UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

BASES DE GRÖBNER: UNA VARIEDAD DE APLICACIONES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A :

CARLOS ENRIQUE AMÉNDOLA CERÓN

DIRECTOR DE TESIS:
DR. ALBERTO LEÓN KUSHNER SCHNUR

2012

BASES DE GRÖBNER: UNA VARIEDAD DE APLICACIONES

Carlos Enrique Améndola Cerón

2012

Índice general

"La esencia de las Matemáticas reside en su libertad"
Georg Cantor

Agradecimientos

Este proyecto no hubiera sido posible sin el apoyo de varias personas. Primeramente mis padres, por darme la vida, su amor y la oportunidad de estudiar todos estos años hasta el presente. Me da inmenso gusto poder compartir este logro con ellos. Asimismo, todos mis familiares y muy especialmente mi hermana Andrea, que me han brindado tanto a lo largo de muchos años.

Agradezco sinceramente al Dr. León Kushner por haberme recibido y orientado consistentemente a lo largo de este trabajo.

Me gustaría expresar toda mi gratitud a la profesora Marcela González y a los profesores Octavio Páez, Rolando Gómez y Javier Alfaro por formar parte de la revisión de este ambicioso proyecto. También agradezco a todos los profesores que me dieron clase a lo largo de la carrera; especialmente a la profesora Carmen Gómez y a los profesores Guillermo Grabinsky y Eduardo Arellano por todas sus sabias enseñanzas y apoyo; a la profesora Clotilde García, al profesor Rafael Rojas y al profesor José Alfredo Amor, que en paz descanse.

Gracias a Berenice Jiménez, por brindarme todo su amor, cariño y comprensión; así como a mis amigos que han formado parte de mi vida y son inolvidables; en particular a mis compañeros de la facultad Edgar Guzmán, Gilberto Santos y Ricardo Hernández. Estoy agradecido con Naoki Solano, Sergio Rangel, Jorge Rodas, Miguel Candia, Michelle Infanzón por todo lo que hemos compartido en estos cinco años.

Y sinceras gracias a todos aquéllos que no están listados pero que saben tienen un lugar en mi memoria y corazón. ¡Que la Fuerza los acompañe!

Introducción

Se expondrá a lo largo de estas páginas una posible introducción al concepto de base de Gröbner, inspirado en un contexto de Álgebra Conmutativa y Geometría Algebraica y, de acuerdo al título de este trabajo, con un enfoque especial en presentar una variedad de aplicaciones.

En el Capítulo 1 se presentan los conceptos y resultados básicos que fundamentan y dan contexto a la teoría a desarrollarse. En las primeras dos secciones se definen los conceptos algebraicos relacionados con anillos, ideales y polinomios; en las siguientes dos los conceptos duales de Geometría Algebraica correspondientes para terminar en la última sección con la conexión entre estos conceptos algebraicos y geométricos.

En el segundo capítulo se desarrolla la teoría básica de las bases de Gröbner, encontradas por Bruno Buchberger en 1965 y nombradas en honor a su asesor Wolfgang Gröbner. Después de los conceptos que llevan a la definición y propiedades de tales bases, presentamos el algoritmo de Buchberger que permite su construcción.

En los últimos dos capítulos se presentan al mismo tiempo extensiones de la teoría así como varias aplicaciones al irse planteando problemas y luego desarrollando las herramientas necesarias para su solución. A diferencia de las aplicaciones presentadas en el Capítulo 4, las aplicaciones del Capítulo 3 son más autocontenidas dentro del contexto planteado en el Capítulo 1. Sin embargo, los conceptos utilizados siguen siendo cubiertos en primeros cursos de Álgebra Lineal y Álgebra Moderna, por lo que no representan una dificultad mayor para poder leerse y comprenderse. En total se han escogido 17 problemas, esperando que al término de éstos el lector quede convencido de la importancia y utilidad de las bases de Gröbner.

Capítulo 1

El contexto algebraico

1.1. Anillos e Ideales

Recordemos las siguientes definiciones y resultados básicos al mismo tiempo que introducimos la notación correspondiente:

Definición 1 *Un* anillo *es un conjunto R con dos operaciones binarias $+$ y $\cdot$ (llamadas suma y producto) tales que:*
(i) R es un grupo abeliano respecto a la suma (con elemento neutro 0)
(ii) R es un semigrupo respecto al producto (i.e. $\cdot$ es asociativa)
(iii) El producto distribuye la suma: $\forall a, b, c \in R : (a + b) \cdot c = a \cdot c + b \cdot c$ y $a \cdot (b + c) = a \cdot b + a \cdot c$

Si el producto es conmutativo, R es un *anillo conmutativo* y si $(R, \cdot)$ es monoide con neutro $1 \neq 0$ es un *anillo con 1.*

Todos los anillos con los que trabajaremos serán anillos conmutativos con 1.

Definición 2 *Sean R y S anillos, una función $\varphi : R \longrightarrow S$ es un* homomorfismo *sii*[1]
(i) $\varphi(a + b) = \varphi(a) + \varphi(b) \quad \forall a, b \in R$
(ii) $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in R$
(iii) $\varphi(1_R) = 1_S$

[1] 'sii' abrevia un 'si y sólo si' de definición, distinguiéndolo así de una doble implicación (en alguna proposición o teorema) que requiere demostración.

Definición 3 *Sea R anillo y $\varnothing \neq I \subseteq R$. I es un* ideal *de R sii*
(i) $\forall a, b \in I \quad a + b \in I$
(ii) $\forall a \in I, \forall r \in R \quad a \cdot r \in I$

I es *trivial* si $I = \{0\}$ e I es *propio* si $I \neq R$.

Dado $\varphi : R \longrightarrow S$ homomorfismo de anillos, el *kernel* de φ es el ideal propio $Ker\varphi = \{a \in R | \varphi(a) = 0\}$.

Definición 4 *Sea $A \subseteq R$, el* ideal generado *por A es el conjunto*

$$\begin{aligned} \langle A \rangle &= \left\{ \sum_{i=1}^{n} a_i r_i | 0 < n \in \mathbb{N}, r_i \in R, a_i \in A, 1 \leq i \leq n \right\} \\ &= \{\textit{sumas finitas de } a_i r_i \textit{ con } a_i \in A, r_i \in R\} \end{aligned}$$

y es el ideal más pequeño que contiene a A. Si $A = \varnothing$, entonces $\langle A \rangle = \{0\}$. Si $I = \langle a \rangle$ [2] para algún $a \in R$, I es un ideal principal. *Un ideal J es* finitamente generado *sii existe A finito tal que $J = \langle A \rangle$.*

Definición 5 *Sean I, J ideales de R, luego se tienen los ideales* intersección, suma *y* producto*: $I \cap J$, $I+J = \langle I \cup J \rangle = \{a+b \mid a \in I, b \in J\}$ y $IJ = \langle \{a \cdot b | a \in I, b \in J\} \rangle$.*

Observación 1 *Se tiene que $IJ \subseteq I \cap J$ (cada $a \cdot b$ con $a \in I, b \in J$ se puede ver tanto en I como en J).*

Definición 6 *Un ideal P de R es ideal* primo *sii $\forall a, b \in R$ tal que $ab \in P$, se tiene que $a \in P$ o $b \in P$. Un ideal M de R es ideal* maximal sii es propio y $\subseteq$*-maximal (es decir, si J es un ideal tal que $M \subseteq J \subseteq R$, entonces $J = M$ o $J = R$).*

Observación 2 *Todo ideal maximal es primo (por contrapuesta: si I no es un ideal primo, entonces existen $a, b \in R$ tal que $ab \in I$ pero $a \notin I$ y $b \notin I$. Como $a \notin I$, el ideal $I + \langle a \rangle$ es tal que $I \subset I + \langle a \rangle$. Si $I + \langle a \rangle = R$, entonces se tendría que $1 = t + ra$ para algunos $t \in I$, $r \in R$, y por tanto $b = tb + rab \in I$, que contradice $b \notin I$. Por lo tanto, $I \subset I + \langle a \rangle \subset R$ y así I no es ideal maximal).*

[2] Formalmente, sería $I = \langle \{a\} \rangle$, pero cuando $A = \{a_1, a_2, ..., a_r\}$ es finito se suele escribir $\langle a_1, a_2, ..., a_r \rangle$ en lugar de $\langle \{a_1, a_2, ..., a_r\} \rangle$

Definición 7 *Sea I ideal de R, se define el* radical *de I como*

$$rad(I) = \sqrt{I} = \{a \in R | \exists m = m(a) \in \mathbb{N} \text{ con } a^m \in I\}$$

Se dice que I es ideal radical *sii $I = rad(I)$. Se comprueba de la definición que $rad(I)$ es siempre un ideal radical que contiene a I.*

Observación 3 *Todo ideal primo es radical.(si $f^m \in I$ para alguna $m \in \mathbb{N}$, por ser I primo se tiene por inducción que algún factor de $f \cdot f \cdot ... \cdot f \in I$, es decir, $f \in I$).*

Definición 8 *Sea R anillo; $0 \neq a \in R$ es un* divisor de cero *sii existe $0 \neq b \in R$ tal que $ab = 0$, y $u \in R$ es* unidad *o* invertible *sii existe $c \in R$ tal que $uc = 1$. R es un* dominio entero *sii no tiene elementos divisores de cero. R es* campo *sii todo elemento distinto de cero es unidad.*

Definición 9 *Un anillo R con la propiedad de que todo ideal es principal es un* anillo de ideales principales *(A.I.P). Si también R es dominio entero, es un* dominio de ideales principales *(D.I.P).*

Ejemplo 1 *$(\mathbb{Z}, +, \cdot, 0, 1)$ es un dominio de ideales principales con unidades 1 y -1 Con las operaciones usuales, $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son campos.*

Definición 10 *Si $I \subseteq R$ es un ideal, se puede definir la relación de equivalencia $a \sim b$ sii $a - b \in I$ lo que lleva al conjunto cociente*

$$R/I = \{a + I | a \in R\}$$

que consta de todas las clases de equivalencia[3]*. Se le da estructura de anillo a R/I mediante las operaciones*

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

que gracias a ser I ideal, están bien definidas, con neutro aditivo la clase $\overline{0}$ y neutro multiplicativo la clase $\overline{1}$. A este anillo le llamamos anillo cociente *módulo I.*

[3]Cuando no haya confusión respecto al ideal I, se denotará la clase $a + I$ (es decir, la clase de a) como $\overline{a}$.

Observación 4 *Se tienen dos caracterizaciones básicas:*
(1) I anillo de R es primo si y sólo si R/I es dominio entero
(gracias a que $a \cdot b \in I \iff \overline{a \cdot b} = \overline{0} \iff \overline{a} \cdot \overline{b} = \overline{0}$).
(2) I anillo de R es maximal si y sólo si R/I es campo
(gracias a que $\overline{a} \neq \overline{0} \iff a \notin I \iff I \subset I + \langle a \rangle$ y que $I + \langle a \rangle = R \iff \exists \overline{b}\, \overline{a} \cdot \overline{b} = \overline{1}$).

Definición 11 *Sea R un anillo. Se dice que una cadena ascendente de ideales $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...I_n \subseteq I_{n+1} \subseteq ...$ es* estacionaria *sii existe una $N \in \mathbb{N}$ tal que $I_N = I_{N+1} = I_{N+2} = ...$, es decir, $I_n = I_{n+1}\ \forall n \geq N$.*

Proposición 1 *"Sea R un anillo. Las siguientes condiciones son equivalentes:*

1. Toda cadena ascendente de ideales en R es estacionaria.
2. Toda familia no vacía de ideales en R tiene elemento maximal.
3. Todo ideal de R es finitamente generado."

Demostración. 1 $\Rightarrow$ 2) Por contrapuesta, supongamos que existe una familia de ideales $\mathcal{F} \neq \varnothing$ sin elemento maximal, es decir, para cada $I \in \mathcal{F}$, puesto que I no es maximal, existe $I' \in \mathcal{F}$ tal que $I \subset I'$. Así, podemos elegir[4] una sucesión $\{I_n\}_{n\in\mathbb{N}} \subseteq \mathcal{F}$ tal que $I_n \subset I_{n+1}\ \forall n \in \mathbb{N}$, por lo que existe una cadena ascendente no estacionaria.

2 $\Rightarrow$ 3) Sea I ideal de R. Consideramos $\mathcal{F} = \{J \subseteq I \mid J$ ideal finitamente generado$\}$, que es una familia no vacía de ideales en R (pues $\{0\} \in \mathcal{F}$). Por hipótesis, $\mathcal{F}$ tiene algún maximal M. Afirmamos que $M = I$, pues si $x \in I - M$ entonces $M \subset M + \langle x \rangle \subseteq I$, que contradiría la maximalidad de M. Como $I = M \in \mathcal{F}$, I es finitamente generado.

3 $\Rightarrow$ 1) Sea $I_1 \subseteq I_2 \subseteq ...I_n \subseteq I_{n+1} \subseteq ...$ una cadena ascendente de ideales; luego consideramos $I = \bigcup_{n=1}^{\infty} I_n$ que es ideal, pues dados $x, y \in I$ existe $j \in \mathbb{N}$ tal que $x, y \in I_j$ (y como I_j es ideal ya se cumple $x + ry \in I_j \subseteq I$). Por hipótesis I es finitamente generado, por lo que $I = \langle x_1, x_2, ..., x_r \rangle$ con $x_k \in I$, $1 \leq k \leq r$. Sea $n_k \in \mathbb{N}$ tal que $x_k \in I_{n_k}$, y sea $N = \max_{1\leq k\leq r} \{n_k\}$. Así, $I = I_N = I_{N+1} = ...$ y la cadena es estacionaria. ■

Un anillo R que satisfaga cualquiera de las condiciones anteriores se llama *Noetheriano*[5].

[4] Por Axioma de Elecciones Dependientes
[5] En honor a la matemática Emmy Noether (1882-1935)

Ejemplo 2 *Como los únicos ideales de un campo k son $\{0\}$ y k mismo, todo campo es Noetheriano.*

1.2. Polinomios

En esta sección presentamos los objetos sobre los que estaremos trabajando, los polinomios. Aunque la idea informal de un polinomio es "algo" de la forma $a_0 + a_1x + a_2x^2 + ... + a_nx^n$, donde x es una "variable", para definirlo desde el punto de vista conjuntista pensaremos en sucesiones de coeficientes que eventualmente son sucesiones constantes 0. Además, pensaremos en varias variables, por lo que en lugar de considerar como dominio a $\mathbb{N} = \{0, 1, 2, ...\}$, consideramos el producto cartesiano de $\mathbb{N}$ consigo mismo n veces: $\mathbb{N}^n$

Definición 12 *Sea R un anillo; un* polinomio en n variables con coeficientes en R *es una función $f : \mathbb{N}^n \longrightarrow R$ tal que $f(\alpha) = 0$ para casi toda $\alpha \in \mathbb{N}^n$ (es decir, para todas salvo una cantidad finita de α's).*

Dada una $f : \mathbb{N}^n \longrightarrow R$, se define el *soporte* de f como

$$sop(f) = \{\alpha \in \mathbb{N}^n | f(\alpha) \neq 0\}$$

Así, los polinomios en R son aquellas f que tienen soporte finito. Al conjunto de todas estas funciones se le denota $R[x_1, x_2, ..., x_n]$. Los polinomios son *univariados* si $n = 1$ y *multivariados* si $n > 1$.

Si $sop(f) = \{\alpha\}$ para algún $\alpha \in \mathbb{N}^n$, entonces se dice que f es un *término*, y si además $f(\alpha) = 1_R$, se dice que f es un *monomio*. Dado $c \in R$, el polinomio *constante* c es aquel $\overline{c} \in R[x_1, x_2, ..., x_n]$ tal que $\overline{c}(\overline{0}) = c$ y $\overline{c}(\alpha) = 0$ $\forall \alpha \neq \overline{0}$.

Sea $i \in \{1, ..., n\}$, la *variable* x_i es el término con $sop(x_i) = \{e_i\}$ con $e_i = (0, ..., 0, 1, 0, ..., 0)$ el vector que tiene 1 en la $i-$ésima coordenada y 0 en las demás.

Dadas $f, g \in R[x_1, x_2, ..., x_n]$, podemos definir una suma y un producto:

$$(f + g)(\alpha) = f(\alpha) + g(\alpha) \quad \forall \alpha \in \mathbb{N}^n$$

$$(f \cdot g)(\alpha) = \sum_{\beta+\gamma=\alpha} f(\beta) \cdot g(\gamma) \quad \forall \alpha \in \mathbb{N}^n$$

Notar que como $sop(f+g) \subseteq sop(f) \cup sop(g)$ y $sop(f \cdot g) \subseteq \{\alpha \in \mathbb{N}^n | \alpha = \beta + \gamma$ con $\beta \in sop(f)$ y como $\gamma \in sop(g)\}$ y $sop(f), sop(g)$ son finitos, entonces $sop(f+g)$ y $sop(f \cdot g)$ son también finitos y por tanto $f+g$ y $f \cdot g \in R[x_1, x_2, ..., x_n]$ de nuevo. También notar que si $a \in R$ y $f \in R[x_1, x_2, ..., x_n]$, tiene sentido hablar del polinomio af, con $(af)(\alpha) = a \cdot f(\alpha) \ \ \forall \alpha \in \mathbb{N}^n$.

De hecho, $R[x_1, x_2, ..., x_n]$ con estas dos operaciones forma un anillo conmutativo con 1. En efecto, el neutro aditivo es el polinomio constante $\overline{0}$ y el neutro multiplicativo es el polinomio constante $\overline{1}$.

Consideremos $n = 1$. Sea $f \in R[x]$ y $m = \text{máx}(sop(f))$, luego si $f(i) = a_i$ para $0 \leq i \leq m$ tenemos que $f = a_0\overline{1} + a_1 x + a_2 x^2 + ... + a_m x^m$, lo cual justifica esta notación usual para un polinomio univariado.

Generalmente escribiremos x, y, z en lugar de x_1, x_2,x_3. Siguiendo la notación usual, por ejemplo en $R[x, y, z]$ con $R = \mathbb{Z}$ el polinomio $f(\alpha) = \begin{cases} 1 \text{ si } \alpha = (2,1,0) \\ -2 \text{ si } \alpha = (1,3,2) \\ 0 \text{ en otro caso} \end{cases}$ se representaría como $f(x, y, z) = x^2 y - 2xy^3 z^2$. En general, todo polinomio f se puede escribir como suma de monomios: $f = \sum_{\alpha \in sop(f)} f(\alpha) \cdot x_1^{\alpha_1} x_2^{\alpha_2} ..., x_n^{\alpha_n}$, donde $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$.

Notar que el producto de dos monomios es de nuevo un monomio, y como 1 es también un monomio, podemos considerar a

$$M_n = \{m \in R[x_1, x_2, ..., x_n] | m \text{ es monomio}\}$$

con el producto como un monoide. El siguiente mapeo exponencial $e : M_n \longrightarrow \mathbb{N}^n$ dado por $e(x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}) = (\alpha_1, \alpha_2, ..., \alpha_n)$ [6] es un isomorfismo de monoides, es decir, e es biyectiva, $e(\overline{1}) = \overline{0}$ y $e(x^\alpha \cdot x^\beta) = \alpha + \beta$ (esto último pues $x^\alpha \cdot x^\beta$ es justamente $x^{\alpha+\beta}$). Este isomorfismo no depende del anillo R.

Definición 13 *Sea $0 \neq f \in R[x_1, x_2, ..., x_n]$, se definen:*
(1) Los términos de f como $T(f) = \{f(\alpha) \cdot x_1^{\alpha_1} x_2^{\alpha_2} ..., x_n^{\alpha_n} | \alpha \in sop(f)\}$
(2) Los monomios de f como $M(f) = \{x_1^{\alpha_1} x_2^{\alpha_2} ..., x_n^{\alpha_n} | \alpha \in sop(f)\}$
(3)Los coeficientes de f como $C(f) = \{f(\alpha) | \alpha \in sop(f)\}$

Observación 5 *"Si R es dominio entero, entonces $R[x_1, x_2, ..., x_n]$ es dominio entero."*

[6] Denotaremos de forma compacta al monomio $x_1^{\alpha_1} x_2^{\alpha_2} ..., x_n^{\alpha_n}$ como x^α, en cuyo caso $e(x^\alpha) = \alpha$

Definición 14 *Sean x^α y x^β ($\alpha, \beta \in \mathbb{N}^n$) monomios en $R[x_1, x_2, ..., x_n]$. Definimos:*
(a) El mínimo común múltiplo (MCM) de x^α y x^β como $[x^\alpha; x^\beta] = x^\gamma$ con $\gamma_i = \max\{\alpha_i, \beta_i\}$ para cada $i = 1, 2, ..., n$
(b) El máximo común divisor (MCD) de x^α y x^β como $(x^\alpha; x^\beta) = x^\gamma$ con $\gamma_i = \min\{\alpha_i, \beta_i\}$ para cada $i = 1, 2, ..., n$

Observación 6 *En el sentido de divisibilidad de términos en que $x^\alpha | x^\beta$ sii $\exists x^\gamma$ ($\gamma \in \mathbb{N}^n$) con $x^\beta = x^\gamma x^\alpha$, se tiene que el MCM y el MCD realmente son múltiplo y divisor común de x^α y x^β, respectivamente, y también son $|-$mínimo y $|-$máximo respectivamente.*

Aunque lo definiremos de forma general en la sección 2.1, por ahora, si $n = 1$ y $f = a_r x^r + a_{r-1}x^{r-1} + ... + a_1 x + a_0$, $(a_r \neq 0)$, entonces a r se le llama *grado* de f y a a_r se le llama *coeficiente líder*, y lo denotamos $CL(f)$.

Teorema 1 *(DE LA BASE DE HILBERT) "Si R es anillo Noetheriano, entonces $R[x]$ es anillo Noetheriano."*

Demostración. Sea I un ideal de $R[x]$ y sea

$$I_j = \{a \in R | \exists f \in I \text{ de grado } j \text{ con } CL(f) = a\} \cup \{0\}$$

con $j \in \mathbb{N}$. Afirmamos que $I_j \subseteq R$ es un ideal. En efecto, esto se sigue de que si $a, b \in I_j$, al tomar la suma o diferencia de los polinomios correspondientes, entonces $a \pm b \in I_j$ y de que si $r \in R$, al multiplicar el correspondiente polinomio por r, entonces $ar \in I_j$. Además, notar que si $a \in I_j$, al multiplicar el correspondiente polinomio por x se tiene que $a \in I_{j+1}$, por lo que

$$I_0 \subseteq I_1 \subseteq ... \subseteq I_j \subseteq I_{j+1} \subseteq ...$$

es una cadena ascendente de ideales en R. Como por hipótesis R es Noetheriano, tenemos que la cadena se estaciona, digamos en I_N ($I_N = I_{N+1} = ...$) y también todo ideal I_j es finitamente generado (proposición 1). Sean

$$\begin{aligned}
&a_1^0, a_2^0, ..., a_{n_0}^0 \text{ generadores de } I_0 \\
&a_1^1, a_2^1, ..., a_{n_1}^1 \text{ generadores de } I_1 \\
&\vdots \\
&a_1^N, a_2^N, ..., a_{n_N}^N \text{ generadores de } I_N.
\end{aligned}$$

Para cada $j = 0, 1, ..., N$ y para cada $i = 1, ..., n_j$ sea f_i^j un polinomio en I de grado j tal que $CL(f_i^j) = a_i^j$. La afirmación es que $F = \{f_i^j | 0 \leq j \leq N, 1 \leq i \leq n_j\}$ genera a I.
En efecto, sea $f \in I$ un polinomio de grado d con $CL(f) = a_d$. Si $d > N$, entonces como $a_d \in I_d = I_N$ se tiene que $a_d \in \left\langle a_1^N, a_2^N, ..., a_{n_N}^N \right\rangle$, es decir, los coeficientes líderes de $x^{d-N} f_1^N, x^{d-N} f_2^N, ..., x^{d-N} f_{n_N}^N$ generan a a_d, por lo que existen $c_1, c_2, ..., c_{n_N} \in R$ tales que

$$f - c_1 x^{d-N} f_1^N - c_2 x^{d-N} f_2^N - \cdots - c_{n_N} x^{d-N} f_{n_N}^N \in I$$

y tiene grado $< d$.(se cancela el término $a_d x^d$) Por otro lado, si $d \leq N$, entonces $a_d \in I_d$ y existen $c_1, c_2, ..., c_{n_d} \in R$ tales que

$$a_d = c_1 a_1^d + c_2 a_2^d + \cdots + c_{n_d} a_{n_d}^d$$

por lo que de nuevo

$$f - c_1 f_1^d - c_2 f_2^d - \cdots - c_{n_d} f_{n_d}^d \in I$$

es un polinomio de grado $< d$. Notar que en ambos casos, los polinomios restados pertenecen a $\langle F \rangle$, y si continuamos este proceso para los nuevos polinomios en I obtenidos, el grado siempre desciende por lo que eventualmente tendremos que $f - g = 0$ con $g \in \langle F \rangle$, es decir, $f = g \in \langle F \rangle$.
Como hemos probado que I es finitamente generado para todo ideal de $R[x]$, (por la proposición 1) concluimos que $R[x]$ es Noetheriano. ■

Haciendo la identificación $R[x_1, x_2, ..., x_n][x_{n+1}] \cong R[x_1, x_2, ..., x_n, x_{n+1}]$ y por Inducción se tiene:

Corolario 1 *"Si R es anillo Noetheriano, entonces $R[x_1, x_2, ..., x_n]$ es también anillo Noetheriano"*

Notar así que en particular todo ideal I de $k[x_1, x_2, ..., x_n]$ con k campo es finitamente generado; este hecho será de fundamental importancia a lo largo de este trabajo.

1.3. Variedades Algebraicas

Definición 15 *Sea k un campo y sea $\mathcal{F} \subseteq k[x_1, x_2, ..., x_n]$ un conjunto de polinomios, entonces la* variedad afín *asociada a $\mathcal{F}$ es*

$$\mathcal{V}(\mathcal{F}) = \{(a_1, a_2, ..., a_n) \in k^n | f(a_1, a_2, ..., a_n) = 0 \ \forall f \in \mathcal{F}\}$$

Cuando $\mathcal{F} = \{f_1, f_2, ..., f_n\}$ sea finito, solemos denotar $\mathcal{V}(\mathcal{F})$ como $\mathcal{V}(f_1, f_2, ..., f_n)$. A continuación unos ejemplos:

Ejemplo 3 *Sea* $k = \mathbb{R}$, *consideramos* $f_1 = x^2 + y^2 - 1$, $f_2 = x - y$ *por lo que* $\mathcal{V}(f_1, f_2) = \{(x, y) \in \mathbb{R}^2 |\ x^2 + y^2 = 1, x = y\}$ *que reconocemos como la intersección de la circunferencia unitaria con la recta identidad, por lo que* $\mathcal{V}(f_1, f_2) = \{(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}), (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})\}$

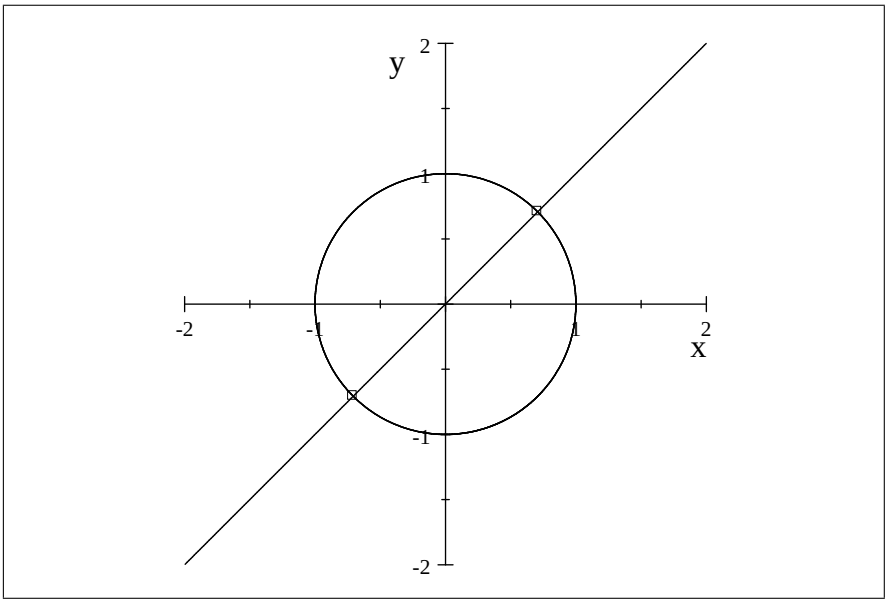

Figura 1.1: Gráfica del Ejemplo 3

Ejemplo 4 *Sea* $k = \mathbb{R}$, $f = x^2 + 1$, *entonces* $\mathcal{V}(f) = \varnothing$ *pero si en cambio* $k = \mathbb{C}$, *tenemos que* $\mathcal{V}(f) = \{i, -i\}$, *por lo que no hay que perder de vista el campo sobre el que se trabaja.*

Ejemplo 5 *Sea* $k = \mathbb{R}$, $f = x^3 - y^2 + x - y$. *Entonces* $\mathcal{V}(f)$ *toma la forma de la gráfica de la siguiente página.*

Observación 7 *Notar que de la definición se sigue que si* $\mathcal{F} \subseteq \mathcal{G}$, *entonces se tiene* $\mathcal{V}(\mathcal{G}) \subseteq \mathcal{V}(\mathcal{F})$ *(un cero común de todos los polinomios en* $\mathcal{G}$ *lo será en particular de los de* $\mathcal{F}$*).*

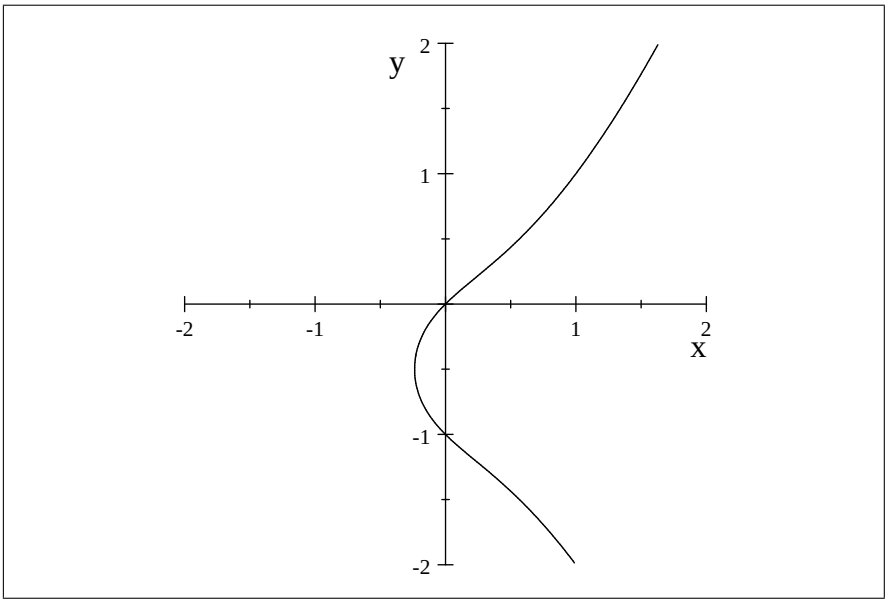

Figura 1.2: Gráfica del Ejemplo 5

Definición 16 *Decimos que un conjunto $A \subseteq k^n$ es* algebraico *sii $A = \mathcal{V}(\mathcal{F})$ para algún $\mathcal{F} \subseteq k[x_1, x_2, ..., x_n]$.*

Proposición 2 *"Sea $\tau = \{U \subseteq k^n | k^n - U$ es algebraico$\}$, entonces τ es una topología en k^n, conocida como la topología de* Zariski*."*

Demostración. Notar que en este caso los conjuntos cerrados son precisamente los conjuntos algebraicos, así que basta checar que cumplen las propiedades de cerrados:
(i) Sea $f \equiv 1$ el polinomio constante 1, luego $\mathcal{V}(f) = \varnothing$. Por otro lado, sea $g \equiv 0$ el polinomio constante 0, luego $\mathcal{V}(g) = k^n$. Así, tanto $\varnothing$ y k^n son algebraicos, y por tanto, pertenecen a τ.
(ii) Sean $A = \mathcal{V}(\mathcal{F})$ y $B = \mathcal{V}(\mathcal{G})$ conjuntos algebraicos, entonces $A \cup B = \mathcal{V}(\mathcal{F} \cdot \mathcal{G})$ donde $\mathcal{F} \cdot \mathcal{G} = \{f \cdot g | f \in \mathcal{F}, g \in \mathcal{G}\}$. En efecto, $(f \cdot g)(\overline{a}) = 0 \Leftrightarrow f(\overline{a}) = 0$ o $g(\overline{a}) = 0$ $\Leftrightarrow \overline{a} \in \mathcal{V}(\mathcal{F})$ o $\overline{a} \in \mathcal{V}(\mathcal{G}) \Leftrightarrow \overline{a} \in A \cup B$. Por lo tanto, $A \cup B$ es algebraico también.
(iii) Sea $\{A_i = \mathcal{V}(\mathcal{F}_i)\}_{i \in I}$ una familia de conjuntos algebraicos, entonces $\bigcap_{i \in I} A_i = \mathcal{V}(\bigcup_{i \in I} \mathcal{F}_i)$. En efecto, $\overline{a} \in \mathcal{V}(\bigcup_{i \in I} \mathcal{F}_i) \Leftrightarrow f(\overline{a}) = 0 \ \forall f \in \mathcal{F}_i, i \in I \Leftrightarrow \overline{a} \in \bigcap_{i \in I} \mathcal{V}(\mathcal{F}_i)$.
Por lo tanto $\bigcap_{i \in I} A_i$ es algebraico también. ■

Observación 8 *Como la cerradura topológica de un conjunto es el cerrado 'más pequeño' (es decir, el $\subseteq -$mínimo) que contiene al conjunto, tenemos que al tomar la cerradura de Zariski $\overline{A}^Z$ de un conjunto $A \subseteq k^n$, se obtiene el conjunto algebraico más pequeño en el que está contenido A.*

Proposición 3 *"Si $I = \langle \mathcal{F} \rangle \subseteq k[x_1, x_2, ..., x_n]$ es el ideal generado por $\mathcal{F}$, entonces $\mathcal{V}(\mathcal{F}) = \mathcal{V}(I)$"*

Demostración. Como $\mathcal{F} \subseteq I$, de la observación 7 se tiene $\mathcal{V}(I) \subseteq \mathcal{V}(\mathcal{F})$. Por otro lado, sea $\overline{a} \in \mathcal{V}(\mathcal{F})$ y $f = c_1 f_1 + c_2 f_2 + \cdots + c_r f_r \in I$ ($f_i \in \mathcal{F}$, $c_i \in k$). Entonces

$$f(\overline{a}) = (c_1 f_1 + c_2 f_2 + \cdots + c_r f_r)(\overline{a}) = c_1 f_1(\overline{a}) + c_2 f_2(\overline{a}) + \cdots + c_r f_r(\overline{a}) = 0 + 0 + \cdots + 0 = 0$$

ya que al estar $\overline{a} \in \mathcal{V}(\mathcal{F})$ se tiene que $f_i(a) = 0$, $i = 1, 2, ..., r$. Así, $\overline{a} \in \mathcal{V}(\mathcal{I})$ también. ■

Corolario 2 *"Si $I = \langle f_1, f_2, ..., f_s \rangle = \langle g_1, g_2, ..., g_t \rangle$, entonces se tiene que $\mathcal{V}(f_1, f_2, ..., f_s) = \mathcal{V}(g_1, g_2, ..., g_t)$"*

Terminamos esta sección con la definición función polinomial:

Definición 17 *Una* función polinomial *es una función $f : k^n \to k^m$ tal que cada proyección es polinomial, es decir, las funciones $f_i = \pi_i \circ f : k^n \to k$ son polinomios en $k[x_1, x_2, ..., x_n]$ $\forall i = 1, ..., m$.*

Ejemplo 6 *La función $f : \mathbb{R}^3 \to \mathbb{R}^4$ dada por $f(x, y, z) = (x^2, y - z^3, xy + 2, 0)$ es una función polinomial.*

1.4. El Ideal de ceros

Así como a un conjunto de polinomios le asociamos un conjunto de puntos (los ceros comunes), el concepto dual requiere asociar a un conjunto de puntos, un conjunto de polinomios:

Definición 18 *Sea k un campo y sea $A \subseteq k^n$ un conjunto de puntos, definimos el* ideal de ceros *asociado a A como:*

$$\mathcal{I}(A) = \{f \in k[x_1, x_2, ..., x_n] | f(a) = 0, \forall a \in A\}$$

Cuando $A = \{a_1, a_2, ..., a_s\}$ sea finito, solemos denotar $\mathcal{I}(A)$ como $\mathcal{I}(a_1, a_2, ..., a_s)$.

