UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

μ-BASES DE CORBES RACIONALS PLANES

Autora: Berta Moner i Farran

Directora: Dra. Maria Eulalia Montoro Lopez
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 12 de juny de 2023

Abstract

In this work, the μ-bases of plane rational curves are shown from the point of view of algebraic geometry and algebraic varieties. Thus, the Gröbner bases are previously presented, which are of great importance in this area but more expensive than the μ-bases. Based on the definition and construction of the latter, two applications are shown: modules and implication, both polynomial and rational. The work is based on the article *The moving line ideal basis of planar rational curves* from Cox, D.A, Sederberg, T.W., Chen, F. published on 1998 by Computer Aided Geometry Design 15.

Resum

En el present treball es mostren les μ-bases de les corbes racionals planes des del punt de vista de la geometria algebraica i les varietats algebraiques. Així, prèviament es presenten les bases de Gröbner, de gran importància en aquest àmbit però més costoses que les μ-bases. A partir de la definició i la construcció d'aquestes darreres, se'n mostren dues aplicacions: els mòduls i la implicitació, tant polinòmica com racional. El treball es basa en l'article *The moving line ideal basis of planar rational curves* de Cox, D.A, Sederberg, T.W., Chen, F. publicat l'any 1998 per Computer Aided Geometry Design 15.

2020 Mathematics Subject Classification. 11G05, 11G10, 14G10

a tota la meva família,
i sobretot a la meva mare

Índex

Introducció

Des del darrer segle, la geometria algebraica ha esdevingut l'eix central de molts estudis matemàtics. Tot i que Niels Henrik Abel (1802-1829), Bernhard Riemann (1826-1866) i Karl Weierstrass (1815-1897), entre d'altres matemàtics, havien presentat nombrosos resultats durant el segle XIX, no va ser a finals d'aquell segle i principis del segle XX que la mentalitat envers aquest camp de les matemàtiques va canviar per complet. La geometria algebraica va desenvolupar-se a partir d'aquest moment en un marc algebraic abstracte, posant al centre les propietats intrínseques de les varietats algebraiques que no depenen de cap espai de coordenades ambient.

La teoria dels ideals va ser presentada pel matemàtic alemany Richard Dedekind (1831-1916) al seu llibre *Vorlesungen über Zahlentheorie* "Lliçons sobre la teoria de nombres". Aquest concepte era una generalització del nombre ideal que havia desenvolupat Ernst Kummer (1810-1893). Posteriorment David Hilbert (1862-1943) i Emmy Noether (1882-1935) van estendre la noció més enllà dels anells numèrics desenvolupant els anells de polinomis, entre d'altres anells commutatius.

A partir d'aquí, va esdevenir una eina fonamental a l'hora d'estudiar corbes i superfícies.

Per a comprendre aquests ideals, sovint es recorre a generadors alternatius, com ara les bases de Gröbner. Donat un ideal d'un anell de polinomis, una base de Gröbner d'aquest ideal consisteix en un conjunt de polinomis que el generen, i que a més estenen l'algoritme de la divisió d'Euclides en el cas multivariant mantenint la unicitat del residu, com a exemple d'alguna de les moltes propietats addicionals que tenen. Gràcies a aquestes bases, es podrà resoldre qualsevol sistema d'equacions polinòmiques.

Les formes paramètrica i implícita son dues representacions bàsiques per a les corbes i superfícies. Com a conseqüència dels seus pros i contres, algunes, com les corbes i superfícies de Bézier solen representar-se de forma paramètrica, mentre que d'altres, com les esferes es representen habitualment de forma implícita.

El problema d'implicitació per a corbes i superfícies racionals s'ha explorat al llarg de la història i son diversos els mètodes que s'han utilitzat per a resoldre'l. En aquest sentit, per exemple, els mètodes basats en les resultats han estat utilitzats en modelització geomètrica, però, en general, no son vàlids quan tenim punts base. També les bases de Gröbner han estat utilitzades tot i la presència de punts base, tot i que el procés per a calcular-les sovint és molt costós. Alternativament a aquests i d'altres mètodes hi ha el mètode de les línies mòbils, proposat per Sederberg i Chen a mitjans de la dècada dels 90.

Les μ-bases generalitzen les bases de Gröbner i son una nova representació per a les corbes i seran essencials perquè serveixen com a pont entre la parametritació i la implicitació d'una corba. Geomètricament, venen representades per línies o plans en

moviment com les que es mostren a continuació:

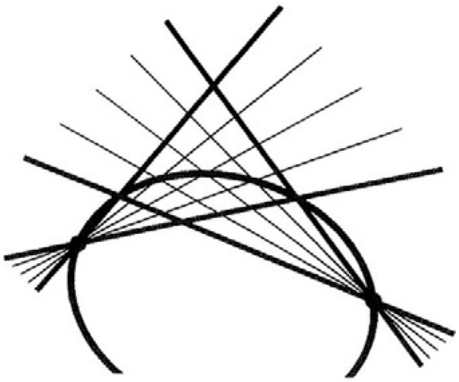

Figura 1: [7] Dues famílies de línies mòbils que segueixen una corba plana racional.

El present treball s'organitza en tres capítols.

Al primer capítol, Preliminars, es presenta la definició i algunes propietats bàsiques de les varietats algebraiques; la teoria basada en ideals; les bases de Gröbner amb el Lema de Dickson i el Teorema de la base de Hilbert com a resultats centrals; la relació d'aquests conceptes amb la teoria d'eliminació mitjançant els teoremes d'eliminació i extensió; i la teoria de mòduls, amb els mòduls lliures com a exemple central.

Al segon capítol, μ-Classificació de corbes planes, es presenta la definició i les propietats de les μ-bases de les corbes planes algebraiques; els mòduls de syzigies; i la determinació de l'estructura del conjunt $\mathcal{P}_n^\mu$ de parametritzacions amb classe μ.

Al tercer capítol, Implicitació, s'estudiarà el problema d'implicitació a partir dels casos de la implicitació polinòmica i la implicitació racional. Aquest darrer cas es relacionarà amb la matriu de Sylvester i les resultants.

Capítol 0

Notació

Abans de començar, establim algunes notacions i terminologia que utilitzarem al llarg del treball.

- Sigui $\mathbb{A}$ un anell qualsevol.
- Sigui $\mathbb{K}$ un cos qualsevol.
- Denotarem per $\mathbb{K}[t]$ l'anell de polinomis en t amb coeficients al cos $\mathbb{K}$.
- Denotarem per $\mathbb{K}[x_1, \ldots, x_n]$ l'anell de polinomis en $x_1, \ldots, x_n$ sobre un cos $\mathbb{K}$.
- Donat $P(t) \in \mathbb{K}[t]$, denotarem per $\deg(P)$ el seu grau.
- Denotarem per $\mathbb{K}[t]_n$ l'espai vectorial de tots els polinomis $P(t)$ amb $\deg(P(t)) \leq n$.
- Donats $p, q \in \mathbb{K}[t]$, denotarem per $mcd(p, q)$ el màxim comú divisor entre p i q.
- Donats $p, q \in \mathbb{K}[t]$, denotarem per $mcm(p, q)$ el mínim comú múltiple entre p i q.
- Denotarem per $\mathcal{P}_n \subset \mathbb{K}[t]_n^3$ el subconjunt de triplets $(a, b, c) \in \mathbb{K}[t]_n^3$, que son relativament primers, i definim $n = max(n_a, n_b, n_c)$ amb $c \neq 0$. Aleshores, $\mathcal{P}_n$ és un espai de totes les parametritzacions racionals de grau n.
- Denotarem per $\amalg$ la unió disjunta entre dos o més conjunts.

Capítol 1

Preliminars

1.1 Varietats algebraiques

Les varietats algebraiques, que es defineixen des del punt de vista clàssic com el conjunt de punts en els quals un conjunt arbitrari de polinomis s'anul·la, son un objecte central d'estudi en la geometria algebraica.

Posteriorment s'han donat altres definicions per a aquests conjunts, preservant sempre la intuició geomètrica que hi ha darrere aquest concepte.

Definició 1.1.1. [2] *Sigui* $\mathbb{K}$ *un cos, i siguin* $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. *Aleshores la varietat afí definida per* $f_1, \ldots, f_s$ *ve donada per*

$$\mathbb{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n | f_i(a_1, \ldots, a_n) = 0 \ \forall 1 \leq i \leq s\}.$$

És a dir, $\mathbb{V}$ *associa a cada subconjunt de polinomis els punts de l'espai afí en el que tots els polinomis del subconjunt s'anul·len.*

Exemple 1.1.2. [2] Donat un cos $\mathbb{K}$, les solucions d'un sistema de m equacions lineals amb n incògnites $x_1, \ldots, x_n$ amb coeficients a $\mathbb{K}$

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n &= b_1, \\ &\vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n &= b_m. \end{aligned} \tag{1.1.1}$$

formen una varietat afí de $\mathbb{K}^n$ anomenada *varietat lineal.*

Lema 1.1.3. [2] *Si* $V, W \subseteq \mathbb{K}^n$ *son varietats afins, amb* $V = \mathbb{V}(f_1, \ldots, f_s), W = \mathbb{V}(g_1, \ldots, g_t)$ *aleshores* $V \cup W$ *i* $V \cap W$ *també ho son.*

Demostració.

$\boxed{V \cap W}$ $(c_1, \ldots, c_n) \in V \cap W$ si, i només si

$$\begin{aligned} f_i(c_1, \ldots, c_n) = 0 \quad \forall 1 \leq i \leq n, \\ g_j(c_1, \ldots, c_n) = 0 \quad \forall 1 \leq j \leq n. \end{aligned}$$

d'on

$$V \cap W = \mathbb{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$$

$\boxed{V \cup W}$

$\boxed{\subseteq}$ Sigui $(a_1, \ldots, a_n) \in V$, aleshores

$$f_i(a_1, \ldots, a_n) = 0 \quad \forall 1 \leq i \leq s$$

d'on també

$$f_i(a_1, \ldots, a_n) g_j(a_1, \ldots, a_n) = 0 \quad \forall 1 \leq i \leq s, \quad \forall 1 \leq j \leq t.$$

D'aquí tenim que $V \subseteq \mathbb{V}(f_i g_j)$ i, anàlogament, $W \subseteq \mathbb{V}(f_i g_j)$.

Per tant,

$$V \cup W \subseteq \mathbb{V}(f_i g_j |\ 1 \leq i \leq s,\ 1 \leq j \leq t)$$

$\boxed{\supseteq}$ Sigui $(a_1, \ldots, a_n) \in \mathbb{V}(f_i g_j)$. Si $(a_1, \ldots, a_n) \in V$, hem acabat. Sinó, sigui i_0 tal que

$$f_{i_0}(a_1, \ldots, a_n) \neq 0$$

Com que

$$f_{i_0} g_j(a_1, \ldots, a_n) = 0 \quad \forall 1 \leq j \leq t$$

aleshores

$$g_j(a_1, \ldots, a_n) = 0 \quad 1 \leq j \leq t$$

i per tant,

$$(a_1, \ldots, a_n) \in W \subseteq V \cap W$$

Obtenim, doncs, la igualtat

$$V \cup W = \mathbb{V}(f_i g_j |\ 1 \leq i \leq s,\ 1 \leq j \leq t).$$

□

Com a conseqüència, tenim que la unió finita de varietats afins és una varietat afí, així com la intersecció finita de varietats afins.

Exemple 1.1.4. Sigui $\mathbb{K} = \mathbb{R}$ un cos. Considerem el sistema d'equacions

$$\left.\begin{aligned} x + y + z = 1 \\ x + 2y - z = 3 \end{aligned}\right\} \tag{1.1.2}$$

Geomètricament, la solució és una recta a $\mathbb{R}^3$. Si prenem $z = t$, les solucions de (1.1.2) son

$$\begin{aligned} x &= -1 - 3t, \\ y &= 2 + 2t, \\ z &= t \end{aligned} \tag{1.1.3}$$

Exemple 1.1.5. Sigui l'equació paramètrica que descriu una corba al pla:

$$\left.\begin{aligned} x &= 1 + t \\ y &= 1 + t^2 \end{aligned}\right\} \tag{1.1.4}$$

$$\begin{gathered} x = 1 + t \to t = x - 1 \\ y = 1 + t^2 = 1 + (x-1)^2 = x^2 - 2x + 2 \to y - x^2 + 2x - 2 = 0 \end{gathered}$$

d'on obtenim que (1.1.4) descriu la varietat afí $\mathbb{V}(y - x^2 + 2x - 2)$.

Definició 1.1.6. *Sigui $V \in \mathbb{K}^n$ una varietat algebraica. Direm que V és reductible si existeixen $V_1, V_2 \in V$ propis tals que*

$$V = V_1 \cup V_2$$

en cas contrari, direm que és irreductible.

1.2 Ideals

Donat un anell $\mathbb{A}$, denotarem per I un subconjunt d'elements de $\mathbb{A}$ tancat respecte a operacions lineals i amb una sèrie de condicions. Es defineixen ideals per la dreta i per l'esquerra, però els ideals commutatius (ideals per ambdues bandes) seran els del nostre interès.

Recordem, en primer lloc, la seva definició:

Definició 1.2.1. *Un subconjunt $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ és un ideal si*

(i) $0 \in I$.

(ii) Si $f, g \in I$, aleshores $f + g \in I$.

(iii) Si $f \in I$ i $h \in \mathbb{K}[x_1, \ldots, x_n]$, aleshores $hf \in I$.

Definició 1.2.2. [2] *Siguin $f_i \in \mathbb{K}[x_1, \ldots, x_n]$, $1 \leq i \leq s$. Definim per*

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n] \right\}$$

l'ideal generat per $f_1, \ldots, f_s$.

Definició 1.2.3. [2] *Sigui $V \subseteq \mathbb{K}^n$ una varietat afí. L'ideal de V ve donat per*

$$I(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in V\}$$

És a dir, I associa a cada subconjunt de punts de l'espai afí l'ideal de tots els polinomis que s'anul·len en aquests punts.

Il·lustrem aquestes definicions amb els següents dos exemples:

Exemple 1.2.4. [2] Sigui $V = \{(0,0)\}$. Volem veure que l'ideal de l'origen és

$$I(\{(0,0)\}) = \langle x, y \rangle$$

$\boxed{\supseteq}$ L'ideal generat per x, y és

$$\langle x, y \rangle = A(x,y)x + B(x,y)y$$

amb $A(x,y), B(x,y) \in \mathbb{K}[x,y]$ i $(0,0)$ s'anul·la per a tot A, B. Per tant,

$$I(\{(0,0)\}) \supseteq \langle x, y \rangle$$

$\boxed{\subseteq}$ Sigui $f \in I(\{(0,0)\})$ de la forma $f = \sum_{i,j} a_{ij} x^i y^j$ i, per tant, $f(0,0) = a_{00} = 0$. Aleshores

$$f = \sum_{i,j} a_{ij} x^i y^j = a_{00} + \sum_{i>0, j>0} a_{ij} x^i y^j = 0 + \sum_{i>0, j} a_{ij} x^i y^j + \sum_{i=0, j>0} a_{ij} x^i y^j = \left(\sum_{i>0, j} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \in \langle x, y \rangle$$

d'on

$$I(\{(0,0)\}) \subseteq \langle x, y \rangle$$

I per tant es compleix la igualtat.

Lema 1.2.5. [2] *Sigui $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Aleshores $\langle f_1, \ldots, f_s \rangle \subseteq I(\mathbb{V}(f_1, \ldots, f_s))$.*

Demostració. Sigui $f \in \langle f_1, \ldots, f_s \rangle$. Per la Definició 1.2.2,

$$f = \sum_{i=1}^{s} h_i f_i, \qquad h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n].$$

Com que $f_1, \ldots, f_s$ s'anul·len en $\mathbb{V}(f_1, \ldots, f_s)$, aleshores f també. Per la Definició 1.2.3, $f \in I(\mathbb{V}(f_1, \ldots, f_s))$.

Veiem ara que la igualtat no sempre es compleix a través d'un contraexemple.

Sigui $f_1 = x^2, f_2 = y^2$ i veurem que

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

Tenim que

$$I(\mathbb{V}(x^2, y^2)) \underset{\substack{\downarrow \\ x^2=0,\ y^2=0}}{=} I(\{(0,0)\}) \underset{\substack{\downarrow \\ Exemple\ 1.2.4}}{=} \langle x, y\rangle \underset{\substack{\downarrow \\ x\notin\langle x^2,y^2\rangle}}{\supsetneq} \langle x^2, y^2\rangle$$

Per tant,

$$\langle f_1, \ldots, f_s\rangle \subsetneq I(\mathbb{V}(f_1, \ldots, f_s)).$$

□

Recordem ara la definició d'ideal primer i veiem-ne un exemple.

