12 del capítol 1) que una parametrització és una aplicació:

$$\begin{array}{rccc} F: & S \subseteq K^m & \longrightarrow & K^n \\ & \bar{t} & \mapsto & F(\bar{t}) \end{array} \tag{3.1}$$

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

$$x_1 = f_1(\bar{t}),\ \ldots,\ x_n = f_n(\bar{t}) \tag{3.2}$$

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 consisteix en trobar la clausura de Zariski $\overline{F(S)}$ de $F(S)$, és a dir, la varietat més petita que conté els punts parametritzats o el que és equivalent, la varietat definida per la parametrització.

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.

3.1. Implicitació polinòmica. Donada la parametrització polinòmica (3.1), on F és polinòmica i $S = K^m$, a fi d'estudiar com actua el mètode d'eliminació, introduïm les funcions següents

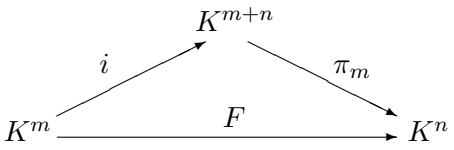
$$\begin{array}{rccc} i: & K^m & \longrightarrow & K^{m+n} \\ & (\bar{t}) & \mapsto & (\bar{t}, F(\bar{t})) \end{array} \qquad \begin{array}{rccc} \pi_m: & K^{n+m} & \longrightarrow & K^n \\ & (\bar{t}, \overline{x}) & \mapsto & (\overline{x}), \end{array}$$

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

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

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

Fem un esquema de com actuen les funcions descrites:



Tenim $F = \pi_m \circ i$. És important destacar que

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

ja que per tot $\bar{t} \in K^m$, els punts $i(\bar{t}) = (\bar{t}, F(\bar{t}))$ verifiquen les equacions que defineixen V, i recíprocament, en les equacions que defineixen V, $\bar{t}$ és arbitrari. 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 2.1 ens assegura que la clausura de Zariski 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. El teorema pot generalitzar-se per tot cos infinit:

Teorema 3.1 (Implicitació polinòmica). *Sigui K un cos infinit, i sigui* (3.2) *l'expressió d'una parametrització polinòmica $F : K^m \longrightarrow K^n$. Sigui $\mathcal{I}$ l'ideal de $K[\bar{t}, \overline{x}]$, definit per $\mathcal{I} = \langle x_1 - f_1(\bar{t}), \ldots, x_n - f_n(\bar{t}) \rangle$, i $\mathcal{I}_m = \mathcal{I} \cap K[\overline{x}]$ l'm-èsim ideal d'eliminació. Llavors la clausura de Zariski 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 discussió anterior quan el cos és algebraicament tancat. Suposem ara que K és un cos infinit qualsevol. Òbviament $\mathbb{Z} \subset \mathbb{Q} \subseteq K \subset \overline{K}$, on $\overline{K}$ és el cos clausura algebraica de K. (Veure cap VII, §2, LANG (1965), Algebra, Addison Wesley, Reading, Massachusetts).

Per provar el teorema a K utilitzarem una tècnica característica que consisteix 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 $\mathbb{V}_K(\mathcal{I}_m) = \overline{F(K^m)}$.

Sabem que $F(K^m) = \pi_m(V_K)$, i pel lema 8.2 del capítol 3 és $\pi_m(V_K) \subseteq \mathbb{V}_K(\mathcal{I}_m)$. Sigui ara $W_K = \mathbb{V}(h_1, \ldots, h_s) \subseteq K^n$ una varietat qualsevol de K^n tal que $F(K^m) \subseteq W_K$. Hem de provar que $\mathbb{V}_K(\mathcal{I}_m) \subseteq W_K$.

Comencem per observar que per tot $\overline{x} \in W_K$ és $h_i(\overline{x}) = 0$ per tot i, i per tant també $h_i(\overline{x}) = 0$ per tot $\overline{x} \in F(K^m)$, doncs $F(K^m) \subseteq W_K$. Això prova que $h_i \circ F \in K[\bar{t}]$ s'anul.la a tot K^m. 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 vam 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, $W_{\overline{K}} = \mathbb{V}_{\overline{K}}(h_1, \ldots, h_s)$ és una varietat de $\overline{K}^n$ que conté $F(\overline{K}^m)$. Ara podem aplicar el teorema de la clausura 2.1 resultant que $\mathbb{V}_{\overline{K}}(\mathcal{I}_m) \subseteq W_{\overline{K}}$.