Observación 9 *$\mathcal{I}(A)$ sí es un ideal en el sentido de la definición de la sección 1.1, pues claramente el polinomio constante $0 \in \mathcal{I}(A)$ y si $f, g \in \mathcal{I}(A)$, $h \in k[x_1, x_2, ..., x_n]$, para cada $a \in A$*

$$(f + g \cdot h)(a) = f(a) + g(a)h(a) = 0 + 0 \cdot h(a) = 0$$

por lo que $(f + g \cdot h) \in \mathcal{I}(A)$.

Proposición 4 *"El operador $\mathcal{I} : \wp(k^n) \to \wp(k[x_1, x_2, ..., x_n])$[7] tiene las siguientes propiedades:*
(1) Si $A \subseteq B$, entonces $\mathcal{I}(B) \subseteq \mathcal{I}(A)$
(2) $\mathcal{I}(\varnothing) = k[x_1, x_2, ..., x_n]$
(3) Si k es infinito, $\mathcal{I}(k^n) = \{\overline{0}\}$
(4) Todo ideal de ceros es ideal radical."

Demostración. (1) Por definición, como los polinomios en $\mathcal{I}(B)$ se anulan en todos los puntos de B, y $A \subseteq B$, en particular se anulan en los de A.

(2) Cualquier polinomio se anula en todos los puntos de $\varnothing$ (por vacuidad), es decir, $f \in \mathcal{I}(\varnothing)\ \forall f \in k[x_1, x_2, ..., x_n]$. Por lo tanto, $\mathcal{I}(\varnothing) = k[x_1, x_2, ..., x_n]$.

(3) Como k es infinito, k^n es infinito. Procedemos por inducción: si $n = 1$, un polinomio distinto del constante 0 puede tener a lo más un número finito de raíces, por lo que $\mathcal{I}(k) = \{\overline{0}\}$. Suponemos para $n - 1$, si tenemos un polinomio $f \in k[x_1, x_2, ..., x_n]$ que se anula en todo k^n escribimos factorizando la variable x_n :

$$f = \sum_{j=0}^{r} g_j(x_1, x_2, ..., x_{n-1}) x_n^j$$

donde cada $g_j \in k[x_1, x_2, ..., x_{n-1}]$. Dado $(a_1, a_2, ..., a_{n-1}) \in k^{n-1}$ fijo tenemos el polinomio $f(a_1, a_2, ..., a_{n-1}, x_n) \in k[x_n]$, que por hipótesis se anula en cualquier $a_n \in k$, entonces por el caso base tal $f \in k[x_n]$ es el polinomio $\overline{0}$. Esto quiere decir que todos los coeficientes $g_j(x_1, x_2, ..., x_{n-1})$ son 0 para todo $(a_1, a_2, ..., a_{n-1}) \in k^{n-1}$, i.e., $g_j \in \mathcal{I}(k^{n-1})$ y por hipótesis de inducción se concluye que cada $g_j = 0$; y por tanto f también.

(4) Sea $I = \mathcal{I}(A)$ ideal de ceros. Siempre se da la contención $I \subseteq rad(I)$. Veamos que $rad(I) \subseteq I$: si $f^m \in I$ para alguna $m \in \mathbb{N}$, entonces para cada $a \in A$ se tiene

[7] $\wp(A)$ denota el conjunto potencia de A (el conjunto de todos los subconjuntos de A)

que $f^m(a) = 0$, y como k es dominio entero tenemos que $f(a) = 0$, es decir, $f \in \mathcal{I}(A) = I$. ■

Y al usarse en conjunción del operador $\mathcal{V} : \wp(k[x_1, x_2, ..., x_n]) \to \wp(k^n)$ tenemos:

Proposición 5 *"Se cumplen las siguientes propiedades para toda* $\mathcal{F} \subseteq k[x_1, x_2, ..., x_n]$ *y* $A \subseteq k^n$*:*
(1) $\mathcal{I}(\mathcal{V}(\mathcal{F})) \supseteq \mathcal{F}$
(2) $\mathcal{V}(\mathcal{I}(A)) \supseteq A$
(3) $\mathcal{V}(\mathcal{I}(\mathcal{V}(\mathcal{F}))) = \mathcal{V}(\mathcal{F})$
(4) $\mathcal{I}(\mathcal{V}(\mathcal{I}(A))) = \mathcal{I}(A)$
(5) Si A *es algebraico, entonces* $A = \mathcal{V}(\mathcal{I}(A))$*"*

Demostración. (1) Por definición de $\mathcal{V}$, los polinomios de $\mathcal{F}$ se anulan en los puntos de $\mathcal{V}(\mathcal{F})$, por lo que pertenecen a $\dot{\mathcal{I}(\mathcal{V}(\mathcal{F}))}$.

(2) Por definición de $\mathcal{I}$, los puntos de A anulan a los polinomios de $\mathcal{I}(A)$, por lo que pertenecen a $\mathcal{V}(\mathcal{I}(A))$.

(3) De (1), $\mathcal{I}(\mathcal{V}(\mathcal{F})) \supseteq \mathcal{F}$ y por la Observación 7 tenemos $\mathcal{V}(\mathcal{I}(\mathcal{V}(\mathcal{F}))) \subseteq \mathcal{V}(\mathcal{F})$ Por otro lado, de (2) con $A = \mathcal{V}(\mathcal{F})$ tenemos $\mathcal{V}(\mathcal{I}(\mathcal{V}(\mathcal{F}))) \supseteq \mathcal{V}(\mathcal{F})$.

(4) De (2), $\mathcal{V}(\mathcal{I}(A)) \supseteq A$ y por (1) de la proposición anterior tenemos $\mathcal{I}(\mathcal{V}(\mathcal{I}(A)))$ $\subseteq \mathcal{I}(A)$. Por otro lado, de (1) con $\mathcal{F} = \mathcal{I}(A)$ tenemos $\mathcal{I}(\mathcal{V}(\mathcal{I}(\mathcal{A}))) \supseteq \mathcal{I}(A)$.

(5) Consecuencia de (3), pues al ser A algebraico se tiene que existe $\mathcal{F} \subseteq k[x_1, x_2, ..., x_n]$ tal que $A = \dot{\mathcal{V}(\mathcal{F})}$. ■

Finalmente, podemos concretizar un poco más a la cerradura de Zariski:

Proposición 6 *"Sea* $A \subseteq k^n$ *, entonces la cerradura de Zariski de* A *es*

$$\overline{A}^Z = \mathcal{V}(\mathcal{I}(A))"$$

Demostración. Este resultado es consecuencia de las propiedades enunciadas en las proposiciones anteriores. Por un lado, $\mathcal{V}(\mathcal{I}(A))$ es un conjunto algebraico que contiene a A (de (2) en la proposición anterior). Veamos que es el $\subseteq -$mínimo: sea B algebraico tal que $A \subseteq B$; entonces $\mathcal{I}(B) \subseteq \mathcal{I}(A)$ (proposición 4 (1)), y por la Observación 7 tenemos $\mathcal{V}(\mathcal{I}(A)) \subseteq \mathcal{V}(\mathcal{I}(B))$, y como B es algebraico, por (5) de la proposición anterior $\mathcal{V}(\mathcal{I}(B)) = B$. Así, $\mathcal{V}(\mathcal{I}(A)) \subseteq B$. Por lo tanto, $\overline{A}^Z = \dot{\mathcal{V}(\mathcal{I}(A))}$.
■

1.5. La Correspondencia entre Ideales y Variedades

Hemos visto en las secciones anteriores el comportamiento básico de los operadores:

$$\begin{aligned} \mathcal{V} &: \wp(k[x_1, x_2, ..., x_n]) \to \wp(k^n) \\ \mathcal{I} &: \wp(k^n) \to \wp(k[x_1, x_2, ..., x_n]) \end{aligned}$$

En particular observamos que ambos operadores invierten contenciones. Nos preguntamos ahora sobre la posible inyectividad o suprayectividad de cada uno, y especialmente nos interesa saber cuándo uno de los operadores pudiera ser el inverso del otro, como lo sugerían las últimas propiedades de la sección anterior.

Por la proposición 3 nos damos cuenta que a cualquier conjunto generador de un ideal I le corresponde la misma variedad $\mathcal{V}(I)$, así que si buscamos que $\mathcal{V}$ sea inyectiva, es necesario (aunque tal vez no suficiente) restringir su dominio a ideales de $k[x_1, x_2, ..., x_n]$. Esto último concuerda con la imagen de $\mathcal{I}$, pues sabemos que justamente está contenida en el conjunto de estos ideales. Por otro lado, notamos que si A es subconjunto de k^n, $\mathcal{I}$ asocia el mismo ideal tanto a A como a su cerradura de Zariski $\overline{A}^Z = \mathcal{V}(\mathcal{I}(A))$. En efecto, de la proposición 5 (4) tenemos $\mathcal{I}(\mathcal{V}(\mathcal{I}(A))) = \mathcal{I}(A)$. Si queremos que $\mathcal{I}$ sea inyectivo, necesariamente debemos restringir su dominio a conjuntos algebraicos, lo que concuerda con la imagen de $\mathcal{V}$.

En conclusión, dado que $\mathcal{V}$ asocia variedades algebraicas e $\mathcal{I}$ asocia ideales, podemos hacer (y debemos hacer, si buscamos cierta invertibilidad) las restricciones:

$$\begin{aligned} \mathcal{V} &: \textit{ideales} \to \textit{variedades} \\ \mathcal{I} &: \textit{variedades} \to \textit{ideales} \end{aligned}$$

¿Serán estas restricciones suficientes? Veamos que para asegurar inyectividad de $\mathcal{I}$ sí.

Proposición 7 *"Si $V \subseteq k^n$ es una variedad algebraica, entonces*

$$\mathcal{V}(\mathcal{I}(V)) = V;$$

en particular, el operador $\mathcal{I}$ tiene inversa izquierda y por tanto es inyectivo."

Demostración. En efecto, como V es algebraico existe $\mathcal{F} \subseteq k[x_1, x_2, ..., x_n]$ tal que $V = \mathcal{V}(\mathcal{F})$ y ya que $\mathcal{V}(\mathcal{I}(\mathcal{V}(\mathcal{F}))) = \mathcal{V}(\mathcal{F})$ por la proposición 5 (3), concluimos el resultado. ■

Así, para que un operador sea el inverso del otro, ya tenemos una de las composiciones: $\mathcal{V} \circ \mathcal{I} = Id$. Sin embargo, consideremos el siguiente

Ejemplo 7 *Sean* $I = \langle x \rangle$ *y* $J = \langle x^2 \rangle$ *en* $k[x]$, *entonces se tiene que* $I \neq J$ *y*

$$\mathcal{V}(I) = \mathcal{V}(J) = \{0\}$$

El fenómeno de no inyectividad de $\mathcal{V}$ en el ejemplo anterior podría intentar adjudicarse a que $\langle x^2 \rangle$ no es un ideal radical (su radical es justamente $\langle x \rangle$), si uno tiene en mente de la proposición 4 que todo ideal de ceros debe ser radical (es decir, la imagen de $\mathcal{I}$ está contenida en el conjunto de ideales radicales). De hecho, se verifica en general la siguiente proposición.

Proposición 8 *"Sea* $I \subseteq k[x_1, x_2, ..., x_n]$ *ideal, entonces*
(1) $\mathcal{V}(I) = \mathcal{V}(rad(I))$
(2) $rad(I) \subseteq \mathcal{I}(\mathcal{V}(I))$*"*

Demostración. (1) $\supseteq$) Como $I \subseteq rad(I)$, entonces $\mathcal{V}(rad(I)) \subseteq \mathcal{V}(I)$.

$\subseteq$) Sea $a \in \mathcal{V}(I)$ y $f \in rad(I)$, entonces existe $m \in \mathbb{N}$ tal que $f^m \in I$ y así por hipótesis $f^m(a) = 0$, y por ser k dominio entero, concluimos $f(a) = 0$, es decir, $a \in \mathcal{V}(rad(I))$.

(2) Por un lado tenemos de la proposición 5 (1) que $rad(I) \subseteq \mathcal{I}(\mathcal{V}(rad(I)))$, y por otro lado de (1) de esta misma proposición que $\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\mathcal{V}(rad(I)))$, por lo que $rad(I) \subseteq \mathcal{I}(\mathcal{V}(I))$. ■

Lo anterior sugeriría restringir aún más los operadores a:

$$\begin{aligned} \mathcal{V} &: \textit{ideales radicales} \rightarrow \textit{variedades} \\ \mathcal{I} &: \textit{variedades} \rightarrow \textit{ideales radicales} \end{aligned}$$

Lo sorprendente es que, aún así, $\mathcal{V}$ podría ser no inyectivo:

Ejemplo 8 *Sean* $I = \langle 1 \rangle = \mathbb{R}[x]$ *y* $J = \langle x^2 + 1 \rangle \subseteq \mathbb{R}[x]$, *entonces se tiene que* $I \neq J$, *ambos radicales*[8], *y*

$$\mathcal{V}(I) = \mathcal{V}(J) = \varnothing$$

[8] Se puede ver que $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$ que es campo, por lo que $J = \langle x^2 + 1 \rangle$ es maximal, y en particular radical.

El ejemplo anterior revela que el campo juega un papel fundamental en esta correspondencia. En particular, si hubiéramos tenido $k = \mathbb{C}$ ya no se hubiera tenido $\mathcal{V}(\langle x^2 + 1\rangle) = \varnothing$. De hecho, si buscamos que $\mathcal{V}$ sea inyectivo, el único ideal radical que puede tener $\mathcal{V}(I) = \varnothing$ es el ideal total $k[x_1, x_2, ..., x_n]$. Como acabamos de probar que $\mathcal{V}(I) = \mathcal{V}(rad(I))$, entonces debería suceder que $\mathcal{V}(I) = \varnothing$ si y sólo si $I = k[x_1, x_2, ..., x_n]$.

Si k es algebraicamente cerrado (es decir, todo polinomio no constante $f \in k[x]$ tiene todas sus raíces en k), sabemos que esto sucede para $n = 1$. En efecto, gracias a que $k[x]$ es un D.I.P. existe una $f \in k[x]$ tal que $I = \langle f_1, f_2, ..., f_s\rangle = \langle f\rangle$ y en virtud del corolario 2, que $\mathcal{V}(I) = \mathcal{V}(f_1, f_2, ..., f_s) = \mathcal{V}(f)$. Si f es constante (no nula), entonces $I = k[x]$ y $\mathcal{V}(f_1, f_2, ..., f_s) = \varnothing$. Por el contrario, si f es no constante, se tiene que $I \subset k[x]$ y como k es algebraicamente cerrado se tiene que sí hay raíces y por tanto que $\mathcal{V}(f_1, f_2, ..., f_s) \neq \varnothing$ Que este mismo fenómeno se sigue observando para $n > 1$ es justo lo que afirma otro célebre teorema de Hilbert conocido como el Nullstellensatz[9], cuya prueba se puede encontrar por ejemplo en [4] o [10]:

Teorema 2 *(NULLSTELLENSATZ DÉBIL) "Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal con k algebraicamente cerrado. Entonces $\mathcal{V}(I) = \varnothing$ si y sólo si $I = \langle 1\rangle = k[x_1, x_2, ..., x_n]$"*

Hay otra versión del Nullstellensatz que se le da el adjetivo de 'fuerte' por concluir algo más general, pero que de hecho es equivalente al anterior Nullstellensatz Débil, ya que este último se usa para demostrarlo. La demostración en particular es muy ingeniosa:

Teorema 3 *(NULLSTELLENSATZ FUERTE) "Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal con k algebraicamente cerrado. Entonces $\mathcal{I}(\mathcal{V}(I)) = rad(I)$"*

Demostración. $\supseteq$) Siempre se cumple para cualquier k, como quedó demostrado en la proposición anterior.

$\subseteq$) Sea $f \in \mathcal{I}(\mathcal{V}(I))$, donde $I = \langle f_1, f_2, ..., f_r\rangle$ el truco ingenioso consiste en tomar una nueva variable y y considerar el ideal

$$\widetilde{I} = \langle f_1, f_2, ..., f_r, 1 - yf\rangle \subseteq k[x_1, x_2, ..., x_n, y]$$

Afirmamos que $\mathcal{V}(\widetilde{I}) = \varnothing$, pues sea $(a_1, a_2, ..., a_n, b) \in k^{n+1}$
Si $(a_1, a_2, ..., a_n) \in \mathcal{V}(I)$, entonces por hipótesis $f(a_1, ..., a_n) = 0$, y por tanto

[9] Puede traducirse del alemán como 'teorema sobre el lugar de ceros'.

$(1 - yf)(a_1, a_2, ..., a_n, b) = 1 \neq 0$. Así, $(a_1, a_2, ..., a_n, b) \notin \mathcal{V}(\widetilde{I})$.
Si $(a_1, a_2, ..., a_n) \notin \mathcal{V}(I)$, entonces existe alguna f_j para la cual $f_j(a_1, a_2, ..., a_n) \neq 0$ y por tanto en $k[x_1, x_2, ..., x_n, y]$ tampoco $(a_1, a_2, ..., a_n, b) \notin \mathcal{V}(\widetilde{I})$.
En cualquier caso $\mathcal{V}(\widetilde{I}) = \varnothing$ y entonces por Nullstellensatz Débil se tiene que $\widetilde{I} = \langle 1 \rangle$, por lo que existen $p_1, p_2, ..., p_r, q \in k[x_1, x_2, ..., x_n, y]$ tales que

$$p_1 f_1 + p_2 f_2 + ... + p_r f_r + q(1 - yf) = 1$$

Al sustituir la misteriosa y por $1/f$ obtenemos:

$$p_1(x_1, x_2, ..., 1/f) f_1 + p_2(x_1, x_2, ..., 1/f) f_2 + ... + p_r(x_1, x_2, ..., 1/f) f_r + 0 = 1$$

Si multiplicamos ahora por una potencia suficientemente grande de f para que ya no haya f como denominador, se logra una igualdad de la forma

$$f^m = \sum_{i=1}^{r} g_i f_i$$

donde $g_i \in k[x_1, x_2, ..., x_n]$, por lo que concluimos que $f^m \in \langle f_1, f_2, ..., f_r \rangle = I$, es decir, $f \in rad(I)$. ■

Así, tenemos por fin las condiciones necesarias para la correspondencia biyectiva entre ideales y variedades. La composición faltante $\mathcal{I} \circ \mathcal{V} = Id$ se obtiene en la restricción de ideales radicales, ya que por el Nullstellensatz fuerte tenemos $\mathcal{I}(\mathcal{V}(I)) = rad(I)$, que para I radical es $\mathcal{I}(\mathcal{V}(I)) = I$. Resumimos esto en el siguiente

Teorema 4 *"Sea k algebraicamente cerrado, entonces los operadores*

$$\begin{aligned} \mathcal{V} &: \textit{ideales radicales} \rightarrow \textit{variedades} \\ \mathcal{I} &: \textit{variedades} \rightarrow \textit{ideales radicales} \end{aligned}$$

son biyecciones, uno inverso del otro."

Hemos visto que los operadores $\mathcal{I}$ y $\mathcal{V}$ permiten traducir conceptos algebraicos en geométricos y viceversa. Más interesante aún es ver cómo se comportan con las operaciones entre ideales y las operaciones entre variedades (¿qué tanto podemos pensar en $\mathcal{V}$ e $\mathcal{I}$ como homomorfismos, y en el caso de k algebraicamente cerrado, como isomorfismos?). Damos algunas propiedades en este sentido:

Teorema 5 *"Sean I y J ideales de $k[x_1, x_2, ..., x_n]$.*
(1) $\mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J)$
(2) $\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$
(3) $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$"

Demostración. (1) Según vimos en la demostración de la proposición 2, $\mathcal{V}(I \cup J) = \mathcal{V}(I) \cap \mathcal{V}(J)$, y puesto $\langle I \cup J \rangle = I + J$, de la proposición 3 tenemos que $\mathcal{V}(I + J) = \mathcal{V}(I \cup J) = \mathcal{V}(I) \cap \mathcal{V}(J)$.
(2) También de la demostración de la proposición 2,

$$\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(\{f \cdot g | f \in I, g \in J\})$$

y puesto $IJ = \langle \{f \cdot g | f \in I, g \in J\} \rangle$, de la proposición 3 concluimos que $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$.
(3) $\subseteq$) Como $IJ \subseteq I \cap J$, tenemos que $\mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ)$ y según (2), ésta última es $\mathcal{V}(I) \cup \mathcal{V}(J)$, por lo que $\mathcal{V}(I \cap J) \subseteq \mathcal{V}(I) \cup \mathcal{V}(J)$
$\supseteq$) Como $I \cap J \subseteq I$ y $I \cap J \subseteq J$, tenemos que $\mathcal{V}(I) \subseteq \mathcal{V}(I \cap J)$ y $\mathcal{V}(J) \subseteq \mathcal{V}(I \cap J)$, y así $\mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(I \cap J)$. ■

Aunque a lo largo de la tesis, seguiremos explorando correspondencias entre ideales y variedades, el lector interesado en tener el panorama completo puede revisar el Apéndice "Diccionario Álgebra-Geometría", como es llamado y revisado en [4].

Capítulo 2

Bases de Gröbner

2.1. Órdenes Monomiales

Para poder hablar de estos conjuntos de generadores de ideales de polinomios necesitamos dar un orden a los monomios. Este orden es natural cuando tratamos en el anillo de polinomios de una variable, pero cuando son varias no tenemos una única forma de establecer cuándo un monomio debería ser mayor que otro. Recordemos los siguientes conceptos generales:

Definición 19 *Una relación $<$ en un conjunto A es un* orden *sii es antireflexiva* $(a \not< a \ \forall a \in A)$ *y transitiva* $(a < b \ y \ b < c \Longrightarrow a < c \ \forall a, b, c \in A)$ *. Un orden se llama* total *sii cualesquiera dos elementos son comparables* $(\forall a \neq b \in A : a < b \ o \ b < a)$*. Una relación de orden es un* buen orden *sii todo subconjunto no vacío tiene mínimo.*

Observación 10 *Todo buen orden es orden total, pues dados $a \neq b \in (A, <)$ con $<$ buen orden, como el subconjunto no vacío $\{a, b\}$ tiene mínimo, se tiene que $a < b$ o bien que $b < a$.*

Es útil esta caracterización (con Axioma de Elección) de buenos órdenes: que no existan sucesiones infinitas descendentes $a_1 > a_2 > a_3 > ...$

Proposición 9 *"Sea A conjunto y $<$ un orden total en A; luego, $<$ es buen orden $\Longleftrightarrow \nexists$ una sucesión $\{a_n\}_{n\in\mathbb{N}}$ en A tal que $a_{n+1} < a_n \ \forall n \in \mathbb{N}$ "*

Demostración. $\Longrightarrow$) Por contrapuesta. Si $\exists$ una sucesión $\{a_n\}_{n\in\mathbb{N}}$ en A tal que $a_{n+1} < a_n \ \forall n \in \mathbb{N}$, entonces al considerar $B = \{a_n | n \in \mathbb{N}\} \neq \varnothing$ tenemos un subconjunto no vacío de A que no tiene mínimo.

$\Longleftarrow$) Nuevamente por contrapuesta, si $<$ no es buen orden en A, existe $B \neq \varnothing$, $B \subseteq A$ tal que no tiene mínimo. Es decir, dado cualquier $b \in B$, existe $b' \in B$ tal que $b' < b$. Por Axioma de Elecciones Dependientes, podemos elegir una sucesión $\{b_n\}_{n\in\mathbb{N}} \subseteq B \subseteq A$ tal que $b_{n+1} < b_n \ \forall n \in \mathbb{N}$. ■

Vamos a definir unos órdenes particulares en $\mathbb{N}^n$, que a su vez inducirán en el conjunto de monomios lo que se conoce como orden monomial:

Definición 20 *Una relación de orden $<$ en $\mathbb{N}^n$ se dice que es un orden* admisible *sii es un buen orden que se preserva bajo sumas, es decir, que $\forall \alpha, \beta, \gamma \in \mathbb{N}^n$: $\alpha < \beta \Longrightarrow \ \alpha + \gamma < \beta + \gamma$.*[1]

Dada la correspondencia entre monomios y vectores de $\mathbb{N}^n$, podemos entonces inducir órdenes de monomios de $k[x_1, x_2, ..., x_n]$:

Definición 21 *Sea $<$ en $\mathbb{N}^n$ un orden admisible, entonces se extiende la relación $<$ al conjunto de monomios $M = \{x^\alpha | \alpha \in \mathbb{N}^n\}$ de $k[x_1, x_2, ..., x_n]$ como $x^\alpha < x^\beta \Longleftrightarrow \alpha < \beta$. A tal orden sobre M se le conoce como* orden monomial.

Observación 11 *Así, ya que $x^\alpha x^\gamma = x^{\alpha+\gamma}$, un orden monomial es un buen orden sobre M que se preserva bajo producto de monomios, es decir, que satisface $\forall \alpha, \beta, \gamma$: $x^\alpha < x^\beta \Longrightarrow \ x^\alpha x^\gamma < x^\beta x^\gamma$.*

Proposición 10 *"Sean x^α, x^β monomios de $k[x_1, x_2, ..., x_n]$ y $<$ orden monomial tal que 1 es el monomio mínimo. Si $x^\alpha | x^\beta$, entonces $x^\alpha \leq x^\beta$"*

Demostración. Como $x^\alpha | x^\beta$, existe x^γ tal que $x^\beta = x^\gamma x^\alpha$. En términos de los multigrados, $\beta = \gamma + \alpha$. Como $1 = x^{\overline{0}}$ es mínimo, $\overline{0} \leq \gamma$. Por otro lado, como $<$ se preserva bajo sumas, $\overline{0} + \alpha \leq \gamma + \alpha$, es decir, $\alpha \leq \beta$. ■

Observación 12 *En términos de vectores en $\mathbb{N}^n$, la proposición anterior indica que si $\alpha, \beta \in \mathbb{N}^n$ tal que $\alpha_i \leq \beta_i$ para toda $1 \leq i \leq n$, entonces $\alpha \leq \beta$ bajo el orden admisible (con $\overline{0}$ vector mìnimo, pero esta hipótesis es redundante como se verá en el siguiente teorema).*

[1] Los ejemplos asociados a esta definición pueden revisarse en la pág. 22

Teorema 6 *"Una relación de orden total $<$ en $\mathbb{N}^n$ que se preserva bajo sumas, es un buen orden (i.e., es admisible) $\Longleftrightarrow$ $\overline{0}$ es $<$-mínimo"*

Demostración. $\Longrightarrow$) Por contrapuesta, si el vector $\overline{0} \in \mathbb{N}^n$ no es el elemento mínimo, existe $a \in \mathbb{N}^n$ tal que $a < \overline{0}$, por la preservación bajo suma, entonces $2a = a + a < a$, $3a = 2a + a < 2a$ y en general tenemos una sucesión $\{na\}_{n\in\mathbb{N}}$ tal que $(n+1)a < na$ $\forall n \in \mathbb{N}$, por lo que concluimos que $<$ no es buen orden.

$\Longleftarrow$) Por Inducción. Cuando $n = 1$ vemos que $<$ coincide necesariamente con el orden usual en $\mathbb{N}$ (como $0 < 1$ y por la preservación bajo sumas, $1 < 2$, $2 < 3$...) por lo que sabemos que es un buen orden.
Suponemos para $n-1$ y consideramos $A \subseteq \mathbb{N}^n$ no vacío. Veamos que A tiene $<-$mínimo. Para poder aplicar la hipótesis de Inducción, definimos un orden en $\mathbb{N}^{n-1}$ de la siguiente forma:

$$(a_1, a_2, ..., a_{n-1}) <' (b_1, b_2, ..., b_{n-1}) \text{ sii } (a_1, a_2, ..., a_{n-1}, 0) < (b_1, b_2, ..., b_{n-1}, 0)$$

Tenemos entonces que $<'$es orden total pues $<$ lo es, también $<'$ se preserva bajo sumas pues $<$ lo hace y en la última entrada $0+0 = 0$. Finalmente, como $\overline{0} \in \mathbb{N}^n$ es el $<-$mínimo, se sigue de la definición del orden que $\overline{0} \in \mathbb{N}^{n-1}$ lo es respectivamente para $<'$. Por lo tanto, $<'$ es un orden que satisface la hipótesis de inducción.
Consideramos

$$A' = \{(a_1, a_2, ..., a_{n-1}) | \exists a_n \in \mathbb{N} \text{ con } (a_1, a_2, ..., a_{n-1}, a_n) \in A\} \subseteq \mathbb{N}^{n-1}.$$

Como $A \neq \varnothing$, luego $A' \neq \varnothing$. Sean $\alpha' = \text{mín}_{<'}(A')$,

$$N = \text{mín}\{k \in \mathbb{N} | (\alpha', k) = (\alpha'_1, \alpha'_2, ..., \alpha'_{n-1}, k) \in A\}$$

y $\alpha = (\alpha', N) = (\alpha'_1, \alpha'_2, ..., \alpha'_{n-1}, N) \in A$. Ahora, para cada $k \leq N$ consideramos

$$A'_k = \{(a_1, a_2, ..., a_{n-1}) | ((a_1, a_2, ..., a_{n-1}, k) \in A\} \subseteq \mathbb{N}^{n-1}.$$

Para cada uno de éstos, si $A'_k \neq \varnothing$ por hipótesis de Inducción tiene $<'$-mínimo $\alpha'_k \in \mathbb{N}^{n-1}$. Sea $\alpha_k = (\alpha'_k, k) \in A \subseteq \mathbb{N}^n$ colocando en la $n-$ésima coordenada la correspondiente $k \in \mathbb{N}$. Ahora, la afirmación es que:

$$\alpha^* = \min_{<}\{\alpha, \alpha_0, \alpha_1, \alpha_2, ..., \alpha_N\} \in \mathbb{N}^n$$

es el mínimo buscado de A. En efecto, sea $\beta = (\beta', b_n) = (b_1, b_2, ..., b_{n-1}, b_n) \in A$. Distinguimos dos casos:
(i) Si $b_n \leq N$, entonces por definición $\beta' = (b_1, b_2, ..., b_{n-1}) \in A_{b_n}$ y se tiene $\alpha'_{b_n} \leq' \beta'$,

es decir, $(\alpha'_{b_n}, 0) \leq (\beta', 0)$ y de la preservación bajo sumas, al añadir de ambos lados el vector $(\overline{0}, b_n)$ obtenemos $\alpha_{b_n} = (\alpha'_{b_n}, b_n) \leq (\beta', b_n) = \beta$. Como $\alpha^* \leq \alpha_{b_n}$ concluimos $\alpha^* \leq \beta$.
(ii) Si $b_n > N$, entonces dado que $\beta' \in A'$ tenemos que $\alpha' \leq' \beta'$, es decir, $(\alpha', 0) \leq (\beta', 0)$ y al sumar con la desigualdad $(\overline{0}, N) \leq (\overline{0}, b_n)$ obtenemos que $\alpha = (\alpha', N) \leq (\beta', b_n) = \beta$. Como $\alpha^* \leq \alpha$ concluimos $\alpha^* \leq \beta$.
Así, en cualquier caso, $\alpha^* \leq \beta \ \ \forall \beta \in A$, por lo que A tiene mínimo y así $<$ es un buen orden. ■

Y una vez más traduciendo al lenguaje de monomios, dado que $x^{\overline{0}} = 1$:

Corolario 3 *"Una relación de orden total $<$ en $M = \{x^\alpha | \alpha \in \mathbb{N}^n\}$ que se preserva bajo producto de monomios, es orden monomial $\iff \forall \alpha \in \mathbb{N}^n$, $\alpha \neq \overline{0}$, se tiene $1 < x^\alpha$"*

Así, en el proceso de verificación de que un orden total sobre monomios es orden monomial, la condición de buen orden se puede cambiar por la condición más sencilla de que el monomio mínimo sea el constante (1).