Definició 1.2.6. [8] *Un ideal I d'un anell $\mathbb{A}$ es diu ideal primer si $I \neq \mathbb{A}$, $I \neq \emptyset$ i, per a $a, b \in \mathbb{A}$, es compleix*

$$ab \in I \Rightarrow a \in I \ o \ b \in I$$

Exemple 1.2.7. Si $\mathbb{A} = \mathbb{C}[x, y]$ és l'anell de polinomis amb coeficients complexes, aleshores l'ideal $I = \langle y^2 - x^3 - x - 1\rangle$ és un ideal primer.

1.3 Bases de Gröbner

Les bases de Gröbner reben aquest nom pel matemàtic austríac Wolfgang Gröbner (1899-1980). L'any 1964, Gröbner, en un seminari amb els seus alumnes de doctorat, va proposar a Bruno Buchberger (1942-) de resoldre el problema de càlcul d'una $\mathbb{K}$-base d'un ideal I en $\mathbb{K}[x_1, \ldots, x_n]$. Conjuntament van desenvolupar un algoritme que era vàlid per a tot ideal I. Va ser a partir del poc ressò que va tenir aquest resultat que Buchberger va encunyar el terme de base de Gröbner que coneixem avui en dia.

Notem, en primer lloc, que tot monomi pot es pot escriure com

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

amb $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.

A més a més, l'anell de polinomis $\mathbb{K}[x_1, \ldots, x_n]$ és un $\mathbb{K}$- espai vectorial i el conjunt de monomis mònics $\mathcal{M}(x_1, \ldots, x_n) = \{x^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0}\}$ és la base canònica.

Com a conseqüència de la correspondència bijectiva

$$x^* : \mathbb{Z}^n_{\geq 0} \to \mathcal{M}(x_1, \ldots, x_n) \subset \mathbb{K}[x_1, \ldots, x_n]$$

tenim que donar un ordre al conjunt $\mathcal{M}(x_1, \ldots, x_n)$ és equivalent a donar un ordre del conjunt d'exponents a $\mathbb{Z}^n_{\geq 0}$.

Tenim que, per a tot parell de monomis x^α, x^β, l'ordre definit té les següents propietats:

- Propietat transitiva: $x^\alpha > x^\beta \ i \ x^\beta > x^\gamma \quad \Rightarrow \quad x^\alpha > x^\gamma$

- Propietat de totalitat: $x^\alpha > x^\beta \quad o \quad x^\alpha = x^\beta \quad o \quad x^\alpha < x^\beta$

A més a més, donat un monomi x^γ, tots els ordres monomials han de tenir la propietat següent referent al producte entre dos monomis:

$$x^\alpha > x^\beta \quad \Rightarrow \quad x^\alpha x^\gamma > x^\beta x^\gamma$$

Definició 1.3.1. [2] *L'ordre monomial $>$ en $\mathbb{K}[x_1, \ldots, x_n]$ és una relació en el conjunt de monomis $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$ tal que*

(i) $>$ és un ordre total en $\mathbb{Z}^n_{\geq 0}$.

(ii) Si $\alpha > \beta$ i $\gamma \in \mathbb{Z}^n_{\geq 0}$, aleshores $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ està ben ordenada en $\mathbb{Z}^n_{\geq 0}$; és a dir, per tot subconjunt $A \subset \mathbb{Z}^n_{\geq 0}$ no buit existeix $\alpha_0 \in A$ tal que $\alpha > \alpha_0$ $\forall \alpha \neq \alpha_0 \in A$.

Donat l'ordre monomial $>$, diem que $\alpha \geq \beta$ si $\alpha > \beta$ o $\alpha = \beta$.

Lema 1.3.2. [2] *Una relació d'ordre $>$ en $\mathbb{Z}^n_{\geq 0}$ està ben ordenada si, i només si, tota seqüència decreixent en $\mathbb{Z}^n_{\geq 0}$*

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots$$

és finita.

Demostració. Ho provarem per contrarecíproc. Veurem que la relació $>$ no està ben ordenada si, i només si, existeix una seqüència infinita decreixent en $\mathbb{Z}^n_{\geq 0}$.

$\boxed{\Rightarrow}$ Si $>$ no està ben ordenada, existeix un subconjunt $S \subseteq \mathbb{Z}^n_{\geq 0}$, $S \neq \emptyset$ sense element minimal. Prenem $\alpha(1) \in S$. Com que $\alpha(1)$ no és l'element minimal, existeix $\alpha(2) < \alpha(1)$ en S. Obtenim la seqüència infinita decreixent

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots$$

$\boxed{\Leftarrow}$ Donada una seqüència infinita

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots$$

aleshores, $\{\alpha(1), \alpha(2), \alpha(3), \ldots\} \subset \mathbb{Z}^n_{\geq 0}$ no buit i sense un element minimal, per tant, la relació $>$ no està ben ordenada. □

Definim ara dos ordres monomials que seran necessaris per a la definició de les bases de Gröbner.

Definició 1.3.3 (Ordre lexicogràfic)**.** [2] *Siguin $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ i $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Direm que $\alpha >_{lex} \gamma$ si el primer valor diferent de zero de la diferència $\alpha - \beta \in \mathbb{Z}^n$ és positiu. En tal cas escriurem*

$$x^\alpha >_{lex} x^\gamma$$

Veiem, per tant, que hi ha una variable que domina a tots els monomis que no continguin aquesta variable. Per exemple,

$$x >_{lex} y >_{lex} z \;\Rightarrow\; x >_{lex} y^4 z^7$$

Definició 1.3.4 (Ordre lexicogràfic graduat)**.** *Siguin* $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ *i* $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$ *amb*

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

Direm que $\alpha >_{grlex} \gamma$ *si*

$$|\alpha| > |\beta| \quad o \quad |\alpha| = |\beta| \text{ i } |\alpha| >_{lex} |\beta|$$

Exemple 1.3.5. Donat

$$f = 7x^2y^2z + 3z^4 - 5x^3 + 2x^2yz^2 \in \mathbb{K}[x, y, z]$$

els seus monomis queden ordenats de la següent manera en funció de l'ordre monomial utilitzat:

- $>_{lex}$: $f = -5x^3 + 7x^2y^2z + 2x^2yz^2 + 3z^4$
- $>_{grlex}$: $f = 7x^2y^2z + 2x^2yz^2 + 3z^4 - 5x^3$

Donat un ordre monomial, donem la definició d'alguns elements principals d'un polinomi f.

Definició 1.3.6. *Sigui* $f = \sum_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ *i sigui* $>$ *un ordre monomial.*

- *El multigrau de* f *és*

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

- *El coeficient líder de* f *és*

$$LC(f) := a_{multideg(f)} \in \mathbb{K}$$

- *El monomi líder de* f *és*

$$LM(f) := x^{multideg(f)}$$

- *El terme líder de* f *és*

$$LT(f) := LC(f)LM(f) = a_{multideg(f)} x^{multideg(f)}$$

Exemple 1.3.7. Prenent el mateix polinomi que a l'Exemple 1.3.5, els elements principals del polinomi son els següents en funció de l'ordre monomial utilitzat:

- $>_{lex}$: $LC(f) = -5,\ LM(f) = x^3,\ LT(f) = -5x^3$
- $>_{grlex}$: $LC(f) = 7, LM(f) = x^2y^2z, LT(f) = 7x^2y^2z$

De forma anàloga al cas d'una variable podem descriure la divisió per a polinomis en diverses variables de la següent manera:

Teorema 1.3.8. (Algoritme de divisió a $\mathbb{K}[x_1, \ldots, x_n]$). [2] *Sigui $>$ un ordre monomial en $\mathbb{Z}^n_{\geq 0}$ i sigui $F = (f_1, \ldots, f_s) \in \mathbb{K}[x_1, \ldots, x_n]$ un conjunt ordenat. Aleshores, tot $f \in \mathbb{K}[x_1, \ldots, x_n]$ es pot escriure com*

$$f = q_1 f_1 + \ldots + q_s f_s + r$$

amb $q_i, r \in \mathbb{K}[x_1, \ldots, x_n]$ i $r = 0$ o r és combinació lineal de monomis amb coeficients a $\mathbb{K}$, no divisibles per $LT(f_1), \ldots, LT(f_s)$.

Observació 1.3.9. Aquest algoritme no preserva alguna de les bones propietats de l'algoritme de divisió per a polinomis en una variable, com per exemple la unicitat del residu. Aquest fet és rellevant i veurem que si al dividir f per $F = (f_1, \ldots, f_s) \in \mathbb{K}[x_1, \ldots, x_n]$ tenim $r = 0$, aleshores $f \in \langle f_1, \ldots, f_s \rangle$, però en cas contrari, no podrem afirmar que $f \notin \langle f_1, \ldots, f_s \rangle$

Els ideals formats només per monomis tenen un paper clau en la construcció i caracterització de les bases de Gröbner. Veiem-ne la definició i una caracterització.

Definició 1.3.10. *Un ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ és un ideal monomial si existeix un sistema de generadors format per monomis, o, equivalentment, si existeix $A \subseteq \mathbb{Z}^n_{\geq 0}$ tal que*

$$I = \left\{ \sum_{\alpha \in A} h_\alpha x^\alpha \mid h_\alpha \in \mathbb{K}[x_1, \ldots, x_n] \right\} = \langle x^\alpha \mid \alpha \in A \rangle.$$

Lema 1.3.11. [2] *Sigui $I = \langle x^\alpha \mid \alpha \in A \rangle$ un ideal monomial. Aleshores $x^\beta \in I$ si, i només si, $x^\alpha | x^\beta$ per a algun $\alpha \in A$.*

Demostració.

$\boxed{\Leftarrow}$ Si x^β és un múltiple de x^α per a algun $\alpha \in A$, aleshores $x^\beta \in I$ per la definició d'ideal.

$\boxed{\Rightarrow}$ Si $x^\beta \in I$, aleshores per $h_i \in \mathbb{K}[x_1, \ldots, x_n],\ \alpha(i) \in A$,

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} = \sum_{i=1}^{s} \left(\sum_j c_{i,j} x^{\beta(i,j)} \right) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}.$$

Aleshores, tot element de la dreta és divisible per a algun $x^{\alpha(i)}$ i, en conseqüència, x^β té la mateixa propietat. □

Veiem ara que tot ideal monomial de $\mathbb{K}[x_1, \ldots, x_n]$ és finitament generat. El Lema de Dickson resol el problema de la descripció d'ideals per al cas d'ideals monomials. Aquest és un resultat clau en la construcció de bases de Gröbner.

Teorema 1.3.12 (Lema de Dickson)**.** *Sigui $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ un ideal monomial. Aleshores*

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

amb $\alpha(1), \ldots, \alpha(s) \in A$. En particular, I té una base finita.

Del Lema de Dickson veiem que la condició (iii) de la Definició 1.3.1 pot simplificar-se a la condició $\alpha \geq 0 \ \forall \alpha \in \mathbb{Z}^n_{\geq 0}$.

Corol·lari 1.3.13. *Sigui $>$ una relació en $\mathbb{Z}^n_{\geq 0}$ tal que:*

(i) $>$ és una relació d'ordre total en $\mathbb{Z}^n_{\geq 0}$.

(ii) Si $\alpha > \beta$ i $\gamma \in \mathbb{Z}^n_{\geq 0}$ aleshores $\alpha + \gamma > \beta + \gamma$.

Aleshores $>$ està ben ordenat si, i només si, $\alpha \geq 0, \ \forall \alpha \in \mathbb{Z}^n_{\geq 0}$.

Demostració.

$\boxed{\Rightarrow}$ Siguin $>$ una relació ben ordenada i α_0 l'element minimal de $\mathbb{Z}^n_{\geq 0}$. Suposem que $\alpha_0 < 0$, aleshores

$$0 > \alpha_0 \underset{(ii)}{\Rightarrow} \alpha_0 > \alpha_0 + \alpha_0 = 2\alpha_0$$

fet que és una contradicció amb la minimalitat de α_0.

$\boxed{\Leftarrow}$ Siguin $\alpha \geq 0 \ \forall \alpha \in \mathbb{Z}^n_{\geq 0}$ i $A \subseteq \mathbb{Z}^n_{\geq 0}, A \neq \emptyset$.

Sigui $I = \langle x^\alpha \mid \alpha \in A \rangle$ un ideal monomial. Pel Lema de Dickson tenim

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

amb $\alpha(1), \ldots, \alpha(s) \in A$. Reordenant els elements, si és necessari, suposem que

$$\alpha(1) < \ldots < \alpha(s)$$

d'on volem veure que $\alpha(1)$ és l'element minimal d'A.

Donat $\alpha \in A$, tenim que $x^\alpha \in I$, d'on, pel Lema 1.3.11, x^α és divisible per a algun $x^{\alpha(i)}$ i, per tant existeix $\gamma \in \mathbb{Z}^n_{\geq 0}$ tal que $\alpha = \alpha(i) + \gamma$. Aleshores,

$$\alpha = \alpha(i) + \gamma \underset{\gamma \geq 0}{\geq} \alpha(i) + 0 = \alpha(i) \underset{(ii)}{\geq} \alpha(1)$$

d'on obtenim que $\alpha(1)$ és l'element minimal d'A. □

Proposició 1.3.14. [2] *Un ideal monomial $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ té una base $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ tals que $x^{\alpha(i)} \nmid x^{\alpha(j)} \ \forall i \neq j$. Aquesta base és única i s'anomena base minimal de I.*

Demostració. Pel Lema de Dickson, I té una base finita. Si $x^{\alpha(i)} \mid x^{\alpha(j)}$ per a algun i, j, aleshores podem descartar $x^{\alpha(j)}$ i repetir el procés fins a obtenir que $x^{\alpha(i)} \nmid x^{\alpha(j)}\ \forall i \neq j$. D'aquí obtenim l'existència d'una base minimal $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$.

Siguin $\left(x^{\alpha(1)}, \ldots, x^{\alpha(s)}\right)$, $\left(x^{\beta(1)}, \ldots, x^{\beta(t)}\right)$ dues bases minimals de I. Pel Lema 1.3.11, existeixen i, j tals que

$$x^{\alpha(1)} \in I \Rightarrow x^{\beta(i)} \mid x^{\alpha(1)}$$
$$x^{\beta(i)} \in I \Rightarrow x^{\alpha(j)} \mid x^{\beta(i)}$$

Per tant, $x^{\alpha(j)} \mid x^{\alpha(1)}$ i per la minimalitat de la base $j = 1$, d'on $x^{\alpha(1)} = x^{\beta(i)}$.

Seguint aquest procedimenet, tenim la igualtat entre les dues bases. □

Per tal de descriure les bases de Gröbner, definim abans l'ideal dels termes principals donat un ideal I. Veurem que, donat un ordre monomial, tot $f \in \mathbb{K}[x_1, \ldots, x_n]$ té un únic terme principal, $LT(f)$.

Definició 1.3.15. *Sigui $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, $I \neq \{0\}$ i $>$ un ordre monomial en $\mathbb{K}[x_1, \ldots, x_n]$. Aleshores*

$$LT(I) = \{cx^\alpha \mid \exists f \in I \setminus \{0\} \text{ amb } LT(f) = cx^\alpha\}$$

i $\langle LT(I)\rangle$ denota l'ideal generat pels elements de $LT(I)$.

Donat un conjunt finit de generadors per $I = \langle f_1, \ldots, f_s\rangle$, tenim que

$$LT(f_i) \in LT(I) \subseteq \langle LT(I)\rangle$$

d'on

$$\langle LT(f_1), \ldots, LT(f_s)\rangle \subseteq \langle LT(I)\rangle$$

però, la inclusió contrària no es compleix sempre.

Exemple 1.3.16. [2] Sigui $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$, amb $f_1, f_2 \in \mathbb{K}[x, y]$ i un ordre monomial. Aleshores

$$x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^3y - 2xy^2 + x^2 - x^3y + 2xy^2 = x^2 \in I$$

Ara tenim que

$$x^2 = LT(x^2) \in LT(I) \subseteq \langle LT(I)\rangle$$

però, pel Lema 1.3.11,

$$x^2 \notin \langle LT(f_1), LT(f_2)\rangle = \langle x^3, x^2y\rangle$$

ja que $x^3 \nmid x^2$ i $x^3 \nmid x^2y$.

Proposició 1.3.17. [2] *Sigui $I \subseteq \mathbb{K}[x_1, \ldots, x_n], I \neq \{0\}$. Aleshores*

(i) $\langle LT(I)\rangle$ *és un ideal monomial.*

(ii) $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$ *per a alguns* $g_1, \ldots, g_s \in I$.

Demostració.

(i) Els monomis líders $LM(g)$ per a $g \in I \setminus\{0\}$ generen l'ideal monomial

$$\langle LM(g) \mid g \in I \setminus\{0\}\rangle$$

Per la definició de $LM(g)$ i $LT(g)$, tenim que

$$\langle LT(g) \mid g \in I \setminus\{0\}\rangle = \langle LT(I)\rangle$$

i, per tant, $\langle LT(I)\rangle$ és un ideal monomial.

