UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN-MANAGUA

RECINTO UNIVERSITARIO "RUBÉN DARÍO"

FACULTAD DE CIENCIAS E INGENIERÍA

DEPARTAMENTO DE MATEMÁTICA Y ESTADÍSTICA

Seminario de Graduación para Optar a la Licenciatura en Matemática

Resolución de Sistemas de Ecuaciones Polinomiales Aplicando Bases de Gröbner y Teoría de Eliminación

Autores: **Br. Lilliam Damaris López Iyescas**

Br. Carlos Mauricio Ruíz Dávila

Br. Ángel Efraín Miranda Mendoza

Tutor: **MSc. José Jesús Mendoza Casanova**

Diciembre 2015

ÍNDICE

1 Título del tema y subtema

Tema: Sistemas de Ecuaciones Polinomiales.

Subtema: Resolución de Sistemas de Ecuaciones Polinomiales Aplicando Bases de Gröbner y Teoría de Eliminación.

2 Dedicatoria

A Dios, a mis padres, Lilliam y Mariano
A mis hermanos, mis sobrinos
Por su apoyo incondicional.
Lilliam López Iyescas

A Dios, a mis padres, Cándida y Félix
Mis sobrinos, Yahoska, Mercedes y Gilberth
Por su apoyo incondicional
Carlos Ruíz Dávila

A Dios, a mis padres, Hernán y Emérita,
A mi esposa Abigail y a mi Hijo Efraín
Gracias a su apoyo incondicional
Que me han brindado en el
Transcurso de mi vida.
Ángel Miranda Mendoza

Quien en vida fuera nuestro
Compañero y Amigo
Juan José Blanco Cea

3 Agradecimientos

Primeramente nuestro agradecimiento se dirige a quien ha forjado nuestros caminos y nos ha dirigido por el sendero correcto. Al creador de todas las cosas, al que nos ha dado fortaleza para continuar día a día, por eso y porque eres quien guía el destino de nuestras vidas te agradecemos padre celestial.

Agradecemos también a nuestro tutor José Jesús Casanova Mendoza por habernos brindado la oportunidad de recurrir a su capacidad y conocimiento. Así como también habernos tenido toda la paciencia del mundo para guiarnos durante todo el desarrollo de nuestro trabajo.

Así mismo expresamos nuestra gratitud a todos los que fueron nuestros maestros y compañeros ya que gracias a sus consejos y compañerismos contribuyeron a que cada uno de nosotros siguiéramos hacia adelante para cumplir nuestras metas.

4 Valoración del Docente

La presente memoria escrita, titulada "Resolución de Sistemas de Ecuaciones Polinomiales Aplicando Bases de Gröbner y Teoría de Eliminación", cumple con el rigor científico y metodológico para optar al título de Licenciado en Matemática.

Esta investigación fue elaborada por los bachilleres Lilliam Damaris López Iyescas, Carlos Mauricio Ruíz Dávila y Ángel Efraín Miranda Mendoza. Y cumple con la estructura reglamentada para presentar el informe final escrito del Seminario de Graduación.

Respecto a la profundidad del tema, su aplicabilidad y por ende el arribo a las conclusiones, vale la pena mencionar que el contenido aquí abordado es de vital importancia para los estudiantes de la Carrera de Matemática y de las diferentes Ingenierías, debido su valor teórico y práctico que permite asombrosas aplicaciones.

Omito hacer comentario alguno respecto a las Bases de Gröbner y la Teoría de Eliminación porque esa es tarea de los autores de esta investigación. No obstante, advierto al lector que está apunto de sumergirse en una de las más bellas teorías que vincula el Álgebra y la Geometría, y que corre el riesgo de engolosinarse como ha ocurrido, afortunadamente, con este grupo de trabajo.

Solamente resta dar mi aval como tutor. Entonces confirmo que López, Ruíz y Miranda tienen un excelente dominio de la teoría expuesta en su informe y están preparados para la defensa pública de su investigación ante el excelentísimo tribunal examinador. Y los invito a seguir su formación profesional porque considero que tienen más que lo necesario para ello.

Managua, Noviembre del 2015

MSc. José Jesús Mendoza Casanova
Tutor
Docente del Departamento de Matemática y Estadística
Facultad de ciencias e Ingeniería
UNAN-MANAGUA

5 Resumen

El objetivo del presente trabajo se inscribe dentro del estudio de las bases de Gröbner para la resolución de sistemas de ecuaciones polinomiales por medio de teoría de eliminación, debemos enfatizar que las bases de Gröbner, son una herramienta fundamental y básicas en muchos aspectos de la geometría algebraica de las cuales fueron introducidas por Bruno Buchberger en su tesis doctoral en 1965 hecha bajo la dirección de Wolfgang Gröbner. Recurriendo a los conceptos de álgebra abstracta tales como Grupo, Grupo abeliano, Campo, Espacios Vectoriales, Módulo, etc. Así como también la introducción de Órdenes Monomiales tales como orden lexicográfico, orden lexicográfico graduado, etc. Ideales, Algoritmo de la división, Algoritmo de Buchberger y Teorema de la Base Hilbert.

Durante el desarrollo de este trabajo se utilizará el software **CoCoA versión 4.7.5** (Computations in Conmutative Álgebra), ya que este nos permitirá solucionar de manera más rápida los cálculos, para la implementación de algoritmos en sistemas de ecuaciones polinomiales. Debemos argumentar que los sistemas polinomiales son una pieza importante dentro de la modelación de problemas reales del estudio y cálculo de sus soluciones exactas constituyendo todo un campo de trabajo con aplicaciones directas en ingeniería, robótica, informática, economía, telemática, etc.

6 Introducción del Tema y Subtema

En sus orígenes, el álgebra clásica era el arte de resolver ecuaciones (la palabra álgebra proviene de un vocablo árabe que significa reducción). El álgebra moderna está caracterizada por el estudio de ciertas estructuras abstractas que tienen en común una gran variedad de objetos matemáticos. En los últimos años nuestra habilidad para manipular sistemas de ecuaciones expresadas mediante polinomios ha experimentado algunas transformaciones cruciales. Comenzando con el descubrimiento de las bases de Gröbner por Bruno Buchberger a finales de los años 60 y apoyado por el espectacular crecimiento de las capacidades de los ordenadores modernos, muchas herramientas de la geometría algebraica clásica han ganado una gran importancia y, a su vez, la han hecho más accesible y aplicable. Recientemente, las bases de Gröbner han sido aplicadas en multitud de problemas por su capacidad de resolver sistemas de ecuaciones polinomiales y como modelo algebraico de computación. Este transcurrir de ambas disciplinas ha proporcionado diversas y fructíferas colaboraciones entre ellas hasta la actualidad, donde las interacciones mutuas son múltiples.

En efecto, el estudio de los sistemas de ecuaciones lineales pasó, hace mucho tiempo, de ser una mera manipulación de fórmulas a convertirse en el estudio de una serie de estructuras algebraicas abstractas. Desde un punto de vista clásico, la geometría algebraica es el estudio de los espacios de soluciones de sistemas de ecuaciones polinomiales en varias variables.

La resolución de sistemas de estos tipos no es un tema trivial. Incluso en algunos casos no podemos llegar a saber las soluciones exactas debido a la gran complejidad que puede llegar a alcanzar dichos sistemas. En cualquier caso, son una herramienta imprescindible a la hora de abordar la resolución de problemas de la vida cotidiana dentro de diversos campos (ingeniería, biología, arquitectura, economía, telecomunicaciones, transportes, etc.).

Probablemente la primera pregunta que surge a partir del título de este trabajo es: ¿Qué es o de qué trata la solución de ecuaciones polinomiales basada en las bases de Gröbner y teoría de eliminación? El objetivo principal será presentar suficientes elementos para ir formando una posible respuesta.

En geometría algebraica computacional, y en álgebra conmutativa computacional el algoritmo de Buchberger constituye una pieza fundamental puesto que dicho algoritmo ha revolucionado los métodos algorítmicos así como las aplicaciones de la geometría algebraica, y es un área de investigación actual. Este algoritmo fue creado por el matemático austriaco Bruno Buchberger y presentado en su tesis doctoral.

7 Justificación

Lo que se pretende realizar en el presente trabajo es dar solución a sistemas de ecuaciones polinomiales, por medio de las bases de Gröbner utilizando Teoría de Eliminación. Ya que en los últimos años ha sido una transformación dramática en nuestra habilidad para manipular sistemas de ecuaciones polinomiales comenzando con el descubrimiento de las bases de Gröbner por Buchberger, a finales de los años 60 y apoyado por el espectacular crecimiento de las capacidades de los ordenadores modernos, muchas herramientas de la geometría clásica han ganado gran importancia siendo estás más accesible y aplicable en las bases de Gröbner.

Recientemente las bases de Gröbner han sido aplicadas en multitudes de problemas por su capacidad de resolver sistemas de ecuaciones polinomiales y como modelo algebraico de computación como (Maple, Mathematica, Reduce, Axiom, Macaulay y CoCoA).

8 Objetivos

8.1 Planteamiento del problema

¿Cómo obtener soluciones exactas en la resolución de Sistemas de Ecuaciones Polinomiales?

En 1964 se presentó un "método" para encontrar una base linealmente independiente para el espacio vectorial del anillo de clases residuales de un ideal polinomial generado por un conjunto de polinomios (multivariados), el cual fue planteado por Wolfgang Gröbner y pregunto "cuando, para un conjunto de polinomios dados este método puede finalizar garantizando que la base obtenida mediante este sea una linealmente independiente" y si este fuese posible como este método podía ser puesto en marcha en un cerebro electrónico.

8.2 Objetivo general

Resolver sistema de ecuaciones polinomiales utilizando Bases de Gröbner y Teoría de Eliminación.

8.3 Objetivos específicos

- Considerar las principales definiciones del álgebra abstracta sobre las cuales desarrollaremos nuestro trabajo.
- Describir la utilización del software CoCoA 4.7.5 para encontrar bases de Gröbner.
- Mostrar la resolución de sistemas de ecuaciones polinomiales por medio de la teoría de eliminación.
- Aplicar las bases de Gröbner y la teoría de eliminación en la solución de un problema de aplicación en el área de la Robótica y la Medicina.

9 Desarrollo del Subtema

9.1 Antecedentes

Desde que el hombre empezó a contar con sus dedos se enfrentó a un sin número de problemas que se presentan cada vez que su mundo se hace más y más complejo. Para darnos una idea de los orígenes del problema que aquí tratamos, será necesario echar un vistazo al pasado.

El período de 1700 A. C. a 1700 D. C., se caracterizó por la invención gradual de símbolos y la resolución de ecuaciones. Dentro de este período encontramos un álgebra desarrollada por los griegos (300 A. C.) llamada álgebra geométrica, rica en métodos geométricos para resolver ecuaciones algebraicas (y algunos sistemas). Thymaridas (400 A. C.). Había encontrado una fórmula para resolver un determinado sistema de n ecuaciones con n incógnitas.

El álgebra aparece acompañada de las primeras ecuaciones lineales de una indeterminada, las que luego pasaron a ser cuadráticas, cúbicas y de grado cuatro. Paralelo a esto surgía la necesidad de resolver sistemas de ecuaciones hasta de tres indeterminadas.

Finalmente, llegamos al planteamiento y solución de los Sistemas de Ecuaciones Polinomiales actuales. Como ocurre a menudo, hay muchas personas que presentaron algunos resultados para formular ciertos aspectos de esta teoría.

El mayor paso fue dado por Bruno Buchberger (matemático austríaco) a mediados de los sesenta. Él formuló el concepto de bases de Gröbner y, ampliando una sugerencia de su asesor Wolfgang Gröbner, encontró un algoritmo para el cálculo de estas. Su algoritmo ha sido estudiado, mejorado y generalizado en los últimos 40 años, y lo más importante, se han encontrado multitud de aplicaciones a las ramas más diversas, incluidas criptografía, física, ingeniería y robótica entre otras. La naturaleza constructiva y computacional de esos métodos, en la era de la informática, lo hace líder de las aplicaciones en muchos campos.

Su algoritmo ha sido puesto en marcha y forma parte de todos los sistemas o paquetes de cálculo simbólico actuales tales como Mathematica, Magma, Maple, Derive y Reduce, CoCoA.

9.2 Marco Teórico

9.2.1 Conceptos Preliminares de Estructuras Algebraicas

En este capítulo introduciremos algunos de los tópicos básicos de la teoría que estudiáremos, podemos definir lo que es un polinomio ya que el lector está familiarizado en una y dos variable, pero aquí necesitaremos discutir sobre los polinomios en n variables (o indeterminadas) $x_1, x_2, \dots, x_n$ con coeficientes en un campo arbitrario K.

Definición 1. Un **Grupo** $(G,\cdot)$ es un conjunto G provisto de una operación $\cdot : G \times G \to G$ que satisface las siguientes condiciones:

- **Asociatividad:** para todo $g_1, g_2, g_3 \in G$, es
$$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3).$$
- **Elemento neutro:** existe un único $e \in G$ tal que para todo $g \in G$ es
$$e \cdot g = g = g \cdot e$$
- **Inverso:** para todo $g \in G, \exists!\ g' \in G$ tal que
$$g \cdot g' = e = g' \cdot g$$
Si además para todo $par\ g, h \in G\ es\ g \cdot h = h \cdot g$ entonces el grupo se llama *abeliano o conmutativo.*

Definición 2. Un subconjunto no vacío H de un grupo G se llama **subgrupo** de G, si H mismo forma un grupo relativo al producto de G.

Definición 3. Un **anillo** $(A, +, \cdot)$ es un conjunto no vacío en donde están definidas un par de operaciones llamadas suma y producto, las cuales denotamos por $+$ y $\cdot$ respectivamente.

Estas operaciones satisfacen cada una de las propiedades siguientes:

- **Cerradura respecto a la suma:** Para todo $a, b \in A$, se tiene que $a + b$ están en A.
- **Asociatividad respecto a la suma:** Para todo $a, b, c \in A$ se tiene que

$$a + (b + c) = (a + b) + c$$

- **Existencia del idéntico aditivo:** Existe un elemento neutro 0 en A, el cual llamaremos cero, tal que

$$a + 0 = a = 0 + a \text{ para todo } a \text{ en } A.$$

- **Existencia del inverso aditivo:** Para todo a en A, existe otro elemento en A, denotado por $-a$, el cual llamamos el Opuesto de a y que verifica

$$a + (-a) = 0 = -a + a$$

- **Conmutatividad respecto a la suma:** Para todo a, b en A se tiene

$$a + b = b + a$$

- **Cerradura respecto al producto:** Para todo $a, b \in A$, se tiene que $a \cdot b$ están en A.

- **Asociatividad respecto al producto:** Para todo $a, b\ y\ c$ en A se satisface

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- **Existencia del idéntico multiplicativo:** Para todo a, existe un (único) elemento, e, en A que es neutro de la operación $\cdot$, es decir

$$\exists\ e \in A, \forall\ a \in A: e \cdot a = a = a \cdot e$$

- **Leyes distributivas del producto respecto a la suma:** Para todo $a, b\ y\ c$ en A se satisface

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Definición 4. Un **Monoide** $(M,\cdot)$ es una estructura algebraica en la que M, es un conjunto y $\cdot$ es una operación binaria interna en M, que cumple las siguientes propiedades.

1) **Operación interna:** para cualesquiera dos elementos del conjunto M operados bajo $\cdot$, el resultado siempre pertenece al mismo semigrupo M. Es decir:
$$\forall x, y \in M: x \cdot y \in M$$
2) **Asociatividad:** para cualesquiera elementos del conjunto M no importa el orden en que se operen las parejas de elementos, mientras no se cambie el orden de los elementos (ver grupo abeliano), siempre dará el mismo resultado. Es decir:
$$\forall x, y, z \in M: x \cdot (y \cdot z) = (x \cdot y) \cdot z \in M$$
3) **Elemento neutro:** existe un (único) elemento, e, en M que es neutro de la operación $\cdot$, es decir:
$$\exists!\, e \in M, \forall x \in M: e \cdot x = x = x \cdot e$$

Un Monoide es **conmutativo** o **abeliano** si satisface la propiedad conmutativa.

Definición 5. Sea K un conjunto no vacío, y sean $+$ y $\cdot$ dos operadores internas sobre K el sistema $(K,+,\cdot)$ es un **campo** si cumple:

- **Asociatividad respecto a la suma:** Para todo $a, b, c \in K$ se tiene que
$$a + (b + c) = (a + b) + c$$
- **Conmutatividad respecto a la suma:** Para todo a, b en K se tiene
$$a + b = b + a$$
- **Existencia del idéntico aditivo:** Existe un elemento neutro 0 en K, el cual llamaremos cero, tal que
$$a + 0 = a = 0 + a \text{ para todo } a \text{ en } K.$$
- **Existencia del inverso aditivo:** Para todo a en K, existe otro elemento en K, denotado por $-a$, el cual llamamos el Opuesto de a y que verifica
$$a + (-a) = 0 = -a + a$$

- **Conmutatividad respecto a la suma:** Para todo a, b en K se tiene

$$a + b = b + a$$

- **Asociatividad respecto al producto:** Para todo $a, b\ y\ c$ en K se satisface

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- **Conmutatividad respecto al producto :** Para todo a, b en K se tiene

$$a \cdot b = b \cdot a$$

- **Existencia del idéntico multiplicativo:** Existe un (único) elemento $e \in K$, tal que para todo a es neutro de la operación $\cdot$, es decir

$$\exists\, e \in K, \forall\, a \in K : e \cdot a = a = a \cdot e$$

- **Existencia de elementos inversos multiplicativo:** Para todo $a \in K, \exists\, a' \in K$, es decir:

$$a' \cdot a = e$$

Definición 6. Un A **−Módulo** a izquierda es un grupo abeliano $(M, +)$ provisto de un morfismo de anillos

$$\rho : A \to End_{\mathbb{Z}}(M)$$
$$a \longmapsto \rho_a$$

En otras palabras, dar una estructura de $A - módulo$ a un grupo abeliano M es asignar a cada elemento $a \in A$ una endomorfismo del grupo M. La condición de que esta asignación sea un morfismo de anillos dice que:

- $\rho_1 = Id_M$.
- $\rho_{ab} = \rho_a \cdot \rho_b$.
- $\rho_{a+b} = \rho_a + \rho_b$.

Definición 7. (Espacio Vectorial) Sean dos conjuntos, no vacíos V y K, donde K es un campo. En V se definen las operaciones:

1. Suma de vectores $u + v$.
2. Multiplicación por un escalar αu.

El conjunto V es un espacio vectorial sobre el campo K, si para todo vector $u, v, w \in V$ y para todo escalar $\alpha, \beta \in K$ se cumple que:

1. $u + v \in V$
2. $(u + v) + w = u + (v + w)$
3. $u + v = v + u$
4. $u + e = u$, donde e es el elemento neutro para la suma.
5. $u + (-u) = e$, donde $-u$ es el elemento inverso de u para la suma
6. $\alpha u \in V$
7. $(\alpha\beta)u = \alpha(\beta u)$
8. $(\alpha + \beta)u = \alpha u + \beta u$
9. $\alpha(u + v) = \alpha u + \alpha v$
10. $(1)u = u$, donde 1 es la unidad del cuerpo.