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

Algorisme. El teorema anterior té una aplicació pràctica evident. Donada una parametrització polinòmica definida per (3.1), (3.2), considerem l'ideal

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

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

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

Llavors $\mathbb{V}(\mathcal{I}_m)$ és la implicitació de la parametrització, o el que és equivalent, la clausura de Zariski dels punts parametritzats, i com sabem, pel teorema 12.4 del capítol 1, és una varietat irreductible.

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

Exemple 3.2. Sigui la parametrització següent:

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

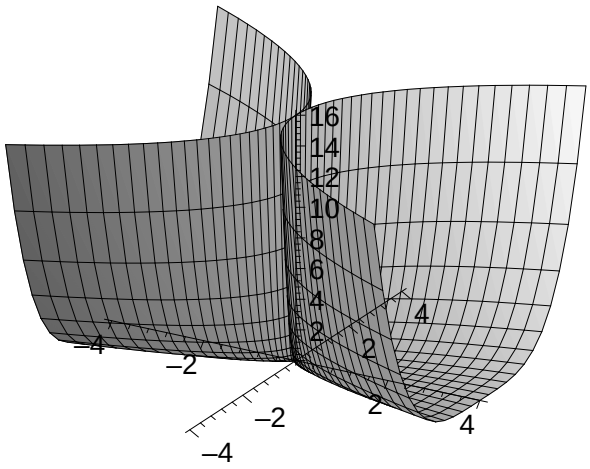
La base de Gröbner lex $G = \mathrm{gb}(\langle x + u^2, y - u\,v, z - v^4 \rangle, \mathrm{lex}(v, u, x, y, z))$ és:

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

Per tant, la varietat clausura de Zariski és

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

Fem un gràfic:



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 discussió 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 aïllar v. Per tant, hi ha un sol valor de v que correspon 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. En canvi, la branca de la varietat que correspon a punts positius de x està parametritzada per valors imaginaris de u i de v, i per tant no estén en $\mathbb{R}$. Posant $u \to Iu, v \to -Iv$, obtenim una parametrització real de l'altre branca real de la varietat: $x = u^2,\ y = u\,v,\ z = v^4$. Pel que fa a l'eix de les z, únicament estan parametritzats a $\mathbb{R}$ els que corresponen a $z \geq 0$, però de fet són els únics reals, ja que $zx^2 - y^4 = 0$.

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

$$x_1 = \frac{f_1(\bar{t})}{g_1(\bar{t})},\ \ldots,\ x_n = \frac{f_n(\bar{t})}{g_n(\bar{t})} \tag{3.3}$$

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:

$$F: \begin{array}{ccc} K^m \setminus W & \longrightarrow & K^n \\ \bar{t} & \mapsto & F(\bar{t}) \end{array} \tag{3.4}$$

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 3.3. 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 fàcil 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 parametrització.

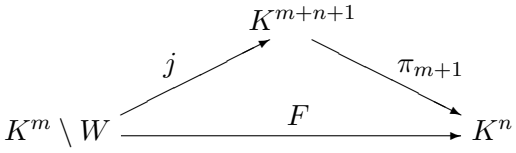
Podem aconseguir el propòsit introduint una nova variable y i un nou polinomi $g = (g_1 g_2 \cdots g_n)_{red}$ per definir l'ideal $J \subset K[y, \bar{t}, \overline{x}]$

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

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:

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

L'esquema de com actuen aquestes funcions és:



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

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

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

Provem la igualtat anterior.

$\subseteq$: Sigui $\bar{t} \in K^m \setminus W$. 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 $(y, \bar{t}, \overline{x}) \in V$, llavors $g \neq 0$, ja que en cas contrari no es verifica la darrera equació que defineix V. Per tant $t \in K^m \setminus W$ i les $\overline{x}$ de V estan determinades unívocament pels valors de $t \in K^m \setminus W$ ja que es poden aïllar totes les x_i en les equacions que defineixen V. Per tant $(y, \bar{t}, \overline{x}) \in j(K^m \setminus W)$ té anti-imatge única per j^{-1} a $K^m \setminus W$.