(ii) Tenim que, pel Lema de Dickson, $\langle LT(I)\rangle$ és un ideal monomial finitament generat. Per tant,

$$\langle LT(I)\rangle = \langle LM(g_1), \ldots, LM(g_s)\rangle$$

i, de nou, per la definició de $LM(g)$ i $LT(g)$, tenim que

$$\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle.$$

□

Una de les qüestions més importants a la teoria d'ideals és saber si tot ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ té una base finita. El següent teorema en dona una resposta afirmativa.

Teorema 1.3.18 (Teorema de la base de Hilbert)**.** [2] *Tot ideal* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *té un conjunt finit de generadors. En altres paraules, donat un ideal* I*, existeix una col·lecció finita de polinomis* $\{f_1, \ldots, f_s\} \in \mathbb{K}[x_1, \ldots, x_n]$ *tal que* $I = \langle f_1, \ldots, f_s\rangle$.

Demostració. Si $I = \{0\}$ el teorema es compleix trivialment.

Suposem, per tant, que I conté algun polinomi $f_i \neq 0$. Per la Proposició 1.3.17, existeixen polinomis $f_1, \ldots, f_s \in I$ tals que

$$\langle LT(I)\rangle = \langle LT(f_1), \ldots, LT(f_s)\rangle$$

Volem veure que $I = \langle f_1, \ldots, f_s\rangle$

$\boxed{\supseteq}$ Com que $f_i \in I\ \forall i$, aleshores tenim, clarament, que

$$\langle f_1, \ldots, f_s\rangle \subseteq I$$

$\boxed{\subseteq}$ Sigui $f \in I$ un polinomi qualsevol. Apliquem l'algoritme de divisió (Teorema 1.3.8) per dividir f per $(f_1, \ldots, f_s)$ i obtenim

$$f = q_1 f_1 + \ldots + q_s f_s + r$$

amb $q_i, r \in \mathbb{K}[x_1, \ldots, x_n]$ i $r = 0$ o r és combinació lineal de monomis amb coeficients a $\mathbb{K}$, no divisibles per $LT(f_1), \ldots, LT(f_s)$. Volem veure que $r = 0$. En cas contrari, com que

$$r = f - q_1 f_1 - \ldots - q_s f_s$$

tindríem que $LT(r) \in \langle LT(f_1), \ldots, LT(f_s) \rangle$, i pel Lema 1.3.11, $LT(f_i) \mid LT(r)$ per a alguna i, fet que és una contradicció amb la definició de residu. Per tant, $r = 0$. D'aquí,

$$f = q_1 f_1 + \ldots + q_s f_s + 0 \in \langle f_1, \ldots, f_s \rangle$$

i per tant, $I \subseteq \langle f_1, \ldots, f_s \rangle$. □

Donem a continuació la definició de base de Gröbner.

Definició 1.3.19. [2] *Donat un ordre monomial en $\mathbb{K}[x_1, \ldots, x_n]$, un subconjunt $G = \{g_1, \ldots, g_s\} \subset I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, $G \neq \emptyset$ és una base de Gröbner si*

$$\langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle$$

Per tant, tenim que $\{f_1, f_2\}$ de l'Exemple 1.3.16 no és una base de Gröbner.

Veiem ara algunes propietats de les bases de Gröbner donats un ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ i $G = \{g_1, \ldots, g_s\}$ una base de Gröbner per a I.

La proposició següent justifica, en bona mesura, la importància de les bases de Gröbner. Estableix que usant com a divisors els elements d'una base de Gröbner d'un ideal, el residu de l'algoritme de la divisió d'un polinomi donat no depèn de l'ordre dels divisors.

Proposició 1.3.20. [2] *Donat $f \in \mathbb{K}[x_1, \ldots, x_n]$, existeix un únic $r \in \mathbb{K}[x_1, \ldots, x_n]$ tal que*

(i) Cap dels termes de r és divisible per $LT(g_1), \ldots, LT(g_s)$.

(ii) $f = g + r$ per a algun $g \in I$.

Demostració. Per l'Algoritme de Divisió 1.3.8 tenim que

$$f = q_1 g_1 + \ldots + q_s g_s + r$$

per a $q_i \in \mathbb{K}[x_1, \ldots, x_n]$, d'on r compleix (i).

Prenent $g = q_1 g_1 + \ldots + q_s g_s$, tenim que

$$f = g + r$$

d'on (ii) queda provat.

Resta veure que r és únic. Siguin $g' \in I$ i $r' \in \mathbb{K}[x_1, \ldots, x_n]$ tals que

$$f = g + r = g' + r'$$

satisfent (i) i (ii). Aleshores

$$r - r' = g' - g \in I$$

Si $r \neq r'$, aleshores

$$LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$$

d'on, pel Lema 1.3.11 $LT(g_i) \mid LT(r - r')$ per a algun g_i. Però això és impossible per (i). Llavors $r - r' = 0$ i la unicitat queda provada. □

D'aquí obtenim que les bases de Gröbner poden caracteritzar-se per la unicitat del residu r. Volem veure ara quan una base d'un ideal I és una base de Gröbner.

Corol·lari 1.3.21. *Sigui una base de Gröbner $G = \{g_1, \ldots, g_s\}$ de l'ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Donat $f \in \mathbb{K}[x_1, \ldots, x_n]$, alehores*

$$f \in I \iff \bar{f}^G = 0$$

on $\bar{f}^G$ és el residu de la divisió de f per G.

Demostració.

$\boxed{\Leftarrow}$ Si $\bar{f}^G = 0$, aleshores $f \in I$.

$\boxed{\Rightarrow}$ Si $f \in I$, per l'algoritme de divisió 1.3.8, podem escriure f com

$$f = h_1 g_1 + \ldots + h_s g_s + \bar{f}^G$$

per a $h_1, \ldots, h_2, \bar{f}^G \in I$. Com que $f \in I$, aleshores tenim que $\bar{f}^G = 0$, ja que, en cas contrari, per i de la Proposició 1.3.20, r cap monomi de r seria divisible per cap dels $LT(g_i)$. □

Per tant, per determinar si un polinomi pertany a un ideal I és suficient fixar un ordre monomial adequat, buscar una base de Gröbner de I i, aplicant l'Algoritme de divisió i el Corol·lari 1.3.21 es podrà saber si hi pertany o no.

Fixat un ordre monomial en $\mathbb{K}[x_1, \ldots, x_n]$,

Definició 1.3.22. *Siguin $f, g \neq 0 \in \mathbb{K}[x_1, \ldots, x_n]$*

(i) Prenent $multideg(f) = \alpha$ i $multideg(g) = \beta$, sigui $\gamma = (\gamma_1, \ldots, \gamma_n)$ amb $\gamma_i = max(\alpha_i, \beta_i)$. Aleshores tenim

$$x^\gamma = mcm(LM(f), LM(g))$$

(ii) L' S-polinomi de f i g és la combinació

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

Notem que la syzygia de f i g, $S(f,g)$ produeix, deliberadament, una cancel·lació d'ambdós termes principals. Al Capítol 2.2 en donarem més detalls.

Veiem a continuació que tota cancel·lació dels termes principals en una suma de polinomis pot realitzar-se utilitzant syzygies. Utilitzant els S-polinomis, determinem quan una base d'un ideal és una base de Gröbner.

Teorema 1.3.23 (Criteri de Buchberger)**.** *Una base $G = \{g_1, \ldots, g_s\}$ de I és una base de Gröbner de I si, i només si, per a tot $i \neq j$, el residu de $S(g_i, g_j)$ per G és zero, és a dir, $\overline{S(g_i,g_j)}^{G} = 0$*

Il·lustrem aquest criteri amb el següent exemple per a determinar si dos polinomis que generen I son una base de Gröbner o no respecte un ordre monomial concret.

Exemple 1.3.24. Donat $I = \langle x - z^2, y - z^3 \rangle$, volem veure, utilitzant l'algoritme de Buchberger, si $\{x - z^2, y - z^3\}$ és una base de Gröbner de I amb

$$x >_{lex} y >_{lex} z$$

Seguint l'algoritme, tenim que

$$S(x - z^2, y - z^3) = \frac{xy}{x}(x - z^2) - \frac{xy}{y}(y - z^3) = xz^3 - yz^2 = z^3(x - z^2) + (-z^2)(y - z^3)$$

on la darrera igualtat l'hem obtingut aplicant l'algoritme de divisió per G. Notem que el residu és zero i, per tant, pel Criteri de Buchberger **??** obtenim que G és una base de Gröbner de I amb l'ordre lexicogràfic.

Donats $f_1, \ldots, f_s$ amb $f_i \in \mathbb{K}[x_1, \ldots, x_n]$, volem calcular la base de Gröbner respecte un ordre monomial. Es mostra a continuació, sense demostració, l'algoritme que va ser inventat pel matemàtic Bruno Buchberger (1942-) amb aquest objectiu.

Teorema 1.3.25 (Algoritme de Buchberger)**.** *Sigui $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ un polinomi. L'algoritme finit per a construir una base de Gröbner per a I és el següent:*

$$\begin{aligned}
&Entrada: \ F = (f_1, \ldots, f_s)\\
&\quad G := F\\
&\quad do\{\\
&\qquad G' := G\\
&\qquad for\{\{p,q\}, p \neq q\} \ \{\\
&\qquad\quad r := \overline{S(p,q)}^{G'}\\
&\qquad\quad if\{r \neq 0\}\\
&\qquad\qquad G := G \cup \{r\}\\
&\qquad \}\\
&\quad while\{G = G'\}\\
&Sortida: G = \langle g_1, \ldots, g_s \rangle \supseteq F
\end{aligned}$$

Il·lustrem aquest algoritme amb un exemple.

1.4 Teoria d'eliminació

La teoria d'eliminació té per objectiu eliminar algunes de les variables dels polinomis d'un sistema, per tal de resoldre'l. Aquest camp d'estudi va ser motivat per la necessitat de mètodes per a resoldre sistemes d'equacions amb polinomis. Resoldre aquests sistemes és important ja que ens permetrà trobar explícitament els punts que conformen les varietats afins algebraiques.

Es mostra a continuació un exemple per a il·lustrar aquesta idea:

Exemple 1.4.1. [2] Resoldrem el sistema d'equacions

$$\left.\begin{aligned} x^2+y+z&=1\\ x+y^2+z&=1\\ x+y+z^2&=1 \end{aligned}\right\} \tag{1.4.1}$$

d'on

$$I=\langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1\rangle \tag{1.4.2}$$

i la base de Gröbner per I respecte l'ordre lexicogràfic és

$$\begin{aligned} g_1&=x^2+y+z-1\\ g_2&=y^2-y-z^2+z\\ g_3&=2yz^2+z^4-z^2\\ g_4&=z^6-4z^4+4z^3-z^2 \end{aligned} \tag{1.4.3}$$

Aleshores (1.4.1) i (1.4.3) tenen les mateixes solucions.

$$g_4=z^6-4z^4+4z^3-z^2=z^2(z-1)^2(z^2+2z-1)$$

d'on les solucions per z son:

$$z_a=0,\ z_b=1,\ z_c=-1+\sqrt{2},\ z_d=-1-\sqrt{2}$$

Si $z_a=0$, aleshores

$$g_2=y^2-y-0^2+0=y^2-y=y(y-1)$$

i $y_a=1, y_b=0$. En el primer cas,

$$g_1=x+1+0^2-1=0$$

d'on $x=0$. I en el segon cas,

$$g_1=x+0+0^2-1=0$$

i $x=1$.

Anàlogament obtenim totes les solucions:

$$(1,0,0),\ (0,1,0),\ (0,0,1)$$
$$(-1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2}),\ (-1-\sqrt{2}.-1-\sqrt{2},-1-\sqrt{2})$$

L'objectiu de la teoria d'eliminació és obtenir una equació que contingui només una incògnita (a l'exemple (1.4.1), la z) i extendre aquest resultat a les equacions originals. La idea bàsica de la teoria d'eliminació és que aquests dos processos puguin fer-se de forma general.

Definició 1.4.2. *Donat $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$, l'ideal d'eliminació l-èsim, $I_l \in \mathbb{K}[x_{l+1}, \ldots, x_n]$ definit per*

$$I_l = I \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$$

El problema d'eliminació consisteix, doncs, en trobar un sistema de generadors de l'ideal $I \in \mathbb{K}[x_1, \ldots, x_n]$ que contingui un sistema de generadors de l'ideal I_l per a tot $l \in \{0, \ldots, n-1\}$. L'ideal d'eliminació varia segons l'ordre monomial escollit. Utilitzant bases de Gröbner aconseguirem eliminar variables gràcies al següent teorema:

Teorema 1.4.3 (Teorema d'eliminació)**.** [4] *Sigui $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ un ideal i sigui G una base de Gröbner de I respecte l'ordre lexicogràfic amb*

$$x_1 > x_2 > \ldots > x_n$$

Aleshores

$$G_l = G \cap \mathbb{K}[x_{l+1}, \ldots, x_n] \quad \forall 0 \leq l \leq n$$

és una base de Gröbner de l'ideal I_l.

Demostració. Sigui $l \in (0, n)$. Tenim que $G_l \subseteq I_l$. De la definició de base de Gröbner tenim que s'ha de complir

$$\langle LT(I_l) \rangle = \langle LT(G_l) \rangle$$

$\boxed{\supseteq}$ Tenim que $G_l \subseteq I_l$, d'on $\langle G_l \rangle \subseteq \langle I_l \rangle$

$\boxed{\subseteq}$ Cal veure que

$$LT(g) \mid LT(f)$$

per a qualsevol $f \in I_l$ i algun $g \in G_l$. En primer lloc, com que $f \in I$ i G és una base de Gröbner de I,

$$LT(g) \mid LT(f)$$

per a algun $g \in G$. Com que $f \in I_l$, aleshores $LT(g) \in \{x_{l+1}, \ldots, x_n\}$.

Com que $x_1 > \ldots > x_n$, tot monomi amb $x_1, \ldots, x_l$ és major que qualsevol monomi de $\mathbb{K}[x_{l+1}, \ldots, x_n]$. D'aquí,

$$LT(g) \in \mathbb{K}[x_{l+1}, \ldots, x_n] \Rightarrow g \in \mathbb{K}[x_{l+1}, \ldots, x_n]$$

d'on $g \in G_l$. □

Exemple 1.4.4. Prenent els mateixos polinomis que a l'exemple (1.4.1), tenim que

$$I_1 = I \cap \mathbb{K}[y,z] = \langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2 \rangle = \langle g_2, g_3 \rangle$$
$$I_2 = I \cap \mathbb{K}[z] = \langle z^6 - 4z^4 + 4z^3 - z^2 \rangle = \langle g_4 \rangle$$

Volem veure ara quines de les solucions de les equacions obtingudes eliminant les primeres l variables poden ser esteses a solucions del sistema inicial.

Recordem abans una definició necessària per al teorema:

Definició 1.4.5. *Direm que $\mathbb{K}$ és un cos algebraicament tancat si tot polinomi $P(x) \in \mathbb{K}[x_1, \ldots, x_n]$ amb $\deg(P) > 1$, té una arrel a $\mathbb{K}$.*

Presentem, sense demostració, el teorema d'extensió.

Teorema 1.4.6 (Teorema d'extensió)**.** [4] *Siguin $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal, amb $\mathbb{K}$ algebraicament tancat, i $(a_2, \ldots, a_n)$ un zero del primer ideal d'eliminació. Suposem que existeix un polinomi $f \neq 0 \in I$ tal que*

$$f = \sum_{i=0}^{t} c_i x_1^i$$

amb $c_i \in \mathbb{K}[x_2, \ldots, x_n]$ i $deg_{x_1}(f) = t$, tal que $c_t(a_2, \ldots, a_n) \neq 0$. Aleshores existeix $a_1 \in \mathbb{K}$ tal que $(a_1, a_2, \ldots, a_n) \in V(I)$.

Notem que aquest teorema diu com estendre solucions de $\mathbb{V}(I_1)$ a $\mathbb{V}(I)$; però es pot aplicar anàlogament per a passar de qualsevol solució en $\mathbb{V}(I_l)$ a una solució en $\mathbb{V}(I_{l-1})$, ja que I_l és el primer ideal d'eliminació de I_{l-1}.

Veiem un exemple de la resolució d'un sistema d'equacions polinomials utilitzant els teoremes d'eliminació (Teorema 1.4.3) i extensió (Teorema 1.4.6).

