UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS
ESCUELA PROFESINAL DE MATEMÁTICAS

"BASES DE GRÖBNER CON APLICACIONES AL ALGEBRA CONMUTATIVA"

Presentado por:

GUSTAVO MARCA CASTROMONTE

Tesis

Para Optar el Título Profesional de:

LICENCIADO EN MATEMÁTICA

Mag. Mario Santiago Saldaña
Asesor

LIMA – PERÚ
2008

DEDICATORIA

A aquel que fundó la tierra y ordeno sus medidas, aquel que dijo sea la Luz y fue la Luz, a aquel Dios que fortaleció a Abraham, Isaac, Jacob, José cuando fue vendido, moisés, David, Salomón y a cada uno de aquellos que confían en él, al Dios que se hizo hombre y habito entre nosotros, en el mundo estaba y el mundo por él fue hecho, pero el mundo no le conoció.

A aquel que dijo:...destruid este templo y en tres días lo levantaré...el que no naciere de nuevo, no puede ver el reino de Dios...ve, tu hijo vive...levántate toma tu lecho y anda...hijas de Jerusalén no lloréis por mí, sino llorad por vosotras miasmas y por vuestros hijos.

Este trabajo y todo lo que hay en él es para el Dios de las escrituras y para el señor Jesucristo el cual es nuestra esperanza y amamos su pronta venida.

AGRADECIMIENTOS

Gracias doy a mis padres y a mi familia por su paciencia, ayuda y dedicación, que el Señor bendiga sus vidas en abundancia y que estemos juntos en la esperanza y en las cosas que no se ven.

Quiero expresar mi más sincero agradecimiento a las personas que de forma directa o indirecta me han ayudado a la realización de esta tesis con sus conocimientos en el tema o con su apoyo moral.

Gracias al Dr. Carlos Chávez por su valiosa ayuda y recomendaciones.

Gracias al profesor Félix Villanueva por su didáctica y método en la enseñanza de las matemáticas las cuales es estimulante escuchalas.

Gracias al profesor Mg. Mario Saldaña por su tiempo y muchas recomendaciones para el presente trabajo.

Este trabajo esta pensado en aquella persona que las escrituras dice bebe el agua de tu misma cisterna y de tu propio pozo y vuelve a decir alégrate con la mujer de tu juventud, para mariela arenas horna por su amor y gracia de mujer y por el mismo sentir en aquel que provee de amor y fidelidad en todas las cosas.

Adquiere sabiduría,
Adquiere inteligencia;
No te olvides ni te apartes
de las razones de mi boca;
No la dejes y ella te guardará;
Amala y te conservará.
Prov.4.5

Indice general

Lista de Algoritmos

Capítulo 1

Introducción

1.1. Conceptos básicos

Definición 1.1.1 *Monomio*

Un monomio en las indeterminadas $x_1, \ldots, x_n$ es un producto de la forma

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

donde $\alpha_1, \ldots, \alpha_n$ son enteros no negativos.

El grado total de este monomio viene dado por la suma

$$\alpha_1 + \alpha_2 + \ldots + \alpha_n$$

Podemos simplificar la notación del modo siguiente.

Sea $\alpha = (\alpha_1, \ldots, \alpha_n)$ n-upla de enteros no negativos. Esto es

$$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}_{\geq 0}^n$$

Denotamos

$$x^\alpha = x_1^{\alpha_1} . x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

Cuando $\alpha = (0, 0, \ldots, 0)$ por convención escribimos $x^\alpha = 1$.

Igualmente

$$|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n$$

denotará el grado total del monomio x^α

Definición 1.1.2 *Combinación lineal finita de monomios*

Un polinomio f en $x_1, \ldots, x_n$ con coeficiente en el cuerpo $\mathbb{K}$, es una combinación lineal finita de monomios. Con la notación establecida un polinomio f se expresa como:

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad a_\alpha \in \mathbf{K}$$

donde la suma indicada está dada por un número finito de n-uplas $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$

El conjunto que agrupa a todos los polinomios en las indeterminadas $x_1, \ldots, x_n$ con coeficientes en $\mathbf{K}$ lo denotamos por:

$$\mathbf{K}[x_1, x_2, \ldots, x_n]$$

Definición 1.1.3

Sea $f = \sum_{\alpha} a_\alpha x^\alpha$ un polinomio en $\mathbf{K}[x_1, x_2, \ldots, x_n]$

(i) a_α será el coeficiente del monomio x^α

(ii) Siempre que $a_\alpha \neq 0$, $a_\alpha x^\alpha$ le llamaremos un término de f

(iii) El grado de f, denotado por $grad(f)$, viene dado por el máximo $|\alpha|$ para el cual el coeficiente a_α es no nulo.

Ejemplo 1.1.1

$$f(x, y, z) = 3xy^2z^3 + \frac{5}{3}y^4z - 2xy^5$$

es un polinomio de grado seis y posee tres términos.

Se muestra que bajo la adición y multiplicación en $\mathbf{K}[x_1, x_2, \ldots, x_n]$ se satisface todos todos los axiomas de cuerpo, excepto la existencia del inverso multiplicativo.

Luego $\mathbf{K}[x_1, x_2, \ldots, x_n]$ es un anillo conmutativo, al cual denominamos anillo de polinomios.

Definición 1.1.4

Dado un campo $\mathbf{K}$ y un entero positivo n, definimos al espacio afin n-dimensional sobre $\mathbf{K}$, como el conjunto.

$$\mathbf{K}^n = \{(a_1, a_2, \ldots, a_n) : a_1, a_2, \ldots, a_n \in \mathbf{K}\}$$

$f = \sum_{\alpha} a_\alpha x^\alpha \in \mathbf{K}[x_1, x_2, \ldots, x_n]$ puede ser visto como una función polinomial

$$f : \mathbf{K}^n \to \mathbf{K}$$

como sigue: $(a_1, a_2, \ldots, a_n) \longrightarrow f(a_1, a_2, \ldots, a_n)$. Note que una función polinomial f puede ser nula y sin embargo f no ser el polinomio cero.

Para ello veamos que el polinomio

$$f = x^2 - x = x(x-1)$$

es no nulo. Pero vista como función $f : \mathbf{Z}_2 \longrightarrow \mathbf{Z}_2$ es nula.

Esto es debido a que el campo es finito, la proposición que sigue aclara esta característica.

Proposición 1.1.1

Sea $\mathbf{K}$ un campo infinito y $f \in \mathbf{K}[x_1, x_2, \ldots, x_n]$. entonces $f = 0$ en $\mathbf{K}[x_1, x_2, \ldots, x_n]$ si y solo si $f : \mathbf{K}^n \to \mathbf{K}$ es función nula.

Demostración

Si se tiene que el polinomio es nulo $f = 0$, todos sus coeficientes son ceros, por lo tanto la función obtenida debe ser nula.

En otro sentido, usaremos inducción sobre el numero de variables n.

Cuando $n = 1$ es conocido que un polinomio no nulo en $\mathbf{K}[x]$ de grado m, tiene a lo más m raíces distintas (probaremos este hecho en el corolario (1.4.1)).

Para nuestro caso $f \in \mathbf{K}[x]$ y asumamos que $f(a) = 0$, $\forall a \in \mathbf{K}$ desde que $\mathbf{K}$ es infinito, hace que f tenga infinitas raíces. Luego debe ser que f es el polinomio nulo.

Asumamos que se verifica para $n-1$ y sea $f \in \mathbf{K}[x_1, x_2, \ldots, x_n]$ un polinomio que se anula para todos los puntos de $\mathbf{K}^n$.

Consideremos f en la forma

$$f = \sum_{i=1}^{N} g_i(x_1, x_2, \ldots, x_{n-1}) x_n^i, \quad \text{donde} \quad g_i \in \mathbf{K}[x_1, x_2, \ldots, x_{n-1}]$$

Se mostrará que cada g_i es el polinomio nulo en $n-1$ variables, con lo cual se tendría que f es el polinomio nulo en $\mathbf{K}[x_1, x_2, \ldots, x_n]$.

Si fijamos $(a_1, a_2, \ldots, a_{n-1}) \in \mathbf{K}^{n-1}$, obtenemos el polinomio

$$f(a_1, a_2, \ldots, a_{n-1}, x_n) \in \mathbf{K}[x_n]$$

Por nuestra hipótesis en f, este es nulo para cada $a_n \in \mathbf{K}$, luego por hipótesis inductiva, se tiene que $f(a_1, a_2, \ldots, a_{n-1}, x_n)$ es el polinomio nulo en $\mathbf{K}[X_n]$.

Como los coeficientes de

$$f(a_1, a_2, \ldots, a_{n-1}, x_n)$$

son $g_i(a_1, a_2, \ldots, a_{n-1})$, se tiene $g_i(a_1, a_2, \ldots, a_{n-1}) = 0, \ \forall i$.

Desde que $(a_1, a_2, \ldots, a_{n-1})$ se escogió arbitrariamente en $\mathbf{K}^{n-1}$ sigue que cada

$$g_i \in \mathbf{K}[x_1, x_2, \ldots, x_{n-1}]$$

es la función nula en $\mathbf{K}^{n-1}$ luego por nuestra hipótesis inductiva, se obtiene que cada g_i es el polinomio nulo en $\mathbf{K}[x_1, x_2, \ldots, x_{n-1}]$.

Concluyendo que f es el polinomio nulo de $\mathbf{K}[x_1, x_2, \ldots, x_n]$. □

Como corolario, veremos que dos polinomios son iguales cuando representan la misma función en el espacio afin.

Corolario 1.1.1

Sea $\mathbf{K}$ un campo infinito y $f, g \in \mathbf{K}[x_1, \ldots, x_n]$ dos polinomios. entonces $f = g$ en $\mathbf{K}[x_1, \ldots, x_n]$ si y solo si $f : \mathbf{K}^n \longrightarrow \mathbf{K}$ y $g : \mathbf{K}^n \longrightarrow \mathbf{K}$ son las mismas funciones (esto es $f(x) = g(x), \ \forall x \in \mathbf{K}^n$)

Demostración

Si f y g son los mismos polinomios en $K[x_1, x_2, \ldots, x_n]$, es claro que son iguales como funciones.

En el otro sentido, si $f, g \in \mathbf{K}[x_1, \ldots, x_n]$ representan la misma función en $\mathbf{K}^n$, luego $f - g$ es la función nula, por lo tanto como el campo $\mathbf{K}$ es infinito, $f - g$ es el polinomio nulo. Esto demuestra que $f = g$ en $\mathbf{K}[x_1, \ldots, x_n]$. $\square$

Diremos que un campo $\mathbf{K}$ es algebraicamente cerrado si cada polinomio no constante en $\mathbf{K}[x]$ tiene un raíz en $\mathbf{K}$.

De este modo $\mathbf{R}$ no es algebraicamente cerrado ($x^2 + 1$ es un polinomio en $\mathbf{R}[x]$ cuyas raíces no están en $\mathbf{R}$).

$\mathbf{C}$ es un campo algebraico cerrado debido a que cada polinomio no constante $f \in \mathbf{C}[x]$ tiene una ráiz en $\mathbf{C}$ [7, pag. 443]

1.2. Variedad afín

Definición 1.2.1

Sea $\mathbf{K}$ un campo, $f_1, \ldots, f_s$ polinomios en $\mathbf{K}[x_1, \ldots, x_n]$ el conjunto

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbf{K}^n : f_i(a_1, \ldots, a_n) = 0, \ \forall i = 1, 2, \ldots, s\}$$

será llamado la variedad afín definida por $f_1, \ldots, f_s$.

De este modo una variedad afín $V(f_1, \ldots, f_s) \subset \mathbf{K}^n$ es el conjunto de todas las soluciones del sistema de ecuaciones:

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

Usaremos las letras V, W etc, para denotar a las variedades afines.

$V(x^2 + y^2 - 1) \subset \mathbf{R}^2$ es una variedad la cual es una circunferencia de radio 1 y centrado en el origen.

Las secciones cónicas estudiadas en geometría analítica: circunferencias, elipses, parábolas, hipérbolas son variedades afines.

También los grafos de funciones polinomiales son variedades afines: si $y = f(x)$, $V(y - f(x)) \subset \mathbf{R}^2$.

Los gráficos de funciones racionales son igualmente variedades afines. Asi

$$y = \frac{x^3 - 1}{x}, \quad V(xy - x^3 + 1)$$

$V(xz, yz) \subset \mathbf{R}^3$ es una variedad afín definida por la unión del plano XY y el eje Z.

Del algebra lineal, consideremos un sistema de m ecuaciones lineales en n variables: $x_1, x_2, \ldots, x_n$ con coeficientes en $\mathbf{K}$.

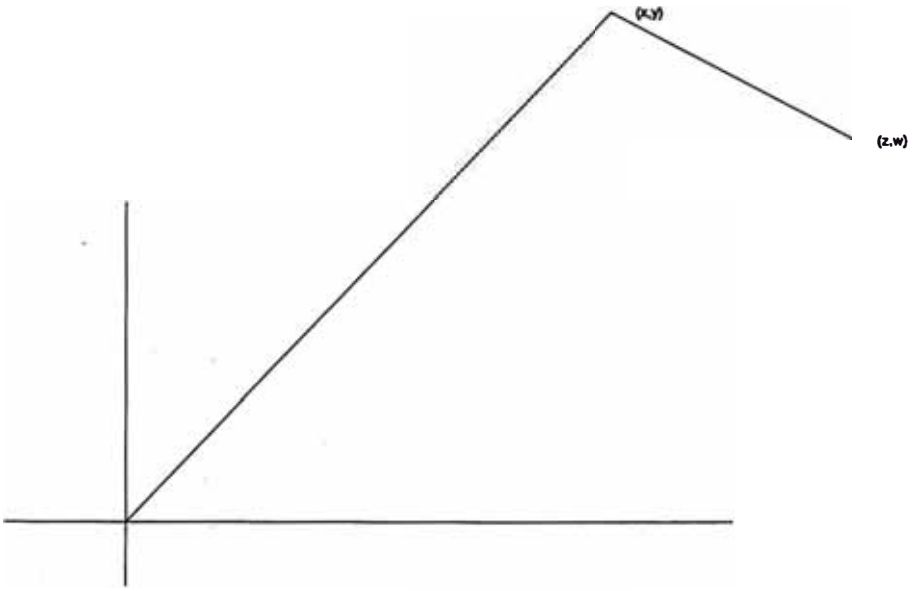
$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

Las soluciones de estas ecuaciones forman una variedad afín en $\mathbf{K}^n$, la cual será llamada variedad lineal.

Las variedades afines también pueden ser conjuntos vacíos, por ejemplo sobre $\mathbf{R}$, $V(x^2 + y^2 + 2) = \emptyset$.

Por dar una idea de la aplicación de variedades afines a la robótica, consideremos el siguiente ejemplo:

Sea un robot armado en el plano consistente de dos varillas de longitudes 1 y 2 en el cual el mas largo está anclado en el origen.



El estado del robot puede describirse completamente por las coordenadas (x, y) y (z, w) indicado en la figura. De este modo el estado puede quedar completamente definido por $(x, y, z, w) \in \mathbf{R}^4$.

Sin embargo no toda 4-upla puede ser estado del robot, pues el subconjunto posible de estados es una variedad afín en $\mathbf{R}^4$, definida por las ecuaciones

$$x^2 + y^2 = 4$$

$$(x - z)^2 + (y - w)^2 = 1$$

Lema 1.2.1

Si $V, W \subset \mathbf{K}^n$ son variedades afines, entonces $V \cup W$ y $V \cap W$ también lo son.

Demostración

Sean

$$V = V(f_1, f_2, \ldots, f_s)$$

$$W = W(g_1, g_2, \ldots, g_t)$$

Se afirma: $V \cap W = V(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$. En efecto

$(\subset)$ Sea $(a_1, a_2, \ldots, a_n) \in V \cap W$ entonces $(a_1, a_2, \ldots, a_n) \in V$ y $(a_1, a_2, \ldots, a_n) \in W$

De aqui f_i y g_j se anulan en $(a_1, a_2, \ldots, a_n)$ para $i = 1, 2, \ldots, s$, $j = 1, 2, \ldots, t$ por lo tanto $(a_1, a_2, \ldots, a_n) \in V(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$.

($\supset$) La otra inconclusión, si $(a_1, a_2, \ldots, a_n) \in V(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$ luego es directo que $(a_1, a_2, \ldots, a_n) \in V(f_1, f_2, \ldots, f_s)$ y $(a_1, a_2, \ldots, a_n) \in V(g_1, g_2, \ldots, g_t)$.

Por lo tanto

$$(a_1, a_2, \ldots, a_n) \in V \cap W \quad \square$$

Se afirma: $V \cup W = V(f_i g_j : i = 1, 2, \ldots, s; \quad j = 1, 2, \ldots, t)$. En efecto

($\subset$) Sea $(a_1, a_2, \ldots, a_n) \in V \cup W$. Supongamos que exista i y j con $i = 1, 2, \ldots, s$, $j = 1, 2, \ldots, t$ tal que $f_i g_j(a_1, a_2, \ldots, a_n) \neq 0$. Entonces $f_i(a_1, a_2, \ldots, a_n) \neq 0$ y $g_i(a_1, a_2, \ldots, a_n) \neq 0$. Luego $(a_1, a_2, \ldots, a_n) \notin V$ y $(a_1, a_2, \ldots, a_n) \notin W$. De aqui $(a_1, a_2, \ldots, a_n) \notin V \cup W$. Y esto no puede ser.

($\supset$) Con respecto a la otra inclusión.

Sea $(a_1, a_2, \ldots, a_n) \in V(f_i g_j : i = 1, 2, \ldots, s \quad j = 1, 2, \ldots, t)$

Supongamos que $(a_1, a_2, \ldots, a_n) \notin W$, entonces existe j, $j = 1, 2, \ldots, t$ tal que $g_j(a_1, a_2, \ldots, a_n) \neq 0$.

Como

$$f_i g_j(a_1, a_2, \ldots, a_n) = 0 \text{ para todo } i = 1, 2, \ldots, s \text{ y } g_j(a_1, a_2, \ldots, a_n) \neq 0$$

entonces $f_i(a_1, a_2, \ldots, a_n) = 0$ para todo $i = 1, 2, \ldots, s$.

Luego $(a_1, a_2, \ldots, a_n) \in V$. Asi $(a_1, a_2, \ldots, a_n) \in V \cup W \quad \square$

Este lema implica que las intersecciones finitas y uniones finitas de variedades afines son igualmente variedades afines.

1.3. Ideales

Definición 1.3.1

Un subconjunto $I \subset K[x_1, x_2, \ldots, x_n]$ es un ideal, si satisface

i) $0 \in I$

ii) Si $f, g \in I$, entonces $f + g \in I$

iii) Si $f \in I$ y $h \in K[x_1, x_2, \ldots, x_n]$, entonces $hf \in I$

Definición 1.3.2

Sea $f_1, \ldots, f_s$ polinomios en $K[x_1, x_2, \ldots, x_n]$.

$$\langle f_1, \ldots, f_s \rangle = \{\sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in K[x_1, x_2, \ldots, x_n]\}$$

Lema 1.3.1

Si $f_1, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$ entonces $\langle f_1, \ldots, f_s \rangle$ es un ideal de $K[x_1, x_2, \ldots, x_n]$ al cual le llamaremos ideal generado por $f_1, \ldots, f_s$. □

Diremos que un ideal I es finitamente generado $(f \cdot g)$, si existen

$$f_1, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$$

de tal manera que $I = \langle f_1, \ldots, f_s \rangle$.

En el capítulo 2, probaremos que cada ideal de $K[x_1, x_2, \ldots, x_n]$ es $f.g$ (teorema de la base de hilbert).

En la proposición siguiente se muestra que una variedad depende unicamente de los generadores.

Proposición 1.3.1

Si $f_1, f_2, \ldots, f_s$ y $g_1, g_2, \ldots, g_t$ son generadores de un mismo ideal en $K[x_1, x_2, \ldots, x_n]$, $\langle f_1, f_2, \ldots, f_s \rangle = \langle g_1, g_2, \ldots, g_t \rangle$.

Entonces

$$V(f_1, f_2, \ldots, f_s) = V(g_1, g_2, \ldots, g_t)$$

Demostración:

Basta notar que cada f_i, $i = 1, 2, \ldots, s$, se puede expresar como

$$f_i = \sum_{i=1}^{t} h_i g_i$$

y cada g_i, $i = 1, 2, \ldots, t$ como

$$g_i = \sum_{i=1}^{s} p_i f_i. \quad \square$$

Asi

$$\begin{aligned} V(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) &= V(x^2 - 4, y^2 - 1) \\ &= \{(2,1), (2,-1), (-2,1), (-2,-1)\} \end{aligned}$$

debido a que

$$\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$$

Definición 1.3.3

Sea $V \subset \mathbf{K}^n$ una variedad afin. Entonces el conjunto

$$I(V) = \{f \in K[x_1, x_2, \ldots, x_n] / f(x) = 0, \ \forall x \in V\}$$

le denominamos el ideal de la variedad V.

Lema 1.3.2

Si $V \subset \mathbf{K}^n$ es una variedad afín, entonces $I(V) \subset K[x_1, x_2, \ldots, x_n]$ es un ideal en $K[x_1, x_2, \ldots, x_n]$.

Demostración:

Como $O(x) = 0, \ \forall x \in V$, entonces $0 \in I(V)$.
Sea $f, g \in I(V)$, luego

$$(f + g)(x) = f(x) + g(x) = 0 + 0 = 0, \ \forall x \in V$$

luego $f+g \in I(V)$.

Por último, sean $h \in K[x_1, x_2, \ldots, x_n]$ y $f \in I(V)$ entonces

$$(hf)(x) = h(x)f(x) = h(x) \cdot 0 = 0, \ \forall x \in V$$

De donde

$$hf \in I(V) \quad \square$$

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

También $I(K^n) = \{0\}$, cuando K es infinito.

$$V = V(y - x^2, z - x^3) \subset \mathbf{R}^3 \ \text{ entonces } \ I(V) = \langle y - x^2, z - x^3 \rangle$$

Lema 1.3.3

Si $f_1, f_2, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$ entonces $\langle f_1, f_2, \ldots, f_s \rangle \subset I(V(f_1, f_2, \ldots, f_s))$.

Demostración

Sea $f \in \langle f_1, f_2, \ldots, f_s \rangle$ entonces $f = \sum_{i=1}^{s} h_i f_i$. Para $a \in V(f_1, f_2, \ldots, f_s)$.

$$f_i(a) = 0, \ \forall i = 1, 2, \ldots, s$$

Por lo tanto

$$\begin{aligned} f(a) &= (\sum_{i=1}^{s} h_i f_i)(a) \\ &= \sum_{i=1}^{s} h_i(a) f_i(a) \\ &= 0 \end{aligned}$$

Asi $f \in I(V(f_1, f_2, \ldots, f_s))$, desde que a es arbitarario. $\square$

Como una observación diremos que la igualdad no necesariamente es verdad.

Veamos que $\langle x^2, y^2 \rangle \subsetneq I(V(x^2, y^2))$.

En efecto, $V(x^2, y^2) = \{(0,0)\}$ pero $I(V(x^2, y^2)) = \langle x, y\rangle$. Es claro que $\langle x^2, y^2\rangle \subseteq \langle x, y\rangle$, pero como $x \in \langle x, y\rangle$ y $x \notin \langle x^2, y^2\rangle$, entonces se tiene $\langle x^2, y^2\rangle \subsetneq \langle x, y\rangle$.

En un campo algebraico cerrado, como $\mathbf{C}$, en el lema (1.3.3), se establece la igualdad, como veremos en el capítulo 4, el teorema de Nullstellensatz.

Proposición 1.3.2

Sean V y W variedades afines en $\mathbf{K}^n$ entonces

(i) $V \subset W$ si y solo si $I(V) \supset I(W)$

(ii) $V = W$ si y solo si $I(V) = I(W)$

Prueba

(i) Sabiendo que $V \subset W$ y $f \in I(W)$ entonces $f(a) = 0,\ \forall a \in W$ en particular para todo $a \in V$, luego $f \in I(V)$. Por lo tanto $I(V) \supset I(W)$.

Consideraremos que $I(V) \supset I(W)$ veamos que $V \subset W$.

Sea $a \in V$ y $V = V(f_1, f_2, \ldots, f_s)$, $W = V(g_1, g_2, \ldots, g_t)$

Luego $f_i(a) = 0,\ \forall\, i = 1, 2, \ldots, s$.

Como

$$\langle g_1, g_2, \ldots, g_t\rangle \subset I(V(g_1, g_2, \ldots, g_t)) = I(W)$$

Entonces $g_k \in I(W),\ \forall\, k = 1, 2, \ldots, t$.

Como $I(V) \supset I(W)$. Por lo tanto $g_k(x) = 0,\ \forall x \in V$. Y como $a \in V$, entonces $g_k(a) = 0,\ \forall\, k = 1, 2, \ldots, t$. Asi $a \in W$.

(ii) Es consecuencia de (i) $\square$

1.4. Polinomios en una variable

Definición 1.4.1

Dado un polinomio no nulo $f \in K[x]$. Si

$$f(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m \text{ donde } a_i \in K,\ a_0 \neq 0,$$

diremos que a_0x^m es el término principal de f y lo denotamos por

$$Tp(f) = a_0x^m$$

Proposición 1.4.1 *El algoritmo de la división*

Sea **K** un cuerpo y g un polinomio no nulo en $K[x]$. Entonces para cada $f \in K[x]$ se tiene:

$$f = q \cdot g + r \text{ donde } q, r \in K[x],\ r = 0 \text{ ó } grad(r) < grad(g).$$

Además q y r son únicos y existe un algoritmo para calcularlos.

Prueba

Mostraremos el algoritmo para determinar q y r.

Algoritmo 1 Algoritmo de división en una variable

Entrada: $g,\ f$

Salida: $q,\ r$

$q := 0$

$r := f$

while $r \neq 0$ y $Tp(g)$ divide $Tp(r)$ **do**

$q := q + \frac{Tp(r)}{Tp(g)}$

$r := r - (\frac{Tp(r)}{Tp(g)})g$

end while

Note que $f = qg + r$ se dá para la evaluación inicial de q y r (es decir $q := 0$, $r := f$) y cuando redefinimos q y r la igualdad $f = qg + r$ también es verdadera:

$$(q + \frac{Tp(r)}{Tp(g)})g + (r - (\frac{Tp(r)}{Tp(g)})g) = qg + r = f$$

El bucle, While ... do, termina cuando $r = 0$ o cuando $Tp(g)$ no divide al $Tp(r)$ esto equivale a decir $grad(r) < grad(g)$. De esta manera, si el algoritmo termina, produce q y r con los requerimientos de la proposición.

Ahora veamos que While y do, nos dá un bucle finito. La clave de ver esto es:

Para

$$r = a_0x^m + \cdots + a_m, Tp(r) = a_0x^m$$

$$g = b_0x^k + \cdots + b_k, Tp(g) = b_0x^k$$

Supongamos que $m \geq k$, entonces

$$r := r - (\frac{Tp(r)}{Tp(g)})g = (a_0x^m + \cdots + a_m) - (\frac{a_0}{b_0})x^{m-k}(b_0x^k + \cdots + b_k)$$

se observa en el segundo miembro que $Tp(r)$ se cancela, luego el grado del nuevo r disminuye mientras que el $grad(g)$ permanece fijo. Después de un número finito de pasos el algoritmo termina (ya que $r = 0$ ó $grad(r) < grad(g)$).

Solo falta probar la unicidad de la representación.

Supongamos que $f = qg + r = q'g + r'$ donde r y r' cumplan con las condiciones de la proposición.

Note que $grad(r' - r) < grad(g)$ y supongamos que $r \neq r'$. Por otro lado

$$(q - q')g = r' - r$$

y $q - q' \neq 0$, ya que si fuesen iguales, $r = r'$

Tenemos

$$\begin{aligned} grad(r - r') &= grad((q - q')g) \\ &= grad(q - q') + grad(g) \\ &\geq grad(g) \end{aligned}$$

y esto no se puede dar. Luego $r = r'$ y por lo tanto $q = q'$ □

Una utilidad de este algoritmo, concierne al número de raíces de un polinomio en una variable sobre un campo.

Corolario 1.4.1

Sea $\mathbf{K}$ un campo y $f \in K[x]$ un polinomio no nulo, entonces f tiene a lo más $grad(f)$ raices en $\mathbf{K}$.

Demostración

Usaremos inducción sobre $m = grad(f)$

i) Si $m = 0$, f es una constante no nula, luego no tiene raíces. El corolario es verdadero.

ii) Asumamos que el corolario es válido para polinomios de grado $m-1$.

iii) Sea f un polinomio de grado m. Si f no tiene raíces en K entonces se verifica el corolario.

Sea a entonces es una raíz de f en $\mathbf{K}$, $f(a) = 0$. Por la proposición 1.4.1 se tiene

$$f = q(x-a) + r, \quad r \in \mathbf{K}$$

Luego evaluando en $x = a$ se deduce que $r = 0$, entonces $f = q(x-a)$ de donde

$$grad(q) = m - 1$$

Consideremos b una raíz de f, $b \neq a$ entonces

$$f(b) = q(b)(b-a)$$

$$0 = q(b)(b-a)$$

como $\mathbf{K}$ es cuerpo (dominio de integridad)

$$q(b) = 0$$

Ya que q tiene a los más $m-1$ raíces en $\mathbf{K}$, entonces f tiene m raíces como máximo en $\mathbf{K}$. □

Otra consecuencia de este algoritmo es describir la forma de cada ideal en $K[x]$

Corolario 1.4.2

Si **K** es un campo, entonces cada ideal de $K[x]$ es de la forma

$$\langle f \rangle \text{ para algún } \quad f \in K[x]$$

Además f es único salvo el producto por una constante no nula en K.

Prueba

Tomamos un ideal $I \subset K[x]$

Si $I = \{0\}$ entnces $I = \langle 0 \rangle$.

En otro caso, sea f un polinomio no nulo de grado mínimo contenido en I (su existencia está garantizada por el teorema del buén orden).

Afirmamos que: $\langle f \rangle = I$

($\subset$) En efecto: $\langle f \rangle \subset I$ es directo desde que $f \in I$.

($\supset$) Consideremos la otra inclusión. Sea $g \in I$ entonces $g = qf + r$, donde $r = 0$ ó $grad(r) < grad(f)$. Desde que $qf \in I$ e I es ideal, $r = g - qf \in I$.

Si $r \neq 0$ entonces como grad(f) es mínimo en I, se tiene

$$grad(r) \geq grad(f), \quad \text{pero esto no se puede dar, luego } r = 0$$

y por lo tanto $g = qf \in \langle f \rangle$. Concluyendose $I \subset \langle f \rangle$. $\square$

Ahora con respecto a la unicidad. Supongamos que

$$\langle f \rangle = \langle g \rangle = I$$

luego $f \in \langle g \rangle$ entonces $f = hg$, para algún polinomio h.

De esta forma

$$grad(f) = grad(h) + grad(g), \quad \text{entonces} \quad grad(f) \geq grad(g)$$

Procediendo de igual forma con $g \in \langle f \rangle$, se deduce $grad(g) \geq grad(f)$.

Por lo tanto $grad(g) = grad(f)$ y como $f = hg$ se tiene que $h \in \mathbf{K}$. Luego se da la unicidad salvo producto por una constante. $\square$

Capítulo 2

Orden monomial y Bases de Gröbner

En el capítulo anterior hemos visto los polinomios en $K[x]$.

El presente capítulo se ha dividido en seis secciones.

Sección 1: Se verá como ordenar a los monomios en $K[x_1, \ldots, x_n]$

Sección 2: Se mostrará un algoritmo para dividir en $K[x_1, \ldots, x_n]$ que es una extensión a los métodos de divisiones conocidas, con la particularidad que se trabajará con dos o mas divisores.

Sección 3: Se definirá lo que es un ideal monomial y el resultado central es mostrar que este ideal es finitamente generado.

Sección 4: El resultado de que todo ideal en $K[x_1, \ldots, x_n]$ es finitamente generado es uno de los resultados importantes en toda la elaboración de la tesis, en esta sección también aparecerá lo que es una Base de Gröbner para un ideal.

Sección 5: Veremos las condiciones para que un conjunto generador de un ideal, pase a ser Base de Gröbner.

Sección 6: Se mostrará el algoritmo de Buchberger, el cual nos permite generarar Bases de Gröbner para un ideal.