Tenint en compte aquesta igualtat resulta ara

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

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

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

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

Teorema 3.4 (Implicitació racional). *Sigui K un cos infinit, i sigui (3.3) una parametrització racional. Posem $g = g_1 \dots g_n$ i $W = \mathbb{V}(g)$. La parametrització estarà definida a $F : K^m \setminus W \longrightarrow K^n$. Sigui $\mathcal{J}$ l'ideal de $K[y, \bar{t}, \overline{x}]$, definit per $\mathcal{J} = \langle x_1 g_1(t) - f_1(\bar{t}), \dots, x_n g_n(t) - f_n(\bar{t}), 1 - g\, y \rangle$, i $\mathcal{J}_{m+1} = \mathcal{J} \cap K[\overline{x}]$ l'$(m+1)$-èsim ideal d'eliminació. Llavors la clausura de Zariski dels punts parametritzats és:*

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

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 $K^m \setminus W$ i cal justificar que els polinomis que s'anul.len a tot $K^m \setminus W$ s'anul.len idènticament. Ho deixem com exercici.

Algorisme. La utilització pràctica del teorema anterior és la següent. Donada una parametrització racional definida per (3.3), definim $g = g_1 \dots g_n$ i considerem l'ideal

$$\mathcal{J} = \langle g_1(\bar{t})x_1 - f_1(\bar{t}), \dots, g_n(\bar{t})x_n - f_n(\bar{t}), 1 - yg \rangle.$$

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

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

Llavors $\mathbb{V}(\mathcal{J}_{m+1})$ és la implicitació de la parametrització, o el que és equivalent, la clausura de Zariski 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 3.5. 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 $G = \mathrm{gb}(\mathcal{J}, \mathrm{lex}(w,t,x,y))$. 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 en que s'anul·len que és $P = (-1, 0)$, i comprovem que no estén, doncs substituint-lo en la segona equació dona $2 \neq 0$. Tots els demés punts estenen, i donat que fora de P alguna de les dues equacions lineals en t permet aïllar-la, el valor de t és únic. Això finalitza la discussió 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 tret de P 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.

4. Quocient d'ideals

Podem completar propietats del quocient d'ideals que vam definir en el capítol 1.

TEOREMA 4.1. *Siguin $\mathcal{I}$ i $\mathcal{J}$ ideals de $K[\overline{x}]$.*

(i) *Llavors*

$$\mathcal{I} : \mathcal{J} \subseteq \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})).$$

(ii) *A més, si K és algebraicament tancat, i $\mathcal{I}$ és radical, llavors:*

$$\mathcal{I} : \mathcal{J} = \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})).$$

DEMOSTRACIÓ.

(i) Sigui $f \in \mathcal{I} : \mathcal{J}$ i $\overline{x} \in \mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})$. Llavors, per tot $g \in \mathcal{J}$, és $fg \in \mathcal{I}$. Per tant, com $\overline{x} \in \mathbb{V}(\mathcal{I})$ és $f(\overline{x})g(\overline{x}) = 0$. Però com $\overline{x} \notin \mathbb{V}(\mathcal{J}))$, existeix algún $g \in \mathcal{J}$ tal que $g(\overline{x}) \neq 0$. Per tant, $f(\overline{x}) = 0$ per tot $\overline{x} \in \mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})$. Per tant, $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J}))$.

(ii) Suposem ara que K és algebraicament tancat i que $\mathcal{I} = \sqrt{\mathcal{I}} = \mathbb{I}(\mathbb{V}(\mathcal{I}))$. Hem de provar que $\mathcal{I} : \mathcal{J} \supseteq \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J}))$. Sigui $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J}))$. Per tot $\overline{x} \in \mathbb{V}(\mathcal{I})$ i $g \in \mathcal{J}$ és $fg(\overline{x}) = 0$, ja que si $\overline{x} \in \mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})$ és $f(\overline{x}) = 0$ i si $\overline{x} \in \mathbb{V}(\mathcal{J})$ és $g(\overline{x}) = 0$. Per tant,

$fg \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$. Així, doncs, pel Nullstellensatz i la hipòtesi de que $\mathcal{I}$ és radical $fg \in \sqrt{\mathcal{I}} = \mathcal{I}$. Però si per tot $g \in \mathcal{J}$ és $fg \in \mathcal{I}$, llavors $f \in \mathcal{I} : \mathcal{J}$, que és el que volíem provar.