Teorema 8. (Teorema fundamental del álgebra)

Todo polinomio en una variable de grado $n \geq 1$ con coeficientes reales o complejos tiene almenos n raíces (real o compleja).

Sea $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n , n \geq 1$, con coeficientes complejos cualesquiera. Podemos ver que al descomponer $f(x)$ en la forma

$$f(x) = (x - \alpha_1)\varphi(x)$$

Los coeficientes de $\varphi(x)$ son nuevamente reales o complejos y entonces, $\varphi(x)$tiene una raíz, en virtud del teorema anterior, de donde

$$f(x) = (x - \alpha_1)(x - \alpha_2)\phi(x)$$

Si continuamos de este modo obtendremos la descomposición (única, salvo el orden de los factores) del polinomio $f(x)$ de $n-$ ésimo grado en un producto de n factores lineales,

$$f(x) = a_0(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_l)^{k_1},$$

Donde

$$k_1 + k_2 + \cdots + k_l = n\ ,\ y\ \ \alpha_1 \neq \alpha_2 \neq \cdots \neq \alpha_l.$$

9.2.2 Polinomios en varias indeterminadas (el anillo $K[x_1,\ldots,x_n]$)

Definición 9. Un **monomio** en $x_1, x_2, \ldots, x_n$ es un producto de la forma

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

Donde todos los exponentes $\alpha_1, \alpha_2, \ldots, \alpha_n$ son enteros no negativos. El grado total de este monomio es la suma $\alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Notación: Escribimos x^α por $x_1{}^{\alpha_1}.x_2{}^{\alpha_2}, \ldots, x_n{}^{\alpha_n}$ donde $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ es una $n-upla$ de entero no negativos. Si $\alpha = (0,0,\ldots,0)$, $x^\alpha = 1$. Además,

$|\alpha| = \sum_{i=1}^{n} \alpha_i$, denota el grado total del monomio x^α.

Ejemplos de monomios

$3x^7y^4z$	$\frac{5}{2}x^3y$	$\frac{8}{3}y^5z^2$

Ejemplos de no monomios

$\frac{x^5}{z^4}$	$y^{\frac{-3}{2}}z^{\frac{5}{2}}$	$\frac{5}{3}x^{-7}\,y^{\frac{2}{7}}z^{\frac{3}{2}}$

Definición 10. Sea K un campo. Un **polinomio** f en $x_1, x_2, \dots, x_n$ con coeficientes en K es una combinación lineal finita (con coeficientes en K) de monomios. Escribiremos un polinomio f en la forma

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

Donde la suma se realiza sobre un número finito de $n - uplas\ \alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$. El conjunto de todos los polinomios en $x_1, x_2, \dots, x_n$ con coeficientes en K se denotara por $K[x_1, x_2, \dots, x_n]$.

Cuando tratemos con polinomios en un número pequeño de variables, usualmente prescindiremos de los subíndices. De esta manera, polinomios en una, dos y tres variables pertenecerán a $K[x]$, $K[x, y]$ y $K[x, y, z]$, respectivamente.

Por ejemplo,

$$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$$

Es un polinomio en $\mathbb{Q}[x, y, z]$. Comúnmente usaremos las letras f, g, h, p, q, r para referirnos a polinomios. Usaremos la siguiente terminología para tratar con ellos.

Definición 11. (Términos y coeficientes)

Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio en $K[x_1, x_2, \dots, x_n]$.

i) Llamaremos al a^α el coeficiente del monomio x^α.

ii) Si $a_\alpha \neq 0$, $a_\alpha x^\alpha$ es un término de f.

iii) El grado total de f denotado $grad(f)$ es el máximo $|\alpha|$ entre todos los monomios cuyos coeficientes a_α son distintos de cero.

Por ejemplo, el polinomio dado anteriormente.

$$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$$

Consta de 4 términos y grado 6. Observe que hay 2 términos de grado total máximo, algo que no puede suceder para los polinomios en una variable.

La suma y el producto de dos polinomios es de nuevo otro polinomio. Diremos que un polinomio f divide al polinomio g si $g = fh$ para algún $h \in K[x_1, x_2, \dots, x_n]$. Podemos observar que bajo la adición y la multiplicación definidas de la manera usual

$$\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha = \sum_\alpha (a_\alpha + b_\alpha)\, x^\alpha \qquad \text{Y}$$

$$\sum_\alpha a_\alpha x^\alpha \cdot \sum_\beta b_\beta x^\beta = \sum_\gamma \left(\sum_{\alpha+\beta=\gamma} a_\alpha \cdot b_\beta \right) x^\gamma$$

$K[x_1, x_2, \dots, x_n]$ Satisface todas las propiedades de campo excepto por la existencia de inverso multiplicativo (porque por ejemplo $\frac{1}{x_1}$, no es un polinomio). Tal estructura matemática es conocida como anillo conmutativo, y por esa razón nos referimos a $K[x_1, x_2, \dots, x_n]$ como un anillo polinomial.

Corolario 12.

Si K es campo, entonces todo ideal de $K[x]$ se puede escribir de la forma $\langle f \rangle$ para algún $f \in K[x]$. Además, f es único salvo por un factor no nulo en K.

Observación 13.

Otros resultados interesantes son: Si $d(x)$ es el máximo común divisor de los polinomios $f(x)$ y $g(x)$, existen polinomios $u(x)$ y $v(x)$ tales que $f(x) \cdot u(x) + g(x) \cdot v(x) = d(x)$, además si los grados de $f(x)$ y $g(x)$ son mayores que cero, entonces el grado de $u(x)$ es menor que el grado de $g(x)$, y el grado de $v(x)$ es menor que el grado de $f(x)$.

Aplicando este resultado a polinomios primos, obtenemos el siguiente resultado:

Los polinomios $f(x)$ y $g(x)$ son primos entre sí, si y sólo si, existen polinomios $u(x)$ y $v(x)$ que satisfacen la igualdad $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$.

¿Existe un algoritmo para decidir si un polinomio dado $f \in K[x]$ pertenece al ideal $\langle f_1, \dots, f_s \rangle$? La repuesta es si, y el algoritmo es fácil de describir. El primer paso es usar los mcd para encontrar un generador h de $\langle f_1, \dots, f_s \rangle$. Entonces, puesto que $f \in \langle f_1, \dots, f_s \rangle$ es equivalente a $f \in \langle h \rangle$, solo necesitamos usar el algoritmo de la división para escribir $f = qh + r$, donde $grad(r) < grad(h)$, se deduce que f pertenece al ideal si y sólo si $r = 0$.

Definición 14. (Máximo Común Divisor Generalizado)

Un máximo común divisor de los polinomios $f_1, \dots, f_s \in K[x]$ es el polinomio h tal que

(i) $h \mid f_1, \dots, h \mid f_s$.

(ii) Si p es otro polinomio que divide a $f_1, \dots, f_s$ entonces $p \mid h$.

Si h cumple estas propiedades escribimos $h = mcd(f_1, \dots, f_s)$.

Proposición 15.

Sean $f_1, \dots, f_s \in K[x]$, donde $s \geq 2$. Entonces:

i. $mcd\ (f_1, \dots, f_s)$ existe y es único salvo por la multiplicación de una constante no nula en K.
ii. $mcd\ (f_1, \dots, f_s)$ es un generador del ideal $\langle f_1, \dots, f_s \rangle$.
iii. Existe un algoritmo para calcular el $mcd\ (f_1, \dots, f_s)$.

Demostración:

Las pruebas de las partes (i) y (ii) son similares a las principales propiedades de los mcd y serán omitidas: para probar (iii), sea $h = mcd(f_2, \dots, f_s)$. Probaremos que:

$$\langle f_1, h \rangle = \langle f_1, f_2, \dots, f_s \rangle.$$

Probemos que $\langle f_1, f_2, \dots, f_s \rangle \subset \langle f_1, h \rangle$. Sea

$$f_1 = f_1 + 0h,$$

$$\vdots$$

$$f_i = m_i h_i \ 2 \leq i \leq s,$$

Entonces $f_1, \dots, f_s \in \langle f_1, h \rangle$. Por tanto, $\langle f_1, f_2, \dots, f_s \rangle \subset \langle f_1, h \rangle$. Sigamos con la otra inclusión $\langle f_1, h \rangle \subset \langle f_1, f_2, \dots, f_s \rangle$. Recordemos que $f_1 \in \langle f_1, f_2, \dots, f_s \rangle$ y que h puede ser expresado de la siguiente forma por (ii)

$$h = m_2 f_2 + \cdots + m_s f_s,$$

$$h = 0 f_1 + m_2 f_2 + \cdots + m_s f_s,$$

entonces, $f_1, h \in \langle f_1, f_2, \dots, f_s \rangle$. De esto se deduce que $\langle f_1, h \rangle \subset \langle f_1, f_2, \dots, f_s \rangle$. Por tanto, $\langle f_1, h \rangle = \langle f_1, f_2, \dots, f_s \rangle$.

Por la parte (ii) de esta proposición vemos que

$$\langle mcd(f_1, h) \rangle = \langle mcd(f_1, \dots, f_s) \rangle.$$

Entonces $mcd(f_1, h) = mcd(f_1, \dots, f_s)$ resulta de la parte de la unicidad del Colorario (12), lo que prueba lo deseado.

Finalmente, necesitamos demostrar que existe un algoritmo para calcular $mcd(f_1, \dots, f_s)$. La idea básica es combinar la parte (iii) con el algoritmo de Euclides. Por ejemplo, supongamos que queremos calcular $mcd(f_1, f_2, f_3, f_4)$ usando dos veces (iii) obtenemos

$$mcd(f_1, f_2, f_3, f_4)$$

$$mcd(f_1, mcd(f_2, f_3, f_4)),$$

$$mcd(f_1, mcd(f_2, mcd(f_3, f_4))).$$

Si usamos tres veces el algoritmo de Euclides (una vez por cada mcd en la segunda línea de (6)). Obtenemos el $mcd\ de\ f_1, f_2, f_3, f_4$. La proposición ha sido probada. ■

Ejemplo 16.

Calcular el $m.c.d$ de los polinomios $f, g, h, i \in K[x]$.

Sean:

$$f = x^6 - 1 \quad ; \quad g = x^4 - 1 \quad ; \quad h = x^3 - 3x + 2 \quad ; \quad i = x^2 - 1$$

El comando del máximo común divisor en la mayoría de los sistemas del álgebra computacional solo maneja dos polinomios a la vez. Por lo tanto, para trabajar más de dos polinomios, tendrá que utilizar el método descrito en la demostración de la proposición anterior.

Consideremos el ideal:

$$I = \langle x^6 - 1\,, x^4 - 1\, x^6, x^3 - 3x + 2\,, x^2 - 1 \rangle \in K[x]$$

Sabemos que $m.c.d\ (x^6 - 1\,, x^4 - 1\,, x^3 - 3x + 2, x^2 - 1\,)$ es un generador. Además, se puede verificar que:

$$m.c.d\ (x^6 - 1\,, x^4 - 1\,, x^3 - 3x + 2, x^2 - 1\ )$$

$$m.c.d\ (m.c.d\ \ (x^6-1\ ,x^4-1)\ ,m.c.d\ \ (x^3-3x+2,x^2-1\ ))$$

lo cual resultan únicamente dos polinomios.

$$m.c.d\ (x^2-1\ \ \ ,x-1)$$

Ahora encontrando el $m.c.d$. Para estos nuevos polinomios por medio del algoritmo de la división tenemos:

$$\begin{array}{r|l} & a=x+1 \\ \hline x-1 & x^2-1 \\ & \underline{-x^2+x\ \ \ \ \ } \\ & \ \ \ \ \ x-1 \\ & \underline{\ \ -x+1\ \ \ } \\ & \ \ \ \ \ 0 \end{array}$$

$$m.c.d\ (x-1)$$

Por tanto por medio del algoritmo de Euclides el $m.c.d$ de I es $\boldsymbol{x-1}$.

9.2.3 Ideales Polinomiales

Definición 17. Un ideal $I \subset K[x_1, \dots, x_n]$ es un **ideal monomial** si existe un subconjunto $A \subseteq \mathbb{Z}_{>0}^n$ (posiblemente infinito) tal que I está formado por todos los polinomios que son sumas finitas de la forma:

$$\sum_{\alpha \in A} h_\alpha x^\alpha$$

Donde $h_\alpha \in K[x_1, \dots, x_n]$. En este caso, escribimos $I = \langle x^\alpha : \alpha \in A \rangle$.

Lema 18. Sea $I = \langle x^\alpha : \alpha \in A \rangle$ un ideal monomial. Entonces un monomio $x^\beta \in I$ si y sólo si x^β es divisible por x^α, para algún $\alpha \in A$.

Demostración:

Si x^β es múltiplo de x^α para algún $\alpha \in A$, entonces $x^\beta \in I$ por definición de ideal. Recíprocamente, si $x^\beta \in I$, entonces $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, donde $h_i \in K[x_1, \dots, x_n]$ y $\alpha(i) \in A$. Si desarrollamos cada h_i como una combinación lineal de monomios, vemos que todo término del miembro derecho de la ecuación es divisible por algún $x^{\alpha(i)}$. Por tanto, el miembro izquierdo x^β debe tener la misma propiedad. ■

Lema 19. Sea I un ideal monomial, y sea $f \in K[x_1, \dots, x_n]$. Las siguientes afirmaciones son equivalentes:

i) $f \in I$

ii) todo término de f está en I.

iii) f es una $K - combinación$ lineal de los monomios en I.

Demostración:

(i) ⇒ (ii). Sea $I = \langle x^{\alpha} : \alpha \in A \rangle \subset K[x_1, \dots, x_n]$ y $f \in I$, entonces

$$f = \sum_{i=1}^{s} h_i x^{\alpha(i)}, \alpha(i) \in A \; y \; h_i \in K[x_1, \dots, x_n].$$

al desarrollar el producto $h_i x^{\alpha(i)}$ nos quedaran términos de la forma $a_j x^{\beta} x^{\alpha(i)}$, donde $x^{\beta} x^{\alpha(i)} \in I$ lo que significa que cada $a_j x^{\beta} x^{\alpha(i)} \in I$.

(ii)⇐ (iii). Para facilitar la demostración veamos que si un término pertenece a I el monomio respectivo pertenece a I.

$$a_{\alpha} x^{\alpha} \in I \Rightarrow \left(\frac{1}{a_{\alpha}}\right)(a_{\alpha} x^{\alpha}) \in I \Rightarrow x^{\alpha} \in I$$

Esto lo podemos hacer porque los coeficientes los tomamos del campo $K \subset K[x_1, \dots, x_n]$. Entonces podemos trabajar con monomios en I y luego pasarnos a términos multiplicando por una constante adecuada al monomio respectivo.

Sea $f = \sum_{j=1}^{s} a_{\beta(j)} x^{\beta(j)} \in K[x_1, \dots, x_n]$, donde cada $a_{\beta(j)} x^{\beta(j)} \in I$. Entonces $x^{\beta(j)} \in I$. Por tanto. f es una $K-combinación$ de monomios en I (recuerde que esto significa que f es una sumatoria de elementos del campo por monomios).

(iii)⇒(i). Si f es una $K-combinación$ lineal de los monomios en I, f es de la forma:

$$f = \sum_{i=1}^{s} a_{\alpha(i)} x^{\alpha(i)}$$

Donde $a_{\alpha(i)} \in k \; y \; x^{\alpha(i)} \in I$, entonces cada $a_{\alpha(i)} x^{\alpha(i)} \in I$, y como f es una sumatoria de elementos de $I, f \in I$. ■

Colorario 20. Dos ideales monomiales son iguales, si y sólo si contienen los mismos monomios.

Definición 21. Un subconjunto $I \subset K[x_1, \dots, x_n]$ 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 $h \in K[x_1, \dots, x_n]$ entonces $hf \in I$.

Definición 22. Sea $I \subset K[x_1, \dots, x_n]$ un subconjunto no vacío. I se llama un **ideal polinomial** si:

$a)$ $f + g \in I$ Siempre que $f \in I$ y $g \in I$

$b)$ $pf \in I$ Siempre que $f \in I$, y $p \in K[x_1, \dots, x_n]$ es un polinomio arbitrario.

Definición 23. (Suma y Producto de Ideales)

Si I y J son ideales, entonces los conjuntos

$$I + J = \{f + g : f \in I, g \in I\}$$

$$I\,J = \left\{ \sum_{k=1}^{n} f_k g_k : f_k \in I, g_k \in J \; con \; n \in N, 1 \leq k \leq n \right\}$$

son ideales.

Lema 24. Si $f_1, \dots, f_s, \in K[x_1, \dots, x_n]$ entonces

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

es un ideal de $K[x_1, \dots, x_n]$ llamado el **Ideal generado** por $f_1, \dots, f_s$.

Demostración:

En primer lugar, $0 \in \langle f_1, \dots, f_s \rangle$ porque $0 = \sum_{i=1}^{s} 0 : f_i$. Supongamos ahora que

$f = \sum_{i=1}^{s} p_i f_i \;\; y \;\; g = \sum_{i=1}^{s} q_i f_i \;\; y \; sea \; h \in K[x_1, \dots, x_n]$. Entonces.

$$f + g = \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i = \sum_{i=1}^{s} (p_i f_i + q_i f_i)$$

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i \in \langle f_1, \dots, f_s \rangle.$$

Porque es de la forma: $\sum_{i=1}^{s} h_i f_i$ donde $h_i = p_i + q_i \in K[x_1, \dots, x_n]$, y

$$hf = \sum_{i=1}^{s} (hp_i) f_i \in \langle f_1, \dots, f_s \rangle$$

porque es de la forma $\sum_{i=1}^{s} h_i f_i$ donde $h_i = hp_i \in K[x_1, \dots, x_n]$.

Esto prueba que $\langle f_1, \dots, f_s \rangle$ es un ideal. ■

Uno de los hechos generales más importante acerca de los ideales en $K[x_1, \dots, x_n]$ es el Teorema de las bases de Hilbert. En este contexto, una base es otra forma de nombrar al conjunto de generadores de un ideal cualquiera. Para polinomios en una variable, este teorema es una consecuencia del algoritmo de la división de polinomios univariados.

Aritmética de los Ideales:

I. $I + J = \{ f + g | \; f \in I, g \in J \}$

II. $I\,J = \{\sum_{i=1}^{n} f_i g_i | \; g_i \in I, g_i \in J, n \in \mathbb{N}\}$

III. $I : J = \{ f \in K[x_1, \dots, x_n] || \; fg \in I, \forall_g \in J \}$

IV. $I \cap J = \{f \in K[x_1, \dots, x_n] | | f \in I, f \in J\}$

V. $I^k = \{\sum f_1 f_2 \cdots f_k | \; f_1, \dots, f_k \in I\}$.

Definición 25. Un **ideal *I* es finitamente generado** si existen $f_1, \dots, f_s \in K[x_1, \dots, x_n]$ tales que

$$I = \langle f_1, \dots, f_s \rangle$$

en este caso décimos que $f_1, \dots, f_s$ forman una base de I.