2.1. Orden monomial en $K[x_1, \ldots, x_n]$

Definición 2.1.1

Un orden monomial en $K[x_1, \ldots, x_n]$ es cualquier relación $>$ en $\mathbf{Z}^n_{\geq 0}$ o equivalentemente, cualquier relación en el conjunto de monomios X^α, $\alpha \in \mathbf{Z}^n_{\geq 0}$ donde se cumplan tres condiciones:

(i) $>$ es una relación de orden (reflexiva, antisimétrica y transitiva) total en $\mathbf{Z}^n_{\geq 0}$.

(ii) Si se tiene $\alpha > \beta$ y $\gamma \in \mathbf{Z}^n_{\geq 0}$, entonces se verifica que $\alpha + \gamma > \beta + \gamma$

(iii) $>$ es de buen orden en $\mathbf{Z}^n_{\geq 0}$. Esto significa, que cada subconjunto no vacio de $\mathbf{Z}^n_{\geq 0}$, posee un elemento mínimo con respecto a $>$.

El siguiente lema nos dá otra perspectiva de visualizar a una relación de buen orden en $\mathbf{Z}^n_{\geq 0}$.

Lema 2.1.1

Una relación de orden $>$ en $\mathbf{Z}^n_{\geq 0}$ es de buén orden si y solamente si cada sucesión estrictamente decreciente en $\mathbf{Z}^n_{\geq 0}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots \quad \text{termina.}$$

Demostración:

($\Longrightarrow$) Dada $>$ una relación de buen orden y supongamos que exista una sucesión estrictamente decreciente en $\mathbf{Z}^n_{\geq 0}$ que no termina

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

Consideremos el conjunto

$$A = \{\alpha(i) : i \in \mathbf{N}\} \subset \mathbf{Z}^n_{\geq 0}$$

como A es no vacio existe $k \in \mathbf{N}$ tal que $\alpha(k) < \alpha(i)$, $\forall\ i \in \mathbf{N}$, pero debido a que la sucesión es estrictamente decreciente podemos decir que $\alpha(k+1)$ es estrictamente menor que $\alpha(k)$, es una contradicción.

Por lo tanto concluímos que la sucesión dada termina.

($\Longleftarrow$) Ahora veamos en el otro sentido. Sea $A \subset \mathbf{Z}_{\geq 0}^{n}$ no vacio. Si A no posee un elemento mínimo con respecto a $>$, podemos originar una sucesión estrictamente decreciente que no termina y ello va en contradicción con la hipótesis, por lo tanto podemos indicar que en A existe un elemento mínimo, luego $>$ es una relación de buen orden. $\square$

Ejemplo 2.1.1

En $\mathbf{Z}_{\geq 0}$: $0 < 1 < 2 < \cdots < n < \cdots$ es un orden monomial en $\mathbf{Z}_{\geq 0}$. Luego podemos indicar que el orden según el grado de un monomio en $K[x]$ es un orden monomial.

A continuación se definirán tres ordenes monomiales en $K[x_1, \ldots, x_n]$ las cuales se utilizarán en el desarrollo del presente trabajo.

(1) Orden lexicográfico (l)

(2) Orden lexicográfico graduado(lg)

(3) Orden lexicográfico graduado reverso(lgr)

Definición 2.1.2 *Orden lexicográfico*

Sea $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbf{Z}_{\geq 0}^{n}$. Diremos que $\alpha >_l \beta$ si la primera componente no nula de la izquierda en el vector diferencia $\alpha - \beta \in \mathbf{Z}^n$ es positiva.

Escribiremos $x^{\alpha} >_l x^{\beta}$ siempre que $\alpha >_l \beta$.

Ejemplo 2.1.2

$\alpha = (1, 3, 8)$, $\beta = (0, 9, 9)$ como $\alpha - \beta = (1, -6, -1)$ podemos indicar que $\alpha >_l \beta$. Igualmente $(5, 4, 1) >_l (5, 3, 8)$

Ejemplo 2.1.3

Debido a que

$$(1, 0, \ldots, 0) >_l (0, 1, 0, \ldots, 0) >_l \cdots >_l (0, \ldots, 0, 1)$$

se puede indicar que

$$x_1 >_l x_2 >_l \cdots >_l x_n \quad \text{en} \quad K[x_1, x_2, \ldots, x_n]$$

Definición 2.1.3 *Orden lexicográfico graduado*

Sean $\alpha, \beta \in \mathbf{Z}^n_{\geq 0}$. Diremos que $\alpha >_{lg} \beta$, si

$$|\alpha| > |\beta| \quad \text{ó}$$

$$|\alpha| = |\beta| \quad \text{y} \quad \alpha >_l \beta$$

De este modo podemos indicar que:

$$(1,2,3) >_{lg} (2,2,0)$$

$$(2,1,4) >_{lg} (1,2,4)$$

también se tiene:

$$x_1 >_{lg} x_2 >_{lg} \cdots >_{lg} x_n \text{ en } K[x_1, x_2, \ldots, x_n]$$

Definición 2.1.4 *Orden lexicográfico graduado reverso*

Sean $\alpha, \beta \in \mathbf{Z}^n_{\geq 0}$. Diremos que $\alpha >_{lgr} \beta$, siempre que $|\alpha| > |\beta|$ ó $|\alpha| = |\beta|$ y en $\alpha - \beta \in \mathbf{Z}^n$ la primera componente por la derecha no nula, es negativa.

Asi tenemos

$$(4,7,1) >_{lgr} (2,2,2) \quad \text{y} \quad (1,6,3) >_{lgr} (2,1,7)$$

debido a que $(1,6,3) - (2,1,7) = (-1,5,-4)$ también tenemos en $K[x_1, \ldots, x_n]$

$$x_1 >_{lgr} x_2 >_{lgr} \cdots >_{lgr} x_n$$

Terminaremos esta sección con cuatro conceptos que se emplearán continuamente.

Definición 2.1.5

Sea $f = \sum_{\alpha} a_\alpha x^\alpha$ un polinomio no nulo en $K[x_1, \ldots, x_n]$, $a_\alpha \in K$ y $>$ un orden monomial.

(i) $grad(f) = max\{\alpha \in \mathbf{Z}^n_{\geq 0} : a_\alpha \neq 0\}$.

(El máximo con respecto a $>$).

(ii) $cp(f) = a_{grad(f)} \in K$.

(El coeficiente principal de f).

(iii) $Mp(f) = x^{grad(f)}$

(El monomio principal de f).

(iv) $Tp(f) = cp(f)Mp(f)$.

(El término principal de f).

Asi tenemos, para

$$f = 4xy^2z + 4z^2 - 8x^3 + 7x^2z^2 \in K[x, y, z]$$

con el orden lexicográfico, se tiene:

1. $grad(f) = (3, 0, 0)$
2. $cp(f) = -8$
3. $Mp(f) = x^3$
4. $Tp(f) = -8x^3$

Utilizando las notaciones anteriores, podemos comprobar que

Lema 2.1.2

Sea $f, g \in K[x_1, \ldots, x_n]$ polinomios no nulos. Entonces

(i) $grad(fg) = grad(f) + grad(g)$

(ii) Si $f + g \neq 0$ entonces $grad(f + g) \leq max\{grad(f),\ grad(g)\}$

Si en la adición, $grad(f) \neq grad(g)$ entonces ocurre la igualdad. □

2.2. Algoritmo de la división en $K[x_1, \ldots, x_n]$

Para estudiar este problema cuando existen mas variables formularemos un algoritmo de división para polinomios en $K[x_1, \ldots, x_n]$ que va a ser una extensión del algoritmo para $K[x]$.

El objetivo es dividir $f \in K[x_1, \ldots, x_n]$ por $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, de modo que

$$f = a_1f_1 + \ldots + a_sf_s + r, \quad \text{donde} \quad a_1, a_2, \ldots, a_s \ \text{y} \ r \in K[x_1, \ldots, x_n]$$

Donde

a_i: Cocientes, $i = 1, 2, \ldots, s$

r: Resto.

Veamos dos ejemplos donde se muestra esta forma de dividir.

Ejemplo 2.2.1

Dividamos $f = xy^2 + 1$ por $f_1 = xy + 1$ y $f_2 = y + 1$ usando el orden lexicográfico.

Queremos a modo de analogía usar el esquema tradicional de división.

$$\begin{array}{l|l|l} xy^2+1 & xy+1 & y+1 \end{array}$$

como $Tp(f_1) = xy$, $Tp(f_2) = y$ y ambos dividen al $Tp(xy^2 + 1) = xy^2$, siendo f_1 el primero en la lista (f_1, f_2), dividamos xy^2 por $Tp(f_1)$ obteniendose y.

$$\begin{array}{rl|l|l} xy^2+1 & xy+1 & y+1 \\ \cline{1-1} -xy^2-y & y & \\ \cline{1-1} -y+1 & & \end{array}$$

Ahora, como $Tp(f_1)$ no divide a $-y + 1$ pero $Tp(f_2)$ si lo divide, se tendría

$$\begin{array}{rl|l|l} xy^2+1 & xy+1 & y+1 \\ \cline{1-1} -xy^2-y & y & -1 \\ \cline{1-1} -y+1 & & \\ \cline{1-1} y+1 & & \\ \cline{1-1} 2 & & \end{array}$$

Debido a que $Tp(f_1)$ y $Tp(f_2)$ no dividen a 2, se considera el resto o residuo $r = 2$.

De esta forma obtenemos

$$f = a_1 f_1 + a_2 f_2 + r \quad \text{donde} \quad a_1 = y, a_2 = -1, r = 2$$

Ejemplo 2.2.2

En este ejemplo encontraremos un inesperado resultado. Consideremos

$$f = x^2y + xy^2 + y^2$$

y dividamos por (f_1, f_2) donde:

$$\begin{aligned} f_1 &= xy - 1 \\ f_2 &= y^2 - 1 \end{aligned}$$

se usará el orden lexicográfico.

Si realizamos el proceso, obtenemos

$$\begin{array}{rl|l|l} x^2y+xy^2+y^2 & xy-1 & & y^2-1 \\ \cline{1-1} -x^2y+x & x+y & & \\ \cline{1-1} xy^2+x+y^2 & & & \\ \cline{1-1} -xy^2+y & & & \\ \cline{1-1} x+y^2+y & & & \end{array}$$

En este punto observemos que

$$Tp(f_1) = xy, \quad Tp(f_2) = y^2$$

no dividen al

$$Tp(x+y^2+y) = x$$

pero como $Tp(f_2)$ divide a uno de los términos de $x+y^2+y$ (este va ser una de las condiciones para caracterizar al resto), este último no puede ser el resto, luego removemos x en $x+y^2-y$ y lo colocamos como parte del resto $r = x + \ldots$

Ahora si podemos seguir dividiendo según la técnica dada, obteniendose el esquema siguiente

$$\begin{array}{rl|l|l} x^2y+xy^2+y & xy-1 & & y^2-1 \\ \cline{1-1} -x^2y+x & x+y & & 1 \\ \cline{1-1} xy^2+x+y^2 & & & \\ \cline{1-1} -xy^2+y & & & \\ \cline{1-1} x+y^2+y & & & \\ \cline{1-1} y^2+y & & & \\ \cline{1-1} -y^2+1 & & & \\ \cline{1-1} y+1 & & & \end{array}$$

Por lo tanto: $r = x+y+1$ obteniendose

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

Teorema 2.2.1 *Algoritmo de la división en* $K[x_1, \ldots, x_n]$

Fijado un orden monomial $>$ en $\mathbf{Z}^n_{\geq 0}$. $F = (f_1, f_2, \ldots, f_s)$ una s-upla ordenada de polinomios en $K[x_1, \ldots, x_n]$

Entonces cada $f \in K[x_1, \ldots, x_n]$ puede ser escrito como

$$f = a_1 f_1 + a_2 f_2 + \ldots + a_s f_S + r \text{ donde } a_i, r \in K[x_1, \ldots, x_n]$$

y $r = 0$ ó r es combinación lineal con coeficientes en K, de monomios en el cual ninguno de ellos es divisible por cualquiera de los términos principales siguientes

$$Tp(f_1), Tp(f_2), \ldots, Tp(f_s)$$

Llamaremos a r, el resto o residuo de dividir f por F Además, si $a_i f_i \neq 0$ entonces tenemos

$$grad(f) \geq grad(a_i f_i).$$

Demostración

Probaremos que existen $a_1, a_2, \ldots, a_s$ y r con las condiciones pedidas, mediante la formulación del algoritmo 2.

Se observa que si algún $Tp(f_i)$ divide a $Tp(f)$ entonces se observa que el algoritmo procede como en el caso de una variable.

Si $Tp(f_i)$ no divide a $Tp(f)$ para ningún i entonces agregamos $Tp(f)$ al resto y ello esta dado por la expresión

$$r := r + Tp(f)$$

Para probar que el algoritmo funciona, mostraremos primero que:

$$f = a_1 f_1 + a_2 f_2 + \ldots + a_s f_s + r + p \tag{2.1}$$

lo obtenemos en cada paso dado en el algoritmo.

Esto es verdadero para la evaluación inicial de $a_1, a_2, \ldots, a_s, p$ y r.

Ahora supongamos que (2.1) es un paso en el algoritmo. Si el paso siguiente es un paso de división, entonces algún $Tp(f_i)$ divide $Tp(p)$ y la igualdad

$$a_i f_i + p = (a_i + \frac{Tp(p)}{Tp(f_i)}) f_i + \{p - \frac{Tp(p)}{Tp(f_i)}) f_i\}$$

Algoritmo 2 Algoritmo de División Generalizada

Entrada: $f_1, f_2, \ldots, fs, f$

Salida: $a_1, a_2, \ldots, a_s, r$

for $i = 1, 2, \ldots s$ **do**
  $a_i := 0$
end for
$r := 0$
$p := f$
while $p \neq 0$ **do**
  $i = 1$
  $divi := false$
  while $i \leq s$ y divi=false **do**
    if $Tp(f_i)$ divide $Tp(p)$ **then**
      $a_i := a_i + Tp(p)/Tp(f_i)$
      $p := p - (Tp(p)/Tp(f_i))f_i$
      $divi := true$
    else
      $i := i + 1$
    end if
  end while
  if $divi = falso$ **then**
    $r := r + Tp(p)$
    $p := p - Tp(p)$
  end if
end while

muestra que $a_i f_i + p$ es inalterable. Desde que las otras variables no son afectadas, la ecuación (2.1) es verdadero (caso en que se entra al While ... Do y el resto no es alterado).

En el otro caso, si el paso siguiente entra en IF ... THEN, entonces p y r son cambiadas, pero la suma $p + r$ no queda alterada ya que:

$$p + r = (p - Tp(p)) + (r + Tp(p))$$

luego se tiene que (2.1) se verifica en este paso.

Como el algoritmo se detiene cuando $p = 0$, luego (2.1) se transforma en lo pedido. Y como cada término de r ($r := r + Tp(p)$) se ha obtenido con cada paso de modo que $Tp(p)$ no es divisible por ningún $Tp(f_i)$, por lo tanto el resto cumple las condiciones del teorema.

Finalmente se mostrará que el proceso del algoritmo termina.

La clave de esto es que en cada tiempo, redefinimos la variable p y su grado disminuye.

En efecto, supongamos que durante un paso de la división, p es redefinido

$$p' = p - (\frac{Tp(p)}{Tp(f_i)})f_i$$

pero también se tiene:

$$Tp((\frac{Tp(p)}{Tp(f_i)})f_i) = ((\frac{Tp(p)}{Tp(f_i)})Tp(f_i) = Tp(p)$$

si $p' \neq 0$ entonces p' tiene el grado menor que p es decir $grad(p') < grad(p)$.

Supongamos que durante el paso restante, p es redefinido $p' = p - Tp(p)$ es directo que si $p' \neq 0$ entonces $grad(p') < grad(p)$.

Por lo tanto en cualquier caso el grado decrece.

Si el algoritmo no termina, podemos obtener una sucesión infinita estrictamente decreciente de grados

$$grad(p) > grad(p') > \cdots$$

pero como $>$ es de buen orden, esto no se puede dar. □

2.3. Ideales monomiales y el lema de Dickson

Definición 2.3.1

Un ideal $I \subset K[x_1, x_2, \ldots, x_n]$ es un ideal monomial, si existe un subconjunto $A \subset \mathbf{Z}^n_{\geq 0}$ tal que I consiste de todos los polinomios de la forma

$$\sum_{\alpha \in A} h_\alpha x^\alpha, \quad \text{donde la suma es finita y} \quad h_\alpha \in K[x_1, x_2, \ldots, x_n]$$

En este caso, escribimos $I = \langle x^\alpha : \ \alpha \in A \rangle$.

El lema siguiente va a caracterizar a los monomios que están en un ideal monomial.

Lema 2.3.1

Sea $I = \langle x^\alpha : \ \alpha \in A \rangle$ un ideal monomial. Entonces un monomio x^β está en I si y solo si x^β es divisible por algún x^α, para $\alpha \in A$.

Demostración:

($\Longrightarrow$) Sea $x^\beta \in I$ entonces

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}, \quad \text{donde} \quad h_i \in K[x_1, x_2, \ldots, x_n], \quad \alpha(i) \in A$$

si desarrollamos el segundo miembro de la expresión anterior notamos que cada término es divisible por $x^{\alpha(i)}$ para algún $\alpha(i) \in A$.

Ahora por la igualdad de polinomios en $K[x_1, x_2, \ldots, x_n]$, como todos los términos del segundo miembro, se reducen a la forma x^β, se tendría que x^β es divisible por $x^{\alpha(i)}$, para algún $\alpha(i) \in A$.

($\Longleftarrow$) En el otro sentido, desde que I es ideal, se obtiene de manera directa. □

Lema 2.3.2

Sea I un ideal monomial y $f \in K[x_1, x_2, \ldots, x_n]$. Entonces las afirmaciones siguientes son equivalentes:

(1) $f \in I$

(2) Cada término de f está en I.

(3) f es k-combinación lineal de monomios en I.

Prueba

(3)$\Longrightarrow$(2): Sea $f = c_1 x^{\alpha(1)} + \cdots + c_s x^{\alpha(s)}$ donde $c_i \in K$, $x^{\alpha(i)}$ es un monomio en I. Luego cada término de f, $c_i x^{\alpha(i)}$ está en I.

(2)$\Longrightarrow$(1): Directo desde que I es un ideal.

(1)$\Longrightarrow$(3): Si $f \in I$ y considerando $I = \langle x^\alpha : \alpha \in A \rangle$, $A \subset \mathbf{Z}_{\geq 0}^n$ entonces

$$f = \sum_{i=1}^{s} h_i x^{\alpha(i)}, \quad \text{donde } h_i \in K[x_1, x_2, \ldots, x_n], \quad \alpha(i) \in A$$

si desarrollamos el segundo miembro, notamos que cada término tiene la forma cx^β, donde $c \in K$ y x^β es un monomio en I por el lema (3.2.1). □

El resultado principal de esta sección es que todos los ideales monomiales en $K[x_1, x_2, \ldots, x_n]$ son finitamente generados (f.g.)

Teorema 2.3.3 *(Dickson)*

Para cada ideal monomial $I = \langle x^\alpha : \alpha \in A \rangle \subset K[x_1, x_2, \ldots, x_n]$ existen

$$\alpha(1), \alpha(2), \ldots, \alpha(s) \in A$$

tal que

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

Prueba

Por inducción sobre el número de variables n.

(i) Si $n = 1$ entonces $I = \langle x_1^\alpha : \alpha \in A \subset \mathbf{Z}_{\geq 0} \rangle$, sea β el menor elemento en $A \subset \mathbf{Z}_{\geq 0}$, luego x_1^β divide a todos los monomios de I, en particular a todos los generadores de I. Por lo tanto se deduce que $I = \langle x_1^\beta \rangle$

(ii) Asumamos que $n > 1$ y que el teorema se cumple para $n - 1$.

(iii) Tomemos $x_1, \ldots, x_{n-1}, y$ como variables en $K[x_1, \ldots x_{n-1}, y]$ luego los monomios en este anillo pueden ser escritos asi

$$x^{\alpha} y^{m}, \text{ donde } \alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbf{Z}_{\geq 0}^{n-1}, \ m \in \mathbf{Z}_{\geq 0}$$

Sea $I \subset K[x_1, \ldots x_{n-1}, y]$ un ideal monomial, demostraremos que I es f.g. por monomios.

Consideremos:

$$J = \langle x^{\alpha} : \ x^{\alpha} y^{m} \in I, \ \text{ para algún } \ m \in \mathbf{Z}_{\geq 0} \rangle \subset K[x_1, \ldots x_{n-1}]$$

es un ideal en $K[x_1, x_2, \ldots, x_{n-1}]$ (se puede decir que J es la proyección de I sobre $K[x_1, \ldots x_{n-1}]$). Luego por hipótesis inductiva

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

Por la construcción dada para obtener J, para cada $x^{\alpha(i)}$, $i = 1, 2, \ldots, s$ existe $m_i \in \mathbf{Z}_{\geq 0}$ tal que $x^{\alpha(i)} y^{m_i} \in I$. Luego tenemos $m_1, \ldots, m_s \in \mathbf{Z}_{\geq 0}$.

Sea

$$m = \text{máx}\{m_1, m_2 \ldots, m_s\}$$

Para cada k, $k = 0, 1, \ldots, m-1$ formemos el ideal

$$J_k = \langle x^{\beta} : \ x^{\beta} y^{k} \in I \rangle \subset K[x_1, x_2, \ldots, x_{n-1}]$$

Luego por hipótesis inductiva

$$J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)} \rangle, \ \ k = 0, 1, \ldots, m-1$$

Se tiene que I es generado por los monomios de la lista siguiente

Desde J : $x^{\alpha(1)} y^{m}, \ldots, x^{\alpha(s)} y^{m}$

: $x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)}$

: $x^{\alpha_1(1)} y^{1}, \ldots, x^{\alpha_1(s_1)} y^{1}$

$\vdots$

J_{m-1} : $x^{\alpha_{m-1}(1)} y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1}$

Para ver esta última afirmación, note que cada monomio de I es divisible por algún elemento de la lista anterior.

En efecto, sea $x^{\alpha}y^{p} \in I$ un monomio arbitrario de I. Si consideramos $p \geq m$ entonces como $x^{\alpha} \in J$ se tiene que x^{α} es divisible por $x^{\alpha(k)}$ para algún k, $k \in \{1, 2, \ldots, s\}$ luego $x^{\alpha} = x^{\gamma}x^{\alpha(k)}$ entonces

$$x^{\alpha}y^{p} = x^{\gamma}x^{\alpha(k)}y^{p-m}y^{m} = (x^{\gamma}y^{p-m})x^{\alpha(k)}y^{m}$$

Por lo tanto es generado por un elemento de la lista.

En otro caso, si $p \leq m-1$, se tiene por construcción de J_p,

$$x^{\alpha} \in J_p$$

luego por el lema (2.3.1) x^{α} es divisible por algún

$$x^{\alpha_p(i)}, \quad i \in \{1, 2, \ldots, s_p\}$$

entonces

$$x^{\alpha} = hx^{\alpha_p(i)}$$

luego

$$x^{\alpha}y^{p} = hx^{\alpha_p(i)}y^{p}$$

entonces $x^{\alpha}y^{p}$ es generado por un elemento de la lista.

Ahora, sea $f \in I$ arbitrario por el lema (2.3.2) f es una k-combinación lineal de monomios de I y como cada monomio de I es divisible por algún elemento de lista, se deduce que f está generado por elementos de la lista anteriormente dada.

Hasta aqui, no se ha dependido de los generadores que por dèfinición tiene el ideal monomial I.

Sea

$$I = \langle x^{\alpha} : \ \alpha \in A \subset \mathbf{Z}^{n}_{\geq 0} \rangle \subset K[x_1, x_2, \ldots, x_n]$$

por lo demostrado existen $\beta(1), \ldots, \beta(s) \in \mathbf{Z}^{n}_{\geq 0}$ tal que

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

como $x^{\beta(i)} \in I$ entonces $x^{\beta(i)}$ es divisible por $x^{\alpha(i)}$ para algún $\alpha(i) \in A$, luego se tiene $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ con $\alpha(1), \alpha(2), \ldots, \alpha(s) \in A$, por lo tanto se deduce que

$$I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle \text{ donde } \alpha(i) \in A \quad \square$$

Podemos utilizar el lema de Dickson para probar un importante resultado del orden monomial en $K[x_1, x_2, \ldots, x_n]$.

Corolario 2.3.1

Sea $>$ una relación en $\mathbf{Z}^n_{\geq 0}$ satisfaciendo

(i) $>$ es de orden total en $\mathbf{Z}^n_{\geq 0}$.

(ii) Si $\alpha > \beta$ y $\gamma \in \mathbf{Z}^n_{\geq 0}$ entonces $\alpha + \gamma > \beta + \gamma$.

Entonces $>$ es un buen orden en $\mathbf{Z}^n_{\geq 0}$ si y solo si $\alpha > 0$ para todo $\alpha \in \mathbf{Z}^n_{\geq 0}$

Demostración:

($\Longrightarrow$) Considerando $>$ una relación en $\mathbf{Z}^n_{\geq 0}$ donde cumpla con (i) y (ii) y sea un buen orden.

Tomemos α_0 el menor elemento en $\mathbf{Z}^n_{\geq 0}$, la cual existe por ser $>$ una relación de buen orden.

Supongamos que $\alpha_0 < 0$ menor estricto, por (ii) $2\alpha_0 < \alpha_0$ pero esto no se puede dar ya que α_0 es mínimo y también que $\alpha_0 \neq 0$, por lo tanto $0 < \alpha_0$.

Sea $\alpha \in \mathbf{Z}^n_{\geq 0}$ arbitrario, entonces $\alpha_0 < \alpha$ por ser α_0 el menor y como $0 < \alpha_0$ por transitividad $0 < \alpha$.

($\Longleftarrow$) Sea $A \subset \mathbf{Z}^n_{\geq 0}$ subconjunto no vacío, tenemos que mostrar que A tiene un elemento mínimo.

Sea $I = \langle x^\alpha : \alpha \in A \rangle$ un ideal monomial, por Dickson

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

por (i), $\{\alpha(1), \ldots \alpha(s)\}$ posee un elemento mínimo.

Sea α_0 tal elemento.

Consideremos $\alpha \in A$ arbitrario, por demostrar que $\alpha_0 < \alpha$.

En efecto, como $x^\alpha \in I$ entonces x^α es divisible por $x^{\alpha(j)}$ para algún $j = 1, 2, \ldots, s$ entonces

$$x^\alpha = x^p x^{\alpha(j)}$$

luego

$$\alpha = p + \alpha(j)$$

como $p > 0$ y por (ii)

$$p + \alpha(j) > \alpha(j)$$

y como $\alpha(j) > \alpha_0$ por ser α_0 elemento mínimo de

$$\{\alpha(1), \ldots, \alpha(s)\}$$

luego $\alpha > \alpha_0$ □

2.4. El teorema de Base de Hilbert y Bases de Gröbner

Definición 2.4.1

Sea $I \subset K[x_1, x_2, \ldots, x_n]$ un ideal, $I \neq \{0\}$

(i) Denotemos por $Tp(I)$ al conjunto de los términos principales de los elementos de I.

$$Tp(I) = \{Tp(f) / \ f \in I\}$$

(ii) Denotemos por $\langle Tp(I) \rangle$ el ideal generado por los elementos de $Tp(I)$, con coeficientes en $K[x_1, x_2, \ldots, x_n]$

En esta sección demostraremos que $\langle Tp(I)\rangle$ es un ideal monomial, por lo cual conseguimos que $\langle Tp(I)\rangle$ sea f.g. por términos principales.

Proposición 2.4.1

Sea $I \subset K[x_1, x_2, \ldots, x_n]$ un ideal

Entonces

(i) $\langle Tp(I)\rangle$ es un ideal monomial.

(ii) Existen $g_1, g_2, \ldots, g_s \in I$ tal que

$$\langle Tp(I)\rangle = \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_s)\rangle$$

Demostración:

(i) Sea $Mp(g)$ el monomio principal de $g \in I - \{0\}$, entonces $\langle Mp(g) :\ g \in I - \{0\}\rangle$ es un ideal monomial, basta considerar

$$A = \{\alpha \in \mathbf{Z}^n_{\geq 0} :\ \exists g \in I - \{0\},\ \ Mp(g) = x^\alpha\}$$

entonces

$$\langle x^\alpha :\ \alpha \in A\rangle = \langle Mp(g) :\ g \in I - \{0\}\rangle$$

como $Mp(g)$ y $Tp(g)$ se diferencian en una constante no nula se tiene que

$$\langle Mp(g) :\ g \in I - \{0\}\rangle = \langle Tp(g) :\ g \in I - \{0\}\rangle$$

Por lo tanto

$$\langle Tp(I)\rangle = \langle Tp(g) :\ g \in I - \{0\}\rangle = \langle Mp(g)/\ g \in I - \{0\}\rangle$$

luego $\langle Tp(I)\rangle$ es un ideal monomial.

(ii) Desde que $\langle Tp(I)\rangle$ es generado por monomios $Mp(g)$ para $g \in I - \{0\}$, por Dickson, se tiene:

$$\langle Tp(I)\rangle = \langle Mp(g_1), Mp(g_2), \ldots, Mp(g_t)\rangle$$

para $g_1, g_2, \ldots, g_t \in I$ y como

$$\langle Mp(g_1), Mp(g_2), \ldots, Mp(g_t)\rangle = \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_t)\rangle$$

entonces

$$\langle Tp(I)\rangle = \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_t)\rangle \quad \square$$

Como un resultado importante de la proposición (2.4.1) se tiene que cada ideal en el anillo de polinomios $K[x_1, x_2, \ldots, x_n]$ es f.g. Esto se dará en el teorema siguiente.

Teorema 2.4.1 *Teorema de Base de Hilbert*

Cada ideal $I \subset K[x_1, x_2, \ldots, x_n]$ tiene un conjunto finito de generadores es decir

$$I = \langle g_1, g_2, \ldots, g_s \rangle \quad \text{donde } g_1, g_2, \ldots, g_s \in I$$

Demostración

Si $I = \{0\}$ luego $I = \langle 0 \rangle$ por lo tanto se verifica el teorema.

Si $I \neq \{0\}$ por la proposición (2.4.1)

$$\langle Tp(I) \rangle = \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_t) \rangle \quad \text{donde } g_1, g_2, \ldots, g_t \in I$$

afirmamos que $I = \langle g_1, g_2, \ldots, g_s \rangle$. En efecto

Sea $f \in I$ arbitrario, considerando $F = (g_1, g_2, \ldots, g_t)$ por el algoritmo de la división se tiene

$$f = a_1 g_1 + a_2 g_2 + \ldots + a_t g_t + r \quad \text{donde } a_i, r \in K[x_1, x_2, \ldots, x_n]$$

y $r = 0$ o ningún término de r es divisible por $Tp(g_1), Tp(g_2), \ldots, Tp(g_t)$

Como $g_1, g_2, \ldots, g_t, f \in I$ se tiene $r \in I$

Si $r \neq 0$ entonces

$$Tp(r) \in \langle Tp(I) \rangle = \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_t) \rangle$$

luego por el lema (2.3.1), $Tp(r)$ es divisible por algún $Tp(g_i)$ pero ello no puede ser, con lo cual resulta $r = 0$.

Por lo tanto

$$f = a_1 g_1 + a_2 g_2 + \ldots + a_t g_t \in \langle g_1, g_2, \ldots, g_t \rangle$$

entonces

$$f \in \langle g_1, g_2, \ldots, g_t \rangle$$

La otra inclusión $I \supset \langle g_1, g_2, \ldots, g_t \rangle$ es directa. $\square$

Definición 2.4.2

Fijado un orden monomial. Un subconjunto finito $G = \{g_1, g_2, \ldots, g_s\}$ de un ideal I, es llamado Base de Gröbner si

$$\langle Tp(g_1), Tp(g_2), \ldots, Tp(g_t)\rangle = \langle Tp(I)\rangle$$

Corolario 2.4.1

Fijado un orden monomial. Entonces cada ideal no nulo $I \subset K[x_1, x_2, \ldots, x_n]$ tiene una base de Gröbner. Además cualquier Base de Gröbner para un ideal I es un conjunto generador de I.

Demostración

Sea I un ideal no nulo en $K[x_1, x_2, \ldots, x_n]$ debido a la proposición (2.4.1) parte (ii), existen $g_1, g_2, \ldots, g_s \in I$ de tal forma que

$$\langle Tp(I)\rangle = \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_s)\rangle$$

por lo tanto, $G = \{g_1, g_2, \ldots, g_s\}$ es una base de Gröbner para I.