A continuación vemos los ejemplos más importantes de órdenes admisibles (monomiales):

Ejemplo 9 *Sean $\alpha \neq \beta \in \mathbb{N}^n$ definimos $\alpha <_{lex} \beta$ sii $\alpha_i < \beta_i$ con $i = \text{mín}\{j | \alpha_j \neq \beta_j\}$, es decir, sii la primera entrada no nula del vector $\beta - \alpha \in \mathbb{Z}^n$ es positiva. Entonces $<_{lex}$ es un orden admisible y recibe el nombre de* orden lexicográfico *(puro).*

1. Orden Total: Por definición, si $\alpha \neq \beta$, al tomar $i = \text{mín}\{j | \ \alpha_j \neq \beta_j\}$, como el orden en $\mathbb{N}$ es total, tenemos que $\alpha_i < \beta_i$ o $\beta_i < \alpha_i$; es decir, $\alpha <_{lex} \beta$ o $\alpha <_{lex} \beta$.

2. Si $\alpha <_{lex} \beta$, para cualquier $\gamma \in \mathbb{N}^n$ se tiene $\beta - \alpha = (\beta + \gamma) - (\alpha + \gamma)$, por lo que la primera entrada no nula de $(\beta + \gamma) - (\alpha + \gamma)$ sigue siendo positiva, es decir, $\alpha + \gamma <_{lex} \beta + \gamma$.

3. Si $\alpha \neq \overline{0}$, $i = \text{mín}\{j | \ \alpha_j \neq 0\} = \text{mín}\{j | \ \alpha_j > 0\}$, por lo que $\alpha_i > 0$ y así $\alpha >_{lex} \overline{0}$.
   De esta forma, $(3, 5, 6) <_{lex} (4, 2, 1)$ y $(2, 2, 6) <_{lex} (2, 3, 4)$.

Definición 22 *Sea $\alpha \in \mathbb{Z}^n$, definimos el* grado total *de α como $|\alpha| = \sum_{k=1}^{n} \alpha_k$.*

El siguiente orden monomial o admisible considera que el vector α es menor al vector β si el grado total de α es menor al grado total de β, y en caso de igualdad se considera el orden lexicográfico.

Ejemplo 10 *Sean $\alpha \neq \beta \in \mathbb{N}^n$ definimos $\alpha <_{grlex} \beta$ sii $|\alpha| < |\beta|$ o si $|\alpha| = |\beta|$ y $\alpha <_{lex} \beta$, es decir, sii $|\beta - \alpha| > 0$ o si $|\beta - \alpha| = 0$ y la primera entrada no nula del vector $\beta - \alpha \in \mathbb{Z}^n$ es positiva. Así, $<_{grlex}$ es un orden admisible y recibe el nombre de* orden graduado lexicográfico.

1. Orden Total: Por definición, sea $\alpha \neq \beta$, si los grados totales $\sum_{k=1}^{n} \alpha_k$, $\sum_{k=1}^{n} \beta_k \in \mathbb{N}$ son distintos, se decide quién es mayor en $<_{grlex}$; si son iguales, se considera el $<_{lex}$que ya conocemos.

2. Si $\alpha <_{grlex} \beta$, para cualquier $\gamma \in \mathbb{N}^n$ se tiene $\beta - \alpha = (\beta + \gamma) - (\alpha + \gamma)$, por lo que tanto el valor de $|(\beta + \gamma) - (\alpha + \gamma)|$ como el vector $(\beta + \gamma) - (\alpha + \gamma)$ se mantienen invariantes, es decir, $\alpha + \gamma <_{grlex} \beta + \gamma$.

3. Si $\alpha \neq \overline{0}$, existe una $\alpha_i > 0$, por lo que $|\alpha| = \sum_{k=1}^{n} \alpha_k > 0 = \left|\overline{0}\right|$ y así $\alpha >_{grlex} \overline{0}$. De esta forma, $(2,3,1) <_{grlex} (1,4,3)$ y $(2,2,5) <_{grlex} (2,3,4)$.

Un orden monomial que, aunque poco intuitivo resulta muy útil, es el que considera como primer criterio el de mayor grado total, y si se empata, se le da preferencia al que tenga menor entrada final. La verificación de que es orden admisible es análoga a las dos anteriores.

Ejemplo 11 *Sean $\alpha \neq \beta \in \mathbb{N}^n$ definimos $\alpha <_{grevlex} \beta$ sii $|\alpha| < |\beta|$ o si $|\alpha| = |\beta|$ y $\alpha_i > \beta_i$ con $i = \text{máx}\{j|\ \alpha_j \neq \beta_j\}$, es decir, sii $|\beta - \alpha| > 0$ o si $|\beta - \alpha| = 0$ y la última entrada no nula del vector $\beta - \alpha \in \mathbb{Z}^n$ es negativa. Así, $<_{grevlex}$es un orden admisible y recibe el nombre de* orden graduado reverso lexicográfico.
De esta forma, $(2,3,1) <_{grevlex} (1,4,3)$, $(2,2,5) <_{grevlex} (2,3,4)$ *y* $(3,0,2,3) <_{grevlex} (2,2,1,3)$.

Definición 23 *Sea $0 \neq f \in R[x_1, x_2, ..., x_n]$, $<$ un orden monomial, definimos*

1. El *monomio líder* de f es $ML(f) = \text{máx}\{M(f)\}$

2. El *término líder* de f es $TL(f) = \text{máx}\{T(f)\}$[2]

3. El *coeficiente líder* de f es $CL(f)$ el coeficiente de $TL(f)$

4. El *multigrado* de f es $e(TL(f))$ (es decir, el exponente del término líder) Notar que los máximos existen pues se toman sobre conjuntos finitos y, naturalmente, $TL(f) = CL(f)ML(f)$.

Recordando que con $n = 1$ el único orden monomial es el usual $1 < x < x^2 < ...$ la noción de multigrado coincide con la de *grado* de un polinomio f en una variable.

Ejemplo 12 *Ordenando los términos del polinomio*

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

resultaría:
lex: $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$
grlex:$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$
grevlex:$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$.

Ejemplo 13 *En el orden lexicográfico, y* $f = 4xy^2z+4z^2-5x^3+7x^2z^2 \in \mathbb{Q}[x, y, z]$, *se tiene que* $ML(f) = x^3, TL(f) = -5x^3, CL(f) = -5$ *y multigrado*$(f) = (3, 0, 0)$

Proposición 11 *"Sea* $<$ *un orden monomial y sean* $f_1, f_2, ..., f_r \in k[x_1, x_2, ..., x_n]$ *polinomios no nulos. Entonces:*
(a) $ML(f_1f_2...f_r) = ML(f_1)ML(f_2)...ML(f_r)$
(b) $ML(f_1 + f_2 + ... + f_r) \leq \text{máx}\{ML(f_1), ML(f_2), ..., ML(f_r)\}$
(c) Sea $c_j = CL(f_j)$ *y* $A = \{j|ML(f_j) = \text{máx}_i\{ML(f_i)\}\}$, *entonces la igualdad se da en (b) si y sólo si* $\sum_{j\in A} c_j \neq 0$*"*

Demostración. (a) Por definición, para cada $i \in \{1, 2, ..., r\}$, $ML(f_i) \geq t_i$ para cualquier monomio t_i de f_i, y como $<$ se preserva bajo productos:

$$ML(f_1)ML(f_2)...ML(f_r) \geq t_1t_2...t_r \ \forall t_1t_2...t_r \text{ término de } f_1f_2...f_r$$

Así, por definición de monomio líder, tenemos que

$$ML(f_1f_2...f_r) = ML(f_1)ML(f_2)...ML(f_r).$$

[2]Cuando se comparen términos en $R[x_1, x_2, ..., x_n]$, se ignora el coeficiente y se considera como un monomio, si bien éste no se modifica.

(b) Como $M(f_1 + f_2 + ... + f_r) \subseteq \bigcup_{i=1}^{r} M(f_i)$, entonces

$$\begin{aligned} ML(f_1 + f_2 + ... + f_r) &= \text{máx}(M(f_1 + f_2 + ... + f_r)) \\ &\leq \text{máx}(\bigcup_{i=1}^{r} M(f_i)) \\ &= \text{máx}\{ML(f_1), ML(f_2), ..., ML(f_r)\}. \end{aligned}$$

(c) Si $\sum_{j\in A} c_j \neq 0$, entonces el término $\text{máx}_i\{ML(f_i)\}$ es no nulo y por tanto pertenece a $f_1 + f_2 + ... + f_r$, de donde

$$ML(f_1 + f_2 + ... + f_r) \geq \text{máx}\{ML(f_1), ML(f_2), ..., ML(f_r)\}$$

y por la desigualdad en (b), tenemos la igualdad. Por otro lado, si $\sum_{j\in A} c_j = 0$, el término $\text{máx}_i\{ML(f_i)\}$ es nulo y no pertenece a $f_1 + f_2 + ... + f_r$, por lo que $ML(f_1 + f_2 + ... + f_r) \neq \text{máx}\{ML(f_1), ML(f_2), ..., ML(f_r)\}$. ■

Proposición 12 *"Sea $I = \langle\{x^\alpha | \alpha \in A\}\rangle \subseteq k[x_1, x_2, ..., x_n]$ con $A \subseteq \mathbb{N}^n$ Entonces:*
(a) Un monomio $x^\beta \in I$ si y sólo si existe $\alpha \in A$ tal que $x^\alpha | x^\beta$
(b) Un polinomio $f \in I$ si y sólo si cada término de f pertenece a I
(c)Existe $A' \subseteq A$ finito tal que $I = \langle\{x^\alpha | \alpha \in A'\}\rangle$"

Demostración. (a)
$\Rightarrow$) Dado $x^\beta \in I$, tenemos $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha_i}$ con $h_i \in k[x_1, x_2, ..., x_n]$, $\alpha_i \in A$. Ahora expandimos el lado derecho como una combinación lineal de monomios; como el lado izquierdo es un monomio con exponente β, eso implica que del lado derecho todos los monomios que no tengan exponente β se cancelan. Esto deja una suma de la forma $\sum_{i=1}^{t} h'_i x^{\alpha_i}$ con h'_i término tal que $h'_i x^{\alpha_i} = c_i x^\beta$ para algunos $c_i \in k\backslash\{0\}$, $1 \leq i \leq t$. De la última igualdad que $x^{\alpha_i} | x^\beta$.

$\Leftarrow$) Si existe tal $\alpha \in A$ con $x^\alpha | x^\beta$, es decir, existe $h \in k[x_1, x_2, ..., x_n]$ tal que $x^\beta = hx^\alpha$, como $x^\alpha \in I$ (ideal) se tiene que x^β también.

(b)
$\Rightarrow$) Si $f = \sum_{i=1}^{s} h_i x^{\alpha_i}$, al expandir como combinación lineal de monomios, llegamos

a que f es combinación $k-lineal$ de múltiplos de monomios en I, es decir, cada término de f es un múltiplo de algún monomio en I. Como I es ideal, cada uno de estos múltiplos vuelve a estar en I.

$\Leftarrow$) Naturalmente, si cada término de f pertenece a I, como I es ideal se tiene que la suma de ellos, que es f, vuelve a pertenecer a I.

(c) Por el Teorema de la Base de Hilbert, sabemos que I es finitamente generado, y por (b) basta tomar monomios como generadores, es decir, existen $\beta_1, \beta_2, ..., \beta_r \in \mathbb{N}^n$ (posiblemente no en A) tal que $I = \left\langle x^{\beta_1}, x^{\beta_2}, ..., x^{\beta_r} \right\rangle$. Como cada $x^{\beta_i} \in I = \langle \{x^\alpha | \alpha \in A\} \rangle$, por (a) existe $\alpha_i \in A$ tal que $x^{\alpha_i} | x^{\beta_i}$, por lo que $\left\langle x^{\beta_i} \right\rangle \subseteq \langle x^{\alpha_i} \rangle$ y así $\langle x^{\alpha_1}, x^{\alpha_2}, ..., x^{\alpha_r} \rangle = I$. ■

Hay formas en que podemos construir nuevos órdenes monomiales a partir de otros. La más sencilla consiste en hacer un reordenamiento de las variables, obteniendo $n!$ posibles nuevos órdenes. En efecto:

Definición 24 *Sea $<$ un orden admisible y $\pi : \{1, 2, .., n\} \to \{1, 2, .., n\}$ una permutación, entonces definimos $\alpha <_\pi \beta$ sii $\pi(\alpha) < \pi(\beta)$, donde*

$$\pi(\gamma) = (\gamma_{\pi(1)}, \gamma_{\pi(2)}, ..., \gamma_{\pi(n)}) \quad \forall \gamma \in \mathbb{N}^n.$$

Ejemplo 14 *Sea $<_{lex}$ y la permutación π con $\pi(1) = n, \pi(2) = n-1, ..., \pi(n) = 1$. Al orden $<_\pi$ resultante se le conoce como orden* antilexicográfico.

Otra manera de construir nuevos órdenes monomiales es asignar un vector de pesos w a las variables:

Definición 25 *Sea $<$ un orden admisible y $w = (w_1, w_2, ..., w_n) \in \mathbb{R}^n$ con $w_i \geq 0$ $\forall i$; definimos para $\alpha, \beta \in \mathbb{N}^n : \alpha <_w \beta$ sii $\alpha \cdot w <_{\mathbb{R}} \beta \cdot w$, o bien $\alpha \cdot w = \beta \cdot w$ y $\alpha < \beta$, donde '$\cdot$' denota el producto punto usual de $\mathbb{R}^n$.*

Observación 13 *Que $<_w$ sea admisible es consecuencia de que $<$ lo es, que $<_{\mathbb{R}}$ es transitivo y que $\overline{0} \cdot w = 0$*

Ejemplo 15 *Sea $<_{lex}$ y vector de pesos $w = (1, 1, ..., 1)$, entonces el orden $<_w$ que se obtiene es el graduado lexicográfico $<_{grlex}$.*

Terminamos definiendo un tipo de orden que será de fundamental importancia después:

Definición 26 *Sea $j \in \{1, 2, ..., n\}$ fijo, un orden monomial en $k[x_1, x_2, ..., x_n]$ se dice $j-$ésimo* orden de eliminación *sii tiene la propiedad de que cualquier monomio en el que aparezca alguna x_i con $i \leq j$ es mayor que cualquier monomio en el que solo aparecen variables x_k con $k > j$.*

Ejemplo 16 *El orden lexicográfico $<_{lex}$es el clásico orden de eliminación (y lo es para toda $j \in \{1, 2, ..., n\}$)*

Ejemplo 17 *Sea $<$ un orden monomial en $k[x_1, x_2, ..., x_n]$ y sea $j \in \{1, 2, ..., n\}$ fijo. Consideramos $w = (1, 1, ..., 1, 0, 0, , , 0)$ con las primeras j entradas igual a 1 y las restantes igual a 0; entonces se sigue que el orden $<_w$es un $j-$ésimo orden de eliminación.*

2.2. Algoritmo de la División Multivariado

En esta sección explicamos un algoritmo de la división para $k[x_1, x_2, ..., x_n]$, generalizando el conocido para $k[x]$ en una sola variable[3]. Además, también es generalización en cuanto a que se podrá dividir un polinomio f entre varios polinomios $f_1, f_2, ..., f_s$. Es decir, se escribirá:

$$f = a_1 f_1 + a_2 f_2 + ... + a_s f_s + r$$

con $a_i, r \in k[x_1, x_2, ..., x_n]$ Y en la comparación de que r sea 'chico' se involucrará el concepto de orden monomial.

Un ejemplo antes de presentar el algoritmo:

Ejemplo 18 *Dividir $f = x^2y + xy^2 + y^2$ por $f_1 = xy - 1$ y $f_2 = y^2 - 1$, todos en $\mathbb{Q}[x, y]$ bajo orden monomial lex.*
Notamos que los términos de los polinomios ya están ordenados en forma descendente, con $TL(f) = x^2y$,$TL(f_1) = xy$ y $TL(f_2) = y^2$. Siguiendo la idea del algoritmo en una variable, encontraremos los cocientes a partir de que $TL(f_1)$ o $TL(f_2)$ dividan a $TL(f)$. Primero vemos que $TL(f_1)|TL(f)$, a saber, $\frac{x^2y}{xy} = x$ por lo que hacemos $f - xf_1$:

$$x^2y + xy^2 + y^2 - x(xy - 1) = xy^2 + x + y^2$$

[3]Esta generalización al algoritmo original no es complicada, por lo que es sorprendente que esta forma haya sido explorada y usada apenas desde unos 40 años. ([4])

Este es nuestro nuevo dividendo y así, $a_1 = x$*, el coeficiente asociado a* f_1*, hasta ahora. Como* xy^2 *que es el nuevo término líder es otra vez divisible por* $TL(f_1) = xy$ *con* $\frac{xy^2}{xy} = y$ *volvemos a restar ese múltiplo (entonces* $a_1 = x + y$*)*

$$xy^2 + x + y^2 - y(xy - 1) = x + y^2 + y$$

Ahora, como x *, que es el nuevo término líder, no es divisible ni por* $TL(f_1)$ *ni por* $TL(f_2)$*, movemos este término al residuo (*$r = x$*); y continuamos con el siguiente término líder,* y^2*, que sí es divisible por* $TL(f_2)$*, teniendo* $a_2 = 1$ *:*

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

Finalmente, en $y + 1$ *ningún término es divisible por lo que pasa al residuo* $r = x + y + 1$*. La expresión final* $f = a_1 f_1 + a_2 f_2 + r$ *es:*

$$x^2y + xy^2 + y^2 = (x + y)(xy - 1) + 1(y^2 - 1) + (x + y + 1) \tag{2.1}$$

Teorema 7 *(ALGORITMO DE LA DIVISION) "Sea* $<$ *un orden monomial fijo en* $k[x_1, x_2, ..., x_n]$ *y sea* $F = (f_1, f_2, ..., f_s)$ *una* $s-$*tupla ordenada de polinomios. Entonces todo* f *se puede escribir de la forma:*

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$$

donde $a_i, r \in k[x_1, x_2, ..., x_n]$ $\forall i = 1, ..., s$ *y tal que* $r = 0$ *o bien cada término de* r *no es divisible por ninguno de* $TL(f_1), TL(f_2), ..., TL(f_s)$*. Además, se tiene que multigrado*$(f) \geq$*multigrado*$(a_i f_i)$ $\forall i = 1, ..., s$*. A* r *se le llama* residuo *de la división de* f *por* F *y lo denotamos como* $\overline{f}^F$*".*

La prueba de este teorema es señalar la existencia de a_i y de r por medio del siguiente algoritmo:

Algoritmo 1 *Entradas:* $f_1, f_2, ..., f_s, f$

Salidas: $a_1, a_2, ..., a_s, r$

$a_1 := a_2 := ... := a_s := r := 0$

$p := f$

MIENTRAS $p \neq 0$

$i := 1$

division?:=0

MIENTRAS $i \leq s$ Y division?=0

SI $TL(f_i)|TL(p)$

$a_i := a_i + TL(p)/TL(f_i)$

$p := p - (TL(p)/TL(f_i))f_i$

division?:=1

SI NO

$i := i + 1$

SI division?:=0

$r := r + TL(p)$

$p := p - TL(p)$

FIN

La variable p representa al dividendo intermedio mientras progresa la división. *division?* es una variable booleana que indica si algún $TL(f_i)$ divide a $TL(p)$. En efecto, en el ciclo del principal MIENTRAS sucede una de estas dos alternativas: si algún $TL(f_i)$ divide a $TL(p)$, se hace el paso de división aumentando el cociente a_i correspondiente y actualizando el nuevo dividendo p al restar ese múltiplo. Por otro lado, si ningún $TL(f_i)$ divide al que es $TL(p)$, se pasa éste al residuo r.

Para demostrar que el algoritmo funciona, notaremos que la ecuación

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + p + r$$

se cumple en cada paso del algoritmo, por lo que en particular cuando el algoritmo termine (por la condición $p = 0$) se tendrá la expresión buscada.
Para los valores de inicialización de p, a_i y de r se cumple la ecuación pues $f = 0 + 0 + \cdots + 0 + f + 0$. Ahora, si el siguiente paso es uno de división por algún $TL(f_i)$ se tiene al actualizar que $a_i f_i + p = (a_i + TL(p)/TL(f_i))f_i + (p - TL(p)/TL(f_i))f_i)$ y como las otras variables no se ven afectadas, se sigue cumpliendo la ecuación. Por otro lado, si el siguiente paso es uno de residuo, al cambiar p y r, su suma queda constante pues: $p + r = (p - TL(p)) + (r + TL(p))$.
Sólo falta justificar que el algoritmo termina. Notar que tanto en el paso de división en el cual el dividendo se actualiza $p' = p - \frac{TL(p)}{TL(f_i)} f_i$ como en el paso de residuo en el que $p' = p - TL(p)$, se le resta a p su término líder (por la proposición 11 se tiene $TL(\frac{TL(p)}{TL(f_i)} f_i) = \frac{TL(p)}{TL(f_i)} TL(f_i) = TL(p)$), por lo que necesariamente

$TL(p') < TL(p)$. En particular, muligrado(p') < multigrado(p). Si el algoritmo nunca terminara, se tendría una sucesión infinita decreciente de multigrados, que contradiría la propiedad de buen orden de $<$; por lo que eventualmente, $p = 0$.
Finalmente, para ver la relación de los multigrados de f y $a_i f_i$, notamos que cuando a_i pasa de 0 a $TL(p)/TL(f_i)$, se tiene que $TL(a_i f_i) = TL(p)$, y como p se inicializa como f y acabamos de ver que el multigrado de p decrece, $TL(p) \leq TL(f)$. Es decir, multigrado($a_i f_i$) $\leq$multigrado(f).

Desafortunadamente, este algoritmo de la División multivariado no comparte la propiedad de unicidad con su contraparte univariada. De hecho, ni siquiera el residuo tiene que ser único, como vemos en el siguiente ejemplo:

Ejemplo 19 *Ilustramos paso a paso con la notación del algoritmo el ejemplo anterior pero intercambiando f_1 y f_2. Así, dividiremos $f = x^2y + xy^2 + y^2$ por $f_1 = y^2 - 1$ y $f_2 = xy - 1$ en $\mathbb{Q}[x, y]$ bajo orden monomial lex. Inicializamos:*
$a_1 := a_2 := r := 0$ y $p := f = x^2y + xy^2 + y^2$
$p \neq 0$ así que $i := 1$, division?:=0 y como también $1 = i \leq s = 2$, preguntamos si $TL(f_1)$=y^2 divide a $TL(p) = x^2y$. Esto no pasa, así que $i := 1 + 1 = 2$. Ahora, division? sigue siendo 0 y $2 = i \leq s = 2$, por lo que preguntamos si $TL(f_2) = xy$ divide a $TL(p) = x^2y$. Como esto sí sucede, $a_2 := 0 + TL(p)/TL(f_2) = 0 + x = x$, $p := x^2y + xy^2 + y^2 - x(xy - 1) = xy^2 + x + y^2$, y division?:=1.
En la condición del MIENTRAS interno, se tiene que $2 = i \leq s = 2$ pero como division?=1, ya no entra en el ciclo ni en el siguiente SI, por lo que regresa al MIENTRAS principal. En éste, $p \neq 0$ todavía por lo que vemos de nuevo si hay una divisibilidad: $i := 1$, division?:=0, $1 = i \leq s = 2$ y preguntamos si $TL(f_1)$=y^2 divide a $TL(p) = xy^2$. Ahora sí sucede, por lo que $a_1 := 0 + TL(p)/TL(f_1) = x$, $p := xy^2 + x + y^2 - x(y^2 - 1) = 2x + y^2$, y division?:=1.
Regresamos al MIENTRAS principal, todavía $p \neq 0$ así que entramos de nuevo: esta vez ni $TL(f_1)$ ni $TL(f_2)$ dividen a $TL(p) = 2x$, por lo que después de dos vueltas, se tendrá $i := 2 + 1 = 3$ y aún division?=0. Entramos pues a la condición del SI y se pasará al residuo: $r := 0 + TL(p) = 2x$ y $p := 2x + y^2 - 2x = y^2$. Al tener ahora $TL(p) = y^2$ sí será divisible por $TL(f_1) = y^2$ y así $a_1 := x + 1$, $p := y^2 - (y^2 - 1) = 1$ y division?:=1. Después de no entrar al SI, se entra una vez más al MIENTRAS principal, y como $TL(p) = 1$ no será divisible por ninguno de los $TL(f_i)$ se pasará al residuo: $r := 2x + 1$ y $p := 1 - 1 = 0$. Cuando se regrese al MIENTRAS principal se tendrá $p = 0$ por lo que el algoritmo termina.
La expresión final para f es pues:

$$x^2y + xy^2 + y^2 = (x + 1)f_1 + xf_2 + r = (x + 1)(y^2 - 1) + x(xy - 1) + (2x + 1)$$

Al comparar con la expresión 2.1, en efecto se tienen coeficientes y residuos distintos. Es decir, aunque siguiendo el algoritmo siempre se llegará al mismo resultado, el orden de los divisores f_i's afecta la expresión final (de ahí que se especificara a F como $s-$tupla ordenada y no simplemente como conjunto). Este fenómeno lleva a la siguiente definición:

Definición 27 *Sea* $f \in k[x_1, x_2, ..., x_n]$, *si* $f_1, f_2, ..., f_s \in k[x_1, x_2, ..., x_n]$ *son tales que*

$$f = a_1 f_1 + a_2 f_2 + ... + a_s f_s + r$$

para algunos $a_1, a_2, ..., a_s, r \in k[x_1, x_2, ..., x_n]$, *con cada término de* r *no divisible por ninguno de* $TL(f_1), TL(f_2), ..., TL(f_s)$ *y multigrado*$(f) \geq$*multigrado*$(a_i f_i)$ $\forall i = 1, ..., n$, *se dice que se tiene una* expresión estándar *de* f *y que* f se reduce *a* r *por medio de* $F = \{f_1, f_2, ..., f_s\}$, *denotado* $f \xrightarrow{F} r$. *Llamamos a* r *una* reducción *de* f *por medio de* F.

Observación 14 *Según lo visto en el teorema anterior, el Algoritmo de la Division Multivariado siempre arroja expresiones estándar de* f. *En particular,* $\overline{f}^F = r$ *implica que* $f \xrightarrow{F} r$.

Ejemplo 20 *De los dos ejemplos anteriores, tenemos que:*

$$\begin{aligned} x^2y + xy^2 + y^2 &= (x+y)(xy-1) + 1(y^2-1) + (x+y+1) \\ x^2y + xy^2 + y^2 &= x(xy-1) + (x+1)(y^2-1) + (2x+1) \end{aligned}$$

son dos expresiones estándar distintas para $f = x^2y + xy^2 + y^2$. *Tanto* $r_1 = x + y + 1$ *y* $r_2 = 2x + 1$ *son reducciones de* f *por medio de* $F = \{xy - 1, y^2 - 1\}$

2.3. Definición y propiedades de Bases de Gröbner

En esta sección definimos finalmente el concepto que nombra a este capítulo. Todo el tiempo se considera un orden monomial $<$ fijo.

Definición 28 *Sea* $G \subseteq k[x_1, x_2, ..., x_n]$, *se define* $TL(G) = \{TL(g) | g \in G \backslash \{\overline{0}\}\}$ *y al ideal generado* $\langle TL(G) \rangle$ *se le llama* ideal inicial *de* G.

Definición 29 *Sean $G \subseteq I \subseteq k[x_1, x_2, ..., x_n]$, G finito e I ideal. G es una* base de Gröbner *de I sii $\langle TL(G)\rangle = \langle TL(I)\rangle$.*

Una idea tentadora para encontrar una base de Gröbner sería la de encontrar un conjunto finito de polinomios generadores del ideal: $g_1, g_2, ..., g_s \in I$ tales que $\langle g_1, g_2, ..., g_s\rangle = I$, y 'esperar' que $\langle TL(g_1), TL(g_2), ..., TL(g_s)\rangle = \langle TL(I)\rangle$. Esto no es cierto en general, es decir, aunque naturalmente es cierto que

$$\langle TL(g_1), TL(g_2), ..., TL(g_s)\rangle \subseteq \langle TL(I)\rangle$$

la contención puede ser propia, como lo muestra el siguiente ejemplo:

Ejemplo 21 *Sea $I = \langle f, g\rangle$ con $f = x^3 - 2xy$, $g = x^2y - 2y^2 + x$ con orden grlex. Entonces $\langle TL(f), TL(g)\rangle = \langle x^3, x^2y\rangle$ pero notar que*

$$h = x \cdot g - y \cdot f = x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^2 \in I$$

por lo que $TL(h) = x^2 \in \langle TL(I)\rangle$ pero x^2 no es divisible ni por x^3 ni por x^2y, es decir, $x^2 \notin \langle x^3, x^2y\rangle$. Así, $\langle TL(f), TL(g)\rangle \subset \langle TL(I)\rangle$ Se puede ver (como lo haremos en la siguiente sección) que una base de Gröbner de I es

$$G = \{2y^2 - x, xy, x^2\}$$

Lo que sí es cierto es que si G es una base de Gröbner de I, entonces G genera a I (de ahí el nombre de 'base'):

Proposición 13 *"Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal y G una base de Gröbner de I, entonces $\langle G\rangle = I$."*

Demostración. Sea $G = \{g_1, g_2, ..., g_s\}$. Puesto que $G \subseteq I$, se tiene $\langle G\rangle \subseteq I$. Ahora, sea $f \in I$, por Algoritmo de la División, si dividimos f por $(g_1, g_2, ..., g_s)$ existen $a_i, r \in k[x_1, x_2, ..., x_n]$ con $i = 1, ..., s$ tales que

$$f = a_1g_1 + a_2g_2 + ... + a_sg_s + r$$

y tal que $r = 0$ o bien $TL(g_i) \nmid t \ \forall i = 1, ..., s \quad \forall t \in T(r)$. Notar que si $r = 0$ hemos acabado pues $f = a_1g_1 + a_2g_2 + ... + a_sg_s$ implica que $f \in \langle G\rangle$. Ésta es la única posibilidad, pues si $r \neq 0$, como $r = f - a_1g_1 - a_2g_2 - ... - a_sg_s \in I$, entonces $TL(r) \in TL(I) \subseteq \langle TL(I)\rangle$. Pero G es base de Gröbner, luego $\langle TL(I)\rangle = \langle TL(g_1), TL(g_2), ..., TL(g_s)\rangle$ y así $TL(r) \in \langle TL(g_1), TL(g_2), ..., TL(g_s)\rangle$, que por la Proposición 12 parte (a) implica que existe $i \in \{1, ..., r\}$ tal que $TL(g_i)|TL(r)$, contradiciendo la propiedad del residuo. ■

Observación 15 *Notar que en la demostración de la proposición anterior probamos que si G es base de Gröbner (ordenada de alguna forma) de I y $f \in I$, entonces $\overline{f}^G = 0$. Este resultado será importante y lo enunciaremos como corolario del siguiente teorema.*

Otra propiedad importante de las bases de Gröbner, es que determinan residuos o reducciones únicas:

Teorema 8 *"Sea $G = \{g_1, g_2, ..., g_s\}$ una base de Gröbner para el ideal $I \subseteq k[x_1, x_2, ..., x_n]$ y $f \in k[x_1, x_2, ..., x_n]$, entonces existe un único $r \in k[x_1, x_2, ..., x_n]$ con las siguientes dos propiedades:*
(i) Ningún término de r es divisible por alguno de $TL(g_1), TL(g_2), ..., TL(g_s)$.
(ii) Existe $g \in I$ tal que $f = g + r$.
En particular, r es el residuo de la división de f por G sin importar el orden de los elementos en G".

Demostración. Al tomar a los elementos de G ordenados $G = (g_1, g_2, ..., g_s)$ y al hacer la división de f por G, obtenemos que $f = a_1g_1 + a_2g_2 + ... + a_sg_s + r$, con r el residuo. Como r cumple (i) y cada $g_i \in I$ implica $g := a_1g_1 + a_2g_2 + ... + a_sg_s \in I$, también r cumple (ii).
Para probar la unicidad, sean r' y g' que cumplen también (i) y (ii), entonces $f = g + r = g' + r'$, por lo que $r - r' = g - g' \in I$. Si $r - r' \neq 0$, al ser G de Gröbner tendríamos que $TL(r - r') \in \langle TL(I)\rangle = \langle TL(g_1), TL(g_2), ..., TL(g_s)\rangle$, de donde el término $TL(r - r')$ sería divisible por alguno de los $TL(g_i)$, que es imposible pues cada uno de los términos de r y r' no lo era.[4] Así, $r - r' = g - g' = 0$, concluyendo la unicidad. ■

Corolario 4 *"Sea $G = \{g_1, g_2, ..., g_s\}$ una base de Gröbner para el ideal $I \subseteq k[x_1, x_2, ..., x_n]$ y $f \in k[x_1, x_2, ..., x_n]$. Entonces $f \in I$ si y sólo si $\overline{f}^G = 0$"*

Demostración. $\Longleftarrow$) Si $f = g$ $(r = 0)$ con $g = a_1g_1 + a_2g_2 + ... + a_sg_s \in I$, claramente $f \in I$.