9.2.4 Órdenes Monomiales y Algoritmo de la División en $K[x_1,\dots,x_n]$

En este capítulo abordaremos algunos de los órdenes monomiales orden $Lex, DegRevLex$, etc. Para estudiar este problema cuando hay más de una variable, formularemos un algoritmo para dividir polinomios en $K[x_1, \dots, x_n]$ que extienda el algoritmo para $K[x]$. En el caso general, la meta es dividir $f \in K[x_1, \dots, x_n]$ por $f_1, \dots, f_s \in K[x_1, \dots, x_n]$. Como veremos, esto significa expresar a f en la forma

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

Donde los "cocientes" $a_1, \dots, a_s$ y el residuo r están en $K[x_1, \dots, x_n]$. Cierto cuidado será necesario en decidir cómo caracterizar al residuo. Aquí es donde usaremos los órdenes monomiales introducidos anteriormente. Veremos entonces, como el algoritmo de la división se aplica al problema de la pertenencia a un ideal.

La idea básica del algoritmo es la misma que en el caso univariado: queremos cancelar al término principal de f (con respecto a un orden monomial fijado) multiplicando y restando cierto f_i por un monomio apropiado. Entonces este monomio se convierte en un término del correspondiente a_i. Antes que establezcamos el algoritmo en general, primero trabajemos con algunos ejemplos para ver lo que está involucrado.

Definición 26. Un **orden monomial** en $K[x_1, \dots, x_n]$ es una relación $>$ en $z_{\geq 0}^n$, o equivalente, una relación en el conjunto de monomios $x^\alpha, \alpha \in z_{\geq 0}^n$, que satisface:

(i) $>$ es un orden total (o lineal) en $z_{\geq 0}^n$.

(ii) si $\alpha > \beta$ y $\gamma \in z_{\geq 0}^n$, entonces $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ es un buen orden en $z_{\geq 0}^n$. Esto significa que todo subconjunto no vacío $z_{\geq 0}^n$ tiene un elemento mínimo bajo $>$.

Lema 27.

Una relación de orden $> en \mathbb{Z}_{>0}^n$ es un buen orden si y sólo si toda sucesión estrictamente decreciente en $\mathbb{Z}_{>0}^n$

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

es finita.

Demostración:

Probaremos esto con el contra recíproco: $>$ no es un buen orden si y sólo si existe una sucesión estrictamente decreciente infinita en $\mathbb{Z}_{>0}^n$.

$(\Rightarrow)$ Si $>$ no es un buen orden, entonces algún subconjunto no vacío $S \subset \mathbb{Z}_{>0}^n$ no tiene elemento mínimo. Escojamos $\alpha(1) \in S$. Como $\alpha(1)$ no es elemento mínimo, de modo que existe un $\alpha(2) \in S$ con $\alpha(1) > \alpha(2)$. Pero $\alpha(2)$ no es el elemento mínimo, de modo que existe un $\alpha(3) \in S$ son $\alpha(2) > \alpha(3)$. Continuando de esta manera, obtenemos una sucesión estrictamente decreciente

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

$(\Leftarrow)$ Dada una sucesión infinita estrictamente decreciente,

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

entonces $\{\alpha(1), \alpha(2), \alpha(3), \dots\}$ es un subconjunto no vacío de $\mathbb{Z}_{>0}^n$. Que no tiene elemento mínimo. Por tanto $>$ no es un buen orden. ■

Definición 28. (Orden lexicográfico) Sea $\alpha = (\alpha_1, \dots, \alpha_n)$ y $\beta = (\beta_1, \dots, \beta_n) \in z_{\geq 0}^n$. Decimos que $\alpha >_{Lex} \beta$ si, en la diferencia vectorial $\alpha - \beta \in z^n$, la primera componente no nula por la izquierda es positiva. Escribiremos $x^\alpha >_{Lex} x^\beta$ si $\alpha >_{Lex} \beta$.

Proposición 29. El orden lexicográfico en $z_{\geq 0}^n$ es un orden monomial.

Demostración:

(i) Que $>_{Lex}$ es un orden total se deduce directamente de la definición y del hecho que el orden numérico usual en $z_{\geq o}$ es un orden total.

(ii) Si $\alpha >_{Lex} \beta$, entonces la primera componente no nula más a la izquierda en $\alpha - \beta$. Digamos $\alpha_k - \beta_k > 0$ es positiva. Pero $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ y $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Entonces en $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, la primera componente no nula más a la izquierda es de nuevo $\alpha_k - \beta_k > 0$.

(iii) Supongamos que $>_{Lex}$ no fuera un buen orden. Entonces por el lema (27), existiría una sucesión estrictamente decreciente infinita

$$\alpha(1) >_{Lex} \alpha(2) >_{Lex} \alpha(3) >_{Lex} \cdots >$$

de elementos de $z_{\geq 0}^n$. Mostraremos que esto conduce a una contradicción.

Consideremos las primeras componentes de los vectores $\alpha(i) \in z_{\geq 0}^n$. Por definición del orden Lex, estas primeras componentes forman una sucesión no creciente de enteros no negativos. Como $z_{\geq 0}^n$ es bien ordenado, las primeras componentes de los $\alpha(i)$ deben eventualmente "estabilizarse". Es decir, existe un K tal que todas las primeras componentes de los $\alpha(i)$ con $i \geq K$ son iguales.

Comenzando en $\alpha(K)$, la segunda y las subsiguientes componentes entran en juego en determinar el orden Lex. Las segundas componentes de $\alpha(K), \alpha(K+1), \dots$. Forman una sucesión decreciente. Por el mismo razonamiento de antes, las segundas componentes también se "estabilizan" en algún momento. Continuando de la misma manera, vemos que para algún I, las $\alpha(I), \alpha(I+1), \dots$ son todas iguales. Esto contradice el hecho que $\alpha(I) >_{Lex} \alpha(I+1)$. ■

Observación 30:

Es importante comprender que existen muchos órdenes Lex, dependiendo de cómo las variables son ordenadas. Hasta aquí, hemos usado el orden Lex con $x_1 > x_2 > \cdots > x_n$. Pero dado cualquier orden de las variables $x_1, \ldots, x_n$, existe un correspondiente orden lexicográfico. Por ejemplo, si las variables son x y y, entonces obtenemos un orden Lex con $x > y$ y un segundo con $y > x$. En el caso general de n variables, existen $n!$ órdenes Lex. En lo que sigue, la frase "orden Lex" se referirá a uno con $x_1 > \cdots > x_n$ a menos que se indique lo contrario.

En el orden Lex, notamos que una variable domina a cualquier monomio que involucre solamente a las variables menores, sin importar su grado total. Así, por el orden Lex con $x > y > z \cdots$ tenemos $x >_{Lex} y^6z^4$. Para ciertos propósitos, podemos también necesitar tomar en cuenta los grados totales de los monomios y ordenar monomios de mayor primer grado. Una manera de hacer esto es con el orden lexicográfico graduado.

Ejemplo 31. (Orden lexicográfico)

Lo desarrollaremos en el siguiente ejemplo; $K[x, y, z]$, $x > y > z$;

Tenemos los monomios

$$(\boldsymbol{a})\ x^6y^3z^2$$

$$(\boldsymbol{b})\ x^3y^4z$$

Vamos a ordenar estos monomios según el orden Lex.

Entonces:

$$x^6y^3z^2 \ >_{Lex}\ x^3y^4$$
$$= (6,3,2) \ - \ (3,4,1)$$
$$= (3,1,1)$$

Por tanto

$$\boldsymbol{x^6y^3z^2 \;\; >_{Lex} \;\; x^3y^4z}$$

Definición 32. (Orden Lexicográfico Graduado)

Sea $\alpha.\beta \in \; z_{\geq 0}^n$. Decimos que $\alpha >_{DegLex} \beta$, si

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i \,, \text{ O } \; |\alpha| = |\beta| \text{ y } \alpha >_{lex} \beta.$$

Vemos que el orden lexicográfico graduado ordena con el grado total primero, luego cuando son iguales usamos el orden lexicográfico.

Ejemplo 33. (Orden Lexicográfico Graduado)

Lo desarrollaremos en el siguiente ejemplo; $K[x,y,z]\,, x > y > z\,;$

Tenemos los monomios

$$(\boldsymbol{a})\; x^6y^3z^2$$

$$(\boldsymbol{b})\; x^3y^4z$$

Vamos a ordenar estos monomios según el orden $DegLex$.

Entonces:

$$x^6y^3z^2 \;\; >_{DegLex} \;\; x^3y^4z$$

$$|(6+3+2)| = \; 11 \quad \text{Y} \quad |(3+4+1)| = \; 8$$

Por tanto

$$\boldsymbol{x^6y^3z^2 \;\; >_{DegLex} \;\; x^3y^4z}$$

Definición 34. (Orden Lexicográfico Graduado Revertido)

Sean $\alpha.\beta \in z_{\geq 0}^{n}$. Decimos que $\alpha >_{DegRevLex} \beta$, si.

$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$, O $|\alpha| = |\beta|$ y en $\alpha - \beta \in \mathbb{Z}^n$, la primera componente no nula por la derecha es negativa.

Ejemplo 35. *(*Orden Lexicográfico Graduado Revertido)

Lo desarrollaremos en el siguiente ejemplo; $K[x, y, z]$, $x > y > z$;

Tenemos los monomios

$$(\boldsymbol{a})\ x^5y^2z$$

$$(\boldsymbol{b})\ x^2y^4z^2$$

Vamos a ordenar estos monomios según el orden $DegRevLex$.

Entonces:

$$x^5y^2z\ >_{DegRevLex}\ x^2y^4z^2$$

$$|(5+2+1)| = 8 \quad \text{Y} \quad |(2+4+2)| = 8$$

Como vemos el grado total de los monomios son iguales, entonces usamos la diferencia vectorial, encontrar la primera componente no nula por la derecha sea negativa.

Luego:

$$x^5y^2z \quad >_{DegRevLex} \quad x^2y^4z^2$$

$$= (5+2+1) - (2+4+2)$$

$$= (3, -2, -1)$$

Por tanto

$$\boldsymbol{x^5y^2z\ >_{DegRevLex}\ x^2y^4z^2}$$

Definición 36. (Orden Lexicográfico Inverso)

Sean $\alpha.\beta \in z_{\geq 0}^{n}$. Diremos que $\alpha >_{Lexin} \beta$, si y sólo si en la diferencia vectorial $\alpha - \beta \in z^{n}$, la primera componente no nula por la derecha es positiva.

Ejemplo 37. (Orden lexicográfico Inverso)

Lo desarrollaremos en el siguiente ejemplo; $K[x, y, z]$, $x > y > z$;

Tenemos los monomios

$$(\boldsymbol{a})\ x^5y^2z$$

$$(\boldsymbol{b})\ x^2y^4z^2$$

Vamos a ordenar estos monomios según el orden $Lexin$

Entonces:

$$x^5y^2z \quad >_{Lexin} \quad x^2y^4z^2$$
$$= (5 + 2 + 1) - (2 + 4 + 2)$$
$$= (3, -2, -1)$$

Por tanto

$$\boldsymbol{x^2y^4z^2 \quad >_{Lexin} \quad x^5y^2z}$$

Observación 38.

Para aclarar la relación entre el orden lexicográfico graduado del orden lexicográfico graduado revertido, observe que ambos usan el grado total del mismo modo. Pero la diferencia está en que $DegLex$ usa el orden Lex.

Es decir, mira la variable (mayor o) más a la izquierda y escoge la mayor potencia. En cambio, cuando en el $DegRegLex$ coinciden los grados totales, mira la variable (menor o) más a la derecha y escoge la menor potencia.

Existen muchos otros órdenes monomiales además de los considerados aquí. Muchos de los sistemas de álgebra computacional implementan el orden lexicográfico y muchos también permiten otros órdenes, tales como $DegLex$ y $DegRevLex$.

Nota 39. Ejemplos de órdenes Monomiales en anexo 12.1 página 93.

Definición 40. (Multigrado, Coeficiente y Monomio Principal)

Sean $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio no nulo en $K[x_1, \dots, x_n]$ y $>$ un orden monomial.

El **Multigrado** de f es

$$multigrad(f) = max\{\alpha \in \mathbb{Z}_{\geq 0}^n : a_\alpha \neq 0\}.$$

(El máximo es tomado respecto a $>$).

El **Coeficiente Principal** de f es

$$cp(f) = a_{multigrad(f)} \in k.$$

El **Monomio Principal** de f es

$$mp = x^{multigrad(f)}$$

(Con coeficiente 1)

El **Término Principal** de f es

$$tp(f) = cp(f) \cdot mp(f)$$

para ilustrar, sea $f = 6xy^3z + 3y^2z - 7x^4 - 8x^2y^3$ y sea $>$ el orden lexicográfico.

Entonces:

$multigrad(f) = (4,0,0)$	$cp(f) = -7$	$mp(f) = x^4$	$tp(f) = 7x^4$

En los ejercicios, se mostrará que el multigrado tiene las útiles propiedades siguientes.

Lema 41.

Sean $f, g \in K[x_1, \dots, x_n]$ polinomios no nulos.

Entonces:

(i) $multigrad(fg) = multigrad(f) + multigrad(g)$.

(ii) Si $f + g \neq 0$, entonces

$$multigrad(f + g) \leq max\{multigrad(f), multigrad(g)\}$$

Si, además $multigrad(f) \neq multigrad(g)$, se cumple la igualdad.

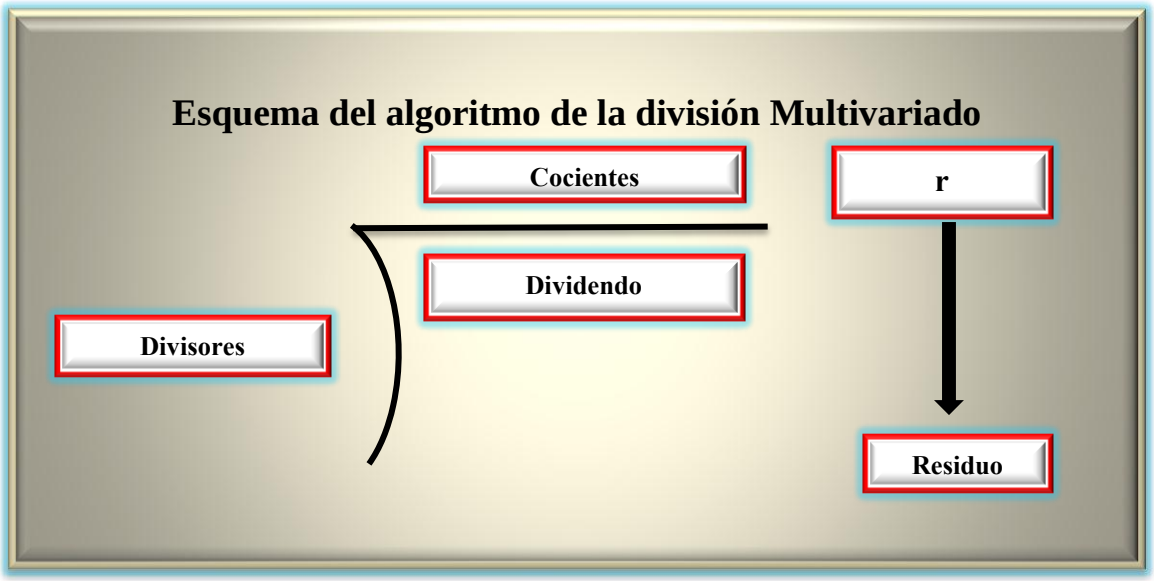
Teorema 42. Algoritmo De La División Multivariado

Fijemos un orden monomial $> en\ \mathbb{Z}_{\geq 0}^n$ y sea $F = (f_1, \dots, f_s)$ una $S - uplas$ ordenada de polinomios en $K[x_1, \dots, x_n]$. Entonces todo $f \in K[x_1, \dots, x_n]$ Puede ser escrito en la forma:

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

Donde $a_1\ r \in K[x_1, \dots, x_n]$, y $r = 0$ o r es una combinación lineal de monomios (con coeficientes en K), ninguno de los cuales es divisible por alguno de $tp(f_1), \dots, tp(f_s)$. Llamaremos a r un residuo de división de $f\ por\ F$. Además, si $a_i f_i \neq 0$, entonces tenemos

$$\text{multigrad(f)} \geq \text{multigrad}(a_i f_i).$$



La importancia de poder dividir m por una $s-upla$ de polinomios, con $s>1$, es porque más adelante los divisores g_i serán considerados como generadores de algún ideal I; en particular; teniendo presente que los ideales en $K[x_1,\dots,x_n]$ para $n\geq 2$ no podrán ser generados por cualquier polinomio.

Ejemplo 43.

Para ilustrar el Algoritmo de la División en $K[x_1,\dots,x_n]$.

Dados:

$$f_1=3x^3-4x^2-5x-2$$

$$f_2=x^2-1$$

$$f_3=x-2$$

Dividiendo f_1 por f_2 y f_3 Obtenemos:

$$
\begin{array}{ll|rl}
 & & a_2 : 3x-4 & \\
 & & a_3 : -2 & \quad r \\
\hline
f_2 = x^2-1 & & 3x^3-4x^2-5x-2 & \\
f_3 = x-2 & & \underline{-3x^3 \qquad +3x} & \\
 & & -4x^2-2x-2 & \\
 & & \underline{4x^2 \qquad -4} & \\
 & & -2x \quad -6 & \\
 & & \underline{2x \quad -4} & \\
 & & \underline{-10} & \\
 & & 0 \longrightarrow & -10
\end{array}
$$

Por tanto:

$$3x^3 - 4x^2 - 5x - 2 = (3x - 4)\, x^2 - 1 \; + (-2)\, x - 2 - 10$$

Definición 44. Sea $I \subset K[x_1, \dots, x_n]$ un ideal distinto de $\{0\}$.

Denotamos por $tp(I)$ al conjunto de todos los **términos principales** de los elementos de I. Así

$$tp(I) = \{cx^\alpha : existe\ f \in I\ con\ tp(f) = cx^\alpha\}$$

denotamos por $\langle tp(I)\rangle$. Al ideal generado por los elementos $tp(I)$.

Proposición 45. Sea $I \subset K[x_1, \dots, x_n]$ un ideal.

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

Existen $g_1, \dots, g_t \in I$ tal que $\langle tp(I)\rangle = \langle tp(g_1), \dots, tp(g_t)\rangle$.