Y debido al argumento utilizado en el teorema (2.4.1) se tiene que

$$I = \langle g_1, g_2, \ldots, g_s\rangle \qquad \square$$

Ejemplo 2.4.1

Sea $J = \langle g_1, g_2\rangle$, $g_1 = x + z$, $g_2 = y - z$ un ideal en $\mathbf{R}[x, y, z]$. Usando el orden lexicográfico, se verifica que $G = \{g_1, g_2\}$ forma una Base de Gröbner para J.

Ejemplo 2.4.2

Sea $I = \langle f_1, f_2\rangle$, donde $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$ un ideal en $\mathbf{R}[x, y]$. Es claro que $G = \{f_1, f_2\}$ es un generador de I pero no una base de Gröbner, con respecto al orden lexicográfico graduado.

En efecto, debido a que

$$x^2 = xf_2 - yf_1$$

entonces $x^2 \in \langle Tp(I)\rangle$, pero $Tp(f_1) = x^3$, $Tp(f_2) = x^2y$

se tiene

$$x^2 \notin \langle Tp(f_1), Tp(f_2) \rangle$$

por lo tanto

$$\langle Tp(I) \rangle \neq \langle Tp(G) \rangle = \langle Tp(f_1), Tp(f_2) \rangle$$

Como aplicación al teorema de Base de Hilbert, se tiene que toda cadena ascendente de Ideales es estacionario.

Teorema 2.4.2 *(La condición de cadena ascendente)*

Sea $I_1 \subset I_2 \subset I_3 \subset \cdots$, una cadena ascendente de ideales en $K[x_1, x_2, \ldots, x_n]$. Entonces existe $N \geq 1$ tal que

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

Demostración

Dada la cadena ascendente $I_1 \subset I_2 \subset I_3 \subset \cdots$

$$I = \bigcup_{i=1}^{\infty} I_i \quad I \text{ es un ideal en } K[x_1, x_2, \ldots, x_n]$$

Por el teorema de Base de Hilbert, se tiene que:

$$I = \langle f_1, f_2, \ldots, f_s \rangle$$

Como $I = \bigcup_{i=1}^{\infty} I_i$, se tiene que $f_i \in I_{j_i}$ para $i = 1, 2, \ldots, s$

Sea N el valor máximo de los j_i. Por ser una cadena ascendente, se tiene que

$$I = \langle f_1, f_2, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I$$

Por lo tanto $I_N = I_{N+1} = I_{N+2} = \cdots$ □

Como segunda aplicación al teorema de Base de Hilbert, es con respecto a la variedad

$$V(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in \mathbf{K}^n / \ f_i(a_1, \ldots, a_n) = 0, \quad \forall\, i\}$$

El teorema nos extiende esta definición indicando que se puede definir para un ideal $I \subset K[x_1, x_2, \ldots, x_n]$.

Definición 2.4.3

Sea $I \subset K[x_1, x_2, \ldots, x_n]$ un ideal.

Entonces

$$V(I) = \{(a_1, a_2, \ldots, a_n) \in \mathbf{K}^n / \ f(a_1, \ldots, a_n) = 0, \ \ \forall\ f \in I\}$$

Proposición 2.4.2

$V(I)$ es una variedad afín. En particular, si $I = \langle f_1, f_2, \ldots, f_s \rangle$ entonces

$$V(I) = V(f_1, f_2, \ldots, f_s)$$

Demostración

Por el teorema de Base de Hilbert $I = \langle f_1, f_2, \ldots, f_s \rangle$ para algún conjunto finito generador.

Afirmación: $V(I) = V(f_1, f_2, \ldots, f_s)$

En efecto, sea $f \in I$ y $f(a_1, a_2, \ldots, a_n) = 0, \ \forall\ f \in I$, entonces

$$f_i(a_1, a_2, \ldots, a_n) = 0$$

luego

$$V(I) \subset V(f_1, f_2, \ldots, f_s)$$

Ahora, sea $(a_1, a_2, \ldots, a_n) \in V(f_1, f_2, \ldots, f_s)$ entonces

$$f_i(a_1, a_2, \ldots, a_n) = 0, \ \ \forall\ i = 1, 2, \ldots, s$$

Sea $f \in I$ arbitrario, como $f \in I = \langle f_1, f_2, \ldots, f_s \rangle$ entonces

$$f = \sum_{i=1}^{s} h_i f_i \ \text{ donde } \ h_i \in \mathbf{K}[x_1, \ldots, x_n]$$

$$\begin{aligned} f(a_1, a_2, \ldots, a_n) &= \textstyle\sum_{i=1}^{s} h_i(a_1, a_2, \ldots, a_n) f_i(a_1, a_2, \ldots, a_n) \\ &= \textstyle\sum_{i=1}^{s} h_i(a_1, a_2, \ldots, a_n) \cdot 0 \\ &= 0 \end{aligned}$$

De este modo se tiene $V(I) \supset V(f_1, f_2, \ldots, f_s)$ $\square$

2.5. Propiedades de Bases de Gröbner

En la sección anterior, se demostró que cada ideal no nulo en $K[x_1, x_2, \ldots, x_n]$ tiene una Base de Gröbner. En esta sección se verá cuando un conjunto generador de un ideal es una Base de Gröbner.

El inconveniente comportamiento del algoritmo de la división en $K[x_1, x_2, \ldots, x_n]$, esto es, el resto o residuo no siempre es único. No ocurre cuando se dividen por los elementos de una Base de Gröbner.

Proposición 2.5.1

Sea $G = \{g_1, g_2, \ldots, g_t\}$ una Base de Gröbner para el ideal $I \subset K[x_1, x_2, \ldots, x_n]$ y $f \in K[x_1, x_2, \ldots, x_n]$. Entonces existe un único $r \in K[x_1, x_2, \ldots, x_n]$ que cumpla con:

(i) Ningún término de r es divisible por

$$Tp(g_1), Tp(g_2), \ldots, Tp(g_t)$$

(ii) Existe $g \in I$ tal que

$$f = g + r$$

En particular r es el resto de la división de f por G.

Demostración

A) Existencia de $r \in K[x_1, x_2, \ldots, x_n]$.

Utilizando el algoritmo de la división se obtiene

$$f = a_1 g_1 + a_2 g_2 + \ldots + a_t g_t + r \quad \text{donde} \quad a_i \in K[x_1, x_2, \ldots, x_n]$$

$r \in K[x_1, x_2, \ldots, x_n]$ satisface (i), considerando $g = a_1 g_1 + a_2 g_2 + \cdots + a_t g_t$ entonces $f = g + r$, satisface (ii).

B) Unicidad:

Sea $f = g + r = g' + r'$, cumpliendo con (i) y(ii).

Entonces

$$r - r' = g' - g \in I \quad \text{debido a que} \quad g, g' \in I.$$

Si $r - r' \neq 0$ entonces

$$Tp(r - r') \in \langle Tp(I) \rangle = \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_s) \rangle$$

luego $Tp(r-r')$ es divisible por algún $Tp(g_i)$, esto no se puede dar ya que ningún término de r y r', es divisible por

$$Tp(g_1), Tp(g_2), \ldots, Tp(g_t)$$

por lo tanto $r - r' = 0$. Entonces $r = r'$ y $g = g'$.

La parte final de la proposición, viene de la unicidad y del algoritmo de la división que nos da un $r \in K[x_1, x_2, \ldots, x_n]$ que cumpla con (i) y (ii). $\square$

Aunque el resto r es único para una Base de Gröbner, los cocientes a_i que produce el algoritmo de la división

$$f = a_1 g_1 + a_2 g_2 + \ldots + a_t g_t + r$$

pueden cambiar si se lista los generadores en orden diferente.

Por lo visto anteriormente

$$I = \langle x + z, y - z \rangle, \quad G = \{x + z, y - z\}$$

es una Base de Gröbner para I.

Dividendo $f = xy$ por $G = \{x+z, y-z\}$, utilizando el orden lexicográfico se obtiene

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

pero al dividirlo por $G = \{y - z, x + z\}$ se obtiene

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

Corolario 2.5.1

Sea $G = \{g_1, g_2, \ldots, g_t\}$ una Base de Gröbner para el ideal $I \subset K[x_1, x_2, \ldots, x_n]$ y $f \in K[x_1, x_2, \ldots, x_n]$.

Entonces $f \in I$ si y solo si el resto en la división de f por G es cero.

Demostración.

($\Longrightarrow$) Si $f \in I$ entonces $f = f + 0$, satisface las condiciones (i) y (ii) de la proposición (2.5.1), pero si se divide por el algoritmo de la división se obtiene

$$f = (a_1 g_1 + a_2 g_2 + \ldots + a_t g_t) + r$$

que también cumple, entonces por la unicidad del resto $r = 0$.

($\Longleftarrow$) Por el algoritmo de la división

$$f = a_1 g_1 + a_2 g_2 + \ldots + a_t g_t + r$$

pero por hipótesis $r = 0$.

Entonces

$$f = a_1 g_1 + a_2 g_2 + \ldots + a_t g_t \in I$$

por lo tanto $f \in I$ $\square$

Notación: Por simplicidad se escribe $\overline{f}^F$ para el resto de dividir f por la s-upla ordenada $F = (f_1, f_2, \ldots, f_s)$.

Ejemplo 2.5.1

Sea

$$F = (x^2y - y^2,\ x^4y^2 - y^2) \subset \mathbf{K}[x, y]$$

usando el orden lexicográfico se tiene

$$\overline{x^5y}^F = xy^3$$

ya que

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0(x^4y^2 - y^2) + xy^3$$

En lo que sigue se discutirá cuando un conjunto generador de un ideal, es una Base de Gröbner.

Definición 2.5.1

Sea $f, g \in \mathbf{K}[x_1, x_2, \ldots, x_n]$ polinomios no nulos.

(i) Si $grad(f) = \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $grad(g) = \beta = (\beta_1, \beta_2, \ldots, \beta_n)$, entonces

$$\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n) \text{ donde } \gamma_i = \text{máx}(\alpha_i, \beta_i) \text{ para cada } i,\ i = 1, 2, \ldots, n$$

se llamará a X^γ el mínimo común multiplo de $MP(f)$ y $MP(g)$ y se denota asi

$$X^\gamma = MCM(MP(f),\ MP(g))$$

(ii) El s-polinomio de f y g es la combinación

$$S(f,g) = \frac{X^\gamma}{Tp(f)} f - \frac{X^\gamma}{Tp(g)} g$$

Ejemplo 2.5.2

$$f = x^3y^2 - x^2y^3 + x, \quad g = 3x^4y + y^2 \text{ en } \mathbf{R}[x, y]$$

con el orden lexicográfico graduado (lg).

Entonces, siendo $MP(f) = x^3y^2$, $MP(g) = x^4y$. Se tiene $\gamma = (4, 2)$, también

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g \\ &= xf - \frac{1}{3} yg \\ &= x(x^3y^2 - x^2y^3 + x) - \frac{1}{3} y(3x^4y + y^2) \\ &= -x^3y^3 + x^2 - \frac{1}{3} y^3 \end{aligned}$$

Un S-polinomio $S(f, g)$ tiene la propiedad de producir la cancelación de los términos principales tanto de f como de g.

Lema 2.5.1

Supongase que se tiene una suma $\sum_{i=1}^{s} c_i f_i$ donde $c_i \in \mathbf{K}$, $f_i \in \mathbf{K}[x_1, x_2, \ldots, x_n]$ y $grad(f_i) = \delta \in \mathbf{Z}^n_{\geq 0}$ para todo i, $i = 1, 2, \ldots, s$.

Si $grad(\sum_{i=1}^{s} c_i f_i) < \delta$ entonces $\sum_{i=1}^{s} c_i f_i$ es una combinación lineal con coeficientes en $\mathbf{K}$ de los S-polinomos $S(f_j, f_k)$ para $1 \leq j, k \leq s$.

Además cada $S(f_i, f_k)$ tiene grado menor que δ.

Demostración

Sea $d_i = cp(f_i)$ entonces $cp(c_i f_i) = c_i d_i$.

Desde que $c_i f_i$ tiene grado δ y su suma tiene el grado estrictamente menor

$$\sum_{i=1}^{s} c_i d_i = 0$$

Se denota $p_i = \frac{f_i}{d_i}$, observamos que el coeficiente principal de p_i es 1.

Considerando la suma telescópica

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i$$

$$= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots$$

$$+(c_1 d_1 + \cdots\cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s$$

Como

$$Tp(f_i) = d_i X^{\delta}$$

con lo cual

$$MCM(MP(f_j), MP(f_k)) = X^{\delta}$$

$$
\begin{aligned}
S(f_j, f_k) &= \frac{X^\delta}{Tp(f_j)} f_j - \frac{X^\delta}{Tp(f_k)} f_k \\
&= \frac{X^\delta}{d_j X^\delta} f_j - \frac{X^\delta}{d_k X^\delta} f_k \\
&= \frac{f_j}{d_j} - \frac{f_k}{d_k} \\
&= p_j - p_k
\end{aligned}
$$

entonces

$$S(f_j, f_k) = p_j - p_k \tag{2.2}$$

Como

$$\sum_{i=1}^{s} c_i d_i = 0$$

entonces en la telescópica

$$
\begin{aligned}
\sum_{i=1}^{s} c_i f_i &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots \\
&\quad + (c_1 d_1 + \cdots\cdots + c_{t-1} d_{t-1}) S(f_{t-1}, f_t)
\end{aligned}
$$

la cual es una suma de la forma deseada.

Desde p_j y p_k tienen grado δ y coeficiente principal 1 la diferencia $p_j - p_k$ tiene grado menor que δ.

Luego por la ecuación (2.2)

$$grad(S(f_j, f_k)) < \delta \quad \square$$

Teorema 2.5.2

Sea I un ideal polinomial. Entonces un generador $G = \{g_1, g_2, \ldots, g_t\}$para I es una Base de Gröbner de I si y solamente si para cada par $i \neq j$, el residuo de la división de $S(g_i, g_j)$ por G es cero.

Demostración

($\Longrightarrow$) Sea G una Base de Gröbner para I. Si $i \neq j$ entonces

$$S(g_i, g_j) = \frac{X^\delta}{Tp(g_i)} g_i - \frac{X^\delta}{Tp(g_j)} g_j \in I$$

por el corolario (2.5.1), el resto de dividir $S(g_i, g_j)$ por G es cero.

($\Longleftarrow$) Por demostrar

$$\langle Tp(I) \rangle = \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_t) \rangle$$

Basta probar que

$$Tp(f) \in \langle Tp(g_1), Tp(g_2), \ldots, Tp(g_t) \rangle \ \ \forall\, f \in I = \langle g_1, g_2, \ldots, g_t \rangle$$

Sea

$$f = \sum_{i=1}^{t} h_i g_i \quad \text{donde} \quad h_i \in \mathbf{K}[x_1, x_2, \ldots, x_n] \tag{2.3}$$

todas las posibles formas de escribirlo. Para cada una de esas formas, sea

$$\delta = \text{máx}\{m(1), m(2), \ldots, m(t)\} \ \text{ donde } \ m(i) = grad(h_i g_i)$$

por lo tanto

$$grad(f) \leq \delta \tag{2.4}$$

Se escoge una expresión para f, de tal manera que δ sea mínimo (su existencia está garantizada por ser $>$ un orden monomial en particular de buen orden).

Si se prueba que $grad(f) = \delta$, entonces $grad(f) = grad(h_i g_i) = \delta$ para algún i, luego

$$grad(f) = grad(h_i) + grad(g_i)$$

entonces $Tp(f)$ es divisible por $Tp(g_i)$ para algún i, con lo cual se tiene

$$Tp(f) \in \langle Tp(g_1), Tp(g_2), \cdots, Tp(g_t) \rangle$$

supongamos que $grad(f) < \delta$, donde δ es el mínimo encontrado. Entonces

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} Tp(h_i) g_i + \sum_{m(i)=\delta} [h_i - Tp(h_i)] g_i + \sum_{m(i)<\delta} h_i g_i \end{aligned} \tag{2.5}$$

Los monomios que aparecen en la segunda y tercera sumatoria es de grado menor que δ. Por lo tanto la suposición $grad(f) < \delta$ se reduce a que la primera sumatoria sea de grado $< \delta$.

Si $Tp(h_i) = c_i X^{\alpha(i)}$, $c_i \in \mathbf{K}$ entonces

$$\sum_{m(i)=\delta} Tp(h_i) g_i = \sum_{m(i)=\delta} c_i X^{\alpha(i)} g_i$$

Esta sumatoria cumple las condiciones del lema (2.5.1) con $f_i = X^{\alpha(i)} g_i$ entonces es una combinacón lineal de S-polinomios:

$$S(X^{\alpha(j)} g_j, X^{\alpha(k)} g_k)$$

Por definición

$$\begin{aligned} S(X^{\alpha(j)} g(j), X^{\alpha(k)} g_k) &= \frac{X^\delta}{X^{\alpha(j)} Tp(g_j)} X^{\alpha(j)} g_j - \frac{X^\delta}{X^{\alpha(k)} Tp(g_k)} X^{\alpha(k)} g_k \\ &= X^{\delta - \gamma_{jk}} S(g_j, g_k) \end{aligned}$$

donde

$$X^{\gamma_{jk}} = MCM(MP(g_j), MP(g_k))$$

Por lo tanto, existen constantes $c_{jk} \in \mathbf{K}$ tal que

$$\sum_{m(i)=\delta} Tp(h_i) g_i = \sum_{m(i)=\delta} c_{jk} X^{\delta - \gamma_{jk}} S(g_j, g_k) \tag{2.6}$$

El paso siguiente es usar la hipótesis que el resto de $S(g_j, g_k)$ en la división por $g_1, g_2, \ldots, g_t$ es cero.

Luego usando el algoritmo de división, cada S-polinomio podemos escribirlo de la forma

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i \tag{2.7}$$

donde $a_{ijk} \in \mathbf{K}[x_1, x_2, \ldots, x_n]$. Por el algoritmo de la división se tiene

$$grad(a_{ijk} g_i) \leq grad(S(g_j, g_k)), \quad \forall\, i, j, k \tag{2.8}$$

Multiplicando a la ecuación (2.7) por $X^{\delta - \gamma_{jk}}$ obtenemos

$$X^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i$$

donde

$$b_{ijk} = X^{\delta - \gamma_{jk}} a_{ijk}$$

por la ecuación (2.8) y el lema (2.5.1) implica

$$grad(b_{ijk} g_i) \leq grad(X^{\delta - \gamma_{jk}} S(g_j, g_k)) < \delta \tag{2.9}$$

sustituyendo $X^{\delta - \gamma_{jk}} S(g_j, g_k)$ en la ecuación (2.6), obtenemos

$$\begin{aligned} \sum_{m(i)=\delta} Tp(h_i) g_i &= \sum_{j,k} c_{jk} X^{\delta - \gamma_{jk}} S(g_j, g_k) \\ &= \sum_{j,k} c_{jk} \Big(\sum_{i} b_{ijk} g_i \Big) \\ &= \sum_{i} \widetilde{h}_i g_i \end{aligned}$$

El cual por la ecuación (2.9) se tiene que para todo i

$$grad(\widetilde{h}_i g_i) < \delta$$

sustituimos en la ecuación (2.5)

$$\sum_{m(i)=\delta} Tp(h_i) g_i = \sum_{i} \widetilde{h}_i g_i$$

y obtenemos una expresión para f como una combinación polinomial de los g_i donde todos tienen grado menor que δ. Esto contradice la minimalidad de δ y se completa la prueba del teorema. □

Ejemplo 2.5.3

Sea

$$I = \langle y - x^2,\ z - x^3 \rangle \subset \mathbf{R}[y, z, x]$$

un ideal con orden lexicográfico $y > z > x$. Si $G = \{y - x^2,\ z - x^3\}$ entonces G es una base de Gröbner para I. En efecto

$$\begin{aligned} S(y - x^2,\ z - x^3) &= \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) \\ &= -zx^2 + yx^3 \end{aligned}$$

Utilizando el algoritmo de la división

$$-zx^2 + yx^3 = x^3(y - x^2) + (-x^2)(z - x^3) + 0$$

así

$$\overline{S(y - x^2,\ z - x^3)}^{G} = 0$$

Entonces G es una Base de Gröbner para I.

Ahora si se usa el orden lexicográfico con $x > y > z$ veamos que G no es una Base de Gröbner para I

$$\begin{aligned} S(y - x^2,\ z - x^3) &= \frac{x^3}{(-x^2)}(y - x^2) - \frac{x^3}{(-x^3)}(z - x^3) \\ &= -xy + z \end{aligned}$$

pero al dividirlo para G

$$-xy + z = 0(y - x^2) + 0(z - x^3) + (-xy + z)$$

entonces

$$\overline{S(y - x^2,\ z - x^3)}^{G} = -xy + z \neq 0$$

2.6. Algoritmo de Buchberger

En la sección anterior, se mostró que cada ideal no nulo en $\mathbf{K}[x_1, x_2, \ldots, x_n]$ tiene una Base de Gröbner, desafortunadamente la prueba no construye una Base de Gröbner.

En esta sección se dará un algoritmo que permita apartir de un conjunto finito de generadores construir una Base de Gröbner.

.Antes de ello, veamos el ejemplo siguiente.

Ejemplo 2.6.1

Sea el anillo de polinomios en dos variables $\mathbf{K}[x, y]$ con orden monomial lexicográfico graduado

$$I = \langle f_1, f_2 \rangle, \quad f_1 = x^3 - 2xy, \quad f_2 = x^2y - 2y^2 + x$$

$$\begin{aligned} S(f_1, f_2) &= \frac{x^3y}{x^3}(x^3 - 2xy) - \frac{x^3y}{x^2y}(x^2y - 2y^2 + x) \\ &= -x^2 \end{aligned}$$

Como $S(f_1, f_2) = 0 \cdot f_1 + 0 \cdot f_2 - x^2$ entonces $G = \{f_1, f_2\}$ no es una Base de Gröbner para I.

Sea $f_3 = -x^2$ y $F = (f_1, f_2, f_3)$

Veamos si $G_1 = \{f_1, f_2, f_3\}$ es una Base de Gröbner para I.

$$\overline{S(f_1, f_2)}^F = 0$$

$$\overline{S(f_1, f_3)}^F = -2xy \neq 0$$

Sea

$$f_4 = -2xy \quad \text{y} \quad F = (f_1, f_2, f_3, f_4)$$

ahora

$$\overline{S(f_1, f_2)}^F = 0$$

$$\overline{S(f_1, f_3)}^F = 0$$

$$\overline{S(f_1, f_4)}^F = 0$$

$$\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0$$

colocando

$$f_5 = -2y^2 + x$$

y

$$F = \{f_1, f_2, f_3, f_4, f_5\} \text{ se tiene } \overline{S(f_i, f_j)}^F = 0 \text{ para } 1 \leq i < j \leq 5$$

luego F constituye una Base de Gröbner para I.

El ejemplo anterior sugiere que se puede extender un conjunto generador para formar una Base de Gröbner, por sucesivos polinomios no nulos $\overline{S(f_i, f_j)}^F$

Teorema 2.6.1 *Algoritmo de Buchberger*

Sea $f = \{f_1, f_2, \ldots, f_m\}$ un conjunto de generadores del ideal $I \subset \mathbf{K}[x_1, x_2, \ldots, x_n]$. Entonces una Base de Gröbner para I puede ser construída por un número finito de pasos por el algoritmo (3):

Demostración

Veamos que $F \subset G \subset I$ en cada etapa o fase del proceso del algoritmo.

Al inicio esto es verdadero con $G := F$ entonces $G \subset I$.

Ahora, si $G := G \cup \{g\}$, con $g = \overline{S(p, q)}^G$ como $S(p, q) \in I$ y por el algoritmo de la división se tiene que $g \in I$, entonces $G \subset I$.

Afirmación: G es un generador de I

En efecto:

Como $F \subset G$ es cualquier etapa del proceso y como F genera I, entonces G genera también I en cualquier etapa.

Algoritmo 3 Algoritmo para determinar una base de Gröbner

Entrada: $F = (f_1, f_2, \ldots, f_m)$

Salida: $G = (g_1, g_2, \ldots, g_t)$ Base de Gröbner para I con $F \subset G$

$G := F$

$B := \{(f_i, f_j) / \ f_i, f_j \in F \text{ y } f_i \neq f_j\}$

while $B \neq \emptyset$ **do**

$(p, q) :=$ un par en B

$B := B - \{(p, q)\}$

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

if $g \neq 0$ **then**

$B := B \cup \{(g, h) / \ h \in G\}$

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

end if

end while

En

$$G := F$$

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

el nuevo G consiste del anterior y de $g = \overline{S(p,q)}^{G}$, esto último me indica por el criterio de la división que ningún término principal de los elementos de G anterior dividen a cualquier término de g en particular a $Tp(g)$.

Por lo tanto si consideramos

$$\langle Tp(G) \rangle = \langle Tp(g) / \ g \in G \rangle$$

y si G' es el anterior al nuevo G, se obtiene

$$\langle Tp(G') \rangle \subsetneq \langle Tp(G) \rangle$$

debido a que

$$Tp(g) \in \langle Tp(G) \rangle \quad \text{pero} \quad Tp(g) \notin \langle Tp(G') \rangle$$

De esta forma se origina una sucesión creciente de ideales en $\mathbf{K}[x_1, x_2, \ldots, x_n]$, por lo tanto esta sucesión termina es decir en algún punto será

$$\langle Tp(G') \rangle = \langle Tp(G) \rangle$$

Se sobreentiende que $G' \subset G$. Si el último $g = \overline{S(p,q)}^{G'}$ hubiera sido $g \neq 0$ se tendría

$$\langle Tp(G') \rangle \nsubseteq \langle Tp(G) \rangle$$

pero esto no puede ser, ya que la sucesión se vuelve estacionaria.

Luego $g = 0$, por lo tanto $G' = G$.

Hasta aqui, G ya no varía, es decir ya no se le añade ningún elemento, esto ha sido posible después de un número finito de pasos. En cada paso en donde se le añade a G, B también varia, añadiendose un número finito de elementos y com B al inicio es finito, se tiene que al final en donde G ya no varia, en ese momento B consta de un número finito de elementos.

Según lo deducido todos los $g := \overline{S(p,q)}^{G}$ después que G no varia si es que existe son ceros, esto me indica que

$$B := B - \{(p,q)\}$$

se le va disminuyendo uno a uno sus elementos y como B es finito, después de un número finito de pasos, $B = \emptyset$. Por lo tanto es bucle mientras termina.

Finalmente el último G obtenido tiene la característica siguiente

$$\forall\, f, g \in G : \ \overline{S(f,g)}^{G} = 0$$

luego G es una base de Gröbner para I. □

El lema siguiente nos muestra que podemos eliminar un polinomio dentro de la Base de Gröbner de modo que no pierda dicha característica.

Lema 2.6.2

Sea G una Base de Gröbner para el ideal polinomial I. Si $p \in G$ un polinomio tal que $Tp(p) \in \langle Tp(G - \{p\})\rangle$, entonces $G - \{p\}$ es igualmente una Base de Gröbner para I.

Demostración

Como G es una Base de Gröbner para I, entonces

$$\langle Tp(I)\rangle = \langle Tp(G)\rangle$$

Afirmación:

$$\langle Tp(G - \{p\})\rangle = \langle Tp(G)\rangle$$

($\subset$) Directo desde que $G - \{p\} \subset G$.

($\supset$) Sea $Tp(g) \in TP(G)$, donde $g \in G$

(i) Si $g \neq p$ entonces

$$Tp(g) \in \langle Tp(G - \{p\})\rangle$$

(ii) Si $g = p$ por hipótesis

$$Tp(g) \in \langle Tp(G - \{p\})\rangle$$

por lo tanto se tiene

$$\langle Tp(I)\rangle = \langle Tp(G - \{p\})\rangle$$

con lo cual $G - \{p\}$ es una Base de Gröbner para I. $\square$

A continuación, se definen dos tipos de Bases de Gröbner especiales

(i) Base de Gröbner minimal.

(ii) Base de Gröbner reducida.

Definición 2.6.1

Una base de Base de Gröbner minimal para un ideal polinomial I, es una Base de Gröbner minimal G para I tal que:

(i) $cp(p) = 1$, para todo $p \in G$

(ii) $Tp(p) \notin \langle Tp(G - \{p\})\rangle$, para cada $p \in G$

Ejemplo 2.6.2

Volviendo al ejemplo (2.6.1)

$$\begin{aligned} f_1 &= x^3 - 2xy \\ f_2 &= x^2y - 2y^2 + x \\ f_3 &= -x^2 \\ f_4 &= -2xy \\ f_5 &= -2y^2 + x \end{aligned}$$

Se tiene $Tp(f_1) = (-x)Tp(f_3)$, por lo tanto podemos quitar f_1 y sigue siendo una Base de Gröbner para I.

También $Tp(f_2) = x^2y = (\frac{-1}{2}x)Tp(f_4)$, igualmente eliminemos f_2. Multiplicando adecuadamente, se obtiene coeficiente principal 1 en:

$$\begin{aligned} \widetilde{f_3} &= x^2 \\ \widetilde{f_4} &= xy \\ \widetilde{f_5} &= y^2 - \frac{1}{2}x \end{aligned}$$

asi

$$\{\widetilde{f_3}, \widetilde{f_4}, \widetilde{f_5}\}$$

es una Base de Gröbner minimal para I.

Desafortunadamente un ideal, puede tener muchas bases de Gröbner minimales. Utilizando el mismo ejemplo anterior

$$\begin{aligned} \widetilde{f_3} &= x^2 + axy \\ \widetilde{f_4} &= xy \\ \widetilde{f_5} &= y^2 - \frac{1}{2}x \end{aligned} \tag{2.10}$$

es una Base de Gröbner minimal para cualquier $a \in \mathbf{K}$.

Definición 2.6.2

Una base de Base de Gröbner reducida para un ideal polinomial $I \subset \mathbf{K}[x_1, x_2, \ldots, x_n]$, es una Base de Gröbner para I tal que:

(i) $cp(p) = 1$, para todo $p \in G$

(ii) Para cada $p \in G$, los monomios de p no pertenecen a $\langle Tp(G - \{p\})\rangle$,

Notece que en el ejemplo anterior, la Base (2.10) unicamente con $a = 0$ es reducida.

Proposición 2.6.1

Sea $I \neq \{0\}$ un ideal polinomial. Entonces para un orden monomial dado, I posee una única Base de Gröbner reducida.

Demostración

Existencia.

Se requiere construir una Base de Gröbner reducida para I, para ello se tiene el hecho que I posee una Base de Gröbner minimal G. Por simplicidad tomemos

$g \in G$ es reducida para $G \Longleftrightarrow$ ningún monomio de g está en $\langle Tp(G - \{g\})\rangle$

El objetivo es modificar G, hasta que todos sus elementos sean reducidos.

Una primera observación es que si g es reducido para G, entonces g es igualmente reducida para cualquier otra Base de Gröbner minimal de I que contiene g y tiene el mismo conjunto de términos principales.

Dada $g \in G$, sea

$$g' = \overline{g}^{G-\{g\}}$$

y

$$G' = (G - \{g\}) \cup \{g'\}$$

Se tiene que G' es una Base de Gröbner minimal de I. Para ver esto, note que

$$Tp(g') = Tp(g)$$

por cuanto al dividir g por $G - \{g\}$, $Tp(g)$ es el resto, desde que no es divisible por cualquier elemento de $Tp(G - \{g\})$.

Esto muestra que $\langle Tp(G')\rangle = \langle Tp(G)\rangle$, desde que $G' \subset I$, se deduce que G' es una Base de Gröbner.

Por la construcción dada g' es reducido por G'. Ahora se toma cada elemento de G y se aplica el proceso anterior hasta que todos los elementos sean reducidos.

La Base de Gröbner puede cambiar en cada tiempo del proceso, pero una vez que un elemento es reducido, esta permanece reducida desde que no cambia el término principal.

Asi hemos construído una Base de Gröbner reducida.

Unicidad.

Probemos la unicidad. Sean G y $\widetilde{G}$ Bases de Gröbner reducida para I. En particular G y $\widetilde{G}$ son bases de Gröbner minimales, esto implica que

$$Tp(G) = Tp(\widetilde{G})$$

En efecto:

Sea $w \in Tp(g)$ entonces

$$w = Tp(g), \quad \text{para algún } g \in G$$

luego

$$w = Tp(g) \in \langle Tp(G)\rangle = \langle Tp(\widetilde{G})\rangle = \langle Tp(I)\rangle$$

entonces

$$Tp(g) \in \langle Tp(\widetilde{G}) \rangle$$

entonces

$$\exists \widetilde{g} \in \widetilde{G} \text{ tal que } Tp(g) \text{ es divisible por } Tp(\widetilde{g}) \tag{2.11}$$

Ahora como $Tp(\widetilde{g}) \in \langle Tp(\widetilde{G}) \rangle = \langle Tp(G) \rangle$, entonces

$$\exists q \in G \text{ tal que } Tp(\widetilde{g}) \text{ es divisible por } Tp(q) \tag{2.12}$$

Si $q \neq g$ entonces por (2.11) y (2.12), $Tp(g)$ es divisible pr $Tp(q)$, siendo $g, q \in G$ esto no se puede dar, ya que

$$Tp(g) \notin \langle Tp(G - \{g\}) \rangle$$

por lo tanto $q = g$.