Exemple 1.4.7. Sigui la varietat afí $V \in \mathbb{C}^3$ determinada per les equacions:

$$\left.\begin{aligned} xy = 1 \\ xz = 1 \end{aligned}\right\}$$

Sigui, per tant, l'ideal

$$I = \langle xy - 1, xz - 1 \rangle$$

La seva base de Gröbner respecte l'ordre lexicogràfic amb $x > y > z$ és

$$G = \{xy - 1, xz - 1, y - z\}$$

i utilitzant el Teorema 1.4.3,

$$G_1 = \{y - z\}$$

és una base de Gröbner de l'ideal I_1. És a dir, que les solucions parcials del sistema obtingut eliminant la primera variable, $\mathbb{V}_{\mathbb{C}^2}(I_1)$, son els punts de la recta $y = z$.

D'aquí obtenim que podem estendre a solucions del sistema totes les solucions parcials del sistema, excepte la solució $(0,0)$, ja que en tal cas

$$0 \cdot 0 = 0 = 1$$

en ambdós casos, fet que és impossible. Si prenem com a solució parcial el punt (a, a) amb $a \neq 0$, aleshores tots els punts de la forma

$$\left(\frac{1}{a}, a, a\right)$$

son solució del sistema original.

1.5 Mòduls

Contràriament a la teoria d'ideals, el concepte de mòdul es remunta varis segles enrere.

Al segle III a.C el matemàtic grec Euclides va utilitzar l'aritmètica modular per a estudiar les propietats dels nombres primers i dels nombres parells i imparells. Més endavant, al segle XVII, el matemàtic i filòsof francès René Descartes, a la seva obra "La Géometrie"(1637) va començar a utilitzar el concepte de mòdul per a referir-se al valor absolut d'un nombre o a la distància entre dos punts al pla utilitzant coordenades cartesianes. Ja al segle XIX, el matemàtic alemany Carl Friedrich Gauss va establir les bases de la teoria de congruències i va desenvolupar mètodes per a resoldre equacions lineals amb congruències. Finalment, durant el segle XX, el concepte de mòdul va generalitzar-se i estendre's a d'altres branques de la matemàtica. En particualr, es va introduir el concepte d'anell i la noció de mòdul sobre un anell.

Sigui $\mathbb{A}$ un anell commutatiu unitari i sigui $\mathbb{A}^k$ el conjunt de vectors fila k-dimensionals amb coeficients a $\mathbb{A}$.

Definició 1.5.1. [4] *Un mòdul sobre un anell $\mathbb{A}$ o un $\mathbb{A}$-mòdul és un conjunt M amb una operació binària (suma, $+$) i una operació de $\mathbb{A}$ sobre M (producte, $\cdot$). De manera que per a tot $a, b \in \mathbb{A}$ i per a tot $f, g \in M$ tenim:*

(i) *M és un grup abelià amb l'operació suma ($+$). És a dir, la suma a M és associativa i commutativa, existeix $0 \in M$ element identitat de la suma, i per a tot element $f \in M$, existeix $-f \in M$ tal que $f + (-f) = 0$, anomenat element invers per a la suma.*

(ii) $a(f + g) = af + ag$.

(iii) $(a + b)f = af + bf$.

(iv) $(ab)f = a(bf)$.

(v) $1f = f$

Exemple 1.5.2. En particular tot ideal I és un mòdul sobre l'anell $\mathbb{A}$.

Definició 1.5.3. *Direm que $M \subset \mathbb{A}^k$ és un mòdul sobre $\mathbb{A}$ si*

$$h_1 f_1 + h_2 f_2 \in M$$

per a tot $f_1, f_2 \in M$ i $h_1, h_2 \in \mathbb{A}$.

Veurem que el concepte de mòdul és útil en el sentit que generalitza simultàniament les nocions d'ideal i d'anell quocient.

Definició 1.5.4. *Donat $N \subset M$, on M és un mòdul, direm que N és un submòdul de M si*

$$an = na \in N \quad \forall n \in N, a \in \mathbb{A}$$

Definició 1.5.5. *Si $N \subset M$, aleshores el conjunt de classes d'equivalència d'elements de M tal que*

$$f \equiv g \iff f - g \in N$$

és un $\mathbb{A}$-mòdul amb les operacions induïdes per M. S'anomena anell quocient de M per N i es denota per M/N.

Definició 1.5.6. *Si M, N son $\mathbb{A}$-mòduls, la funció*

$$\begin{array}{rccc} \phi: & M & \to & N \\ & am+n & \mapsto & a\phi(m)+\phi(n) \end{array}$$

és un homeomorfisme entre M, N, i té per nucli el conjunt

$$ker(\phi) = \{f \in M : \phi(f) = 0\}$$

Definició 1.5.7. *Sigui $M \subset \mathbb{A}^k$ un mòdul. Direm que M és finitament generat si existeixen $f_1, \ldots, f_m \in M$ tals que*

$$f = a_1 f_1 + \ldots + a_m f_m \tag{1.5.1}$$

amb $a_1, \ldots, a_m \in \mathbb{A}$. En tal cas direm que $\{f_1, \ldots, f_m\}$ és el conjunt generador de M i ho denotarem per $\langle f_1, \ldots, f_m \rangle$.

Proposició 1.5.8. [4] *Sigui M un $\mathbb{A}$-mòdul. $F = \{f_1, \ldots, f_m\} \subset M$ és una base de M si, i només si, tot $f \in M$ es pot escriure com (1.5.1) de manera única.*

Il·lustrem el concepte de base de M amb el següent exemple:

Exemple 1.5.9. Sigui l'ideal $M = \langle x^2, y^3 \rangle \subset \mathbb{A}$. El conjunt $\{x^2, y^3\}$ no és una base de M com a mòdul ja que

$$y^3 x^2 - x^2 y^3 = 0$$

amb $y^3, x^2 \neq 0$, i per tant no són linealment independents. En canvi, sí que és una base de M com a ideal.

Definició 1.5.10. *Sigui M un $\mathbb{A}$-mòdul. M és un mòdul lliure si M té una base.*

En el cas general d'un anell de polinomis $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_n]$, el mòdul lliure M de s generadors consisteix en tots els possibles vectors de polinomis $(g_1, \ldots, g_s)$, $g_i \in \mathbb{A}$. Per tant, el mòdul lliure és un conjunt $\mathbb{A}^s$.

Sigui $e_i = (0, \ldots, 1, \ldots, 0)$, amb 1 a la posició i-èsima. Aleshores, podem escriure

$$(g_1, \ldots, g_s) = g_1 e_1 + \ldots + g_s e_s,$$

i aquesta representació és única, d'on la base canònica és una base de M com a $\mathbb{A}$-mòdul.

Teorema 1.5.11 (Quillen Suslin)**.** [4] *Sigui $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_n]$ i suposem que $a_1, \ldots, a_m \in \mathbb{A}$ generen tot $\mathbb{A}$. Aleshores el mòdul M de totes les solucions $(X_1, \ldots, X_m) \in \mathbb{A}^m$ de l'equació lineal*

$$a_1 X_1 + \ldots + a_m X_m = 0$$

és lliure.

Capítol 2

μ-Classificació de corbes planes

L'equació paramètrica d'una corba plana racional és

$$(x, y) = \left(\frac{a(t)}{c(t)}, \frac{b(t)}{c(t)}\right) \tag{2.0.1}$$

on

$$a(t) = \sum_{i=0}^{n_a} a_i t^i, \qquad b(t) = \sum_{i=0}^{n_b} b_i t^i, \qquad c(t) = \sum_{i=0}^{n_c} c_i t^i. \tag{2.0.2}$$

amb $n_a = \deg(a)$, $n_b = \deg(b)$, $n_c = \deg(c)$.

El grau de la corba és $n = max(n_a, n_b, n_c)$.

Suposem que $a(t), b(t), c(t)$ son relativament primers i que $c(t) \neq 0$. Definim

$$f = c(t)x - a(t), \qquad g = c(t)y - b(t).$$

2.1 μ-bases

Definició 2.1.1. [3] *L'ideal I de la corba (2.0.1) ve donat per*

$$I = \langle f, g \rangle = \{p_1 f + p_2 g \quad | \quad p_1, p_2 \in \mathbb{K}[x, y, t]\}$$

Observem que l'ideal I està generat per f i g. L'objectiu és trobar generadors amb deg_t mínim. Comencem enunciant un lema tècnic.

Lema 2.1.2. *Siguin $A(t), B(t), C(t) \in \mathbb{K}[t]$ tals que*

$$a(t)A(t) + b(t)B(t) + c(t)C(t) \equiv 0. \tag{2.1.1}$$

Aleshores existeixen $h_1(t), h_2(t), h_3(t) \in \mathbb{K}[t]$ tals que

$$\begin{aligned} A(t) &= c(t)h_1(t) + b(t)h_3(t); \\ B(t) &= c(t)h_2(t) - a(t)h_3(t); \\ C(t) &= -a(t)h_1(t) - b(t)h_2(t); \end{aligned}$$

Demostració. Com que $mcd(a(t), b(t), c(t)) = 1$, això implica que, per l'identitat de Bézout, existeixen $u(t), v(t), w(t) \in \mathbb{K}[t]$ tals que

$$u(t)a(t) + v(t)b(t) + w(t)c(t) = 1 \tag{2.1.2}$$

Si multipliquem l'equació (2.1.2) per $A(t)$ i usem (2.1.1), obtenim

$$1 \cdot A = uaA + vbA + wcA = u(-bB - cC) + vbA + wcA = c(-uC + wA) + b(-uB + vA).$$

Anàlogament

$$B = c(-vC + wB) - a(-uB + vA);$$
$$C = -a(-uC + wA) - b(-vC + wB).$$

Prenem

$$h_1(t) = -u(t)C(t) + w(t)A(t)$$
$$h_2(t) = -v(t)C(t) + w(t)B(t)$$
$$h_3(t) = -u(t)B(t) + v(t)A(t)$$

i el resultat queda demostrat. □

Veiem ara, doncs, una caracterització dels polinomis $P(t) = A(t)x + B(t)y + C(t) \in I$, amb I definit com a la Definició 2.1.1.

Lema 2.1.3. *Donat $P(t) = A(t)x + B(t)y + C(t) \in \mathbb{K}[x, y, t]$, llavors*

$$P(t) \in I = \langle c(t)x - a(t), c(t)y - b(t) \rangle$$

si, i només si,

$$a(t)A(t) + b(t)B(t) + c(t)C(t) \equiv 0$$

Demostració.

$\boxed{\Rightarrow}$ Suposem que $P(t) \in I$. Definim l'homeomorfisme d'anells

$$\begin{array}{ccc} \alpha : \mathbb{K}[x, y, t] & \to & \mathbb{K}(t) \\ x & \mapsto & \dfrac{a(t)}{c(t)} \\ y & \mapsto & \dfrac{b(t)}{c(t)} \\ t & \mapsto & t \end{array}$$

per tant

$$\alpha(c(t)x - a(t)) = c(t)\frac{a(t)}{c(t)} - a(t) = a(t) - a(t) = 0$$
$$\alpha(c(t)y - b(t)) = c(t)\frac{b(t}{c(t)} - b(t) = b(t) - b(t) = 0$$

Si $P(t) \in I$, tenim que

$$0 = \alpha(P(t)) = A(t)\frac{a(t)}{c(t)} + B(t)\frac{b(t)}{c(t)} + C(t)$$

i, per tant, multiplicant per $c(t)$ tenim que

$$a(t)A(t) + b(t)B(t) + c(t)C(t) \equiv 0$$

tal i com volíem veure.

$\boxed{\Leftarrow}$ Suposem que existeixen $A(t), B(t), C(t) \in \mathbb{K}[t]$ tals que

$$a(t)A(t) + b(t)B(t) + c(t)C(t) \equiv 0$$

Aleshores, pel Lema 2.1.2 existeixen $h_1(t), h_2(t), h_3(t) \in \mathbb{K}[t]$ tals que

$$\begin{aligned} A(t) &= c(t)h_1(t) + b(t)h_3(t); \\ B(t) &= c(t)h_2(t) - a(t)h_3(t); \\ C(t) &= -a(t)h_1(t) - b(t)h_2(t); \end{aligned}$$

Per tant,

$$\begin{aligned} P(t) = A(t)x + B(t)y + C(t) &= (ch_1 + bh_3)x + (ch_2 - ah_3)y + (-ah_1 - bh_2) = \\ &= ch_1x + bh_3x + ch_2y - ah_3y - ah_1 - bh_2 = \\ &= ch_1x + ch_3xy - ah_1 - ah_3y + ch_2y - ch_3xy - bh_2 + bh_3x = \\ &= (h_1 + yh_3)(cx - a) + (h_2 - xh_3)(cy - b) \in I \end{aligned}$$

□

Corol·lari 2.1.4. [3]

(i) Si $P(t) = A(t)x + B(t)y + C(t) \in I$ i $h \in \mathbb{K}[t]$ és tal que $h \mid P$, aleshores $P/h \in I$.

(ii) Si $a = d\hat{a}$ i $c = d\hat{c}$ amb $d = mcd(a, c)$, aleshores

$$\{rx + s | r, s \in \mathbb{K}[t]\} \cap I = \{h(\hat{c}x - \hat{a}) | h \in \mathbb{K}[t]\}.$$

Demostració.

(i) Escrivim $A = hA', B = hB'$ i $C = hC'$. Llavors

$$P(t) = A(t)x + B(t)y + C(t) \in I \underset{\text{Lema 2.1.3}}{\Rightarrow} aA + bB + cC = 0 \Rightarrow$$

$$ahA' + bhB' + chC' = 0 \Rightarrow aA' + bB' + cC' = 0 \underset{\text{Lema 2.1.3}}{\Rightarrow}$$

$$P/h = A'x + B'y + C' \in I$$

(ii) $\boxed{\subset}$ Suposem, en primer lloc, que $rx + s \in I$. Pel Lema 2.1.3, tenim que

$$ar + b \cdot 0 + cs = 0 \Rightarrow d\hat{a}r + d\hat{c}s = 0 \Rightarrow \hat{a}r + \hat{c}s = 0$$

Com que $\hat{a}$ i $\hat{c}$ son relativament primers per hipòtesi, tenim que $r = \hat{c}h$ i $s = -\hat{a}h$ per a algun $h \in \mathbb{K}[t]$. Així,

$$rx + s = \hat{c}hx - \hat{a}h = h(\hat{c}x - \hat{a})$$

$\boxed{\supset}$ Com que

$$hf = h(cx - a) = h(d\hat{c}x - d\hat{a}) = dh(\hat{c}x - \hat{a}) \in I$$

i és divisible per d, per a. tenim que

$$\frac{hf}{d} = h(\hat{c}x - \hat{a}) \in I$$

□

Donat l'ideal I podem definir el següent $\mathbb{K}$-espai vectorial.

Definició 2.1.5. [3] *Sigui $I = \langle c(t)x - a(t), c(t)y - b(t)\rangle$, aleshores definim*

$$I_{1,m} = \{P(t) = A(t)x + B(t)y + C(t) \in I \mid deg_{x,y}(P) \leq 1, deg_t(P) \leq m\}.$$

Donem a continuació un resultat per a acotar inferiorment el nombre d'elements linealment independents de $I_{1,m}$.

Lema 2.1.6. [3] *El nombre d'elements en $I_{1,m}$ linealment independents és $\geq 2m+2-n$.*

Demostració. Sigui $P(t) = A(t)x + B(t)y + C(t) \in I$ amb

$$A(t) = \sum_{i=0}^{m} A_i t^i \qquad B(t) = \sum_{i=0}^{m} B_i t^i \qquad C(t) = \sum_{i=0}^{m} C_i t^i \tag{2.1.3}$$

La condició (2.1.1) pot ser expressada com a l'equació matricial $Mv = 0$ on

$$M = \begin{pmatrix} a_0 & b_0 & c_0 & 0 & \cdots & 0 & 0 & 0 \\ a_1 & b_1 & c_1 & a_0 & \cdots & 0 & 0 & 0 \\ a_2 & b_2 & c_2 & a_1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ a_n & b_n & c_n & a_{n-1} & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & a_n & \cdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a_{n-1} & b_{n-1} & c_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & a_n & b_n & c_n \end{pmatrix} \in \mathbb{K}^{(n+m+1)\times(3m+3)} \tag{2.1.4}$$

i

$$v = [A_0 B_0 C_0 \cdots A_m B_m C_m]^T \tag{2.1.5}$$

La dimensió del conjunt de solucions és de $3m + 3 - rang(M)$ i com que $rang(M) \leq n + m + 1$, aleshores hi ha com a mínim $3m + 3 - (n + m + 1) = 2m + 2 - n$ elements de $I_{1,m}$ linealment independents. □

D'aquí veiem que

Definició 2.1.7.

$$\mu = min\{m \mid I_{1,m} \neq 0\} \in \mathbb{Z}.$$

En el cas general, $\mu = \lfloor n/2 \rfloor$. Això és degut al fet que si al sistema del Lema 2.1.6 escollim $m = \lfloor n/2 \rfloor - 1$, aleshores $Mv = 0$ no té cap solució i per tant $\mu = \lfloor n/2 \rfloor$.