$\Longrightarrow$) Como se puede escribir $f = f + 0$ con $f \in I$, la unicidad implica que $r = \overline{f}^G = 0$. ■

Dado $I \subseteq k[x_1, x_2, ..., x_n]$, ¿siempre existe una base de Gröbner de I? La respuesta es afirmativa, puesto que $\langle TL(I)\rangle$ es un ideal en $k[x_1, x_2, ..., x_n]$ y recordando de

[4] Recordar que por la Proposición 11 parte (b), $M(r - r') \subseteq M(r) \cup M(r')$

la Sección 1.1 que éste debe ser finitamente generado (consecuencia del TEOREMA DE LA BASE DE HILBERT), y así (ver la Proposición 12 parte (c)) del conjunto de generadores $TL(I) = \{TL(g)|g \in I\backslash\{\overline{0}\}\}$ se puede extraer un número finito de $g_1, g_2, ..., g_s \in I$ tal que $\langle TL(I)\rangle = \langle TL(g_1), TL(g_2), ..., TL(g_s)\rangle$, es decir, $G = \{g_1, g_2, ..., g_s\}$ es base de Gröbner de I.

Ahora, ¿es única la base de Gröbner? La respuesta es negativa, puesto que si G es base de Gröbner, entonces cualquier $G \subseteq G' \subseteq I$ también lo será:

$$\langle TL(I)\rangle = \langle TL(G)\rangle \subseteq \left\langle TL(G^{'})\right\rangle \subseteq \langle TL(I)\rangle$$

Sin embargo, en este caso pensaríamos que hay elementos 'redundantes' en G', pues nos bastan como generadores los de G.
Notar que de hecho como lo que importa en la definición de base de Gröbner es el ideal generado por los términos líderes, los coeficientes de los polinomios se pueden variar y los demás términos pueden modificarse con 'flexibilidad' En el ejemplo 21 con base de Gröbner $G = \{2y^2 - x, xy, x^2\}$, entonces $G' = \{2y^2 - x, xy, x^2 + \lambda xy\}$ con $\lambda \in k$ también sería base de Gröbner, siendo el término λxy 'redundante' pues es divisible por $TL(xy) = xy$.
La anterior discusión inspira la siguiente definición:

Definición 30 *Una base de Gröbner G para un ideal I es* reducida *sii todos los polinomios en G son mónicos (es decir, $CL(g) = 1\ \forall g \in G$) y $\forall i \neq j$ ningún monomio $m \in M(g_j)$ es divisible por $TL(g_i)$*

Teorema 9 *"Todo ideal $I \subseteq k[x_1, x_2, ..., x_n]$ tiene una única base de Gröbner reducida"*

Demostración. Primero veamos cómo a partir de una base de Gröbner $G = \{g_1, g_2, ..., g_s\}$ de I se puede obtener una reducida. Sin pérdida de generalidad podemos suponer que los elementos de G ya cumplen que ningún $TL(g_j)$ es divisible por algún otro $TL(g_i)$ (de lo contrario, se puede eliminar g_j y $G - \{g_j\}$ sigue siendo base de Gröbner). La condición de que sean mónicos se puede verificar simplemente multiplicando al final cada g_i por $1/CL(g_i)$, y el ideal generado es invariante. Para asegurar la segunda condición, llamemos a $g_j \in G$ *reducido* sii ningún $m \in M(g_j)$ es divisible por $TL(g_i)\ \forall i \neq j$. Es claro entonces que buscamos que todos los elementos de G sean reducidos.
Sea $g_j \in G$, y consideramos $g'_j = \overline{g_j}^{G-\{g_j\}}$, por definición de residuo se tiene que ningún $m \in M(g'_j)$ es divisible por $TL(g_i)\ \forall i \neq j$. Pero además como $TL(g_j)$ no es

divisible por ningún $TL(g_i)$, en el Algoritmo de la División se tendrá que $TL(g_j)$ irá al residuo g'_j. Es decir, $TL(g_j) = TL(g'_j)$ y $G' = (G - \{g_j\}) \cup \{g'_j\}$ es base de Gröbner de I con g'_j reducido.
Finalmente, notar que si g es reducido para G entonces también lo será para cualquier otra base de Gröbner de I que lo contenga y tenga al mismo conjunto de términos líderes. Como éste es el caso al cambiar cada g_j por g'_j, en un número finito de reemplazos obtenemos una base de Gröbner reducida.

Para la unicidad, sean $G = \{g_1, g_2, ..., g_r\}$ y $G' = \{g'_1, g'_2, ..., g'_m\}$ bases de Gröbner reducidas de I. Como

$$\langle TL(g_1), TL(g_2), ..., TL(g_r)\rangle = \langle TL(I)\rangle = \langle TL(g'_1), TL(g'_2), ..., TL(g'_m)\rangle$$

de la Proposición 12 parte (a), se tiene que para $TL(g_i)$ existe un $TL(g'_j)$ que lo divide y viceversa, para este último existe algún $TL(g_k)$ que lo divide. Pero esto implica $TL(g_k)|TL(g_i)$, y por ser G reducida esto implica que $i = k$, lo que implica a su vez que $TL(g_i) = TL(g'_j)$. Así $m = r$ y reordenando, podemos suponer sin pérdida de generalidad que $TL(g_i) = TL(g'_i)$ con $i = 1, 2, ..., r$.
Consideramos $g_j - g'_j \in I$, luego $\overline{g_j - g'_j}^G = 0$, pero por otro lado ningún término en $g_j - g'_j$ es divisible por alguno de los $TL(g_i)$ con $i \neq j$ (g_j y g'_j reducidos). Es más, ni siquiera son divisibles por $TL(g_j) = TL(g'_j)$ porque este término se cancela en la resta $g_j - g'_j$, por lo que el residuo es el mismo polinomio $g_j - g'_j = \overline{g_j - g'_j}^G = 0$, de donde concluimos que $g_j = g'_j$. Por lo tanto, $G = G'$. ■

Ejemplo 22 *La base de Gröbner reducida del ideal total $I = k[x_1, x_2, ..., x_n]$ es $G = \{1\}$. En efecto, sea $G = \{g_1, g_2, ..., g_r\}$ base de Gröbner reducida de I. Como $1 \in I$ tenemos que existe algún $j \in \{1, ..., r\}$ tal que $TL(g_j)|TL(1) = 1$, por lo que $TL(g_j)$ es constante. Así, $TL(g_j)$ divide a cualquier otro $TL(g_i)$ y como G es reducida significa que $r = 1$, es decir, $G = \{g_j\}$. Finalmente, como g_j debe ser mónico, entonces $g_j = 1$.*

2.4. Algoritmo de Buchberger

Aunque la existencia de bases de Gröbner queda resuelta en la sección anterior, la demostración no indica cómo poder encontrar una base de Gröbner en la práctica. Es más, dado un conjunto propuesto como base de Gröbner de un ideal, no tenemos una forma eficiente de demostrar que efectivamente lo es. En esta sección presentamos un algoritmo que sí lo hace, ideado por el mismo Bruno Buchberger.

Definición 31 *Sean $<$ orden monomial y $f, g \in k[x_1, x_2, ..., x_n] - \{0\}$, definimos el $S-$polinomio de f y g como*

$$S(f,g) = \frac{[ML(f); ML(g)]}{TL(f)} f - \frac{[ML(f); ML(g)]}{TL(g)} g$$

Observación 16 *Notar que por definición $S(g,f) = -S(f,g)$ y también que:*

$$TL\left(\frac{[ML(f); ML(g)]}{TL(f)} f\right) = [ML(f); ML(g)] = TL\left(\frac{[ML(f); ML(g)]}{TL(g)} g\right)$$

por lo que este término se cancela en $S(f,g)$.

Ejemplo 23 *Sean $f = x^3y^2 - x^2y^3 + x$ y $g = 3x^4y + y^2$ en $\mathbb{R}[x,y]$ con grlex. Entonces $[ML(f); ML(g)] = [x^3y^2; x^4y] = x^4y^2$ y así*

$$S(f,g) = \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g = x(x^3y^2 - x^2y^3 + x) - \frac{y}{3}(3x^4y + y^2) = -x^3y^3 + x^2 - \frac{1}{3}y^3$$

Sea $I = \langle f, g \rangle$ y queremos ver si $\langle TL(I) \rangle = \langle TL(f), Tl(g) \rangle$, es decir, si $G = \{f, g\}$ es base de Gröbner. Por la observación anterior, $S(f,g)$ sería un candidato de un polinomio en I de forma que

$$TL(S(f,g)) \in \langle TL(I) \rangle \text{ pero } TL(S(f,g)) \notin \langle TL(f), Tl(g) \rangle .$$

De hecho, en el ejemplo 21, notar que el polinomio h propuesto es justo $S(g,f)$. Éste no era divisible por $TL(f)$ ni $TL(g)$ por lo que sirvió para mostrar que G no era base de Gröbner. El célebre Criterio de Buchberger permite caracterizar las bases de Gröbner mediante los residuos de los $S-$*polinomios* :

Teorema 10 *(CRITERIO DE BUCHBERGER) "Sea $<$ un orden monomial en $k[x_1, x_2, ..., x_n]$ e $I = \langle g_1, g_2, ..., g_m \rangle$ un ideal con $g_i \neq 0$ $\forall i = 1, ..., m$. Entonces $G = \{g_1, g_2, ..., g_m\}$ es una base de Gröbner de I si y sólo si $S(g_i, g_j) \xrightarrow{G} 0$ $\forall 1 \leq i < j \leq m$"*

Demostración. $\Longrightarrow$) Como $S(g_i, g_j) \in I$ y $G = \{g_1, g_2, ..., g_m\}$ es una base de Gröbner de I, sabemos que $\overline{S(g_i, g_j)}^G = 0$ $\forall 1 \leq i < j \leq m$, por lo que (según la Observación 14) $S(g_i, g_j) \xrightarrow{G} 0$ $\forall 1 \leq i < j \leq m$.

$\Longleftarrow$) Sup. $S(g_i, g_j) \xrightarrow{G} 0 \quad \forall 1 \leq i < j \leq m$ y sin pérdida de generalidad que todos los g_i son mónicos. Sea $0 \neq f \in I$. Queremos demostrar que $TL(f)$ es divisible por algún $TL(g_i)$ p.a. $i = 1, ..., m$, pues esto implicaría que $TL(I) \subseteq \langle TL(g_1), TL(g_2), ..., TL(g_s)\rangle$ y concluiríamos que G es base de Gröbner de I. Como $f \in I$, existen $h_1, h_2, ..., h_m \in k[x_1, x_2, ..., x_n]$ tal que $f = \sum_{i=1}^{m} h_i g_i$ y por la Proposición 11 (b) tenemos que $TL(f) \leq \text{máx}_{1\leq i\leq m}\{TL(h_i g_i)\}$. Si se diera la igualdad, $TL(f) = TL(h_j g_j) = TL(h_j)TL(g_j)$ para alguna j, de donde habríamos terminado.
Consideremos pues el caso $TL(f) < \text{máx}_{1\leq i\leq m}\{TL(h_i g_i)\}$ y veamos que existe una nueva expresión $f = \sum_{i=1}^{m} h'_i g_i$ tal que

$$TL(f) \leq \max_{1\leq i\leq m} \{TL(h'_i g_i)\} < \max_{1\leq i\leq m} \{TL(h_i g_i)\}$$

por lo que podemos continuar de esta manera hasta que se dé la igualdad, reduciendo al caso anterior la demostración.
Sea $t = \text{máx}_{1\leq i\leq m}\{TL(h_i g_i)\}$ y sin pérdida de generalidad suponemos que $TL(h_i g_i) = t \quad \forall 1 \leq i \leq r$ y $TL(h_i g_i) < t \ \forall r < i \leq m$. Como $TL(f) < t$, por la proposición 11 (c) tenemos que si $c_i = CL(h_i)$, entonces $\sum_{i=1}^{r} c_i = 0$. Como $TL(h_1)TL(g_1) = TL(h_i)TL(g_i) = t \quad \forall i \leq r$, se sigue $[ML(g_1); ML(g_i)] \mid t$ y si denotamos

$$d_i = \frac{TL(h_1)TL(g_1)}{[ML(g_1); ML(g_i)]} = \frac{TL(h_i)TL(g_i)}{[ML(g_1); ML(g_i)]}$$

entonces $d_i S(g_1, g_i) = TL(h_1)g_1 - TL(h_i)g_i$ y $TL(d_i S(g_1, g_i)) < t$.
Ahora, como por hipótesis $S(g_i, g_j) \xrightarrow{G} 0 \ \forall i = 1, ..., m$ existen $h'_{ij} \in k[x_1, x_2, ..., x_n]$ tal que $S(g_1, g_i) = \sum_{j=1}^{m} h'_{ij} g_j$y $\forall g_j \neq 0$ se cumple que multigrado$(h'_{ij} g_j)$ es menor o igual que multigrado$(S(g_1, g_i))$, i.e., $TL(h'_{ij} g_j) \leq TL(S(g_1, g_i))$. Se sigue que:

$$d_i S(g_1, g_i) = \sum_{j=1}^{m} d_i h'_{ij} g_j = \sum_{j=1}^{m} h_{ij} g_j$$

con $h_{ij} = d_i h'_{ij}$ y $TL(h_{ij} g_j) \leq TL(d_i S(g_1, g_i)) < t \ \forall i, j$. Así:

$$TL(h_1)g_1 - TL(h_i)g_i - \sum_{j=1}^{m} h_{ij} g_j = 0$$

con $TL(h_{ij}g_j) < t \ \ \forall i,j$. Por otro lado, recordando que $\sum_{i=1}^{r} c_i = 0$, tenemos:

$$\sum_{i=2}^{r} c_i(TL(h_1)g_1 - TL(h_i)g_i) = TL(h_1)g_1(-c_1) - \sum_{i=2}^{r} c_i TL(h_i)g_i = -\sum_{i=1}^{r} c_i TL(h_i)g_i$$

Por lo que podemos reescribir a f de la siguiente forma:

$$\begin{aligned}
f &= \sum_{i=1}^{r} h_i g_i + \sum_{i=r+1}^{m} h_i g_i \\
&= \sum_{i=1}^{r} h_i g_i + \sum_{i=2}^{r} c_i \cdot 0 + \sum_{i=r+1}^{m} h_i g_i \\
&= \sum_{i=1}^{r} h_i g_i + \sum_{i=2}^{r} c_i \left(TL(h_1)g_1 - TL(h_i)g_i - \sum_{j=1}^{m} h_{ij} g_j \right) + \sum_{i=r+1}^{m} h_i g_i \\
&= \sum_{i=1}^{r} h_i g_i + \sum_{i=2}^{r} c_i \left(TL(h_1)g_1 - TL(h_i)g_i \right) - \sum_{i=2}^{r} c_i \left(\sum_{j=1}^{m} h_{ij} g_j \right) + \sum_{i=r+1}^{m} h_i g_i \\
&= \sum_{i=1}^{r} h_i g_i - \sum_{i=1}^{r} c_i TL(h_i)g_i + \sum_{i=r+1}^{m} h_i g_i - \sum_{i=2}^{r}\sum_{j=1}^{m} c_i h_{ij} g_j \\
&= \sum_{i=1}^{r} (h_i - c_i TL(h_i))g_i + \sum_{i=r+1}^{m} h_i g_i - \sum_{j=1}^{m} \left(\sum_{i=2}^{r} c_i h_{ij} \right) g_j \\
&= \sum_{i=1}^{r} (h_i - c_i TL(h_i))g_i + \sum_{i=r+1}^{m} h_i g_i - \sum_{i=1}^{m} \left(\sum_{j=2}^{r} c_j h_{ji} \right) g_i \\
&= \sum_{i=1}^{r} \left(h_i - c_i TL(h_i) - \sum_{j=2}^{r} c_j h_{ji} \right) g_i + \sum_{i=r+1}^{m} \left(h_i - \sum_{j=2}^{r} c_j h_{ji} \right) g_i \\
&= \sum_{i=1}^{m} h'_i g_i
\end{aligned}$$

con

$$h'_i = \begin{cases} h_i - c_i TL(h_i) - \sum_{j=2}^{r} c_j h_{ji} \text{ si } i = 1, ..., r \\ h_i - \sum_{j=2}^{r} c_j h_{ji} \text{ si } i = r+1, ..., m \end{cases}$$

Finalmente, de la definición de h'_i y recordando que $TL(h_{ji}g_i) < t \ \ \forall i,j$, tenemos que $\text{máx}_{1 \le i \le m}\{TL(h'_i g_i)\} < t = \text{máx}_{1 \le i \le m}\{TL(h_i g_i)\}$, como buscábamos. ■

Gracias al teorema anterior, podemos definir finalmente un algoritmo que calcule una base de Gröbner para un ideal $I = \langle f_1, f_2, ..., f_r \rangle$. Comenzamos con $G = \{f_1, f_2, ..., f_r\}$ y para cada par de elementos en G calculamos su $S-$polinomio y su residuo respecto a G. Si todos los residuos son 0, el algoritmo termina y tenemos una base de Gröbner. Si algún residuo no es cero, lo agregamos a G como generador y volvemos al paso anterior. Tanto en los pasos intermedios como al final se puede reducir G para obtener la base de Gröbner reducida. La forma más básica del algoritmo estructurado se vería así:

Algoritmo 2 *(DE BUCHBERGER)*

Entradas: $F = (f_1, f_2, ..., f_s)$ generadores de I

Salidas: $G = (g_1, g_2, ..., g_t)$ base de Gröbner de I con $F \subseteq G$

$G := F$

REPITE

$G' := G$

PARA cada $\{p, q\}$, $p \neq q$ en G'

$S := \overline{S(p,q)}^{G'}$

SI $S \neq 0$

$G := G \cup \{S\}$

HASTA $G = G'$

FIN

Vale la pena notar que en cada paso no es necesario checar todos los S-polinomios, los que ya dieron 0 seguirán dando 0 cuando G se aumente. Asimismo, al agregar $\overline{S(p,q)}^{G'} \neq 0$ a G, es claro que ya se tendrá que $\overline{S(p,q)}^{G} = 0$ por lo que ya no es necesario checarlo en el siguiente ciclo cuando se actualice G'.

Demostremos que el algoritmo funciona. Notar que siempre se cumple que $G \subseteq I$, pues esto sucede en la inicialización y cada $S(p,q) \in I$, por lo que cada residuo no cero agregado S está en I. De hecho, en todo momento cada G genera a I pues F lo generaba y $F \subseteq G$. El algoritmo termina cuando $G = G'$, es decir, no se agregó ningún residuo que modificara G. En otras palabras, $\overline{S(p,q)}^{G} = 0$ $\forall p \neq q \in G$, y en particular $S(p,q) \xrightarrow{G} 0 \ \ \forall p \neq q \in G$, que por el Criterio de Buchberger implica que G es base de Gröbner.

Sólo resta probar algo esencial: que el algoritmo termina. Notar que cada vez que se agrega un residuo S a G, se tiene que $G' \subset G$, por lo que

$$\langle TL(G')\rangle \subseteq \langle TL(G)\rangle$$

pero afirmamos que la contención es propia. En efecto, sea $r \in G - G'$ un residuo no cero agregado. Entonces $TL(r) \in \langle TL(G)\rangle$, pero como r es el residuo de dividir por G', $TL(r)$ no es divisible por ninguno de los términos líderes de G', es decir, $TL(r) \notin \langle TL(G')\rangle$. Así que cada vez que se agrega algún elemento a G, se tiene:

$$\langle TL(G')\rangle \subset \langle TL(G)\rangle$$

Si el algoritmo nunca terminara, se tendría una cadena ascendente infinita que no se estaciona, contradiciendo que $k[x_1, x_2, ..., x_n]$ es Noetheriano. (TEOREMA DE LA BASE DE HILBERT).

Ejemplo 24 *Sea* $I = \langle f, g\rangle$ *con* $f = xy - zw$ *y* $g = -y^2 + xz$ *en* $k[x, y, z, w]$ *con orden monomial grevlex. Así* $F = \{f, g\}$ *e inicializamos* $G := F$. *Así,* $G' := G$ *también y la única pareja de polinomios en* G' *es* $\{f, g\}$. *De* $TL(f) = xy$ *y de* $TL(g) = -y^2$ *tenemos* $[ML(f); ML(g)] = xy^2$. *Calculamos*

$$S(f, g) = \frac{xy^2}{xy}f - \frac{xy^2}{-y}g = y(xy - zw) + x(-y^2 + xz) = x^2z - yzw$$

En este caso el residuo $S := \overline{S(f, g)}^{G}$ *es el mismo* $h = x^2z - yzw$, *que es distinto de* 0 *y por tanto se actualiza* $G := \{f, g\} \cup \{h\}$. *Como* $G = \{f, g\} \neq G'$ *se entra de nuevo al ciclo.* $G' := G = \{f, g, h\}$. *De la observación ya hecha, no es necesario checar* $S(f, g)$ *pues es* h *(*$h = 0 \cdot f + 0 \cdot g + 1 \cdot h + 0$ *con residuo* 0*) y así el residuo* $\overline{S(f, g)}^{h} = 0$ *y no se agrega. Vamos por la pareja* (f, h).*Como* $TL(h) = x^2z$ *tenemos que* $[ML(f); ML(h)] = x^2yz$, *entonces*

$$S(f, h) = \frac{x^2yz}{xy}f - \frac{x^2yz}{x^2z}h = xz(xy - zw) - y(x^2z - yzw) = -xz^2w + y^2zw$$

pero notar que $S(f, h) = zw\,(y^2 - xz) = zw \cdot g + 0$, *por lo que* $\overline{S(f, h)}^{G'} = 0$, *y* G *no cambia. Falta verificar* (g, h). *Tenemos que* $[ML(g); ML(h)] = x^2y^2z$ *y*

$$S(g, h) = \frac{x^2y^2z}{-y^2}g - \frac{x^2y^2z}{x^2z}h = -x^2z(-y^2 + xz) - y^2(x^2z - yzw) = y^3zw - x^3z^2$$

pero al dividir tenemos que $S(g, h) = -yzw \cdot g - xz \cdot h + 0$, *por lo que* $\overline{S(g, h)}^{G'} = 0$, *y* G *no cambia. Ya agotamos todas las parejas en* G' *por lo que al salir del ciclo y llegar a la condición* $G = G'$, *ésta se cumple (*$G = G' = \{f, g, h\}$*) y el algoritmo se detiene. Es decir,* $G = \{f, g, h\}$ *es una base de Gröbner de* I.

Terminamos esta sección completando lo prometido en el ejemplo 21:

Ejemplo 25 *Tenemos* $f_1 = x^3 - 2xy$ *y* $f_2 = x^2y - 2y^2 + x$ *con grlex y vimos que* $S(f_1, f_2) = -x^2$. *De hecho, de* $TL(f_1) = x^3$, $TL(f_2) = x^2y$ *y* $TL(S(f_1, f_2)) = -x^2$ *se tiene que* $\overline{S(f_1, f_2)}^{\{f_1,f_2\}} = -x^2 \neq 0$. *Sea entonces* $f_3 = -x^2$. *Ya tenemos pues* $\overline{S(f_1, f_2)}^{\{f_1,f_2,f_3\}} = 0$. *Por otro lado,*

$$S(f_1, f_3) = \frac{x^3}{x^3}(x^3 - 2xy) - \frac{x^3}{-x^2}(-x^2) = -2xy$$

y concluimos que $\overline{S(f_1, f_3)}^{\{f_1,f_2,f_3\}} = -2xy \neq 0$. *Llamamos pues a* $f_4 = -2xy$. *Seguimos checando:*

$$S(f_2, f_3) = \frac{x^2y}{x^2y}(x^2y - 2y^2 + x) - \frac{x^2y}{-x^2}(-x^2) = -2y^2 + x$$

y de nuevo $\overline{S(f_2, f_3)}^{\{f_1,f_2,f_3,f_4\}} = -2y^2+x \neq 0$. *Por lo tanto agregamos* $f_5 = -2y^2+x$ *que tiene* $TL(f_5) = -2y^2$. *Ahora:*

$$\begin{aligned}
S(f_1, f_4) &= \frac{x^3y}{x^3}(x^3 - 2xy) - \frac{x^3y}{-2xy}(-2xy) = -2xy^2 = yf_4 \\
S(f_2, f_4) &= \frac{x^2y}{x^2y}(x^2y - 2y^2 + x) - \frac{x^2y}{-2xy}(-2xy) = x - 2y^2 = -f_5 \\
S(f_3, f_4) &= \frac{x^2y}{-x^2}(-x^2) - \frac{x^2y}{-2xy}(-2xy) = 0 \\
S(f_1, f_5) &= \frac{x^3y^2}{x^3}(x^3 - 2xy) - \frac{x^3y^2}{-2y^2}(-2y^2 + x) = \frac{1}{2}x^4 - 2xy^3 = -\frac{1}{2}x^2f_3 + y^2f_4 \\
S(f_2, f_5) &= \frac{x^2y^2}{x^2y}(x^2y - 2y^2 + x) - \frac{x^2y^2}{-2y^2}(-2y^2 + x) = \frac{1}{2}f_1 - \frac{1}{2}f_4 + yf_5 \\
S(f_3, f_5) &= \frac{x^2y^2}{-x^2}(-x^2) - \frac{x^2y^2}{-2y^2}(-2y^2 + x) = \frac{1}{2}x^3 = -\frac{1}{2}xf_3 \\
S(f_4, f_5) &= \frac{xy^2}{-2xy}(-2xy) - \frac{xy^2}{-2y^2}(-2y^2 + x) = \frac{1}{2}x^2 = -\frac{1}{2}f_3
\end{aligned}$$

Por lo que $\overline{S(f_i, f_j)}^{\{f_1,f_2,f_3,f_4,f_5\}} = 0$ $\forall i < j$, *y así*

$$G = \{f_1, f_2, ..., f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$$

es base de Gröbner.
Ilustrando el proceso de reducción, notamos que $TL(f_1) = -xTL(f_3)$, *es decir,*

$TL(f_3)|TL(f_1)$ por lo que podemos eliminar a f_1 de G. Análogamente, $TL(f_2) = -\frac{1}{2}xTL(f_4)$, es decir, $TL(f_4)|TL(f_1)$ por lo que también podemos eliminar a f_2 de G. Así obtenemos la base de Gröbner del ejemplo 21 (salvo múltiplos constantes) y la base de Gröbner reducida es: $G_{red} = \{x^2, xy, y^2 - \frac{1}{2}x\}$.

Vale la pena mencionar que esta primera forma del Algoritmo está lejos de ser óptima. El lector atento puede haber notado que en los ejemplos anteriores hemos estado pidiendo la condición más restrictiva $\overline{S(p,q)}^G = 0 \ \ \forall p \neq q \in G$ en lugar de la enunciada en el Teorema: $S(g_i, g_j) \xrightarrow{G} 0 \ \forall p \neq q \in G$. Esto se debe a que gracias al Algoritmo de la División, tenemos una forma clara de calcular $\overline{S(p,q)}^G$, por lo que es sencillo saber si es o no 0. Por el contrario, en general no tenemos una forma de saber si $S(g_i, g_j) \xrightarrow{G} 0$ o no. Sin embargo, hay un caso en el que sí podemos explotar la idea de que basta pedir que el S-polinomio se reduzca a cero, aunque su residuo no sea cero:

Proposición 14 *"Sea $G \subseteq k[x_1, x_2, ..., x_n]\backslash\{\overline{0}\}$ y $f, g \in G$ tales que $ML(f)$ y $ML(g)$ son primos relativos, es decir, que*

$$[ML(f); ML(g)] = ML(f) \cdot ML(g),$$

entonces $S(f, g) \xrightarrow{G} 0$."

Demostración. Como ML no toma en cuenta el coeficiente líder, sin pérdida de generalidad podemos suponer que f y g son mónicos, de forma que $f = ML(f) + p$ y $g = ML(g) + q$. Entonces

$$\begin{aligned} S(f,g) &= \frac{[ML(f); ML(g)]}{ML(f)} f - \frac{[ML(f); ML(g)]}{ML(g)} g \\ &= \frac{ML(f) \cdot ML(g)}{ML(f)} f - \frac{ML(f) \cdot ML(g)}{ML(g)} g \\ &= ML(g)f - ML(f)g = (g-q)f - (f-p)g \\ &= gf - qf - fg + pg = pg - qf \end{aligned}$$

Se afirma que $pg - qf$ es una expresión estándar para $S(f, g)$ (de donde se seguiría que $S(f, g) \xrightarrow{G} 0$). En efecto, se debe tener que

$$multigrado(S(f,g)) = \text{máx}\{multigrado(pg), multigrado(qf)\}$$

(por lo que, $multigrado(pg) \leq multigrado(S(f,g))$ y
$multigrado(qf) \leq multigrado(S(f,g))$), pues si no se da la igualdad, de acuerdo a la Proposición 11 tendríamos que $ML(pg) = ML(qf)$ y por tanto

$$ML(p)ML(g) = ML(q)ML(f).$$

Pero entonces $ML(g)$ divide a $ML(q)ML(f)$, y como $ML(f)$ y $ML(g)$ son primos relativos, concluimos que $ML(g)|ML(q)$, que es imposible, pues $ML(q) < ML(g)$.

Ejemplo 26 *Ilustramos cómo el criterio de la proposición anterior puede ahorrar iteraciones en el algoritmo de Buchberger retomando el ejemplo anterior. En efecto, como*

$$TL(f_1) = x^3 \quad y \quad TL(f_5) = -2y^2$$

se tiene que son primos relativos y ya no es necesario checar $\overline{S(f_1, f_5)}^G = 0$. *Análogamente, como* $TL(f_3) = -x^2$ *entonces también es primo relativo con* $TL(f_5)$ *y ya no es necesario calcular el S-polinomio correspondiente* $S(f_3, f_5)$.

■

Para ver más mejoras al algoritmo se puede consultar [4] y [1]. Aún así, se puede apreciar que las cuentas pueden ser bastante tediosas si se hacen 'a mano'. Hay varios programas computacionales que calculan bases de Gröbner, entre ellos MAPLE con el paquete *Groebner* y otros programas más algebraicos como MACAULAY y REDUCE[5].

Como último comentario, como con k campo, $k[x]$ es un Dominio de Ideales Principales, el Algoritmo de Buchberger generaliza el Algoritmo de Euclides para encontrar el máximo común divisor $(f; g)$ de dos polinomios $f, g \in k[x]$. Lo anterior sucede porque $\langle f, g\rangle = \langle (f; g)\rangle$, por lo que la base de Gröbner reducida G del ideal $I = \langle f, g\rangle$ debe ser $G = \{(f; g)\}$.

[5] Para cuestiones de unicidad, el programa suele regresar una base de Gröbner reducida o uno de sus múltiplos escalares.

Capítulo 3

Aplicaciones de Bases de Gröbner

Veamos unas aplicaciones de esta teoría.

3.1. Problema de la Igualdad de Ideales

Resolvemos el siguiente problema:

Problema 1 *Dado* $I \subseteq k[x_1, x_2, ..., x_n]$ *ideal generado por* $f_1, f_2, ..., f_r$ *y* $J \subseteq k[x_1, x_2, ..., x_n]$ *ideal generado por* $g_1, g_2, ..., g_s$*, determinar si* $I = J$ *o* $I \neq J$*.*

Este problema no es trivial pues la relación entre los generadores puede ser nada evidente. Sin embargo, de la unicidad de las bases de Gröbner reducidas tenemos:

Solución 1 *Sea* G_I *la base de Gröbner reducida de* $I = \langle f_1, f_2, ..., f_r \rangle$ *y sea* G_J *la base de Gröbner reducida de* $J = \langle g_1, g_2, ..., g_s \rangle$*. Luego* $I = J$ *si y sólo si* $G_I = G_J$*.*

Por supuesto, la solución se justifica recordando que $\langle G_I \rangle = I$ y que $\langle G_J \rangle = J$.

Ejemplo 27 *Sean* $I = \langle x^2y + xy^2 - 2y, x^2 + xy - x + y^2 - 2y, xy^2 - x - y + y^3 \rangle$ *y* $J = \langle x - y^2, xy - y, x^2 - y \rangle$ *en* $k[x, y]$*. ¿Será cierto que* $I = J$*?*
Usando orden lex y sin entrar en detalles en el algoritmo de Buchberger, obtenemos que la base de Gröbner reducida de I *es* $G_I = \{x - y, y^2 - y\}$*. Por otro lado, la base de Gröbner reducida de* J *resulta* $G_J = \{x - y, y^2 - y\}$*. Como* $G_I = G_J$*, tenemos que* $I = J$*.*

3.2. Problema de la Membresía a un Ideal

Consideramos el siguiente problema:

Problema 2 *Sea I ideal en $k[x_1, x_2, ..., x_n]$ y $f \in k[x_1, x_2, ..., x_n]$. Determinar si $f \in I$ o $f \notin I$.*

De nuevo este problema puede ser difícil, sin embargo ya tenemos una forma de solucionarlo con el Corolario 4:

Solución 2 *Sea G una base de Gröbner de I, y dividimos f por G. Luego $f \in I$ si y sólo si el residuo $\overline{f}^G = 0$*

Ejemplo 28 *Sea $I = \langle xz - y^2, x^3 - z^2 \rangle$ en $\mathbb{R}[x, y, z]$ y $f = -4x^2y^2z^2 + y^6 + 3z^5$, $g = x^7y^2 + 2z^2 - xy^2z^3$ ¿$f, g \in I$?*
Usando orden grlex obtenemos la base de Gröbner:

$$G = \left\langle xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5 \right\rangle$$

Dividiendo f por $G = \{g_1, g_2, ..., g_5\}$ tenemos:

$$f = (-4xy^2z - 4y^4)g_1 + 0 \cdot g_2 + 0 \cdot g_3 + 0 \cdot g_4 - 3g_5 + 0$$

Como el residuo $\overline{f}^G = 0$, tenemos que $f \in I$.
Por otro lado, dividiendo g por G tenemos:

$$g = (x^3y^2z + x^2y^4 - y^2z^2)g_1 + x^4y^2g_2 + y^4g_3 + 0 \cdot g_4 + 0 \cdot g_5 + (y^4z^3 - y^4z^2 + 2z^2)$$

Como el residuo $\overline{g}^G = y^4z^3 - y^4z^2 + 2z^2 \neq 0$, tenemos que $g \notin I$.