9.3 Metodología

9.3.1 Tipo de investigación

El presente estudio, según el diseño es de tipo descriptivo, ya que se describe el algoritmo de Buchberger por medio de los $S-polinomios$ y los criterios de los $S-pares$ de Buchberger, la idea inmediata es tratar primero de extender el conjunto generador original hasta conseguir una base de Gröbner, luego describimos el teorema de eliminación, el paso de eliminación significa dar un procedimiento sistemático para encontrar elementos de I_l $(l-ésimo,$ ideal eliminación$)$, con un orden monomial apropiado, las bases de Gröbner nos permite hacer esto instantáneamente, describimos el teorema de extensión que se utiliza para eliminar cualquier número de variables. Todo esto es fundamental para la resolución de sistemas de ecuaciones polinomiales, así como también la solución de un problema aplicado y se hace mención de las aplicaciones de la bases de Gröbner.

9.3.2 Recursos computacionales

En el desarrollo del presente trabajo llevamos a cabo la resolución del problema de interés, resolver sistemas de ecuaciones polinomiales, los cuales se logran por medio de la obtención de una base de Gröbner. Para encontrar una base de Gröbner observamos que se requiere de mucho tiempo y de mucha destreza en el cálculo aritmético, los cual nos lleva a la necesidad de utilizar una herramienta que nos facilitará la obtención de dicha base de Gröbner.

El problema planteado es de actual interés por tanto como herramienta básica se utiliza el software CoCoA 4.7.5 para facilitar la obtención de una base de Gröbner, como también se utiliza para obtener ideales de eliminación que nos permite encontrar la variedad de un sistema de ecuación polinomial.

Cabe mencionar que en la actualidad existen diversos software para dar solución a un sinnúmero de problemas matemáticos tales software son (Maple, Mathematica, Reduce, Axiom, Macaulay, CoCoA, Sage, etc.)

9.3.3 ¿Qué es CoCoA?

Computations in Commutative Álgebra

El CoCoA es un sistema de álgebra computacional. Es libremente disponible y se puede encontrar en Internet, en la dirección URL

http://cocoa.dima.unige.it

CoCoA se entenderá "Cálculos en Álgebra conmutativa". Es capaz de realizar operaciones sencillas y sofisticadas en polinomios multivariados y sobre diversos datos relacionados con ellas (ideales, módulos, matrices, funciones racionales). Por ejemplo, se puede calcular fácilmente las bases de Gröbner, sicigias y resolución mínima libre, intersección, la división, el radical de un ideal, el ideal de los sistemas de cero-dimensionales, series de Poincaré y funciones de Hilbert, factorización de polinomios. Las capacidades de CoCoA y la flexibilidad de su uso se han mejorado aún más por el lenguaje de programación de alto nivel dedicado. Para mayor comodidad, el sistema ofrece una interfaz textual, un modo de Emacs, y una interfaz gráfica de usuario común a la mayoría de las plataformas.

Cabe destacar que en el presente trabajo se utiliza el software CoCoA 4.7.5 y que a partir de este momento todos los ejemplos resueltos manualmente se presentaran por medio del software CoCoA 4.7.5.

Aquí mostramos el ejemplo (43) realizado por medio del software CoCoA 4.7.5.

```
------------------------------
Use R ::= QQ[x,y,z],Lex;
  F := 3x^3-4x^2-5x-2;
  L := [x^2-1,x-2];
  Print "El resultado de la división algebraica es:";
  DivAlg(F, L);

El resultado de la división algebraica es:
------------------------------
Record[Quotients := [3x - 4, -2], Remainder := -10]
------------------------------
```

9.4 Sistemas de Ecuaciones Polinomiales

La geometría algebraica es la parte del álgebra que se ocupa de los sistemas de ecuaciones polinomiales con más de una incógnita y cuyas soluciones son elementos de un cuerpo.

Los sistemas de ecuaciones polinomiales aparecen en muchos modelos matemáticos de sistemas físicos, en el estudio de estructuras algebraicas y en la descripción algebraicas de objetos geométricos. Por tal razón debemos tener en mente que la meta principal es resolver dichos sistemas.

En este capítulo pretendemos aprender un poco sobre la naturaleza de las variedades.

9.4.1 Algoritmo de Buchberger y Bases de Gröbner

Buchberger bautizó estas bases con el nombre de bases de Gröbner, en honor a su director de tesis, W. Gröbner, que estimuló su interés por este problema, en realidad, H. Hironaka había descubierto ya este tipo de bases con antelación, a las que llamó bases estándar. Sin embargo, aunque demostró su existencia, su demostración, que no era constructiva, no arrojaba luz sobre el problema de cómo calcularlas. Buchberger, junto a su demostración, presentó un algoritmo que permitía construir una base de Gröbner a partir de un conjunto de polinomios dado.

Las bases de Gröbner, aunque inicialmente no tuvieron demasiada difusión, tuvieron finalmente un gran impacto en áreas muy diversas. Se emplean fundamentalmente para resolver el problema de la pertenencia al ideal en un anillo de polinomios y para decidir la relación de congruencia inducida por el ideal.

Una corta historia B. Buchberger.

Comencé mis estudios en matemática en 1960 en la Universidad de Innsbrukc, Austria, a la edad de 17 años. A partir de 1963 empecé a ganarme la vida trabajando como programador tiempo completo. A principios de 1964 trate de encontrar un tema para mi tesis de doctorado y asistí al seminario del profesor Wolfgang Gröbner (1899-1980).

Un día, en su seminario, el presento un "método" para encontrar una base linealmente independiente para el espacio vectorial del anillo de clases residuales de un ideal polinomial generado por un conjunto de polinomios (multivariados) y pregunto "cuando, para un conjunto de polinomios dados este método puede finalizar garantizando que la base obtenida mediante este sea una linealmente independiente" y, si este fuese posible como este método podía ser implementado en un cerebro electrónico. Yo pensé "esta es mi oportunidad", y después del seminario lo busque en su oficina y le pregunte si me podía permitir trabajar en esta pregunta. El asintió, le pregunte si existía literatura sobre este tema y me respondió que no, además no me dijo que el problema (mejor dicho una versión de este problema) era conocido como "El problema principal de la teoría de ideales polinomial") en el famoso libro de álgebra de Van Warden.

Luego Siguieron meses de trabajar duro seguidos con decenas de intentos de atacar el problema por un lado y por otro. Entonces, en algún momento de claridad. Vi que los puntos decisivos en los que "algo interesante" podía suceder durante el proceso de reducción con respecto a un sistema de polinomios eran los mínimos común múltiplos de los términos principales de los polinomios, la noción de lo que entonces llamarías "$S-polinomios$" (S por el tipo especial de "sustracción") y que si se sabe que los $S-polinomios$ reducen a cero, todas las reducciones de los polinomios en el ideal deben reducirse también a cero. A partir de este momento, todo fue rápido y fácil.

Mi algoritmo consistía de repetidos cálculos de $S-polinomios$, corrección de la prueba, finalización de la prueba, implementación en el lenguaje del computador, y primeras consideraciones de complejidad, primeras aplicaciones (para resolver sistema de ecuaciones polinomiales, para cálculos de Hilbert) y también la noción de "base con la propiedad "base de Gröbner").

En 1965 entregue mi tesis, en la oficina de estudios de mi profesor Wolfgang Gröbner, Pienso que tenía suficientes pruebas de que no leería mi tesis, más bien, se la entregó a un asistente para revisarle, recibí algunos comentarios sin importancia de su asistente y esto si era importante una carta de la oficina de estudio que decía que mi tesis había sido aceptada y que era admitido para el examen final. Gröbner en ese entonces, nunca me dio un comentario de mi trabajo, siendo franco, estaba completamente frustrado por esto Como consecuencia, cambie completamente mi campo, pero, antes de hacer esto, afortunadamente publique los resultados de mi tesis en un artículo periodístico.

En 1976 cuando las bases de Gröbner aparecen en el tapete de una manera bien rápida: fui invitado a dar una charla sobre mi nueva investigación ("machine Independent algoritm theory") en la Universidad de Kaiserslautern. Antes de mi charla, un colega vino a mi oficina (su nombre es Ruidiger loos). Él era un físico de educación y me dijo "Señor Buchberger, no quiero asistir a su charla. No porque no tenga tiempo si no porque encuentro, de cierto modo el título de su charla tonta". Claro que quede en shock por un momento y luego pensé que quizás estaba en lo correcto. Pero antes de ceder, cogí toda mi resistencia: psicológica y pregunte: "¿Señor Loos, que es lo que está haciendo que aparentemente cree que es importante y no tonto?" Él respondió: "Soy físico necesitamos nuevos algoritmos matemáticos, no los numéricos sino exactos, algebraicos y, en esta área, aparentemente, para los problemas más simples no sabemos algoritmos" Replique "por ejemplo". Loos: "Dados dos polinomios multivariados y un conjunto de relaciones laterales polinomiales queremos saber si los dos polinomios dados son equivalentes bajo las relaciones laterales. Si bien todo esto puede ser expresados en términos de $+,*$ y variables, nadie parecer tener un algoritmo para este aparentemente simple problema". Señor Loos, creo que sé cómo resolver su problema". Él me vio dubitativamente y yo le prometí enviarle mi artículo de Aequationes Mathematica, al día siguiente me telefoneó diciendo: "Buchberger", esto es fantástico, por favor escribe lo más pronto posible una presentación detallada de tu algoritmo y su teoría para nuestra revista ACM SIGSAM.

A partir de este momento, mi vida cambió drásticamente, fue como una explosión: invitaciones a muchas conferencias, instituciones, etc. Muchos grupos en el mundo empezaron a investigar mi "Teoría de las bases de Gröbner" y el interés de las investigaciones sobre mi teoría continúa extendiéndose hasta el presente.

Definición 46. Fijemos un orden monomial. Un conjunto finito $G = \{g_1, \dots, g_t\}$ de un ideal I es una **base de Gröbner** para I (o base estándar) si

$$\langle tp(g_1), \dots, tp(g_t)\rangle = \langle tp(I)\rangle.$$

Equivalentemente, aunque muy informal, un conjunto $G = \{g_1, \dots, g_t\} \subset I$ es una base de Gröbner de I si y sólo si el término principal de cualquier elemento de I es divisible por uno de los $tp(g_i)$.

Colorario 47. Fijemos un orden monomial. Entonces un ideal $I \neq \{0\} \subset K[x_1, \dots, x_n]$ tiene una base Gröbner. Además, toda base de Gröbner de un ideal I es una base de I.

9.4.1.1 Propiedades de las Bases de Gröbner

Proposición 48. Sea $G = \{g_1, \dots, g_t\}$ una base de Gröbner para un ideal $I \subset K[x_1, \dots, x_n]$, y sea $f \in K[x_1, \dots, x_n]$. Entonces existe un único $r \in K[x_1, \dots, x_n]$ con las siguientes propiedades.

i) Ningún término de r es divisible por cualquiera de $tp(g_1), \dots, tp(g_t)$

ii) Existe un $g \in I$ tal que $f = g + r$.

En particular, r es el residuo en la división de f por G sin importar como los elementos de G sean listados cuando usemos el algoritmo de la división.

Observación 49.

El residuo r es a veces llamado la forma normal de f y sus propiedades de unicidad serán exploradas en los ejercicios. En realidad las bases de Gröbner pueden ser caracterizadas por la unicidad del residuo.

Aunque el residuo r es único, para una base de Gröbner, los "coeficientes" a_i producidos por el algoritmo de la división $f = a_1 g_1 + \cdots + a_t g_t + r$ pueden cambiar si listados los generadores en un orden.

Corolario 50. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para un ideal $I \subset K[x_1, \ldots, x_n]$. Y sea $f \in K[x_1, \ldots, x_n]$. Entonces $f \in I$ si y sólo si el residuo de la división de f por G es cero.

Definición 51. Denotaremos por $\boldsymbol{\bar{f}^F}$. Al residuo que resulta de dividir f por la $S - upla$ ordenada $F = (f_1, \ldots, f_s)$. Si F es una base de Gröbner para $\langle f_1, \ldots, f_s \rangle$, entonces podemos considerar a F como un conjunto (sin orden en particular).

Ejemplo 52.

Sea $f: x^6 y^2$ con $F: (x^3 y^2 - y^3, x^5 y^3 - y^3) \in K[x, y]$

$$
\begin{array}{l|l l}
 & a_2 : x^3 + y & \\
 & a_3 : 0 & \qquad\qquad r \\
\hline
f_2 = x^3 y^2 - y^3 & x^6 y^2 & \\
f_3 = x^5 y^3 - y^3 & \underline{-x^6 y^2 + x^3 y^3} & \\
 & \quad x^3 y^3 & \\
 & \quad \underline{-x^3 y^3 + y^4} & \\
 & \qquad y^4 & \\
 & \qquad \underline{y^4} & \\
 & \qquad 0 & \longrightarrow \; y^4
\end{array}
$$

Entonces:

$$\overline{f}^{F} = r$$

$$\overline{x^6y^2}^{\{x^3y^2-y^3,x^5y^3-y^3\}} = y^4$$

Puesto que con el algoritmo de la división produce

$$x^6y^2 = (x^3 + y)\,(x^3y^2 - y^3) + 0(x^5y^3 - y^3) + y^4$$

Comprobación mediante CoCoA.

```
------------------------------
Use R ::= QQ[x,y,z],Lex;
  F := x^6y^2;
  L := [x^3y^2-y^3,x^5y^3-y^3];
  Print "El resultado de la división algebraica es:";
  DivAlg(F, L);

El resultado de la división algebraica es:
------------------------------
Record[Quotients := [x^3 + y, 0], Remainder := y^4]
------------------------------
```

Discutiremos después cómo saber si un conjunto generador dado de un ideal es una base de Gröbner. Como hemos indicado, el "obstáculo" para que $\{f_1, \dots, f_s\}$ sea una base de Gröbner es la posible aparición de combinaciones polinomiales de los f_i cuyos términos principales no estén en el ideal generado por $tp(f_i)$. Una forma en que esto pueda ocurrir es si los términos principales en una combinación adecuada

$$ax^{\alpha}f_i - bx^{\beta}f_j$$

Se cancelan, dejando solo términos más pequeños. Por otra parte,

$$ax^{\alpha}f_i - bx^{\beta}f_j \in I,$$

Así su término principal está en $\langle tp(I)\rangle$. Para estudiar este fenómeno de cancelación, introducimos las siguientes combinaciones especiales.

Definición 53. ($S-polinomio$) Sean $f, g \in K[x_1, \dots, x_n]$ polinomios no nulos.

Si el $multigrad\ (f) = \alpha$ y el $multigrad\ (g) = \beta$, entonces $\rho = (\gamma_1, \dots, \gamma_n)$ donde $\rho_i = \max(\alpha_i, \beta_i)$ para cada I. Llamamos a x^ρ el mínimo común múltiplo del $mp\ (f)$ y $mp\ (g)$, y escribimos

$$x^\rho = mcm\big(mp\ (f), mp\ (g)\big).$$

El $S-polinomio$ de $f\ y\ g$ es la combinación

$$S(f,g) = \frac{x^\rho}{tp(f)} \cdot f - \frac{x^\rho}{tp(g)} \cdot g$$

Un $S-polinomio\ S(f,g)$ está diseñado para producir la cancelación de los términos principales.

Ejemplo 54.

Calcular el $S-Polinomio$ de $f = (4x^2z - 7y^2),\ g = (xyz^2 + 3xz^2) \in R[x,y]$ con el orden Lex.

$$S(f,g) = \frac{x^\rho}{tp(f)} \cdot f - \frac{x^\rho}{tp(g)} \cdot g$$

$\boldsymbol{x^\rho = x^2yz^2}$
$\boldsymbol{tp(f) = 4x^2z}$
$\boldsymbol{tp(g) = xyz^2}$

$$S(f,g) = \frac{x^2yz^2}{4x^2z}(4x^2z - 7y^2) - \frac{x^2yz^2}{xyz^2}(xyz^2 + 3xz^2)$$

$$S(f,g) = \frac{yz}{4}(4x^2z - 7y^2) - x(xyz^2 + 3xz^2)$$

$$S(f,g) = x^2yz^2 - \frac{7}{4}y^3z - x^2yz^2 - 3x^2z^2$$

$$S(f,g) = -\frac{7}{4}y^3z - 3x^2z^2$$

Ordenando según Lex.

$$\boldsymbol{S(f,g) = -3x^2z^2 - \frac{7}{4}y^3z}$$

Comprobación de $S - polinomios$ mediante CoCoA.

```
------------------------------
Use R ::= QQ[x,y,z],Lex;
F1:= 4x^2z-7y^2;
F2:= xyz^2+3xz^2;
TP1:=LT(F1);
TP2:=LT(F2);
M:=LCM(TP1, TP2);
SPOLY:=(M/TP1)*(F1)-(M/TP2)*(F2);
Print "El S-polinomio es:";
SPOLY;

El S-polinomio es:
------------------------------
- 3x^2z^2 - 7/4y^3z
------------------------------
```

Nota 55. Cabe destacar que el algoritmo que presentamos para calcular $S-polinomios$ es un algoritmo especial que fue programado para correrse en el CoCoA 4.7.5, esté programa fue elaborado por nuestro equipo de investigación, además de esté programa existen otros software que calculan directamente $S-polinomios$ como el Mathematica, Maple, etc.

Comprobación de $S-polinomios$ mediante Maple.

```
>
  with(Groebner) :
  f := 4*x^2*z - 7*y^2 :
  g := x*y*z^2 + 3*x*z^2 :
  SPolynomial(f, g, plex(x, y, z));
                                  -12 x^2 z^2 - 7 y^3 z
```

Lema 56. Supongamos que tenemos una suma $\sum_{i=1}^{s} c_i f_i$, donde $c_i \in K$ y el $multigrad(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$ para todo i. Si el $multigrad(\sum_{i=1}^{s} c_i f_i) < \delta$, entonces $\sum_{i=1}^{s} c_i f_i$ es una combinación lineal. Con coeficientes en K, de los $S-polinomio\ S(f_j, f_k)$ para $1 \leq jK \leq s$. Además cada $S(f_j, f_k)$ tiene $multigrad < \delta$.

Teorema 57. (*Criterio de los S −pares de Buchberger)*

Sea I un ideal polinomial. Entonces una base $G = \{g_1, \dots, g_t\}$ de I es una base de Gröbner de I si y sólo si para todas las parejas $i \neq j$, el residuo de la división de $S(g_i, g_j)$ por G (listado en cierto orden) es cero.

Demostración:

($\Rightarrow$) Si G es una base de Gröbner, entonces, dado que $S(g_i, g_j) \in I$, el residuo de la división por G es cero por el Corolario 50.

($\Leftarrow$) Sea $f \in I$ un polinomio no nulo. Debemos probar que si todos los $S-polinomios$ tienen residuo cero al dividirlos por G, entonces $tp(f) \in \langle tp(g_1), \dots, tp(g_t)\rangle$. Antes de dar los detalles, vamos a bosquejar la estrategia de la demostración.