Amb l'objectiu de definir les μ-bases, es donen a continuació els següents resultats:

Lema 2.1.8. [3] *Si $p \in I_{1,\mu}, p \not\equiv 0$, aleshores:*

(i) p és irreductible en $\mathbb{K}[x, y, t]$.

(ii) $\exists\ q \in I_{1,n-\mu}$ per al qual $q \notin \langle p \rangle$

Demostració.

(i) Raonarem per reducció a l'absurd.

Si $p = AB$ amb $A, B \in \mathbb{K}[t]$ no constants, com que $deg_{x,y}(p) \leq 1$, aleshores $A \in \mathbb{K}[t]$ o $B \in \mathbb{K}[t]$. Si $A \in \mathbb{K}[t]$, aleshores, pel Corol·lari 2.1.4, tenim que, $p/A \in I_{1,k}$ amb $k < \mu$, però això contradiu la minimalitat de μ. Per tant, p és irreductible.

(ii) Considerem $q \in I_{1,n-\mu}$ i considerem $q \in \langle p \rangle$. Aleshores $\exists h \in \mathbb{K}[t]$ tal que $q = hp$, d'on

$$\deg(q) = \deg(h) + \deg(p) \Rightarrow \deg(h) = \deg(q) - \deg(p) \leq n - \mu - \mu \leq n - 2\mu.$$

Així, els elements de $\langle p \rangle \cap I_{1,n-\mu}$ pertanyen a un espai vectorial de dimensió $n-2\mu+1$. Tot i així, d'acord amb el Lema 2.1.6, hi ha com a mínim $n - 2\mu + 2$ elements de $I_{1,n-\mu}$ linelament independents.

□

Per tant, els polinomis p i q no poden tenir cap factor comú polinomial, ja que p és irreductible i q no és un múltiple de p.

Donats $f = c(t)x - a(t)$, $g = c(t)y - b(t)$, veiem que l'ideal generat per f, g és el mateix a l'ideal generat per p, q definits com al Lema 2.1.8.

Teorema 2.1.9. [3] *Siguin $p, q \in \mathbb{K}[t]$ definits com al Lema 2.1.8, aleshores $\langle p, q\rangle = \langle f, g\rangle$.*

Demostració.

$\boxed{\subset}$ És immediat ja que $f, g \in \langle p, q\rangle$.

$\boxed{\supset}$ És suficient demostrar que $f, g \in \langle p, q\rangle$.

Escrivim

$$p = p_x x + p_y y + p_w, \qquad q = q_x x + q_y y + q_w$$

on $p_x, p_y, p_w, q_x, q_y, q_w \in \mathbb{K}[t]$ i

$$d = mcd(a, c), \qquad e = mcd(b, c)$$

Pel Lema 2.1.3, $p_x a + p_y b + p_w c = 0$, i com que d/a i d/c, aleshores $d/p_y b$. Però ara tenim

$$mcd(a, b, c) = mcd(mcd(a, c), b) = mcd(d, b) = 1$$

Per tant, d/p_y i podem escriure

$$p_y = d\widehat{p_y}.$$

Anàlogament, podem escriure

$$p_x = e\widehat{p_x}.$$

Així, tenim

$$p = \widehat{p_x} ex + \widehat{p_y} dy + p_w$$

on $\deg(\widehat{p_x}) \leq \mu - n_e, \deg(\widehat{p_y}) \leq \mu - n_d$ i $\deg(p_w) \leq \mu$.

Anàlogament per a q, tenim

$$q = \widehat{q_x} ex + \widehat{q_y} dy + q_w$$

on $\deg(\widehat{q_x}) \leq n - \mu - n_e, \deg(\widehat{q_y}) \leq n - \mu - n_d, \deg(q_w) \leq n - \mu$.

Definim ara

$$\begin{aligned} \widetilde{f} := \widehat{p_y} q - \widehat{q_y} p = \widehat{p_y}(\widehat{q_x} ex + \widehat{q_y} dy + q_w) + \widehat{q_y}(\widehat{p_x} ex + \widehat{p_y} dy + p_w) = \\ (\widehat{p_y}\widehat{q_x} - \widehat{q_y}\widehat{p_x}) ex + (\widehat{p_y} q_w - \widehat{q_y} p_w) = \widetilde{c} ex - \widetilde{a}; \end{aligned} \tag{2.1.6}$$

$$\begin{aligned} \widetilde{g} := \widehat{q_x} p - \widehat{p_x} q = \widehat{q_x}(\widehat{p_x} ex + \widehat{p_y} dy + p_w) + \widehat{p_x}(\widehat{q_x} ex + \widehat{q_y} dy + q_w) = \\ (\widehat{p_y}\widehat{q_x} - \widehat{q_y}\widehat{p_x}) dy + (\widehat{q_x} p_w - q_w \widehat{p_x}) = \widetilde{c} dy - \widetilde{b}; \end{aligned} \tag{2.1.7}$$

on $\tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{K}[t]$ amb $\deg(\tilde{a}) \leq n - n_d, \deg(\tilde{b}) \leq n - n_e, \deg(\tilde{c}) \leq n - n_d - n_e$.

Pel Corol·lari 2.1.4 tenim que $\tilde{f}$ és un múltiple de f/d, i que $\tilde{g}$ és un múltiple de g/e. Així

$$\tilde{c}ex - \tilde{a} = \beta_1(f/d) = (\beta_1/d)(cx - a); \tag{2.1.8}$$

$$\tilde{c}dy - \tilde{b} = \beta_2(g/e) = (\beta_2/e)(cy - b); \tag{2.1.9}$$

on $\beta_1, \beta_2 \in \mathbb{K}[t]$. Comparant els coeficients de x en (2.1.8) i y en (2.1.9), tenim que $\beta_1 = \beta_2$.

Com que $n = max(n_a, n_b, n_c)$, aleshores $deg_t(f) = n$ o $deg_t(g) = n$. Suposem $deg_t(f) = n$. Aleshores $deg_t(f/d) = n - n_d$ i com que $deg_t(\tilde{f}) \leq n - n_d$, (2.1.8) implica que $\beta_1 = \beta_2$ ha de ser constant.

Si $\beta \neq 0$ aleshores $\beta_1 = \beta_2$ son escalars diferents de zero, i per (2.1.8) i (2.1.9) tenim que $f/d, g/c \in \langle p, q\rangle$, d'on $f, g, \in \langle p, q\rangle$, tal i com volíem veure.

Si $\beta_1 = 0$, aleshores tindríem que $\tilde{a} = \tilde{b} = \tilde{c} \equiv 0$ ja que $\beta_1 = \beta_2$ en (2.1.8) i (2.1.9). En $\mathbb{K}[t]$, això implica que p i q son linealment dependents:

$$h_1 p + h_2 q = 0 \tag{2.1.10}$$

per a $h_1, h_2 \in \mathbb{K}[t]$ diferents de zero. Suposem ara que h_1 i h_2 son polinomis relativament primers en $\mathbb{K}[t]$. D'aquesta manera, h_2/p, d'on, pel Corol·lari 2.1.4, tenim que $p/h_2 \in I$. Per la minimalitat de $\mu, h_2 \neq 0$ i, per tant, $q \in \langle p\rangle$, fet que és una contradicció. Per tant, $\beta_1 \neq 0$. □

Definició 2.1.10. *Els polinomis p i q del Lema 2.1.8 s'anomenen μ − base de l'ideal $I = \langle f, g\rangle$.*

Veiem un exemple on, donada una corba plana algebraica obtenim la seva μ-base.

Exemple 2.1.11. Sigui

$$(x, y) = \left(\frac{-6t^2 + 4}{-t^4}, \frac{-4t^3 + 4t}{-t^4}\right)$$

una corba plana, on

$$a(t) = -6t^2 + 4$$
$$b(t) = -4t^3 + 4t$$
$$c(t) = -t^4$$

Llavors

$$n = max(n_a, n_b, n_c) = max(2, 3, 4) = 4$$

En aquest cas, una μ-base ve donada per

$$p = 2tx + (t^2 - 2)y - 4t \qquad q = t^2x - ty - 2$$

i $\deg(p) = \mu = 2,\ \deg(q) = n - \mu = 4 - 2$

Corol·lari 2.1.12. [3] *Sigui p, q una $\mu-$base de I. Si*

$$p = p_x x + p_y y + p_w \qquad q = q_x x + q_y y + q_w$$

llavors $\exists \lambda \in \mathbb{R}, \lambda \neq 0$ tal que

$$\begin{aligned} p_x q_y - p_y q_x &= -\lambda c; \\ p_x q_w - p_w q_x &= \lambda b; \\ p_y q_w - p_w q_y &= -\lambda a. \end{aligned} \tag{2.1.11}$$

i $deg_t(p) = \mu$ i $deg_t(q) = n - \mu$.

Demostració. Sigui $\lambda = \beta_1 = \beta_2 \in \mathbb{R}, \lambda \neq 0$ amb β_1, β_2 definides com al Teorema 2.1.9 Utilitzant (2.1.7) i (2.1.9), tenim que

$$p_x q_w - p_w q_x = (e\widehat{p}_x)q_w - p_w(e\widehat{q}_x) = e(\widehat{p}_x q_w - p_w \widehat{q}_x) = e\hat{b} = e\beta_2 \frac{b}{e} = \beta_2 b = \lambda b.$$

Anàlogament obtenim que $p_x q_y - p_y q_x = -\lambda c$ i $p_y q_w - p_w q_y = -\lambda a$.

Per provar la darrera afirmació, tenim que $deg_t(p) = \mu$ per la definició de μ. Suposem que $deg_t(q) < n - \mu$. Aleshores tindríem, per (2.1.11) que $deg_t(a) < n, deg_t(b) < n, deg_t(c) < n$, fet que és impossible. Per tant, $deg_t(q) = n - \mu$. □

A continuació vegem una condició necessària per a una μ-base.

Teorema 2.1.13. [3] *Siguin p, q una $\mu-$base de $I = \langle f, g \rangle$. Aleshores, tot polinomi $P(t) = A(t)x + B(t)y + C(t) \in I$ es pot escriure de manera única de la forma*

$$Ax + By + C = h_1 p + h_2 q, \qquad h_1, h_2 \in \mathbb{K}[t].$$

A més a més, si $m = max(n_A, n_B, n_C)$, aleshores $\deg(h_1) \leq m - \mu$ *i* $\deg(h_2) \leq m + \mu - n$.

Demostració. Provarem, en primer lloc, la unicitat de h_1 i h_2. Suposem que existeixen h_1' i h_2' complint $Ax + By + C = h_1' p + h_2' q$. Aleshores, igualant les dues equacions obtenim que

$$\begin{gathered} h_1 p + h_2 q = h_1' p + h_2' q \\ (h_1 - h_1')p = (h_2 - h_2')q \\ (h_1 - h_1')p - (h_2 - h_2')q = 0 \\ h_1 - h_1' = 0 \qquad h_2 - h_2' = 0 \\ h_1 = h_1' \qquad h_2 = h_2' \end{gathered}$$

utilitzant (2.1.10).

Provem ara l'existència de h_1, h_2. Donats $h_1, h_2, h_3 \in \mathbb{K}[t]$ utilitzem el Lema 2.1.3 per escriure

$$Ax + By + C = (h_1 + yh_3)f + (h_2 - xh_3)g = h_1 f + h_2 g + h_3(bx - ay)$$

Per tant, és suficient veure que f, g i $bx - ay$ es poden expressar com a combinació de p, q amb coeficients en $\mathbb{K}[t]$. Ara, per (2.1.11), tenim que

$$\begin{aligned} p_y q - p_x p &= \lambda f \\ q_x p - p_x q &= \lambda g \\ q_x p - p_w q &= \lambda(bx - ay) \end{aligned}$$

Com que $\lambda \in \mathbb{R}, \lambda \neq 0$, obtenim el resultat desitjat.

Finalment, ens falta acotar $\deg(h_1), \deg(h_{2)}$ en termes de $\deg(A), \deg(B), \deg(C)$. L'equació $Ax + By + C = h_1 p + h_2 q$ implica que

$$\begin{aligned} A &= h_1 p_x + h_2 q_x; \\ B &= h_1 p_y + h_2 q_y; \\ C &= h_1 p_w + h_2 q_w. \end{aligned}$$

Resolent per h_1 i utilitzant (2.1.11), obtenim les fórmules

$$\begin{aligned} -\lambda c h_1 = h_1(p_x q_y - p_y q_x) &= q_y A - q_x B; \\ \lambda b h_1 = h_1(p_x q_w - p_w q_x) &= q_w A - q_x C; \\ -\lambda a h_1 = h_1(p_y q_w - p_w q_y) &= q_w B - q_y C. \end{aligned}$$

Com que $\deg(q_x), \deg(q_y), \deg(q_w) \leq n - \mu$, aleshores $\deg(-\lambda c h_1), \deg(\lambda b h_1), deg(-\lambda a h_1) \leq m + n - \mu$. Però $\lambda \neq 0$ i $n = max(n_a, n_b, n_c)$, per tant algun dels polinomis de l'esquerra té grau $\deg(h_1) + n$. Això dona la cota de $\deg(h_1)$.

Resolent per h_2 i utilitzant (2.1.11), obtenim les fórmules

$$\begin{aligned} -\lambda c h_2 = h_2(p_x q_y - p_y q_x) &= p_x A - p_y B; \\ \lambda b h_2 = h_2(p_x q_w - p_w q_x) &= p_x C - p_w A; \\ -\lambda a h_2 = h_2(p_y q_w - p_w q_y) &= p_y C - p_w B. \end{aligned}$$

Com que $\deg(p_x), \deg(p_y), \deg(p_w) \leq n - \mu$, aleshores $\deg(-\lambda c h_2), \deg(\lambda b h_2), \deg(-\lambda a h_2) \leq m + n - \mu$. Però $\lambda \neq 0$ i $n = max(n_a, n_b, n_c)$, per tant algun dels polinomis de l'esquerra té grau $\deg(h_2) + n$. Això dona la cota de $\deg(h_2)$ i acaba la demostració. □

Corol·lari 2.1.14. [3] *Sigui p, q una μ-base de $I = \langle f, g \rangle$.*

a. *Si $\mu < n - \mu$, aleshores p és únic llevat d'un múltiple escalar, i q és únic fins a un múltiple escalar més un múltiple de p per un element de $\mathbb{K}[t]$.*

b. *Si $\mu = n - \mu = n/2$, aleshores p i q poden ser qualsevol base de l'espai vectorial de dimensió 2: $I_{1,n/2}$.*

Demostració.

a. El grau ve acotat pel Teorema 2.1.13 i $\mu < n - \mu$ implica que tot element de $I_{1,\mu}$ es pot escriure de la forma $h_1 p + 0q = h_1 p$, on h_1 és constant. Pel Teorema 2.1.13 també tenim que tot element de $I_{1,n-\mu}$ és de la forma $h_1 p + h_2 q$, on $\deg(h_1) \leq n - 2\mu$ i h_2 és constant. □

Recordem que donat $I = \langle c(t)x - a(t), c(t)y - b(t) \rangle$, l'espai vectorial $I_{1,m}$ ve definit per

$$I_{1,m} = \{P(t) = A(t)x + B(t)y + C(t) \in I \mid \deg_{x,y}(P) \leq 1, \deg_t(P) \leq m\}.$$

Ara estem en condicions de calcular la dimensió del $\mathbb{K}$-espai vectorial $I_{1,m}$, que depèn de m i de μ.

Corol·lari 2.1.15.

$$\dim(I_{1,m}) = \begin{cases} 0 & si \quad 0 \leq m < \mu \\ m - \mu + 1 & si \quad \mu \leq m < n - \mu - 1 \\ 2m + 2 - n & si \quad m \geq n - \mu - 1. \end{cases}$$

Demostració.

- Si $0 \leq m < \mu$, $\dim(I_{1,m}) = 0$ per la minimalitat de μ.
- Si $\mu \leq m < n - \mu - 1$, $\dim(I_{1,m}) = m - \mu + 1$ ja que $I_{1,m}$ és un espai vectorial i, pel Corol·lari 2.1.14, tot element es pot escriure de la forma $h_1 p$ amb $\deg(h_1) < m - \mu + 1$.
- Si $n - \mu - 1 \leq m$, $\dim(I_{1,m}) = 2m + 2 - n$ ja que tenim polinomis de la forma $h_1 p + h_2 q$ amb $\deg(h_1) \leq m - \mu$ i $\deg(h_2) \leq m + \mu - n$. Per la unicitat provada al Teorema 2.1.13 tenim que

$$\dim(I_{1,m}) = (m - \mu + 1) + (m + \mu - n) = 2m + 1 - n + 1 = 2m + 2 - n.$$

□

2.2 Mòdul de syzigies

La paraula syzigia s'utilitza en astronomia per indicar un alineament de tres planetes o altres cossos celestes. L'arrel és una paraula grega que significa "unir". En una syzigia matemàtica, direm que els polinomis estan "units", fent referència a com s'utilitzaria en el camp de l'astronomia.