Notar que en caso afirmativo, el algoritmo de división multivariado da explícitamente coeficientes que evidencian la pertenencia al ideal. También vale la pena observar que no se puede subestimar el papel que juegan las bases de Gröbner en este problema, considerando el siguiente ejemplo:

Ejemplo 29 *Sea $I = \langle xy + 1, y^2 - 1 \rangle$ y $f = xy^2 - x$. Si no consideramos una base de Gröbner de I y dividimos directamente por los generadores f_1, f_2 obtenemos del Algoritmo de la División:*

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$$

por lo que $\overline{f}^{(f_1,f_2)} = -x - y \neq 0$, pero NO podemos concluir que $f \notin I$. De hecho, $f = xf_2$ (pues $xy^2 - x = x(y^2 - 1)$), lo que evidencia que $f \in I$.

3.3. Problema de Consistencia

En el caso de que k es algebraicamente cerrado como con $k = \mathbb{C}$, podemos resolver el siguiente

Problema 3 *Sean $f_1, f_2, ..., f_s \in k[x_1, x_2, ..., x_n]$ que conforman el sistema de ecuaciones polinomiales en n variables*

$$\begin{aligned} f_1(x_1, x_2, ..., x_n) &= 0 \\ f_2(x_1, x_2, ..., x_n) &= 0 \\ &\vdots \\ f_s(x_1, x_2, ..., x_n) &= 0 \end{aligned}$$

¿El sistema tiene solución (es decir, es consistente) o bien, es inconsistente?

El problema en otros términos en realidad pregunta si $\mathcal{V}(f_1, f_2, ..., f_s) \neq \varnothing$ o bien $\mathcal{V}(f_1, f_2, ..., f_s) = \varnothing$. Este problema debe resultar conocido, pues lo discutimos en la sección de correspondencia entre ideales y variedades (sección 1.5). En efecto, ahí enunciamos el Nullstellensatz ('Débil'), que establecía que si k algebraicamente cerrado entonces

$$\mathcal{V}(I) = \varnothing \Leftrightarrow I = \langle 1 \rangle = k[x_1, x_2, ..., x_n]$$

Recordemos que si $n = 1$ podemos argumentar que gracias a que $k[x]$ es un D.I.P., $I = \langle f_1, f_2, ..., f_s \rangle = \langle f \rangle$ para alguna $f \in k[x]$ y así $\mathcal{V}(I) = \mathcal{V}(f_1, f_2, ..., f_s) = \mathcal{V}(f)$. Si f es constante no nula, se tiene $I = k[x]$ y $\mathcal{V}(f_1, f_2, ..., f_s) = \varnothing$. mientras que si f es no constante, se tiene que sí tiene raíces (k algebraicamente cerrado), concluyendo que $\mathcal{V}(f_1, f_2, ..., f_s) \neq \varnothing$. Así, podemos pensar que el Nullstellensatz dice que la situación con el ideal $I = \langle f_1, f_2, ..., f_s \rangle$ sigue determinando de la misma forma el problema cuando tenemos $n > 1$.

Así, cuando k algebraicamente cerrado tenemos la siguiente

Solución 3 *Sea G la base de Gröbner reducida de $I = \langle f_1, f_2, .., f_s \rangle \subseteq k[x_1, x_2, .., x_n]$ entonces el sistema es consistente si y sólo si $G \neq \{1\}$.*

Es claro que (aún con k no algebraicamente cerrado) que si $G = \{1\}$ entonces $\mathcal{V}(I) = \varnothing$ y el sistema es inconsistente. Por otro lado, si el sistema es inconsistente se tiene $\mathcal{V}(I) = \mathcal{V}(f_1, f_2, ..., f_s) = \varnothing$ por lo que Nullstellensatz Débil afirma que $I = k[x_1, x_2, ..., x_n]$, y por el ejemplo 22 se tiene que $G = \{1\}$.

Ejemplo 30 *Consideremos el sistema en* $\mathbb{C}[x, y]$:

$$\begin{aligned} x^2 + xy - 10 &= 0 \\ x^3 + xy^2 - 25 &= 0 \\ x^4 + xy^3 - 70 &= 0 \end{aligned}$$

Al calcular la base de Gröbner del ideal generado por los polinomios bajo orden monomial grlex (en realidad, bajo cualquiera) obtenemos que $G = \{1\}$, *por lo que el sistema es inconsistente.*

Ejemplo 31 *Consideremos el siguiente sistema en* $\mathbb{C}[x, y]$, *que es casi el del ejemplo anterior:*

$$\begin{aligned} x^2 + xy - 10 &= 0 \\ x^3 + xy^2 - 26 &= 0 \\ x^4 + xy^3 - 70 &= 0 \end{aligned}$$

Al calcular la base de Gröbner del ideal generado por los polinomios bajo orden monomial grlex obtenemos $G = \{x - 2, y - 3\} \neq \{1\}$ *por lo que el sistema sí es consistente, y es más, gracias a la base de Gröbner vemos inmediatamente que tiene como única solucíón al punto* $(2, 3) \in \mathbb{C}^2$.

3.4. Resolución de Sistemas de Ecuaciones Polinomiales

Generalizamos el problema clásico de resolución de sistemas de ecuaciones lineales a ecuaciones polinomiales:

Problema 4 *Sean* $f_1, f_2, ..., f_s \in k[x_1, x_2, ..., x_n]$ *que determinan el sistema de ecuaciones polinomiales*

$$\begin{aligned} f_1(x_1, x_2, ..., x_n) &= 0 \\ f_2(x_1, x_2, ..., x_n) &= 0 \\ &\vdots \\ f_s(x_1, x_2, ..., x_n) &= 0 \end{aligned}$$

Si el sistema es consistente, encontrar sus soluciones $(a_1, a_2, ..., a_n) \in k^n$ *(preferiblemente todas).*

Observación 17 *En otras palabras, dado* $I = \langle f_1, f_2, ..., f_s \rangle \subseteq k[x_1, x_2, ..., x_n]$, *determinar su variedad* $\mathcal{V}(I) \subseteq k^n$.

Por supuesto que este problema no es nada fácil en general, y no esperamos que las bases de Gröbner lo resuelvan mágicamente por completo. Sin embargo, sí pueden ser una técnica de ataque al problema bastante útil para dar con la solución. La idea será calcular cierta base de Gröbner $G = \{g_1, g_2, ..., g_t\}$ del ideal $I = \langle f_1, f_2, ..., f_s \rangle$ para cambiar el sistema original al sistema

$$\begin{aligned} g_1(x_1, x_2, ..., x_n) &= 0 \\ g_2(x_1, x_2, ..., x_n) &= 0 \\ &\vdots \\ g_t(x_1, x_2, ..., x_n) &= 0 \end{aligned}$$

que puesto que generan ambos al mismo ideal, por el Corolario 2 tenemos que el conjunto de soluciones $\mathcal{V}(I)$ es exactamente el mismo.
Idealmente, el sistema obtenido de esta forma será más sencillo de resolver que el original. Notar que esto fue justamente lo que sucedió en el Ejemplo 31, en el que obtuvimos ecuaciones que sólo involucraban x y y. En efecto, siguiendo la idea de Eliminación Gaussiana en el problema clásico, lo que buscaremos será ir eliminando variables consecutivamente para obtener ecuaciones sencillas de resolver, y luego hacer sustitución hacia atrás para completar de resolver el sistema. Para lograr esta eliminación, introducimos la siguiente

Definición 32 *Sea* $I \subseteq k[x_1, x_2, ..., x_n]$ *ideal y* $j \in \{1, 2, ..., n\}$ *fijo. Definimos el* $j-$*ésimo* ideal de eliminación I_j *como*

$$I_j = I \cap k[x_{j+1}, x_{j+2}, ..., x_n]$$

Observación 18 I_j *sí es un ideal en* $k[x_{j+1}, x_{j+2}, ..., x_n]$ *y es el conjunto de todos los polinomios en* I *en el que sólo pueden 'aparecer' variables desde* x_{j+1} *hasta* x_n.

Los ideales de eliminación cumplen la interpretación intuitiva de estar proyectando la variedad asociada $\mathcal{V}(I) \subseteq k^n$ sobre un espacio de dimensión menor.

Proposición 15 *"Sea* I_j *el j-ésimo ideal de eliminación de* $I \subseteq k[x_1, x_2, ..., x_n]$ *y* $\pi_j : k^n \to k^{n-j}$ *la función proyección*

$$\pi_j(a_1, a_2, ..., a_n) = (a_{j+1}, ..., a_n)$$

entonces $\pi_j(\mathcal{V}(I)) \subseteq \mathcal{V}(I_j)$*."*

Demostración. Si $f \in I_j$ y $(a_1, a_2, ..., a_n) \in \mathcal{V}(I)$, entonces $f(a_1, a_2, ..., a_n) = 0$; pero como f sólo tiene variables $x_{j+1}, ..., x_n$, podemos escribir

$$f(a_{j+1}, ..., a_n) = f(\pi_j(a_1, a_2, ..., a_n)) = 0$$

por lo que f se anula en todo $\pi_j(\mathcal{V}(I))$ y éste está contenido en los ceros comunes de los polinomios en I_j. ■

La idea entonces será estudiar las variedades asociados a los ideales de eliminación $\mathcal{V}(I_j)$, que en vista de la proposición contienen a las soluciones parciales $\pi_j(\mathcal{V}(I))$ de la solución buscada $\mathcal{V}(I)$.
El siguiente teorema, increíblemente útil para el resto de las aplicaciones, llamado incluso "almost too good to be true" en [12], permite calcular bases de Gröbner de ideales de eliminación:

Teorema 11 *(DE ELIMINACIÓN) "Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal y G una base de Gröbner de I respecto a un j-ésimo orden de eliminación, con $j \in \{1, 2, ..., n\}$. Entonces se tiene que*

$$G_j = G \cap k[x_{j+1}, x_{j+2}, ..., x_n]$$

es una base de Gröbner (bajo el orden inducido) del ideal de eliminación I_j"

Demostración. Sea $j \in \{1, 2, ..., n\}$, por definición tenemos que $G_j \subseteq I_j$ por lo que para probar que

$$\langle TL(I_j)\rangle = \langle TL(G_j)\rangle$$

resta probar que $\langle TL(I_j)\rangle \subseteq \langle TL(G_j)\rangle$. Sea $TL(f) \in TL(I_j)$ p.a. $f \in I_j$, como $I_j \subseteq I$ y G es base de Gröbner de I tenemos que para $f \in I$ existe $g \in G$ tal que $TL(g)|TL(f)$, pero como $f \in I_j$ en particular $TL(f)$ no contiene ninguna de las variables $x_1, x_2, ..., x_j$, por lo que $TL(g)$ tampoco. La observación esencial es que como estamos usando un j-ésimo orden de eliminación, cualquier término que contenga alguna de las variables $x_1, x_2, ..., x_j$ será necesariamente mayor en el orden que $TL(g)$, y puesto que $TL(g)$ es el $<-$máximo de los términos de g, se concluye que todos los términos restantes de g tampoco contienen a ninguna de las variables $x_1, x_2, ..., x_j$, por lo que $g \in I_j$. Es decir, $TL(f) \in TL(G_j)$ y así G_j es base de Gröbner de I_j. ■

Corolario 5 *"Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal y G una base de Gröbner de I respecto al orden lex con $x_1 > x_2 > ... > x_n$. Entonces para toda $j \in \{1, 2, ..., n\}$ se tiene que*

$$G_j = G \cap k[x_{j+1}, x_{j+2}, ..., x_n]$$

es una base de Gröbner del ideal de eliminación I_j"

De esta forma, basta con calcular una base de Gröbner para I y luego para tener una base de Gröbner para el j-ésimo ideal de eliminación sólo consideramos los polinomios en G en los que no aparece ninguna de las variables $x_1, x_2..., x_j$. En el contexto de la resolución del sistema de ecuaciones, al obtener éstas, estamos encontrando generadores para todas las consecuencias posibles de las ecuaciones generales que sólo involucran ciertas variables.

Solución 4 *(Parcial) Calcular una base de Gröbner bajo orden lexicográfico de forma que las variables se eliminarán de mayor a menor, y ahora resolver el nuevo sistema.*

Ejemplo 32 *Sea el sistema en* $\mathbb{C}[x, y]$:

$$\begin{aligned} xy^3 - x^2 &= 0 \\ x^3y^2 - y &= 0 \end{aligned}$$

Bajo el orden lexicográfico $y > x$ *obtenemos la base de Gröbner*

$$G = \{y - x^7, x^{12} - x^2\}$$

De donde rápidamente concluimos que las soluciones del sistema son:

$$\{(0, 0)\} \cup \{(\xi, \xi^7) | \xi^{10} = 1\}$$

Veamos otro ejemplo, ahora en tres variables:

Ejemplo 33 *Sea el sistema en* $\mathbb{R}[x, y, z]$:

$$\begin{aligned} x^2 + y^2 + z^2 - 1 &= 0 \\ 2x - 3y - z &= 0 \\ x^2 - 2x + y^2 + z^2 &= 0 \end{aligned}$$

Bajo el orden lexicográfico $z > y > x$ *obtenemos la base de Gröbner*

$$G = \{2x - 1, 3y + z - 1, 40z^2 - 8z - 23\}$$

De la primera ecuación tenemos inmediatamente que $x = \frac{1}{2}$ *y de la cuadrática en* z *obtenemos las dos soluciones:*

$$z = \frac{2 \pm 3\sqrt{26}}{20}$$

Por lo que sustituyendo en la segunda se obtiene

$$y = \frac{6 \mp \sqrt{26}}{20}$$

Para terminar presentamos un ejemplo de Multiplicadores de Lagrange, que suelen resolverse mediante un análisis de varios casos e ingenio para eliminar las variables. Veamos cómo simplifica el trabajo una base de Gröbner:

Ejemplo 34 *Consideramos el siguiente problema de optimización:*

$$\text{máx } x^2 + y^2 + xy$$

$$s.a. \quad x^2 + 2y^2 = 1$$

El sistema de multiplicadores de Lagrange asociado en $\mathbb{R}[x, y, \lambda]$ *es:*

$$\begin{aligned} 2x + y - 2\lambda x &= 0 \\ 2y + x - 4\lambda y &= 0 \\ x^2 + 2y^2 - 1 &= 0 \end{aligned}$$

Ya que conocer el valor del multiplicador λ *es secundario, eliminamos primeramente tal variable al utilizar orden lexicográfico* $\lambda > y > x$*. La base de Gröbner obtenida es:*

$$G = \{2\lambda - 3x^2, y - 3x^3 + 2x, 6x^4 - 6x^2 + 1\}$$

De la última ecuación ya se pueden obtener los cuatro valores posibles de x*, pues es una cuadrática en* x^2*. Así,*

$$x = \frac{\sqrt{18 \pm 6\sqrt{3}}}{6}, x = -\frac{\sqrt{18 \pm 6\sqrt{3}}}{6}$$

Sustituyendo cada valor en la segunda ecuación se obtienen rápidamente los valores correspondientes de y *(*y *en caso de desearse, también de* λ*). Se puede verificar que los dos puntos en los que la función alcanza el máximo son:*

$$\left(\pm\frac{\sqrt{18 + 6\sqrt{3}}}{6}, \pm\frac{\sqrt{18 + 6\sqrt{3}}}{12}(\sqrt{3} - 1) \right)$$

Aunque los sistemas bien podrían resolverse mediante 'trucos' o manipulaciones ingeniosas, vemos cómo las bases de Gröbner dan una forma concreta de cómo reducir variables a partir de las ecuaciones. De hecho, en este sentido, el Algoritmo de Buchberger es una generalización del Algoritmo de Eliminación Gaussiana.

3.5. Problema de la Intersección de Ideales

Es inmediato ver que intersección de ideales es ideal, y parecería que no es difícil resolver el siguiente

Problema 5 *Sean* $I = \langle f_1, f_2, ..., f_r \rangle$ *y* $J = \langle g_1, g_2, ..., g_x \rangle$ *ideales de* $k[x_1, x_2, ..., x_n]$, *encontrar generadores para el ideal* $I \cap J \subseteq k[x_1, x_2, ..., x_n]$

De hecho, encontrar generadores para las otras dos operaciones entre ideales que hemos definido (a saber, suma y producto) es fácil. En efecto, bajo los mismos generadores de I y J se tiene

$$\begin{aligned} I + J &= \langle f_1, f_2, ..., f_r, f_1, f_2, ..., f_r \rangle \\ IJ &= \langle f_i g_j | 1 \leq i \leq r, 1 \leq j \leq s \rangle \end{aligned}$$

Sin embargo, para el ideal intersección como veremos a continuación, el problema puede complicarse bastante. Primero introducimos una notación: si I ideal de $k[x_1, x_2, ..., x_n]$ y p es un polinomio en otra variable t, entonces

$$p(t)I := \langle \{ p(t)h(\overline{x}) | h \in I \} \rangle \subseteq k[x_1, x_2, ..., x_n, t]$$

Observación 19 *De la definición del ideal* $p(t)I$ *se tiene que si* $I = \langle f_1, f_2, ..., f_r \rangle$ *en* $k[x_1, x_2, ..., x_n]$, *entonces* $p(t)I = \langle p(t)f_1, p(t)f_2, ..., p(t)f_r \rangle$ *en* $k[x_1, x_2, ..., x_n, t]$.

El siguiente teorema nos caracteriza la intersección $I \cap J$ con los ideales anteriores:

Teorema 12 *"Sean* $I, J \subseteq k[x_1, x_2, ..., x_n]$ *ideales, entonces*

$$I \cap J = (tI + (1-t)J) \cap k[x_1, x_2, ..., x_n]"$$

Demostración. $\subseteq$) Sea $f \in I \cap J \subseteq k[x_1, x_2, ..., x_n]$, entonces podemos escribir

$$f = tf + (1-t)f \in tI + (1-t)J$$

por lo que $f(tI + (1-t)J) \cap k[x_1, x_2, ..., x_n]$.
$\supseteq$) Sea $f \in (tI + (1-t)J) \cap k[x_1, x_2, ..., x_n]$, entonces existen polinomios $g \in I$ y $h \in J$ tal que

$$f = tg + (1-t)h$$

Puesto que $f \in k[x_1, x_2, ..., x_n]$ (no contiene a la variable t), entonces haciendo $t = 0$ en la igualdad obtenemos que

$$f = 0 + 1h \in J$$

mientras que por otro lado, haciendo $t = 1$:

$$f = 1g + 0 \in I$$

por lo que $f \in I \cap J$. ■

Recordando nuestra teoría de eliminación, tenemos la siguiente

Solución 5 *Consideramos el ideal*

$$tI + (1-t)J = \langle tf_1, tf_2, ..., tf_r, (1-t)g_1, (1-t)g_2, ..., (1-t)g_x \rangle$$

y calculamos una base de Gröbner G bajo un orden de eliminación para t ($t > x_i$, $1 \leq i \leq n$) en $k[x_1, x_2, ..., x_n, t]$. Entonces $G \cap k[x_1, x_2, ..., x_n]$ es una base de Gröbner de $I \cap J$.

Esta solución se justifica pues estamos considerando el ideal de eliminación

$$I_{x_n} = (tI + (1-t)J) \cap k[x_1, x_2, ..., x_n]$$

que por el Teorema anterior sabemos es $I \cap J$. Así, el Teorema de Eliminación nos asegura que $G \cap k[x_1, x_2, ..., x_n]$ es la base de Gröbner de ese ideal de eliminación I_{x_n}. En conclusión, basta calcular la base de Gröbner de $tI + (1-t)J \subseteq k[x_1, x_2, ..., x_n, t]$ y luego considerar sólo los polinomios que no contienen la variable t. Estos últimos generarán a $I \cap J$ (y es más, conformarán una base de Gröbner de tal ideal).

Ejemplo 35 *Sean $I = \langle x^2y \rangle$ y $J = \langle xy^2 \rangle$. Comprobemos mediante el método anterior que se tiene $I \cap J = \langle x^2y^2 \rangle$. En este caso*

$$tI + (1-t)J = \left\langle tx^2y, (1-t)xy^2 \right\rangle$$

Dado que estos ideales son sencillos, hagamos por esta vez las cuentas sin ayuda de la computadora. Al calcular el S-polinomio (orden $lex(t > x > y)$):

$$\begin{aligned} S(tx^2y, txy^2 - xy^2) &= \frac{tx^2y^2}{tx^2y} tx^2y - \frac{tx^2y^2}{txy^2} \left(txy^2 - xy^2\right) \\ &= tx^2y^2 - tx^2y^2 + x^2y^2 = x^2y^2 \end{aligned}$$

Además,

$$S(tx^2y, x^2y^2) = \frac{tx^2y^2}{tx^2y}tx^2y - \frac{tx^2y^2}{txy^2}x^2y^2 = tx^2y^2 - x^3y^2$$

$$S(txy^2 - xy^2, x^2y^2) = \frac{tx^2y^2}{txy^2}\left(txy^2 - xy^2\right) - \frac{tx^2y^2}{x^2y^2}x^2y^2 = -x^2y^2$$

como x^2y^2 *divide a ambos tenemos* $\overline{S(tx^2y, x^2y^2)}^{x^2y^2} = \overline{S(txy^2 - xy^2, x^2y^2)}^{x^2y^2} = 0$, *y por tanto*

$$G = \{tx^2y, txy^2 - xy^2, x^2y^2\}$$

es base de Gröbner de $tI + (1-t)J$. *Según la teoría,*

$$I \cap J = \langle G \cap k[x,y] \rangle = \left\langle x^2y^2 \right\rangle$$

como buscábamos.

A continuación vemos un ejemplo en el que realmente se aprecia la utilidad de acudir a bases de Gröbner:

Ejemplo 36 *Sean* $I = \langle xz - y^2, x^3 - yz \rangle$ *y* $J = \langle x, z^2 \rangle$ *ideales en* $k[x,y,z]$. *La base de Gröbner correspondiente al ideal*

$$tI + (1-t)J = \left\langle txz - ty^2, tx^3 - tyz, x - tx, z^2 - tz^2 \right\rangle$$

en $k[x,y,z,t]$ *con orden* $lex(t > x > y > z)$ *es*

$$\begin{aligned} G \;=\; & \{tx - x, ty^2 - xz, tyz - x^3, tz^2 - z^2, x^4 - xyz, x^3y - xz^2, \\ & x^2y^2 - yz^2, x^2z - xy^2, xy^4 - yz^3, xz^3 - y^2z^2, y^6z^2 - yz^6\} \end{aligned}$$

por lo que concluimos que

$$I \cap J = \left\langle x^4 - xyz, x^3y - xz^2, x^2y^2 - yz^2, x^2z - xy^2, xy^4 - yz^3, xz^3 - y^2z^2, y^6z^2 - yz^6 \right\rangle$$

Vale la pena mencionar que, aunque no lo parezca, la hipótesis de estar trabajando en $k[x_1, x_2, ..., x_n]$ anillo Noetheriano es fundamental. En efecto, uno podría pensar que es bastante intuitivo que el ideal intersección de dos ideales finitamente generados es finitamente generado otra vez. Sorprendentemente, ¡esto es falso en general!

Ejemplo 37 *Sea R un anillo (conmutativo con 1) y $B = R[x_1, x_2, ..., x_n, x_{n+1}, ...]$ el anillo de polinomios con cantidad de variables numerable*[1]*. Sea*

$$I = \langle \{(x_1 - x_2)x_i | i \geq 3\} \rangle \subseteq R[x_n]_{n=1}^{\infty}$$

y consideramos el anillo cociente B/I. Sean $I_1 = \langle \overline{x_1} \rangle$ y $I_2 = \langle \overline{x_2} \rangle$ en B/I. Notar que no sólo I_1 y I_2 son finitamente generados, sino principales. Aún así, afirmamos que $I_1 \cap I_2 \subseteq B/I$ es un ideal no *finitamente generado.*
Supongamos que $I_1 \cap I_2 = \langle \overline{p_1}, \overline{p_2}, ..., \overline{p_m} \rangle$ para alguna $m \in \mathbb{N}$. Primero notemos que dado que $x_1x_k - x_2x_k = (x_1 - x_2)x_k \in I \ \forall k \geq 3$, entonces tenemos que $\overline{x_1x_k} = \overline{x_2x_k}$ y además $\overline{x_1x_k} = \overline{x_2x_k} \in \langle \overline{x_1} \rangle \cap \langle \overline{x_2} \rangle = I_1 \cap I_2 \ \ \forall k \geq 3$. Así, $\overline{x_1x_k} \in \langle \overline{p_1}, \overline{p_2}, ..., \overline{p_m} \rangle$ y luego existen $q_i^k \in B \ 1 \leq i \leq m$ tal que

$$x_1x_k - \sum_{i=1}^{m} q_i^k p_i \in I = \langle \{(x_1 - x_2)x_i | i \geq 3\} \rangle \quad \forall k \geq 3$$

Veremos que esto es imposible. Antes observemos que como cada $\overline{p_i} \in I_1 \cap I_2$ se tiene que existen $h_i, h_i', g_{ij}, g_{ij}' \in B$ tales que

$$\begin{aligned} p_i &= x_1 h_i + \sum_{j=3}^{\infty} (x_1 - x_2)x_j g_{ij} \\ &= x_2 h_i' + \sum_{j=3}^{\infty} (x_1 - x_2)x_j g_{ij}' \end{aligned}$$

donde $g_{ij} = g_{ij}' = 0$ para toda j suficientemente grande. Si $x_3 = x_4 = ... = 0$, tenemos

$$\begin{aligned} p_i &= x_1 h_i(x_1, x_2, 0, 0, ...) + 0 \\ &= x_2 h_i'(x_1, x_2, 0, 0, ...) + 0 \end{aligned}$$

por lo que haciendo alternativamente $x_2 = 0$ y luego $x_1 = 0$ tenemos:

$$\begin{aligned} x_1 h_i(x_1, 0, 0, 0, ...) &= 0 \\ x_2 h_i'(0, x_2, 0, 0, ...) &= 0. \end{aligned}$$

Así, $h_i \in \langle x_2, x_3, ... \rangle$ y $h_i' \in \langle x_1, x_3, ... \rangle$. A partir de las expresiones de p_i concluimos entonces que en cada uno de ellos no aparecen potencias puras de ninguna x_n

[1] Notar que B no es Noetheriano porque existe la cadena infinita ascendente de ideales $\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \langle x_1, x_2, x_3 \rangle \subseteq ...$

$\forall n \in \mathbb{N}^+$, *y como* $p_i(0,0,...,0) = 0$, *no tienen términos constantes.*
Regresando a que $x_1x_k - \sum_{i=1}^{m} q_i^k p_i \in \langle\{(x_1 - x_2)x_i | i \geq 3\}\rangle$ *para cada* $k \geq 3$, *esto implica que, o bien aparece en la suma un término* x_2x_k *o bien se cancela con otro* x_1x_k. *Sin pérdida de generalidad para el siguiente argumento, supongamos aparece* x_2x_k. *Se tendrían las siguientes posibilidades:*
(1) x_2 *aparece en* q_i^k *y el* x_k *aparece en* p_i *para alguna* i, *¡pero esto es para cada* $k \geq 3$*! Como entre todas las* p_i $1 \leq i \leq m$ *sólo se tienen un número finito de términos, que aparezca* x_k *con* $k \geq 3$ *es imposible.*
(2) una constante aparece en q_i^k *y el término* x_2x_k *aparece en* p_i *para alguna* i, *¡pero de nuevo esto es para cada* $k \geq 3$*! Por el argumento de finitud del caso anterior, esto es imposible.*
(3) el x_k *aparece en* q_i^k *y* x_2 *aparece en* p_i *para alguna* i, *pero entonces* x_2 *aparece 'puro' en* p_i, *¡lo que habíamos visto es imposible!*
(4) x_2x_k *aparece en* q_i^k *y una constante en* p_i *para alguna* i, *¡pero habíamos observado que* p_i *no puede tener términos constantes!*
Así, en cualquier caso, tenemos una contradicción y $I_1 \cap I_2$ *no puede ser finitamente generado.*

3.6. Problema del Ideal Cociente

En esta sección definimos el ideal cociente de dos ideales así como la saturación de un ideal para luego plantear el problema de encontrar generadores para cada uno y resolverlo una vez más con la teoría de Bases de Gröbner.