De (2.11) y (2.12) se tiene

$Tp(g)$ es divisible por $Tp(\widetilde{g})$ y

$Tp(\widetilde{g})$ es divisible por $Tp(g)$

como $cp(g) = cp(\widetilde{g}) = 1$ se tiene

$$Tp(g) = Tp(\widetilde{g})$$

como $w = Tp(g)$ entonces

$$w \in Tp(\widetilde{G})$$

entonces

$$Tp(G) \subset Tp(\widetilde{G})$$

de manera similar: $Tp(G) \supset Tp(\widetilde{G})$.

Por lo tanto $Tp(G) = Tp(\widetilde{G})$.

Afirmación: $G = \widetilde{G}$

($\subset$) Sea $g \in G$ arbitrario, como $Tp(G) = Tp(\widetilde{G})$ existe $\widetilde{g} \in \widetilde{G}$ tal que $Tp(g) = Tp(\widetilde{g})$ como

$$g - \widetilde{g} \in I$$

entonces

$$\overline{g - \widetilde{g}}^{G} = 0$$

por ser G Base de Gröbner.

Por otro lado como $Tp(g) = Tp(\widetilde{g})$, los términos principales en $g - \widetilde{g}$ se cancelan y como ningún término de $g - \widetilde{g}$ es divisible por $Tp(G) = Tp(\widetilde{G})$ entonces

$$\overline{g - \widetilde{g}}^{G} = g - \widetilde{g}$$

por la unicidad del resto

$$g - \widetilde{g} = 0$$

entonces

$$g = \widetilde{g}$$

($\supset$) Similarmente. $\square$

Capítulo 3

Teoría de Eliminación

En este capítulo exponemos métodos sistemáticos para eliminar variables de un sistema de ecuaciones polinomiales. La estrategia para la teoria de Eliminación está dada en dos teoremas principales: El teorema de Eliminación y el teorema de Extensión. Se probará estos teoremas usando bases de Gröbner y la teoría de resultantes.

3.1. Los teoremas de Eliminación y Extensión

Definición 3.1.1

Dada

$$I = \langle f_1, f_2, \ldots, f_s \rangle \subset \mathbf{K}[x_1, x_2, \ldots, x_n]$$

El ideal de l-ésima eliminación, denotado por I_l es el ideal de $\mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n]$ definido por

$$I_l = I \cap \mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n], \quad 0 \leq l < n$$

Debido a que I es un ideal, se comprueba que I_l es un ideal en $\mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n]$.

Teorema 3.1.1 *El Teorema de Eliminación*

Sea $I \subset \mathbf{K}[x_1, x_2, \ldots, x_n]$ un ideal y G una Base de Gröbner para I con respecto al orden lexicográfico donde $x_1 > x_2 > \cdots > x_n$. Entonces para cada $0 \leq l < n$, el conjunto

$$G_l = G \cap \mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n]$$

es una Base de Gröbner para el l-ideal de eliminación I_l

Demostración

Fijemos l entre 0 y n. Como

$$G_l = G \cap \mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n] \subset I \cap \mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n] = I_l$$

entonces $G_l \subset I_l$.

Mostraremos que

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

por doble inclusión.

($\supset$) Como $G_l \subset I_l$ entonces

$$Tp(G_l) \subset Tp(I_l)$$

entonces

$$\langle Tp(G_l) \rangle \subset \langle Tp(I_l) \rangle$$

($\subset$) Para ello unicamente necesitamos mostrar que un término principal $Tp(f)$, para $f \in I_l$ es divisible por $Tp(g)$ para algún $g \in G_l$.

Para probar esto, note que $f \in I$ ya que $I_l \subset I$.

Entonces $Tp(f)$ es divisible por $Tp(g)$ algún $g \in G$. Desde que G es Base de Gröbner para I, esto es $\langle Tp(I) \rangle = \langle Tp(G) \rangle$.

Desde que $f \in I_l$ luego $Tp(g)$ contiene únicamente las variables $x_{l+1}, \ldots, x_n$.

Como hemos usado el orden lex con $x_1 > x_2 > \ldots > x_n$, cualquier monomio conteniendo las variables $x_1, \ldots, x_l$, es mayor que todos los monomios en $\mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n]$, de este modo

$$Tp(g) \in \mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n]$$

implica

$$g \in \mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n]$$

Esto muestra que

$$g \in G \cap \mathbf{K}[x_{l+1}, x_{l+2}, \ldots, x_n] = G_l$$

luego el teorema está probado. □

Dado el ideal de elimiación I_l, llamaremos a un elemento $(a_{l+1}, \ldots, a_n) \in V(I_l)$ una solución parcial del sistema de ecuaciones originales.

Restringimos nuestra atención al caso que eliminemos la primera variable x_1. Así, queremos conocer si una solución parcial $(a_2, a_3, \ldots, a_n) \in V(I_1)$ puede extenderse para la solución $.(a_1, a_2, \ldots, a_n) \in V(I)$. El siguiente teorema nos indica cuando es posible ello.

Teorema 3.1.2 *El Teorema de Extensión*

Sea $I = \langle f_1, f_2, \ldots f_s \rangle \subset \mathbf{C}[x_1, x_2, \ldots, x_n]$ e I_1 el ideal de primera eliminación de I. Para cada $1 \leq i \leq s$, escribamos f_i en la forma

$f_i = g_i(x_2, x_3, \ldots, x_n)X_1^{N_i} +$ términos en el cual X_1 tiene grado menor que N_i

donde $N_i \geq 0$ y $g_i \in \mathbf{C}[x_2, \ldots, x_n]$ es no nulo.

Supongase que se tiene la solución parcial $(a_2, a_3, \ldots, a_n) \in V(I_1)$. Si

$$(a_2, a_3, \ldots, a_n) \notin V(g_1, \ldots, g_s)$$

Entonces

$$\text{existe} \quad a_1 \in \mathbf{C} \quad \text{tal que} \quad (a_1, a_2, \ldots, a_n) \in V(I)$$

Demostración

Se realizará en el apéndice C. □

Aunque el teorema de Extensión es únicamente para el caso de eliminación de la primera variable x_1, podemos usarla para eliminar cualquier número de variables.

Ejemplo 3.1.1

Consideremos las ecuaciones

$$\begin{aligned} x^2+y^2+z^2 &= 1 \\ xyz &= 1 \end{aligned} \tag{3.1}$$

Una Base de Gröbner para $I = \langle x^2+y^2+z^2-1, xyz-1\rangle$ con respecto al orden lex es

$$g_1 = y^4z^2+y^2z^4-y^2z^2+1$$

$$g_2 = x+y^3z+yz^3-yz$$

Por el teorema de eliminación, obtenemos

$$I_1 = I \cap \mathbf{C}[y,z] = \langle g_1\rangle$$

$$I_2 = I \cap \mathbf{C}[z] = \{0\}$$

Desde que $I_2 = \{0\}$, tenemos $V(I_2) = \mathbf{C}$, luego cada $c \in \mathbf{C}$ es una solución parcial. Nos preguntamos ¿Cuál solución parcial $c \in \mathbf{C} = V(I_2)$ se extiende a $(a,b,c) \in V(I)$?.

La idea es extender c primero a (b,c), y luego a (a,b,c). La observación crucial es que I_2 es el ideal de primera eliminación de I_1.

Aplicaremos el teorema de extensión para ir de I_2 a $I_1 = \langle g_1\rangle$. El coeficiente de y^4 en g_1 es z^2, asi $c \in \mathbf{C} = V(I_2)$ se extiende a (b,c), siempre que $c \neq 0$. Notece que la ecuación $g_1 = 0$ no tiene solución cuando $c = 0$. El siguiente paso es ir desde I_1 a I, el cual es hallar a tal que $(a,b,c) \in V(I)$. Si sustituímos $(y,z) = (b,c)$ en la ecuación (3.1), obtenemos dos ecuaciones en x, no es obvio la existencia de una solución en común $x = a$. Aqui es donde el teorema de extensión muestra su eficiencia. El coeficiente principal de x en $x^2+y^2+z^2-1$ y $xyz-1$ es 1 y yz respectivamente. Desde que 1 no es anulado el teorema de Extensión garantiza que exista a. Luego hemos probado que toda solución parcial $c \neq 0$ se extiende a $V(I)$.

El teorema de extensión es especialmente directo, cuando uno de los coeficientes principales es una constante.

Corolario 3.1.1

Sea $I = \langle f_1, \ldots, f_s \rangle \subset \mathbf{C}[x_1, \ldots, x_n]$ y asuma que para algún i, f_i es de la forma

$$f_i = cX_1^N + \text{ términos en el cual } \quad X_1 \quad \text{tiene grado menor que } \quad N$$

donde $c \in \mathbf{C}$ no nulo y $N > 0$.

Si I_1 es el ideal de primera eliminación de I y $(a_2, a_3, \ldots, a_n) \in V(I_1)$.

Entonces

$$\text{existe } \quad a_1 \in \mathbf{C} \quad \text{tal que } \quad (a_1, a_2, \ldots, a_n) \in V(I)$$

Demostración

Esta es inmediata desde el teorema de Extensión, desde que $g_i = c \neq 0$ implica $V(g_1, \ldots, g_s) = \emptyset$ luego $(a_2, \ldots, a_s) \notin V(g_1, \ldots, g_s)$ para toda solución parcial. □

3.2. La Geometría de Eliminación

Veamos una interpretación geométrica para los dos teoremas anteriores. La idea consiste en el hecho de que un ideal de eliminación corresponda a una proyección de una variedad sobre un subespacio de dimensión menor.

Sea $V = V(f_1, \ldots, f_s) \subset \mathbf{C}^n$. Para eliminar las primeras l variables $x_1, \ldots, x_l$ consideremos la proyección

$$\Pi_l : \mathbf{C}^n \longrightarrow C^{n-l}$$

$$\Pi_l(a_1, a_2, \ldots, a_n) = (a_{l+1}, \ldots, a_n)$$

Lema 3.2.1

Sea $I_l = \langle f_1, \ldots, f_s \rangle \cap \mathbf{C}[x_{l+1}, \ldots, x_n]$ el l-ideal de eliminación.

Entonces en $\mathbf{C}^{n-l}$ tenemos

$$\Pi_l(V) \subset V(I_l)$$

Demostración

Fijemos un polinomio $f \in I_l$.

Si $(a_1, \ldots, a_n) \in V$. Entonces por demostrar

$$f(a_{l+1}, \ldots, a_n) = 0$$

como

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

entonces

$$f \in I = \langle f_1, \ldots, f_s \rangle$$

y contiene únicamente variables $x_{l+1}, \ldots, x_n$. Ahora

$$0 = f(a_1, a_2, \ldots, a_n) = f(a_{l+1}, \ldots, a_n)$$

$$f(a_{l+1}, a_2, \ldots, a_n) = f(\Pi_l(a_1, \ldots, a_n)) = 0 \quad \square$$

Usando el lema (3.2.1) podemos escribir $\Pi_l(V)$:

$$\Pi_l(V) = \{(a_{l+1}, a_2, \ldots, a_n) \in V(I_l) : \text{ existan } a_1, \ldots, a_l \in \mathbf{C} \text{ con } (a_1, a_2, \ldots, a_n) \in V\}$$

De este modo $\Pi_l(V)$ consiste exactamente de las soluciones parciales que se extienden a soluciones completas.

Teorema 3.2.2

Dado $V = V(f_1, \ldots, f_s) \subset \mathbf{C}^n$. Sea g_i como en el teorema (3.1.2). Si I_1 es el ideal de primera eliminación de $\langle f_1, \ldots, f_s \rangle$, entonces en $\mathbf{C}^{n-1}$ tenemos

$$V(I_1) = \Pi_1(V) \cup (V(g_1, \ldots, g_s) \cap V(I_1))$$

donde $\Pi_1 : \mathbf{C}^n \longrightarrow \mathbf{C}^{n-1}$ es la proyección sobre las últimas $n-1$ componentes.

Demostración

Por doble contenido

($\subset$) Sea $(a_2, \ldots, a_n) \in V(I_1)$. Supongase que

$$(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_s) \cap V(I_1)$$

entonces

$$(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_s)$$

luego, por el teorema de extensión, existe $a_1 \in \mathbf{C}$ tal que

$$(a_1, a_2, \ldots, a_n) \in V(I)$$

luego

$$(a_2, \ldots, a_n) \in \Pi_1(V)$$

($\supset$) Sea $(a_1, \ldots, a_n) \in \Pi_1(V) \cup (V(g_1, \ldots, g_s) \cap V(I_1))$. Si $(a_2, \ldots, a_n) \in \Pi_1(V)$. Por el lema (3.2.1)

$$(a_2, \ldots, a_n) \in V(I_1)\cdot$$

Por otro lado, si $(a_2, \ldots, a_n) \in V(g_1, \ldots, g_s) \cap V(I_1)$, entonces

$$(a_2, \ldots, a_n) \in V(I_1) \quad \square$$

Lo siguiente es la versión geométrica del corolario (3.1.1).

Corolario 3.2.1

Sea $V = V(f_1, \ldots, f_s) \subset \mathbf{C}^n$ y asuma que para algún i, f_i es de la forma

$$f_i = cX_1^N + \text{ términos en el cual } \quad X_1 \quad \text{tiene grado menor que } \quad N$$

donde $c \in \mathbf{C}$ es no nulo y $N > 0$.

Si I_1 es el ideal de primera eliminación, entonces en $\mathbf{C}^{n-1}$

$$\Pi_1(V) = V(I_1)$$

donde Π_1 es la proyección en las $n-1$ últimas componentes.

Observación 3.2.1

Una observación final es que el teorema de extensión es verdadero sobre cuaquier campo algebraicamente cerrado. No se ha requerido en cada una de las demostraciones de cualidades propias de $\mathbf{C}$ que no sean las de un campo algebraicamente cerrado.

Capítulo 4

El Algebra y la Geometría

En este capítulo exploraremos la correspondencia entre los ideales y las variedades. Aqui mismo se dará el fundamento teórico para las aplicaciones finales.

En el presente capítulo se ha dividido en cuatro secciones.

Sección 1: En esta parte probaremos el célebre teorema de los ceros de Hilbert Nullstellensatz.

Sección 2: Se definirá un ideal radical y el radical de un ideal y exploraremos un relación entre ellas. Daremos el fundamento para resolver el problema de la pertenencia para el radical de un ideal.

Sección 3: Se verá algunas operaciones con ideales : Adición, producto e intersección, con el fin de resolver el problema de determinar la intersección de dos ideales en $\mathbf{K}[x_1, \ldots, x_n]$.

Sección 4: Veremos también el problema de determinar un generador para el ideal cociente.

4.1. Teorema de los ceros de Hilbert.

Teorema 4.1.1

Sea K un cuerpo algebraicamente cerrado, I un ideal en $\mathbf{K}[x]$. Si $V(I) = \emptyset$.

Entonces I es igual al anillo, es decir $I = \mathbf{K}[x]$

Demostración

Ya que $\mathbf{K}[x]$ es un dominio de ideales principales (DIP). Entonces

$$\exists\ f \in \mathbf{K}[x] \ \text{ tal que } \ I = \langle f \rangle$$

Debido a que f no es el polinomio nulo (ya que si $f = 0$ entonces I sería el ideal nulo), entonces

$$f = k, \quad \text{donde} \quad k \in \mathbf{K}$$

En efecto, si f no fuese un polinomio constante, como K es un campo algebraicamente cerrado

$$\exists\ \alpha \in \mathbf{K} \ \text{ tal que } \ f(\alpha) = 0$$

luego $\alpha \in V(I)$ con lo cual $V(I) \neq \emptyset$ que es contradictorio a nuestra hipótesis.

Por lo tanto f es un polinomio constante no nulo, es decir $f \in \mathbf{K}$ entonces

$$1 = f^{-1} f \in I$$

luego

$$I = \mathbf{K}[x] \quad \square$$

Note que si $\mathbf{K}$ no es algún cerrado (4.1.1) no es cierto. Por ejemplo considere $I = \langle 1 + x^2 \rangle \subset \mathbf{R}[x]$. Se tiene $V(I) = \emptyset$, para $I \neq \mathbf{R}[x]$, esto es porque $\mathbf{R}$ no es algebraicamente cerrado.

Este resultado se extiende a un anillo $\mathbf{K}[x_1, \ldots, x_n]$ de n variables, como se expresa en el siguiente teorema.

Teorema 4.1.2

Sea K un campo algebraicamente cerrado y sea $I \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal con $V(I) = \emptyset$. Entonces

$$I = \mathbf{K}[x_1, \ldots, x_n]$$

Demostración

Basta demostrar que el polinomio constante 1 está en I.
La prueba es por inducción sobre el número de variables n.

(i) Si $n = 1$ se tiene un ideal I en $\mathbf{K}[x]$ con $V(I) = \emptyset$ entonces por el teorema (4.1.1) $I = \mathbf{K}[x]$

(ii) Asumiendo que el resultado es verdadero para anillos polinomiales de $n-1$ variables $\mathbf{K}[x_2, \ldots, x_n]$.

(iii) Sea $I = \langle f_1, \ldots, f_s \rangle \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal arbitrario para el cual $V(I) = \emptyset$.

Podemos asumir que f_1 no es un polinomio constante, pues, caso contrario $1 \in I$, $I = \mathbf{K}[x_1, \ldots, x_n]$.

Supongamos que f_1 tiene grado $N \geq 1$. El siguiente cambio de coordenadas para f_1 hace que tenga una forma muy especial. En concreto, considerando

$$\begin{aligned} x_1 &= \widetilde{x}_1 \\ x_2 &= \widetilde{x}_2 + a_2\widetilde{x}_1 \\ &\vdots \\ x_n &= \widetilde{x}_n + a_n\widetilde{x}_1 \end{aligned} \tag{4.1}$$

donde los a_i son constantes en $\mathbf{K}$ todavia no determinadas. Teniendo en cuenta la forma general de un polinomio y el binomio de Newton, al reemplazar (4.1) en f_1, se tiene

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= f_1(\widetilde{x}_1, \widetilde{x}_2 + a_2\widetilde{x}_1, \ldots, \widetilde{x}_n + a_n\widetilde{x}_1) \\ &= C(a_2, \ldots, a_n)\widetilde{x}_1^N + \text{términos en el cual } \widetilde{x}_1 \text{ tiene grado menor que } N \end{aligned}$$

Para mostrar que $C(a_2, \ldots, a_n)$ es un polinomio evaluado en $a_2, \ldots, a_n$ no nulo, necesitamos de

Afirmación 1.

Sea $h(x_1, \ldots, x_n)$ un polinomio homogéneo. Entonces h es un polinomio nulo en $\mathbf{K}[x_1, \ldots, x_n] \iff h(1, x_2, \ldots, x_n)$ es un polinomio nulo en $K[x_2, \ldots, x_n]$

En efecto

($\Longrightarrow$) Por evaluación se tiene lo pedido.

($\Longleftarrow$) Debido a que h es homogéneo, cada término tiene el mismo grado y debe observarse que al suprimir la variable x_1, haciendo $h(1, x_2, \ldots, x_n)$, no se obtiene términos semejantes, (esto es, términos que se puedan sumar o restar unos con otros) y como $h(1, x_2, \ldots, x_n)$ es nulo por hipótesis, cada uno de sus coeficientes que son los mismos en $h(x_1, \ldots, x_n)$ son nulos. Luego $h(x_1, x_2, \ldots, x_n)$ es un polinomio nulo.

Ahora si consideramos

$$f = h_N + h_{N-1} + \cdots + h_0$$

donde cada h_i es un polinomio homogéneo no nulo. Entonces $h_N(1, x_2, \ldots, x_n)$ es no nulo debido a la afirmación anterior.

También se nota que

$$h_N(1, x_2, \ldots, x_n) = C(a_2, \ldots, a_n)$$

entonces $C(a_2, \ldots, a_n)$ es no nulo.

Por otro lado, si un campo algebraicamente cerrado fuese finito

$$K = \{\alpha_1, \ldots, \alpha_s\}$$

podemos construir un polinomio no constante en $\mathbf{K}[x]$

$$p = (x - \alpha_1) \ldots (x - \alpha_s) + 1$$

el cual no tiene raices en $\mathbf{K}$. Por lo tanto , todo campo algebraico cerrado es infinito.

Utilizando estos resultados en la proposición (1.1.1), nos origina la existencia de $a_2, \ldots, a_n$ en K de tal manera que $C(a_2, \ldots, a_n) \neq 0$.

Con estos valores fijos en $\mathbf{K}$ para $a_2, \ldots, a_n$ y mediante el cambio (4.1) se obtiene

$$f \in \mathbf{K}[\widetilde{x}_1, \ldots, \widetilde{x}_n] \quad \text{donde} \quad f \in \mathbf{K}[x_1, \ldots, x_n]$$

Sea $\widetilde{I} = \{\widetilde{f} : \ f \in I\}$

Afirmación 2.

$\widetilde{I}$ es un ideal en $\mathbf{K}[\widetilde{x}_1, \ldots, \widetilde{x}_n]$

En efecto

Como $0 \in I$ entonces $0 \in \widetilde{I}$ ya que el cambio de coordenadas no le afecta.

Sea $\widetilde{f}, \widetilde{g} \in \widetilde{I}$ donde $f, g \in I$ entonces

$$f + g \in I$$

como $\widetilde{f+g} = \widetilde{f} + \widetilde{g}$ entonces

$$\widetilde{f} + \widetilde{g} \in \widetilde{I}$$

de igual forma, si $\widetilde{f} \in \widetilde{I}$ con $f \in I$ y sea $\widetilde{h} \in \mathbf{K}[\widetilde{x}_1, \ldots, \widetilde{x}_n]$ luego existe $h \in \mathbf{K}[x_1, \ldots, x_n]$ de tal forma que al hacer el cambio (4.1) se obtiene $\widetilde{h}$ como $hf \in I$ entonces

$$\widetilde{hf} = \widetilde{h}\widetilde{f} \in I$$

De este modo se ha demostrado que $\widetilde{I}$ es un ideal en $\mathbf{K}[\widetilde{x}_1, \ldots, \widetilde{x}_n]$.

Si $V(\widetilde{I}) \neq \emptyset$ entonces existirá una n-upla que anula a todo $\widetilde{I}$ por (4.1) se puede conseguir una n-upla que anularía a todo I, por lo tanto $V(I) \neq \emptyset$ y esto va en contra de nuestra hipótesis general. Por lo tanto $V(\widetilde{I}) = \emptyset$.

Además si demostramos que $1 \in \widetilde{I}$ entonces $1 \in I$ debido a que las constantes no son afectadas por la operación $\widetilde{\ }$. De aqui es suficiente probar que $1 \in \widetilde{I}$.

Por lo anterior $f_1 \in I$, se transforma en $\widetilde{f}_1 \in \widetilde{I}$ con la propiedad

$\widetilde{f}_1(\widetilde{x}_1, \ldots, \widetilde{x}_n) = C(a_2, \ldots, a_n)\widetilde{x}_1^N +$ términos en el cual $\widetilde{x}_1$ tiene grado menor que N

Donde $C(a_2, \ldots, a_n) \neq 0$.

Esto nos permite utilizar el corolario (3.2.1), para $V(\widetilde{I})$ con la proyección dentro del subespacio con coordenadas $\widetilde{x}_2, \ldots, \widetilde{x}_n$. Como se observó en el capítulo 3, el teorema de Extensión y su corolario está dada sobre cualquier campo algebraicamente cerrado.

Sea $\Pi_1 : K^n \longrightarrow K^{n-1}$ la aplicación proyección dentro de las $n-1$ últimas componentes.

Si $\widetilde{I}_1 = \widetilde{I} \cap \widetilde{K}[\widetilde{x}_2, \ldots, \widetilde{x}_n]$ entonces por el corolario (3.2.1)

$$V(\widetilde{I}_1) = \Pi_1(V(\widetilde{I}))$$

Entonces

$$V(\widetilde{I}_1) = \Pi_1(V(\widetilde{I})) = \Pi_1(\emptyset) = \emptyset$$

luego $V(\widetilde{I}_1) = \emptyset$ en este punto utilizaremos la hipótesis inductiva, se tiene

$$\widetilde{I}_1 = \mathbf{K}[\widetilde{x}_2, \ldots, \widetilde{x}_n]$$

entonces $1 \in \widetilde{I}_1 \subset \widetilde{I}$ entonces $1 \in \widetilde{I}$ y esto completa la prueba. □

En el caso especial cuando $\mathbf{K} = \mathbf{C}$ es decir el cuerpo son los complejos, el anterior teorema es visto como, El teorema fundamental del Algebra para polinomios en varias variables, que indica: Cada sistema de polinomios que generan un ideal propio de $\mathbf{C}[x_1, \ldots, x_n]$, tiene una raíz común en $\mathbf{C}$.

El teorema (4.1.2) nos permite resolver la situación siguiente: ¿Cuándo un sistema

$$\begin{aligned} f_1 &= 0 \\ f_2 &= 0 \\ &\vdots \\ f_s &= 0 \qquad \text{donde} \qquad f_i \in \mathbf{C}[x_1, \ldots, x_n] \end{aligned}$$

de ecuaciones polinomiales tiene solución común en $\mathbf{C}^n$?

Es claro que el sistema anterior no posee un cero en común si y solo si

$$V(f_1, \ldots, f_s) = \emptyset$$

Pero por el teorema

$$V(f_1, \ldots, f_s) = \emptyset \Longleftrightarrow 1 \in \langle f_1, \ldots, f_s \rangle$$

De esta manera el problema de consistencia de un sistema de ecuaciones polinomiales, se reduce a determinar cuando 1 pertenece al ideal generado por dichos polinomios. Esto se debe a que cualquier orden monomial, $\{1\}$ es la única Base de Gröbner reducida para el ideal $\langle 1 \rangle$.

Probemos esto último. Sea $\{g_1, \ldots, g_t\}$ una Base de Gröbner para $I = \langle 1 \rangle$. Asi $1 \in \langle Tp(I) \rangle = \langle Tp(g_1), \ldots, Tp(g_t) \rangle$ implica que 1 es divisible por algún $Tp(g_i)$, esto fuerza a que $Tp(g_i)$ es una constante y como cada uno de los otros $Tp(g_j)$ es multiplo de dicha constante, podemos removerlo de la Base de Gröbner a los otros g_j por el lema (2.6.2).

Finalmente $Tp(g_i)$ es una constante, esto hace que para cualquier orden monomial g_i sea una constante, multiplicando por su inversa en $\mathbf{K}$, se obtiene que $\{1\}$ es una Base de Gröbner reducida para $\langle 1 \rangle$.

Teorema 4.1.3 *Hilbert's Nullstellensatz*

Sea K un campo algebraico cerrado.

Si $f, f_1, \ldots, f_s \in \mathbf{K}[x_1, \ldots, x_n]$ de tal manera que $f \in I(V(f_1, \ldots, f_s))$.

Entonces, existe un entero $m \geq 1$ tal que

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

y viceversa.

Demostración

($\Longrightarrow$) Dada un polinomio f el cual se anula para cada cero en común de los polinomios $f_1, f_2, \ldots, f_s$ mostraremos que existe un entero $m \geq 1$ y polinomios $A_1, \ldots, A_s$ tal que

$$f^m = \sum_{i=1}^{s} A_i f_i$$

Considerando el ideal

$$\widetilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset \mathbf{K}[x_1, \ldots, x_n, y]$$

donde $f_1, f_2, \ldots, f_s$ son los dados en la hipótesis.

Se cumple que

$$V(\widetilde{I}) = \emptyset$$

En efecto:

Sea $(a_1, \ldots, a_n, a_{n+1}) \in \mathbf{K}^{n+1}$ arbitrario.

Por demostrar que

$$(a_1, \ldots, a_n, a_{n+1}) \notin V(\widetilde{I})$$

Entonces $(a_1, \ldots, a_n)$ es un cero en común de $f_1, \ldots, f_s$ o $(a_1, \ldots, a_n)$ no lo es.

En el primer caso, $f(a_1, \ldots, a_n) = 0$, debido a que f es un polinomio que se anula en cualquier cero en común de $f_1, \ldots, f_s$.

Asi el polinomio $1 - yf$ toma su evaluación

$$1 - a_{n+1} f(a_1, \ldots, a_n) = 1$$

para cualquier punto $(a_1, \ldots, a_n, a_{n+1})$, en particular $(a_1, \ldots, a_n, a_{n+1}) \notin V(\widetilde{I})$.

En el segundo caso, para algún i, $1 \leq i \leq s$, se tiene

$$f_i(a_1, \ldots, a_n) \neq 0$$

Si pensamos que f_i es una función de $n + 1$ variables el cual no depende de la última variable, se tiene

$$f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$$

En particular, se obtiene

$$(a_1, \ldots, a_n, a_{n+1}) \notin V(\widetilde{I})$$

Siendo $(a_1, \ldots, a_n, a_{n+1}) \in \mathbf{K}^{n+1}$ arbitrario, se concluye que

$$V(\widetilde{I}) = \emptyset$$

Entonces por el teorema (4.1.2) $\widetilde{I} = \mathbf{K}[x_1, \ldots, x_n, y]$, luego $1 \in \widetilde{I}$, esto es

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf) \tag{4.2}$$

para algunos polinomios p_i, $q \in \mathbf{K}[x_1, \ldots, x_n, y]$

Se coloca

$$y = \frac{1}{f(x_1, \ldots, x_n)}$$

entonces la relación (4.2) implica

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, \frac{1}{f}) f_i$$

Multiplicando ambos lados de la ecuación por una potencia f^m donde m es lo suficientemente grande para cancelar todos los denominadores.

Esto implica que

$$f^m = \sum_{i=1}^{s} A_i f_i$$

para algunos polinomios $A_i \in \mathbf{K}[x_1, \ldots, x_n]$

($\Longleftarrow$) Para la segunda parte de la demostración se tiene la existencia de un entero $m \geq 1$ tal que

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

entonces existen $A_1, \ldots, A_s \in \mathbf{K}[x_1, \ldots, x_n]$ tal que

$$f^m = \sum_{i=1}^{s} A_i f_i \tag{4.3}$$

Sea $x \in V(f_1, \ldots, f_s)$ arbitrario entonces

$$f_i(x) \doteq 0 \quad \text{para todo } i, \quad 1 \leq i \leq s$$

De la ecuación (4.3)

$$(f^m)(x) = \sum_{i=1}^{s} A_i(x) f_i(x)$$

entonces

$$f^m(x) = 0$$

Luego se tiene

$$f(x) = 0$$

Por lo tanto

$$f \in I(V(f_1, \ldots, f_s)) \quad \square$$

4.2. Ideal radical y radical de un ideal

Lema 4.2.1

Sea V una variedad. Si $f^m \in I(V)$, entonces $f \in I(V)$.

Demostración

Sea $x \in V$ arbitrario. Si $f^m \in I(V)$, entonces $(f(x))^m = 0$, desde que $\mathbf{K}$ es un dominio de integridad se obtiene $f(x) = 0$, entonces $f \in I(V)$ $\square$

Esto nos permite dar la siguiente definición

Definición 4.2.1

Sea I un ideal en $\mathbf{K}[x_1, \ldots, x_n]$. I es un ideal radical (o simplemente radical), si $f^m \in I$ implica que $f \in I$.

Según el lema (4.2.1), $I(V)$ es un ideal radical y lo enunciaremos en el corolario siguiente

Corolario 4.2.1

$I(V)$ es un ideal radical.

Demostración

Usando el lema (4.2.1).

Definición 4.2.2

Sea $I \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal. El radical de I, denotado por $\sqrt{I}$ es el conjunto

$$\{f \in \mathbf{K}[x_1, \ldots, x_n] / \ f^m \in I \text{ para algún entero } \ m \geq 1\}$$

De la definición (4.2.2) se deduce que $I \subset \sqrt{I}$ es decir todo ideal está contenido en su radical, desde que $f \in I$ implica $f^1 \in I$ entonces $f \in \sqrt{I}$.

El lema siguiente nos muestra que: Si I es un ideal. I es radical $\Longleftrightarrow I = \sqrt{I}$.