Fins al moment, hem tractat amb polinomis de la forma

$$I_{1,*} = \{A(t)x + B(t)y + C(t); A(t), B(t), C(t) \in \mathbb{K}[t]\} \cap I.$$

Com que $I = \langle f, g \rangle$ és un ideal a l'anell de polinomis $\mathbb{K}[x, y, t]$, el conjunt $I_{1,*}$ és tancat per la suma i per la multiplicació per elements arbitraris de $\mathbb{K}[t]$. Per tant, $I_{1,*}$ és un mòdul sobre l'anell de polinomis $\mathbb{K}[t]$.

Modificant el procediment per a trobar bases de Gröbner $G = \{g_1, \ldots, g_s\}$ per a un ideal $I \subset \mathbb{K}$ utilitzant l'algoritme de Bubhberger, podrem trobar generadors per al mòdul de syzigies $Syz(g_1, \ldots, g_s)$.

Proposició 2.2.1. [4] *Sigui $(f_1, \ldots, f_s)$ un conjunt ordenat d'elements de $\mathbb{K}[x_1, \ldots, x_n]$. El (primer) mòdul de syzygies*

$$Syz(f_1, \ldots, f_s) = \{(g_1, \ldots, g_s), g_i \in \mathbb{K}[x_1, \ldots, x_n] \quad | \quad g_1 f_1 + \cdots + g_s f_s = 0\}$$

és un submòdul de $\mathbb{K}[x_1, \ldots, x_n]^s$.

Demostració. Siguin $(a_1, \ldots, a_s), (b_1, \ldots, b_s) \in Syz(f_1, \ldots, f_s)$ i $c \in \mathbb{K}$. Aleshores

$$\begin{array}{l} a_1 f_1 + \ldots + a_s f_s = 0 \\ b_1 f_1 + \ldots + b_s f_s = 0 \end{array} \Rightarrow \begin{array}{c} ca_1 f_1 + \ldots + ca_s f_s = 0 \\ b_1 f_1 + \ldots + b_s f_s = 0 \end{array} \Rightarrow (ca_1 + b_1) f_1 + \ldots + (ca_s + b_s) f_s = 0$$

d'on $(ca_1 + b_1, \ldots, ca_s + b_s) \in Syz(f_1, \ldots, f_s)$ i per tant $Syz(f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]^s$.

□

Tenim que $Syz(f_1, \ldots, f_s)$ és un mòdul sobre $\mathbb{K}[x_1, \ldots, x_n]$, ja que les syzigies poden multiplicar-se i sumar-se per elements de $\mathbb{K}[x_1, \ldots, x_n]$. A més a més tenim

$$Syz(f_1, \ldots, f_s) \subset \mathbb{K}^s[x_1, \ldots, x_n]$$

i el mòdul de syzigia és un submòdul d'un mòdul lliure. Tot i això, en general, el mòdul de syzigia (ni tampoc qualsevol altre submòdul d'un mòdul lliure) no és lliure.

Veiem ara dos exemples que relacionen l'equació (2.0.1) i el Lema 2.1.3 amb els mòduls de syzigies.

Exemple 2.2.2. Notem que de la parametrització (2.0.1)

$$(x, y) = \left(\frac{a(t)}{c(t)}, \frac{b(t)}{c(t)} \right)$$

tenim que $a(t), b(t), c(t) \in \mathbb{K}[t]$. Per tant el mòdul $Syz(a, b, c)$ està format per tots els triplets de polinomis $(A(t), B(t), C(t)) \in \mathbb{K}[t]^3$ tals que

$$Syz(a, b, c) = \{(A(t), B(t), C(t)) \in \mathbb{K}[t]^3 \ | \ A(t)a(t) + B(t)b(t) + C(t)c(t)\} \equiv 0$$

d'on

$$I_{1,*} \simeq Syz(a, b, c).$$

2.3 Estructura de les parametritzacions amb classe μ

Amb l'objectiu de tenir una idea de la "quantitat" de parametritzacions hi ha per una $\mu - classe$, calcularem la dimensió de totes les parametritzacions racionals amb classe μ.

Sigui

$$\mathbb{K}[t]_n = \{P(t) \mid deg(P(t)) \leq n\}$$

un espai vectorial de dimensió $n+1$. Definim

$$\mathcal{P}_n = \{(a,b,c) \in \mathbb{K}[t]_n^3 \mid mcd(a,b,c) = 1,\ n = max(n_a, n_b, n_c),\ c \neq 0\}$$

Siguin $\mathcal{P}_n^\mu \subset \mathcal{P}_n$ les parametritzacions amb classe μ. Volem determinar l'estructura d'aquest conjunt.

Podem descriure subconjunts de $\mathcal{P}_n$ utilitzant equacions algebraiques. Definim abans la clausura de Zariski d'una varietat algebraica.

Definició 2.3.1. [4] *La clausura de Zariski és la varietat algebraica més petita contenint al conjunt. Si $S \subseteq \mathbb{K}^n$, denotem per $\overline{S}$ la clausura de Zariski de S i*

$$V(I(S)) = \overline{S}$$

D'aquí veiem la relació entre $\mathcal{P}_n^\mu$ i $\overline{\mathcal{P}}_n^\mu$. Enunciem abans, sense demostració, un teorema previ:

Teorema 2.3.2. [6] *Si $f : X \to Y$ és una aplicació regular entre varietats irreductibles amb $f(X) = Y, \dim(X) = n, \dim(Y) = m$, aleshores $m \leq n$ i*

(i) $\dim(f^{-1}(y)) \geq n - m$ *per a tot punt $y \in Y$.*

(ii) Existeix $U \subset Y, Y \neq \emptyset$ tal que $f^{-1}(y) = n - m$ amb $y \in U$.

Teorema 2.3.3. [3] *Siguin $\mathcal{P}_n^\mu \subset \mathcal{P}_n$ el conjunt de totes les parametritzacions de classe μ i $\overline{\mathcal{P}}_n^\mu$ la seva clausura de Zariski. Aleshores*

(i) Per a cada $0 \leq \mu \leq \lfloor n/2 \rfloor$, $\overline{\mathcal{P}}_n^\mu$ és una varietat irreductible de $\mathcal{P}_n$ i

$$dim(\overline{\mathcal{P}}_n^\mu) = \begin{cases} 3n+3 & \mu = \lfloor n/2 \rfloor \\ 2n + 2\mu + 4 & \mu < \lfloor n/2 \rfloor. \end{cases}$$

(ii) Per a tot μ, existeix $\mathcal{W}^\mu \subset \overline{\mathcal{P}}_n^\mu$ tal que

$$\mathcal{P}_n^\mu = \overline{\mathcal{P}}_n^\mu - \mathcal{W}^\mu$$

i $\mathcal{W}^\mu \neq \overline{\mathcal{P}}_n^\mu$. Direm que $\mathcal{P}_n$ és el complementari en $\overline{\mathcal{P}}_n^\mu$ d'una varietat pròpia.

Demostració.

(i) Sigui $\mu < \lfloor n/2 \rfloor$. Considerem l'aplicació

$$\begin{array}{rccc} \Phi: & \mathbb{K}[t]^3_\mu \times \mathbb{K}[t]^3_{n-\mu} & \to & \mathbb{K}[t]^3_n \\ & (p,q) = (p_x,\ p_y,\ p_z,\ q_x,\ q_y,\ q_z) & \mapsto & (p_w q_y - p_y q_w,\ p_x q_w - p_w q_x,\ p_y q_x - p_x q_y) \end{array}$$

Sigui $U = \Phi^{-1}(\mathcal{P}_n) \subset \mathbb{K}[t]^3_\mu \times \mathbb{K}[t]^3_{n-\mu}$. Aleshores tenim l'aplicació

$$\Phi_{|U} : U \to \mathcal{P}_n \tag{2.3.1}$$

Veiem ara que la imatge de Φ és $\mathcal{P}_n^\mu$.

$\boxed{\Rightarrow}$ Si $(a,b,c) \in \mathcal{P}_n^\mu$ i p, q son una μ-base de $\langle cx - a,\ cy - b\rangle$, aleshores per (2.1.11) tenim que

$$\Phi(p,q) = (p_w q_y - p_y q_w,\ p_x q_w - p_w q_x,\ p_y q_x - p_x q_y) = (-(-\lambda a),\ \lambda b,\ -(-\lambda c)) = \lambda(a,b,c)$$

d'on $(a,b,c) \in \Phi(p,q)$.

$\boxed{\Leftarrow}$ Sigui (p,q) tal que $\Phi(p,q) = (a,b,c) \in \mathcal{P}_n$, μ' la classe de (a,b,c) i $I = \langle cx - a,\ cy - b\rangle$.

Tenim, en primer lloc que

$$ap_x + bp_y + cp_w = p_x p_w q_y - p_x p_y q_w + p_y p_x q_w - p_y p_w q_x + p_w p_y q_x - p_w p_x q_y = 0$$

de la definició de Φ i, per tant, $p \in I$ pel Lema 2.1.3. Com que $p \in I_{1,\mu}$, aleshores $\mu' \leq \mu$. Si tinguéssim $\mu' < \mu < \lfloor n/2 \rfloor$, aleshores, pel Teorema 2.1.13 tindríem que existeix $h \in \mathbb{K}[t],\ deg_t(h) > 0$ tal que

$$p = p'h$$

i, per tant,

$$\Phi(p,q) = \Phi(p'h, q) = (a,b,c)$$

també és múltiple de h. Però

$$(a,b,c) \in \mathcal{P}_n \Rightarrow mcd(a,b,c) = 1$$

fet que és una contradicció. D'aquí tenim que $\mu' = \mu$ i per tant

$$(a,b,c) \in \mathcal{P}_n^\mu$$

D'aquí tenim que

$$\Phi(U) = \mathcal{P}_n^\mu$$

Com que $\mathcal{P}_n^\mu \subset \overline{\mathcal{P}}_n^\mu$ tenim que podem escriure

$$\Phi : U \to \overline{\mathcal{P}}_n^\mu$$

i, per tant, com que U és irreductible, aleshores la clausura de Zariski $\overline{\mathcal{P}}_n^\mu$ també ho és.

Veiem ara que

$$\dim(\overline{\mathcal{P}}_n^\mu) = 2n + 2\mu + 4.$$

Siguin $(a,b,c) \in \mathcal{P}_n^\mu$ i el conjunt

$$\Phi^{-1}(a,b,c) = \{(p,q) \in \mathbb{K}[t]_\mu \times \mathbb{K}[t]_{n-\mu} : \ \Phi(p,q) = (a,b,c)\}$$

que anomenarem fibra de Φ.

Per la primera part de la demostració, tenim que

$$\Phi^{-1}(a,b,c) = \{\mu - \textit{bases } p,q \textit{ de } I \textit{ amb } \lambda = 1 \textit{ en } (2.1.11)\}$$

Afirmació 2.3.4. *Fixat $(p,q) \in \Phi^{-1}(a,b,c)$, existeix un altre parell $(p',q') \in \mathbb{K}[t]_\mu^3 \times \mathbb{K}[t]_{n-\mu}^3$ tal que*

$$(p',q') \in \Phi^{-1}(a,b,c) \iff p' = \alpha p \ \ i \ \ q' = \frac{1}{\alpha}q + hp.$$

per a algun $\alpha \in \mathbb{K} - \{0\}$ i $h \in \mathbb{K}[t]_{n-2\mu}$.

Demostració.

$\boxed{\Leftarrow}$ Siguin $p' = \alpha p, \ q' = \frac{1}{\alpha}q + hq$. Aleshores

$$\Phi(p',q') = \Phi\left(\alpha p, \ \frac{1}{\alpha}q + hq\right) = \Phi(p,q) = (a,b,c)$$

ja que

$$p'_w q'_y - p'_y q'_w = \alpha p_w \left(\frac{1}{\alpha}q_y + hp_y\right) - \alpha p_y \left(\frac{1}{\alpha}q_w + hp_w\right) = p_w q_y - p_y q_w$$

$$p'_x q'_w - p'_w q'_x = \alpha p_x \left(\frac{1}{\alpha}q_w + hp_w\right) - \alpha p_w \left(\frac{1}{\alpha}q_x + hp_x\right) = p_x q_w - p_w q_x$$

$$p'_y q'_x - p'_x q'_y = \alpha p_y \left(\frac{1}{\alpha}q_x + hp_x\right) - \alpha p_x \left(\frac{1}{\alpha}q_y + hp_y\right) = p_y q_x - p_x q_y$$

$\boxed{\Rightarrow}$ Si $\Phi(p',q') = (a,b,c)$, aleshores, per la primera part de la demostració, p', q' son una μ-base de I. Aleshores, pel Corol·lari 2.1.14 tenim que es compleix

$$p' = \alpha p$$
$$q' = \frac{1}{\alpha}q + hp.$$

amb $\deg(p') < \mu$ i $\deg(q') < (n-2\mu) + \mu = n - \mu$.

□

Del Corol·lari 2.1.15 tenim que

$$\dim\left(\Phi^{-1}(a,b,c)\right) = (\mu - \mu + 1) + (n - \mu - \mu + 1) = n - 2\mu + 2.$$

ja que $\alpha \in \mathbb{K} - \{0\}$ i $h \in \mathbb{K}_{n-2\mu}$.

Hem vist a la primera part de la demostració que $\Phi(U) = \mathcal{P}_n^\mu$ i $\overline{\mathcal{P}}_n^\mu$ és irreductible. En tal cas, se satisfan les hipòtesis del Teorema 2.3.2 i per tant

$$\begin{aligned}\dim(\overline{\mathcal{P}}_n^\mu) &= \dim(U) - \dim(\Phi^{-1}(a,b,c)) = (3(\mu+1) + 3(n-\mu+1)) - (n - 2\mu + 2)) \\ &= 2n + 2\mu + 4.\end{aligned}$$

(ii) Per a la segona part de la demostració, sigui el conjunt de totes les parametritzacoins de classe $\leq \mu$:

$$\widetilde{\mathcal{P}}_n^\mu = \mathcal{P}_n^0 \amalg \mathcal{P}_n^1 \amalg \cdots \amalg \mathcal{P}_n^\mu. \tag{2.3.2}$$

Afirmació 2.3.5. *$\widetilde{\mathcal{P}}_n$ és una varietat de $\mathcal{P}_n$*

Demostració. Per la primera part de la demostració, sabem que (a,b,c) és de classe $\leq \mu$ si, i només si, $I_{1,\mu} \neq 0$. Com que

$$n + \mu + 1 > 3\mu + 3$$

i pel Lema 2.1.6 tenim que es compleix quan $rang(M) < 3\mu+3$, fet que és impossible ja que $\mu < \lfloor n/2 \rfloor$. Per tant, $(a,b,c) \in \widetilde{\mathcal{P}}_n$ si, i només si, $rang(M) < 3\mu + 3$ i d'aquí obtenim que $\widetilde{\mathcal{P}}_n$ ve definida per equacions i per tant és una varietat de $\mathcal{P}_n$. □

De l'equació (2.3.2) tenim que

$$\mathcal{P}_n^\mu \subset \widetilde{\mathcal{P}}_n^\mu = \mathcal{P}_n^0 \amalg \mathcal{P}_n^1 \amalg \cdots \amalg \mathcal{P}_n^\mu = \widetilde{\mathcal{P}}_n^{\mu-1} \amalg \mathcal{P}_n^\mu$$

i també, de la definició de clausura de Zariski tenim que

$$\overline{\mathcal{P}_n^\mu} \subset \widetilde{\mathcal{P}}_n^{\mu-1} \amalg \mathcal{P}_n^\mu$$

Per tant,

$$\overline{\mathcal{P}_n^\mu} = \mathcal{P}_n^\mu \amalg (\widetilde{\mathcal{P}}_n^{\mu-1} \cap \overline{\mathcal{P}_n^\mu})$$

i, per tant $\mathcal{P}_n^\mu$ és el complementari en $\overline{\mathcal{P}_n^\mu}$ de $\widetilde{\mathcal{P}}_n^{\mu-1} \cap \overline{\mathcal{P}_n^\mu}$ tal i com volíem veure.