Definición 33 *Sean* $I, J \subseteq R$ *ideales de un anillo, se define el* ideal cociente *de* I *y* J *como*

$$I : J = \{f \in R | fg \in I \ \forall g \in J\}$$

Observación 20 $I : J$ *sí es un ideal, el cual contiene a* I. *(*$I \subseteq I : J$ *pues si* $f \in I$, *por ser* I *ideal,* $fg \in I \ \forall g \in J$. *Así,* $0 \in I \subseteq I : J$. *Si* $f_1, f_2 \in I : J$ *y* $h \in R$ *entonces* $(f_1 + hf_2)g = f_1g + hf_2g \in I \ \forall g \in J$ *pues* $f_1g \in I$, $f_2g \in I$ *al estar en* $I : J$*)*

Observación 21 *Notar que de la definición de* $I : J$ *se cumple que:*
(1) $R : I = R$ *(*$R \subseteq R : I$ *por la observación anterior)*
(2) $I : R = I$ *(si* $f \in I : R$, *en particular para* $1 \in R$ *se tiene* $f \cdot 1 \in I$*)*
(3) $IJ \subseteq K \iff I \subseteq K : J$
(4) $J \subseteq I \iff I : J = R$

A continuación vemos algunas propiedades del cociente:

Proposición 16 *"Sean $I, J, K \subseteq R$ ideales, entonces:*
(1) $(I : J) : K = I : JK$
(2) $I : (J + K) = (I : J) \cap (I : K)$
(3) $(I \cap J) : K = (I : K) \cap (J : K)$"

Demostración. (1) $\subseteq$) Sea $f \in (I : J) : K$ y $gh \in JK$ $(g \in J, h \in K)$, entonces por hipótesis $fh \in I : J$, que a su vez implica $fhg \in I$, es decir, $f(gh) \in I$ y por tanto $f \in I : JK$
$\supseteq$) Sea $f \in I : JK$, para ver que $f \in (I : J) : K$ sea $h \in K$, y veamos que $fh \in I : J$, pero esto sucede pues si $g \in J$ entonces por hipótesis $f(gh) \in I$, es decir, $fhg \in I$.
(2) $\subseteq$) Como $J \subseteq J + K$ y $K \subseteq J + K$ entonces $I : (J + K) \subseteq I : J$ y también $I : (J + K) \subseteq I : K$ y por tanto $I : (J + K) \subseteq (I : J) \cap (I : K)$.
$\supseteq$) Sea $f \in (I : J) \cap (I : K)$, y $g + h \in J + K$, entonces $f(g + h) = fg + fh \in I$ pues por hipótesis fg y fh lo están.
(3) $\subseteq$) Como $I \cap J \subseteq I$ y $I \cap J \subseteq J$ entonces $(I \cap J) : K \subseteq I : K$ y $(I \cap J) : K \subseteq J : K$ y por tanto $(I \cap J) : K \subseteq (I : K) \cap (J : K)$.
$\supseteq$) Sea $f \in (I : K) \cap (J : K)$, si $h \in K$ entonces por hipótesis $fh \in I$ y $fh \in J$ por lo que $fh \in I \cap J$ y así $f \in (I \cap J) : K$. ■

Cuando J es principal, es decir, $J = \langle f \rangle$, denotamos $I : J$ por $I : f$. Notar que de (2) de la Proposición anterior, se tiene que si $J = \langle g_1, g_2, ..., g_s \rangle$, como $\langle g_1, g_2, ..., g_s \rangle = \langle g_1 \rangle + \langle g_2 \rangle + ... + \langle g_s \rangle$ entonces

$$I : J = I : (\langle g_1 \rangle + \langle g_2 \rangle + ... + \langle g_s \rangle) = \bigcap_{i=1}^{s} I : g_i$$

Dentro de la correspondencia entre ideales y variedades, ¿a qué corresponde el ideal cociente $I : J$? Este es el contenido del siguiente

Teorema 13 *"Sean $I, J \subseteq k[x_1, x_2, ..., x_n]$, entonces*
(1) $\mathcal{V}(I : J) \supseteq \overline{\mathcal{V}(I) - \mathcal{V}(J)}^{Z}$
(2) $\mathcal{I}(V) : \mathcal{I}(W) = \mathcal{I}(V - W)$
(2) Si k es algebraicamente cerrado e I es radical, entonces $\mathcal{V}(I : J) = \overline{\mathcal{V}(I) - \mathcal{V}(J)}^{Z}$"

Queremos resolver entonces el siguiente:

Problema 6 *Sean* $I = \langle f_1, f_2, ..., f_r \rangle$ *y* $J = \langle g_1, g_2, ..., g_x \rangle$ *ideales de* $k[x_1, x_2, ..., x_n]$, *encontrar generadores para el ideal* $I : J \subseteq k[x_1, x_2, ..., x_n]$

Dado que ya observamos que

$$I : J = \bigcap_{i=1}^{s} I : g_i$$

el problema se reduce al caso en que J es principal, y luego se aplica el método anterior de intersección de ideales (dos a dos inductivamente hasta llegar a s intersectandos).
Encontramos generadores para $I : g$ a partir de generadores de $I \cap \langle g \rangle$ con la siguiente

Proposición 17 *"Sean* I *ideal y* g *en* $k[x_1, x_2, ..., x_n]$, *si* $I \cap \langle g \rangle = \langle h_1, h_2, ..., h_r \rangle$ *entonces* $I : g = \left\langle \frac{h_1}{g}, \frac{h_2}{g}, ..., \frac{h_r}{g} \right\rangle$*"*

Demostración. Primeramente notar que h_i/g sí es un polinomio dado que cada $h_i \in \langle g \rangle$. Ahora, verifiquemos que cada $h_i/g \in I : g$. En efecto, si $hg \in \langle g \rangle$ (con $h \in k[x_1, x_2, ..., x_n]$) entonces

$$\frac{h_i}{g} \cdot hg = h_i h \in I$$

pues cada $h_i \in I$. Así, ya se tiene que $\left\langle \frac{h_1}{g}, \frac{h_2}{g}, ..., \frac{h_r}{g} \right\rangle \subseteq I : g$. Basta ver la otra contención: sea $f \in I : g$, entonces $fg \in I$, pero de hecho $fg \in I \cap \langle g \rangle$, que implica $fg \in \langle h_1, h_2, ..., h_r \rangle$ y por tanto $f \in \left\langle \frac{h_1}{g}, \frac{h_2}{g}, ..., \frac{h_r}{g} \right\rangle$. ■

Así, logramos la siguiente

Solución 6 *Para cada* g_i *de* $J = \langle g_1, g_2, ..., g_x \rangle$, *calcular generadores para la intersección* $I \cap g_i$, *luego dividir cada uno por* g_i *para obtener generadores de* $I : g_i$. *Finalmente, encontrar generadores para la intersección*

$$\bigcap_{i=1}^{s} I : g_i = I : J$$

Ejemplo 38 *Calcular* $I : J$ *si* $I = \langle xz - y^2, x^3 - yz\rangle$ *y* $J = \langle x, z\rangle$ *. Procedemos según la solución, primero consideramos*

$$tI + (1-t)x = \left\langle txz - ty^2, tx^3 - tyz, (1-t)x\right\rangle$$

y eliminamos t *con* $lex(t > x > y > z)$ *en la base de Gröbner para obtener*

$$I \cap \langle x\rangle = \left\langle x^4 - xyz, x^3y - xz^2, x^2y^3 - xz^3, x^2z - xy^2, xy^5 - xz^4\right\rangle$$

por lo que

$$I : x = \left\langle x^3 - yz, x^2y - z^2, xy^3 - z^3, xz - y^2, y^5 - z^4\right\rangle$$

Ahora consideramos el ideal

$$tI + (1-t)y = \left\langle txz - ty^2, tx^3 - tyz, (1-t)y\right\rangle$$

y eliminamos t *con* $lex(t > x > y > z)$ *en la base de Gröbner para obtener*

$$I \cap \langle y\rangle = \left\langle x^3y - y^2z, x^2y^2 - yz^2, xy^4 - yz^3, xyz - y^3, y^6 - yz^4\right\rangle$$

por lo que

$$I : y = \left\langle x^3 - yz, x^2y - z^2, xy^3 - z^3, xz - y^2, y^5 - z^4\right\rangle$$

Como $I : x = I : y$*, tenemos que*

$$I : J = (I : x) \cap (I : y) = \left\langle x^3 - yz, x^2y - z^2, xy^3 - z^3, xz - y^2, y^5 - z^4\right\rangle$$

3.7. Problema de la Saturación y Membresía a Radical

Definición 34 *Sean* I *ideal y* f *en* $k[x_1, x_2, ..., x_n]$*, se define la* saturación *de* I *respecto a* f *como el ideal*

$$I : f^\infty = \{g \in k[x_1, x_2, ..., x_n] | f^m g \in I \ p.a.\ m > 0\}$$

es decir,en notación de ideal cociente,

$$I : f^\infty = \bigcup_{m=1}^{\infty} I : f^m$$

El primer problema que nos planteamos entonces es:

Problema 7 *Sean $I = \langle f_1, f_2, ..., f_r \rangle$ ideal y f en $k[x_1, x_2, ..., x_n]$, calcular generadores para la saturación $I : f^\infty$*

Notar que si $f^m g \in I$ p.a. $m > 0$, entonces para cualquier potencia N mayor a m, $f^N g \in I$ también. Es decir,

$$I : f \subseteq I : f^2 \subseteq ... \subseteq I : f^m \subseteq I : f^{m+1} \subseteq ...$$

usando una vez más que $k[x_1, x_2, ..., x_n]$ es Noetheriano, concluimos que de hecho debe existir una $N \in \mathbb{N}$ suficientemente grande tal que

$$I : f \subseteq I : f^2 \subseteq ... \subseteq I : f^N = I : f^{N+1} = ...$$

y así

$$I : f^\infty = \bigcup_{m=1}^{N} I : f^m = I : f^N$$

Así que una forma de resolver el problema sería ir calculando para cada $m \in \mathbb{N}$ el ideal cociente $I : f^m$ (mediante el método de la sección anterior), y en el momento que $I : f^N = I : f^{N+1}$ entonces detenemos el proceso y declaramos a este último como la saturación $I : f^\infty$. Podemos darnos cuenta que este algoritmo no es muy eficiente. Afortunadamente, tenemos otra forma, que utiliza el mismo truco ingenioso[2] de la prueba del Nullstellensatz Fuerte:

Teorema 14 *"Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal y $f \in k[x_1, x_2, ..., x_n]$, y consideremos el ideal*

$$\widetilde{I} = \langle I \cup \{1 - yf\} \rangle \subseteq k[x_1, x_2, ..., x_n, y]$$

entonces $I : f^\infty = \widetilde{I} \cap k[x_1, x_2, ..., x_n]$""

Demostración. Sea $I = \langle f_1, f_2, ..., f_r \rangle$ y luego

$$\widetilde{I} = \langle f_1, f_2, ..., f_r, 1 - yf \rangle$$

$\subseteq$) Sea $g \in I : f^\infty$, entonces existe $m \geq 1$ tal que $f^m g \in I$. Así,

$$\begin{aligned} g &= g f^m y^m + (1 - f^m y^m) g \\ &= (f^m g) y^m + (1 - yf)(1 + yf + ... + y^{m-1} f^{m-1}) g \end{aligned}$$

[2] A veces se le da el nombre de "truco de Rabinowitz".

por lo que $g \in \langle I \cup \{1 - yf\}\rangle = \widetilde{I}$. Como $g \in I : f^\infty \subseteq k[x_1, x_2, ..., x_n]$ también, se concluye $g \in \widetilde{I} \cap k[x_1, x_2, ..., x_n]$.
$\supseteq$) Sea $g \in \widetilde{I} \cap k[x_1, x_2, ..., x_n]$, entonces existen $p_1, p_2, ..., p_s, h \in k[x_1, x_2, ..., x_n, y]$ tal que

$$g = p_1 f_1 + p_2 f_2 + ... + p_r f_r + h(1 - yf)$$

entonces sustituyendo $y = 1/f$ tenemos

$$g = p_1(x_1, x_2, ..., 1/f) f_1 + ... + p_s(x_1, x_2, ..., 1/f) f_s + 0$$

así que multiplicando por una potencia f^N suficientemente grande para que ya no haya denominadores, se tiene una combinación polinomial

$$f^N g = h_1 f_1 + ... + h_r f_s \in I$$

por lo que $g \in I : f^\infty$. ■

El teorema anterior nos indica que la saturación se puede ver como un ideal de eliminación, y gracias a las bases de Gröbner sabemos que podemos calcularlo:

Solución 7 *Considerar el ideal* $\widetilde{I} = \langle I \cup \{1 - yf\}\rangle \subseteq k[x_1, x_2, ..., x_n, y]$ *con orden* $lex(y > x_1 > ... > x_n)$, *calculamos una base de Gröbner* G *de* $\widetilde{I}$, *entonces* $G \cap k[x_1, x_2, ..., x_n]$ *genera a* $I : f^\infty$

Naturalmente, la solución se justifica en el Teorema de Eliminación con $G \cap k[x_1, x_2, ..., x_n]$ la base de Gröbner del ideal de eliminación

$$\widetilde{I}_{x_n} = \widetilde{I} \cap k[x_1, x_2, ..., x_n] = I : f^\infty.$$

El trabajo invertido en este problema de hecho nos resuelve otro problema importante: el de la Membresía a Radical.

Problema 8 *Sea* I *ideal en* $k[x_1, x_2, ..., x_n]$ *y* $f \in k[x_1, x_2, ..., x_n]$. *Determinar si* $f \in rad(I)$ *o* $f \notin rad(I)$.

Un poco ingenuamente, uno podría tratar de resolver el problema mediante la solución del Problema de Membresía a Ideal. Puesto que

$$rad(I) = \sqrt{I} = \{f \in k[x_1, x_2, ..., x_n] | f^m \in I \text{ p.a. } m \in I\}$$

entonces podemos ir resolviendo: ¿$f \in I$? ¿$f^2 \in I$? ¿$f^3 \in I$?... hasta obtener una respuesta afirmativa. El problema evidente con este método propuesto es que si $f \notin rad(I)$, entonces el algoritmo nunca termina. Una mucho mejor forma de resolver el problema es mediante la siguiente sencilla

Proposición 18 *"Sean $I = \langle f_1, f_2, ..., f_r\rangle$ ideal y f en $k[x_1, x_2, ..., x_n]$, entonces $f \in \sqrt{I}$ si y sólo si $I : f^\infty = k[x_1, x_2, ..., x_n]$"*

Demostración. $\Rightarrow$) Sea $f \in \sqrt{I}$, entonces existe $m \in \mathbb{N}$ tal que $f^m \in I$, es decir, $f^m 1 \in I$ y por tanto $1 \in I : f^\infty$, lo que obliga a que $I : f^\infty = k[x_1, x_2, ..., x_n]$.
$\Leftarrow$) Sup. que $I : f^\infty = k[x_1, x_2, ..., x_n]$, entonces en particular $1 \in I : f^\infty$, lo que implica que existe $m \in \mathbb{N}$ tal que $f^m 1 \in I$, es decir, $f^m \in I$ y así $f \in \sqrt{I}$. ■

Dado que $1 \in \widetilde{I} \Leftrightarrow 1 \in \widetilde{I} \cap k[x_1, x_2, ..., x_n]$, tenemos la siguiente

Solución 8 *Considerar el ideal $\widetilde{I} = \langle I \cup \{1 - yf\}\rangle \subseteq k[x_1, x_2, ..., x_n, y]$ y calcular una base de Gröbner reducida G de $\widetilde{I}$ (bajo cualquier orden monomial), luego $f \in rad(I)$ si y sólo si $G = \{1\}$.*

Ejemplo 39 *Sea $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1\rangle \subseteq \mathbb{Q}[x, y]$ y $f = y - x^2 + 1$. Determinamos si $f \in \sqrt{I}$ o no. Consideramos el ideal*

$$\widetilde{I} = \left\langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - t(y - x^2 + 1)\right\rangle \subseteq \mathbb{Q}[x, y, t]$$

que tiene base de Gröbner bajo $lex(t > x > y > z)$:

$$G = \{1\}$$

por lo que $f \in \sqrt{I}$. Si se quisiera saber a qué potencia $m \in \mathbb{N}$ se tiene que $f^m \in I$ entonces se pueden ir encontrando los residuos respecto a una base de Gröbner de I, hasta encontrar el primero que da 0. En este caso,

$$\begin{aligned} G_I &= \{y^2, x^4 - x^2 + 1\} \\ \overline{f}^{G_I} &= f = y - x^2 + 1 \\ \overline{f^2}^{G_I} &= -2x^2y + 2y \\ \overline{f^3}^{G_I} &= 0 \end{aligned}$$

por lo que la mínima potencia es $m = 3$.

De hecho, así tenemos un resuelto un problema más, el Problema de Igualdad de Radicales:

Problema 9 *Sean $I = \langle f_1, f_2, ..., f_r\rangle$ y $J = \langle g_1, g_2, ..., g_x\rangle$ ideales de $k[x_1, x_2, ..., x_n]$, determinar si $rad(I) = rad(J)$ o $rad(I) \neq rad(J)$*

Solución 9 *Mediante el algoritmo de membresía a radical, determinar si cada $f_i \in rad(J)$ $1 \leq i \leq n$ ($I \subseteq \sqrt{J}$, que implica $\sqrt{I} \subseteq \sqrt{J}$) y viceversa, si cada $g_j \in rad(I)$ ($J \subseteq \sqrt{I}$, que implica $\sqrt{J} \subseteq \sqrt{I}$). Se tiene que $rad(I) = rad(J)$ si y sólo si $f_i \in rad(J)$ $1 \leq i \leq n$ y $g_j \in rad(J)$ $1 \leq j \leq s$.*

Capítulo 4

Más Aplicaciones de Bases de Gröbner

Asumiendo familiaridad con otros conceptos algebraicos, damos más aplicaciones de estas útiles bases de Gröbner:

4.1. Teorema de Macaulay

El uso original de las bases de Gröbner (la razón por la que Buchberger las introdujo) fue para poder hacer cálculos en anillos cociente. Dado I ideal de $k[x_1, x_2, ..., x_n]$ y el anillo cociente

$$\frac{k[x_1, x_2, ..., x_n]}{I}$$

si tenemos un elemento del cociente (es decir, una clase de equivalencia), lo que Buchberger buscaba era un representante estándar para ella.

Problema 10 *Sea I ideal de $k[x_1, x_2, ..., x_n]$, encontrar representantes para cada clase de $\frac{k[x_1,x_2,...,x_n]}{I}$ y determinar las operaciones del anillo en términos de éstos.*

Las bases de Gröbner nos permiten justo eso, consecuencia del Teorema 8:

Proposición 19 *"Sea $<$ un orden monomial e I ideal en $k[x_1, x_2, ..., x_n]$, entonces cada $f \in k[x_1, x_2, ..., x_n]$ es congruente módulo I (es decir, está relacionada bajo $\sim$) con un único polinomio r tal que es combinación lineal de monomios en el complemento de $\langle TL(I) \rangle$"*

Demostración. Sea G base de Gröbner de I, entonces sabemos que el residuo $r = \overline{f}^G$ es único por el Teorema 8, cumpliendo que existe un único $g \in I$ con $f = g + r$ (por lo que $f - r \in I$ y así $f \sim r$) y también que r cumple que cada término de r no pertenece a $\langle TL(G)\rangle = \langle TL(I)\rangle$. ■

De hecho, de la unicidad del residuo se tiene la siguiente

Proposición 20 *"Sean $f, g \in k[x_1, x_2, ..., x_n]$, $a \in k$ y G base de Gröbner de I ideal, entonces*
(i) $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$
(II) $\overline{af}^G = a\overline{f}^G$ "

Demostración. El resultado se sigue de observar que si $f = p + r_1$ y $g = q + r_2$ con $p, q \in I$ y r_1, r_2 los respectivos residuos, entonces

$$\begin{aligned} f + g &= (p + q) + (r_1 + r_2) \\ af &= ap + ar_1 \end{aligned}$$

entonces como $p + q, ap \in I$ y $r_1 + r_2, ar_1 \notin \langle TL(I)\rangle$, apelamos a la unicidad de los residuos para concluir que justo $r_1 + r_2$ y ar_1 son tales. ■

¿Cuál es entonces la relación entre el anillo cociente y una base de Gröbner de I? Según las líneas anteriores, la clave esta en $\langle TL(I)\rangle$, o mejor dicho, en su complemento. Esto es lo que conecta el Teorema de Macaulay:

Teorema 15 *(DE MACAULAY) "Sea $<$ orden monomial en $k[x_1, x_2, ..., x_n]$ e I ideal, entonces*

$$\frac{k[x_1, x_2, ..., x_n]}{I} \cong \langle \{x^\alpha | x^\alpha \notin \langle TL(I)\rangle\}\rangle$$

como k-espacios vectoriales"

Demostración. Consideremos la proyección natural

$$\pi : \{x^\alpha | x^\alpha \notin \langle TL(I)\rangle\} \longrightarrow \frac{k[x_1, x_2, ..., x_n]}{I}$$

dada por $\pi(x^\alpha) = \overline{x^\alpha}$. Notamos que esta función es inyectiva, ya que si $\overline{x^\alpha} = \overline{x^\beta}$ se tendría $x^\alpha - x^\beta \in I$, pero ni x^α ni x^β están en $TL(I)$ por lo que no puede existir

$TL(x^\alpha - x^\beta)$, es decir, $x^\alpha - x^\beta$ está forzado a ser 0, de donde $x^\alpha = x^\beta$. Así, se tiene la biyección

$$\pi : \{x^\alpha | x^\alpha \notin \langle TL(I)\rangle\} \longleftrightarrow \{\overline{x^\alpha} | x^\alpha \notin \langle TL(I)\rangle\}$$

En particular, ambos conjuntos tienen la misma cardinalidad. Observar que como cada monomio no se puede obtener como combinación lineal de monomios diferentes, $\{x^\alpha | x^\alpha \notin \langle TL(I)\rangle\}$ es un conjunto linealmente independiente. Si probáramos que $\{\overline{x^\alpha} | x^\alpha \notin \langle TL(I)\rangle\}$ también es linealmente independiente (pero mod I), los espacios vectoriales generados por ambos conjuntos serían isomorfos. De esta manera, basta probar que $\{\overline{x^\alpha} | x^\alpha \notin \langle TL(I)\rangle\}$ es base de $\frac{k[x_1,x_2,...,x_n]}{I}$:
(i) Veamos que $\{\overline{x^\alpha} | x^\alpha \notin \langle TL(I)\rangle\}$ es un conjunto linealmente independiente, entonces sean $a_1, a_2, ..., a_m \in k$ y $\alpha_1, \alpha_2, ..., \alpha_m \in \mathbb{N}^n$ tal que

$$a_1\overline{x^{\alpha_1}} + a_2\overline{x^{\alpha_2}} + ...a_m\overline{x^{\alpha_m}} = \overline{0}$$

es decir,$\overline{a_1x^{\alpha_1} + a_2x^{\alpha_2} + ...a_mx^{\alpha_m}} = \overline{0}$, por lo que

$$f = a_1x^{\alpha_1} + a_2x^{\alpha_2} + ...a_mx^{\alpha_m} \in I$$

con cada $x^{\alpha_i} \notin \langle TL(I)\rangle$, $1 \leq i \leq m$. Si suponemos que no todos los a_i son 0, f no es el polinomio 0, pero entonces como $f \in I$ tenemos que $TL(f) \in TL(I)$,lo que es imposible pues cada término de f pertenece al complemento de $\langle TL(I)\rangle$. Por lo tanto $a_1 = a_2 = ... = a_m = 0$.
(ii) El hecho de que $\{\overline{x^\alpha} | x^\alpha \notin \langle TL(I)\rangle\}$ genera al anillo cociente es consecuencia de lo ya probado en la Proposición 19. Según esta proposición, dada $\overline{f}$ clase en el anillo cociente, existe un representante que es combinación lineal de monomios en el complemento de $\langle TL(I)\rangle$, es decir, existen $a_1, a_2, ..., a_m \in k$ y $\alpha_1, \alpha_2, ..., \alpha_m \in \mathbb{N}^n$ tal que

$$r = a_1x^{\alpha_1} + a_2x^{\alpha_2} + ...a_mx^{\alpha_m}$$

con $x^{\alpha_i} \notin \langle TL(I)\rangle$, por lo que

$$\overline{f} = \overline{r} = a_1\overline{x^{\alpha_1}} + a_2\overline{x^{\alpha_2}} + ...a_m\overline{x^{\alpha_m}}$$

■

Notar que en la demostración no interviene de forma directa o explícita el concepto de base de Gröbner, pero es justo esto lo que no permite hablar concretamente de quiénes son esos representantes o cómo calcularlos. Al introducir una base de Gröbner G de I, entonces, como ya probablemente se haya intuido según los resultados anteriores, se puede dar el isomorfismo concreto $\phi : \frac{k[x_1,x_2,...,x_n]}{I} \longrightarrow \langle\{x^\alpha | x^\alpha \notin \langle TL(I)\rangle\}\rangle$ dado por

$$\phi(\overline{f}) = \overline{f}^G.$$

La función está bien definida por la Proposición 19 y porque $\overline{f} = \overline{g}$ implica $f - g \in I$ y entonces $0 = \overline{f-g}^G = \overline{f}^G - \overline{g}^G$ según la Proposición 20, es decir, $\overline{f}^G = \overline{g}^G$. De hecho, la misma proposición 20 nos asegura que ϕ es lineal. Como $f \in \ker\phi$ implica que $\overline{f}^G = 0$ que a su vez implica $f \in I$, tenemos que $\overline{f} = \overline{0}$ y así ϕ es inyectiva. Finalmente, si $r \in \langle\{x^\alpha | x^\alpha \notin \langle TL(I)\rangle\}\rangle$ entonces $\overline{r} = r$ en el Algoritmo de la División Multivariado y ϕ también es suprayectiva. Por lo tanto, ϕ es en efecto un isomorfismo entre ambos espacios vectoriales.

De la forma anterior, ya se podrían hacer cálculos con sumas y productos por escalares en $\frac{k[x_1,x_2,\ldots,x_n]}{I}$ usando los representantes estándar que son los residuos bajo G. ¿Cómo se manejaría para el producto de dos clases? Como para $\overline{f}, \overline{g} \in \frac{k[x_1,x_2,\ldots,x_n]}{I}$ se tiene

$$\overline{f} \cdot \overline{g} = \overline{fg} = \overline{\overline{fg}^G}$$

tenemos que el representante que corresponde al producto de dos clases no es más que el residuo del producto de los representantes.

Solución 10 *Considerar una base de Gröbner para I, entonces las operaciones entre clases en el anillo cociente se pueden efectuar tomando como representantes estándar de cada clase $\overline{f}$ al residuo $\overline{f}^G$.*

Ejemplo 40 *Sea $I = \langle xy^3 - x^2, x^3y^2 - y\rangle \subseteq k[x,y]$ con orden $grlex(x > y)$. La base de Gröbner G correspondiente es*

$$G = \{x^3y^2 - y, x^4 - y^2, xy^3 - x^2, y^4 - xy\}$$

por lo que $\langle TL(I)\rangle = \langle TL(G)\rangle = \langle x^3y^2, x^4, xy^3, y^4\rangle$. Los monomios que están en el complemento de $\langle TL(I)\rangle$ son

$$\beta = \{1, x, x^2, x^3, y, xy, x^2y, x^3y, y^2, xy^2, x^2y^2, y^3\}$$

así que tomando clases tenemos ya una base para el anillo cociente y además

$$\dim_k\left(\frac{k[x,y]}{I}\right) = 12$$

Por curiosidad, podemos considerar otro orden, por ejemplo, $lex(x > y)$. La base de Gröbner es entonces

$$G' = \{x^2 - y^6, xy - y^4, y^{11} - y\}$$

por lo que $\langle TL(I)\rangle = \langle TL(G')\rangle = \langle x^2, xy, y^{11}\rangle$ *. Los monomios que están en el complemento de* $\langle TL(I)\rangle$ *son*

$$\beta' = \{1, x, y, y^2, y^3, y^4, y^5, y^6, y^7, y^8, y^9, y^{10}\}$$

teniendo una nueva base para el anillo cociente. Notar que, en efecto, la dimensión del espacio sigue siendo 12.
Como último experimento, calculamos la base de Gröbner de I *correspondiente a orden lexicográfico pero ahora* $lex(y > x)$*, entonces*

$$G'' = \{y - x^7, x^{12} - x^2\}$$

por lo que $\langle TL(I)\rangle = \langle TL(G'')\rangle = \langle y, x^{12}\rangle$ *. Los monomios que están en el complemento de* $\langle TL(I)\rangle$ *son*

$$\beta'' = \{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}\}$$

obteniendo una base más para el anillo cociente. Se comprueba una vez más lo que ya sabíamos a partir del Teorema de Macaulay: que la cardinalidad de los monomios que no pertenecen a $\langle TL(I)\rangle$ *(en este ejemplo igual a* 12*) sería invariante a cambios de orden monomial.*

4.2. Problema de Finitud de Soluciones

Nos enfocamos en el siguiente

Problema 11 *Sea* $I \subseteq k[x_1, x_2, ..., x_n]$ *ideal, determinar si la variedad* $V = \mathcal{V}(I)$ *es finita o infinita*

En otras palabras, determinar cuándo un sistema de ecuaciones polinomiales tiene una cantidad finita o infinta de soluciones. Al igual que en el problema de consistencia, para una solución completa se pedirá k algebraicamente cerrado. Por ahora, tenemos lo siguiente:

Proposición 21 *"Sea* $I \subseteq k[x_1, x_2, ..., x_n]$ *ideal, entonces son equivalentes:*
(a) $\frac{k[x_1,x_2,...,x_n]}{I}$ *es un* $k-$*espacio vectorial de dimensión finita*
(b) Para cualquier $<$ *orden monomial, el conjunto* $\{x^\alpha | x^\alpha \notin \langle TL(I)\rangle\}$ *es finito*
(c) Si $<$ *orden monomial, para cada* $1 \leq i \leq n$ *existe* $m_i \in \mathbb{N}$ *tal que* $x_i^{m_i} \in \langle TL(I)\rangle$
(d) Si $<$ *orden monomial,* G *base de Gröbner de* I*, entonces para cada* $1 \leq i \leq n$ *existen* $m_i \in \mathbb{N}$*,* $g \in G$ *tal que* $TL(g) = x_i^{m_i}$*"*

Demostración. (a)⇔(b): Son equivalentes por el Teorema de Macaulay.
(b)⇒(c): Sea $<$ orden monomial y $i \in \{1, ..., n\}$, como $\{x^\alpha | x^\alpha \notin \langle TL(I)\rangle\}$ es finito, en particular el subconjunto $\{x_i^j | x_i^j \notin \langle TL(I)\rangle\,,\ j \in \mathbb{N}\}$ es finito, por lo que existe $m_i \in \mathbb{N}$ (incluso mínimo) tal que $x_i^{m_i} \in \langle TL(I)\rangle\,.$
(c)⇒(d): Sea $<$ orden monomial, G base de Gröbner de I y $i \in \{1, ..., n\}$, como por hipótesis existe $m \in \mathbb{N}$ tal que $x_i^m \in \langle TL(I)\rangle = \langle TL(G)\rangle\,,$ entonces existe $g \in G$ tal que $TL(g)|x_i^m$, por lo que $TL(g) = x_i^{m_i}$ con $m_i \in \mathbb{N}$ tal que $m_i \leq m$.
(d)⇒(b): Como para cada $i \in \mathbb{N}$ existen $m_i \in \mathbb{N}$, $g \in G$ tal que $TL(g) = x_i^{m_i}$, luego $x_i^{m_i} \in \langle TL(I)\rangle$ para m_i con $1 \leq i \leq n$. Si $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n} \notin \langle TL(I)\rangle\,,$ entonces se debe tener que $0 \leq \alpha_i < m_i$ para $1 \leq i \leq n$, en particular sólo hay una cantidad finita de $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ que cumplen esto (acotada de hecho por $m_1 m_2 ... m_n$). ■

¿Y qué tiene que ver la proposición anterior con que $\mathcal{V}(I)$ sea finita?

Teorema 16 *"Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal, $V = \mathcal{V}(I)$ y considerar el enunciado:*
(e) V es finita
entonces cualquiera de los enunciados (a)-(d) de la Proposición anterior implica (e), y si además k es algebraicamente cerrado, (e) es equivalente a ellos."

Demostración. (a)⇒(e): Vamos a demostrar que para cada $(a_1, a_2, ..., a_n) \in V$, cada coordenada a_i con $1 \leq i \leq n$, sólo puede tomar una cantidad finita de valores, con lo que habremos terminado. Sea entonces $i \in \{1, 2, ..., n\}$ y consideramos el conjunto

$$\{(\overline{x_i})^j\,| j \in \mathbb{N}\} \subseteq \frac{k[x_1, x_2, ..., x_n]}{I}$$

como el espacio vectorial es de dimensión finita, tal conjunto debe ser linealmente dependiente, por lo que existen $c_0, c_1, c_2, ..., c_m \in k$ no todas cero tal que

$$c_0\overline{1} + c_1\overline{x_i} + c_2\overline{x_i}^2 + ... + c_m\,(\overline{x_i})^m = \overline{0}$$

es decir, $\overline{c_0 1 + c_1 x_i + c_2 x_i^2 + ... + c_m x_i^m} = \overline{0}$ por lo que

$$f_i = c_0 1 + c_1 x_i + c_2 x_i^2 + ... + c_m x_i^m \in I$$

Como f_i es un polinomio distinto de 0 en una variable (x_i), sólo puede tener a lo más m raíces, y así sólo hay una cantidad finita de soluciones para cada x_i. Concluimos que $\mathcal{V}(I) \subseteq k^n$ es un conjunto finito.
(e)⇒(c): Supongamos k algebraicamente cerrado. Si $V = \mathcal{V}(I) = \varnothing$ por el Nullstellensatz Débil se tiene que $I = k[x_1, x_2, ..., x_n]$ por lo que $1 \in I$ y así podemos

tomar $m_i = 0\ \forall i \in \{1, 2, ..., n\}$ para que $x_i^{m_i} \in \langle TL(I)\rangle = I$.
Si $V \neq \varnothing$, para cada $i \in \{1, 2, ..., n\}$ consideremos

$$\pi^i(V) = \{a_i \in k | (a_1, a_2, ., a_i, ., a_n) \in V\},$$

todas las coordenadas $i-$ésimas de los puntos de V (por hipótesis hay una cantidad finita $a_i^1, a_i^2, ..., a_i^k$ de éstos). Formamos entonces el polinomio en $k[x_1, x_2, ..., x_n]$

$$f_i(x_1, x_2, .., x_i, .., x_n) = \prod_{j=1}^{k}(x_i - a_i^j)$$

Notar que por construcción f_i se anula en cada punto $(a_1, a_2, ., a_i, ., a_n) \in V$, por lo que $f \in \mathcal{I}(V) = \mathcal{I}(\mathcal{V}(I))$ y como por el Nullstellensatz Fuerte se tiene $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ entonces existe $r_i \in \mathbb{N}$ tal que $f_i^{r_i} \in I$. Así,

$$TL(f_i^{r_i}) = (x_i^k)^{r_i} = x_i^{kr_i} \in TL(I)$$

Tomando $m_i = kr_i \in \mathbb{N}$ hemos terminado. ■

Examinando de nuevo la prueba de la implicación (a)⇒(e), tenemos una cota para el número de soluciones en $\mathcal{V}(I)$:

Corolario 6 *"Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal, entonces*

$$|\mathcal{V}(I)| \leq \dim_k \left(\frac{k[x_1, x_2, ..., x_n]}{I}\right) \text{"}$$

Así, cuando k algebraicamente cerrado tenemos la siguiente

Solución 11 *Calcular una base de Gröbner de I, determinar a partir de ella el ideal $\langle TL(I)\rangle$ contar los monomios que no aparecen en él y por tanto determinar la dimensión de $\dim_k \left(\frac{k[x_1,x_2,...,x_n]}{I}\right)$. Entonces $V = \mathcal{V}(I)$ es una variedad finita si y sólo si la dimensión es finita. Además, en este caso, dicha dimensión es una cota superior al número de puntos en V.*

Ejemplo 41 *Consideremos $I = \langle x^2y - x - y, xy + x\rangle \subseteq \mathbb{C}[x, y]$, la base de Gröbner con orden grlex es*

$$G = \{x^2 + x + y, xy + x, y^2 + y\}$$

así que $\langle TL(I)\rangle = \langle x^2, xy, y^2\rangle$ *y según la sección anterior tenemos que*

$$\frac{\mathbb{C}[x,y]}{I} = \langle \overline{1}, \overline{x}, \overline{y}\rangle$$

por lo que su dimensión es 3*, y es cota para el número de soluciones. Aprovechando la base de Gröbner, calculamos fácilmente* $V = \mathcal{V}(I)$*:*

$$y^2 + y = 0 \Longrightarrow y = 0, y = -1$$

sustituyendo en la segunda ecuación cada una de las posibilidades obtenemos:

$$\begin{aligned} x\cdot 0 + x &= 0 \Longrightarrow x = y = 0 \\ x(-1) + x &= 0 \Longrightarrow x \in \mathbb{C},\ y = -1 \end{aligned}$$

y finalmente en la tercera ecuación:

$$\begin{aligned} x^2 + x + y &= 0 \Longrightarrow (x,y) = (0,0) \\ x^2 + x - 1 &= 0, x = \frac{1 \pm \sqrt{5}}{2}, y = -1 \end{aligned}$$

por lo que la cota se alcanza y tenemos 3 *soluciones, a saber:*

$$\mathcal{V}(I) = \left\{(0,0), \left(\frac{1+\sqrt{5}}{2}, -1\right), \left(\frac{1-\sqrt{5}}{2}, -1\right)\right\}$$

Por supuesto, si en el ejemplo anterior hubiéramos utilizado como campo $k = \mathbb{Q}$, hubiéramos perdido las últimas dos soluciones y $|\mathcal{V}(I)| = 1$. Es por esto que si queremos asegurar el mayor número de puntos pedimos k algebraicamente cerrado. Vemos entonces que la cota de la dimensión puede alcanzarse, pero también podría ser que se tenga una desigualdad estricta, como lo muestra el siguiente

Ejemplo 42 *Consideremos el ideal del ejemplo 40, verificamos ahí que*

$$\dim_k\left(\frac{k[x,y]}{I}\right) = 12$$

Por otro lado, en el ejemplo 32 calculamos $\mathcal{V}(I)$ *sobre* $k = \mathbb{C}$ *obteniendo las* 11 *soluciones:*

$$\mathcal{V}(I) = \{(0,0)\} \cup \{(\xi, \xi^7) | \xi^{10} = 1\}$$

Como un ejemplo más, veamos un caso en el que se tiene dimensión infinita:

Ejemplo 43 *Sea* $I = \langle x^2 + y^2 + 1 \rangle \subseteq k[x, y]$, *cuyo generador es ya la base de Gröbner reducida correspondiente a orden lex. Así,* $\langle TL(I) \rangle = \langle x^2 \rangle$ *y por tanto*

$$\frac{k[x,y]}{I} = \left\langle \overline{1}, \overline{x}, \overline{y}, \overline{y^2}, \overline{y^3}, ... \right\rangle$$

es un espacio de dimensión infinita. Por el Teorema 16 tenemos entonces que en $k = \mathbb{C}$, $\mathcal{V}(I)$ *es también un conjunto infinito. En efecto,*

$$\mathcal{V}(I) = \left\{ (z, i\sqrt{z^2+1}) | z \in \mathbb{C} \right\}$$

También este ejemplo nos ilustra que la equivalencia de finitud no se cumple necesariamente si k *no es algebraicamente cerrado. Específicamente, si* $k = \mathbb{R}$ *entonces tenemos que* $\mathcal{V}(I) = \varnothing$, *que sí es un conjunto finito.*

Antes de cerrar la sección, respondemos a la pregunta natural: ¿qué condición aparte de que k sea algebraicamente cerrado necesitamos pedir para que se cumpla la igualdad en el Corolario 6? La respuesta una vez leída no debería de sorprender: que I sea radical. Sin embargo, primero un

Lema 1 *"Sean* $z_1, z_2, ..., z_m \in k^n$ *puntos distintos, entonces existen* $p_1, p_2, ..., p_m \in k[x_1, x_2, ..., x_n]$ *tal que*

$$p_i(z_j) = \delta_{ij} = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ si } i \neq j \end{cases} \text{ „}$$

Demostración. Estos polinomios se pueden construir de la siguiente manera: en general dados $a \neq b \in k^n$, como difieren en al menos una coordenada $a_j \neq b_j \in k$, el polinomio $f \in k[x_1, x_2, ..., x_n]$ definido como

$$f(x_1, x_2, ..., x_n) = \frac{x_j - b_j}{a_j - b_j}$$

cumple $f(a) = 1$, $f(b) = 0$. Luego, en el caso de $z_1, z_2, ..., z_m$, si escogemos $i \in \{1, 2, ..., n\}$ se puede construir tal polinomio f_j al considerar las parejas de puntos $z_i \neq z_j$ $(i \neq j)$. Así, el polinomio

$$p_i = f_1 f_2 ... f_{i-1} f_{i+1} ... f_m$$

cumple justo que $p_i(z_j) = \delta_{ij}$. ■

Ahora sí concluimos con el

Teorema 17 *"Sea k algebraicamente cerrado, $I \subseteq k[x_1, x_2, ..., x_n]$ ideal radical y $V = \mathcal{V}(I)$ finita, entonces*

$$|V| = \dim_k \left(\frac{k[x_1, x_2, ..., x_n]}{I} \right) \text{"}$$

Demostración. Sea $V = \{z_1, z_2, ..., z_m\} \subseteq k^n$., por el Lema, sean $p_1, p_2, ..., p_m$ en $k[x_1, x_2, ..., x_n]$ tal que

$$p_i(z_j) = \delta_{ij}$$

y entonces proponemos a

$$\beta = \{\overline{p_1}, \overline{p_2}, ..., \overline{p_m}\}$$

como base de $\frac{k[x_1,x_2,...,x_n]}{I}$. Como ya sabemos que se cumple la desigualdad $m \leq \dim_k \left(\frac{k[x_1,x_2,...,x_n]}{I} \right)$, basta demostrar que β es un conjunto generador.
Sea entonces $\overline{p} \in \frac{k[x_1,x_2,...,x_n]}{I}$ y definimos $a_i = p(z_i)$. Consideramos $h \in k[x_1, x_2, ..., x_n]$ dado por

$$h = p - \sum_{i=1}^{m} a_i p_i$$

y notamos que $h(z_j) = p(z_j) - \sum_{i=1}^{m} a_i p_i(z_j) = p(z_j) - \sum_{i=1}^{m} a_i \delta_{ij} = a_j - a_j \cdot 1 = 0$ $\forall j = 1, .., m$, por lo que $h \in \mathcal{I}(V) = \mathcal{I}(\mathcal{V}(I))$. Pero por el Nullstellensatz Fuerte y como I es radical: $\mathcal{I}(\mathcal{V}(I)) = rad(I) = I$. Concluimos que $h \in I$ y así

$$\overline{p - \sum_{i=1}^{m} a_i p_i} = \overline{0}$$

por lo que

$$\overline{p} = \sum_{i=1}^{m} a_i \overline{p_i}$$

que es lo que queríamos probar. Así, $\dim_k \left(\frac{k[x_1,x_2,...,x_n]}{I} \right) = |\beta| = m$. ■

4.3. Problema de Mapeos Polinomiales

Vamos a plantear los problemas en el contexto de $k[x_1, x_2, ..., x_n]$ no sólo como anillo, sino como k-álgebra. La definición en general es:

Definición 35 *Una* k-álgebra *es un anillo que contiene al campo* k *como subanillo. Si* A *y* B *son* k*-álgebras,* $\phi : A \longrightarrow B$ *es un* homomorfismo *de* k*-álgebras sii es un homomorfismo de anillos tal que* $\phi|_k = Id$*, es decir, tal que* $\phi(a) = a \ \forall a \in k$*.*

Ya que estaremos trabajando con k-álgebras de polinomios, notar que si

$$\phi : k[y_1, y_2, ..., y_m] \longrightarrow k[x_1, x_2, ..., x_n]$$

es un homomorfismo, entonces queda determinado por los valores que toma en y_i:

$$\phi(y_i) = f_i$$

para $i = 1, ..., m$, pues si $h \in k[y_1, y_2, ..., y_m]$, $h = \sum_{\alpha} c_\alpha \cdot y_1^{\alpha_1} y_2^{\alpha_2} ... y_m^{\alpha_m}$ entonces

$$\phi(h) = \sum_{\alpha} c_\alpha \cdot f_1^{\alpha_1} f_2^{\alpha_2} ... f_m^{\alpha_m} = h(f_1, f_2, ..., f_m) \in k[x_1, x_2, ..., x_n]$$

Definición 36 *Recordemos que dado* $\phi : k[y_1, y_2, ..., y_m] \longrightarrow k[x_1, x_2, ..., x_n]$ *se tienen el ideal*

$$\ker \phi = \{h \in k[y_1, y_2, ..., y_m] | \phi(h) = 0\}$$

conocido como el kernel *o* núcleo *de* ϕ *y la subálgebra* imagen *de* ϕ *:*

$$\operatorname{Im} \phi = \{g \in k[x_1, ..., x_n] | \exists h \in k[y_1, ..., y_m] \text{ con } \phi(h) = g\}$$

El Primer Teorema de Isomorfismo (de k-álgebras) dice que:

$$k[y_1, y_2, ..., y_m]/Ker\phi \cong \operatorname{Im} \phi$$

¿Qué tienen que ver estos homomorfismos con las funciones polinomiales que habíamos definido tan pronto como en la pág. 11? Si tenemos $f : k^n \to k^m$ función polinomial, entonces automáticamente induce un homomorfismo de k-álgebras dado justo por

$$\phi(y_i) = f_i \in k[x_1, x_2, ..., x_n]$$

(y viceversa). Resolveremos primero el siguiente problema:

Problema 12 *Sea* $\phi : k[y_1, y_2, ..., y_m] \longrightarrow k[x_1, x_2, ..., x_n]$ *homomorfismo de* k*-álgebras, determinar generadores para* $Ker\phi$*.*

Para resolver el problema primero un

Lema 2 *"Sean* $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in R$*, entonces*

$$a_1a_2...a_n - b_1b_2...b_n \in \langle a_1 - b_1, a_2 - b_2, ..., a_n - b_n\rangle \text{ "}$$

Demostración. Por inducción, si $n = 1$ claramente $a_1 - b_1 \in \langle a_1 - b_1\rangle$.
Supongamos la proposición se cumple para $n-1$ términos a_i, b_i, entonces consideremos

$$a_1a_2...a_n - b_1b_2...b_n = a_1(a_2...a_n - b_2...b_n) + b_2...b_n(a_1 - b_1)$$

por hipótesis de inducción se tiene que $a_2...a_n - b_2...b_n \in \langle a_2 - b_2, ..., a_n - b_n\rangle$ y así $a_1a_2...a_n - b_1b_2...b_n \in \langle a_1 - b_1, a_2 - b_2, ..., a_n - b_n\rangle$ ■

Ahora sí presentamos el teorema principal:

Teorema 18 *"Sea* $\phi : k[y_1, y_2, ..., y_m] \longrightarrow k[x_1, x_2, ..., x_n]$ *homomorfismo tal que* $\phi(y_i) = f_i$ *y sea* $I = \langle y_1 - f_1, y_2 - f_2, ..., y_n - f_n\rangle \subseteq k[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$*, entonces*

$$\ker\phi = I \cap k[x_1, x_2, ..., x_n] \text{"}$$

Demostración. $\supseteq$) Sea $g \in I \cap k[x_1, x_2, ..., x_n]$, entonces existen $h_i \in k[x_1, .., x_n, y_1, .., y_m]$ tal que g se escribe como

$$g = \sum_{i=1}^{m} h_i(x_1, ..., x_n, y_1, ..., y_m)(y_i - f_i(x_1, ..., x_n))$$

sabemos que la evaluación de ϕ en g es la correspondiente de sustituir cada y_i por f_i:

$$\phi(g) = \sum_{i=1}^{m} h_i(x_1, ..., x_n, f_1, ..., f_m)(f_i - f_i)) = 0$$

por lo que $g \in \ker\phi$.
$\subseteq$) Sea $g \in \ker\phi \subseteq k[y_1, y_2, ..., y_m]$, con

$$g = \sum_{\alpha} c_\alpha \cdot y_1^{\alpha_1} y_2^{\alpha_2} ... y_m^{\alpha_m}$$

como por hipótesis

$$0 = \phi(g) = g(f_1, f_2, ..., f_m) = \sum_{\alpha} c_\alpha \cdot f_1^{\alpha_1} f_2^{\alpha_2} ... f_m^{\alpha_m}$$

entonces

$$\begin{aligned} g &= \sum_{\alpha} c_\alpha \cdot y_1^{\alpha_1} y_2^{\alpha_2} ... y_m^{\alpha_m} - \sum_{\alpha} c_\alpha \cdot f_1^{\alpha_1} f_2^{\alpha_2} ... f_m^{\alpha_m} \\ &= \sum_{\alpha} c_\alpha \cdot (y_1^{\alpha_1} y_2^{\alpha_2} ... y_m^{\alpha_m} - f_1^{\alpha_1} f_2^{\alpha_2} ... f_m^{\alpha_m}) \end{aligned}$$

y por el Lema tenemos que cada sumando pertenece a

$$\langle y_1^{\alpha_1} - f_1^{\alpha_1}, y_2^{\alpha_2} - f_2^{\alpha_2}, ..., y_n^{\alpha_n} - f_n^{\alpha_n} \rangle \subseteq \langle y_1 - f_1, y_2 - f_2, ..., y_n - f_n \rangle = I,$$

por lo que $g \in I$ también. ■

Así, tenemos por el teorema que el $\ker \phi$ es un cierto ideal de eliminación, en este caso eliminando las variables x_i. Con el método de eliminación mediante bases de Gröbner, tenemos una forma de cálculo de generadores del núcleo:

Solución 12 *Sea $I = \langle y_1 - f_1, y_2 - f_2, ..., y_n - f_n \rangle$ y G base de Gröbner bajo un orden de eliminación ($x_i > y_j \ \forall i, j$). Entonces*

$$\ker \phi = \langle G \cap k[y_1, y_2, ..., y_m] \rangle$$

Apliquemos este teorema a ejemplos concretos:

Ejemplo 44 *Sea $\phi : \mathbb{Q}[u, v] \longrightarrow \mathbb{Q}[x]$ definida por $\phi(u) = x^4 + x$ y $\phi(v) = x^3$. Determinamos el $\ker \phi$ con el método anterior. Consideramos*

$$I = \left\langle u - (x^4 + x), v - x^3 \right\rangle$$

y la base de Gröbner de I bajo orden $lex(x > y > u > v)$ es:

$$\begin{aligned} G &= \{x^3 - v,\ x^2u - v^2 - v,\ xu^2 - v^3 - 2v^2 - v, \\ &\quad xv + x - u,\ u^3 - v^4 - 3v^3 - 3v^2 - v\} \end{aligned}$$

por lo que al considerar el único polinomio que no contiene x ni y tenemos

$$\ker \phi = \left\langle u^3 - v^4 - 3v^3 - 3v^2 - v \right\rangle$$

Ejemplo 45 *Sea $\phi : \mathbb{Q}[u, v, w] \longrightarrow \mathbb{Q}[x, y]$ definida por los valores $\phi(u) = x^2 + y$, $\phi(v) = x + y, \phi(w) = x - y^2$. Encontramos $\ker \phi$ mediante la solución anterior. Consideramos el ideal*

$$I = \left\langle u - (x^2 + y), v - (x + y), w - (x - y^2) \right\rangle \subseteq \mathbb{Q}[x, y, u, v, w]$$

y calculamos una base de Gröbner de I bajo el orden $lex(x > y > u > v > w)$:

$$\begin{aligned} G &= \{x + y - v,\ y^2 + y - v + w,\ 2yu + 2yw + uv + 3u - v^3 - 3vw - 3v + 3w, \\ &\quad 2yv + u - v^2 - v + w, u^2 - 2uv^2 - 4uv + 2uw + v^4 + 2v^2w + 3v^2 - 4vw + w^2\} \end{aligned}$$

por lo que

$$\ker \phi = \left\langle v^4 + (3 - 2u + 2w)v^2 - 4(u + w)v + (u + w)^2 \right\rangle$$

Ahora nos preguntamos sobre la $\operatorname{Im} \phi$ en el siguiente

Problema 13 *Sea $\phi : k[y_1, y_2, ..., y_m] \longrightarrow k[x_1, x_2, ..., x_n]$ homomorfismo de k-álgebras, y sea $f \in k[x_1, x_2, ..., x_n]$. Determinar si $f \in \operatorname{Im} \phi$ o no.*

Podemos resolver este problema mediante el siguiente

Teorema 19 *"Sea $\phi : k[y_1, y_2, ..., y_m] \longrightarrow k[x_1, x_2, ..., x_n]$ homomorfismo tal que $\phi(y_i) = f_i$ y sea $I = \langle y_1 - f_1, y_2 - f_2, ..., y_n - f_n \rangle \subseteq k[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$ y G la base de Gröbner reducida respecto a un orden de eliminación con $x_i > y_j\ \forall i, j$, y sea $f \in k[x_1, x_2, ..., x_n]$, entonces se tiene que*

$$f \in \operatorname{Im} \phi \Longleftrightarrow h = \overline{f}^G \in k[y_1, y_2, ..., y_m].$$

Es más, en este caso, $\phi(h) = f$"

Demostración. $\Longrightarrow$) Sea $f \in \operatorname{Im} \phi$, entonces existe $g \in k[y_1, y_2, ..., y_m]$ tal que $f = \phi(g) = g(f_1, f_2, ..., f_n)$. Si consideramos el polinomio

$$f(x_1, x_2, ..., x_n) - g(y_1, y_2, ..., y_m) \in k[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$$

como $f(x_1, x_2, ..., x_n) = g(f_1, f_2, ..., f_n)$, entonces $f(x_1, x_2, ..., x_n) - g(y_1, y_2, ..., y_m)$ es $g(f_1, f_2, ..., f_n) - g(y_1, y_2, ..., y_m)$ y por el Lema 2 aplicado a cada diferencia de término a término correspondiente tenemos que entonces

$$f(x_1, x_2, ..., x_n) - g(y_1, y_2, ..., y_m) \in I$$

y luego al tomar residuos respecto a la base de Gröbner de I, tenemos $\overline{f - g}^G = 0$, es decir, $\overline{f}^G - \overline{g}^G = 0$ y así:

$$h = \overline{f(x_1, ..., x_n)}^G = \overline{g(y_1, ..., y_m)}^G$$

pero el residuo de g respecto a G sólo puede seguir teniendo variables $y_1, y_2, ..., y_m$ ya que estamos en un orden de eliminación con las $x_i > y_j$. Por lo tanto, $h = \overline{f}^G \in k[y_1, y_2, ..., y_m]$.
$\Longleftarrow$) Si $h = \overline{f}^G \in k[y_1, y_2, ..., y_m]$ entonces como $f - h \in I$ tenemos

$$f(x_1, .., x_n) - h(y_1, .., y_m) = \sum_{i=1}^{m} g_i(y_1, .., y_m, x_1, .., x_n)(y_i - f_i(x_1, .., x_n))$$

y al evaluar cada y_i en f_i en la expresión anterior obtenemos

$$f(x_1, ..., x_n) - h(y_1, ..., y_m) = 0$$

es decir, $\phi(h) = h(f_1, f_2, ..., f_m) = f(x_1, x_2, ..., x_n)$. ■

Solución 13 *Aplicar el método descrito en el Teorema anterior. Calcular la base de Gröbner G correspondiente y luego con Algoritmo de la División Multivariado dividir f por G para determinar el residuo $h = \overline{f}^G$, examinando si contiene o no solamente variables y_i con $1 \leq i \leq m$.*

Vemos que la solución propuesta no sólo resuelve el problema, sino que además en caso de resolver afirmativamente la cuestión, encuentra $h \in k[y_1, y_2, ..., y_m]$ tal que $\phi(h) = f$.

Ejemplo 46 *Sea $\phi : \mathbb{Q}[u, v] \longrightarrow \mathbb{Q}[x]$ dada por $\phi(u) = x^4 + x^2 + x$ y $\phi(v) = x^3 - x$. Usamos el método para determinar si $f = x^3$ y $g = 3x^7 - x^6 + 6x^4 - 3x^3 - 3x^2 + x$ pertenecen a $\operatorname{Im}\phi$. Consideramos entonces el ideal*

$$I = \left\langle u - (x^4 + x^2 + x), v - (x^3 - x) \right\rangle \subseteq \mathbb{Q}[x, u, v]$$

la base de Gröbner reducida bajo orden $lex(x > u > v)$ es

$$\begin{aligned} G \;=\; & \{2x^2 + x + xv - u, xv^2 + 2xu + 2vx - uv - u - 3x - 4v, \\ & xv^3 + 3xv^2 - 9xv - 3x + 2u^2 - uv^2 - 2uv - 5u - 8v^2 - 8v, \\ & u^3 - v^4 - 7uv^2 - 3v^3 - 4u^2 - 8uv - 7v^2 + 3u + 3v\} \end{aligned}$$

Al tomar el residuo de f se obtiene $\overline{x^3}^G = x + v$ que no pertenece a $\mathbb{Q}[u, v]$ y por tanto concluimos que $f \notin \operatorname{Im}\phi$.
Por otro lado, al tomar el residuo de $g = 3x^7 - x^6 + 6x^4 - 3x^3 - 3x^2 + x$ respecto a G se obtiene $\overline{g}^G = u - v^2 + 3uv$ que sí pertenece a $\mathbb{Q}[u, v]$, por lo que $g \in \operatorname{Im}\phi$ y además

$$\phi(u - v^2 + 3uv) = g$$

Como último problema de la sección, consideramos el Problema de Suprayectividad:

Problema 14 *Sea* $\phi : k[y_1, y_2, ..., y_m] \longrightarrow k[x_1, x_2, ..., x_n]$ *homomorfismo de* k*-álgebras, determinar si* ϕ *es suprayectivo o no lo es.*

Notar que un homomorfismo ϕ de k-álgebras es suprayectivo si y sólo si cada $x_i \in \operatorname{Im}\phi$. Así, podríamos proponer como solución al problema que se cheque esto con el método anterior para cada x_i $1 \leq i \leq n$. Sorprendentemente, no es necesario calcular los residuos y el problema puede resolverse simplemente inspeccionando la base de Gröbner:

Teorema 20 *"Sea* $\phi : k[y_1, y_2, ..., y_m] \longrightarrow k[x_1, x_2, ..., x_n]$ *homomorfismo tal que* $\phi(y_i) = f_i$ *y sea* $I = \langle y_1 - f_1, y_2 - f_2, ..., y_n - f_n\rangle \subseteq k[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$ *y* G *la base de Gröbner reducida respecto a un orden de eliminación con* $x_i > y_j$ $\forall i, j$*, entonces* ϕ *es sobre si y sólo si para cada* $1 \leq i \leq n$ *existe* $g_i \in G$ *tal que* $g_i = x_i - h_i$ *con* $h_i \in k[y_1, y_2, ..., y_m]$*. Es más, en este caso,* $x_i = \phi(h_i)$*"*

Demostración. $\Longrightarrow$) Supongamos que ϕ es sobre y sin pérdida de generalidad $x_1 < x_2 < ... < x_n$ en el orden. Como $x_1 \in \operatorname{Im}\phi$, por el Teorema anterior tenemos que $\overline{x_1}^G = h_1' \in k[y_1, y_2, ..., y_m]$, y así $x_1 - h_1' \in G$. Como G es base de Gröbner, existe g_1 tal que $TL(g_1)|TL(x_1 - h_1') = x_1$ (pues $h_i' \in k[y_1, y_2, ..., y_m]$, y $x_1 > y_j$ $\forall j$), y como g_1 es mónico: $TL(g_1) = x_1$. Pero los únicos términos que pueden ser menores que x_1 involucran sólo a las variables y_j con $j = 1, ..., m$, así que $g_1 = x_1 - h_1$ con $h_1 \in k[y_1, y_2, ..., y_m]$. Similarmente, para x_2 que está en $\operatorname{Im}\phi$, por el Teorema anterior $\overline{x_2}^G = h_2' \in k[y_1, y_2, ..., y_m]$ y de nuevo $x_2 - h_2' \in G$, concluyendo que existe $g_2 \in G$ tal que $TL(g_2)|TL(x_2 - h_2') = x_2$, es decir, $TL(g_2) = x_2$. Los términos menores que x_2 involucran a las variables x_1 y y_j. Pero no puede haber un término que involucre a x_1 porque $g_1 = x_1 - h_1 \in G$ y entonces $TL(g_1)$ divide a ese término de g_2, contradiciendo el hecho de que G es reducida. Así, $g_2 = x_2 - h_2$ con $h_2 \in k[y_1, y_2, ..., y_m]$. Continuando este mismo argumento para x_i con $i = 3$ hasta $i = n$, tenemos el resultado.
$\Longleftarrow$) Si $g_i = x_i - h_i$ con $h_i \in k[y_1, y_2, ..., y_m]$, entonces tenemos que $x_i - h_i \in I$ por lo que existen $a_j \in k[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$ tal que

$$x_i - h_i(y_1, .., y_m) = \sum_{j=1}^{m} a_j(y_1, .., y_m, x_1, .., x_n)(y_i - f_i(x_1, .., x_n))$$

y al evaluar cada y_j en f_j se obtiene $x_i - h_i(f_1, .., f_m) = 0$, es decir,

$$\phi(h_i) = h_i(f_1, f_2, ..., f_m) = x_i.$$

Como cada $x_i \in \operatorname{Im}\phi$, y $\operatorname{Im}\phi$ es subálgebra de $k[x_1, x_2, ..., x_n]$, entonces $\operatorname{Im}\phi$ es $k[x_1, x_2, ..., x_n]$, es decir, ϕ es sobre. ■

Solución 14 *Aplicar el Teorema anterior, para la base de Gröbner del ideal* $I = \langle y_1 - f_1, y_2 - f_2, ..., y_n - f_n \rangle$, *inspeccionar la existencia de cada* $g_i \in G$ *tal que* $g_i = x_i - h_i$ *con* $h_i \in k[y_1, y_2, ..., y_m]$. *Se tiene la suprayectividad si y sólo si existe tal* g_i *para cada* $i = 1, ..., n$.

Ejemplo 47 *Ni en la base de Gröbner correspondiente al mapeo del ejemplo 44 ni en la base de Gröbner correspondiente al mapeo del ejemplo 45 aparece un polinomio de la forma* $x - h$ *con* h *en* u, v, w, *por lo que ninguno de estos homomorfismos es suprayectivo.*

Ejemplo 48 *Sea* $\phi : \mathbb{R}[u, v, w] \longrightarrow \mathbb{R}[x, y]$ *dado por* $\phi(u) = x^2 + y$, $\phi(v) = x - y^2$ *y* $\phi(w) = x^2 - y$. *Calculamos la base de Gröbner reducida de*

$$I = \left\langle u - (x^2 + y), v - (x - y^2), w - (x - y^2) \right\rangle$$

obteniendo

$$\begin{aligned} G \;=\; & \Big\{ x - v - \frac{1}{4}u^2 + \frac{1}{2}uw - \frac{1}{4}w^2, y - \frac{1}{2}u + \frac{1}{2}w,\ u^4 - 4u^3w + 8u^2v \\ & +6u^2w^2 - 16uvw - 4uw^3 - 8u + 16v^2 + 8vw^2 + w^4 - 8w \Big\} \end{aligned}$$

Podemos notar que los primeros dos polinomios son justamente de la forma $x - h_1$ *y* $y - h_2$ *con* $h_1, h_2 \in \mathbb{R}[u, v, w]$ *por lo que* ϕ *es sobre.*

4.4. Problema de los Polinomios Simétricos

Un polinomio $f \in k[x_1, x_2, .., x_n]$ se llama *simétrico* sii

$$f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

para cualquier permutación de n elementos

$$\sigma \in S_n = \{f : \{1, 2, ..., n\} \longrightarrow \{1, 2, ..., n\} | f \text{ biyectiva}\}.$$

El teorema de Gauss, mejor conocido el Teorema Fundamental de los Polinomios Simétricos, asegura que los polinomios

$$\begin{aligned} s_1 &= x_1 + x_2 + ... + x_n \\ s_2 &= x_1x_2 + x_1x_3 + ... + x_1x_n + x_2x_3 + ... + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2...x_n \end{aligned}$$

generan a todos los polinomios simétricos. Es decir, se tiene el siguiente teorema (cuya prueba se puede encontrar por ejemplo en [11]):

Teorema 21 *(FUNDAMENTAL DE LOS POLINOMIOS SIMÉTRICOS) "Todo polinomio simétrico en $k[x_1, x_2, ..., x_n]$ se puede escribir de forma única como un polinomio en los polinomios simétricos elementales $s_1, s_2, ..., s_n$"*

A raíz del teorema, uno puede formular el siguiente

Problema 15 *Sea $f \in k[x_1, x_2, .., x_n]$, determinar si f es simétrico o no, y en caso afirmativo, encontrar el polinomio en $s_1, s_2, ..., s_n$ que representa a f.*

Para resolver el problema, lo planteamos en el lenguaje de homomorfismos de k-álgebras que estudiamos en la sección anterior. Vemos $s_1, s_2, ..., s_n$ como variables y entonces consideramos $\phi : k[s_1, s_2, ..., s_n] \longrightarrow k[x_1, x_2, ..., x_n]$ dado por

$$\begin{aligned} \phi(s_1) &= x_1 + x_2 + ... + x_n \\ \phi(s_2) &= x_1x_2 + x_1x_3 + ... + x_1x_n + x_2x_3 + ... + x_{n-1}x_n \\ &\vdots \\ \phi(s_n) &= x_1x_2...x_n \end{aligned}$$

Entonces el problema se traduce a preguntar si dado $f \in k[x_1, x_2, .., x_n]$, $f \in \operatorname{Im}\phi$ y en dado caso encontrar $h \in k[s_1, s_2, ..., s_n]$ tal que $\phi(h) = f$. Este problema ya lo resolvimos en la sección anterior, por lo que inmediatamente presentamos la

Solución 15 *Sea G base de Gröbner del ideal $I \subseteq k[x_1, x_2, ..., x_n, s_1, s_2, ..., s_n]$,*

$$I = \langle s_1 - (x_1 + x_2 + ... + x_n), ..., s_n - x_1x_2...x_n \rangle$$

bajo un orden de eliminación con $x_i > s_j \ \forall i, j \in \{1, 2, ..., n\}$. Luego $f \in k[x_1, x_2, ..., x_n]$ es simétrico si y sólo si $h = \overline{f}^G \in k[s_1, s_2, ..., s_n]$, en cuyo caso h es el polinomio en $s_1, s_2, ..., s_n$ buscado.

Ejemplo 49 *Sea* $f = x^4+y^4+z^4-x^2y^2-x^2z^2-y^2z^2 \in k[x,y,z]$. *Se puede ver que* f *es simétrico (aunque de todas formas el método lo comprueba). Consideramos*

$$I = \langle s_1 - (x+y+z), s_2 - (xy+xz+yz), s_3 - xyz\rangle$$

y la base de Gröbner con $lex(x > y > z > s_1 > s_2 > s_3)$ *es*

$$\begin{aligned} G &= \{x+y+z-s_1, y^2+yz-ys_1+z^2-s_1z+s_2, \\ &\quad z^3-z^2s_1+zs_2-s_3\} \end{aligned}$$

Así, al calcular $\overline{f}^G$ *se tiene*

$$\overline{f}^G = s_1^4 - 4s_1^2s_2 + s_2^2 + 6s_1s_3$$

y éste es el polinomio buscado.

4.5. Problema de Implicitación

Ahora pasamos a una aplicación que es muy útil. Es común tener funciones que parametrizan ciertas curvas o superficies, pero a menudo se busca encontrar una ecuación implícita que las defina, librándonos de los parámetros. Como ejemplo muy sencillo, la función $\phi : \mathbb{R} \to \mathbb{R}^2$ dada por

$$\phi(t) = (\cos(t), sen(t))$$

tiene como imagen al círculo unitario que puede representarse implícitamente como

$$\phi(\mathbb{R}) = \{(x,y) \in \mathbb{R}^2 | x^2+y^2 = 1\}$$

Nosotros buscaremos hacer esto cuando tenemos una función polinomial $\phi : k^m \to k^n$, con componentes $\phi_i = f_i \in k[t_1, t_2, ..., t_m]$, $1 \leq i \leq n$ describiendo la imagen $\phi(k^m)$ como la variedad asociada a un conjunto de polinomios en n variables; es decir, encontrando un conjunto finito $F \subseteq k[x_1, x_2, ..., x_m]$ tal que $\phi(k^n) = \mathcal{V}(F)$
En general, esto no siempre es posible, pues la imagen $\phi(k^n)$ puede no ser una variedad algebraica. En ese caso, el problema de implicitación polinomial 'puro' no tiene solución, pero en el sentido extendido ahora se querría encontrar la implicitación para la mínima variedad algebraica que contiene a $\phi(k^n)$, es decir, su cerradura de Zariski $\overline{\phi(k^n)}^Z = \mathcal{V}(\mathcal{I}(\phi(k^n))$.

Problema 16 *Supongamos que se tienen las ecuaciones paramétricas que definen a* $V \subseteq k^n$

$$\begin{aligned} x_1 &= f_1(t_1, t_2, ..., t_m) \\ x_2 &= f_2(t_1, t_2, ..., t_m) \\ &\vdots \\ x_n &= f_n(t_1, t_2, ..., t_m) \end{aligned}$$

con $f_i \in k[t_1, t_2, ..., t_m]$. *Encontrar, si es posible, ecuaciones polinomiales en las variables* x_i *que definan* V.

La idea es considerar la variedad en k^{m+n} determinada por el sistema polinomial en $k[t_1, t_2, ..., t_m, x_1, x_2, ..., x_n]$:

$$\begin{aligned} x_1 - f_1(t_1, t_2, ..., t_m) &= 0 \\ x_2 - f_2(t_1, t_2, ..., t_m) &= 0 \\ &\vdots \\ x_n - f_n(t_1, t_2, ..., t_m) &= 0 \end{aligned}$$

es decir,

$$V = V(x_1 - f_1, x_2 - f_2, ..., x_n - f_n)$$

Reconocemos que $V = V(I)$ con $I = \langle x_1 - f_1, x_2 - f_2, ..., x_n - f_n \rangle$. Necesitamos estudiar el comportamiento de esta variedad respecto a los ideales de eliminación de I para poder dar la conexión necesaria con nuestra teoría.

En el problema de Resolución de Sistemas de Ecuaciones Polinomiales, lo que se hizo fue estudiar los ideales de eliminación I_j para obtener información parcial de $\mathcal{V}(I)$ por medio de sus proyecciones $\pi_j(V)$, a raíz de la Proposición 15. Cuando k es algebraicamente cerrado, podemos decir incluso más:

Teorema 22 *(DE LA CERRADURA) "Sea* k *algebraicamente cerrado,* $V = \mathcal{V}(f_1, f_2, ..., f_s) = \mathcal{V}(I) \subseteq k^n$ *y* $\pi_j : k^n \to k^{n-j}$ *la proyección sobre las últimas* $n - j$ *componentes, entonces*

$$\mathcal{V}(I_j) = \overline{\pi_j(V)}^Z$$

Es decir, el ideal de eliminación I_j *define la cerradura de Zariski de la proyección de* V *sobre* k^{n-j} *"*

Demostración. $\supseteq$) De la Proposición 15 tenemos que $\pi_j(V) \subseteq \mathcal{V}(I_j)$ y como $\overline{\pi_j(V)}^Z$ es la variedad algebraica más pequeña que contiene a $\pi_j(V)$ entonces $\overline{\pi_j(V)}^Z \subseteq \mathcal{V}(I_j)$.