Lema 4.2.2

Si I es un ideal en $\mathbf{K}[x_1, \ldots, x_n]$ entonces

(i) $\sqrt{I}$ es un ideal en $\mathbf{K}[x_1, \ldots, x_n]$ conteniendo I.

(ii) $\sqrt{I}$ es un ideal radical.

(iii) I es radical $\Longleftrightarrow I = \sqrt{I}$.

Demostración

(i) Sea $f, g \in \sqrt{I}$ entonces existen enteros m y l tal que $f^m, \ g^l \in I$. En la expansión binomial de $(f+g)^{m+l-1}$ cada término tiene un factor $f^i g^j$ con $i+j = m+l-1$. Desde que $i \geq m$ o $j \geq l$ se tiene f^i o g^j está en I. Entonces $f^i g^j \in I$ y como cada término de la expansión binomial está en I se tiene

$$(f+g)^{m+l-1} \in I$$

por lo tanto

$$f+g \in \sqrt{I}$$

Finalmente, supongase que $f \in \sqrt{I}$ y $h \in \mathbf{K}[x_1, \ldots, x_n]$.

Entonces $f^m \in I$ para algún entero $m \geq 1$.

Desde que I es un ideal, se tiene

$$(hf)^m = h^m f^m \in I$$

entonces $hf \in \sqrt{I}$

Por lo tanto queda probado que $\sqrt{I}$ es un ideal.

(ii) Para mostrar que $\sqrt{I}$ es un ideal radical. Sea $f^m \in \sqrt{I}$ para $m \geq 1$ arbitrariamente dado.

Por demostrar que $f \in \sqrt{I}$. En efecto como $f^m \in \sqrt{I}$, existe $s \geq 1$ tal que $(f^m)^s \in I$ luego $f^{ms} \in I$ con lo cual $f \in \sqrt{I}$.

(iii)($\Longrightarrow$) Sea I un ideal radical. Para probar $I = \sqrt{I}$ basta ver que $\sqrt{I} \subset I$. En efecto sea $f \in \sqrt{I}$ entonces $f^m \in I$ para algún $m \geq 1$ entero, como I es un radical, se tiene $f \in I$.

($\Longleftarrow$) Sabiendo que $I = \sqrt{I}$. Se tiene que I es un ideal radical.

En efecto:

Sea

$$f^m \in I$$

entonces

$$f^m \in \sqrt{I}$$

entonces

$$f^{ms} \in I, \quad \text{para algún} \quad s \geq 1$$

luego $f \in \sqrt{I}$ entonces como $\sqrt{I} = I$, $f \in I$ $\square$.

Teorema 4.2.3

Sea K un cuerpo algebraicamente cerrado. Si I es un ideal en $\mathbf{K}[x_1, \ldots, x_n]$, entonces

$$I(V(I)) = \sqrt{I}$$

Demostración

Se demostrará por doble inclusión.

($\subset$) Sea $f \in I(V(I))$, entonces f es anulado en $V(I)$. Por el teorema (4.1.3) existe un entero $m \geq 1$ tal que $f^m \in I$, con lo cual $f \in \sqrt{I}$.

Asi $I(V(I)) \subset \sqrt{I}$.

($\supset$) Sea $f \in \sqrt{I}$ entonces $f^m \in I$ para algún $m \geq 1$.

Luego f^m es anulado en $V(I)$, con lo cual f es anulado en $V(I)$, de este modo $f \in I(V(I))$. Por lo tanto $I(V(I)) \supset \sqrt{I}$ $\square$

Una relación entre el algebra y la geometría está contenida en el teorema siguiente.

Teorema 4.2.4

Sea K un campo arbitrario.

(i) Sean I_1, I_2 dos ideales en $K[x_1, \ldots, x_n]$. Entonces si $I_1 \subset I_2$ entonces $V(I_1) \supset V(I_2)$

(ii) Sean V_1, V_2 dos variedades en K^n. Si $V_1 \subset V_2$ entonces $I(V_1) \supset I(V_2)$.

(iii) Sea V una variedad en K^n entonces

$$V(I(V)) = V$$

(iv) Sea K un campo algebraicamente cerrado. Si I es un ideal radical entonces $I(V(I)) = I$.

Demostración

(i) Sea $x \in V(I_2)$ entonces

$$f(x) = 0 \quad \forall f \in I_2$$

como $I_1 \subset I_2$ entonces en particular,

$$\forall\ f \in I_1, \quad f(x) = 0$$

luego $x \in V(I_1)$

(ii) Sea $f \in I(V_2)$, luego

$$f(x) = 0 \quad \text{para todo} \quad x \in V_2$$

debido a que $V_1 \subset V_2$, se tiene

$$f(x) = 0, \ \forall x \in V_1$$

entonces $f \in I(V_1)$.

(iii) Sea V una variedad entonces

$$V = V(f_1, \ldots, f_s)$$

Notece que $f_1, \ldots, f_s \in I(V)$ entonces

$$\langle f_1, \ldots, f_s \rangle \subset I(V)$$

por lo tanto

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

entonces $V(I(V)) \subset V$.

Veamos la otra inclusión.

Sea $x \in V$ arbitrario y $f \in I(V)$ como f es anulado por V en particular por $x \in V$ $f(x) = 0$. Entonces

$$x \in V(I(V))$$

con lo cual $V \subset V(I(V))$ y se tiene

$$V(I(V)) = V$$

(iv) Por el teorema (4.2.3), $I(V(I)) = \sqrt{I}$, por el lema (4.2.2) (iii), se tiene $I = \sqrt{I}$ siendo I un ideal radical, con lo cual

$$I(V(I)) = I \quad \square$$

En esta parte se pretende resolver el problema de pertenencia en un radical de un ideal, es decir cuando $f \in \sqrt{I}$, necesitaríamos encontrar un $m > 0$, tal que $f^m \in I$. Esto es un trabajo muy arduo. Afortunadamente podemos adaptar la prueba de Hilbert's Nullstellensatz, para dar un algoritmo, para determinar cuando $f \in \sqrt{\langle f_1, \ldots, f_s \rangle}$.

Proposición 4.2.1

Sea K un campo arbitrario, $I = \langle f_1, \ldots, f_s \rangle \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal. Entonces $f \in \sqrt{I}$ si y solo si la constante polinomial 1 pertenece al ideal

$$\widetilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset \mathbf{K}[x_1, \ldots, x_n, y]$$

es decir $\widetilde{I} = \mathbf{K}[x_1, \ldots, x_n, y]$

Demostración

($\Longrightarrow$) Sea $f \in \sqrt{I}$ entonces $f^m \in I \subset \widetilde{I}$, para algún entero positivo m.

También se tiene

$$1 - yf \in \widetilde{I}$$

por lo tanto

$$\begin{aligned} 1 &= y^m f^m + (1 - y^m f^m) \\ &= y^m f^m + (1 - yf)(1 + yf + \cdots + y^{m-1} f^{m-1}) \in \widetilde{I} \end{aligned}$$

luego $1 \in \widetilde{I}$

($\Longleftarrow$) Sabiendo que

$$1 \in \widetilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle$$

entonces

$$1 = \sum_{i=1}^{s} h_i(x_1, \ldots, x_n, y) f_i + p(x_1, \ldots\ldots, x_n, y)(1 - fy)$$

reeplazando

$$y = \frac{1}{f(x_1, \ldots, x_n)}$$

y multplicando a toda la ecuación por una potencia de f que hace posible eliminar todos los denominadores, para luego tener

$$f^m = \sum_{i=1}^{s} A(x_1, \ldots, x_n) f_i, \text{ para algún } m \geq 0$$

entonces $f^m \in I$, por lo tanto $f \in \sqrt{I}$ $\square$

Ejemplo 4.2.1

Como un ejemplo consideremos el ideal

$$I = \langle xy^2 + 2y^2,\ x^4 - 2x^2 + 1 \rangle \in \mathbf{K}[x, y]$$

Sea $f = y - x^2 + 1$. Usando el orden lexicográfico en $\mathbf{K}[x, y, z]$ el ideal

$$\widetilde{I} = \langle xy^2 + 2y^2,\ x^4 - 2x^2 + 1,\ 1 - z(y - x^2 + 1) \rangle \subset \mathbf{K}[x, y, z]$$

tiene com base de Gröbner reducida a $\{1\}$. Luego se reduce por la proposición (4.2.1) que

$$y - x^2 + 1 \in \sqrt{I}$$

usando el algoritmo de la división se puede describir que potencia de $y - x^2 + 1$ pertenece a I:

$$\begin{aligned} \overline{y - x^2 + 1}^G &= y - x^2 + 1 \\ \overline{(y - x^2 + 1)^2}^G &= -2x^2y + 2y \\ \overline{(y - x^2 + 1)^3}^G &= 0 \end{aligned}$$

donde $G = \{x^4 - 2x^2 + 1,\ y^2\}$ es una base de Gröbner para I con respecto al orden lex y $\overline{p}^G$ es el resto de dividir p entre G. Por lo tanto

$$(y - x^2 + 1)^3 \in I$$

y no existe una potencia menor de $y - x^2 + 1$ que esté en I (en particular $y - x^2 + 1 \notin I$).

4.3. Suma, producto e intersección de ideales

Los ideales son objetos algebraicos, que se pueden con ellos generar nuevos objetos mediante operaciones algebraicas naturales.

En esta sección consideraremos tres de ellas: Suma, intersección y producto. Ellas son operaciones binarias donde para cada par de ideales, ella asocia un nuevo ideal.

Estamos interesados en que dados los generadores de un par de ideales, calcular los generadores de los nuevos ideales.

En partcular, se dará un algoritmo que nos permitirá calcular la intersección de ideales.

4.3.1. Suma de Ideales

Definición 4.3.1

Sea I, J dos ideales en el anillo $\mathbf{K}[x_1, \ldots, x_n]$, entonces la suma de I y J, denotado por $I + J$, está definido por

$$I + J = \{f + g / \ f \in I, \ g \in J\}$$

Proposición 4.3.1

Si I y J son ideales en $\mathbf{K}[x_1, \ldots, x_n]$ entonces $I+J$ es igualmente un ideal en $\mathbf{K}[x_1, \ldots, x_n]$. También $I + J$ es el ideal más pequeño (con respecto a la inclusión) que contenga a I y J.

Además, si

$$I = \langle f_1, \ldots, f_r \rangle \quad \text{y} \quad J = \langle g_1, \ldots, g_s \rangle$$

entonces

$$I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$$

Demostración

Es directo que $I + J$ es un ideal más pequeño que contenga a I y J. También $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$ $\square$

Como un resultado particular de la proposición (4.3.1), lo enunciamos en el corolario siguiente.

Corolario 4.3.1

Si $f_1, \ldots, f_r \in \mathbf{K}[x_1, \ldots, x_n]$ entonces

$$\langle f_1, \ldots, f_r \rangle = \langle f_1 \rangle + \langle f_2 \rangle + \cdots + \langle f_r \rangle$$

Ejemplo 4.3.1

Sea $I = \langle x^2 + y \rangle$, $J = \langle z \rangle$ ideales en $\mathbf{R}[x, y, z]$.

Fig.(1) $V(I) = V(x^2 + y)$

Fig.(2) $V(J) = V(z)$

Por la proposición (4.3.1), $I + J = \langle x^2 + y,\ z \rangle$. Así la variedad $V(I + J)$ consiste en todos los puntos donde $x^2 + y$ y z se anulan, la cual es la intersección de $V(I)$ y V(J).

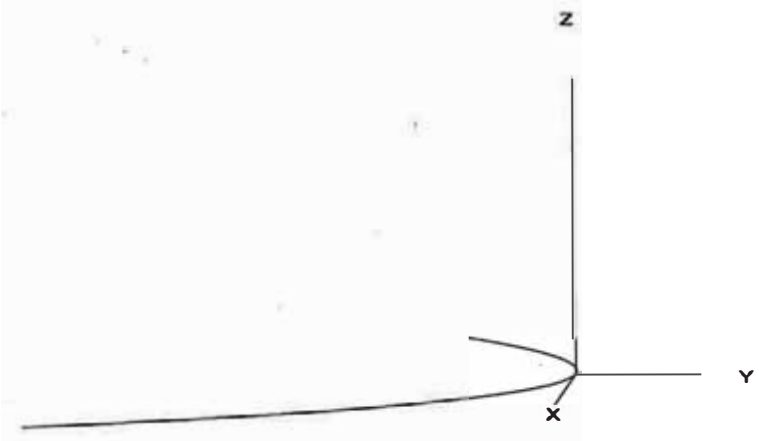


Fig.(3) $V(I + J) = V(x^2 + y, z) = V(I) \cap V(J)$

Generalizamos esta cualidad.

Teorema 4.3.1

Sean I, J dos ideales en $\mathbf{K}[x_1, \ldots, x_n]$, entonces

$$V(I + J) = V(I) \cap V(J)$$

Demostración

($\subset$) Sea $x \in V(I + J)$, luego

$$h(x) = 0, \ \forall h \in I + J$$

como $I \subset I + J$ se tiene en particular

$$h(x) = 0, \ \forall h \in I$$

entonces $x \in V(I)$.

De manera similar se obtiene $x \in V(J)$, con la cual $x \in V(I) \cap V(J)$.

($\supset$) Sea $x \in V(I) \cap V(J)$.

Sea

$$h = f + g \in I + J, \ \text{ donde } \ f \in I \ \text{ y } \ g \in J$$

Se tiene $f(x) = 0$, ya que $x \in V(I)$ también $g(x) = 0$ porque $x \in V(J)$.

Asi se tiene $h(x) = f(x) + g(x) = 0 + 0 = 0$. Concluímos que $x \in V(I + J)$ $\square$

Si $V = V(f_1, \ldots, f_r)$, $W = V(g_1, \ldots, g_s)$ variedades afines en $\mathbf{K}^n$.
Entonces

$$V \cap W = V(f_1, \ldots, f_r, g_1, \ldots, g_s)$$

$$V \cup W = V(f_i g_j / \ 1 \leq i \leq r, \ \ 1 \leq j \leq s)$$

Es un resultado análogo al dado en el capítulo 1.

4.3.2. Producto de Ideales

En el capítulo 1 encontramos que el ideal generado por el producto de los generadores de dos ideales corresponde a la unión de variedades.

$$V(f_1,\ldots,f_r)\cup V(g_1,\ldots,g_s)=V(f_ig_j,\ \ 1\le i\le r,\ 1\le j\le s)$$

por ejemplo la variedad $V(xz,yz)$ corresponde al ideal generado por el producto de los generadores de los ideales $\langle x,y\rangle$ y $\langle z\rangle$ en $\mathbf{K}[x,y,z]$ es la unión de $V(x,y)$ (eje Z) y $V(z)$ (plano XY). Esto sugiere la siguiente definición.

Definición 4.3.2

Si I, J son dos ideales en $\mathbf{K}[x_1,\ldots,x_n]$ entonces el producto denotado por IJ es definido como el ideal generado por todos los polinomios fg donde $f\in I$ y $g\in J$.

Proposición 4.3.2

Sea $I=\langle f_1,\ldots,f_r\rangle$ y $J=\langle g_1,\ldots,g_s\rangle$ dos ideales en $\mathbf{K}[x_1,\ldots,x_n]$. Entonces IJ es generado por el producto de todos los generadores de I y J:

$$IJ=\langle f_ig_j:\ \ 1\le i\le r,\ 1\le j\le s\rangle$$

Demostración

Como cualquier elemento de IJ es la suma de polinomios de la forma fg con $f\in I$ y $g\in J$. Pero f y g podemos expresarlo en términos de los generadores $f_1,\ldots,f_r$ y $g_1,\ldots,g_s$ respectivamente, como

$$f=\sum_{i=1}^{r}a_if_i,\qquad g=\sum_{j=1}^{s}b_jg_j$$

para polinomios apropiados $a_1,\ldots,a_r$ y $b_1,\ldots,b_s$. De este modo fg y cualquier suma de polinomios de esta forma, puede ser escrita como una suma

$$\sum c_{ij}f_ig_j\quad\text{donde } c_{ij}\in\mathbf{K}[x_1,\ldots,x_n]$$

Por lo tanto $IJ\subset\langle f_ig_i:\ \ 1\le i\le r,\ 1\le j\le s\rangle$.

La otra inclusión es directa. □

Con respecto a sus variedades podemos decir.

Teorema 4.3.2

Sean I y J ideales en $\mathbf{K}[x_1, \ldots, x_n]$, entonces

$$V(IJ) = V(I) \cup V(J)$$

Demostración

($\subset$) Sea $x \in V(IJ)$ Entonces

$$g(x)h(x) = 0 \quad \forall g \in I, \quad h \in J$$

(i) Si $g(x) = 0, \quad \forall g \in I$, entonces $x \in V(I)$ luego $x \in V(I) \cup V(J)$.

(ii) Si $g(x) \neq 0$), para algún $g \in I$, entonces $h(x) = 0$, para todo $h \in J$. Luego $x \in V(J)$. Por lo tanto $x \in V(I) \cup V(J)$.

($\supset$) Sea $x \in V(I) \cup V(J)$ entonces $x \in V(I)$ o $x \in V(J)$.

Por lo tanto

$$g(x)h(x) = 0, \quad \text{para todo} \quad g \in I \quad \text{y} \quad h \in J$$

Luego $f(x) = 0$, para todo $f \in IJ$. De aqui se obtiene $x \in V(IJ)$. $\square$

4.3.3. Intersección de Ideales

La operación de intersección de dos ideales, es la más primitiva que las operaciones de adición y multiplicación.

Definición 4.3.3

La intersección $I \cap J$ de dos ideales I y J en $\mathbf{K}[x_1, \ldots, x_n]$ es el conjunto de los polinomios que pertenecen a ambos ideales I y J.

Proposición 4.3.3

Si I y J son ideales en $\mathbf{K}[x_1, \ldots, x_n]$, entonces $I \cap J$ es igualmente un ideal. $\square$

Se tiene que $IJ \subset I \cap J$ desde que los elementos de IJ son sumas de polinomios de la forma fg con $f \in I, g \in J$, con lo cual cada $fg \in I \cap J$.

Además IJ puede estar contenido estrictamente en $I \cap J$.

Ejemplo 4.3.2

Sea $I = J = \langle x, y \rangle$, entonces

$$IJ = \langle x^2,\ xy,\ y^2 \rangle$$

está contenido estrictamente en

$$I \cap J = I = \langle x,\ y \rangle$$

desde que $x \in I \cap J$, pero $x \notin IJ$.

Dados dos ideales y el conjunto de generadores de cada uno de ellos.

¿Cómo calcular el conjunto de generadores de la intersección?. Esto es mucho más dificil que el cálculo para la suma y el producto de ideales.

Ejemplo 4.3.3

Sea

$$I = \langle f \rangle, \quad f = (x+y)^4(x^2+y)^2(x-5y)$$

y

$$J = \langle g \rangle, \quad g = (x+y)(x^2+y)^3(x+3y)$$

ideales en $\mathbf{K}[x, y]$.

Entonces

$$I \cap J = \langle (x+y)^4(x^2+y)^3(x-5y)(x+3y) \rangle$$

Esto resulta directo desde que f y g están factorizados en polinomios irreducibles.

En general esta factorización no siempre es directa, así que cualquier algoritmo para determinar la intersección, tendría que vencer ésta dificultad.

Sin embargo, existe una salida elegante, que reduce el cálculo de la intersección eliminando variables, pero este último problema ya fué resuelto.

Para ver esto, necesitamos la notación siguente:

Si I es un ideal en $\mathbf{K}[x_1, \ldots, x_n]$ y $f(t) \in \mathbf{K}[t]$ un polinomio en variable t, entonces fI denota el ideal en $\mathbf{K}[x_1, \ldots, x_n, t]$ generado por el conjunto de polinomios

$$\{fh : \ h \in I\}$$

Es claro que el ideal $I \subset \mathbf{K}[x_1, \ldots, x_n]$ no es un ideal en $\mathbf{K}[x_1, \ldots, x_n, t]$ a causa de no ser cerrado bajo la multiplicación por t.

Si queremos enfatizar que el polinomio $f \in \mathbf{K}[t]$ es un polinomio unicamente en t, escribiremos

$$f = f(t)$$

Si queremos acentuar que el polinomio $h \in \mathbf{K}[x_1, \ldots, x_n]$ envuelve unicamente las variables $x_1, \ldots, x_n$ escrbiremos

$$h = h(x)$$

De manera similar, si $g \in \mathbf{K}[x_1, \ldots, x_n, t]$ deseamos indicar que depende de las variedades $x_1, \ldots, x_n, t$ escribiremos

$$g = g(x, t)$$

Lema 4.3.3

(i) Sea I un ideal en $\mathbf{K}[x_1, \ldots, x_n]$ generado por

$$p_1(x), \ldots, p_r(x)$$

entonces $f(t)I$ es un ideal en $\mathbf{K}[x_1, \ldots, x_n, t]$ generado por

$$f(t)p_1(x), \ldots, f(t)p_r(x)$$

(ii) Si $g(x, t) \in f(t)I$ y $a \in K$ arbitrario, entonces $g(x, a) \in I$.

Demostración

(i) Sea $g(x,t) \in f(t)I$. Puede ser expresado como una suma de términos de la forma:

$$h(x,t)f(t)p(x), \text{ para } h \in \mathbf{K}[x_1,\ldots,x_n,t] \text{ y } p(x) \in I$$

Pero a causa que I es generado por $p_1(x),\ldots,p_r(x)$ el polinomio $p(x)$ es una suma de términos de la forma

$$q_i(x)p_i(x), \quad 1 \leq i \leq r$$

Esto es

$$p(x) = \sum_{i=1}^{r} q_i(x)p_i(x)$$

de aqui se tiene

$$h(x,t)f(t)p(x) = \sum_{i=1}^{r} h(x,t)q_i(x)f(t)p_i(x)$$

donde $h(x,t)q_i(x) \in \mathbf{K}[x_1,\ldots,x_n,t]$ para $1 \leq i \leq r$.

De este modo $h(x,t)f(t)p(x)$ pertenece al ideal en $\mathbf{K}[x_1,\ldots,x_n,t]$ generado por $f(t)p_1(x),\ldots,f(t)p_r(x)$.

Desde que $g(x,t)$ es una suma de tales términos se tiene

$$g(x,t) \in \langle f(t)p_1(x),\ldots,f(t)p_r(x)\rangle$$

(ii) Sea $g(x,t) \in f(t)I$. De la parte (i) se tiene

$$g(x,t) = \sum_{i=1}^{r} h_i(x,t)f(t)p_i(x)$$

donde $I = \langle p_1(x),\ldots,p_r(x)\rangle$

entonces

$$g(x,a) = \sum_{i=1}^{r} h_i(x,a)f(a)p_i(x)$$

como $h_i(x,a)f(a) \in \mathbf{K}[x_1,\ldots,x_n]$, entonces $g(x,a) \in I$. $\square$

Teorema 4.3.4

Sean I, J dos ideales en $\mathbf{K}[x_1, \ldots, x_n]$.

Entonces $I \cap J = (tI + (1-t)J) \cap \mathbf{K}[x_1, \ldots, x_n]$

Demostración

($\subset$) Sea $f \in I \cap J$ desde que $f \in I$ se tiene $tf \in tI$. Similarmente, $f \in J$ implica $(1-t)f \in (1-t)J$, de este modo

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

como $f \in I \subset \mathbf{K}[x_1, \ldots, x_n]$ se tiene

$$f \in (tI + (1-t)J) \cap \mathbf{K}[x_1, \ldots, x_n]$$

esto muestra que

$$I \cap J \subset (tI + (1-t)J) \cap \mathbf{K}[x_1, \ldots, x_n]$$

($\supset$) Sea $f \in (tI + (1-t)J) \cap \mathbf{K}[x_1, \ldots, x_n]$ entonces

$$f(x) = g(x,t) + h(x,t) \quad \text{donde} \quad g(x,t) \in tI \ \text{ y } \ h(x,t) \in (1-t)J$$

Si hacemos $t = 0$, se tiene $g(x, 0) = 0$, desde que cada elemento de tI es múltiplo de t.

Luego

$$f(x) = h(x, 0)$$

y por el lema (4.3.3) $f(x) \in J$.

Luego considerando $t = 1$ en la relación $f(x) = g(x,t) + h(x,t)$ se tiene

$$h(x, 1) = 0$$

desde que cada elemento de $(1-t)J$ es múltplo de $(1-t)$.

Asi

$$f(x) = g(x, 1)$$

luego $f(x) \in I$. Por lo tanto

$$f(x) \in I \cap J \quad \square$$

Con el resultado anterior y el teorema de eliminación nos permite calcular la intersección de ideales.

Ejemplo 4.3.4

Sean

$$I = \langle x^2y \rangle, \quad J = \langle xy^2 \rangle \text{ ideales en } \mathbf{K}[x, y]$$

(i)

$$\begin{aligned} tI + (1-t)J &= \langle tx^2y,\ (1-t)xy^2 \rangle \\ &= \langle tx^2y, txy^2 - xy^2 \rangle \text{ en } \mathbf{K}[t, x, y] \end{aligned}$$

(ii) Calculando los S-polinomios de los generadores obtenemos.

$$tx^2y^2 - (tx^2y^2 - x^2y^2) = x^2y^2$$

(iii) Luego

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

es una base de Gröbner para $tI + (1-t)J$ con respecto al orden lex con $t > x > y$.

Por el teorema de eliminación, $\{x^2y^2\}$ es una de Gröbner para

$$(tI + (1-t)J) \cap \mathbf{K}[x, y]$$

Asi

$$I \cap J = \langle x^2y^2 \rangle$$

Teorema 4.3.5

Si I y J son ideales en $\mathbf{K}[x_1, \ldots, x_n]$, entonces

$$V(I \cap J) = V(I) \cup V(J)$$

Demostración

($\subset$) Se sabe $IJ \subset I \cap J$ entonces

$$V(I \cap J) \subset V(IJ)$$

luego

$$V(I \cap J) \subset V(I) \cup V(J)$$

($\supset$) Sea $x \in V(I) \cup V(J)$ entonces

$$x \in V(I) \quad \text{ó} \quad x \in V(J)$$

Si $f \in I \cap J$ arbitrario,

(i) si $x \in V(I)$ entonces $f \in I$, $f(x) = 0$
entonces

$$x \in V(I \cap J)$$

(ii) si $x \in V(J)$, como $f \in J$, $f(x) = 0$
entonces

$$x \in V(I \cap J)$$

con lo cual

$$V(I \cap J) \supset V(I) \cap V(J) \quad \square$$

Proposición 4.3.4

Sean I, J dos deales en $\mathbf{K}[x_1, \ldots, x_n]$ entonces

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

Demostración

($\subset$) Sea $f \in \sqrt{I \cap J}$ entonces

$$f^m \in I \cap J \text{ para algún entero } m > 0,$$

luego

$$f^m \in I \quad \text{y} \quad f^m \in J$$

entonces

$$f \in \sqrt{I} \quad \text{y} \quad f \in \sqrt{J}$$

por lo tanto

$$f \in \sqrt{I} \cap \sqrt{J}$$

($\supset$) Sea

$$f \in \sqrt{I} \cap \sqrt{J}$$

luego

$$\text{existen } m, p > 0 \text{ tal que } f^m \in I, \quad f^p \in J.$$

Asi

$$f^{m+p} \in I \cap J$$

Por lo tanto

$$f \in \sqrt{I \cap J} \quad \square$$

Definición 4.3.4

Sean I y J dos ideales en $\mathbf{K}[x_1, \ldots, x_n]$

Entonces

$$I : J = \{f \in \mathbf{K}[x_1, \ldots, x_n] / \ fg \in I, \text{ para todo } \ g \in J\}$$

será el ideal cociente de I por J.

Ejemplo 4.3.5

En $\mathbf{K}[x, y, z]$ tenemos:

$$\begin{aligned} \langle xz,\ yz\rangle : \langle z\rangle &= \{f \in \mathbf{K}[x, y, z] / \ fz \in \langle xz,\ yz\rangle\} \\ &= \{f \in \mathbf{K}[x, y, z] / \ fz = Axz + Byz\} \\ &= \{f \in \mathbf{K}[x, y, z] / \ f = Ax + By\} \\ &= \langle x, y\rangle \end{aligned}$$

Proposición 4.3.5

Si I, J son ideales en $\mathbf{K}[x_1, \ldots, x_n]$ entonces $I : J$ es un ideal en $\mathbf{K}[x_1, \ldots, x_n]$ y $I : J$ contiene a I es decir $I \subset I : J$

Demostración

(i) Para mostrar que $I : J$ contiene a I, note que si $f \in I$ entonces

$$fg \in I, \ \text{ para todo } \ g \in \mathbf{K}[x_1, \ldots, x_n]$$

en particular para todo $g \in J$, luego $I \subset I : J$.

(ii) $I : J$ es un ideal, desde que $0 \in I$ entonces $0 \in I : J$.

(iii) Sea $f_1,\ f_2 \in I : J$

entonces

$$f_1 g,\quad f_2 g \in I \quad \text{para todo} \quad g \in J$$

luego

$$(f_1 + f_2)g = f_1 g + f_2 g \in I,\ \forall g \in J$$

entonces

$$f_1 + f_2 \in I : J$$

(iv) Similar manera $hf \in I : J$, para todo $h \in \mathbf{K}[x_1, \ldots, x_n]$ $\square$

Proposición 4.3.6

Sean I, J y K ideales en $\mathbf{K}[x_1, \ldots, x_n]$. Entonces

(i) $I : \mathbf{K}[x_1, \ldots, x_n] = I$

(ii) $IJ \subset K \Longleftrightarrow I \subset K : J$

(iii) $J \subset I \Longleftrightarrow I : J = \mathbf{K}[x_1, \ldots, x_n]$

(iv) $\mathbf{K}[x_1, \ldots, x_n] : I = \mathbf{K}[x_1, \ldots, x_n]$

Demostración

(i) ($\subset$) Sea $f \in I : \mathbf{K}[x_1, \ldots, x_n]$ tomando $1 \in \mathbf{K}[x_1, \ldots, x_n]$ entonces $f \cdot 1 \in I$ luego $f \in I$

($\supset$) Directo de la proposición (4.3.5).

(ii)($\Longrightarrow$) Sea $f \in I$ arbitrario y $g \in J$ entonces $fg \in IJ$ entonces como $IJ \subset K$, $fg \in K$ luego $f \in K : J$

($\Longleftarrow$) Sean $fg \in IJ$ donde $f \in I$ y $g \in J$ como $f \in I \subset K : J$ entonces $f \in K : J$ luego $fg \in K$. Debido a que cada elemento de IJ es generado por elementos de la forma fg. Entonces $IJ \subset K$

(iii)($\Longrightarrow$) Veamos que $I : J = \mathbf{K}[x_1, \ldots, x_n]$. En efecto

($\subset$) Directo.

($\supset$) Sea $f \in \mathbf{K}[x_1, \ldots, x_n]$ y $g \in J$ como $J \subset I$ entonces $g \in I$ entonces $fg \in I$, $\forall g \in J$. Por lo tanto $f \in I : J$.

($\Longleftarrow$) Sea $g \in J$, como $1 \in I : J = \mathbf{K}[x_1, \ldots, x_n]$ entonces $1g \in I$ entonces $g \in I$.