Dado $f \in I = \langle g_1, \dots, g_t\rangle$, existen polinomios $h_i \in K[x_1, \dots, x_n]$ tales que

$$f = \sum_{i=1}^{t} h_i g_i \qquad (2)$$

Del lema 18, se sigue que

$$multigrad\ (f) \leq \max\big(multigrad\ (h_i g_i)\big) \qquad (3)$$

Si la igualdad no ocurre, entonces alguna cancelación entre los términos principales de (2) debe ocurrir. El lema 56 nos permitirá reescribir esto en términos de los $S-polinomios$. Entonces nuestra suposición de que los $S-polinomios$ tienen residuo cero permitirá reemplazar los $S-polinomios$ por expresiones que involucren menos cancelaciones. Así, obtendremos una expresión para f que tenga menos cancelaciones de términos principales. Continuando de esta manera, encontráremos eventualmente una expresión (2) para f donde la igualdad ocurre en (3). Entonces

$$multigrad\ (f) = \big(multigrad\ (h_i g_i)\big)$$

Para algún i, y de ello se seguirá que $tp(f)$ es divisible por $tp(g_i)$. Esto demostrará que $tp(f) \in \langle tp(g_1), \dots, tp(g_t)\rangle$, que es lo que queremos probar.

Demos ahora los detalles de la demostración. Dada una expresión (2) para f, sea $m(i) = multigrad\ (h_i g_i)$, y definamos $\delta = max(m(1), \dots, m(t))$.

Entonces la desigualdad (3) se vuelve

$$multigrad\ (f) \leq \delta.$$

Ahora consideremos todas las posibles maneras en que f puede ser escrito de la forma (2). Para cada una de estas expresiones, obtenemos posiblemente un δ diferente. Ya que un

orden monomial es un buen orden, podemos seleccionar una expresión (2) para f tal que δ sea mínimo.

Mostraremos que una vez que este δ mínimo es escogido, tenemos $multigrad\,(f) = \delta$. Entonces la igualdad ocurre en (3), y como observamos, se sigue que $tp(f) \in \langle tp(g_1), \dots, tp(g_t)\rangle$. Esto probará el teorema.

Resta probar que $multigrad\,(f) = \delta$. Probaremos esto por contradicción. La igualdad prueba fallar solo cuando el $multigrad\,(f) < \delta$. Para aislar los términos de multigrado δ, escribimos f en la forma siguiente:

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} tp(h_i) g_i + \sum_{m(i)<\delta} \big(h_i - tp(h_i)\big)\, g_i + \sum_{m(i)<\delta} h_i g_i \qquad (4)$$

Los monomios que aparecen en la segunda y la tercera suma del miembro derecho de la igualdad tienen $multigrad\ < \delta$. Así, la suposición de que $multigrad\,(f) < \delta$ significa que la primera suma también $multigrad\ < \delta$.

Sea $tp(h_i) = c_i x^{\alpha(i)}$. Entonces la primera suma

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

tiene exactamente la forma descrita en el lema 65 con $f_i = x^{\alpha(i)} g_i$. Así el lema 56 implica esta suma es una combinación lineal de los $S - polinomios.\ S\big(x^{\alpha(j)} g_j\,, x^{\alpha(k)} g_k\big)$. Sin embargo,

$$S\big(x^{\alpha(j)} g_j\,, x^{\alpha(k)} g_k\big) = \frac{x^{\delta}}{x^{\alpha(j)} tp\big(g_j\big)} x^{\alpha(j)} g_i - \frac{x^{\delta}}{x^{\alpha(k)} tp(g_k)} x^{\alpha(k)} g_k.$$

$$= \frac{x^{\delta}}{tp\big(g_j\big)} g_j - \frac{x^{\delta}}{tp(g_k)} g_k$$

$$= \frac{x^{\delta}.x^{\gamma_{jk}}}{x^{\gamma_{jk}}.tp\big(g_j\big)} g_j - \frac{x^{\delta}.x^{\gamma_{jk}}}{x^{\gamma_{jk}}.tp(g_k)} g_k$$

$$= x^{\delta-\gamma_{jk}} \left[\frac{x^{\gamma_{jk}}}{tp(g_j)} g_j - \frac{x^{\gamma_{jk}}}{tp(g_k)} g_k\right]$$

$$= x^{\delta-\gamma_{jk}}\, S(g_j, g_k)$$

Donde $x^{\gamma_{jk}} = mcm\big(mp(g_i), mp(g_k)\big)$. Asi existen las constante $c_{jk} \in k$ tales que

$$\sum_{m(i)=\delta} tp(h_i)g_i = \sum_{jk} c_{jk}\, x^{\delta-\gamma_{jk}}\, S(g_j, g_k) \qquad (5)$$

El próximo paso es usar nuestra hipótesis de que el residuo de $S(g_j, g_k)$ en la división por los $g_1, \dots, g_t$ es cero. Usando el algoritmo de la división, esto significa que cada $S-polinomio$ puede ser escrito en la forma

$$S\big(g_j, g_k\big) = \sum_{i=1}^{t} a_{ijk} g_i, \qquad (6)$$

Donde $a_{ijk} \in K[x_1, \dots, x_n]$. El algoritmo de la división también nos dice que

$$multigrad\,\big(a_{ijk}g_i\big) \leq multigrad\,\big(S(g_i, g_k)\big) \qquad (7)$$

Para todo i, j, k ver Teorema (42). Intuitivamente, esto dice que cuando el residuo es cero, podemos encontrar una expresión para los $S(g_i, g_k)$ en términos de G donde los términos principales no todos se cancelan.

Para explotar esto, multiplique la expresión para los $S(g_i, g_k)$ por $x^{\delta-\gamma_{jk}}$ para obtener

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

Donde $b_{ijk} = x^{\delta-\gamma_{jk}} a_{ijk}$. Entonces (7) y el Lema (56) implica que

$$multigrad\,\big(b_{ijk}g_i\big) \leq multigrad\,\Big(x^{\delta-\gamma_{jk}} S(g_i, g_k)\Big) < \delta \qquad (8)$$

Si sustituimos la expresión de arriba para $x^{\delta-\gamma_{jk}} S(g_i, g_k)$ en (5), obtenemos la ecuación.

$$\sum_{m(i)=\delta} tp(h_i)g_i = \sum_{jk} c_{jk}\, x^{\delta-\gamma_{jk}}\, S\big(g_j, g_k\big) = \sum_{jk} c_{jk} \left(\sum_{i} b_{ijk} g_i\right) = \sum_{i} \bar{h}_i g_i,$$

La que por (8) tiene la propiedad que para todo i,

$$multigrad\,\big(\bar{h} g_i\big) < \delta$$

Para el paso final de la prueba, sustituyamos $\sum_{m(i)=\delta} tp(h_i)g_i = \sum_i \bar{h}_i g_i$ en la ecuación (4) para obtener una expresión para f como una combinación polinomial de los g_i donde todos los términos tienen $multigrado < \delta$ esto contradice la minimalidad de δ y completa la prueba del teorema. ■

Teorema 58.* (*Algoritmo de Buchberger)

Sea $\mathcal{G} = (g_1, \dots, g_s) \in (p^r)^s$ una tupla no nula de elementos los cuales generan un submódulo $M = \langle g_1, \dots, g_s \rangle \subseteq p^r$. Para $i = 1, \dots, s$, sea $mp_\sigma(g_i) = c_i t_i e_{\gamma_i}$ con $c_i \in K \setminus \{0\}, t_i \in \mathbb{T}^n, y\ \gamma_i \in \{1, \dots, r\}$. Considere la siguiente secuencia de instrucciones.

1) Sea $s' = s$ y $B = \mathbb{B} = \left\{(i,j) \,\middle|\, 1 \le i < j \le s', \gamma_i = \gamma_j\right\}$.
2) Si $B = \emptyset$, retorna el resultado $\mathcal{G}$. De otro modo, escoger un par $(i,j) \in B$ y eliminarlo de B.
3) Calcular

$$S_{i,j} = \frac{t_j}{c_i mcd(t_i, t_j)} g_i - \frac{t_i}{c_j mcd(t_i, t_j)} g_j$$

Y $RN_{\sigma,\mathcal{G}}(S_{i,j})$. Si el resultado es $RN_{\sigma,\mathcal{G}}(S_{i,j}) = 0$, continuar con el paso 2).

4) Incrementar s' en uno. Añadir $g_{s'} = RN_{\sigma,\mathcal{G}}(S_{i,j})$ a $\mathcal{G}$ y el conjunto de pares $\left\{(i,j) \,\middle|\, 1 \le i < j \le s', \gamma_i = \gamma_j\right\}$ a B. Entonces continuar con el paso 2).

Este es un algoritmo, es decir que se detiene después de un número finito de pasos. Retorna una $n - uplas\ \mathcal{G}$ de vectores los cuales forman una $\sigma - base$ de Gröbner de M.

Prueba. Cada vez que el paso 2) es ejecutado, un par es cancelado de B. El conjunto B es ampliado solo en el paso 4). Cuando esto ocurre, un elemento es añadido a G el cual tiene un término principal, con respecto a σ, que no está en el submódulo generado por los términos principales de los elementos previos de M. Por consiguiente, el paso 4) debe ser ejecutado solo un número finito de veces, es decir, el procedimiento se detiene después de un número finito de pasos.

Ejemplo 59. Encontrar una base de Gröbner para el ideal I.

Consideremos el anillo $K[x, y, z]$ con el orden lexicográfico y sea:

$$I = \langle f_1, f_2 \rangle = \langle x^2y^2 - z\ , xy^2z - xyz \rangle.$$

$f_1 = x^2y^2 - z$

$f_2 = \ xy^2z - xyz$

f_1, f_2 Se encuentran ordenados según el orden lex.

Ahora encontrando $S - polinomios$ para$f_1, f_2,$ tenemos la fórmula.

$$S(f_1, f_2) = \frac{x^\rho}{tp(f_1)} \cdot\ f_1 - \frac{x^\rho}{tp(f_2)}\ \cdot f_2$$

$\boldsymbol{x^\rho = x^2y^2z}$
$\boldsymbol{tp(f_1) = x^2y^2}$
$\boldsymbol{tp(f_2) = xy^2z}$

$$S(f_1, f_2) = \frac{x^2y^2z}{x^2y^2}(x^2y^2 - z\ ) - \frac{x^2y^2z}{xy^2z}(\ xy^2z - xyz)$$

$$S(f_1, f_2) = z(x^2y^2 - z) - x(\ xy^2z - xyz)$$

$$S(f_1, f_2)\ = x^2y^2z - z^2 - x^2y^2z + x^2yz$$

$$S(f_1, f_2) = -z^2 + x^2yz$$

Ordenado según Lex.

$$S(f_1, f_2) = x^2yz - z^2$$

Luego utilizando el algoritmo de la división para $S(f_1,f_2)$ por f_1 y f_2.

$$
\begin{array}{r|l}
 & a_1 : 0 \\
 & a_2 : 0 \qquad\qquad r \\
f_1 = x^2y^2 - z & \overline{x^2yz - z^2} \\
f_2 = xy^2z - xyz & \underline{0} \\
 & x^2yz - z^2 \\
 & \underline{-z^2} \longrightarrow x^2yz \\
 & 0 \longrightarrow x^2yz - y^2
\end{array}
$$

Ya que nuestro residuo no es nulo. Por tanto, debemos incluir el residuo en nuestro conjunto generador, como un nuevo generador. $f_3 = x^2yz - z^2$

Entonces $F = \{f_1,f_2,f_3\} = \{x^2y^2 - z, xy^2z - xyz,\ x^2yz - z^2\}$.

Por otro lado determinando $\overline{S(f_1,f_2)}^F$ Obtenemos:

$$
\begin{array}{r|l}
 & a_1 : 0 \\
 & a_2 : 0 \\
 & a_3 : 1 \\
f_1 = x^2y^2 - z & \overline{x^2yz - z^2} \\
f_2 = xy^2z - xyz & \underline{-x^2yz + z^2} \\
f_3 = x^2yz - z^2 & 0
\end{array}
$$

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

Encontrando $S-polinomio\ S(f_1,f_3)$

$x^{\rho}=x^2y^2z$
$tp(f_1)=x^2y^2$
$tp(f_3)=x^2yz$

$$S(f_1,f_3)=\frac{x^2y^2z}{x^2y^2}(x^2y^2-z)-\frac{x^2y^2z}{x^2yz}(x^2yz-z^2)$$

$$S(f_1,f_3)=z(x^2y^2-z)-y(x^2yz-z^2)$$

$$S(f_1,f_3)=x^2y^2z-z^2-x^2y^2z+yz^2$$

$$S(f_1,f_3)=-z^2+yz^2$$

Ordenado según Lex.

$$S(f_1,f_3)=yz^2-z^2$$

Luego utilizando el algoritmo de la división para $S(f_1,f_3)$ por F

$$\begin{array}{l} a_1:0 \\ a_2:0 \\ a_3:0 \end{array} \qquad r$$

$$\begin{array}{l} f_1=x^2y^2-z \\ f_2=xy^2z-xyz \\ f_3=x^2yz-z^2 \end{array} \Big)\ \overline{yz^2-z^2}$$

$$\underline{0}$$

$$\underline{yz^2-z^2}$$

$$\underline{-z^2} \longrightarrow yz^2$$

$$0 \longrightarrow yz^2-z^2$$

Ya que nuestro residuo no es nulo. Por tanto, debemos incluir el residuo en nuestro conjunto generador, como un nuevo generador $f_4 = \ yz^2 - z^2$.

Entonces

$$F = \{f_1, f_2, f_3, f_4\} = \{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2\}$$

Por otro lado determinando $\overline{S(f_1,f_3)}^F$ Obtenemos:

$$\begin{array}{l} f_1 = x^2y^2 - z \\ f_2 = xy^2z - xyz \\ f_3 = x^2yz - z^2 \\ f_4 = yz^2 - z^2 \end{array} \quad \begin{array}{l} a_1 = 0 \\ a_2 = 0 \\ a_3 = 0 \\ a_4 = 1 \end{array} \quad \Big| \begin{array}{r} \mathrm{yz^2 - z^2} \\ \mathrm{-yz^2 + z^2} \\ \hline 0 \end{array}$$

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

Encontrando $S - polinomio\ \ S(f_1,f_4)$

$x^\rho = x^2y^2z^2$
$tp(f_1) = x^2y^2$
$tp(f_4) = yz^2$

$$S(f_1,f_4) = \frac{x^2y^2z^2}{x^2y^2}(x^2y^2 - z) - \frac{x^2y^2z^2}{yz^2}(yz^2 - z^2)$$

$$S(f_1,f_4) = z^2(x^2y^2 - z) - x^2y(yz^2 - z^2)$$

$$S(f_1,f_4) = x^2y^2z^2 - z^3 - x^2y^2z^2 + x^2yz^2$$

$$S(f_1,f_4) = -z^3 + x^2yz^2$$

Ordenado según Lex.

$$S(f_1,f_4) = x^2yz^2 - z^3$$

Luego utilizando el algoritmo de la división para $S(f_1,f_4)$ por F

$$\begin{array}{l} f_1 = x^2y^2 - z \\ f_2 = xy^2z - xyz \\ f_3 = x^2yz - z^2 \\ f_4 = yz^2 - z^2 \end{array} \quad \begin{array}{l} a_1 = 0 \\ a_2 = 0 \\ a_3 = 0 \\ a_4 = 0 \end{array} \quad \left| \begin{array}{r} x^2yz^2 - z^3 \\ -x^2yz^2 + z^3 \\ \hline 0 \end{array} \right.$$

Ya que nuestro residuo es nulo. Por tanto, no debemos incluir el residuo en nuestro conjunto generador. Por tanto, F no tiene ningún cambio.

$$F = \{f_1,f_2,f_3,f_4\} = \{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2\}$$

Encontrando $S-polinomio\ S(f_2,f_3)$

$x^\rho = x^2y^2z$
$tp(f_2) = xy^2z$
$tp(f_3) = x^2yz$

$$S(f_2,f_3) = \frac{x^2y^2z}{xy^2z}(xy^2z - xyz) - \frac{x^2y^2z}{x^2yz}(x^2yz - z^2)$$

$$S(f_2,f_3) = x(xy^2z - xyz) - y(x^2yz - z^2)$$

$$S(f_2,f_3) = x^2y^2z - x^2yz - x^2y^2z + yz^2$$

$$S(f_2, f_3) = -x^2yz + yz^2$$

$$S(f_2, f_3) = -x^2yz + yz^2$$

Luego utilizando el algoritmo de la división para $S(f_{2,}f_3)$ por F

$$f_1 = x^2y^2 - z$$
$$f_2 = xy^2z - xyz$$
$$f_3 = x^2yz - z^2$$
$$f_4 = yz^2 - z^2$$

$$a_1 = 0$$
$$a_2 = 0$$
$$a_3 = -1$$
$$a_4 = 1$$

$$\begin{array}{r} -x^2yz + yz^2 \\ x^2yz - z^2 \\ \hline yz^2 - z^2 \\ -yz^2 + z^2 \\ \hline 0 \end{array}$$

Ya que nuestro residuo es nulo. Por tanto, no debemos incluir el residuo en nuestro conjunto generador. Por tanto, F no tiene ningún cambio.

$$F = \{f_{1,}f_2, f_3, f_4\} = \{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2\}$$

Encontrando $S - polinomio$ $S(f_{2,}f_4)$

$x^\rho = xy^2z^2$
$tp(f_2) = xy^2z$
$tp(f_4) = yz^2$

$$S(f_2, f_4) = \frac{xy^2z^2}{xy^2z}(xy^2z - xyz) - \frac{xy^2z^2}{yz^2}(yz^2 - z^2)$$

$$S(f_2, f_4) = z(xy^2z - xyz) - xy(yz^2 - z^2)$$

$$S(f_2, f_4) = xy^2z^2 - xyz^2 - xy^2z^2 + xyz^2$$

$S(f_2, f_4) = 0$

Ya que nuestro $S - polinomio$ es nulo. Por tanto, F no tiene ningún cambio.

$$F = \{f_1, f_2, f_3, f_4\} = \{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2\}$$

Encontrando $S - polinomio$ $S(f_3, f_4)$

$x^\rho = x^2yz^2$
$tp(f_3) = x^2yz$
$tp(f_4) = yz^2$

$$S(f_3, f_4) = \frac{x^2yz^2}{x^2yz}(x^2yz - z^2) - \frac{x^2yz^2}{yz^2}(yz^2 - z^2)$$

$$S(f_3, f_4) = z(x^2yz - z^2) - x^2(yz^2 - z^2)$$

$$S(f_3, f_4) = x^2yz^2 - z^3 - x^2yz^2 + x^2z^2$$

$$S(f_3, f_4) = -z^3 + x^2z^2$$

Ordenado según *Lex*

$$S(f_3, f_4) = x^2z^2 - z^3$$

Luego utilizando el algoritmo de la división para $S(f_3, f_4)$ por F

$$\begin{array}{l} a_1 = 0 \\ a_2 = 0 \\ a_3 = 0 \\ a_4 = 0 \end{array}$$

$$\begin{array}{l} f_1 = x^2y^2 - z \\ f_2 = xy^2z - xyz \\ f_3 = x^2yz - z^2 \\ f_4 = yz^2 - z^2 \end{array} \quad \Big| \quad \begin{array}{r} x^2z^2 - z^3 \\ \hline 0 \\ \hline x^2z^2 - z^3 \\ \hline -z^3 \\ \hline 0 \end{array} \qquad \begin{array}{l} r \\ \\ \\ \\ \longrightarrow x^2z^2 \\ \longrightarrow x^2z^2 - z^3 \end{array}$$

Ya que nuestro residuo no es nulo. Por tanto, debemos incluir el residuo en nuestro conjunto generador, como un nuevo generador $f_5 = x^2z^2 - z^3$.