Provem ara el teorema per a $\mu = \lfloor n/2 \rfloor$. En tal cas tenim, anàlogament a (2.3.2)

$$\mathcal{P}_n = \mathcal{P}_n^0 \amalg \ldots \amalg \mathcal{P}_n^{\lfloor n/2 \rfloor} = \widetilde{\mathcal{P}}_n^{\lfloor n/2 \rfloor - 1} \amalg \mathcal{P}_n^{\lfloor n/2 \rfloor} \tag{2.3.3}$$

i, per la primera part de la demostració, $\widetilde{\mathcal{P}}_n^{\lfloor n/2 \rfloor - 1}$ és una varietat pròpia de $\mathcal{P}_n$. Finalment, tenim que $\deg(\overline{\mathcal{P}}_n) = 3n + 3$. □

Aquest teorema dona informació sobre l'estructura de $\mathcal{P}_n^\mu$, però no explica la unió entre aquests $\mathcal{P}_n^\mu$. De fet, tenim la següent conjectura:

Conjectura 2.3.6. [3] *La clausura de Zariski $\overline{\mathcal{P}}_n^\mu$ ve donada per*

$$\overline{\mathcal{P}}_n^\mu = \mathcal{P}_n^0 \cup \ldots \cup \mathcal{P}_n^\mu.$$

Capítol 3

Implicitació

Amb l'objectiu de descriure varietats $\mathbb{V} \in \mathbb{K}^n$, estudiarem a continuació el problema d'implicitació.

Tot i el coneixement de la implicitació matemàtica des de fa molts segles, no va ser fins al segle XVII quan René Descartes a la seva obra "La Géométrie" va obrir la porta a la representació d'equacions en forma implícita. Durant el segle XVIII, el matemàtic alemany Leonard Euler (1707-1783) va treballar en la teoria de funcions i equacions diferencials, on les equacions implícites tenien un paper fonamental. Durant el segle XIX, el concepte es va anar desenvolupant gràcies a matemàtics com Augustin-Louis Cauchy (1789-1857), Bernhard Riemann (1826-1866) i Karl Wierestrass (1815-1897). Al segle passat, ja amb un camp de les matemàtiques més avançat, la teoria de conjunts, la topologia i l'àlgebra abstracta van jugar un paper important en l'estudi de les solucions d'equacions implícites en contextos més generals.

La gran importància de convertir varietats definides paramètricament a varietats definides implícitament (i viceversa) és deguda a que cadascuna d'elles és adient per a un tipus de problema. Per exemple, és preferible usar la representació paramètrica per a generar punts d'una varietat, però és millor utilitzar la representació implícita per determinar si un punt és o no a una varietat. A més a més, tota corba racional parametritzada es pot escriure de forma implícita; però no tota corba implícita té una parametrització racional.

Estudiarem a continuació l'equació implícita $h(x, y) = 0$ de la corba parametritzada (2.0.1).

Lema 3.0.1. [3] *Si* $h \in \mathbb{K}[x, y, t]$ *i* $ch \in I = \langle cx - a, cy - b \rangle$, *aleshores* $h \in I$.

Demostració. Si existeixen $P, Q \in \mathbb{K}[x, y, t]$ tals que

$$ch = P(cx - a) + Q(cy - b)$$

aleshores

$$ch - P(cx - a) - Q(cy - b) = aP + bQ + c(h - xP - yQ) = 0$$

i, pel Lema 2.1.2, existeixen $H_1, H_2, H_3 \in \mathbb{K}[x,y,t]$ tals que

$$\begin{aligned} P &= aH_1 + bH_3; \\ Q &= cH_2 - aH_3; \\ h - xP - yQ &= -aH_1 - bH_2. \end{aligned}$$

Per tant de la darrera igualtat obtenim

$$\begin{aligned} h = xP + yQ - aH_1 - bH_2 = x(aH_1 + bH_3) + y(cH_2 - aH_3) - aH_1 - bH_2 = \\ (H_1 + yH_3)(cx - a) + (H_2 - xH_3)(cy - b). \end{aligned}$$

d'on $h \in I$. □

Lema 3.0.2. *$I = \langle cx - a, cy - b \rangle$ és un ideal primer.*

Demostració. Definim l'homeomorfisme d'anells

$$\begin{array}{rccc} \alpha: & \mathbb{K}[x,y,t] & \to & \mathbb{K}(t) \\ & x & \mapsto & \frac{a(t)}{c(t)} \\ & y & \mapsto & \frac{b(t)}{c(t)} \\ & t & \mapsto & t \end{array}$$

Com que $\mathbb{K}(t)$ és un domini d'integritat, aleshores $\ker(\alpha)$ és un ideal primer; i per tant, només cal veure que $I = \ker(\alpha)$.

$\boxed{\subseteq}$ Pel Lema 2.1.3 tenim que $I \in \ker(\alpha)$, i per tant, $I \subset \ker(\alpha)$.

$\boxed{\supseteq}$ Sigui ara $h(x,y,t) \in ker(\alpha)$, per tant

$$h\left(\frac{a}{c}, \frac{b}{c}, t\right) = 0 \quad \in \mathbb{K}(t)$$

Utilitzant l'Algoritme de divisió, si dividim $h(x,y,t)$ per $x - \frac{a}{c}$ i $y - \frac{b}{c}$ en $\mathbb{K}[x,y]$, obtenim

$$h = \tilde{P}\left(x - \frac{a}{c}\right) + \tilde{Q}\left(y - \frac{b}{c}\right) + h\left(\frac{a}{c}, \frac{b}{c}, t\right) = \tilde{P}\left(x - \frac{a}{c}\right) + \tilde{Q}\left(y - \frac{b}{c}\right).$$

Com que els denominadors de $\tilde{P}$ i $\tilde{Q}$ son únicament potències de c, multiplicant per una potència adequada de c, c^N, obtenim

$$c^N = P(cx - a) + Q(cy - b).$$

amb $P, Q \in \mathbb{K}[x,y,t]$. D'aquí obtenim que $c^N h \in I$, i pel Lema 3.0.1 tenim que $h \in I$.

□

3.1 Implicitació polinòmica

Comencem a estudiar el problema d'implicitació amb el cas en què tinguem una parametrització polinòmica de la forma

$$\begin{aligned} x_1 &= f_1(t_1,\dots,t_m) \\ &\vdots \\ x_n &= f_n(t_1,\dots,t_m) \end{aligned} \tag{3.1.1}$$

amb $f_1,\dots,f_n \in \mathbb{K}[t_1,\dots,t_m]$.

Considerem la varietat $V = \mathbb{V}(x_1 - f_1,\dots,x_n - f_n) \subseteq \mathbb{K}^{m+n}$, els punts de la qual son la imatge de l'aplicació i:

$$\begin{array}{rccc} i: & \mathbb{K}^m & \to & \mathbb{K}^{m+n} \\ & t_1,\dots,t_m & \mapsto & (t_1,\dots,t_m, f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)) \end{array}$$

Aleshores considerem el següent diagrama commutatiu:

$$\begin{array}{ccc} & \mathbb{K}^{m+n} & \\ {\scriptstyle i}\nearrow & & \searrow{\scriptstyle \pi_m} \\ \mathbb{K}^m & \xrightarrow{\quad F \quad} & \mathbb{K}^n \end{array} \tag{3.1.2}$$

d'on

$$F(\mathbb{K}^m) = \pi_m(i(\mathbb{K}^m) = \pi_m(V). \tag{3.1.3}$$

ja que $i(\mathbb{K}^m) = V$.

En aquest lema utilitzem la idea que l'eliminació correspon a projectar una varietat sobre un subespai de menor dimensió.

Lema 3.1.1. [2] *Sigui $I_1 = \langle f_1,\dots,f_s\rangle \cap \mathbb{K}[x_{l+1},\dots,x_n]$ l'l-èssim ideal d'eliminació. Considerem la projecció*

$$\begin{array}{rccc} \pi_l: & \mathbb{K}^n & \to & \mathbb{K}^{n-1} \\ & (a_1,\dots,a_n) & \mapsto & (a_{l+1},\dots,a_n) \end{array}$$

Aleshores

$$\pi_l(V) \subseteq V(I_l).$$

Teorema 3.1.2 (Implicitació polinòmica)**.** [2] *Siguin $\mathbb{K}$ un cos infinit i*

$$\begin{array}{rccc} F: & \mathbb{K}^m & \to & \mathbb{K}^n \\ & t_1,\dots,t_m & \mapsto & (f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)). \end{array}$$

l'aplicació definida per la parametrització polinòmica. Siguin $I = \langle x_1 - f_1,\dots,x_n - f_n\rangle \subseteq \mathbb{K}[t_1,\dots,t_m,x_1,\dots,x_n]$ un ideal i

$$I_m = I \cap \mathbb{K}[x_1,\dots,x_n]$$

l'm-èssim ideal d'eliminació. Aleshores $V(I_m) \subset \mathbb{K}^n$ és la varietat més petita que conté a $F(\mathbb{K}^m)$.

Demostració. Pel Lema 3.1.1 i l'equació (3.1.3), tenim que

$$F(\mathbb{K}^m) = \pi_m(V) \subseteq V(I_m).$$

Veiem ara que $V(I_m)$ és la varietat més petita que conté a $F(\mathbb{K}^m)$. Suposem que $h \in \mathbb{K}[x_1, \ldots, x_n]$ s'anul·la en $F(\mathbb{K}^m)$ i volem veure que $h \in I_m$.

Si $h \in \mathbb{K}[t_1, \ldots, t_m, x_1, \ldots, x_n]$, aleshores, utilitzant l'Algoritme de divisió teo:q233 amb l'ordre lexicogràfic $x_1 > \ldots > x_n > t_1 > \ldots > t_m$ obtenim que

$$h(x_1, \ldots, x_n) = q_1(x_1 - f_1) + \ldots + q_n(x_n - f_n) + r(t_1, \ldots, t_m) \tag{3.1.4}$$

Volem veure ara que $r = 0$. Prenem $(a_1, \ldots, a_m) \in \mathbb{K}^m$ i escrivim $x_i = f_i(a_1, \ldots, a_m)$. Aleshores

$$0 = h(f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m)) = 0 + \ldots + 0 + r(a_1, \ldots, a_m).$$

Per tant, com que $\mathbb{K}$ és un cos infinit, tenim que r és un polinomi nul. D'aquí obtenim que

$$h(x_1, \ldots, x_n) \in I \cap \mathbb{K}[x_1, \ldots, x_n] = I_m.$$

Per veure que és minimal, suposem que existeix un altre $Z = \mathbb{V}(h_1, \ldots, h_s) \subseteq \mathbb{K}^n$ amb $F(\mathbb{K}^m) \subseteq Z$. Aleshores per la primera part de la demostració

$$\mathbb{V}(I_m) \subseteq \mathbb{V}(h_1, \ldots, h_s)$$

d'on es prova la minimalitat de $\mathbb{V}(I_m)$. □

3.2 Implicitació racional

En el cas general de la parametrització racional tenim,

$$\begin{aligned} x_1 &= \tfrac{f_1(t_1,\ldots,t_m)}{g_1(t_1,\ldots,t_m)} \\ &\vdots \\ x_n &= \tfrac{f_n(t_1,\ldots,t_m)}{g_n(t_1,\ldots,t_m)} \end{aligned} \tag{3.2.1}$$

amb $f_i, g_i \in \mathbb{K}[t_1, \ldots, t_m]$ $\forall i = 1, \ldots, n$. Una primera idea per a abordar aquest problema és eliminar els denominadors i utilitzar el mateix mètode que la implicitació polinòmica, però sovint aquest argument no funciona.

L'aplicació

$$F : \mathbb{K}^m \to \mathbb{K}^n$$

definida per (3.2.1) podria no estar ben definida per a tot $\mathbb{K}^m$ si els denominadors s'anul·lessin, però prenent $W = \mathbb{V}(g_1 g_2 \dots g_n) = \mathbb{V}(g) \subseteq \mathbb{K}^m$, aleshores

$$F(t_1, \dots, t_m) = \left(\frac{f_1(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}, \dots, \frac{f_n(t_1, \dots, t_m)}{g_n(t_1, \dots, t_m)} \right)$$

defineix l'aplicació

$$F : \mathbb{K}^m \backslash W \to \mathbb{K}^n$$

que està ben definida ja que W és el conjunt de tots els punts en els que algun dels denominadors s'anul·la.

El problema d'implicitació es tradueix, doncs, en trobar la menor varietat afí de $\mathbb{K}^n$ que contingui $F(\mathbb{K}^m \backslash W)$.

Enunciem ara, sense demostració, el teorema per a determinar aquesta varietat minimal.

Teorema 3.2.1. [2] *Donat $\mathbb{K}$ un camp infinit, sigui*

$$F : \mathbb{K}^m \setminus W \to \mathbb{K}^n$$

la funció determinada per (3.2.1). Sigui l'ideal

$$J = \langle g_1 x_1 - f_1, \dots, g_n x_n - f_n, 1 - gy \rangle \subseteq \mathbb{K}[y, t_1, \dots, t_m, x_1, \dots, x_n]$$

Sigui també

$$J_{m+1} = J \cap \mathbb{K}[x_1, \dots, x_n]$$

el $(1+m)$-è ideal d'eliminació. Aleshores $\mathbb{V}(J_{1+m})$ és la menor varietat en $\mathbb{K}^n$ que conté $F(\mathbb{K}^m \setminus W)$.

Donada l'equació paramètrica d'una corba racional plana, tenim la següent caracterització:

Lema 3.2.2. *L'equació implícita $h(x, y) = 0$ de (2.0.1) és irreductible amb $\deg(h) | n$, i $I \cap \mathbb{K}[x, y] = \langle h \rangle$.*

Demostració. Sigui l'ideal

$$J = \langle cx - a, cy - b, cu - 1 \rangle \subset \mathbb{K}[x, y, u, t].$$

Pel Torema 3.2.1 tenim que l'ideal $J \cap \mathbb{K}[x, y]$ dona l'equació que defineix la corba 2.0.1.

La demostració del Lema 3.0.2 pot adaptar-se prenent

$$I = \langle cx - a, cy - b \rangle = \langle cx - a, cy - b, cu - 1 \rangle \cap \mathbb{K}[x, y, t] = J \cap \mathbb{K}[x, y, t]$$

Per tant,

$$I \cap \mathbb{K}[x, y] = J \cap \mathbb{K}[x, y, t] \cap \mathbb{K}[x, y] = J \cap \mathbb{K}[x, y]$$

Com que I és primer, $I \cap \mathbb{K}[x,y] = \langle h \rangle$ és primer, i per tant h és irreductible.

Resta veure que $\deg(h) | \ n$. Sigui

$$C = V(h) \subset \mathbb{K}^2$$

una corba algebraica i prenem l'aplicació

$$F(x,y) = \lambda_1 x + \lambda_2 y$$

Aleshores

$$F_{|C} : C \to \mathbb{K}$$

és una aplicació de grau $\deg(h)$. Si prenem l'aplicació

$$\begin{array}{rccc} G: & \mathbb{K} & \to & C \\ & t & \mapsto & \left(\frac{a(t)}{c(t)}, \frac{b(t)}{c(t)}\right) \end{array}$$

tenim que la composició

$$F_{|C} \circ G : \mathbb{K} \to \mathbb{K}$$

té grau n. Com que n és producte de $\deg(F_{|C})$ i $\deg(G)$, tenim que $\deg(F_{|C}) = \deg(h)$ divideix n. □

3.2.1 Resultants

Recordem, en primer lloc, l'estructura de la matriu de Sylvester, que rep aquest nom en honor al matemàtic anglès James Joseph Sylvester (1814-1897).

Definició 3.2.3. *Siguin*

$$\begin{aligned} p &= p_0 + p_1 z + p_2 z^2 + \ldots + p_m z^m \\ q &= q_0 + q_1 z + q_2 z^2 + \ldots + q_n z^n \end{aligned}$$

amb $\deg(p) = m, \deg(q) = n$. *Aleshores la matriu de Sylvester associada a* p *i* q *és*

$$Syl(p,q) = \begin{pmatrix} p_m & p_{m-1} & \cdots & p_1 & p_0 & & & \\ & p_m & p_{m-1} & \cdots & p_1 & p_0 & & \\ & & \ddots & \ddots & & \ddots & \ddots & \\ & & & p_m & p_{m-1} & \cdots & p_1 & p_0 \\ q_n & q_{n-1} & \cdots & q_1 & q_0 & & & \\ & q_n & q_{n-1} & \cdots & q_1 & q_0 & & \\ & & \ddots & \ddots & & \ddots & \ddots & \\ & & & q_n & q_{n-1} & \cdots & q_1 & q_0 \end{pmatrix} \in \mathbb{K}^{(n+m)\times(n+m)}$$

que va aparèixer per primera vegada en un article de Sylvester l'any 1840.

Introduïm ara el concepte de resultants, ja que trobem moltes aplicacions on aquest mètodes és molt més eficient que altres mètodes utilitzant bases de Gröbner. El concepte de les resultants està estretament relacionat amb el de la matriu de Sylvester, ja que el determinant d'aquesta matriu és el valor de la seva resultant, que val 0 quan els dos polinomis tenen alguna arrel en comú (en un cos) o un comú divisor no constant (en el cas d'un domini d'integritat).

Definició 3.2.4. *Donats dos polinomis $h_1, h_2 \in \mathbb{K}[x, y, t]$, la resultant de h_1 i h_2 respecte t ve donada pel producte*

$$Res(h_1, h_2, t) := Res(h_1, h_2) = \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

on α_i, β_j son les arrels de h_1, h_2, respectivament.