□

COROL·LARI 4.2. *Siguin $\mathcal{I}$ i $\mathcal{J}$ ideals de $K[\overline{x}]$.*

(i) *Llavors*

$$\mathbb{V}(\mathcal{I} : \mathcal{J}) \supseteq \overline{\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})}.$$

(ii) *A més, si K és algebraicament tancat, i $\mathcal{I}$ és radical, llavors:*

$$\mathbb{V}(\mathcal{I} : \mathcal{J}) = \overline{\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})}.$$

DEMOSTRACIÓ. S'obtenen directament del teorema anterior, aplicant la inclusió inversa i el teorema de la clausura. □

Aquestes proposicions refinen una proposició del capítol 1.

EXEMPLE 4.3. Comprovem la fórmula (ii) del corol·lari 4.2, en un exemple concret. Siguin

$$\mathcal{I} = \langle x(x-y), x(x-z)\rangle\,, \quad \mathcal{J} = \left\langle (z-y)^2\, y\right\rangle.$$

L'ideal $\mathcal{I}$ donat és radical i podem considerar els polinomis a $\mathbb{C}[x,y,z]$, complint-se les hipòtesis del corol.lari. Tenim:

$$\begin{array}{lcl}
\mathbb{V}(\mathcal{I}) & = & \mathbb{V}(x) \cup \mathbb{V}(x-y, x-z), \\
\mathbb{V}(\mathcal{J}) & = & \mathbb{V}(y) \cup \mathbb{V}(z-y), \\
\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J}) & = & (\mathbb{V}(x) \setminus (\mathbb{V}(x,y) \cup \mathbb{V}(x, z-y))) \\
 & & \cup\, (\mathbb{V}(x-y, x-z) \setminus (\mathbb{V}(y, x-y, x-z) \cup \mathbb{V}(x-y, x-z, z-y))) \\
 & = & \mathbb{V}(x) \setminus (\mathbb{V}(x,y) \cup \mathbb{V}(x, z-y))
\end{array}$$

i per tant

$$\overline{\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})} = \mathbb{V}(x).$$

D'altra banda:

$$\begin{array}{l}
\mathrm{gb}([t\,\mathcal{I} + (1-t\,\mathcal{J}], \mathrm{lex}(t,x,y,z)) \cap \mathbb{C}[x,y,z] = [xy(y-z)^2] \\
\mathcal{I} \cap \mathcal{J} = \left\langle xy(y-z)^2 \right\rangle \\
\mathcal{I} : \mathcal{J} = \langle x \rangle
\end{array}$$

quedant comprovat aquí que

$$\overline{\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})} = \mathbb{V}(\mathcal{I} : \mathcal{J})$$

5. Saturació

Els resultats de la secció anterior poden refinar-se més emprant el concepte de saturació.

DEFINICIÓ 5.1. Donats dos ideals $\mathcal{I}, \mathcal{J} \subset K[\overline{x}]$ denominem saturació de $\mathcal{I}$ per $\mathcal{J}$, i el denotem per $\mathcal{I} : \mathcal{J}^{\infty}$, a l'ideal $\mathcal{I} : \mathcal{J}^N$ tal que $\mathcal{I} : \mathcal{J}^N = \mathcal{I} : \mathcal{J}^{N+1}$.

PROPOSICIÓ 5.2. *Donats dos ideals $\mathcal{I}, \mathcal{J} \subset K[\overline{x}]$, existeix sempre $N \in \mathbb{Z}$ tal que $\mathcal{I} : \mathcal{J}^\infty = \mathcal{I} : \mathcal{J}^N$.*

DEMOSTRACIÓ. La demostració es fonamenta en constatar que

$$\mathcal{I} : \mathcal{J} \subset \mathcal{I} : \mathcal{J}^2 \subset \cdots \subset \mathcal{I} : \mathcal{J}^n \subset \ldots$$

formen una cadena ascendent d'ideals que estaciona per la condició ACC de cadena ascendent d'ideals Noetherians. □

Ara podem refinar el teorema 4.1 de la secció anterior amb el següent:

TEOREMA 5.3. *Siguin $\mathcal{I}$ i $\mathcal{J}$ ideals de $K[\overline{x}]$.*

(i) *Llavors*

$$\mathcal{I} : \mathcal{J}^\infty \subseteq \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})).$$

(ii) *A més, si K és algebraicament tancat, i $\mathcal{I}$ és radical, llavors:*

$$\sqrt{\mathcal{I} : \mathcal{J}^\infty} = \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})).$$

DEMOSTRACIÓ.