(iv) Direct. $\square$

Proposición 4.3.7

Sean I, I_i, J, J_i y K ideales en $\mathbf{K}[x_1, \ldots, x_n]$ para $1 \leq i \leq r$. Entonces

(i) $(\bigcap_{i=1}^{r} I_i) : J = \bigcap_{i=1}^{r} (I_i : J)$

(ii) $I : (\sum_{i=1}^{r} J_i) = \bigcap_{i=1}^{r} (I : J_i)$

(iii) $(I : J) : K = I : JK$

Demostración

(i) ($\subset$) Sea

$$f \in (\bigcap_{i=1}^{r} I_i) : J$$

entonces

$$\forall g \in J, \quad fg \in \bigcap_{i=1}^{r} I_i$$

entonces

$$f \in I_i : J, \quad \forall i,\ 1 \leq i \leq r$$

entonces

$$f \in \bigcap_{i=1}^{r} (I_i : J)$$

($\supset$) Sea

$$f \in \bigcap_{i=1}^{r} (I_i : J)$$

entonces

$$\forall i = 1, \ldots, r \quad f \in I_i : J$$

entonces

$$fg \in I_i, \ \forall i, \forall g \in J$$

entonces

$$fg \in \bigcap_{i=1}^{r} I_i$$

luego

$$f \in (\bigcap_{i=1}^{r} I_i) : J$$

(ii) ($\subset$) Sea $f \in I : (\sum_{i=1}^{r} J_i)$

entonces

$$\text{para cada } \ i = 1, \ldots, r \ \ \forall g \in J_i, \ \ fg \in I$$

entonces

$$f \in I : J_i$$

luego

$$f \in \bigcap_{i=1}^{r} (I : J_i)$$

($\supset$) Sea $f \in \bigcap_{i=1}^{r} (I : J_i)$

Entonces $\forall i = 1, \ldots, r$, $f \in I : J_i$. Sea

$$\sum_{i=1}^{r} g_i \in \sum_{i=1}^{r} J_i \ \text{ donde } \ g_i \in J_i \ \text{ arbitrariamente dado.}$$

como $f \sum_{i=1}^{r} g_i \in I$, entonces

$$f \in I : (\sum_{i=1}^{r} J_i)$$

(iii) ($\subset$) Sea $f \in (I : J) : K$ entonces

$$\forall h \in K, \qquad fh \in I : J$$

$$\forall g \in J, \qquad (fhg) \in I$$

luego $f \in I : JK$

($\supset$) Sea $f \in I : JK$ entonces

$$fgh \in I,\ \forall g \in I,\ \forall h \in K$$

$$fh \in I : J$$

$$f \in (I : J) : K \qquad \square$$

Si f es un polinomio e I un ideal, escibimos

$$I : f \quad \text{en vez de} \quad I : \langle f \rangle$$

Luego

$$I : \langle f_1, \ldots, f_r \rangle = \bigcap_{i=1}^{r} (I : f_i) \tag{4.4}$$

Estamos interesados en calcular los generadores del ideal cociente $I : J$, dados los generadores de I y J. La siguiente observación es clave para ese proceso.

Teorema 4.3.6

Sea I un ideal y g un elemento de $\mathbf{K}[x_1, \ldots, x_n]$. Si $\{h_1, \ldots, h_p\}$ es un generador del ideal $I \cap \langle g \rangle$ entonces

$$\{h_1/g, \ldots, h_p/g\} \text{ es un generador de } I : \langle g \rangle \tag{4.5}$$

Demostración

Si $a \in \langle g \rangle$ entonces $a = bg$ para algún polinomio b.

Así, si

$$f \in \langle h_1/g, \ldots, h_p/g \rangle$$

entonces

$$af = bgf \in \langle h_1, \ldots, h_p \rangle = I \cap \langle g \rangle \subset I$$

por lo tanto $f \in I : \langle g \rangle$. Esto significa que

$$\langle h_1/g, \ldots, h_p/g \rangle \subset I : \langle g \rangle$$

Ahora, sea $f \in I : \langle g \rangle$ entonces $fg \in I$, desde que $fg \in \langle g \rangle$ se tiene $fg \in I \cap \langle g \rangle$, como $I \cap \langle g \rangle = \langle h_1, \ldots, h_p \rangle$ entonces

$$fg = \sum_{i=1}^{p} \gamma_i h_i, \quad \text{para algunos polinomios } \gamma_i$$

desde que cada $h_i \in \langle g \rangle$, significa que cada h_i/g es un polinomio, luego

$$f = \sum_{i=1}^{p} \gamma_i (h_i/g)$$

de donde

$$f \in \langle h_1/g, \ldots, h_p/g \rangle$$

asi se tiene la otra inclusión

$$\langle h_1/g, \ldots, h_p/g \rangle \supset I : \langle g \rangle \quad \square$$

Este teorema, juntamente con el procedimiento para computar la intersección de ideales y la ecuación (4.5), nos va a permitir generar un algoritmo para computar una base (en el sentido de generador) para el ideal cociente. Es decir, dada $I = \langle f_1, \ldots, f_r \rangle$ y $J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \ldots + \langle g_s \rangle$, deseamos encontrar un conjunto generador de $I : J$, calculamos primero un generador para $I : \langle g_i \rangle$, $1 \leq i \leq s$. En virtud del teorema (4.3.6) primero calculamos una base de

$$\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$$

(es decir podemos hallar una base de Gröbner para $\langle tf_1, \ldots, tf_r, (1-t)g_i \rangle$ con respecto al orden lex en el cual t precede a todos los x_i y tomamos elementos de dicha base en el cual no depende de t y ello nos origina una bese de Gröbner para $\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$).

Usando el algoritmo de la división, dividimos cada uno de esos elementos de la base encontrada por g_i para obtener un generador de $I : \langle g_i \rangle$.

Finalmente, computamos una base para $I : J$ por aplicaciones de intersecciones algoritmicas $S - 1$ tiempos.

Es decir, $I : \langle g_1, g_2 \rangle = (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle)$ luego una base para

$$I : \langle g_1, g_2, g_3 \rangle = (I : \langle g_1, g_2 \rangle) \cap (I : \langle g_3 \rangle)$$

y asi sucesivamente.

Capítulo 5

Aplicaciones

En este capítulo se mostrará siete aplicaciones de las bases de Gröbner en el anillo de polinomios, las cuales se mostrarán utilizando los capítulos anteriores y ls apéndices A, B, C y D.

Aplicación 1 : Pertenencia a un ideal.

Dados los generadores de un ideal I en $\mathbf{K}[x_1, \ldots, x_n]$ y un elemento cualquiera $f \in \mathbf{K}[x_1, \ldots, x_n]$. Se dará un algoritmo para determinar si $f \in I$ o $f \notin I$

Aplicación 2 : Consistencia de un sistema de ecuaciones.

Dada un sistema de ecuaciones

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_s &= 0, \qquad f_1, \ldots, f_s \in \mathbf{K}[x_1, \ldots, x_n] \end{aligned}$$

Se verá las condiciones para determinar si el sistema es consistente o no.

Aplicación 3 : Conjunto solución de un sistema, es finito o no.

Si un sistema de ecuaciones polinomiales es compatible (tiene solución), se desea dar condiciones para determinar si el conjunto solución del sistema es finito o no.

Aplicación 4 : Resolución de un sistema de ecuaciones polinomiales.

En base a los teoremas de eliminación y extensión, se determinará el conjunto solución de un sistema de ecuaciones en $\mathbf{K}[x, \ldots, x_n]$.

Aplicación 5 :Intersección de Ideales.

Dados dos ideales I y J en $\mathbf{K}[x, \ldots, x_n]$, se determinará los generadores para la intersección $I \cap J$.

Aplicación 6 :Pertenencia al radical de un ideal.

Dado un ideal $I \subset \mathbf{K}[x, \ldots, x_n]$ y $f \in \mathbf{K}[x, \ldots, x_n]$. Se dará un algoritmo para determinar si $f \in \sqrt{I}$ ó $f \notin \sqrt{I}$.

Aplicación 7 :Ideal cociente.

Dada dos ideales I y $J \in \mathbf{K}[x, \ldots, x_n]$ se resuelve el problema de de determinar el ideal cociente $I : J$, mediante el cálculo de sus generadores.

Todos los cálculos en los siguientes ejemplos de aplicación fueron realizados Maple 9.5.

5.1. El problema de pertenencia a un ideal de $\mathbf{K}[x_1, \ldots, x_n]$

Sea f un elemento cualquiera en $\mathbf{K}[x, \ldots, x_n]$ e $I = \langle f_1, \ldots, f_n \rangle$ un ideal en $\mathbf{K}[x, \ldots, x_n]$. Queremos determinar si $f \in I$ o $f \notin I$. Note que para esto no es suficiente realizar el algoritmo de la división generalizado por la m-upla ordenada $(f_1, \ldots, f_m)$, teorema (2.2.1), como ilustra el siguiente ejemplo.

Ejemplo 5.1.1

Sea $f_1 = xy - 1$, $f_2 = x^2 + 1$ y $f = x^2y + y$ en $\mathbf{K}[x, y]$ con el orden lexicográfico y la 2-upla ordenada (f_1, f_2). Pregunta ¿f pertenece al ideal $I = \langle f_1, f_2 \rangle$?

Como en el caso de una variable queremos aplicar el algoritmo de la división y concluir que $f \in I$ si y solo si el resto de la división es cero.

Aplicando el algoritmo anterior obtenemos

$$f = x \cdot f_1 + 0 \cdot f_2 + (x + y)$$

esto es, $q_1 = x$, $q_2 = 0$ y el resto $r = x + y \neq 0$. Ya que el resto de dividir no es cero. ¿Podemos concluir que $f \notin \langle f_1, f_2 \rangle$? La respuesta es no, pues

$$f = y \cdot f_2 + 0 \cdot f_1$$

Así $f \in \langle f_1, f_2 \rangle = I$

¿Qué sucede entonces con el algoritmo de la división generalizado? ¿Porqué no soluciona el problema de Pertenencia? Como notamos en el ejemplo, el algoritmo de la división generalizada es influenciado por el orden en que aparecen los divisores $f_1, \ldots, f_m$.

De la definición (2.4.2), una Base de Gröbner G para un ideal solucionará nuestro problema pues el algoritmo de la división por G siempre deja el mismo resto sin importar el orden de aparición de los elementos de G. Por lo tanto si dividimos f por una base de Gröbner para el ideal I , si el resto es cero entonces $f \in I$ en caso contrario $f \notin I$ (corolaro (2.5.1)).

Por lo tanto la solución al problema de pertenencia de un polinomio f a un ideal I está dada por el siguiente algoritmo:

(i) Fije un orden monomial en $\mathbf{K}[x_1, \ldots, x_n]$

(ii) Determine un base de Gröbner G, para I.

(iii) Divida f por G.

(iv) $f \in I$ si y solo si el resto de la división en (iii) es cero.

Ejemplo 5.1.2

Sea

$$I = \langle f_1, f_2 \rangle = \langle xz - y^2, x^3 - z^3 \rangle \subset \mathbf{C}[x, y, z]$$

y

$$f = -4x^2y^2z^2 + y^6 + 3z^5$$

¿$f \in I$?

(i) Utilizando el orden lexicográfico graduado.

(ii) $G = (f_1, f_2, f_3, f_4, f_5) = (xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5)$ es una base de Gröbner en particular reducida para I.

(iii) Dividiendo, hallamos: $f = (-4xy^2z - 4y^4) \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + (-3) \cdot f_5 + 0$

(iv) Como $\overline{f}^G = 0$ entonces concluimos $f \in I$.

Ejemplo 5.1.3

Dada el ideal $I = \langle xz - y^2, x^3 - z^2 \rangle \subset \mathbf{C}[x, y, z]$. ¿$-4x^2y^2z^2 + y^6 + 3z^5 \in I$?

Veamos: Utilizando el orden lexicográfico, se obtiene

$$G = \{x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, xz - y^2, y^6 - z^5\}$$

una base de Gröbner para I.

Ahora, como

$$\overline{-4x^2y^2z^2 + y^6 + 3z^5}^G = 0$$

se tiene que

$$-4x^2y^2z^2 + y^6 + 3z^5 \in I$$

Ejemplo 5.1.4

Sea $I = \langle g_1, g_2 \rangle \subset \mathbf{C}[x, y]$ donde

$$g_1 = 2x^2 + 3y^2 - 11$$

$$g_2 = x^2 - y^2 - 3$$

$G = \{x^2 - 4, y^2 - 1\}$ es una base de Gröbner para I, con el orden monomial lex.

Como

$$\overline{yx^2 - 4}^G = -4 + 4y$$

entonces

$$yx^2 - 4 \notin I$$

luego

$$\overline{y^2x^2 - 4}^G = 0$$

se tiene

$$y^2x^2 - 4 \in I$$

5.2. El problema de la consistencia de un sistema en $\mathbf{K}[x_1, \ldots, x_n]$

Dados los polinomios $f_1, \ldots, f_s \in \mathbf{K}[x_1, \ldots, x_n]$ donde $\mathbf{K}$ es un cuerpo algebraicamente cerrado y el sistema de ecuaciones que se origina con ellos.

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned} \tag{5.1}$$

Se desea saber las condiciones necesarias y suficientes para que la ecuación (5.1) sea un sistema consistente es decir $V(f_1, \ldots, f_s) \neq \emptyset$.

Por el teorema de los ceros de Hilbert's (teorema 4.1.2), se tiene que

$$V(f_1, \ldots, f_s) = \emptyset \Longleftrightarrow 1 \in \langle f_1, \ldots, f_s \rangle$$

Es decir el sistema (5.1) no posee solución si y solo si el polinomio 1 está en el ideal generado por estos polinomios.

De esta manera el problema de consistencia de un sistema de ecuaciones polinomiales, se reduce a determinar o saber cuando 1 pertenece al ideal generado por dichos polinomios.

Es en este punto donde la base de Gröbner reducida (definición 2.6.2) nos ayudará, ya que para cualquier orden monomial, $\{1\}$ es la única base de Gröbner reducida para el ideal $\langle 1 \rangle = \mathbf{K}[x_1, \ldots, x_n]$.

Con todo lo anterior, tenemos el siguiente proceso para determinar si el sistema (5.1) es consistente o no.

(i) Fijar un orden monomial en $\mathbf{K}[x_1, \ldots, x_n]$.

(ii) Determinar una base de Gröbner reducida para el ideal $I = \langle f_1, \ldots, f_s \rangle$

(iii) Si la base obtenida en (ii) es $\{1\}$, el sistema (5.1) no posee solución es decir no tiene un cero en común.

Si la base obtenida en (ii) no es $\{1\}$, el sistema (5.1) es consistente, es decir posee un cero en común.

Si el cuerpo no fuese algebraicamente cerrado, se tendría solo en un sentido, es decir: Si se verifica que $\{1\}$ es una base de Gröbner reducida para $I = \langle f_1, \ldots, f_s \rangle$, entonces

$\mathbf{K}[x_1, \ldots, x_n] = I$, luego $V(f_1, \ldots, f_s) = \emptyset$ con lo cual el sistema $f_1 = 0, \ldots, f_s = 0$ no tiene solución.

Si $\{1\}$ no fuese una base de Gröbner reducida para $I = \langle f_1, \ldots, f_s \rangle \subset \mathbf{K}[x_1, \ldots, x_n]$ donde $\mathbf{K}$ es un cuerpo (no necesariamente algebraicamente cerrado) no se puede asegurar nada.

Por ejemplo $I = \langle x^2 + 1 \rangle \subset \mathbf{R}[x]$, tiene Gröbner reducida diferente de $\{1\}$, pero el sistema $x^2 + 1 = 0$, no tiene solución en $\mathbf{R}$.

Para un cuerpo no algebraico cerrrado el proceso anterior solo indicará la no compatibilidad del sistema.

Ejemplo 5.2.1

Considerando el orden lexicográfico en $\mathbf{C}[x, y]$ el sistema:

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

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

Luego

$$I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$$

entonces

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

es una base de Gröbner reducida para I. Como $G \neq \{1\}$ entonces el sistema dado es compatible.

Ejemplo 5.2.2

Dado el orden monomial lexicográfico en $\mathbf{C}[x, y, z, w]$. El sistema

$$3x - 6y - 2z = 0$$

$$2x - 4y + 4w = 0$$

$$x - 2y - z - w = 0$$

Siendo $I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w \rangle$ un ideal y desde que $G = \{x - 2y + 2w, w + \frac{z}{3}\}$ una base de Gröbner reducida para I, el sistema tiene solución.

Ejemplo 5.2.3

Considerando

$$x^2 - 4 = 0$$

$$x^2 - 9 = 0$$

Un sistema en $\mathbf{C}[x]$ y el orden lexicográfico. $\{1\}$ es una base de Gröbner reducida para $I = \langle x^2 - 4, x^2 - 9\rangle$. Por lo tanto, como es notorio, el sistema no posee solución.

5.3. El problema de determinar si el conjunto solución de un sistema es finito o infinito

Sea $f_1, \ldots, f_s$ polinomios en $\mathbf{K}[x_1, \ldots, x_n]$ donde $\mathbf{K}$ es un cuerpo algebraicamente cerrado y dado el sistema de ecuaciones

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned} \tag{5.2}$$

En esta parte, estamos interesados en determinar, bajo la hipótesis de que (5.2) es consistente, si el conjunto solución de (5.2) es finito o infinito.

Para ello consideremos $I = \langle f_1, \ldots, f_s\rangle$ en $\mathbf{K}[x_1, \ldots, x_n]$ y ordenamos los monomios según el orden lexicográfico $x_1 > \ldots > x_n$. Sea G una base de Gröbner para I.

El fundamento teórico lo encontramos en el apéndice D, en particular el teorema (D.0.6), solucionará nuestro problema.

Sea $V = V(I)$

V es un conjunto finito $\iff$ Siendo G una base de Gröbner para I·
Entonces, para cada i, $1 \leq i \leq n$, existe $m_i \geq 0$ tal que
$x_i^{m_i} = Mp(g_i)$, para algún $g_i \in G$

Es decir para afirmar que el conjunto solución de (5.2) es finito, basta con observar los monomios principales da cada elemento en la base de Gröbner determinada.

Por lo tanto, para determinar la naturaleza (finita o infinita) del conjunto solución del sistema (5.2), basta seguir los pasos siguientes:

(i) Fijar el orden lexicográfico en $\mathbf{K}[x_1, \ldots, x_n]$

(ii) Determinar una base de Gröbner G para el ideal $I = \langle f_1, \ldots, f_s \rangle$ que se origina del sistema (5.2).

(iii) Verificar si para cada i, $1 \leq i \leq n$, existe $m_i \geq 0$ tal que $x_i^{m_i} = Mp(g)$, para algún $g \in G$, donde G es hallado en (ii).

(iv) Si (iii) es verdadero, entonces, el conjunto solución es finito.

Ejemplo 5.3.1

Consideremos el sistema de ecuaciones en $\mathbf{C}[x, y, z]$.

$$x^2 + y^2 + z^2 = 1$$

$$xyz = 1$$

una base de Gröbner para $I = \langle x^2 + y^2 + z^2 - 1, xyz - 1 \rangle$ con respecto al orden lex es

$$g_1 = y^4z^2 + y^2z^4 - y^2z^2 + 1$$

$$g_2 = x + y^3z + yz^3 - yz$$

como $Mp(g_1) = y^4z^2$, $Mp(g_2) = x$, además como no existe para algún $g \in G$ tal que $Mp(g)$ sea y^m, para algún m. Entonces el sistema es compatible y tiene infinitas soluciones.

Ejemplo 5.3.2

Sea el sistema de ecuaciones en $\mathbf{C}[x, y]$

$$xy = 4$$

$$y^2 = x^3 - 1$$

Usando el orden lex, obtenemos una base de Gröbner, dada por

$$g_1 = 16x - y^2 - y^4$$

$$g_2 = y^5 + y^3 - 64$$

como $Mp(g_1) = x$, $Mp(g_2) = y^5$ entonces el sistema es compatible y con un número finito de puntos en el conjunto solución.

5.4. Resolución de un sistema de ecuaciones en $\mathbf{K}[x_1, \ldots, x_n]$

Hasta ahora podemos saber si un sistema de ecuaciones en $\mathbf{K}[x_1, \ldots, x_n]$ es compatible o no, es decir si posee al menos una solución en común (El problema de consistencia), y si fuese compatible conocer si el conjunto solución es finito o infinito (aplicación 3).

Estamos interesados en esta parte, conocer el procedimiento para hallar el conjunto solución de un sistema de ecuaciones en $\mathbf{K}[x_1, \ldots, x_n]$ siempre que su conjunto solución es finito.

Si ordenamos lexicográficamente los monomios en $\mathbf{K}[x_1, \ldots, x_n]$ y determinamos una base de Gröbner reducida para el ideal inducido por el sistema de ecuaciones, con teorema (D.0.6) podemos conocer si el conjunto solución es finito y se puede eliminar variables (teorema (3.1.2), teorema de eliminación) y como estamos utilizando el orden lex, podemos encontrar en elemento de la base de Gröbner dependiente unicamente de la variable x_n.

Para luego por el teorema de extensión (teorema (3.1.2)) podemos extender esta solución parcial en forma recursiva.

Por lo tanto, estamos en condiciones en dar un algoritmo para resolver un sistema de ecuaciones en $\mathbf{K}[x_1, \ldots, x_n]$ que sea consistente y su conjunto solución finita.

Dado el sistema de ecuaciones en $\mathbf{K}[x_1, \ldots, x_n]$

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_s &= 0, \qquad \text{donde } f_1, \ldots, f_s \in \mathbf{K}[x_1, \ldots, x_n] \end{aligned}$$

Procedemos como sigue:

(i) Formar el ideal $I = \langle f_1, \ldots, f_s \rangle$ en $\mathbf{K}[x_1, \ldots, x_n]$.

(ii) Determinar una base de Gröbner reducida G para I, utilizando el orden lexicográfico $x_1 > \ldots > x_n$

(iii) Halle las raíces del generador que dependa de x_n aplicando técnicas para una variable.

(iv) Sustituya estos valores en el elemento de la base de Gröbner G, donde dependa de x_{n-1} y x_n, hallando x_{n-1}

(v) seguir con este proceso, hasta determinar el conjunto solución del sistema dado.

Ejemplo 5.4.1

Resolver en $\mathbf{C}^4$ el sistema de ecuaciones algebraicas

$$\begin{aligned} xz - yw - z + 1 &= 0 \\ yz + xw - w - 2 &= 0 \\ y^2 + x^2 - 1 &= 0 \\ z^2 + w^2 - 1 &= 0 \end{aligned}$$

Calculando una base de Gröbner para el ideal

$$I = \langle xz - yw - z + 1, yz + xw - w - 2, y^2 + x^2 - 1, z^2 + w^2 - 1 \rangle$$

adoptando el orden lex $x > y > z > w$ obtenemos $G = \{g_1, g_2, g_3, g_4\}$ donde

$$\begin{aligned} g_1 &= x + z - 2w - 1 \\ g_2 &= y - 2z - w \\ g_3 &= z - 2w - \frac{5}{2} \\ g_4 &= w^2 + 2w + \frac{21}{20} \end{aligned}$$

En g_4 determinamos w, este valor lo reeplazamos en g_3 para hallar z y así sucesivamente, obtenemos:

$$w_1 = \frac{-10 + i\sqrt{5}}{10}, \quad z_1 = \frac{5 + 2i\sqrt{5}}{10}, \quad y_1 = \frac{i\sqrt{5}}{2}, \quad x_1 = \frac{-25 + i4\sqrt{5}}{10}$$

$$w_2 = \frac{-10 - i\sqrt{5}}{10}; \quad z_2 = \frac{5 - 2i\sqrt{5}}{10}, \quad y_2 = \frac{-i\sqrt{5}}{2}, \quad x_2 = \frac{-25 - +i4\sqrt{5}}{10}$$

Ejemplo 5.4.2

Considere las ecuaciones en $\mathbf{C}^3$.

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

Ellos determinan un ideal

$$I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z \rangle \subset \mathbf{C}[x, y, z]$$

y queremos determinar todos los puntos en $V(I)$.

La base de Gröbner de I con respecto al orden lex $x > y > z$ esta dada por

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

Resolviendo g_3 en z obtenemos cuatro valores.

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5} - 1}$$

Luego sustituyendo cada valor en $g_1 = 0$ y $g_2 = 0$, obtenemos los valores para x e y.

De esta manera está resuelto el sistema original.

Ejemplo 5.4.3

Resolver el sistema de ecuaciones en C^3

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

obtenemos el ideal

$$I = \langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1 \rangle$$

el cual con respecto al orden lex obtenemos una base de Gröbner de cuatro polinomios

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

Resolviendo $g_4 = 0$, obtenemos los posibles valores de z: 0, 1 y $-1 \pm \sqrt{2}$ sustituyendo en g_2 y $g_3 = 0$ y finalmente en $g_1 = x+y+z^2 = 0$ los valores para x.

Por lo tanto se verifican cinco soluciones $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2})$, $(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})$.

5.5. El problema del cálculo de la intersección de dos ideales en $\mathbf{K}[x_1, \ldots, x_n]$

Sean $I = \langle f_1, \ldots, f_r \rangle$, $J = \langle g_1, \ldots, g_s \rangle$ dos ideales en $\mathbf{K}[x_1, \ldots, x_n]$.

En esta parte se pretende hallar los generadores (en particular una base de Gröbner) de la intersección $I \cap J$.

Para ello extendemos nuestro anillo de polinomios $\mathbf{K}[x_1, \ldots, x_n]$ con una variable t, $\mathbf{K}[x_1, \ldots, x_n, t]$.

Por el lema (4.3.3) (i), podemos hallar los generadores de los ideales: tI y $(1-t)J$.

Por el corolario (4.3.1) podemos determinar los generadores del ideal suma:

$$tI + (1-t)J$$

Podemos ordenar los monomios lexicográficamente en $\mathbf{K}[x_1, \ldots, x_n, t]$ con la cualidad de $t > x_1 > \ldots > x_n$. Para determinar una base de Gröbner para $tI + (1-t)J$ consideremos el ideal de primera eliminación (eliminando t) para $tI + (1-t)J$ obtenemos una base de Gröbner G para $(tI + (1-t)J) \cap \mathbf{K}[x_1, \ldots, x_n]$ tomando unicamente los elementos que no contenga la variables t, según el teorema (4.3.6),

$$I \cap J = (tI + (1-t)J) \cap \mathbf{K}[x_1, \ldots, x_n]$$

entonces se tiene una base de Gröbner para $I \cap J$, pero por el corolario (2.4.1) también es un generador para $I \cap J$.

Por lo tanto podemos seguir el siguiente algoritmo para determinar la intersección de dos ideales.

Sean $I = \langle f_1, \ldots, f_r \rangle$, $J = \langle g_1, \ldots, g_s \rangle$ dos ideales en $\mathbf{K}[x_1, \ldots, x_n]$.

(i) Considere el orden lexicográfico para $\mathbf{K}[x_1, \ldots, x_n, t]$en el cual $t > x_1 > \ldots > x_n$.

(ii) Calcule una base de Gröbner con respecto al orden dado (i) para el ideal

$$tI + (1-t)J = \langle tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s \rangle \subset \mathbf{K}[x_1, \ldots, x_n, t]$$

(iii) Los elementos de la base hallada en (ii), la cual no contenga la variable t, formará un generador (en particular una base de Gröbner) para $I \cap J$.

Ejemplo 5.5.1

Sea $I = \langle x^2y \rangle$ y $J = \langle xy^2 \rangle$ en $\mathbf{K}[x, y]$. Deseamos conocer $I \cap J$. Consideremos

$$tI + (1-t)J = \langle tx^2y, (1-t)xy^2 \rangle \text{ en } \mathbf{K}[t, x, y]$$

Calculamos una base de Gröbner para $tI + (1-t)J$ con respecto al orden lex con $t > x > y$ la cual es $\{tx^2y, txy^2 - xy^2, x^2y^2\}$.

Por lo tanto $\{x^2y^2\}$ es una base de Gröbner para $I \cap J$.

Asi $I \cap J = \langle x^2y^2 \rangle$

Ejemplo 5.5.2

Sea $I = \langle xy - 1, x^2 + 1\rangle$ y $J = \langle x^2y + y\rangle$ ideales en $\mathbf{C}[x, y]$.

Considerando el orden lexicográfico en $\mathbf{C}[t, x, y]$.

La base de Gröbner para el ideal

$$\langle t(xy - 1), t(x^2 + 1), (1 - t)(x^2y + y)\rangle$$

es

$$G = \{tx + ty, ty^2 + t, x^2y + y\}$$

Luego $I \cap J = \langle x^2y + y\rangle$

5.6. El problema de pertenencia en el radical de un ideal

Sea $I = \langle f_1, \ldots, f_s\rangle \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal arbitrario y $\sqrt{I}$ el radical de I (definición (4.2.2)). Sea $f \in \mathbf{K}[x_1, \ldots, x_n]$ un polinomio arbitrario. Queremos saber si f pertenece o no al radical de I. Según la definición (4.2.2) necesitaríamos determinar un $m > 0$ tal que $f^m \in I$ para indicar que $f \in \sqrt{I}$, en caso contrario $f \notin \sqrt{I}$.

La proposición (4.2.1) nos permite resolver este problema extendiendo el anillo a $\mathbf{K}[x_1, \ldots, x_n, y]$ y luego mediante la base de Gröbner reducida la cual es también un generador del ideal y gracias a la unicidad de la base de Gröbner reducida obtenemos el siguiente algoritmo:

Sea $I = \langle f_1, \ldots, f_s\rangle \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal y $f \in \mathbf{K}[x_1, \ldots, x_n]$

(i) Dar un orden monomial arbitrario en $\mathbf{K}[x_1, \ldots, x_n]$.

(ii) Determinar un base de Gröbner reducida del siguiente ideal

$$\langle f_1, \ldots, f_s, 1 - yf\rangle \subset \mathbf{K}[x_1, \ldots, x_n, y]$$

(iii) Si $\{1\}$ es la base encontrada en (ii), entonces

$$f \in \sqrt{\langle f_1, \ldots, f_s\rangle}$$

En caso contrario

$$f \notin \sqrt{\langle f_1, \ldots, f_s\rangle}$$

Ejemplo 5.6.1

Sea

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

Sea $I = \langle p, q \rangle$ un ideal en $\mathbf{C}[x, y]$ con orden monomial lexicográfico. Se desea saber si $f \in \sqrt{I}$ o no.

Desde que $\{1\}$ es una base de Gröbner reducida para

$$\langle p, q, 1 - zf \rangle \subset \mathbf{C}[x, y, z]$$

Entonces

$$y - x^2 + 1 \in \sqrt{\langle p, q \rangle}$$

Ejemplo 5.6.2

Considerando en $\mathbf{C}[x, y, z]$.

$$I = \langle x + z, x^2 y, x - z^2 \rangle$$

con orden lexicográfico.

Será, $f = x^2 + 3xz \in \sqrt{I}$.

Veamos, $G = \{x - 1, y, 1 + z, w + \frac{1}{2}\}$ es una base de Gröbner reducida para

$$\langle x + z, x^2 y, x - z^2, 1 - w(x^2 + 3xz) \rangle \subset \mathbf{C}[x, y, z, w]$$

Luego

$$f = x^2 + 3xz \notin \sqrt{I}$$

5.7. Problema del cálculo del ideal cociente

Dada dos ideales $I = \langle f_1, \ldots, f_r \rangle$, $J = \langle g_1, \ldots, g_s \rangle$ en el anillo de polinomios $\mathbf{K}[x_1, \ldots, x_n]$, por el corolario (4.3.1) se tiene

$$J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \ldots + \langle g_s \rangle$$

Se quiere calcular los generadores del ideal cociente de I por J (definición (4.3.4)).

Para ello calculamos un generador para $I : \langle g_i \rangle$, $1 \leq i \leq s$ en virtud del teorema (4.3.6) la cual nos indica que en primer lugar debemos calcular una base para $\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$, es decir una base de Gröbner para

$$\langle tf_1, \ldots, tf_r, (1-t)g_i \rangle$$

con respecto al orden lex en el cual t precede a todos los x_i, y tomamos los elementos de dicha base que no dependan de t.

Ello nos origina una base de Gröbner para

$$\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$$

Luego usando el algoritmo de la división, dividamos cada uno de los elementos de la base de Gröbner encontrada por g_i para obtener un generador de $I : \langle g_i \rangle$.

Luego como se conoce el calculo de la intersección de dos ideales (teorema (4.3.4)), podemos calcular

$$I : \langle g_1 g_2 \rangle = (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle)$$

ver el teorema (4.3.6) (ii).

Luego

$$I : \langle g_1, g_2, g_3 \rangle = (I : \langle g_1, g_2 \rangle) \cap (I : \langle g_3 \rangle)$$

y así sucesivamente mediante aplicaciones de intersecciones sucesivas, hasta calcular un generador en

$$I : J = I : \langle g_1, \ldots, g_3 \rangle = (I : \langle g_1, \ldots, g_{s-1} \rangle) \cap (I : \langle g_s \rangle)$$

Por lo tanto, a modo de resumen, tenemos el siguiente algoritmo para el calculo del ideal cociente de $I : J$

(i) Para cada i, $1 \leq i \leq s$ determine una base de Gröbner para $I : \langle g_i \rangle$, con respecto al orden lex.

(ii) Determine en forma recursiva los generadores de:

$$\begin{aligned} I : \langle g_1, g_2 \rangle &= (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle) \\ I : \langle g_1, g_2, g_3 \rangle &= (I : \langle g_1, g_2 \rangle) \cap (I : \langle g_3 \rangle) \\ &\vdots \\ I : J &= (I : \langle g_1, \ldots, g_{s-1} \rangle) \cap (I : \langle g_s \rangle) \end{aligned}$$

Ejemplo 5.7.1

Sea

$$I = \langle x^2y + 3xy, 2xy^2 \rangle = \langle f_1, f_2 \rangle$$

y

$$J = \langle x^3 + 6x + y^2x, 4xy^2 \rangle = \langle g_1, g_2 \rangle$$

ideales en $\mathbf{C}[x, y]$.