$\subseteq$) Veamos que $\mathcal{I}(\pi_j(V)) \subseteq rad(I_j)$:
Sea $f \in \mathcal{I}(\pi_j(V))$, es decir, $f(a_{j+1}, ..., a_n) = 0 \ \forall (a_{j+1}, ..., a_n) \in \pi_j(V)$, entonces considerado en el anillo mayor $k[x_1, x_2, ..., x_n]$ como las variables $x_1, x_2, ..., x_l$ no aparecen en f, podemos escribir

$$f(a_1, a_2, ..., a_n) = 0 \quad \forall (a_1, a_2, ..., a_n) \in V$$

es decir, $f \in \mathcal{I}(V)$. Pero por el Nullstellensatz Fuerte (Teorema 3):

$$\mathcal{I}(V) = rad(I)$$

por lo que existe $m > 0$ tal que $f^m \in I$, pero como al elevar f a la m siguen sin aparecer las variables $x_1, x_2, ..., x_l$ tenemos que de hecho $f^m \in I_j$, de donde $f \in rad(I_j)$ como buscábamos.
También por la Proposición 4(parte 4) se sigue $\mathcal{V}(I_j) = \mathcal{V}(rad(I_j))$ así que finalmente al aplicar $\mathcal{V}$ a $\mathcal{I}(\pi_j(V)) \subseteq rad(I_j)$:

$$\mathcal{V}(I_j) = \mathcal{V}(rad(I_j)) \subseteq \mathcal{V}(\mathcal{I}(\pi_j(V))) = \overline{\pi_j(V)}^Z$$

■

Aunque el Teorema de la Cerradura pide que k sea algebraicamente cerrado, sorprendentemente nos permite probar el siguiente teorema que vale para cualquier k infinito (no necesariamente algebraicamente cerrado). Este teorema es el que buscábamos para poder ver la solución al Problema de Implicitación:

Teorema 23 *"Sea k campo infinito y $\phi : k^m \to k^n$ una función polinomial con componentes $f_i \in k[t_1, t_2, ..., t_m]$, $1 \leq i \leq n$. Sea*

$$I = \langle x_1 - f_1, x_2 - f_2, ..., x_n - f_n \rangle \subseteq k[t_1, t_2, ..., t_m, x_1, x_2, ..., x_n]$$

y sea $I_m = I \cap k[x_1, x_2, ..., x_n]$ el m-ésimo ideal de eliminación. Entonces

$$\mathcal{V}(I_m) = \overline{\phi(k^m)}^Z$$

es decir, la variedad $\mathcal{V}(I_m)$ es la variedad más pequeña en k^n que contiene a la imagen $\phi(k^m)$"

Demostración. Sea $V = \mathcal{V}(I) \subseteq k^{m+n}$, es decir,

$$\begin{aligned} V &= \{(t_1, t_2, ..., t_m, x_1, x_2, ..., x_n) | f_1(t_1, ..., t_m) = x_1, ..., f_n(t_1, ..., t_m) = x_n\} \\ &= \{(t_1, ..., t_m, x_1, ..., x_n) \in k^{m+n} | \phi(t_1, ..., t_m) = (x_1, x_2, ..., x_n)\} \\ &= \{(\overline{t}, \overline{x}) \in k^{m+n} | \phi(\overline{t}) = \overline{x}\} \end{aligned}$$

por lo que V es la gráfica de $\phi : k^m \to k^n$. Por otro lado, al proyectar la gráfica sobre k^m

$$\begin{aligned} \pi_m(V) &= \{(x_1, x_2, ..., x_n) | f_1(t_1, ..., t_m) = x_1, ..., f_n(t_1, ..., t_m) = x_n\} \\ &= \{(f_1(t_1, ..., t_m), ..., f_n(t_1, ..., t_m)) | (t_1, ..., t_m) \in k^m\} \\ &= \{\phi(t_1, ..., t_m) | (t_1, ..., t_m) \in k^m\} = \phi(k^m) \end{aligned}$$

es decir, se recupera la imagen $\phi(k^m)$. [1]Consideramos dos casos:
(i) k es algebraicamente cerrado: Entonces podemos aplicar el Teorema de la Cerradura para obtener $\mathcal{V}(I_m) = \overline{\pi_m(V)}^Z$, pero como de lo anterior tenemos que $\pi_m(V) = \phi(k^m)$, se concluye que $\mathcal{V}(I_m) = \overline{\phi(k^m)}^Z$.

(ii) k no es algebraicamente cerrado: Se puede probar usando Axioma de Elección (en su forma equivalente de Lema de Zorn) que todo campo tiene una cerradura algebraica, es decir, que existe una extensión K de k tal que K es algebraicamente cerrado y contiene como subcampo a k. Tal demostración se puede revisar en [11]. Consideremos pues a K, sobre el cual ya se puede aplicar el Teorema de la Cerradura. Notar que el ideal de eliminación $I_m = I \cap k[x_1, x_2, ..., x_n]$ no cambia al considerarlo en K, es decir, $I_m = I \cap K[x_1, x_2, ..., x_n]$ pues el algoritmo que tenemos para calcularlo es exactamente el mismo independientemente del campo. Sin embargo, hacemos distinción con subíndice entre $\mathcal{V}_k(I_m)$ y $\mathcal{V}_K(I_m)$ (el primero está contenido en el segundo). Ahora probamos $\mathcal{V}_k(I_m) = \overline{\phi(k^m)}^Z$:

$\supseteq$) Como tenemos de la Proposición 15 que $\pi_m(V) \subseteq \mathcal{V}_k(I_m)$ y además $\pi_m(V) = \phi(k^m)$, concluimos que $\phi(k^m) \subseteq \mathcal{V}_k(I_m)$, de donde $\overline{\phi(k^m)}^Z \subseteq \mathcal{V}_k(I_m)$.

$\subseteq$) Sea $Z_k = \mathcal{V}_k(g_1, g_2, .., g_s) \subseteq k^n$ una variedad que también contiene a $\phi(k^m)$ y veamos que $\mathcal{V}_k(I_m) \subseteq Z_k$. Como cada g_j se anula en Z_k, y $\phi(k^m) \subseteq Z_k$, en particular se anula en $\phi(k^m)$. Entonces $g_j \circ \phi(k^m) \equiv 0$, es decir, $g_i \circ \phi$ se anula en todo k^m. Como $g_j \in k[x_1, x_2, ..., x_n]$ y cada $f_i \in k[t_1, t_2, ...t_m]$, entonces $g_j \circ \phi \in k[t_1, t_2, ...t_m]$; es decir, es un polinomio tal que $g_i \circ \phi \in \mathcal{I}(k^m)$ Como k es infinito, por la Proposición 4 (parte 3), concluimos que $g_j \circ \phi \equiv 0$ es el polinomio constante 0 para cada $j = 1, 2, .., s$. Entonces claramente los $g_j \circ \phi$ también se anulan en K^m, y por tanto

[1]Esto se expresa diciendo que la imagen de la parametrización es la proyección de su gráfica.

cada g_j se anula en $\phi(K^m)$; es decir, $\phi(K^m) \subseteq Z_K = \mathcal{V}_K(g_1, g_2, .., g_s)$.
Por otro lado, como K es algebraicamente cerrado, por el caso (i) tenemos que $\overline{\phi(K^m)}^Z = \mathcal{V}_K(I_m)$, y ya que acabamos de probar que $\phi(K^m) \subseteq Z_K$ con Z_K variedad, entonces $\mathcal{V}_K(I_m) \subseteq Z_K$. Así, al restringirnos a los ceros $\mathcal{V}_k(I_m) \subseteq \mathcal{V}_K(I_m)$ tenemos que están contenidos en los ceros $\mathcal{V}_k(g_1, g_2, .., g_s) = Z_k$, por lo que $\mathcal{V}_k(I_m) \subseteq Z_k$ y queda probado que $\mathcal{V}_k(I_m)$ es la variedad más pequeña que contiene a $\phi(k^m)$, es decir, $\mathcal{V}_k(I_m) = \overline{\phi(k^m)}^Z$. ■

Así, tenemos:

Solución 16 *Escoger un orden de eliminación con $t_i > x_j$ (como el orden lexicográfico $t_1 > t_2 > ...t_m > x_1 > x_2 > ... > x_n$) y calcular una base del ideal de eliminación $I_{t_m} \subseteq k[x_1, x_2, ..., x_n]$, donde*

$$I = \langle x_1 - f_1(t_1, t_2, ..., t_m), ..., x_n - f_n(t_1, t_2, ..., t_m) \rangle$$

Los polinomios generadores igualados a 0 definirán implícitamente a la cerradura de Zariski de V (generarán a $\mathcal{I}(\phi(k^n))$).

Esto se logra calculando una base de Gröbner del ideal generado por el sistema y luego considerar las que sólo constan de $x_1, x_2, ..., x_n$). Entonces estas ecuaciones restantes definen la variedad implícitamente.

Ejemplo 50 *Sea $\phi : k \to k^2$ dada por $\phi(t) = (t^2, t^3)$. Entonces consideramos el ideal $I = \langle x - t^2, y - t^3 \rangle \subseteq k[t, x, y]$ con orden lexicográfico $t > x > y$. La base de Gröbner reducida de I es:*

$$G = \{t^2 - x, xt - y, yt - x^2, x^3 - y^2\}$$

El único polinomio que pertenece al ideal de eliminación I_t (es decir, en el que no aparece t) es $x^3 - y^2$, por lo que la ecuación implícita de $\phi(k^n)$ quedaría caracterizada por la ecuación

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

Dicho de otra forma, $\mathcal{I}(\phi(k^n)) = \langle x^3 - y^2 \rangle$. Viendo la parametrización original, no debería sorprendernos esta ecuación.

Veamos un ejemplo en el que la implicitación no se ve inmediata de la parametrización:

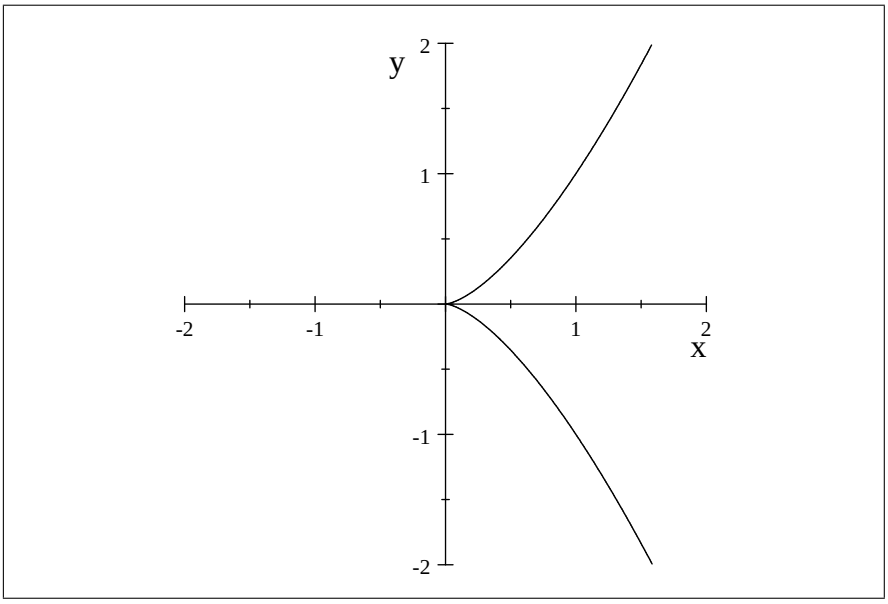

Figura 4.1: Gráfica del Ejemplo 50

Ejemplo 51 *Sea* $\phi : k^2 \to k^3$ *dada por* $\phi(t,u) = (ut, 1-u, u+t-ut)$. *Entonces consideramos el ideal* $I = \langle x - tu, y - 1 + u, z - u - t + tu\rangle \subseteq k[t,u,x,y,z]$. *La base de Gröbner con orden* $lex(t > u > x > y > z)$ *es:*

$$G = \{t - x - y - z + 1, y - 1 + u, xy + yz + y^2 - 2y - z + 1\}$$

La última ecuación implícita es la buscada:

$$xy + yz + y^2 - 2y - z + 1 = 0$$

Como se mencionó al inicio de la sección, la implicitación está definiendo a la cerradura de Zariski $\overline{\phi(k^n)}^Z$, por lo que pueden existir puntos que cumplan las ecuaciones implícitas pero que no pertenezcan a la imagen de ϕ. Cerramos la sección con un ejemplo de lo anterior, aún cuando k es algebraicamente cerrado:

Ejemplo 52 *Sea* $\phi : \mathbb{C}^2 \to \mathbb{C}^3$ *dada por* $\phi(s,t) = (s^2, st, st)$ *Entonces la imagen queda definida por:*

$$\begin{aligned}
\phi(\mathbb{C}^2) &= \{(x,y,z) \in \mathbb{C}^3 | y = z \ y \ x = 0 \Rightarrow y = 0\} \\
&= (\mathcal{V}(y-z) \backslash \mathcal{V}(x, y-z)) \cup \{(0,0,0)\} \\
&= (\mathcal{V}(y-z) \backslash \mathcal{V}(x, y-z)) \cup \mathcal{V}(x,y,z)
\end{aligned}$$

Pero (y como se puede comprobar por el método de Implicitación)

$$\overline{\phi(\mathbb{C}^2)}^Z = \mathcal{V}(y-z)$$

Así, por ejemplo $(0,1,1) \in \overline{\phi(\mathbb{C}^2)}^Z$ *pero* $(0,1,1) \notin \phi(\mathbb{C}^2)$.

Esta aplicación de bases de Gröbner para la implicitación puede llevarse incluso al caso en que las funciones que parametrizan no son necesariamente polinomiales, sino racionales. Al lector interesado en seguir esta línea de aplicación, se recomienda revisar [4].

4.6. Problema del Polinomio Mínimo

Mediante las mismas líneas, las bases de Gröbner tienen aplicación a la teoría de extensiones algebraicas de campos. Si K es extensión de k y se toma $\alpha \in k$ algebraico sobre k, existe $p \in k[x]$ conocido como polinomio mínimo de α, que es mónico y de grado mínimo que satisface $p(\alpha) = 0$.La conexión con los mapeos polinomiales o homomorfismos de k-álgebras que hemos estudiado es considerar

$$\phi : k[x] \longrightarrow k(\alpha)$$

dado por $\phi(x) = \alpha$. Entonces $\ker \phi = \langle p \rangle$ y de hecho

$$\frac{k[x]}{\langle p \rangle} \cong k(\alpha)$$

Planteamos entonces el

Problema 17 *Sea $K = k(\alpha)$ extensión donde α algebraico sobre k con polinomio mínimo p y sea $\beta \in K$ cualquier elemento de la extensión. Encontrar el polinomio mínimo de β.*

Necesitamos primero generalizar el Teorema 18 cuando tenemos un anillo cociente:

Teorema 24 *"Sea $I \subseteq k[x_1, x_2, ..., x_n]$ ideal y $\phi : k[y_1, y_2, ..., y_m] \longrightarrow \frac{k[x_1,x_2,...,x_n]}{I}$ homomorfismo tal que $\phi(y_i) = \overline{f_i}$ y sea*

$$\widetilde{I} = \langle y_1 - f_1, y_2 - f_2, ..., y_n - f_n \rangle + \langle I \rangle \subseteq k[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$$

entonces $\ker \phi = \widetilde{I} \cap k[x_1, x_2, ..., x_m]$*"*

Demostración. Se puede seguir la demostración del Teorema 18 pero recordando que ahora $\phi(y_i) = \overline{f_i}$ y por tanto ahora $\phi(g) = g(\overline{f_1}, \overline{f_2}, ..., \overline{f_m})$. También, en la contención $\subseteq$), que $g \in \ker \phi$ significa ahora que

$$\overline{0} = g(\overline{f_1}, \overline{f_2}, ..., \overline{f_m})$$

por lo que $g(f_1, f_2, ..., f_m) \in I$ y de ahí que

$$g \in \langle y_1 - f_1, y_2 - f_2, ..., y_n - f_n \rangle + \langle I \rangle = \widetilde{I}.$$

■

Y ahora presentamos el Teorema que nos indicará la solución al problema planteado:

Teorema 25 *"Sea $K = k(\alpha)$ extensión donde α algebraico sobre k con polinomio mínimo $p \in k[x]$ y sea $\beta \in K - \{0\}$ dado por*

$$\beta = \frac{f(\alpha)}{g(\alpha)} = \frac{a_0 + a_1\alpha + ... + a_n\alpha^n}{b_0 + b_1\alpha + ... + b_n\alpha^m}$$

con $f(y), g(y) \in k[y]$. Si $\widetilde{I} = \langle p, gy - f \rangle \subseteq k[x, y]$, entonces el polinomio mínimo de β sobre k es el polinomio mónico que genera a $\widetilde{I} \cap k[y]$"

Demostración. Como $g(\alpha) \neq 0$ y $g(\alpha) \in k(\alpha)$ campo, existe su inverso $l(\alpha) \in k(\alpha)$ tal que $g \cdot l = 1 \in k(\alpha) \cong \frac{k[x]}{\langle p \rangle}$, es decir, $gl - 1 \in \langle p \rangle$ ($\overline{gl} = \overline{1}$). Consideramos $h = fl \in k[x]$ y entonces

$$h(\alpha) = f(\alpha)l(\alpha) = \frac{f(\alpha)}{g(\alpha)} = \beta$$

Definimos entonces el homomorfismo $\phi : k[y] \longrightarrow \frac{k[x]}{\langle p \rangle}$ dado por $\phi(y) = \overline{h}$. Afirmamos que $\ker \phi = \langle q \rangle$ donde q es el polinomio mínimo de β. En efecto, un polinomio $r(y) \in \ker \phi$ si y sólo si $\phi(r) = r(\overline{h}) = \overline{0}$, es decir, $r(h) \in \langle p \rangle$ y esto sucede si y sólo si $r(h(\alpha)) = p(\alpha) = 0$, es decir, $r(\beta) = 0$. Notar que en efecto $\widetilde{I} \cap k[y]$ es principal pues $k[y]$ es un D.I.P. Por el Teorema anterior, tenemos entonces que

$$\ker \phi = \langle y - h \rangle + \langle p \rangle = \langle p, y - h \rangle$$

Sólo resta probar que $\widetilde{I} = \langle p, y - h \rangle$, es decir, $\langle p, gy - f \rangle = \langle p, y - h \rangle$, y habremos terminado.
$\subseteq$)Dado que $\overline{gl} = \overline{1}$, entonces $\overline{gfl} = \overline{f}$ y así:

$$\overline{gy - f} = \overline{gy} - \overline{f} = \overline{gy} - \overline{gfl} = \overline{g(y - fl)} = \overline{g(y - h)}$$

por lo que $(gy-f)-g(y-h)\in\langle p\rangle$, es decir, $gy-f\in\langle p, y-h\rangle$
$\supseteq$) Dado que $\overline{gl}=\overline{1}$, entonces $\overline{gly}=\overline{y}$ y así:

$$\overline{y-h}=\overline{y}-\overline{fl}=\overline{lgy}-\overline{lf}=\overline{l(gy-f)}$$

por lo que $(y-h)-l(gy-f)\in\langle p\rangle$, es decir, $y-h\in\langle p, gy-f\rangle$ ■

Así, basta encontrar el polinomio generador del ideal de eliminación $\widetilde{I}\cap k[y]$, cosa que ya sabemos hacer con bases de Gröbner. Podemos enunciar entonces la

Solución 17 *Si $\beta=\frac{f(\alpha)}{g(\alpha)}\in k(\alpha)$ entonces calcular una base de Gröbner del ideal $\widetilde{I}=\langle p, gy-f\rangle\subseteq k[x,y]$ con orden $lex(x>y)$, el polinomio en G que contenga solamente la variable y es el polinomio mínimo de β buscado.*

Ejemplo 53 *Sea α una raíz del polinomio irreducible $x^3-x-1\in\mathbb{Q}[x]$, y sea $\beta=\dfrac{\alpha^2+\alpha}{\alpha+3}$. Encontramos con el método anterior el polinomio mínimo de β. Reconocemos $f(x)=x^2+x$ y $g(x)=x+3$ y entonces*

$$\widetilde{I}=\left\langle x^3-x-1,(x+3)y-(x^2+x)\right\rangle\subseteq\mathbb{Q}[x,y]$$

que tiene como base de Gröbner con $lex(x>y)$ a

$$G=\{5x-150y^2+61y+26, 25y^3-6y^2-7y-1\}$$

así que $q(y)=y^3-\frac{6}{25}y^2-\frac{7}{25}y-\frac{1}{25}$ es el polinomio mínimo buscado.

El problema puede presentarse como una variante en la que a veces no se tiene explícitamente la extensión $\mathbb{Q}(\alpha)$ y uno debe proponerla. A continuación un par de ejemplos de esto:

Ejemplo 54 *Queremos calcular el polinomio mínimo de $\dfrac{\sqrt{2}+7}{\sqrt[4]{2}+1}$ sobre $\mathbb{Q}$. Para resolver este problema escogemos una extensión algebraica conveniente, a saber $\mathbb{Q}(\alpha)$ con $\alpha=\sqrt[4]{2}$. Entonces $p=x^4-2$ y $f=x^2+7$, $g=x+1$. Tomamos pues*

$$\widetilde{I}=\left\langle x^4-2,(x+1)y-(x^2+7)\right\rangle\subseteq\mathbb{Q}[x,y]$$

que tiene base de Gröbner con lex a

$$\begin{aligned}G &= \{127887x-520y^3-19472y^2-149793y-410639,\\ &\quad y^4+36y^3-346y^2+1316-2209\}\end{aligned}$$

por lo que el polinomio mínimo buscado es justamente $y^4+36y^3-346y^2+1316-2209$.

Ejemplo 55 *Queremos calcular el polinomio mínimo de* $\sqrt{2}+\sqrt[3]{2}+5$ *sobre* $\mathbb{Q}$. *Entonces escogemos una extensión conveniente, a saber* $\mathbb{Q}(\alpha)$ *con* $\alpha=\sqrt[6]{2}$. *De esta forma* $p=x^6-2$, $\beta=\alpha^3+\alpha^2+5$ *y ya podemos considerar*

$$\widetilde{I}=\left\langle x^6-2, y-(x^3+x^2+5)\right\rangle \subseteq \mathbb{Q}[x,y]$$

que tiene como base de Gröbner (lex) a

$$\begin{aligned} G &= \{310x-16y^5+394y^4-3825y^3+18379y^2-43913y+42311, \\ &\quad y^6-30y^5+396y^4-2384y^3+8547y^2-16194y+12791\} \end{aligned}$$

siendo el segundo el polinomio mínimo buscado.

Esta aplicación de bases de Gröbner para la determinación de polinomios mínimos se puede extender al caso de extensiones algebraicas $k(a_1,\alpha_2,...,\alpha_n)$ e incluso decidir si dado α en tal extensión, es o no elemento primitivo en el sentido de que $k(a_1,\alpha_2,...,\alpha_n)=k(\alpha)$. Al lector interesado en continuar esta línea de aplicación se le sugiere revisar [1].

Conclusión

A lo largo de estas páginas se ha presentado el concepto de Base de Gröbner y una variedad de aplicaciones a partir de tal. Espero que el lector haya quedado convencido de la trascendencia y utilidad para resolver una considerable cantidad de problemas que surgen en el Álgebra Conmutativa y la Geometría Algebraica. Naturalmente, estas técnicas repercuten en otras áreas de las Matemáticas por conexiones tan simples como lo es un sistema de ecuaciones polinomiales.

Quiero mencionar al menos otras tres áreas en las que las bases de Gröbner han tenido aplicaciones. En Teoría de Gráficas, se pueden utilizar para resolver el problema de los $3-$colores, es decir, determinar si una gráfica dada es o no $3-$coloreable. En Optimización, se pueden utilizar para resolver problemas de Programación Entera. En ambos casos se utiliza una traducción ingeniosa al lenguaje algebraico, en el que se resuelve el problema, y luego se traduce de vuelta al contexto original. Estas dos aplicaciones se pueden revisar en [1].

Otra mención especial de aplicación en otra rama es en Estadística, pues las bases de Gröbner dieron pie a todo un nuevo campo conocido como Estadística Algebraica. En 1998, se descubrió una conexión inesperada entre el problema de muestrear con métodos MCMC (Markov-Chain Monte Carlo) de distribuciones condicionales discretas y el Álgebra Conmutativa mediante el concepto de Base de Markov. Este tipo de aplicación tiene consecuencias muy importantes para esta área, pues justamente las bases de Markov empiezan justificándose teóricamente y obteniéndose a partir de las Bases de Gröbner. Así, se tienen herramientas para resolver problemas de pruebas de hipótesis que surgen en Estadística Inferencial. Al lector interesado en esta tercera rama se le sugiere revisar el artículo original de Diaconis y Sturmfels, [6], así como los subsecuentes desarrollos en [14], [13] y [7]. (de hecho, el autor confiesa que es a partir del comienzo de estudio de esta área por las que conoció las bases de Gröbner).

El concepto de base de Gröbner se ha generalizado para que se aplique en módulos y en anillos más generales que los de polinomios. La teoría sigue desarrollándose

y cada vez surgen más algoritmos para calcular o resolver en la práctica muchos problemas teóricos. Por ejemplo, encontrar explícitamente el ideal radical de un ideal dado, o encontrar descomposiciones primarias de ideales. Así, la teoría y práctica de las bases de Gröbner sigue avanzando y permeando diferentes áreas. En los últimos años se está aplicando también a Teoría de Códigos y Criptografía.

Me atrevo a concluir que las bases de Gröbner son un concepto revolucionario dentro de las Matemáticas, fortaleciendo las a veces subestimadas conexiones entre la teoría y la práctica.

Apéndice A

Diccionario Álgebra-Geometría

Este diccionario da la correspondencia biyectiva entre ideales y radicales tomando en cuenta operaciones entre ellos, así como se presenta en [4]. Se supone que k es algebraicamente cerrado y todos los ideales son radicales. Se usa notación que hemos estado trabajando, como $\overline{()}^Z$ para cerradura de Zariski y I_j para el j-ésimo ideal de eliminación. C.A.E. abrevia cadenas ascendentes estacionarias y C.D.E. abrevia cadenas descendentes estacionarias.

ÁLGEBRA	$\overset{\mathcal{V}}{\underset{\mathcal{I}}{\leftrightarrow}}$	GEOMETRÍA
ideales radicales	$\leftrightarrow$	variedades
I	$\rightarrow$	$\mathcal{V}(I)$
$\mathcal{I}(V)$	$\leftarrow$	V
$I + J$	$\rightarrow$	$\mathcal{V}(I) \cap \mathcal{V}(J)$
$\sqrt{\mathcal{I}(V) + \mathcal{I}(W)}$	$\leftarrow$	$V \cap W$
IJ	$\rightarrow$	$\mathcal{V}(I) \cup \mathcal{V}(J)$
$\sqrt{\mathcal{I}(V)\mathcal{I}(W)}$	$\leftarrow$	$V \cup W$
$I \cap J$	$\rightarrow$	$\mathcal{V}(I) \cup \mathcal{V}(J)$
$\mathcal{I}(V) \cap \mathcal{I}(W)$	$\leftarrow$	$V \cup W$
$I : J$	$\rightarrow$	$\overline{\mathcal{V}(I) \cup \mathcal{V}(J)}^Z$
$\mathcal{I}(V) : \mathcal{I}(W)$	$\leftarrow$	$\overline{V - W}^Z$
$\sqrt{I_j}$	$\rightarrow$	$\overline{\pi_j(\mathcal{V}(I))}^Z$
ideal primo	$\leftrightarrow$	var. irreducible
ideal maximal	$\leftrightarrow$	punto
C.A.E.	$\leftrightarrow$	C.D.E.

Apéndice B

Código en MAPLE

Se presentan varios ejemplos de instrucciones en MAPLE para algunos cálculos mencionados a través del trabajo. Cargar el paquete correspondiente *Groebner*.

- Ejemplo de cálculo de término líder[1] (ejemplo 12, pág. 12):

  $f := 4 * x * y\hat{}2 * z + 4 * z\hat{}2 - 5 * x\hat{}3 + 7 * x\hat{}2 * z\hat{}2$
  $LeadingTerm(f, plex(x, y, z))$

  $$-5, x\hat{}3$$

  $LeadingTerm(f, grlex(x, y, z))$

  $$7, x\hat{}2 * z\hat{}2$$

  $LeadingTerm(f, tdeg(x, y, z))$

  $$4, x * y\hat{}2 * z$$

- Ejemplo de cálculo de Base de Gröbner (ejemplo 27, pág. 27):

  $F := [x\hat{}2*y+x*y\hat{}2-2*y, x\hat{}2+x*y-x+y\hat{}2-2*y, x*y\hat{}2-x-y+y\hat{}3]$
  $Basis(F, plex(x, y))$

  $$[y\hat{}2 - y, x - y]$$

[1] Los órdenes monomiales se especifican de la siguiente manera: lex como *plex*, grlex se denota igual y grevlex como *tdeg*; y entre paréntesis el orden de las variables.

- Ejemplo de cálculo de residuo/forma normal (ejemplo 28, pág. 45):

  $F := [x * z - y\hat{}2, x\hat{}3 - z\hat{}2]$
  $G := Basis(F, grlex(x, y, z))$

  $$G := [x * z - y\hat{}2, x\hat{}3 - z\hat{}2, x\hat{}2 * y\hat{}2 - z\hat{}3, x * y\hat{}4 - z\hat{}4, y\hat{}6 - z\hat{}5]$$

  $NormalForm(-4 * x\hat{}2 * y\hat{}2 * z\hat{}2 + y\hat{}6 + 3 * z\hat{}5, G, grlex(x, y, z))$

  $$0$$

  $NormalForm(x\hat{}7 * y\hat{}2 + 2 * z\hat{}2 - x * y\hat{}2 * z\hat{}3, G, grlex(x, y, z))$

  $$2 * z\hat{}2 - y\hat{}4 * z\hat{}2 + y\hat{}4 * z\hat{}3$$

- Ejemplo de cálculo de cociente de ideales $I : J$ (ejemplo 38, pág. 59):

$Basis(\{x - t * x, t * x\hat{}3 - t * y * z, t * x * z - t * y\hat{}2\}, plex(t, x, y, z))$

$$[y\hat{}5 * x - z\hat{}4 * x, z * x\hat{}2 - y\hat{}2 * x, y\hat{}3 * x\hat{}2 - z\hat{}3 * x, y * x\hat{}3 - z\hat{}2 * x,$$
$$x\hat{}4 - z * y * x, t * y * z - x\hat{}3, t * y\hat{}2 - x * z, -x + t * x]$$

$Basis(\{y - t * y, t * x\hat{}3 - t * y * z, t * x * z - t * y\hat{}2\}, plex(t, x, y, z))$

$$[y\hat{}6 - z\hat{}4 * y, z * y * x - y\hat{}3, y\hat{}4 * x - z\hat{}3 * y, y\hat{}2 * x\hat{}2 - z\hat{}2 * y$$
$$, y * x\hat{}3 - y\hat{}2 * z, -y + t * y, t * x * z - y\hat{}2, t * x\hat{}3 - y * z]$$

- Ejemplo de cálculo de polinomio mínimo (ejemplo 54, pág. 89):

  $Basis(\{x\hat{}4 - 2, (x + 1) * y - x\hat{}2 - 7\}, plex(x, y))$

  $$[-2209 + 1316 * y - 346 * y\hat{}2 + 36 * y\hat{}3 + y\hat{}4,$$
  $$-410639 + 149793 * y - 19472 * y\hat{}2 - 520 * y\hat{}3 + 127887 * x]$$

  $eval(-2209+1316*y-346*y\hat{}2+36*y\hat{}3+y\hat{}4, y = (sqrt(2)+7)/(2\hat{}(1/4)+1))$

  $$-2209 + (1316 * (sqrt(2) + 7))/(2\hat{}(1/4) + 1) - 346 *$$
  $$(sqrt(2) + 7)\hat{}2/(2\hat{}(1/4) + 1)\hat{}2 + 36 * (sqrt(2) + 7)\hat{}3/(2\hat{}(1/4) + 1)\hat{}3$$
  $$+(sqrt(2) + 7)\hat{}4/(2\hat{}(1/4) + 1)\hat{}4$$

  $simplify(\%)$

  $$0$$

Bibliografía

[1] W. Adams, P. Loustaunau. *An Introduction to Gröbner Bases.* AMS Press, Providence, RI, 1994.

[2] T. Becker, H. Kredel, V. Weispfenning. *Gröbner bases: a computational approach to commutative algebra.* Springer, 1993.

[3] N. Bourbaki, *Algebra I.* Elements of Mathematics. Springer, 1988.

[4] D. Cox, J. Little, D. O'Shea. *Ideals, Varietes, and Algorithms*. Undergraduate Text in Mathematics. Springer-Verlag, New York,1996.

[5] D. Cox, J. Little, D. O'Shea. *Using Algebraic Geometry.* Graduate Texts in Mathematics 185. Springer-Verlag, New York,1998.

[6] P. Diaconis, B. Sturmfels. *Algebraic Algorithms for sampling from conditional distributions*. Annals of Statistics. 26.no.1 (363-397),1998.

[7] M. Drton, B. Sturmfels, S. Sullivant. *Lectures on Algebraic Statistics*. Springer, 2008.

[8] V. Ene, J. Herzog. *Gröbner Bases in Commutative Algebra.* Graduate Studies in Mathematics 130. AMS Press, Providence, RI, 2012.

[9] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry.* Graduate Texts in Mathematics 150. Springer, 1995.

[10] W. Fulton. *Algebraic Curves: an introduction to Algebraic Geometry*, Addison-Wesley, 1989.

[11] S. Lang. *Algebra* . Addison-Wesley, 1974.

[12] N. Lauritzen. *Concrete Abstract Algebra: From Numbers to Gröbner Bases*. Cambridge University Press, Cambridge, 2003.

[13] L. Pachter, B. Sturmfels. *Algebraic Statistics for Computational Biology.* Cambridge University Press, Cambridge, 2005.

[14] G. Pistone, E. Riccomagno, H. Wynn. *Algebraic Statistics.* CRC Press, Boca Raton, FL, 2001.

[15] B. Sturmfels. *Gröbner Bases and Convex Polytopes.* University Lecture Series 8. AMS Press, Providence, RI, 1996.