(i) Sigui $f \in \mathcal{I} : \mathcal{J}^N$, amb N qualsevol i $\overline{x} \in \mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})$. Llavors, per tot $g \in \mathcal{J}^N$, és $fg \in \mathcal{I}$. Per tant, com $\overline{x} \in \mathbb{V}(\mathcal{I})$ és $f(\overline{x})g(\overline{x}) = 0$. Però com $\overline{x} \notin \mathbb{V}(\mathcal{J}))$, existeix algún $g \in \mathcal{J}^N$ tal que $g(\overline{x}) \neq 0$. Per tant, $f(\overline{x}) = 0$ per tot $\overline{x} \in \mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})$. Per tant, $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J}))$.

(ii) Suposem ara que K és algebraicament tancat. Hem de provar que $\mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})) \subseteq \sqrt{\mathcal{I} : \mathcal{J}^\infty}$. Sigui $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J}))$. Per tot $\overline{x} \in \mathbb{V}(\mathcal{I})$ i $g \in \mathcal{J}^N$ és $fg(\overline{x}) = 0$, ja que si $\overline{x} \in \mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})$ és $f(\overline{x}) = 0$ i si $\overline{x} \in \mathbb{V}(\mathcal{J})$ és $g(\overline{x}) = 0$. Per tant, $fg \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$. Així, doncs, pel Nullstellensatz existeix n tal que $f^n g^n \in \mathcal{I}$, on $g^n \in \mathcal{J}^{Nn}$. Per tant, per un M suficientment gran, per tot $g \in \mathcal{J}^M$ és $f^n \in \mathcal{I}$ i per tant $f \in \sqrt{\mathcal{I} : \mathcal{J}^M} = \sqrt{\mathcal{I} : \mathcal{J}^N}$ on N és l'exponent de saturació més petit.

□

COROL·LARI 5.4. *Siguin $\mathcal{I}$ i $\mathcal{J}$ ideals de $K[\overline{x}]$.*

(i) *Llavors*

$$\mathbb{V}(\mathcal{I} : \mathcal{J}^\infty) \supseteq \overline{\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})}.$$

(ii) *A més, si K és algebraicament tancat llavors:*

$$\mathbb{V}(\mathcal{I} : \mathcal{J}^\infty) = \overline{\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})}.$$

DEMOSTRACIÓ. S'obtenen directament del teorema anterior, aplicant la inclusió inversa i el teorema de la clausura. □

La darrera igualtat permet calcular la clausura de $\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})$ sense necessitat de calcular radicals.

EXEMPLE 5.5. Per comprovar i veure la fórmula en acció, considerem $\mathcal{I} = \langle x^3y^5 \rangle$ i $\mathcal{J} = \langle y \rangle$. Tindrem $\mathbb{V}(\mathcal{I}) = \mathbb{V}(xy) = \mathbb{V}(x) \cup \mathbb{V}(y)$ i $\mathbb{V}(\mathcal{J}) = \mathbb{V}(y)$. Per tant $\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J}) = \mathbb{V}(x) \setminus \mathbb{V}(x, y)$, i fent la clausura $\overline{\mathbb{V}(\mathcal{I}) \setminus \mathbb{V}(\mathcal{J})} = \mathbb{V}(x)$. Calculem ara

$$\mathcal{I} : \mathcal{J} \subseteq \mathcal{I} : \mathcal{J}^2 \subseteq \mathcal{I} : \mathcal{J}^3 \subseteq \mathcal{I} : \mathcal{J}^4 \subseteq \mathcal{I} : \mathcal{J}^5 \subseteq \mathcal{I} : \mathcal{J}^6$$

Tenim:

$$\langle x^3y^4 \rangle \subseteq \langle x^3y^3 \rangle \subseteq \langle x^3y^2 \rangle \subseteq \langle x^3y \rangle \subseteq \langle x^3 \rangle \subseteq \langle x^3 \rangle$$

que ja estabilitza, i per tant $N = 5$. Resulta doncs $\mathcal{I} : \mathcal{J}^\infty = \langle x^3 \rangle$, d'on $\mathbb{V}(\mathcal{I} : \mathcal{J}^\infty) = \mathbb{V}(x)$ com era d'esperar.

6. Exercicis

Secció 1.