Entonces

$$F = \{f_1, f_2, f_3, f_4, f_5\} = \{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2, x^2z^2 - z^3\}$$

Por otro lado determinando $\overline{S(f_3, f_4)}^F$ Obtenemos:

$$\begin{array}{l} a_1 = 0 \\ a_2 = 0 \\ a_3 = 0 \\ a_4 = 0 \\ a_5 = 1 \end{array}$$

$$\begin{array}{l} f_1 = x^2y^2 - z \\ f_2 = xy^2z - xyz \\ f_3 = x^2yz - z^2 \\ f_4 = yz^2 - z^2 \\ f_5 = x^2z^2 - z^3 \end{array} \quad \Big| \quad \begin{array}{r} x^2z^2 - z^3 \\ \hline -x^2z^2 + z^3 \\ \hline 0 \end{array}$$

$$\overline{S(f_3, f_4)}^F = 0$$

Encontrando $S-polinomio$ $S(f_3,f_5)$

$x^{\rho}=x^2yz^2$
$tp(f_3)=x^2yz$
$tp(f_5)=x^2z^2$

$$S(f_3,f_5)=\frac{x^2yz^2}{x^2yz}(x^2yz-z^2)-\frac{x^2yz^2}{x^2z^2}(x^2z^2-z^3)$$

$$S(f_3,f_5)=z(x^2yz-z^2)-y(x^2z^2-z^3)$$

$$S(f_3,f_5)=x^2yz^2-z^3-x^2yz^2+yz^3$$

$$S(f_3,f_5)=-z^3+yz^3$$

Ordenado según Lex

$$S(f_3,f_5)=yz^3-z^3$$

Luego utilizando el algoritmo de la división para $S(f_3,f_5)$ por F

$$\begin{array}{l} a_1=0 \\ a_2=0 \\ a_3=0 \\ a_4=0 \\ a_5=0 \end{array}$$

$$\begin{array}{l} f_1=x^2y^2-z \\ f_2=xy^2z-xyz \\ f_3=x^2yz-z^2 \\ f_4=yz^2-z^2 \\ f_5=x^2z^2-z^3 \end{array} \quad \overline{\left.\begin{array}{r} yz^3-z^3 \\ -yz^3+z^3 \\ \hline 0 \end{array}\right)}$$

Ya que nuestro residuo es nulo. Por tanto, no debemos incluir el residuo en nuestro conjunto generador. Por tanto, F no tiene ningún cambio.

$$F=\{f_1,f_2,f_3,f_4,f_5\}=\{x^2y^2-z,xy^2z-xyz,x^2yz-z^2,yz^2-z^2,\ x^2z^2-z^3\}$$

Encontrando $S-polinomio \quad S(f_4,f_5)$

$x^{\rho}=x^2yz^2$
$tp(f_4)=yz^2$
$tp(f_5)=x^2z^2$

$$S(f_4,f_5)=\frac{x^2yz^2}{yz^2}(yz^2-z^2)-\frac{x^2yz^2}{x^2z^2}(x^2z^2-z^3)$$

$$S(f_4,f_5)=x^2(yz^2-z^2)-y(x^2z^2-z^3)$$

$$S(f_4,f_5)=x^2yz^2-x^2z^2-x^2yz^2+yz^3$$

$$S(f_4,f_5)=-x^2z^2+yz^3$$

Luego utilizando el algoritmo de la división para $S(f_4,f_5)$ por F

$$\begin{array}{l} a_1=0 \\ a_2=0 \\ a_3=0 \\ a_4=z \\ a_5=-1 \end{array}$$

$$\begin{array}{l} f_1=x^2y^2-z \\ f_2=xy^2z-xyz \\ f_3=x^2yz-z^2 \\ f_4=yz^2-z^2 \\ f_5=x^2z^2-z^3 \end{array} \;\Big|\; \begin{array}{r} -x^2z^2+yz^3 \\ \underline{x^2z^2-z^3} \\ yz^3-z^3 \\ \underline{-yz^3+z^3} \\ 0 \end{array}$$

Ya que nuestro residuo es nulo. Por tanto, no debemos incluir el residuo en nuestro conjunto generador. Por tanto, F no tiene ningún cambio.

$$F=\{f_1,f_2,f_3,f_4,f_5\}=\{x^2y^2-z,xy^2z-xyz,x^2yz-z^2,yz^2-z^2,\ x^2z^2-z^3\}$$

Encontrando $S - polinomio\ \ S(f_1, f_5)$

$x^{\rho} = x^2y^2z^2$
$tp(f_1) = x^2y^2$
$tp(f_5) = x^2z^2$

$$S(f_1, f_5) = \frac{x^2y^2z^2}{x^2y^2}(x^2y^2 - z) - \frac{x^2y^2z^2}{x^2z^2}(x^2z^2 - z^3)$$

$$S(f_1, f_5) = z^2(x^2y^2 - z) - y^2(x^2z^2 - z^3)$$

$$S(f_1, f_5) = x^2y^2z^2 - z^3 - x^2y^2z^2 + y^2z^3$$

$$S(f_1, f_5) = -z^3 + y^2$$

Ordenado según *Lex*

$$S(f_1, f_5) = y^2z^3 - z^3$$

Luego utilizando el algoritmo de la división para $S(f_1, f_5)$ por F

$$
\begin{array}{l|l}
 & a_1 = 0 \\
 & a_2 = 0 \\
 & a_3 = 0 \\
 & a_4 = yz + z \\
 & a_5 = 0 \\
\hline
f_1 = x^2y^2 - z & y^2z^3 - z^3 \\
f_2 = xy^2z - xyz & -y^2z^3 + yz^3 \\
\cline{2-2}
f_3 = x^2yz - z^2 & yz^3 - z^3 \\
f_4 = yz^2 - z^2 & -yz^3 + z^3 \\
\cline{2-2}
f_5 = x^2z^2 - z^3 & 0
\end{array}
$$

Ya que nuestro residuo es nulo. Por tanto, no debemos incluir el residuo en nuestro conjunto generador. Por tanto, F no tiene ningún cambio.

$$F = \{f_1, f_2, f_3, f_4, f_5\} = \{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2,\ x^2z^2 - z^3\}$$

Encontrando $S - polinomio$ $S(f_2, f_5)$

$x^\rho = x^2y^2z^2$
$tp(f_2) = xy^2z$
$tp(f_5) = x^2z^2$

$$S(f_2, f_5) = \frac{x^2y^2z^2}{xy^2z}(xy^2z - xyz) - \frac{x^2y^2z^2}{x^2z^2}(x^2z^2 - z^3)$$

$$S(f_2, f_5) = xz(xy^2z - xyz) - y^2(x^2z^2 - z^3)$$

$$S(f_2, f_5) = x^2y^2z^2 - x^2yz^2 - x^2y^2z^2 + y^2z^3$$

$$S(f_2, f_5) = -x^2yz^2 + y^2z^3$$

Luego utilizando el algoritmo de la división para $S(f_2, f_5)$ por F

$$
\begin{array}{l|l}
 & a_1 = 0 \\
 & a_2 = 0 \\
 & a_3 = 0 \\
 & a_4 = yz \\
 & a_5 = -y \\
\hline
f_1 = x^2y^2 - z & -x^2yz^2 + y^2z^3 \\
f_2 = xy^2z - xyz & \underline{x^2yz^2 - yz^3} \\
f_3 = x^2yz - z^2 & y^2z^3 - yz^3 \\
f_4 = yz^2 - z^2 & \underline{-yz^3 + yz^3} \\
f_5 = x^2z^2 - z^3 & 0
\end{array}
$$

Ya que nuestro residuo es nulo. Por tanto, no debemos incluir el residuo en nuestro conjunto generador. Por tanto, F no tiene ningún cambio.

$$F = \{f_1, f_2, f_3, f_4, f_5\} = \{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2,\ x^2z^2 - z^3\}$$

Habiendo realizado todas las combinaciones posibles podemos observar que

$$\overline{S(f_i, f_j)}^{\{f_1, f_2, f_3, f_4, f_5\}} = \mathbf{0}\ \forall\ \boldsymbol{i} > \mathbf{j},$$ Y así concluimos que

$$\boldsymbol{F = \{f_1, f_2, f_3, f_4, f_5\}}$$

$\boldsymbol{F} = \{\boldsymbol{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2,\ x^2z^2 - z^3}\}$. Es base de Gröbner.

Aquí mostramos la solución del ejemplo (59) realizado por el CoCoA.

Encontrar una base de Gröbner para el ideal I.

$$I = \langle f_1, f_2 \rangle = \langle x^2y^2 - z\ , xy^2z - xyz \rangle$$

```
-------------------------------
Use R ::= QQ[x,y,z],Lex;
  I := Ideal(x^2y^2-z, xy^2 z-xyz);
  Print "A continuación se describe el ideal:";
  Describe I;
  Print "La base de Gröbner es:";
  GBasis(I);

A continuación se describe el ideal:
-------------------------------
Record[Type := IDEAL, Value := Record[Gens := [x^2y^2 - z, xy^2z - xyz]]]
-------------------------------
La base de Gröbner es:
-------------------------------
[xy^2z - xyz, x^2y^2 - z, -x^2yz + z^2, yz^2 - z^2, x^2z^2 - z^3]
-------------------------------
```

Nota 60. Los cálculos detallados para los $S - polinomios$ del ejemplo (59) se encuentran realizados con el CoCoA en anexo 12.2 página 94.

Definición 61. Una **base de Gröbner reducida** de un ideal polinomial I es una base de Gröbner G de I tal que:

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

(ii) Para todo $p \in G$, ningún monomio de p pertenece a $\langle tp(G - \{p\}) \rangle$.

Proposición 62. Sea $I \neq \{0\}$ un ideal polinomial. Entonces, para un orden monomial dado, I tiene una única base de Gröbner reducida.

Demostración:

Sea G una base de Gröbner minimal de I. Decimos que $g \in G$ es residuo para G si ningún monomio de g pertenece a $\langle tp(G - \{p\})\rangle$. Nuestro 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 también reducido para cualquier otra base de Gröbner minimal de I que contenga a g y tenga el mismo conjunto de términos principales. Esto se cumple porque la definición de reducido involucra solamente a los términos principales.

Ahora dado $g \in G$, sea $g' = \bar{g}^{G-\{g\}}$ y hagamos $G' = (G - \{g\} \cup \{g'\}$. Afirmamos que G' es una base de Gröbner minimal para I. En efecto, primero observemos que $tp(g') = tp(g)$ porque cuando dividimos g por $G - \{g\}, tp(g)$ pasa al residuo puesto que no es divisible por algún elemento de $tp(G - \{g\})$. Esto prueba que $\langle tp(G')\rangle = \langle tp(G)\rangle$. Como G' está contenida en I, G' es una base de Gröbner, cumpliéndose la minimalidad. Finalmente, observemos que g' es reducido para G' por construcción.

Tomemos ahora los elementos de G y apliquemos el proceso anterior hasta que todos sean reducidos. La base de Gröbner puede cambiar cada vez que repitamos el proceso, pero por nuestra observación anterior, si un elemento es reducido continúa siéndolo porque el término principal no cambia, obteniéndose al final una base de Gröbner reducida.

Finalmente, para probar la unicidad, supongamos que $G\ y\ \tilde{G}$ son bases de Gröbner reducidas de I. En particular $G\ y\ \tilde{G}$ son bases de Gröbner reducida minimales, se probará que estos tienen los mismos términos principales, i.e.,

$$tp(G) = tp(\tilde{G}).$$

Luego, dado $g \in G$, existe $\tilde{g} \in \tilde{G}$ talque $tp(g) = tp(\tilde{g})$. si podemos probar que $g' = \tilde{g}$, se deducirá que $G = \tilde{G}$, y la unicidad estará probada.

Para demostrar que $g = \tilde{g}$. Consideremos $g - \tilde{g}$. Este pertenece a I, y como G es una base de Gröbner, se cumple que $\overline{g - \tilde{g}}^{G} = 0$. Pero también sabemos que $tp(g) = tp(\tilde{g})$. Por tanto, estos términos se cancelan en $g - \tilde{g}$, y los términos restantes no son divisibles por ningún elemento de $tp(G) = tp(\tilde{G})$ porque $G\ y\ \tilde{G}$ son reducidas. Esto prueba que $\overline{g - \tilde{g}}^{G} = g - \tilde{g}$, y entonces, se deduce que $g - \tilde{g} = 0$. Esto completa la prueba. ■

Teorema 63.* (*Teorema de la Base de Hilbert)

Todo ideal $I \subset K[x_1, \dots, x_n]$ tiene un conjunto generador finito.

Es decir

$$I = \langle g_1, \dots, g_t \rangle, \text{ para algunos } g_1, \dots, g_t \in I.$$

Demostración:

Si $I = \{0\}$, el conjunto de generadores será $\{0\}$, el cual es ciertamente finito. Si I contiene algún polinomio no nulo, entonces se puede construir un conjunto generador $g_1, \dots, g_t\ para\ I$ de la siguiente manera: por la proposición 45, existe $g_1, \dots, g_t \in I$ tal que $\langle tp(I) \rangle = \langle tp(g_1), \dots, tp(g_t) \rangle$. Afirmamos que $I = \langle g_1, \dots, g_t \rangle$.

Es evidente que $\langle g_1, \dots, g_t \rangle \subset I$ porque cada $g_i \in I$. Para la otra inclusión, sea $f \in I$ un polinomio arbitrario. Si aplicamos el algoritmo de la división para dividir f por $\{g_1, \dots, g_t\}$, entonces obtenemos una expresión de la forma.

$$f = a_1 g_1 + \cdots + a_s g_t + r$$

Donde ningún término de r es divisible por alguno de los $tp(g_1), \dots, tp(g_t)$. Afirmamos que $r = 0$. Para ver esto observemos que

$$r = -a_1 g_1 - \cdots - a_t g_t \in I$$

Si $r \neq 0$, entonces $tp(r) \in \langle tp(I) \rangle = \langle tp(g_1), \dots, tp(g_t) \rangle$, y por el lema 18 $tp(r)$ debe ser divisible por algún $tp(g_i)$. Esto contradice al hecho de que r es residuo y por lo tanto, r debe ser cero. Así,

$$f = a_1 g_1 + \cdots + a_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle.$$

Lo cual deja de manifiesto que $I \subset \langle g_1, \ldots, g_t \rangle$ completándose así la demostración. ■

9.4.2 Sistemas de Ecuaciones Polinomiales y Variedades

Las soluciones de un sistema de ecuaciones polinomiales con n incógnitas se pueden estudiar como el conjunto de puntos del espacio afín $n - dimencional$ cuyas coordenadas satisfacen el sistema. Los conjuntos de soluciones se corresponden con ideales del anillo de polinomios en n variables, y muchas de sus propiedades geométricas se traducen en propiedades algebraicas de dichos ideales y viceversa. Esta correspondencia se conoce comúnmente como diccionario álgebra − geometría.

Dados los polinomios $f_1, \ldots, f_s$ en el anillo de polinomios $P = K[x_1, \ldots, x_n]$ sobre un campo $K, e\ I = \langle f_1, \ldots, f_s \rangle$, si, donde además $\overline{K}$ es la cerradura algebraica de K y $\overline{P} = \overline{K}[x_1, \ldots, x_n]$, podemos estudiar el siguiente sistema de ecuaciones polinomiales que denotaremos por S.

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

Definición 64. (Variedades afín) sea K un campo y sean $f_1, \ldots, f_s$ polinomios en $K[x_1, \ldots, x_n]$. Entonces

$$V = V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_s) = 0, 1 \leq i \leq s\}$$

Designamos a $V(f_1, \ldots, f_s)$ como la variedad afín V definida por $f_1, \ldots, f_s \ldots$

***Lema 65.* (*Ideal de una variedad*)** sea $V \subset k^n$ una variedad afín. Establezcamos que

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

Si $V \subset k^n$ es una variedad afín, entonces $I(V) \subset K[x_1, \ldots, x_n]$ es un ideal, llamado el ideal de V.

Definición 66. (Variedad de un Ideal) Sea $I \subset K[x_1, \dots, x_n]$ un ideal. Denotaremos por $V(I)$ al conjunto

$$V(I) = \{(a_1, \dots, a_n) \in K^n : f(a_1, \dots, a_n) = 0 \; \forall \; f \in I\}.$$

Aun cuando un ideal no nulo I siempre contenga un número infinito de polinomios diferentes, el conjunto $V(I)$ puede ser definido por un conjunto finito de ecuaciones polinomiales.

Proposición 67. Sean V y W variedades afines en K^n. Entonces

1. $V \subset W$ Si y sólo si $I(V) \supset I(W)$.
2. $V = W$ Si y sólo si $I(V) = I(W)$.

Propiedad 68. Sean K un campo algebraicamente cerrado, $V, W \subset K^n$ variedades, y sean $I, J \subset K[x_1, \dots, x_n]$ ideales. Entonces en la correspondencia Ideal $-$Variedad se cumple:

1. $V(I + J) = V(I) + V(J)$
2. $V(I \cdot J) = V(I) \cup V(J)$
3. $V(I \cup J) = V(I) \cap V(J)$
4. $V(I \cap J) = V(I) \cup V(J)$
5. $I(V \cup W) = I(V) \cap I(W)$
6. $I(V \cap W) = \sqrt{I(V) + I(W)}$

9.4.3 Método de Solución

La eliminación de variables para resolver sistemas de ecuaciones ha sido uno de los artificios más utilizados.

Antes de introducirnos al objetivo principal de nuestro trabajo, presentaremos un método para resolver sistemas de ecuaciones lineales (Eliminación Gaussiana). Del cual no nos permite resolver sistemas de ecuaciones polinomiales.

En este capítulo se logra el objetivo principal de nuestro trabajo, a saber, resolver sistemas de ecuaciones polinomiales. Hasta aquí ya conocemos todo lo necesario para introducir el método que vamos a usar para darle solución a nuestro problema. Estudiáremos el método sistemático para eliminar variable de sistemas de ecuaciones polinomiales. La estrategia básica de la teoría de eliminación será dada en dos teoremas fundamentales: el teorema de la eliminación y el teorema de extensión. Probaremos estos resultados usando base de Gröbner.

9.4.3.1 Teorema de Eliminación y Extensión

Definición 69.