Se desea conocer $I : J$

Se tiene

$$I : \langle g_1 \rangle = \langle xy + 3y, y^2 \rangle$$

desde que

$$\begin{aligned} I \cap \langle g_1 \rangle &= \langle x^4y + 6x^2y + y^3x^2 + 3x^3y + 18xy + 3y^3x, x^3y^2 + 6y^2x + y^4x \rangle \\ &= \langle h_1, h_2 \rangle \end{aligned}$$

y

$$\frac{h_1}{g_1} = xy + 3y, \qquad \frac{h_2}{g_1} = y^2$$

De manera similar: $I : \langle g_2 \rangle = \langle 1 \rangle$

Desde que:

$$I \cap \langle g_2 \rangle = \langle y^2x \rangle \qquad \text{y} \qquad \frac{y^2x}{4xy^2} = \frac{1}{4}$$

Luego

$$\begin{aligned} I : \langle g_1, g_2 \rangle &= (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle) \\ &= \langle xy + 3y, y^2 \rangle \end{aligned}$$

Por lo tanto:

$$I : J = \langle xy + 3y, y^2 \rangle$$

Capítulo 6

Conclusiones

En los últimos cuarenta años ha sido abordada una transformación dramática en nuestra habilidad para manipular sistemas de ecuaciones polinomiales. Comenzando con el descubrimiento de las bases de Gröbner por B. Buchberger y apoyado por el espectacular crecimiento de las capacidades de las modernas computadoras, muchas herramientas de la geometría algebraica clásica han ganado una gran importancia y a su vez se han hecho más asequibles y aplicables. En este trabajo establecemos los fundamentos de la teoría de Bases de Gröbner. Gracias a los teoremas de Hilbert (Teorema de los ceros fuerte y débil), se logra un vinculo indivisible entre el Algebra conmutativa y la Geometría Algebraica que es de vital importancia en esta tesis. Como aplicaciones de la teoría de Bases de Gröbner se resolvieron los siguientes problemas: Todo ideal es con respecto al anillo de polinomios $\mathbf{K}[x_1, \ldots, x_n]$.

- Pertenencia en un Ideal.
- Consistencia de un sistema de ecuaciones polinomiales.
- Determinar si el conjunto solución de un sistema de ecuaciones polinomiales es finito o no.
- Resolución de un sistema de ecuaciones polinomiales.
- Determinación de la intersección de dos ideales.
- Pertenencia en un radical de un ideal.
- Determinación de un ideal cociente.

En 1965 Buchberger introdujo el concepto de Base de Gröbner para un ideal del anillo de polinomios conmutativos, desde entonces, la teoría de Bases de Gröbner ha experimentado un notable desarrollo, tanto en el terreno teórico como en el de sus aplicaciones. A juzgar por los expertos, la variedad de campos donde se están aplicando con éxito estas nuevas herramientas alienta las expectativas de los investigadores. "Modelos para movimiento de robots, estados de equilibrio de ecuaciones de cinética química , diseño de experimentos en estadística, configuraciones moleculares, diseño asistido por computadora, diseño algebraico de controladores, problemas de optimización combinatoria, estudio de redes bayesianas (independencia de variables aleatorias discretas), análisis de sistemas dinámicos con finitos estados, que modelan en particular sistemas biológicos y las aplicaciones económicas derivadas del calculo de equilibrios de Nash", nos dan una muestra de la diversidad de campos donde se aplica esta teoría.

Espero que el contenido de este trabajo, sea el inicio y la motivación a los lectores para un estudio mas especializado sobre este tema.

Apéndice A

Factorización única

Definición A.0.1

Sea $\mathbf{K}$ un cuerpo. Un polinomio de $f \in \mathbf{K}[x_1, \ldots, x_n]$ es irreducible sobre $\mathbf{K}$, si f es no constante y no se puede expresar como el producto de dos polinomios no constantes en $\mathbf{K}[x_1, \ldots, x_n]$.

El concepto de irreducible depende del campo, así: $x^2 + 1$ es irreducible sobre $\mathbf{Q}$ y $\mathbf{R}$ pero no sobre $\mathbf{C}$: $x^2 + 1 = (x + i)(x - i)$.

Proposición A.0.1

Cada polinomio no constante $f \in \mathbf{K}[x_1, \ldots, x_n]$ puede ser escrito como el producto de polinomios los cuales son irreducibles sobre $\mathbf{K}$.

Demostración

Si f es irreducible sobre $\mathbf{K}$, no hay nada que probar.

En otro caso, existen $g, h \in \mathbf{K}[x_1, \ldots, x_n]$ no constante tal que $f = gh$. Es claro que el grado de g y h es menor que f. Si g o h no fuesen irreducibles, se puede seguir descomponiendo, y esta puede dar un número finitos de pasos, por lo tanto se verifica. □

En el teorema (A.0.2) se mostrará que esta factorización es única.

Teorema A.0.1

Sea $f \in \mathbf{K}[x_1, \ldots, x_n]$ un polinomio irreducible sobre $\mathbf{K}$ y supongamos que f divide al producto gh donde $gh \in \mathbf{K}[x_1, \ldots, x_n]$. Entonces f divide a g o h.

Demostración

Por indución sobre el número de variables.

(i) Cuando $n = 1$. Sea $p = MCD(f, g)$ entonces $f = kp$. Si p es no constante, como f es un polinomio irreducible se tiene que k es una constante. Ahora como p divide a g entonces kp divide a g luego f divide a g.

En el otro caso, si p es constante. Se sabe que $\langle f, g\rangle = \langle p\rangle$, debido a que $\langle p\rangle = k[x_1]$ entonces $1 \in \langle f, g\rangle$. Luego existen $A,\ B \in \mathbf{K}[x_1]$ tal que $1 = Af + Bg$ entonces $h = Afh + Bgh$, como f divide a gh entonces $gh = q \cdot f$, para algún $q \in \mathbf{K}[x_1]$. Entonces $h = Afh + Bq \cdot f = (Ah + Bq)f$. Por lo tanto f divide a h.

(ii) Asumamos que el teorema es válido para $n - 1$ variables.

(iii) Afirmación 1: Sea $u \in \mathbf{K}[x_2, \ldots, x_n]$ irreducible. Si u divide a $gh \in \mathbf{K}[x_1, \ldots, x_n]$ entonces u divide a g o u divide a h.

En efecto

Notación: Si p divide a q, lo simbolizaremos así: $p|q$.

Si p no divide a q: $p \nmid q$

Escribamos

$$g = \sum_{i=0}^{l} a_i x_1^i, \quad h = \sum_{i=0}^{m} b_i x_1^i, \quad \text{donde } a_i,\ b_i \in \mathbf{K}[x_2, \ldots, x_n]$$

Supongamos que u no divide a ninguno de los dos polinomios: g y h. Entonces existen $i, j \geq 0$ tal que

$$\begin{aligned} u &\quad \text{no divide a } a_i, \\ u &\quad \text{no divide a } b_j, \end{aligned} \tag{A.1}$$

Podemos asumir que i y j son los valores menores que cumplen con dicha situación.

En el desarrollo de gh existe un término de la forma $C_{i+j}x_1^{i+j}$ donde

$$C_{i+j} = (a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0)$$

por ser i, j valores mínimos hallados, u divide a cada uno de los paréntesis ya que:

$$u|a_0,\ u|a_1, \ldots, u|a_{i-1}$$

$$u|b_{j-1},\ u|b_{j-2}, \ldots, u|b_0$$

como $u|(gh)$, divide a cada uno de los coeficientes de x_1 en gh por lo tanto $u|C_{i+j}$ entonces $u|(a_ib_j)$ pero como u tiene $n-1$ variables ($\mathbf{K}[x_2, \ldots, u_n]$), por hipótesis inductiva $u|a_i$ o $u|b_j$ lo cual va en contradicción con la ecuación (A.1). Por lo tanto la afirmación 1 se verifica.

Veamos el caso general.

Supongamos que $f|gh$.

(a) Si f no depende de x_1, la afirmación 1 hace que se cumpla lo pedido.

(b) Si f es no constante que dependa de x_1. Se usará $\mathbf{K}(x_2, \ldots, x_n)[x_1]$ el cual es un anillo de polinomios en una variable de x_1, sobre el campo $\mathbf{K}(x_2, \ldots, x_n)$ donde los elementos de este campo es el cociente de polinomios en $\mathbf{K}[x_2, \ldots, x_n]$. Podemos considerar también a $\mathbf{K}[x_1, \ldots, x_n]$ dentro de $\mathbf{K}(x_2, \ldots, x_n)[x_1]$.

Afirmación 2. $f \in \mathbf{K}[x_1, \ldots, x_n]$ es irreducible como elememto de $\mathbf{K}(x_2, \ldots, x_n)[x_1]$.

Demostración

Sea $f = AB$ una factorización en $\mathbf{K}(x_2, \ldots, x_n)[x_1]$. A y B son polinomios en x_1, con coeficientes en $\mathbf{K}(x_2, \ldots, x_n)$. Mostraremos que A o B tiene grado 0 en x_1.

Sea $d \in \mathbf{K}[x_2, \ldots, x_n]$ el producto de todos los denominadores en A y B. Entonces $\widetilde{A} = dA$, $\widetilde{B} = dB$ están en $\mathbf{K}[x_1, \ldots, x_n]$ y como $f = AB$ entonces

$$d^2f = dA \cdot dB$$

luego

$$d^2 f = \widetilde{A}\widetilde{B} \text{ en } \mathbf{K}[x_1, \ldots, x_n] \tag{A.2}$$

por la proposición A.0.1, podemos escribir d^2 como el producto de factores irreducibles en $\mathbf{K}[x_2, \ldots, x_n]$. Además por la afirmación 1 y $d^2|\widetilde{A}\widetilde{B}$, cada uno de ellos divide a $\widetilde{A}$ o $\widetilde{B}$ pero como $\widetilde{A} = dA$ y $\widetilde{B} = dB$, dicho factor de d^2, no puede dividir a d, luego debe dividir a A ó a B.

Cancelando dicho factores en ambos lados de la ecuación (A.2) y asi con los otros factores primos de d^2 se obtiene:

$$f = \widetilde{A_1}\widetilde{B_1} \text{ en } \mathbf{K}[x_1, \ldots, x_n]$$

Desde que f es irreducible en $\mathbf{K}[x_1, \ldots, x_n]$ entonces $\widetilde{A}_1$ ó $\widetilde{B}_1$ es una constante.

Sea $\widetilde{A}_1$ constante en $\mathbf{K}[x_1, \ldots, x_n]$, como

$$\widetilde{A} = dA$$

y

$$d \in \mathbf{K}[x_2, \ldots, x_n], \qquad A \in \mathbf{K}(x_2, \ldots, x_n)[x_1]$$

A no tiene como indeterminada a x_1, luego $A \in \mathbf{K}(x_2, \ldots, x_n)$ luego debido a que $f = AB$ entonces f es irreducible y se verifica la afirmación 2.

Ahora que f es irreducible en $\mathbf{K}(x_2, \ldots, x_n)[x_1]$, por el caso $n = 1$ se tiene $f|g$ ó $f|h$ en $\mathbf{K}(x_2, \ldots, x_n)[x_1]$ digamos $g = Af$ para $A \in \mathbf{K}(x_2, \ldots, x_n)[x_1]$, entonces

$$dg = dAf$$

donde, d es el producto de todos los denominadores en A.

Entonces

$$dg = \widetilde{A}f \text{ en } \mathbf{K}[x_1, \ldots, x_n], \quad \widetilde{A} = dA, \quad d \in \mathbf{K}[x_2, \ldots, x_n] \tag{A.3}$$

Por afirmación 1, cada factor irreductible de d divide a $\widetilde{A}$ ó a f pero como f es irreductible y depende de x_1 con grado positivo en x_1, d no puede dividir a f entonces $d|\widetilde{A}$ en la ecuación (A.3) podemos cancelar todos los factores irreducibles de d entonces

$$g = \widetilde{c}f$$

luego

$$f|g \text{ en } \mathbf{K}[x_1, \ldots, x_n]$$

Esto completa la prueba. □

Corolario A.0.1

Supongamos que $f, g \in \mathbf{K}[x_1, \ldots, x_n]$ tiene grado positivo en x_1. Entonces f y g tiene un factor común en $\mathbf{K}[x_1, \ldots, x_n]$ de grado positivo en x_1 si y solo si existe un factor común en $\mathbf{K}(x_2, \ldots, x_n)[x_1]$.

Demostración

($\Longrightarrow$) Si f y g tienen un factor común h en $\mathbf{K}[x_1, \ldots, x_n]$ de grado positivo en x_1, pero como dicho factor común también lo es en $\mathbf{K}(x_2, \ldots, x_n)[x_1]$, luego se verifica.

($\Longleftarrow$) Supongamos que f y g tienen un factor en común $\widetilde{h} \in \mathbf{K}(x_2, \ldots, x_n)[x_1]$, entonces

$$f = \widetilde{h}\widetilde{f_1}$$

$$g = \widetilde{h}\widetilde{g_1}, \quad \widetilde{f_1}, \widetilde{g_1} \in \mathbf{K}(x_2, \ldots, x_n)[x_1]$$

Sea además $d \in \mathbf{K}[x_2, \ldots, x_n]$ el denominador en común de los polinomios $\widetilde{h}$, $\widetilde{f_1}$ y $\widetilde{g_1}$.

Considerando

$$h = d\widetilde{h}$$

$$f_1 = d\widetilde{f_1}$$

$$g_1 = d\widetilde{g_1} \in \mathbf{K}[x_1, \ldots, x_n]$$

como $f = \widetilde{h}\widetilde{f_1}$ entonces

$$d^2 f = d\widetilde{h} \cdot d\widetilde{f_1}$$

luego

$$d^2 f = h f_1$$

Igualmente $g = \widetilde{h}\widetilde{g_1}$ entonces

$$d^2 g = d\widetilde{h} \cdot d\widetilde{g_1}$$

luego

$$d^2 g = h g_1 \text{ en } \mathbf{K}[x_1, \ldots, x_n]$$

Como $\widetilde{h}$ no es una constante en $\mathbf{K}(x_2, \ldots, x_n)[x_1]$ y $h = d\widetilde{h}$ además $d \in \mathbf{K}[x_2, \ldots, x_n]$, se tiene h posee un factor irreducible h_1 de grado postivo en x_1.

Como $d^2 f = h f_1$ entonces por el teorema (A.0.1)

$$h_1 | d^2 \quad \text{ó} \quad h_1 | f$$

Pero $h_1 \nmid d^2$ ya que $d^2 \in \mathbf{K}[x_2, \ldots, x_n]$ entonces

$$h_1 | f \text{ en } \mathbf{K}[x_1, \ldots, x_n]$$

De manera similar se tiene

$$d^2 g = h g_1$$

entonces

$$h_1 | d^2 \quad \text{ó} \quad h_1 | g$$

entonces

$$h_1 | g$$

Por lo tanto se tiene lo buscado, h_1 es el factor en común de f y g en $\mathbf{K}[x_1, \ldots, x_n]$ □

Teorema A.0.2

Cada polinomio no constante $f \in \mathbf{K}[x_1, \ldots, x_n]$ puede ser escrito como el producto de $f = f_1 \cdot f_2 \cdot \ldots \cdot f_r$ de irreducibles en $\mathbf{K}[x_1, \ldots, x_n]$. Además, si $f = g_1 \ldots g_s$ es otra

factorización de irreducibles en $\mathbf{K}$, entonces $r = s$ y f_i es un multiplo constante de g_i para alguna permutación.

Demostración

La primera parte es la proposición (A.0.1).

Por el teorema (A.0.1) y por un proceso de inducción matemática se cumple que si g es irreducible y divide al producto $h_1, \ldots, h_s$ entonces f divide a h_i para algún i.

Ahora, como

$$f_i | f = g_1, \ldots, g_s$$

podemos considerar

$$f_1 | g_1 \Longrightarrow g_1 = k_1 f_1, \quad k_1 \in \mathbf{K}$$

multiplo constante de f_1, luego

$$\begin{aligned} \text{como} \quad f_1 f_2 \ldots f_r &= g_1 g_2 \cdots g_s \\ &= (k_1 f_1) g_2 \ldots g_s \end{aligned}$$

entonces

$$f_2 \ldots f_r = k_1 g_2 \ldots g_s$$

procediendo de igual forma se obtiene $r \leq s$.

Igualmente si consideramos que $g_1 | f_1$, $s \leq r$. Por lo tanto

$$r = s \quad \text{y} \quad f_i = k_i g_i, \ \forall i = 1, \ldots, r \quad \text{con} \quad k_i \in \mathbf{K} \quad \square$$

Apéndice B

Resultantes

Lema B.0.3

Sea $f, g \in \mathbf{K}[x]$ polinomios de grados $l > 0$ y $m > 0$ respectivamente.

Entonces f y g tienen un factor no constante en común si y sólo si existen polinomios A y B en $\mathbf{K}[x]$ tal que:

(i) A y B son polinomios no nulos.

(ii) $grad(A) \leq m - 1$ y $grad(B) \leq l - 1$

(iii) $Af + Bg = 0$

Demostración

($\Longrightarrow$) Asumamos que f y g tienen un factor no constante en común $h \in \mathbf{K}[x]$.

Entonces $f = hf_1$ y $g = hg_1$, donde f_1, $g_1 \in \mathbf{K}[x]$.

Se nota que

$$grad(f_1) \leq l - 1 \quad \text{y} \quad grad(g_1) \leq m - 1$$

Entonces considerando $A = g_1$, $B = -f_1$, son polinomios no nulos y poseen $grad(A) \leq m - 1$, $\quad grad(B) \leq l - 1$.

También se tiene

$$\begin{aligned} Af + Bg &= g_1 f + (-f_1)g \\ &= g_1 h f_1 - f_1 h g_1 \\ &= 0 \end{aligned}$$

entonces

$$Af + Bg = 0$$

($\Longleftarrow$) Recíprocamente, supongamos que f y g no tienen ningún factor en común, luego

$$MCD(f, g) = 1$$

entonces existen $\widetilde{A},\ \widetilde{B} \in \mathbf{K}[x]$ tal que

$$\widetilde{A}f + \widetilde{B}g = 1$$

entonces

$$B\widetilde{A}f + B\widetilde{B}g = B$$

pero por (iii) $Bg = -Af$ entonces

$$B\widetilde{A}f - \widetilde{B}Af = B$$

luego

$$B = (\widetilde{A}B - \widetilde{B}A)f$$

Como $B \neq 0$, $grad(B) \geq l$, pero esto es contradictorio con (ii).

Por lo tanto f y g tienen un factor en común de grado positivo. □

Encontrar los polinomios A y $B \in \mathbf{K}[x]$ que cumplan tales condiciones no siempre es facil hallarlos. Con el algebra lineal nos permite relacionarlos de la manera siguiente.

Escribamos

$$\begin{aligned} A &= c_0 x^{m-1} + \ldots + c_{m-1} \\ B &= d_0 x^{l-1} + \ldots + d_{l-1} \end{aligned}$$

donde consideramos $l+m$ coeficientes: $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{l-1}$ como variables.

Nuestra meta es hallar $c_i, d_i \in \mathbf{K}$ no todos ceros tal que

$$Af + Bg = 0$$

donde

$$f = a_0x^l + \ldots + a_l, \quad a_0 \neq 0$$

$$g = b_0x^m + \ldots + b_m, \quad b_0 \neq 0 \text{ donde } a_i, b_i \in \mathbf{K}$$

Si desarrollamos $Af + Bg = 0$, obtenemos un sistema de ecuaciones lineales con incognitas c_i y d_i, con coeficientes en a_i, b_i.

$$\begin{array}{lllllll} a_0c_0 & & + & b_0d_0 & & = 0, & \text{coeficientes de } x^{l+m-1} \\ a_1c_0 & + & a_0c_1 & + & b_1d_0 + b_0d_1 & = 0, & \text{coeficientes de } x^{l+m-2} \end{array} \tag{B.1}$$

$$a_lc_{m-1} + b_md_{l-1} = 0, \quad \text{coeficientes de } x^0$$

En este sistema existen $l+m$ ecuaciones lineles y $l+m$ variables.

Se sabe que el sistema posee solución no nula si y solo si la matriz de coeficientes tiene determinante cero.

Esto nos sugiere la definición siguiente.

Definición B.0.2

Dados dos polinomios f, $g \in \mathbf{K}[x]$ de grado positivo, de la forma

$$f = a_0x^l + \ldots a_l, \quad a_0 \neq 0$$

$$g = b_0x^m + \ldots b_m, \quad b_0 \neq 0$$

La Matriz Sylvester de f y g con respecto a x, denotado por $Syl(f,g,x)$ es la matriz de coeficientes del sistema de ecuaciones dada en la ecuación (B.1). Así, $Syl(f,g,x)$ es una matriz de orden $(m+l)\times(m+l)$:

$$Syl(f,g,x) = \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & \ddots & \ddots & a_0 & \vdots & \vdots & & b_0 \\ a_l & \vdots & & a_1 & b_m & \vdots & & \\ & a_l & & & & b_m & & \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \\ \underbrace{\qquad\qquad\qquad}_{m \text{ columnas}} & & & & \underbrace{\qquad\qquad\qquad}_{l \text{ columnas}} & & & \end{pmatrix}$$

Donde todos los espacios vacíos son ceros. La resultante de f y g con respecto a x denotado por $Res(f,g,x)$ viene dado por el determinante de la matriz de Sylverter.

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

Un polinomio es llamado polinomio entero, si cada uno de sus coeficientes son enteros.

Proposición B.0.2

Dados f, $g \in \mathbf{K}[x]$ de grado positivo, la resultante $Res(f,g,x) \in \mathbf{K}$ es un polinomio entero en los coeficientes de f y g. Además f y g tienen un factor en común en $\mathbf{K}[x]$ si y solo si $Res(f,g,x) = 0$

Demostración

La fórmula estandar para el determinante de la matriz $A = (a_{ij})$, $1 \le i,j \le s$ es:

$$\det(A) = \sum sgn(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \ldots a_{s\sigma(s)} \quad \sigma \text{ es una permutación de } \{1,\ldots,s\}$$

Donde

$sgn(\sigma)$ es $+1$, si σ intercambia un número par de pares de elementos de $\{1,\ldots,s\}$

$sgn(\sigma)$ es -1, si σ intercambia un número impar de pares.

Esto muestra que el determnante es un polinomio entero con respecto a los coeficientes de f y g.

Para la segunda parte de la proposición.

($\Longrightarrow$) Si f y g tienen un factor en común, entonces por el lema (B.0.3)

$$\exists\ A \ \text{ y } \ B \in \mathbf{K}[x] \ \text{ no nulos tal que } \ Af + Bg = 0$$

Luego el sistema (B.1) tiene una solución no trivial. En consecuencia el determinante del sistema es cero. Asi $Res(f, g, x) = 0$.

($\Longleftarrow$) Si $Res(f, g, x) = 0$ entonces el sistema (B.1) tiene solución no nulo. Luego existe A, B no nulos que cumplan con (i), (ii) y (iii) del lema (B.0.3). De este modo f y g tienen un factor en común. $\square$

Ejemplo B.0.2

Se verá si

$$f = 2x^2 + 3x + 1 \quad \text{y} \quad g = 7x^2 + x + 3$$

tienen un factor común en $\mathbf{Q}[x]$.

$$Res(f, g, x) = \begin{pmatrix} 2 & 0 & 7 & 0 \\ 3 & 2 & 1 & 7 \\ 1 & 3 & 3 & 1 \\ 0 & 1 & 0 & 3 \end{pmatrix} = 153 \neq 0$$

entonces no poseen un factor en común.

Proposición B.0.3

Dados f, $g \in \mathbf{K}[x]$ polinomios de grado positivo.

Entonces existen polinomios A, $B \in \mathbf{K}[x]$ tal que

$$Af + Bg = Res(f, g, x)$$

Además los coeficientes de A y B son polinomios enteros en los coeficientes de f y g.

Demostración

(i) Si $Res(f, g, x) = 0$, basta considerar $A = B = 0$.

(ii) Si $Res(f,g,x) \neq 0$, por la proposición (B.0.5) existen $\widetilde{A}$, $\widetilde{B} \in \mathbf{K}[x]$ tal que

$$\widetilde{A}f + \widetilde{B}g = 1 \tag{B.2}$$

Considerando

$$\begin{aligned} f &= a_0x^l + \ldots a_l, \quad +a_0 \neq 0 \\ g &= b_0x^m + \ldots b_m, \quad +b_0 \neq 0 \\ \widetilde{A} &= c_0x^{m-1} + \ldots + c_{m-1} \\ \widetilde{B} &= d_0x^{l-1} + \ldots + d_{l-1} \end{aligned}$$

Donde $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{l-1}$ son desconcidos en $\mathbf{K}$.

Si sustituímos estas expresiones en (B.2) y comparamos los coeficientes de las potencias de x entonces obtenemos el siguiente sistema de ecuaciones lineales donde se desconoce c_i, d_i y los coeficientes a_i, b_i en $\mathbf{K}$

$$\begin{array}{lllllll} a_0c_0 & + & b_0d_0 & & & = 0, & \text{coeficientes de } x^{l+m-1} \\ a_1c_0 + & a_0c_1 & + b_1d_0 + & b_0d_1 & & = 0, & \text{coeficientes de } x^{l+m-2} \\ \ddots & & \ddots & & & & \\ a_lc_{m-1} & & + & b_md_{l-1} & = & 1, & \text{coeficientes de } x^0 \end{array} \tag{B.3}$$

Este sistema es el mismo que en (B.1) excepto el segundo miembro de la última ecuación.

Así la matriz de coeficientes es la matriz de Sylverter de f y g y como

$$Res(f,g,x) \neq 0$$

esto indica que la ecuación (B.3) tiene solución única en $\mathbf{K}$.

Usando cramer

$$c_0 = \frac{1}{Res(f,g,x)} \det \begin{pmatrix} 0 & & & b_0 & & \\ 0 & a_0 & & \vdots & \ddots & \\ \vdots & \vdots & \ddots & \vdots & & b_0 \\ & a_l & & a_0 \; b_m & & \vdots \\ \vdots & & \ddots & \vdots & \ddots & \vdots \\ 1 & & & a_l & & b_m \end{pmatrix}$$

Desde que el determinante es un polinomio entero, sigue que

$$c_0 = \frac{\text{un polinomio entero en } a_i,\ b_i}{Res(f,g,x)}$$

De este modo se puede obtener también para los otros coeficientes c_i y d_i.

Ahora desde que $\widetilde{A} = c_0 x^{m-1} + \ldots + c_{m-1}$, podemos reemplazarlo y como tienen un denominador en común $Res(f,g,x)$ se puede escribir

$$\widetilde{A} = \frac{1}{Res(f,g,x)} A, \quad \text{donde} \quad A \in \mathbf{K}[x]$$

y los coeficientes de A son polinomios enteros en a_i, b_i.

De manera similar, podemos escribir

$$\widetilde{B} = \frac{1}{Res(f,g,x)} B, \quad \text{donde} \quad B \in \mathbf{K}[x]$$

Tiene la misma propiedad en común que A.

Entonces

$$\widetilde{A} f + \widetilde{B} g = 1$$

luego

$$Af + Bg = Res(f,g,x) \quad \square$$

Ahora adaptaremos la teoría de resultantes en el caso de polinomios en n variables. Sean $f, g \in \mathbf{K}[x_1, \ldots, x_n]$ de grado positivo en x_1 escribiendo

$$f = a_0 x_1^l + \ldots + a_l, \quad a_0 \neq 0$$

$$g = b_0 x_1^m + \ldots + b_m, \quad b_0 \neq 0$$

donde a_i, $b_i \in \mathbf{K}[x_1, \ldots, x_n]$.

definamos la resultante de f y g con respecto a x_1 al determinante siguiente

$$Res(f, g, x_1) = \det \begin{pmatrix} a_0 & & & & & \\ & \ddots & & & \ddots & \\ a_1 & & & b_1 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ a_l & & a_1 & b_m & & b_1 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l & & & b_m \\ \underbrace{\qquad\qquad} & & & \underbrace{\qquad\qquad} & & \end{pmatrix}$$

Donde todos los espacios vacios son ceros.

Proposición B.0.4

Sean f, $g \in \mathbf{K}[x_1, \ldots, x_n]$ tienen grado positivo en x_1. Entonces

(i) $Res(f, g, x_1)$ pertenece al ideal de primera eliminación $\langle f, g \rangle \cap \mathbf{K}[x_2, \ldots, x_n]$.

(ii) $Res(f, g, x_1) = 0$ si y solo si f y g tiene un factor en común en $\mathbf{K}[x_1, \ldots, x_n]$ que tiene grado positivo en x_1.

Demostración

(i) Cuando escribimos f y g en términos de x_1, los coeficientes a_i, b_i están en $\mathbf{K}[x_2, \ldots, x_n]$.

Siendo la resultante polinomios enteros en a_i, b_i sigue que

$$Res(f, g, x_1) \in \mathbf{K}[x_2, \ldots, x_n]$$

También existe A y B polinomios en x_1 donde sus coeficientes son polinomios enteros en a_i, b_i según la proposición (B.0.3), tal que

$$Af + Bg = Res(f, g, x_1)$$

Así

$$A, B \in \mathbf{K}(x_2, \ldots, x_n)[x_1] = \mathbf{K}[x_1, \ldots, x_n]$$

Lo cual implica que

$$Res(f, g, x_1) \in \langle f, g \rangle$$

(ii) Para probar la segunda parte, utlizando la proposición (B.0.2). Siendo f y g polinomios en x_1 con coeficientes en $\mathbf{K}[x_2, \ldots, x_n]$, el campo de coeficientes está en $\mathbf{K}(x_2, \ldots, x_n)$ campo de fracciones.

. Entonces aplicando a $f, g \in \mathbf{K}(x_2, \ldots, x_n)[x_1]$ se tiene $Res(f, g, x_1) = 0$ si y solo si tiene un factor común en $\mathbf{K}(x_2, \ldots, x_n)[x_1]$ el cual tiene grado positivo.

Por lo tanto del corolario (A.0.1) nos indica que es equivalente a tener un factor común en $\mathbf{K}[x_1, \ldots, x_n]$ de grado positivo en x_1. □

Corolario B.0.2

Si f, $g \in \mathbf{C}[x]$ entonces $Res(f, g, x) = 0$ si y solo si f y g tiene una raíz común en $\mathbf{C}$.

Demostración

($\Longrightarrow$) Si $Res(f, g, x) = 0$, entonces f y g tienen un factor común en $\mathbf{C}[x]$ con grado positivo en x.

Como $\mathbf{C}$ es algebraicamente cerrado dicho factor común tiene una raíz en $\mathbf{C}$.

($\Longleftarrow$) Si tienen una raíz en común. Luego f y g tienen un factor común. Entonces $Res(f, g, x) = 0$ □

Proposición B.0.5

Dados f, $g \in \mathbf{C}[x_1, \ldots, x_n]$. Sea

$$f = a_0 x_1^l + \ldots a_l$$

$$g = b_0 x_1^m + \ldots b_m, \quad a_0, b_0 \in \mathbf{C}[x_2, \ldots, x_n] \text{ no nulos}$$

Si $Res(f, g, x_1) \in \mathbf{C}[x_1, \ldots, x_n]$ es anulado por $(c_2, \ldots, c_n) \in \mathbf{C}^{n-1}$, entonces se cumple uno de los dos casos:

(i) a_0 ó b_0 es anulado por $(c_2, \ldots, c_n)$

(ii) Existe $c_1 \in C$ tal que f y g es anulado por $(c_1, c_2 \ldots, c_n) \in \mathbf{C}^n$.

Demostración

Considerando $c = (c_2, \ldots, c_n)$

$$f(x_1, c) = f(x_1, c_2, \ldots, c_n)$$

Es suficiente mostrar que $f(x_1, c)$ y $g(x_1, c)$ tiene una raíz en común, cuando $a_0(c)$ y $b_0(c)$ no son nulos.