EXERCICI 4.1. .

a) Proveu que si K és algebraicament tancat, i $\mathcal{I}$ és un ideal primer de $K[\overline{x}]$, llavors $\mathcal{I} = \mathbb{IV}(\mathcal{I})$ i $\mathbb{V}(\mathcal{I})$ és irreductible.
b) Doneu un exemple amb un cos K que no sigui algebraicament tancat i no sigui certa la igualtat anterior.

EXERCICI 4.2. Donats dos ideals $\mathcal{I}$, $\mathcal{J}$ de $K[\overline{x}]$, diem que són comaximals si i sols si $\mathcal{I} + \mathcal{J} = \langle 1 \rangle = K[\overline{x}]$.

a) Proveu que si K és algebraicament tancat, llavors $\mathcal{I}$ i $\mathcal{J}$ són comaximals ssi $\mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J}) = \phi$. Doneu un exemple que mostri que això no és cert en general.
b) Proveu que si $\mathcal{I}$ i $\mathcal{J}$ són comaximals, llavors $\mathcal{I} \cdot \mathcal{J} = \mathcal{I} \cap \mathcal{J}$.
c) És cert el recíproc de b)? Doneu una demostració o un contreexemple.
d) Si $\mathcal{I}$ i $\mathcal{J}$ són comaximals, proveu que $\mathcal{I}$ i $\mathcal{J}^2$ també ho són. De fet, proveu que $\mathcal{I}^r$ i $\mathcal{J}^s$ són comaximals per qualssevulla enters r, s positius.
e) Siguin $\mathcal{I}_1, \ldots, \mathcal{I}_r$ ideals de $K[\overline{x}]$ i suposem que $\mathcal{I}_i$ i $\mathcal{J}_i = \cap_{j \neq i} \mathcal{I}_j$ són comaximals per cada i. Proveu que

$$\mathcal{I}_1^m \cap \cdots \cap \mathcal{I}_r^m = (\mathcal{I}_1 \cdots \mathcal{I}_r)^m = (\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_r)^m$$

EXERCICI 4.3. Sigui $\mathcal{I}$ un ideal de $K[\overline{x}]$ on K és un cos algebraicament tancat. Direm que $\mathcal{I}$ és un ideal zero-dimensional ssi $V = \mathbb{V}(\mathcal{I})$ consta d'un nombre finit no nul de punts:

$$V = \{P_1, \ldots, P_s\}$$

a) Utilitzant el Nullstellensatz, proveu que si $\mathcal{I}$ és zero-dimensional llavors tota base de Gröbner $G = \mathrm{gb}(\mathcal{I}, \succ)$ per un ordre monomial $\succ$ qualsevol conté algún polinomi g_i que té monomi principal $\mathrm{lm}(g_i) = x_i^{M_i}$ per cada variable x_i, on $M_i > 0$.
b) Proveu el recíproc si afegim la hipòtesi de que l'ordre monomial és $\mathrm{lex}(x_1, \ldots, x_n)$.
c) Proveu el recíproc per a qualsevol ordre monomial.
d) Proveu que $\mathcal{I}$ és zero-dimensional també és equivalent a que per cada variable x_i és $\mathcal{I} \cap K[x_i] = \langle g_i \rangle$, on $\deg(g_i) > 0$.
e) Donat l'ideal zero-dimensional

$$\mathcal{I} = \langle x^2(y^4 - 2y^3 - x + 1), y^2(x^3 + y^2 - 2y + 1), x^2y^2 \rangle$$

(1) Determineu $\mathcal{I}_x = \mathcal{I} \cap K[x]$ i $\mathcal{I}_y = \mathcal{I} \cap K[y]$.
(2) Determineu $\mathbb{I}(\mathbb{V}(\mathcal{I}))$.

Secció 3.

EXERCICI 4.4. Considerem $V \subset K^3$ la varietat definida per la parametrització

$$\begin{array}{rccc} F: & K^2 & \to & K^3 \\ & (u,v) & \mapsto & (uv, u^2, v^2). \end{array}$$

a) Trobeu un polinomi $f \in \mathbb{Z}[x,y,z]$ homogeni de grau 2 tal que $f \in \mathbb{I}(V)$ (independentment de K).
b) Proveu que si K és infinit llavors $V = \mathbb{V}(f)$ i $\mathbb{I}(V) = \langle f \rangle$ (*Indicació: Per tal de demostrar que $g \in \mathbb{I}(V)$ implica que $g \in \langle f \rangle$ utilitzeu la divisió en un ordre monomial adequat i el fet que si un polinomi en dos variables s'anul·la en $S \times S$, amb $S \subset K$ infinit llavors ha de ser el polinomi zero*).
c) Proveu que F cobreix tota V en el cas $K = \mathbb{C}$ pero no si K és $\mathbb{Q}$ o $\mathbb{R}$.
d) En el cas en que $K = \mathbb{F}_2$, determineu V i $\mathbb{I}(V)$.