Dado $I = \langle f_1, \dots, f_s \rangle \subset K[x_1, \dots . x_n]$ $el\ l-ésima\ I_l$ **ideal de eliminación** I_l es el ideal de $K[x_{l+1}, \dots, x_n]$ definido por

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

Por lo tanto, I_l consiste en todas las consecuencias de $f_1 = \cdots = f_s = 0$ que eliminan las variables $x_1, \dots, x_l$ es fácil verificar que I_l es un ideal de $K[x_{l+1}, \dots, x_n]$. Sea $I = K[x_1, \dots, x_n]$ un ideal $0 \in I$ y lo podemos expresar como

$$0 = 0x_{l+1} + 0x_{l+2} + \cdots + 0x_n \in K[x_{l+1}, \dots, x_n,]$$

Y por tanto, $0 \epsilon I_l$ si $f, g \epsilon I_l \subset I$, entonces $f + g \epsilon I$, como $f\ y\ g$ pertenecen a I_l ellos solo involucran las variables $x_{l+1}, \dots, x_n$ y así $f + g$ involucra las mismas variables, es decir, $f + g \in K[x_{l+1}, \dots, x_n]$. Por tanto, $f + g \in I_l$. Argumentos similares muestran que para $f \in K[x_{l+1}, \dots, x_n]\ y\ g \in I_l, fg \in I_l$.

Observemos que $I = I_0$ es el $O - ésimo$ ideal de eliminación, y que diferentes órdenes de las variables producen ideales de eliminación diferentes.

Usando este lenguaje, vemos que la eliminación de $x_1, \dots, x_l$ significa encontrar polinomios no nulos en el $l - ésimo$ ideal de eliminación I_l. En suma, una solución del paso de eliminación significa dar un procedimiento sistemático para encontrar elementos de I_l. Con un orden monomial apropiado, de las bases de Gröbner nos permiten hacer esto instantáneamente.

Teorema 70. (Teorema de la eliminación)

Sean $I \in K[x_{l+1}, \dots, x_n]$ un ideal y G de Gröbner de I respecto al orden lex donde $x_1 > x_2 > \cdots > x_n$. Entonces para cada $0 \leq l \leq n$, en el conjunto

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

Es una base de Gröbner del $l - ésimo$ ideal de eliminación I_l.

Demostración.

Fijemos l entre 0 y n como $G_l \subset I_l$ por construcción basta probar que $\langle \text{tp}(I_l) \rangle \subset \langle tp(G_l) \rangle$, debemos verificar únicamente que para un $f \epsilon I_l$ arbitrario. El término principal $tp(f)$ es divisible por $tp(g)\ para\ algún\ g \in G_l$. Para probar esto, que $f \in I_l$, lo cual significa que $tp(f)$ es divisible por $tp(g)$, para algún $g \epsilon G$ dado que g es una base de Gröbner de I. Como $f \in I_l$, esto significa que $tp(g)$ incluye solamente las variables $x_{l+1}, \dots, x_n$. Ahora viene la observación crucial al usar el orden $Lex\ con\ x_1 > x_2 > \cdots > x_n$, de modo que $tp(g) \in K[x_{l+1}, \dots, x_n]$ implica que $tp(g) \in K[x_{l+1}, \dots, x_n]$ implica que $g \in K[x_{l+1}, \dots, x_n]$, probandose que $g \in G_l$, y el teorema queda demostrado. ■

Observación 71. El Teorema de Eliminación muestra que una base de Gröbner con el orden Lex elimina no solo la primera variable, sino las dos primeras variables, las tres primeras variables, y así sucesivamente. En algunos casos deseamos eliminar solamente algunas variables, sin importarnos las otras. En dicha situación, es bastante complicado calcular bases de Gröbner utilizando el orden Lex siendo cierto porque pueden obtener bases de Gröbner desagradables.

Teorema 72. (Teorema de extensión)

Sea $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{C}[x_1, \dots, x_n]$ y sea I_1 el primer ideal de eliminación de I. para cada $1 \leq i \leq s$, escribamos f_i en la forma

$$f_1 = g_i\,(x_2, \dots, x_n)x_1^{N_i} + \text{Términos en } x_1 \text{ con grado} < N_i,$$

Donde $N_i \geq 0\ y\ g_i \in \mathbb{C}[x_2, \dots, x_n]$ es no nulo. Supongamos que tenemos una solución parcial $(a_2, \dots, a_n) \in V(I_1)$. Si $(a_2, \dots, a_n) \notin V(g_1, \dots, g_s)$,. Entonces existe un $a_1 \in \mathbb{C}$ tal que $(a_1, a_2, \dots, a_n) \in V(I)$.

9.4.3.2 Análisis del Método de Eliminación Gaussiana y Teoría de Eliminación

Para concluir este capítulo señalaremos brevemente algunas de las conexiones entre el método de Eliminación Gaussiana y teoría de eliminación (teorema de eliminación y teorema de extensión) de un sistema de ecuación lineal. El hecho aquí es que el método de Gauss transforma la matriz de coeficientes en una matriz triangular superior. El método continúa el proceso de transformación hasta obtener una matriz diagonal de la cual obtenemos los valores correspondientes para cada una de las variables. Lo que en si el método de Eliminación Gaussiana realiza es la eliminación por reglones para cada una de las variables.

Teoría de eliminación nos permite trabajar sobre un sistema de ecuación lineal, trasladando estos cálculos al álgebra. Tomando a cada una de las ecuaciones del sistema lineal como ideal. Para encontrar una base de Gröbner para el ideal, luego a dicha base de Gröbner encontramos los ideales de eliminación obteniendo así el último ideal de eliminación generado por un solo polinomio en una variable que resultaría ser factorizable. Si este polinomio no es factorizable se utilizan métodos de aproximación numérica (Newton-Raphson, Runge-Kutta, Horner, etc.). Por medio del teorema de extensión obtenemos cada uno de los valores correspondientes de las variables.

Cabe recalcar que el método de Eliminación Gaussiana resuelve únicamente sistemas de ecuaciones lineales no nos permite resolver sistemas de ecuaciones polinomiales, sin embargo, la teoría de eliminación (teorema de eliminación y teorema de extensión) nos da solución no únicamente a un sistema de ecuaciones lineal sino también a sistema de ecuaciones polinomiales lo cual es el objetivo de nuestro trabajo.

Ejemplo 73. Vamos a resolver el siguiente sistema de ecuaciones por el método de **Eliminación Gaussiana**, es decir, obteniendo una forma escalonada reducida de dicho sistema

$$w - 2x + 2y - 3z = 15$$
$$3w + 4x - y + z = -6$$
$$2w - 3x + 2y - z = 17$$
$$w + x - 3y - 2z = -7$$

Para ello, trabajamos directamente sobre la matriz ampliada asociada al sistema, teniendo presente en todo momento que es lo que representan los coeficientes de dicha matriz:

$$\left(\begin{array}{cccc|c} 1 & -2 & 2 & -3 & 15 \\ 3 & 4 & -1 & 1 & -6 \\ 2 & -3 & 2 & -1 & 17 \\ 1 & 1 & -3 & -2 & -7 \end{array}\right) \begin{array}{c} R_2 = 3R_1 + R_2 \\ R_3 = -2R_1 + R_3 \\ R_4 = -R_1 + R_4 \end{array} \rightarrow \left(\begin{array}{cccc|c} 1 & -2 & 2 & -3 & 15 \\ 0 & 10 & -7 & 10 & -51 \\ 0 & 1 & -2 & 5 & -13 \\ 0 & 3 & -5 & 1 & -22 \end{array}\right)$$

$$\begin{array}{c} R_2 = -10R_3 + R_2 \\ R_4 = -3R_3 + R_4 \end{array} \rightarrow \left(\begin{array}{cccc|c} 1 & -2 & 2 & -3 & 15 \\ 0 & 10 & -7 & 10 & -51 \\ 0 & 0 & 13 & -40 & 79 \\ 0 & 0 & 1 & -14 & 17 \end{array}\right) R_3 = -13R_4 + R_3 \rightarrow$$

$$\left(\begin{array}{cccc|c} 1 & -2 & 2 & -3 & 15 \\ 0 & 10 & -7 & -10 & -51 \\ 0 & 0 & 13 & -40 & 79 \\ 0 & 0 & 0 & -142 & 142 \end{array}\right) R_4 = R_4/142 \rightarrow \left(\begin{array}{cccc|c} 1 & -2 & 2 & -3 & 15 \\ 0 & 10 & -7 & 10 & -51 \\ 0 & 0 & 13 & 40 & 79 \\ 0 & 0 & 0 & 1 & -1 \end{array}\right)$$

$$\begin{array}{c} R_2 = -10R_4 + R_2 \\ R_3 = 40R_4 + R_3 \end{array} \rightarrow \left(\begin{array}{cccc|c} 1 & -2 & 2 & -3 & 15 \\ 0 & 10 & -7 & 0 & -41 \\ 0 & 0 & 13 & 0 & 39 \\ 0 & 0 & 0 & 1 & -1 \end{array}\right) R_3 = R_3/13 \rightarrow$$

$$\left(\begin{array}{cccc|c} 1 & -2 & 2 & -3 & 15 \\ 0 & 10 & -7 & 0 & -41 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & -1 \end{array}\right) \begin{array}{c} R_1 = -2R_3 + R_1 \\ R_2 = 7R_3 + R_2 \end{array} \rightarrow \left(\begin{array}{cccc|c} 1 & -2 & 0 & 0 & 6 \\ 0 & 10 & 0 & 0 & -20 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & -1 \end{array}\right)$$

$$R_2 = R_2/10 \rightarrow \left(\begin{array}{cccc|c} 1 & -2 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & -1 \end{array}\right) R_1 = 2R_2 + R_1 \rightarrow \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & -1 \end{array}\right)$$

La última matriz ampliada representa el sistema en forma escalonada reducida. El sistema es, por tanto. Compatible queda determinada su solución.

Ejemplo 74. Vamos a resolver el siguiente sistema de ecuaciones del ejemplo 73 por medio de software CoCoA aplicando teoría de eliminación.

$$w - 2x + 2y - 3z = 15$$
$$3w + 4x - y + z = -6$$
$$2w - 3x + 2y - z = 17$$
$$w + x - 3y - 2z = -7$$

Inicialmente encontramos la base de Gröbner

```
------------------------------
Use R ::= QQ[w,x,y,z],Lex;
  I := Ideal(w-2x+2y-3z-15,3w+4x-y+z+6,2w-3x+2y-z-17,w+x-3y-2z+7);
  Print "A continuación se describe el ideal:";
  Describe I;
  Print "La base de Gröbner es:";
  GBasis(I);

A continuación se describe el ideal:
------------------------------
Record[Type := IDEAL, Value := Record[Gens := [w - 2x + 2y - 3z - 15, 3w + 4x -
y + z + 6, 2w - 3x + 2y - z - 17, w + x - 3y - 2z + 7]]]
------------------------------
La base de Gröbner es:
------------------------------
[w - 2x + 2y - 3z - 15, 5/2x - 4y - 3/2z + 31/2, -16/5y - 38/15z + 106/15, 71/24z +
71/24]
------------------------------
```

Una vez obtenida la base de Gröbner encontramos el ideal de eliminación respecto a x.

```
-------------------------------
Use R ::=  QQ[w,x,y,z],Lex;
Set Indentation;
Print "El resultado del primer ideal de eliminación respecto a x es:";
Elim(x,Ideal(w-2x+2y-3z-15,5/2x-4y-3/2z+31/2,-16/5y-38/15z+106/15,
71/24z + 71/24));

El resultado del primer ideal de eliminación respecto a x es:
-------------------------------
Ideal(71/24z + 71/24, -16/5y - 38/15z + 106/15,1/2w - 1)
-------------------------------
```

Luego encontramos el ideal de eliminación respecto a y.

```
-------------------------------
Use R ::=  QQ[w,x,y,z],Lex;
Set Indentation;
Print "El resultado del segundo ideal de eliminación respecto a y es:";
Elim(y,Ideal(71/24z+71/24, -16/5y - 38/15z + 106/15, 1/2w- 1));

El resultado del segundo ideal de eliminación respecto a y es:
-------------------------------
Ideal(1/2w-1, 71/24z + 71/24)
-------------------------------
```

Luego encontramos el ideal de eliminación respecto a z.

```
------------------------------
Use R ::=  QQ[w,x,y,z],Lex;
Set Indentation;
Print "El resultado del tercer ideal de eliminación respecto a z es:";
Elim(z,Ideal(71/24z + 71/24,1/2w - 1));

El resultado del tercer ideal de eliminación respecto a z es:
------------------------------
Ideal(1/2w - 1)
------------------------------
```

Entonces tenemos que:

$$I_1 = I \cap \mathbb{Q}[y,z] = \langle 71/24\mathrm{z} + 71/24, -16/5\mathrm{y} - 38/15\mathrm{z} + 106/15, 1/2\mathrm{w} - 1\rangle$$

$$I_2 = I \cap \mathbb{Q}[z] = \langle 1/2\mathrm{w} - 1, 71/24\mathrm{z} + 71/24\rangle$$

$$I_3 = I \cap \mathbb{Q}[z] = \langle 1/2\mathrm{w} - 1\rangle$$

Entonces procedemos a encontrar los valores de w, x, y, z.

Encontráremos primeramente el valor de w en la ecuación asociada en el polinomio del tercer ideal de eliminación.

$$\frac{1}{2}w - 1 = 0$$

$$w = 2$$

Luego encontráremos el valor de z en la segunda ecuación asociada al segundo polinomio en el segundo ideal de eliminación obtenemos.

$$71/24\mathrm{z} + 71/24 = 0$$

$$z = -1$$

Sustituyendo el valor z en la segunda ecuación asociada al primer polinomio del ideal de eliminación obtenemos.

$$-16/5\mathrm{y} - 38/15\mathrm{z} + 106/15 = 0$$

$$y = -3$$

Finalmente, sustituyendo el valor de w, y, z en el primer polinomio de nuestra base de Gröbner obtenemos.

$$\mathrm{w} - 2\mathrm{x} + 2\mathrm{y} - 3\mathrm{z} - 15 = 0$$

$$x = -2$$

Como podemos observar la teoría de eliminación nos permite resolver sistemas de ecuaciones lineales ahora mostraremos como la teoría de eliminación es capaz de resolver sistemas de ecuaciones polinomiales más complejos.

Ejemplo 75.

Consideremos los tres polinomios

$$f_1 = x^2 + y^2 + z^2 - 4$$
$$f_2 = x^2 + 2y^2 - 5$$
$$f_3 = xz - 1$$

f_1, f_2, f_3 en $P = \mathbb{Q}[x, y, z]$ que definen el sistema de ecuaciones polinomiales $f_1 = f_2 = f_3 = 0$ y generan el ideal

$$I = \langle f_1, f_2, f_3 \rangle \text{ en } P.$$

Encontremos a continuación las soluciones de

$$\begin{cases} x^2 + y^2 + z^2 = 4 \\ x^2 + 2y^2 = 5 \\ xz = 1 \end{cases}$$

Primero, calculemos una base de Gröbner de I con respecto al orden Lex, usando el CoCoA:

```
------------------------------
Use R ::= QQ[x,y,z],Lex;
  I := Ideal(x^2+y^2+z^2-4, x^2+2y^2-5, xz-1);
  Print "A continuación se describe el ideal:";
  Describe I;
  Print "La base de Gröbner es:";
  GBasis(I);

A continuación se describe el ideal:
------------------------------
Record[Type := IDEAL, Value := Record[
   Gens := [x^2+y^2+z^2-4, x^2+2y^2- 5, xz - 1]]]
------------------------------
La base de Gröbner es:
------------------------------
[y^2- z^2-1, -x- 2z^3+3z, -2z^4+3z^2-1]
------------------------------
```

La base Gröbner está dada por los polinomios.

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

$$g_2 = -x - 2z^3 + 3z$$

$$g_3 = -2z^4 + 3z^2 - 1.$$

Usando siempre el CoCoA, encontramos los ideales de eliminación:

Ideal de eliminación de x

```
------------------------------
Use R ::=  QQ[w,x,y,z],Lex;
Set Indentation;
Print "El resultado del primer ideal de
eliminación respecto a x es:";
Elim(x,Ideal(y^2-z^2-1, -x-2z^3+3z, -
2z^4+3z^2-1));

El resultado del primer ideal de eliminación
respecto a x es:
------------------------------
Ideal(y^2-z^2-1, -2z^4+3z^2-1)
------------------------------
```

Ideal de eliminación de y

```
------------------------------
Use R ::=  QQ[w,x,y,z],Lex;
Set Indentation;
Print "El resultado del segundo ideal de eliminación respecto a y es:";
Elim(y,Ideal(y^2-z^2-1, -2z^4+3z^2-1));

El resultado del segundo ideal de eliminación respecto a y es:
------------------------------
Ideal(-2z^4+3z^2-1)
------------------------------
```

Entonces tenemos que:

$$\begin{aligned} I_1 &= I \cap \mathbb{Q}[y,z] \\ &= \langle y^2 - z^2 - 1, -2z^4 + 3z^2 - 1 \rangle \\ I_2 &= I \cap \mathbb{Q}[z] \\ &= \langle -2z^4 + 3z^2 - 1 \rangle. \end{aligned}$$

Por el método de factorización por evaluación, conocido desde la secundaria, obtenemos que

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

Consecuentemente la variedad de I_2 es:

$$V(I_2) = \left\{1, -1, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right\}$$

Utilicemos ahora el Teorema de extensión. Sustituyendo los valores de z en la ecuación asociada al primer polinomio en la primera ideal eliminación, encontramos la variedad de I_1 :

$$V(I_1) = \left\{(\pm\sqrt{2}, 1), (\pm\sqrt{2}, -1), \left(\pm\frac{\sqrt{6}}{2}, \frac{1}{\sqrt{2}}\right), \left(\pm\frac{\sqrt{6}}{2}, -\frac{1}{\sqrt{2}}\right)\right\}$$

Finalmente, la tercera ecuación de nuestro sistema original nos da los correspondientes valores de "x", los cuales son recíprocos de los valores de z. De esta manera obtenemos que la variedad de I, y por tanto la solución de nuestro sistema, es:

$$V(I) = \left\{(1, \pm\sqrt{2}, 1), (-1, \pm\sqrt{2}, -1), \left(\sqrt{2}, \pm\frac{\sqrt{6}}{2}, \frac{1}{\sqrt{2}}\right), \left(-\sqrt{2}, \pm\frac{\sqrt{6}}{2}, -\frac{1}{\sqrt{2}}\right)\right\}$$

9.5 Solución de un Problema Aplicado

En nuestra vida cotidiana estamos acostumbrados a utilizar toda clase de dispositivos electrónicos que fundamentalmente tienen la complicada misión de solucionarnos o simplificarnos una gran cantidad de dificultades o problemas que tenemos, convirtiéndose entonces en una herramienta de trabajo más y en muchas ocasiones hasta nos permite reducir el tiempo de trabajo o bien incrementar notoriamente la productividad y rendimiento.