Para probar esto

$$\begin{aligned} f(x_1, c) &= a_0(c)x_1^l + \ldots a_l(c), \quad a_0(c) \neq 0 \\ g(x_1, c) &= b_0(c)x_1^m + \ldots b_m(c), \quad b_0(c) \neq 0 \end{aligned} \tag{B.4}$$

Por hipótesis $h = Res(f, g, x_1)$ se anula en c

$$0 = h(c) = \det \begin{pmatrix} a_0(c) & & & b_0(c) & & \\ & \ddots & & & \ddots & \\ & & a_0(c) & & & b_0(c) \\ \vdots & & & \vdots & & \\ a_l(c) & & \vdots & b_m(c) & & \vdots \\ & \ddots & & & \ddots & \\ & & a_l(c) & & & b_m(c) \\ \underbrace{\qquad\qquad}_{\text{m columnas}} & & & \underbrace{\qquad\qquad}_{\text{l columnas}} & & \end{pmatrix} \tag{B.5}$$

De la ecuación (B.4) la resultante de $f(x_1, c)$ y $g(x_1, c)$ es exactamente igual al determinante dada en la ecuación (B.5).

Entonces

$$0 = h(c) = Res(f(x_1, c), g(x_1, c), x_1)$$

Por el corolario (B.0.2), $f(x_1, c)$ y $g(x_1, c)$ poseen una raíz en común. Por lo tanto la proposición (B.0.5) está probada. □

Apéndice C

El teorema de extensión

Con los apéndices A, B y el desarrollo del capítulo 4, tenemos lo necesario para probar el teorema de extensón.

En primer lugar veamos el caso especial cuando el ideal es generado por dos polinomios.

Teorema C.0.4 *(El teorema de Extensión para dos polinomios)*

Sea $I = \langle f, g \rangle \subset \mathbf{C}[x_1, \ldots, x_n]$ e I_1 el ideal de primera eliminación de I.

$$f = a_0 x_1^l + \ldots + a_l, \quad a_0 \neq 0$$

$$g = b_0 x_1^m + \ldots + b_m, \quad b_0 \neq 0, \quad a_i,\ b_i \in \mathbf{C}[x_2, \ldots, x_n]$$

Sea $(c_2, \ldots, c_n) \in V(I_1)$ una solución parcial. Si $(c_2, \ldots, c_n) \notin V(a_0, b_0)$.

Entonces existe $c_1 \in \mathbf{C}$ tal que $(c_1, c_2, \ldots, c_n) \in V(I)$.

Demostración

Denotando $c = (c_2, \ldots, c_n)$. De la proposición (B.0.4) se tiene

$$Res(f, g, x_1) \in I_1 \tag{C.1}$$

Por lo tanto, como $c \in V(I_1)$, $Res(f, g, x_1)$ se anula en c.

Ahora, por (B.0.5) existe c_1 tal que f y g es anulado por $c = (c_1, \ldots, c_n) \in \mathbf{C}^n$, (esto es $(c_1, \ldots, c_n) \in V(I)$), siempre que ni a_0 ni b_0 es anulado por c. Veamos esto último.

Supongamos que

$$a_0(c) \neq 0 \quad \text{y} \quad b_0(c) = 0$$

Entonces $g(x_1, c)$ tiene grado en x_1 estrictamnente menor que m.

Afirmación: Si N es un entero positivo arbitrario. Entonces

$$\langle f, g \rangle = \langle f, g + x_1^N f \rangle$$

En efecto.

($\subset$) Sea $h \in \langle f, g \rangle$ entonces para $p, q \in \mathbf{K}[x_1, \ldots, x_n]$

$$\begin{aligned} h &= pf + qg \\ &= pf + q(g + x_1^N f - x_1^N f) \\ &= pf + q(g + x_1^N f) - qx_1^N f \\ &= (p - qx_1^N)f + q(g + x_1^N f) \end{aligned}$$

Entonces

$$h \in \langle f, g + x_1^N f \rangle$$

($\supset$) Sea $h \in \langle f, g + x_1^N f \rangle$ entonces

$$\begin{aligned} h &= pf + q(g + x_1^N f) \\ &= pf + qg + qx_1^N f \\ &= (p + qx_1^N)f + qg \end{aligned}$$

Entonces

$$h \in \langle f, g \rangle$$

Ahora considerando N suficientemente grande de tal manera que $x_1^N f$ tenga mayor grado en x_1 que g. Por lo tanto el coeficiente principal de $g + x_1^N f$ con respecto a x_1 es a_0, el cual es no nulo en c.

Aplicando el argumento previo para f y $g + x_1^N f$, veamos que

$$Res(f, g + x_1^N f, x_1) \in \mathbf{C}[x_2, \ldots, x_n]$$

es anulado en $(c_2, \ldots, c_n) \in \mathbf{C}^{n-1}$, ya que de la ecuación (C.1) la $Res(f, g, x_1)$ se anula para $(c_2, \ldots, c_n) \in \mathbf{C}^{n-1}$. Entonces por la proposición (B.0.5), como a_0 es el coeficiente principal de f y $g + x_1^N f$ en x_1 se tiene que

$$\exists \ c_1 \in \mathbf{C} \quad \text{tal que} \quad (c_1, c_2, \ldots, c_n) \in V(f, g + x_1^N f) = V(f, g) = V(I)$$

Por lo tanto

$$(c_1, \ldots, c_n) \in V(I) \quad \square$$

Para probar el teorema de extensión, para un ideal arbitrario $\langle f_1, \ldots, f_s \rangle \subset \mathbf{C}[x_1, \ldots, x_n]$ necesitamos definir la resultante para mas de dos polinomios. Sean $f_1, f_2, \ldots, f_s \in \mathbf{C}[x_1, x_2, \ldots, x_n] \in \mathbf{C}[x_1, \ldots x_n]$.

Introduciremos nuevas variables $u_2, \ldots\ldots, u_s$

$$u_2 f_2 + \ldots + u_s f_s \in \mathbf{C}[u_2, \ldots, u_s, x_1, \ldots, x_n]$$

Ahora por la proposición (B.0.2), la resultante de f_1 y $u_2 f_2 + \ldots + u_s f_s$ con respecto a x_1 está en $\mathbf{C}[u_2, \ldots, u_s, x_2, \ldots, x_n]$.

Para obtener polinomios en $x_2, \ldots, x_n$ expandimos el resultado en términos de las potencias de $u_2, \ldots, u_s$.

Así

$$Res(f_1, u_2 f_2 + \ldots, + u_s f_s, x_1) = \sum_{\alpha} h_\alpha(x_2, \ldots, x_n) u^\alpha \qquad \text{(C.2)}$$

Donde u^α es el monomio $u_2^{\alpha_2} \ldots u_s^{\alpha_s}$, $h_\alpha \in \mathbf{C}[x_2, \ldots, x_n]$ para cada α.

Se dirá que los polinomios h_α son las resultantes generalizadas de $f_1, \ldots\ldots, f_s$.

Ejemplo C.0.3

Como un ejemplo, calculamos la resultante generalizada de los polinomios

$$f_1 = x^2 + y + z - 1$$

$$f_2 = x + y^2 + z - 1$$

$$f_3 = x + y + z^2 - 1$$

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

Teorema C.0.5 *(El teorema de Extensión)*

Sea $I = \langle f_1, \ldots, f_s \rangle \subset \mathbf{C}[x_1, \ldots, x_n]$ y sea I_1 el ideal de primera eliminación para I.

Para cada $1 \leq i \leq s$

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ términos en el cual } x_1 \text{ tiene grado } < N_i$$

Donde $N_i \geq 0$ y $g_i \in \mathbf{C}[x_2, \ldots, x_n]$ es no nulo.

Supóngase que se tiene una solución parcial $(c_2, \ldots, c_n) \in V(I_1)$.

Si $(c_2, \ldots, c_n) \notin V(g_1, \ldots, g_s)$

Entonces

$$\exists \quad c_1 \in \mathbf{C} \quad \text{tal que} \quad (c_1, c_2, \ldots, c_n) \in V(I)$$

Demostración

Sea $c = (c_2, \ldots, c_n)$, se encontrará una raíz común $c_1 \in \mathbf{C}$ de $f_1(x_1, c), \ldots, f_s(x_1, c)$.

(i) El caso cuando $s = 2$ fué tratado en teorema (C.0.4)

(ii) Para $s = 1$ igualmente $V(f_1) = V(f_1, f_1)$

(iii) El resto de la prueba será para $s \geq 3$.

Como $c \notin V(g_1, \ldots, g_s)$ podemos asumir que $g_1(c) \neq 0$.

Sea $h_\alpha \in \mathbf{C}[x_2, \ldots, x_n]$ de la resultante generalizada de $f_1, \ldots, f_s$.

Así

$$Res(f_1, u_2 f_2 + \ldots + u_s f_s, x_1) = \sum_\alpha h_\alpha u^\alpha \tag{C.3}$$

Afirmación 1: $\forall\ \alpha,\ h_\alpha \in I_1 = I \cap \mathbf{C}[x_2, \ldots, x_n]$

En efecto. Como la resultante está en el anillo $\mathbf{C}[u_2, \ldots, u_s, x_2, \ldots, x_n]$ de la proposición (B.0.3)

$$Af_1 + B(u_2 f_1 + \ldots + u_s f_s) = Res(f_1, u_2 f_2 + \ldots + u_s f_s, x_1) \tag{C.4}$$

Donde $A, B \in \mathbf{C}[u_2, \ldots, u_s, x_2, \ldots, x_n]$.

$$A = \sum_\alpha A_\alpha u^\alpha, \quad B = \sum_\beta B_\beta u^\beta, \quad A_\alpha,\ B_\beta \in \mathbf{C}[x_2, \ldots, x_n]$$

Considerando $e_2 = (1, 0, \ldots, 0), \ldots, e_s = (0, \ldots, 0, 1)$ asi

$$u_2 f_2 + \ldots + u_s f_s = \sum_{i \geq 2} u^{e_i} f_i$$

Veamos que de las ecuaciones (C.3) y (C.4)

$$\sum_{\alpha} h_\alpha u^\alpha = (\sum_{\alpha} A_\alpha u^\alpha) f_1 + (\sum_{\beta} B_\beta u^\beta)(\sum_{i\geq 2} u^{e_i} f_i)$$

como $f_1 \in \mathbf{C}[x_1, \ldots, x_n]$

$$= \sum_{\alpha} (A_\alpha f_1) u^\alpha + \sum_{i\geq 2,\beta} B_\beta f_i u^{\beta+e_i}$$

$$= \sum_{\alpha} (A_\alpha f_1) u^\alpha + \sum_{\alpha} (\sum_{i\geq 2,\beta} B\beta f_i) u^\alpha$$

$$\beta + e_i = \alpha$$

$$= \sum_{\alpha} (A_\alpha f_1 + \sum_{i\geq 2,\beta} B_\beta f_i) u^\alpha$$

$$\beta + e_i = \alpha$$

Igualando coeficientes

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

$$\beta + e_i = \alpha$$

Entonces

$$h_\alpha \in \langle f_1, \ldots, f_s \rangle = I$$

Luego $h_\alpha \in I$, $\forall\ \alpha$. Esto demuestra la afirmación 1.

Desde que $c \in V(I_1)$ y $h_\alpha \in I_1$, $\forall\ \alpha$, entonces $h_\alpha(c) = 0$, $\forall\ \alpha$.

De la ecuación (C.3) la resultante

$$h = Res(f_1, u_2 f_2 + \ldots + u_s f_s, x_1) \quad \text{se anula en} \quad c$$

$$h(c, u_2, \ldots, u_s) = 0 \tag{C.5}$$

Asumamos que

$$g_2(c) \neq 0 \quad \text{y} \quad f_2 \quad \text{tiene grado en} \quad x_1 \quad \text{mayor que en} \quad f_3, \ldots, f_s \tag{C.6}$$

Como

$$h(c, u_2, \ldots, u_s) = Res(f_1(x_1, c), u_2 f_2(x_1, c) + \ldots + u_s f_s(x_1, c), x_1) \tag{C.7}$$

De la ecuación (C.5) y (C.7)

$$Res(f_1(x_1, c), u_2 f_2(x_1, c) + \ldots + u_s f_s(x_1, c), x_1) = 0$$

Luego por la proposición (B.0.4), los polinomios

$$f_1(x_1, c) \text{ y } \; u_2 f_2(x_1, c) + \ldots + u_s f_s(x_1, c), x_1) \in \mathbf{C}[x_1, u_2, \ldots, u_s]$$

poseen un factor en común F de grado positivo en x_1. Desde que F divide a $f_1(x_1, c)$ entonces $F \in \mathbf{C}[x_1]$ también

$$F(x_1) \cdot A(x_1, u_2, \ldots, u_s) \;\; = \;\; u_2 f_2(x_1, c) + \ldots + u_s f_s(x_1, c)$$

$$\text{para algún} \;\; A \in \mathbf{C}[x_1, u_2, \ldots, u_s]$$

comparando los coeficientes de $u_2, \ldots, u_s$ se tiene que F divide a

$$f_2(x_1, c), \ldots, f_s(x_1, c)$$

Entonces F es un factor en común de grado positivo de todos los $f_i(x_1, c)$

Sea c_1 una raíz de F (existe tal raíz en $\mathbf{C}$), entonces se obtiene lo que se estaba buscando c_1 es una raíz común para los $f_i(x_1, c)$.

Finalmente, si la ecuación (C.6) no es verdadera, para $f_1, \ldots, f_s$ entonces reemplazando f_2 por $f_2 + x_1^N f_1$ donde N es entero positivo. Pues

$$I = \langle f_1, f_2 + x_1^N f_1, f_3, \ldots, f_s \rangle$$

En efecto.

($\subset$) Sea $p \in I$

Entonces

$$p = \gamma_1 f_1 + \ldots + \gamma_s f_s, \quad \gamma_i \in \mathbf{K}[x_1, \ldots, x_n]$$

Entonces

$$\begin{aligned} p &= \gamma_1 f_1 + \gamma_2 f_2 + \gamma_2 x_1^N f_1 - \gamma_2 x_1^N f_1 + \gamma_2 x_1^N f_1 + \gamma_3 f_3 + \ldots + \gamma_s f_s \\ &= (\gamma_1 - \gamma_2 x_1^N) f_1 + \gamma_2 (f_2 + x_1^N f_1) + \gamma_3 f_3 + \ldots + \gamma_s f_s \end{aligned}$$

($\supset$) Directo.

Si N es suficientemente grande, el coeficiente de $f_2 + x_1^N f_1$ será el g_1, el cual no se anula en C.

Podemos asumir que $f_2 + x_1^N f_1$ tiene el grado mayor en x_1 que en $f_3, \ldots, f_s$.

Luego repitiendo el proceso anterior se obtendría un $c_1 \in \mathbf{C}$ raíz en común de

$$f_1(x_1, c), f_2(x_1, c) + x_1^N f_1(x_1, c), f_3(x_1, c), \ldots, f_s(x_1, c)$$

entonces $c_1 \in \mathbf{C}$ es una raiz en común de todas las $f_i(x_1, c)$. $\square$

Apéndice D

Variedades finitas

Definición D.0.3

Se $I \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal y $f, g \in \mathbf{K}[x_1, \ldots, x_n]$. Diremos que f y g son congruentes módulo I y lo escribiremos

$$f \equiv g \; mod \; I, \quad \text{si} \quad f - g \in I$$

Ejemplo D.0.4

Por ejemplo, si

$$I = \langle x^2 - y^2, x + y^3 + 1 \rangle \subset \mathbf{K}[x, y]$$

entonces

$$f = x^4 - y^4 + x \quad \text{y} \quad g = x + x^5 + x^4 y^3 + x^4$$

son congruentes módulo I, desde que

$$\begin{aligned} f - g &= x^4 - y^4 - x^5 - x^4 y^3 - x^4 \\ &= (x^2 + y^2)(x^2 - y^2) - (x^4)(x + y^3 + 1) \in I \end{aligned}$$

La propiedad más importante de la relación de congruencia es dada por la siguiente proposición.

Proposición D.0.6

Sea $I \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal.

La congruencia módulo I es una relación de equivalencia en $\mathbf{K}[x_1, \ldots, x_n]$.

Demostración

(i) Es reflexiva: Desde que $f - f = 0 \in I$ cada $f \in \mathbf{K}[x_1, \ldots, x_n]$

(ii) Es simétrica: Supóngase que $f \equiv g \ mod \ I$.

Entonces

$$f - g \in I$$

Luego

$$g - f = (-1)(f - g) \in I.$$

Por lo tanto

$$g \equiv f \ mod \ I$$

(iii) Es transitiva. Si $f \equiv g \ mod \ I$ y $g \equiv h \ mod \ I$, entonces

$$f - g, g - h \in I$$

Desde que I es de clausura bajo la adición, se tiene

$$f - g + g - h = f - h \in I$$

Por lo tanto

$$f \equiv h \ mod \ I \quad \square$$

Definición D.0.4

El cociente de $\mathbf{K}[x_1, \ldots, x_n]$ modulo I, escrito como

$$\mathbf{K}[x_1, \ldots, x_n]/I$$

es el conjunto clases de equivalencia para la congruencia módulo I

$$\mathbf{K}[x_1, \ldots, x_n]/I = \{[f] : \ f \in \mathbf{K}[x_1, \ldots, x_n]\}$$

Como $\mathbf{K}[x_1, \ldots, x_n]$ es un anillo, dado dos clases cualesquiera $[f], [g] \in \mathbf{K}[x_1, \ldots, x_n]/I$, se define dos operaciones con clases usando las correspondientes operaciones con los elementos de $\mathbf{K}[x_1, \ldots, x_n]$.

$$\begin{aligned} \left[f \right] + \left[g \right] &= \left[f + g \right] \\ \left[f \right] \cdot \left[g \right] &= \left[f \cdot g \right] \end{aligned} \tag{D.1}$$

Es directo mostrar que si $f' \in [f]$ y $g' \in [g]$ entonces

$$\left[f' + g' \right] = \left[f + g \right]$$

$$\left[f' \cdot g' \right] = \left[f \cdot g \right]$$

Mostrando así que dichas operaciones están bién definidas.

También se tiene que $\mathbf{K}[x_1, \ldots, x_n]/I$ satisface todos los axiomas de anillo conmutativo con las operaciones antes mencionadas.

Proposición D.0.7

Fijando un orden monomial en $\mathbf{K}[x_1, \ldots, x_n]$ y sea $I \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal. Como en el capítulo 2, $\langle Tp(I) \rangle$ denota el ideal generado por los términos principales de los elementos de I.

(i) Cada $f \in \mathbf{K}[x_1, \ldots, x_n]$ es congruente módulo I a un único polinomio r el cual es una k-combinación lineal de los monomios en el complemento de $\langle Tp(I) \rangle$.

(ii) Los elementos de $\{x^\alpha : x^\alpha \notin \langle Tp(I) \rangle\}$ son linealmente independientes módulo I. Esto es, si

$$\sum_\alpha c_\alpha x^\alpha \equiv 0 \bmod I, \quad c_\alpha \in \mathbf{K}$$

Donde los x^α están en el complemento de $\langle Tp(I) \rangle$. Entonces $c_\alpha = 0$ para todo α.

Demostración

(i) Sea G una base de Gröbner para I y $f \in \mathbf{K}[x_1, \ldots, x_n]$.

Por el algoritmo de la división, el residuo $r = \overline{f}^G$ satisface

$$f \equiv q + r, \quad \text{donde} \quad q \in I$$

Luego $f - r = q \in I$ por lo tanto

$$f \equiv r \bmod I$$

El algoritmo de la división igualmente nos indica que r es una k-combinación lineal de monomios $x^\alpha \notin \langle Tp(I) \rangle$.

La unicidad de r proviene de la proposición (2.5.1).

(ii) El argumento para establecer esta parte de la proposición, es esencialmente la misma como en la prueba de la unicidad del resto en la proposición (2.5.1).

Es decir, si

$$\sum_\alpha c_\alpha x^\alpha \equiv 0 \bmod I, \quad \text{donde } x^\alpha \notin \langle Tp(I) \rangle, \ c_\alpha \in \mathbf{K}$$

Entonces

$$\sum_\alpha c_\alpha x^\alpha \in I$$

Si

$$\sum_\alpha c_\alpha x^\alpha \neq 0$$

Entonces

$$Tp(\sum_\alpha c_\alpha x^\alpha) \in \langle Tp(I) \rangle$$

Luego $Tp(\sum_\alpha c_\alpha x^\alpha)$ es divisible por $Tp(g)$ para algún $g \in I$ pero esto no se puede dar ya que ningún x^α está en $\langle Tp(I) \rangle$.

Por lo tanto

$$\sum_\alpha c_\alpha x^\alpha = 0$$

Como x^α son monomios, se tiene

$$c_\alpha = 0, \quad \forall\, \alpha \quad \square$$

Ejemplo D.0.5

Sea

$$I = \langle xy^3 - x^2, x^3y^2 - y \rangle \quad \text{en} \quad \mathbf{R}[x, y]$$

y con el orden lexicográfico graduado, se tiene

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

una base de Gröbner para I. Luego

$$\langle Tp(I) \rangle = \langle x^3y^2, x^4, xy^3, y^4 \rangle$$

Podemos graficar en $\mathbf{Z}^2_{\geq 0}$ los vectores exponentes de todos los monomios en $\langle Tp(I) \rangle$.

Asi sea

$$\alpha(1) = (3, 2), \ \alpha(2) = (4, 0), \ \alpha(3) = (1, 3), \ \alpha(4) = (0, 4),$$

Son los vectores exponentes de los generadores de $\langle Tp(I) \rangle$.

Asi los elementos de

$$\left((3, 2) + \mathbf{Z}^2_{\geq 0}\right) \cup \left((4, 0) + \mathbf{Z}^2_{\geq 0}\right) \cup \left((1, 3) + \mathbf{Z}^2_{\geq 0}\right) \cup \left((0, 4) + \mathbf{Z}^2_{\geq 0}\right)$$

Son los vectores exponentes de todos los monomios en $\langle Tp(I) \rangle$.

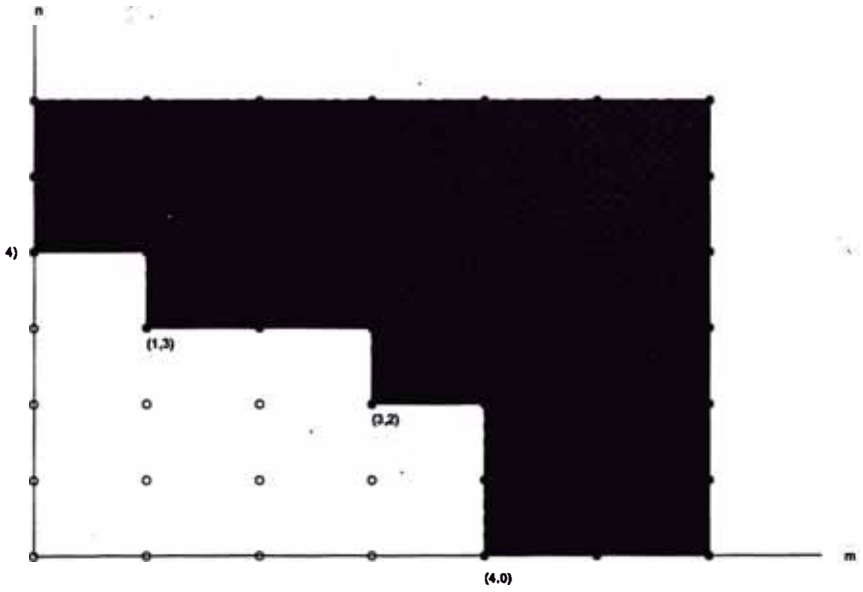


Fig.(3) $(m,n) \longleftrightarrow x^m y^n$

Dado cualquier $f \in \mathbf{R}[x,y]$, la proposición (D.0.7) implica que el resto $\overline{f}^G$ es una $\mathbf{R}$-combinación lineal de 12 monomios

$$1, x, x^2, x^3, y, xy, x^2y, x^3y, y^2, xy^2, x^2y^2, y^3$$

no contenidos en la gráfica sombreada.

Proposición D.0.8

Sea $I \subset \mathbf{K}[x_1, \ldots, x_n]$ un ideal. Entonces $\mathbf{K}[x_1, \ldots, x_n]/I$ es isomorfo como $\mathbf{K}$-espacio vectorial a $S = span(x^\alpha : \ x^\alpha \notin \langle Tp(I) \rangle)$

Demostración

Por la proposición (D.0.7), la función

$$\phi : \mathbf{K}[x_1, \ldots, x_n]/I \longrightarrow S$$

Donde

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

está bien definida y es una biyección entre las clases en $\mathbf{K}[x_1, \ldots, x_n]/I$ y los elementos de S.

Solo falta verificar que ϕ preserva operaciones en el $\mathbf{K}$-espacio vectorial.

Consideremos la operación suma en $\mathbf{K}[x_1, \ldots, x_n]/I$ dada en la ecuación (D.1).

Si $[f]$, $[g]$ son elementos de $\mathbf{K}[x_1, \ldots, x_n]/I$, entonces por la proposición (D.0.7) podemos estandarizar nuestras representaciones por el resto al dividirlo por una base de Gröbner G para I.

Por el algoritmo de la división y la unicidad del resto al dividirla por una base de Gröbner G, se tiene

$$\overline{f+g}^G = \overline{f}^G + \overline{g}^G$$

así se tiene, si

$$\overline{f}^G = \sum_\alpha c_\alpha x^\alpha \quad \text{y} \quad \overline{g}^G = \sum_\alpha d_\alpha x^\alpha \quad \text{donde } x^\alpha \notin \langle Tp(I) \rangle$$

Entonces

$$\overline{f+g}^{G} = \sum_{\alpha}(c_\alpha + d_\alpha)x^\alpha$$

Así tenemos

$$\begin{aligned}\phi([f]+[g]) &= \phi([f+g]) \\ &= \overline{f+g}^{G} \\ &= \overline{f}^{G} + \overline{g}^{G} \\ &= \phi([f]) + \phi([g])\end{aligned}$$

Así también, sea $c \in \mathbf{K}$ se tiene

$$\overline{cf}^{G} = c\overline{f}^{G} = \sum_{\alpha} cc_\alpha x^\alpha$$

Por lo tanto

$$\begin{aligned}\phi(c[f]) &= \phi([cf]) \\ &= \overline{cf}^{G} \\ &= c\,\overline{f}^{G} \\ &= c\,\phi([f])\end{aligned}$$

Así se tiene que ϕ es lineal y los espacios son isomorfos. □

Teorema D.0.6

Sea $V = V(I)$ una variedad afín en $\mathbf{C}^n$ y fijamos un orden monomial en $\mathbf{C}[x_1, \ldots, x_n]$. Entonces los enunciados siguientes son equivalentes

(i) V es un conjunto finito.

(ii) Para cada i, $1 \leq i \leq n$, existe $m_i \geq 0$ tal que

$$x_i^{m_i} \in \langle Tp(I) \rangle$$

(iii) Sea G una base de Gröbner para I. Entonces para cada i, $1 \leq i \leq n$, existe $m_i \geq 0$ tal que

$$x_i^{m_i} = Mp(g) \text{ para algún } g \in G$$

(iv) El $\mathbf{C}$-espacio vectorial $S = span(x^\alpha : x^\alpha \notin \langle Tp(I) \rangle)$ es de dimensión finita.

(v) El $\mathbf{C}$-espacio vectorial $\mathbf{C}[x_1, \ldots, x_n]/I$ es de dimensión finita.

Demostración

(i)$\Longrightarrow$ (ii) Si $V = \emptyset$ entonces por Nullstellensatz

$$I = \mathbf{C}[x_1, \ldots, x_n]$$

Luego $1 \in I$, entonces para cada i, $1 \leq i \leq n$, basta tomar $m_i = 0$

$$x_i^{m_i} = 1 \in \langle Tp(I) \rangle$$

Si $V \neq \emptyset$, entonces para i fijo. Sea a_j, $j = 1, \ldots, k$ los números complejos distintos que aparecen en la i-ésma coordenada de los puntos en V.

Formamos

$$f(x_i) = \prod_{j=1}^{k} (x_i - a_j)$$

Por la construcción, f es anulado por cada punto de $V = V(I)$, luego $f \in I(V(I))$, por Nullstellensatz, existe $m \geq 1$ tal que $f^m \in I$. Ello nos indica que el monomio principal de f^m están en $\langle Tp(I) \rangle$.

Examinando nuestra expresión f, se observa que

$$x_i^{km} \in \langle Tp(I) \rangle$$

(ii)$\Longleftrightarrow$ (iii) Veamos.

($\Longrightarrow$) Sea $x_i^{m_i} \in \langle Tp(I) \rangle$. Desde que G es una base de Gröbner para I,

$$\langle Tp(I) \rangle = \langle Tp(g) : g \in G \rangle$$

$$\text{existe algún } g \in G \text{ tal que } Tp(g) | x_i^{m_i}$$

esto implica que $Tp(g)$ es una potencia de x_i.

($\Longleftarrow$) Es directo de la definición.

(ii)$\Longrightarrow$ (iv) Si $x_i^{m_i} \in \langle Tp(I)\rangle$ para cada i, entonces los monomios

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n}$$

para el cual $\alpha_i \geq m_i$ todos están en $\langle Tp(I)\rangle$.

Los monomios en el complemento de $\langle Tp(I)\rangle$ son para $\alpha_i \leq m_i - 1$ para cada i. Por lo tanto el número de monomios en el complemento de $\langle Tp(I)\rangle$ es a los más

$$m_1 \cdot m_2 \cdot \ldots \cdot m_n$$

(iv)$\Longleftrightarrow$ (v) Está dada de la proposición (D.0.8).

(v)$\Longrightarrow$ (i) Para mostrar que V es finito, es suficiente mostrar que para cada i, $1 \leq i \leq n$, existen un número finito de valores distintos para la i-ésima coordenada de puntos en $V = V(I)$.

Fijando i, y considerando las clases

$$[x_i^j] \text{ en } \mathbf{C}[x_1, \ldots, x_n]/I \quad \text{donde } j = 0, 1, 2, \ldots$$

Desde que $\mathbf{C}[x_1, \ldots, x_n]/I$ es finitamente dimensional, el $[x_i^j]$, $j = 0, 1, 2, \ldots$ son linealmente dependientes módulo I. Luego existen constantes c_j no todas ceros y m tal que

$$\sum_{j=0}^{m} c_j [x_i^j] = \left[\sum_{j=0}^{m} c_j x_i^j\right] = [0]$$

Esto implica que

$$\sum_{j=0}^{m} c_j x_i^j \in I$$

Desde que cualquier polinomio no nulo posee un número finito de raíces en $\mathbf{C}$. Esto nos indica que los puntos de V tiene unicamente un número finito, diferentes en la i-ésima coordenada. $\square$

Un ideal $I \neq \mathbf{K}[x_1, x_2, \ldots, x_n]$ que satisface cualquiera de las condiciones del teorema (D.0.6) es llamado cero dimensional, está terminología es adoptada a causa de que $V(I)$ consiste de un número finito de puntos.

Bibliografía

[1] Bourbaki Nicolas, *ELEMENTS OF MATHEMATICS ALGEBRA I* Edit.Publishers in arts and science. Paris France.Año 1974. 188p.

[2] Cox David, Little John, O'Shea Donal. *IDEALS, VARIETIES, AND ALGORITHMS* Edit. Springer- Velag New York, Inc. Segunda Edición.EE.UU. 1997. 536 p.

[3] I. N. Herstein. *ALGEBRA ABSTRACTA* Edit. Grupo Editorial Iberoamérica, S.A de C.V. Año 1986. 248 p.

[4] Kreuzer Martin and Lorenzo Robbiano. *COMPUTATIONAL COMMUTATIVE ALGEBRA I* Edit. Springer- Verlog New York. Año 2000. 321 p.

[5] Landin Joseph. *AN INTRODUCTION TO ALGEBRAIC STRUCTURES* Edit. Board. EE.UU. Año 1980. 247 p.

[6] M. F. Atiyah, I. G. Macdonald. *INTRODUCCION AL ALGEBRA CONMUTATIVA* Edit. Reverté, S.A. Barcelona España. Año 1989. 147 p.

[7] Monteiro L.H. Jacy. *ELEMENTOS DE ÁLGEBRA* Edit. Sedegra. Sna Paulo Brail. Premera edicion. 552 p.

[8] Polo Grillo Incola.*ALGORITHMS COMPUTING POLYNOMIAL AND A LAURENDT POLYNOMIAL SETTING* Tesi di Laureal. Universita'Di Padova, Facolta' Di Ingegneria.Italia. año 2000. 122 p.

[9] W. Adams William, Loustaunau Philippe. *AN INTRODUCTION TO GROBNER BASES* Volimen 3. Edit. Board.EE.UU. 1996. 289 p.

[10] Wolmer V. Vasconcelos. *COMPUTATIONAL METHODS IN COMMUTATIVE ALGEBRA AND ALGEBRAIC GEOMETRY* Edit. Springer - Varlag Berlin Heidelberg. Volumen 3. Año 1998. 394 p.