Considerem ara la varietat W definida per la parametrització F' següent:

$$\begin{array}{rccc} F' & : K^2 & \to & K^3 \\ & (u,v) & \mapsto & (uv^2, uv, uv^3). \end{array}$$

e) Demostreu que si K és infinit, $W = V$, la varietat de l'apartat b). (*Indicació: feu un raonament anàleg al de l'apartat b*).
f) Demostreu que ara F' no cobreix W ni en $\mathbb{Q}$ ni en $\mathbb{R}$ ni en $\mathbb{C}$.
g) Si $K = \mathbb{F}_2$, calculeu la varietat W i el seu ideal de varietat $\mathbb{I}(W)$.
h) Finalment, utilitzeu ara l'algorisme d'implicitació emprant *Maple* per trobar les varietats definides per cada una de les dues parametritzacions, i discutiu els resultats anteriors a la llum del teorema de l'extensió, comparant resultats.

EXERCICI 4.5. Proveu que si K és un cos algebraicament tancat i $p(\overline{x}) \in K[\overline{x}]$ és irreductible sobre K, llavors $\mathbb{V}(p)$ és una varietat irreductible.

EXERCICI 4.6. Sigui $I = \langle z^3 - x^5, y^3 - x^2 \rangle \subset K[x,y,z]$ i $V = \mathbb{V}(I)$.

a) Sigui $K = \mathbb{C}$. Demostreu que V té tres components irreductibles V_1, V_2, V_3 i que els seus ideals de varietat són respectivament:

$$\begin{aligned} I_1 &= \langle z - xy, y^3 - x^2 \rangle \\ I_2 &= \langle z - \xi_2 xy, y^3 - x^2 \rangle \\ I_3 &= \langle z - \xi_3 xy, y^3 - x^2 \rangle \end{aligned}$$

on $1, \xi_2, \xi_3$ són les tres arrels cúbiques de la unitat. (Indicació: *Empreu parametritzacions i ordres monomials adients*).

b) Proveu que

$$I_1 \cap I_2 \cap I_3 =$$
$$\langle t_1(z - xy), t_2(z - \xi_2 xy), (1 - t_1 - t_2)(z - \xi_3 xy), y^3 - x^2 \rangle \cap \mathbb{C}[x,y,z].$$

Computada la base de Gröbner de l'ideal anterior emprant ordre $\text{lex}(z, y, x)$ s'obté $\langle z^3 - x^5, y^3 - x^2\rangle$. Deduïu que $I = \mathbb{I}(V)$.

c) Sigui $K = \mathbb{Q}$. Proveu que ara V és irreductible i determineu el seu ideal de varietat.

Secció 4.

EXERCICI 4.7. A $\mathbb{R}^2$ siguin

$$V = \{(i, j) \in \mathbb{Z}^2 \ : \ 0 \leq i \leq n, 0 \leq j \leq m\}, \quad V_1 = \{(0, 0)\},$$
$$W = V \setminus V_1.$$

a) Doneu una base de $\mathbb{I}(W)$ i proveu que ho és. És una base de Gröbner per algún ordre? Tant si us en sortiu com si no passeu a l'apartat següent. Aquest apartat podeu resoldre-ho en d).

b) Per n, m fixats, indiqueu tots els passos que calen per determinar $\mathbb{I}(W)$ de forma algorísmica.

c) Procediu segons l'apartat b) i determineu $\mathbb{I}(W)$. Doneu tots els resultats intermedis. Donat que n, m són qualsevulla, els algorismes no funcionen de forma automàtica, però no resulta difícil preveure els resultats.

d) Si no ho heu fet en a), proveu ara que la base obtinguda en c) és realment base de $\mathbb{I}(W)$, i comenteu si és base de Gröbner o no.

Nota: No cal que proveu els resultats intermedis en l'apartat c). N'hi ha prou en que els plantegeu i els doneu. Concreteu únicament la prova del resultat final (apartat a) o d)).