En la década de 1800, Augustin-Louis Cauchy, un pionero en el análisis matemático, estudió la rigidez de un "octaedro articulado", que es el antepasado del hexápodo. En 1949, VE avances Gough en la investigación y construido un mecanismo paralelo para probar neumáticos de bajo varias cargas. Unos años más tarde, en 1965, D. Stewart comienza a utilizar una variante del hexápodo para simuladores de vuelo. El robot que construyó en su nombre pasará a llamarse la "plataforma Stewart". Como es de los años, el hexápodo fue actualizado por varios ingenieros (K. Cappel, McCallion, etc.).

Un hexápodo es un dispositivo de base mecatrónico fija (Stewart-Gough plataforma) o cuya locomoción se basa en tres pares de patas móviles. El estudio de los insectos a pie es de particular interés para presentar una alternativa a las ruedas de uso de robots de locomoción. Así, el término se refiere a los robots de inspiración biológica imitando en este caso los animales hexápodos tales como insectos. Robots hexápodos se consideran más estables que los robots bípedos que en la mayoría de los casos, el hexápodo son estáticamente estables. Por lo tanto, no dependen de controladores en tiempo real para estar de pie o caminar. Sin embargo, se ha demostrado que las grandes velocidades de desplazamiento, los insectos son dependientes de factores dinámicos.

Plataformas o hexápodo Stewart estructuras han sido utilizado durante mucho tiempo en los simuladores de vuelo para proporcionar rápido movimiento multi-eje. Sistemas similares aussi apareció recientemente en parques temáticos para simular montañas rusas, coches de carreras, las arrugas de dinosaurios etc.

A mediados de la década de 1990 tiene totalmente nueva aplicación lleva del campo de la medicina. El Instituto Fraunhofer de Ingeniería de Producción y Automatización (IPA), IP acercó con la idea de un robot quirúrgico. La M-850 versatilidad de movimiento, viene muy cerca de igualar la manera que un cirujano mueve su mano. La diferencia es la del que hexápodo puede ser programada para suprimir las fluctuaciones y los viajes pueden ser limitadas a los rangos de seguridad predefinidas. Proporcionar mayor rigidez, capacidad de carga y la precisión en un paquete más pequeño que los posicionadores de varios ejes convencionales "apilados", el principio hexápodo permite precisión sub-micras incluso bajo cargas elevadas.

La M-850 Hexápodo es el primer sistema de micro posicionamiento disponible en el mercado proporcionando buenos seis grados de libertad con 1 micra resolución que permite al usuario definir el punto de giro en cualquier lugar dentro o fuera del sistema. Rotación sobre ese punto de giro se puede especificar (con la resolución microradián) para cualquier eje de rotación. Tarea de posicionamiento de alta precisión compleja donde se requiere movimiento independiente en seis grados de libertad.

El Software également Permite una fácil programación de las secuencias de movimiento.

9.5.1 Estabilidad del Robot M-850

La resolución del sistema de ecuación polinomial nos permite la estabilidad del Robot M-850. Este es un robot que se utiliza en medicina específicamente en el área de cirugías, es decir, que se mueve con la mano del cirujano.

$$9x^2 + 44xy - 53y^2 - 84x + 22y = -75$$

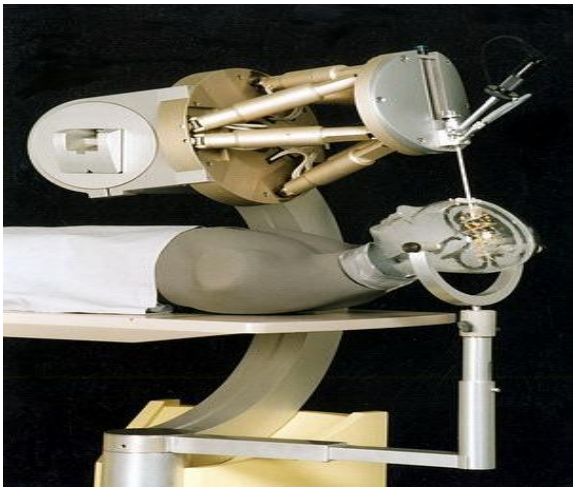
$$y^3 + xy = -1$$

$$xy^2 - 5xy + 5y^2 + 9x - 3y = 8$$

Consideremos el Ideal:

$$I = \langle 9x^2 + 44xy - 53y^2 - 84x + 22y + 75, y^3 + xy + 1, xy^2 - 5xy + 5y^2 + 9x - 3y - 8 \rangle$$

No es fácil encontrar a mano las soluciones de este sistema. Utilizaremos el software CoCoA (4.7.5). Para encontrar una base de Gröbner, luego encontráremos nuestro ideal de eliminación I_1. Con la ayuda del teorema de extensión encontramos la variedad de I.



Robots M-850.

Encontrando la Base de Gröbner para el ideal I.

```
------------------------------
Use R ::= QQ[x,y],Lex;
 I := Ideal(9x^2+44xy-53y^2-84x+22y+75,y^3+xy+1,xy^2-5xy+5y^2+9x-3y-8);
 Print "A continuación se describe el ideal:";
 Describe I;
 Print "La base de Gröbner es:";
 GBasis(I);

A continuación se describe el ideal:
------------------------------
Record[Type := IDEAL,Value := Record[Gens := [9x^2+44xy-84x-53y^2+
22y+75, xy+y^3+1, xy^2-5xy+9x+5y^2-3y- 8]]]
------------------------------
La base de Gröbner es:
------------------------------
[-9x+y^4-5y^3-5y^2+4y+3, 1/9y^5-5/9y^4+4/9y^3+4/9y^2+1/3y+1]
------------------------------
```

Encontrando el ideal de eliminación I_1.

```
------------------------------
Use R ::=  QQ[w,x,y,z],Lex;
Set Indentation;
Print "El resultado del primer ideal de eliminación respecto a x es:";
Elim(x,Ideal(-9x+y^4-5y^3-5y^2+4y+3, 1/9y^5-5/9y^4+4/9y^3+4/9y^2+1/3y+1));

El resultado del primer ideal de eliminación respecto a x es:
------------------------------
Ideal(y^5 - 5y^4 + 4y^3 + 4y^2 + 3y + 9)
------------------------------
```

Entonces tenemos que:

$$I_1 = I \cap \mathbb{Q}[y] = \langle y\text{^}5 - 5y\text{^}4 + 4y\text{^}3 + 4y\text{^}2 + 3y + 9 \rangle$$

Entonces procedemos a encontrar los valores de x, y

Encontráremos primeramente el valor de y en la ecuación asociada en el polinomio del ideal de eliminación.

$$y\text{^}5 - 5y\text{^}4 + 4y\text{^}3 + 4y\text{^}2 + 3y + 9 = 0$$

Por el método de factorización por evaluación obtenemos que:

$$(y+1)(y-3)^2(y^2+1)$$

$$y = (-1,3,\pm i)$$

Utilizando el CoCoA para factorizar I_1.

```
--------------------------------
Use R ::= QQ[x,y,z],Lex;
  F := y^5 - 5y^4 + 4y^3 + 4y^2 + 3y + 9;
    Print "La factorización de f es:";
  Factor(F);

La factorización de f es:
--------------------------------
[[y + 1,1], [y^2 + 1,1], [y - 3,2]]
--------------------------------
```

Utilizando el teorema de extensión. Sustituyendo el valor de y en la ecuación asociada al primer polinomio del ideal de la base de Gröbner obtenemos el valor de x.

$$x = \left(0, \frac{28}{3}, 1 \pm i\right)$$

Como podemos observar los puntos de estabilidad del Robot M-850 son:

$$x = \left(0, \frac{28}{3}, 1 \pm i\right)$$

$$y = (-1{,}3, \pm i)$$

Nota 76. Esquema del robot M-850 en anexo 12.4 página 100.

9.5.2 Otras aplicaciones de las base de Gröbner

Las bases de Gröbner han sido estudiadas intensamente en los últimos años, sin embargo, es desde fechas relativamente recientes que su aplicación ha experimentado un auge, sin duda motivado por la aparición de máquinas con capacidad de cálculo suficiente.

Existen aplicaciones interesantes en varias ramas de las matemáticas tales como el álgebra conmutativa, el álgebra homológica, el álgebra diferencial, la geometría algebraica, la teoría de grafos, entre otras. Además, las bases de Gröbner han sido usadas en ciencias aplicadas tales como estadística, robótica y teoría del control.

Nota 77. Más aplicaciones de las bases de Gröbner en anexo 12.3 página 99.

10 Conclusiones

10.1 En relación a los objetivos de la investigación

Resolver sistemas de ecuaciones polinomiales ha sido una de las tareas más comunes en matemática y a la vez una de las más difíciles. Por ello, desde la antigüedad se han buscado técnicas para resolverlos de forma eficaz y menos compleja, lo que ha conducido a la invención de una serie de métodos para solucionar estos sistemas que traen consigo una cantidad sorprendente de resultados provenientes de muchas disciplinas matemáticas. En nuestro trabajo lo primero que se aborda es una temática muy general sobre el conocimiento de las estructuras más importantes para el desarrollo de nuestro tema (anillo polinomial, ideal polinomial, etc.).

Ha quedado patente que el método de bases de Gröbner para reducir la complejidad de un sistema de ecuaciones es útil en casos en los que los sistemas están compuestos por polinomios en varias variables teniendo, a priori, una solución engorrosa de calcular mediante los métodos tradicionales.

10.2 En relación a la metodología aplicada

No se ha de olvidar que el cálculo de las bases de Gröbner con el algoritmo de Buchberger es relativamente tedioso pero, gracias al uso de los computadores, esta tarea puede llevarse a cabo con relativa facilidad.

En el caso de la eliminación podemos concluir que este método, aplicado a un sistema de ecuaciones lineales, coincide con el de Eliminación Gaussiana, conocido por nosotros desde la secundaria, es decir, que Eliminación Gaussiana es un caso particular de la teoría de eliminación que aquí exponemos.

10.3 Perspectivas de futuro (Recomendaciones)

- A los profesores del departamento, se les insta fomentar en los estudiantes de matemática la investigación en este tema de la Geometría Algebraica. También, se aconseja que se tome en cuenta, en este contexto de transformación curricular, este tema para su incorporación en clases como Estructuras Algebraicas.

- A los estudiantes de matemática, utilizar el presente documento como base para estudios futuros acerca del tema y profundizar un poco más sobre las aplicaciones de los sistemas de ecuaciones polinomiales en diversas áreas.

- Instar a los estudiantes del departamento de matemática y estadística hacer uso de estos nuevos métodos para resolución de sistemas de ecuaciones polinomiales por medio de bases de Gröbner.

- Experimentar más usos de software computacionales matemáticos (CoCoA, MAPLE, SINGULAR) para una mejor explotación de los cursos en el departamento de Matemática y Estadística.

11 Bibliografía

Adams, W. y Loustaunau, P. (1994). *An Introduction to Gröbner Bases 3.* American Mathematical Society.

Becker, T. y Weispfenning, V. (1993). *Gröbner bases: a computational approach to commutative álgebra*. New York: Springer-Verlag.

Bourbaki, N. (1974). *Elements Of Mathematics: Álgebra I*. Gran Bretaña: Hermann

Cox D., Little, J. y O`Shea, D. (2005). *Using Álgebraic Geometry*. New York: Springer-Verlag.

Cox, D., Little, J. y O`Shea, D. (2007). *Ideals, Varieties, and Algorithms: An Introduction to Computational Álgebraic Geometry and Commutative Álgebra*. New York: Springer-Verlag.

Kreuzer, M. y Robbiano, L. (2000). *Computational Commutative Álgebra 1*. Berlin Heidelberg: Springer-Verlag.

Kurosch, A. (1987). *Curso de Álgebra Superior*. Moscú: Editorial Mir.

O. Zariski, O. y Samuel, P. (1958). *Commutative Álgebra 1*. New York: Springer-Verlag.

Solotar, A., Farinati, M. y Suárez, M. (2007). *Anillos y sus categorías de representación.* Argentina.

12 Anexos

12.1 Más ejemplos de órdenes monomiales

Ordenando los términos de los polinomios.

Polinomio		Polinomio	
$F: 5xy^2z + 5z^2 - 6x^3 + 8x^2z^2 \epsilon Q[x,y,z]$		$G: x^2y + y + y^3 - x - 1 + xy^2 \epsilon Q[x,y,z]$	
Orden	Resultados	Orden	Resultados
Lex	$-6x^3 + 8x^2z^2 + 5xy^2z + 5z^2$	Lex	$x^2y + xy^2 - x + y^3 + y - 1$
$DegLex$	$8x^2z^2 + 5xy^2z - 6x^3z + 5z^2$	$DegLex$	$x^2y + xy^2 + y^3 - x + y - 1$
$DegvReLex$	$5xy^2z + 5x^2z^2 - 6x^3 + 5z^2$	$DegRevLex$	$x^2y + xy^2 + y^3 - x + y - 1$
$Lexin$	$8x^2z^2 + 5z^2 + 5xy^2z - 6x^3$	$Lexin$	$y^3 + xy^2 + x^2y + y - x - 1$

12.2 Detalles del ejemplo (59) con CoCoA

Aquí mostramos todos los $S-polinomios$ del ejemplo (59) realizados por el CoCoA.

$\boldsymbol{S-polinomio\ (f_1, f_2)}$	$\boldsymbol{S-polinomio\ (f_1, f_3)}$
------------------------------	------------------------------
Use R ::= QQ[x,y,z],Lex;	Use R ::= QQ[x,y,z],Lex;
F1:= x^2y^2-z;	F1:= x^2y^2-z;
F2:= xy^2z-xyz;	F3:= x^2yz-z^2;
TP1:=LT(F1);	TP1:=LT(F1);
TP2:=LT(F2);	TP2:=LT(F3);
M:=LCM(TP1, TP2);	M:=LCM(TP1, TP2);
SPOLY:=(M/TP1)*(F1)-	SPOLY:=(M/TP1)*(F1)-
(M/TP2)*(F2);	(M/TP2)*(F3);
Print "El S-polinomio es:";	Print "El S-polinomio es:";
SPOLY;	SPOLY;
El S-polinomio es:	El S-polinomio es:
------------------------------	------------------------------
x^2yz - z^2	yz^2 - z^2
------------------------------	------------------------------

$S-polinomio\ (f_1, f_4)$	$S-polinomio(f_2, f_3)$
----------	----------
Use R ::= QQ[x,y,z],Lex;	Use R ::= QQ[x,y,z],Lex;
F1:= x^2y^2-z;	F2:= xy^2z-xyz;
F4:= yz^2-z^2;	F3:= x^2yz-z^2;
TP1:=LT(F1);	TP1:=LT(F2);
TP2:=LT(F4);	TP2:=LT(F3);
M:=LCM(TP1, TP2);	M:=LCM(TP1, TP2);
SPOLY:=(M/TP1)*(F1)-(M/TP2)*(F4);	SPOLY:=(M/TP1)*(F2)-(M/TP2)*(F3);
Print "El S-polinomio es:"; SPOLY;	Print "El S-polinomio es:"; SPOLY;
El S-polinomio es:	El S-polinomio es:
----------	----------
x^2yz^2-z^3	-x^2yz+yz^2
----------	----------

$S-polinomio\ (f_2, f_4)$	$S-polinomio\ (f_3, f_4)$
----------	----------
Use R ::= QQ[x,y,z],Lex;	Use R ::= QQ[x,y,z],Lex;
F2:= xy^2z-xyz;	F3:= x^2yz-z^2;
F4:= yz^2-z^2;	F4:= yz^2-z^2;
TP1:=LT(F2);	TP1:=LT(F3);
TP2:=LT(F4);	TP2:=LT(F4);
M:=LCM(TP1, TP2);	M:=LCM(TP1, TP2);
SPOLY:=(M/TP1)*(F2)-(M/TP2)*(F4);	SPOLY:=(M/TP1)*(F3)-(M/TP2)*(F4);
Print "El S-polinomio es:"; SPOLY;	Print "El S-polinomio es:"; SPOLY;
El S-polinomio es:	El S-polinomio es:
----------	----------
0	x^2z^2-z^3
----------	----------

$S-polinomio\ (f_3, f_5)$	$S-polinomio\ (f_4, f_5)$
----------	----------
Use R ::= QQ[x,y,z],Lex;	Use R ::= QQ[x,y,z],Lex;
F3:= x^2yz-z^2;	F4:= yz^2-z^2;
F5:= x^2 z^2-z^3;	F5:= x^2z^2-z^3;
TP1:=LT(F3);	TP1:=LT(F4);
TP2:=LT(F5);	TP2:=LT(F5);
M:=LCM(TP1, TP2);	M:=LCM(TP1, TP2);
SPOLY:=(M/TP1)*(F3)-(M/TP2)*(F5);	SPOLY:=(M/TP1)*(F4)-(M/TP2)*(F5);
Print "El S-polinomio es:"; SPOLY;	Print "El S-polinomio es:"; SPOLY;
El S-polinomio es:	El S-polinomio es:
----------	----------
yz^3-z^3	-x^2z^2+yz^3
----------	----------

$S-polinomio\ (f_1, f_5)$	$S-polinomio\ (f_2, f_5)$
----------	----------
Use R ::= QQ[x,y,z],Lex;	Use R ::= QQ[x,y,z],Lex;
F1:= x^2y^2-z;	F2:= xy^2z-xyz;
F5:= x^2z^2-z^3;	F5:= x^2z^2-z^3;
TP1:=LT(F1);	TP1:=LT(F2);
TP2:=LT(F5);	TP2:=LT(F5);
M:=LCM(TP1, TP2);	M:=LCM(TP1, TP2);
SPOLY:=(M/TP1)*(F1)-(M/TP2)*(F5);	SPOLY:=(M/TP1)*(F2)-(M/TP2)*(F5);
Print "El S-polinomio es:"; SPOLY;	Print "El S-polinomio es:"; SPOLY;
El S-polinomio es:	El S-polinomio es:
----------	----------
y^2z^3-z^3	-x^2yz^2+y^2z^3
----------	----------

12.3 Otras aplicaciones de las bases de Gröbner

En la siguiente lista presentamos las mayores áreas en las que las bases de Gröbner han sido aplicadas con gran éxito.

Geometría Algebraica y teoría de los ideales Polinomiales	Álgebra conmutativa y no conmutativa
Tería de códigs	Combinatoria
Criptografía	Teoría de Invariantes
Programación Entera	Teoría de Grafos
Estadística	Integración simbólica
Ecuaciones diferenciales	Teoría de sistemas

Algunas aplicaciones prácticas de la teoría de las bases de Gröbner son:

Resolver sistemas de ecuaciones Polinomiales	Resolver el problema de la pertenencia a un ideal
Decidir si dos ideales son iguales	Demostración automática de teoremas
Operaciones con ideales	Cálculos con matrices de transferencia
Solución del problema de Cauchy	Cálculo de componentes irreducibles

12.4 Esquema del robot M-850