Teorema 3.2.5. [3] *Sigui p, q una μ-base per $I = \langle cx - a, cy - b \rangle$. Aleshores, existeix $\lambda \neq 0 \in \mathbb{R}$ tal que*

$$\tilde{h} = Res(p, q) = \lambda h^{n/\deg(h)}$$

Demostració. Si escrivim $\tilde{h}$ com el determinant de la matriu de Sylvester per a polinomis de grau μ i $n - \mu$ en t, aleshores $\tilde{h} = Res_{\mu, n-\mu}(p, q) \in \mathbb{K}[x, y]$, i per $(x_0, y_0) \in \mathbb{K}^2$, tenim que

$$\tilde{h} = Res_{\mu, n-\mu}\left(p(x_0, y_0, t), q(x_0, y_0, t)\right)$$

Per les propietats de les resultants tenim que

$$\tilde{h}(x_0, y_0) = 0 \iff \begin{array}{cc} p(x_0, y_0, t_0) = q(x_0, y_0, t_0) = 0 & (i) \\ o & \\ \deg(p(x_0, y_0, t)) < \mu,\ \deg(q(x_0, y_0, t)) < n - \mu & (ii) \end{array}$$

(i) Com que $(x_0, y_0, t_0) \in \mathbb{V}(p, q) = \mathbb{V}(t)$, aleshores $h(x_0, y_0) = 0$.

(ii) Tenim

$$(x_0, y_0, 1)(p_{x,\mu}, p_{y,\mu}, p_{w,\mu}) = (x_0, y_0, 1)(q_{x,n-\mu}, q_{y,n-\mu}, q_{w,n-\mu}) = 0 \tag{3.2.2}$$

on $p_{x,\mu}$ és el coficient de t^μ en p_x. Els vectors $(p_{x,\mu}, p_{y,\mu}, p_{w,\mu})$ i $(q_{x,n-\mu}, q_{y,n-\mu}, q_{w,n-\mu})$ son linealment independents. Si no ho fossin, tindríem que

$$\det \begin{pmatrix} p_{x,\mu} & q_{x,n-\mu} \\ p_{y,\mu} & q_{y,n-\mu} \\ p_{w,\mu} & q_{w,n-\mu} \end{pmatrix} = 0. \tag{3.2.3}$$

això implicaria que $\deg(a), \deg(b), \deg(c) < n$, fet que ja hem vist al Corol·lari 2.1.12 que és impossible.

D'aquesta manera tenim que els vectors son linealment independents , i per tant de (3.2.2) tenim que $(x_0, y_0, 1)$ ha de ser un múltiple escalar dels seus productes creuats. Pel Corol·lari 2.1.12 tenim que

$$(x_0, y_0) = \left(\frac{a_n}{c_n}, \frac{b_n}{c_n}\right)$$

on a_n, b_n, c_n son els coficients de t^n en a, b, c, respectivament. Aquest és el punt de $h(x, y) = 0$ corresponent a $t = \infty$, d'on $h(x_0, y_0) = 0$.

Hem vist, per tant, que

$$\tilde{h}(x_0, y_0) = 0 \Rightarrow h(x_0, y_0) = 0$$

i per tant $\mathbb{V}(\tilde{h}) \subset \mathbb{V}(h)$. Com que h és irreductible, tenim que $\mathbb{V}(\tilde{h}) = \mathbb{V}(h)$ i per tant $\tilde{h}$ és potència de h.

Només falta veure que $\deg(\tilde{h}) = n$. Els termes de grau n en $\tilde{h}$ venen donats per

$$Res_{\mu,n-\mu}(p_x x + p_y y, q_x x + q_y y)$$

I si

$$Res_{\mu,n-\mu}(p_x x + p_y y, q_x x + q_y y) = 0$$

aleshores

$$\deg(p_x x + p_y y) < \mu \ i \ \deg(q_x x + q_y y) < n - \mu \tag{3.2.4}$$

o

$$p_x x + p_y y, \ q_x x + q_y y \ \text{ tenen un factor comú en } \mathbb{K}[x, y, t] \tag{3.2.5}$$

Suposem que es compleix (3.2.4). Aleshores $\deg(p_x), \deg(p_y) < n$ i $\deg(q_x), \deg(q_y) < n - \mu$. Pel Corol·lari 2.1.12 això implica que $\deg(a), \deg(b), \deg(c) < n$, fet que és impossible.

Suposem que es compleix (3.2.5). Sigui $R \in \mathbb{K}[x, y, t]$ el factor comú no constant entre $p_x x + p_y y$ i $q_x x + q_y y$:

$$p_x x + p_y y = RS_1$$
$$q_x x + q_y y = RS_2$$

amb $S_1, S_2 \in \mathbb{K}[x, y, t]$.

- Si $\deg_{x,y} R = 0$, aleshores $R \in \mathbb{K}[t]$ seria un factor comú entre a, b, c, fet que és impossible, ja que, per hipòtesi, $a(t), b(t), c(t)$ son relativament primers.
- Si $\deg_{x,y} R = 1$, aleshores $R = rx + sy, \ r, s \in \mathbb{R}$ i $S_1, S_2 \in \mathbb{K}[t]$. Per tant, $p_x q_y - p_y q_x = \lambda c = 0$, fet que és impossible.

Per tant,

$$Res_{\mu,n-\mu}(p_x x + p_y y, q_x x + q_y y) \neq 0$$

i $\deg(\tilde{h}) = n$.

□

Tenim, doncs, que podem escriure l'equació implícita $\tilde{h} = 0$ com el determinant d'una matriu $n \times n$ amb coeficients ≤ 1 en x, y.

Suposem a continuació

$$p = \sum_{i=0}^{\mu} p_i t^i \qquad q = \sum_{i=0}^{n-\mu} q_i t^i \tag{3.2.6}$$

amb coeficients a $\mathbb{K}$ i definim

$$R_i = p \sum_{l=0}^{n-\mu-i-1} q_{i+l+1} t^l - q \sum_{l=0}^{n-\mu-1} p_{i+l+1} t^l \quad i = 0, \ldots, \mu - 1 \tag{3.2.7}$$

Definim, abans de continuar, la matriu de Bézout associada a dos polinomis. Va ser introduïda per James Joseph Sylvester i Arthur Cayley. El determinant d'aquesta matriu és igual a la resultant dels dos polinomis. Sovint s'utilitza per analitzar l'estabilitat d'un polinomi donat.

Definició 3.2.6. *Siguin p, q com a* (3.2.6)*. Aleshores la matriu de Bézout d'ordre n associada als polinomis p, q és*

$$B_n(p, q) = (b_{ij})_{i,j=0,\ldots,n-1}$$

on

$$\frac{p(x)q(y) - p(y)q(x)}{x - y} = \sum_{i,j=0}^{n-1} b_{ij} x^i y^j.$$

Si prenem $m_{ij} = \min\{i, n-1-j\}$ per a tot $i, j = 0, \ldots, n-1$, aleshores

$$b_{ij} = \sum_{k=0}^{m_{ij}} (p_{j+k+1} q_{i-k} - p_{i-k} q_{j+k+1}.$$

De manera similar al cas $\mu = n - \mu$ mostrat a la Definició 3.2.6, tenim que $\deg_t(R_0), \ldots, \deg_t(R_{\mu-1}) < n - \mu - 1$. A més a més, R_i es pot escriure

$$R_i = \sum_{j=0}^{n-\mu-1} R_{ij} t^j \tag{3.2.8}$$

on

$$R_{ij} = \sum_{\substack{k_1 \leq min(i,j) \\ k_1 + k_2 = i+j+1}} (p_{k_1} q_{k_2} - p_{k_2} q_{k_1}) \underset{\substack{\downarrow \\ [k_1 k_2] = p_{k_1} q_{k_2} - p_{k_2} q_{k_1}}}{=} \sum_{\substack{k_1 \leq min(i,j) \\ k_1 + k_2 = i+j+1}} [k_1 k_2] \tag{3.2.9}$$

amb $0 \leq i \leq \mu - 1, 0 \leq j \leq n - \mu - 1$.

Definim també

$$R_i = p\, t^{n-\mu-1-i}, \quad i = \mu, \ldots, n - \mu - 1.$$

amb $\deg(R_i) \leq \mu + (n-\mu-1-\mu) = n-\mu-1$.

Prenent R_i com a (3.2.8), podem escriure

$$R_{ij} = p_{i+j+1+\mu-n}, \quad \mu \leq i \leq n-\mu-1,\ 0 \leq j \leq n-\mu-1. \tag{3.2.10}$$

Enunciem, sense demostració una proposició prèvia a la generalització de la fórmula de Bézout per la resultant.

Proposició 3.2.7.

$$Res(f,g) = p_0^n \det(m_g : A_f \to A_f)$$

on p_0 és el terme independent de p definit com a la Definició 3.2.3, $A_f = \frac{\mathbb{K}[x]}{\langle f \rangle}$ és l'anell quocient i m_g és l'aplicació

$$m_g([h]) = [g] \cdot [h] = [gh] \in A_f$$

Podem ara escriure la generalització de la fórmula de Bézout per la resultant.

Teorema 3.2.8. [3] *Siguin $p, q \in \mathbb{K}[x,y,t]$ amb $\deg(p) = \deg(q) = \mu \leq n-\mu$ i R_{ij} com a (3.2.9) i (3.2.10). Aleshores la resultant $Res(p,q)$ ve donada pel determinant*

$$Res(p,q) = (-1)^{\mu(n-\mu)} \det \begin{pmatrix} R_{n-\mu-1,0} & \cdots & R_{n-\mu-1,n-\mu-1} \\ \vdots & \ddots & \vdots \\ R_{0,0} & \cdots & R_{0,n-\mu-1} \end{pmatrix} \tag{3.2.11}$$

Veiem que aquest teorema dona la resultant com una matriu $(n-\mu) \times (n-\mu)$ on, per (3.2.9) hi ha μ files quadràtiques en els coeficients de p, q i, per (3.2.10), les $(n-\mu)-\mu = n-2\mu$ files restants son lineals en els coeficients de p.

Notem que quan $\mu = n/2$, (3.2.11) es redueix a la resultant de Bézout.

Demostració. La fila i-èsima de la matriu de (3.2.11) correspon als coeficients de R_i. A més, tenim, usant que

$$Res(p,q) = (-1)^{\deg(p)\deg(q)}\ Res(q,p)$$

que (3.2.11) és equivalent a

$$Res(q,p) = \det \begin{pmatrix} R_{0,n-\mu-1} & \cdots & R_{n-\mu-1,n-\mu-1} \\ \vdots & \ddots & \vdots \\ R_{0,0} & \cdots & R_{n-\mu-1,0} \end{pmatrix} \tag{3.2.12}$$

on la columna i-èsima correspon als coeficients de R_i.

Si prenem cadascuna de les columnes com un polinomi de grau $\leq n-\mu-1$ respecte de la base $t^{n-\mu-1}, t^{t-\mu-2}, \ldots, t, 1$, aleshores

$$Res(q,p) = \det \begin{pmatrix} R_{0,n-\mu-1} & \ldots & R_{n-\mu-1,n-\mu-1} \\ \vdots & \ddots & \vdots \\ R_{0,0} & \ldots & R_{n-\mu-1,0} \end{pmatrix} = \det\left(R_0, \ldots, R_{n-\mu-1}\right) \quad (3.2.13)$$

Siguin l'anell quocient $A = \mathbb{K}[t]/\langle q \rangle$ i l'aplicació

$$\begin{array}{rccc} m_p: & A & \to & A \\ & h + \langle q \rangle & \mapsto & ph + \langle q \rangle \end{array}$$

Sabem ara, per la Proposició 3.2.7 que

$$Res(q,p) = q_{n-\mu}^{\mu} det(m_p) \quad (3.2.14)$$

Usant la funció residu tenim

$$\begin{array}{ccc} A & \stackrel{\cong}{\to} & \mathbb{K}[t]_{\leq n-\mu-1} \\ h + \langle q \rangle & \mapsto & Rem_q(h) \end{array}$$

d'on podem escriure m_p de la forma

$$\begin{array}{rccc} m_p: & A & \to & A \\ & h & \mapsto & Rem_q(h) \end{array}$$

Ara tenim que

$$\det(m_p) = \det\left(Rem_q(t^{n-\mu-1}p), Rem_q(t^{n-\mu-2}p), \ldots, Rem_q(tp), Rem_q(p)\right)$$

on escrivim els polinomis per columnes.

Usant (3.2.14) tenim que hem de veure

$$q_{n-\mu}^{\mu} \det(m_p) = q_{n-\mu}^{\mu} \det\left(Rem_q(t^{n-\mu-1}p), \ldots, Rem_q(p)\right) = \det\left(R_0, \ldots, R_{n-\mu-1}\right)$$

Multiplicant les primeres μ columnes per $q_{n-\mu}$, l'equació és equivalent a

$\det\left(q_{n-\mu}Rem_q(t^{n-\mu-1}p), \ldots, q_{n-\mu}Rem_q(t^{n-2\mu}p), Rem_q(t^{n-2\mu-1}p), \ldots, Rem_q(p)\right) =$
$\det(R_0, \ldots R_{n-\mu-1})$.

Ara, com que $\deg(R_i = t^{n-\mu-1-i}p) \leq n-\mu-1$, per $\mu \leq i \leq n-\mu-1$, aleshores

$$R_i = Rem_q(t^{n-\mu-1-i}p); \qquad \mu \leq i \leq n-\mu-1. \quad (3.2.15)$$

i, per tant, provar (3.2.12) és equivalent a provar

$$\det\left(q_{n-\mu}Rem_q(t^{n-\mu-1}p),\ldots,q_{n-\mu}Rem_q(t^{n-2\mu}p),Rem_q(t^{n-2\mu-1}p),\ldots,Rem_q(p)\right)=$$
$$\det(R_0,\ldots R_{n-\mu-1}).$$

Tenim que $Rem_q(h)$ és linear en h i $\deg(R_i)\leq n-\mu-1$. Per tant, per (3.2.7) tenim que

$$R_i=\sum_{i=0}^{n-\mu-i-1} q_{i+l+1}Rem_q(t^l p)\quad i=0,\ldots,\mu-1.$$

Per tant, podem escriure

$$\begin{aligned}
R_0 &= q_1R_{n-\mu-1}+\ldots+q_{n-2\mu}R_\mu+q_{n-2\mu+1}Rem_q(t^{n-2\mu}p)+\ldots\\
&\quad+q_{n-\mu}Rem_q(t^{n-\mu-1}p);\\
R_1 &= q_2R_{n-\mu-1}+\ldots+q_{n-2\mu+1}R_\mu+q_{n-2\mu-1}Rem_q(t^{n-2\mu}p)+\ldots\\
&\quad+q_{n-\mu}Rem_q(t^{n-\mu-2}p);\\
&\vdots\\
R_{\mu-1} &= q_\mu R_{n-\mu-1}+\ldots+q_{n-\mu+1}R_\mu+q_{n-\mu}Rem_q(t^{n-2\mu}p);\\
R_\mu &= Rem_q(t^{n-2\mu-1});\\
&\vdots\\
R_{n-\mu-1} &= Rem_q(t^0).
\end{aligned}$$

D'aquí, utilitzant transformacions per files, obtenim que

$$\det\left(q_{n-\mu}Rem_q(t^{n-\mu-1}p),\ldots,q_{n-\mu}Rem_q(t^{n-2\mu}p),Rem_q(t^{n-2\mu-1}p),\ldots,Rem_q(p)\right)=$$
$$\det(R_0,\ldots R_{n-\mu-1}).$$

i el resultat queda demostrat. □

Bibliografia

[1] Becker, T. i Weispfenning, V. (1993). *Gröbner Bases*, Springer-Verlag, New York.

[2] Cox, D.A., Little, J. i O'Shea, D. (1992). *Ideals, Varieties and Algorithms*, Springer, Berlin.

[3] Cox, D.A, Sederberg, T.W., Chen, F. (1996). *The moving line ideal basis of planar rational curves*, Computer Aided Geometry Design 15 (1998) 803-827.

[4] Cox, D.A., Little, J. i O'Shea, D. (1998). *Using Algebraic Geometry*, Springer, Berlin.

[5] Jia, X., Shi, X. i Chen, F. (2016). *Survey on the thery and applications of μ-bases for rational curves and surfaces*. Elsevier B.V.

[6] Shafarevich, I.R (1974). *Basic Algebraic Geometry*, Springer, Berlin.

[7] Song, N., Chen, F. i Goldman, R. (2007). *Axial moving lines and singularities of rational planar curves*. Elsevier B.V.

[8] Travesa Grau, A. (2016). *Estructures Algebraiques*.

[9] Zheng, J. i Sederberg, T.W.(2001). *A direct approach to computing the μ-basis of planar rational curves*. J. Symbolic Computation. 31:619-629.