UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA
UNAN-MANAGUA
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 utilizando las Bases de Gröbner y el Método de Autovalores

Autores: **Bra. Katerin Diaskana Solórzano Rojas.**

Bra. Yahoska Rebeca Lanzas Arechavala.

Br. Yader Alexander Ramírez Bonilla.

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 utilizando las Bases de Gröbner y el Método de Autovalores.

2. Dedicatoria

A Dios, a mi abuela Esterlina,

a mi madre Guissel, a mis

Maestros y amigos.

Yader Alexander Ramírez

A Dios, a mis padres, a mi esposo

por darme su apoyo incondicional

en la formación de mi vida.

Katerin D. Solórzano

A Dios, a mi madre Priscila, a mi hijo Jarid,

a la memoria de mi padre Francisco Lanza,

a mis hermanos, mis sobrinos,

mis maestros y mis amigos

por todo su apoyo.

Yahoska R. Lanzas

3. Agradecimientos

Primordialmente agradecemos a Dios que día a día nos dio bendición en nuestros estudios y nos permitió culminar esta meta, a nuestras familias por todo el apoyo brindado en todos estos años, a nuestros docentes por compartir con nosotros sus conocimientos, nos forjaron y motivaron siempre con sus consejos, y a nuestros amigos y compañeros.

4. Valoración del docente

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

Esta investigación fue elaborada por los bachilleres Katerin Diaskana Solórzano Rojas, Yahoska Rebeca Lanzas Arechavala y Yader Alexander Ramírez Bonilla. 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 el Método de Autovalores 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 Solórzano, Lanzas y Ramírez 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 presente trabajo nos permite mostrar una introducción a otra parte de las ecuaciones polinomiales ya que daremos a conocer otro método más general a los tratados comúnmente que nos permitirá la solución de sistemas de ecuaciones polinomiales.

En el transcurso de nuestros estudios no percibimos muchos el desarrollo de este método de solución, esperamos que el presente trabajo de un aporte a que estudiantes de nuestra carrera enfaticen más sobre dicho estudio en el Álgebra Abstracta y la Geometría Algebraica.

Las herramientas a utilizar en nuestro trabajo son las Bases de Gröbner al ver las variedades de los sistemas de ecuaciones polinomiales, es un interesante método de solución en dichas ecuaciones.

Al presentar los ejemplos en nuestro trabajo utilizaremos el sistema computacional CoCoA para la comprobación de los ejercicios presentados. En los ejercicios propuestos hemos sido lo más claro, preciso y coherente para dar a entender los métodos utilizados y ayudar a ser más reflexivas las soluciones para los lectores y estudiantes de la carrera.

El método de Autovalores nos permite encontrar las soluciones de un sistema de ecuaciones polinomiales, es decir encontrar los puntos de la variedad de un Ideal generado por los polinomios.

6. Introducción del tema y subtema

En matemática el Álgebra es una base de nuestros conocimientos tanto como la aritmética, la geometría, los diversos tipos de funciones; al fusionar estas bases hemos encontrado nuevas cosas por aprender en nuestro universo matemático.

Este trabajo tiene como finalidad el explicar de manera sencilla los diversos tipos de órdenes Monomiales y el algoritmo de la división en ecuaciones multivariadas en $K\ x_1, \dots, x_n$.

Nuestro trabajo presenta las definiciones básicas de polinomios, anillos, monomios, campo; para estructurar y comprender fácilmente la lectura de nuestros ejemplos.

7. Justificación

La matemática juega un papel muy importante en nuestra vida, una rama de la matemática que se aplica es el álgebra para ser más conciso los métodos para resolver sistemas de ecuaciones lineales, pero si en vez de tener un sistema lineal obtenemos un sistema polinomial puesto que se ha escogido un enfoque intermedio que hace uso de métodos tanto abstractos como computacionales. Los métodos convencionales no resuelven dicho sistema es por ello que introducimos un nuevo concepto "BASES DE GRÖBNER''.

Es por eso que nos introducimos un poco en poder resolver los problemas para aplicar el método de Autovalores ya que para estudiar a fondo estos métodos se deben conectar al álgebra y a la geometría para estudiar los polinomios sobre un cuerpo.

Para la obtención de las BASES DE GRÖBNER utilizaremos el software CoCoA, el cual nos permite simplificar los cálculos y comprobación de los datos propuestos.

El presente trabajo radica en mostrar la importancia que tiene esta nueva teoría ya que resulta muy útil en campos como la genética, la programación, investigación de operaciones, en las ingenierías, etc. Pero también es mostrar a los estudiantes y profesores un nuevo método para resolver sistema de ecuaciones polinomiales, el método de Autovalores.

8. Objetivos

8.1 Planteamiento del problema

En nuestros estudios de secundaria vimos la división de polinomios de una variable en la división sintética vemos cada paso a respetar en los polinomios, identificar sus grados para analizar si la división puede realizarse.

Nos planteamos la pregunta ¿Cómo será la división si el polinomio posee dos o más variables? Empezamos a investigar y vimos los tipos de órdenes de los polinomios, el algoritmo de la división, los S-polinomios, etc.

De igual manera descubrimos las aplicaciones importantes que tienen los sistemas de ecuaciones polinomiales en la vida cotidiana al analizar los resultados de estos.

8.2 Objetivo general

- Resolver sistemas de ecuaciones polinomiales utilizando las Bases de Gröbner y la Teoría de Autovalores.

8.3 Objetivos específicos

- Definir los conceptos de Estructura Algebraica que serán abordados en el presente trabajo.

- Calcular las bases de Gröbner para los sistemas de ecuaciones polinomiales.

- Resolver sistemas de ecuaciones polinomiales utilizando el método de Autovalores para solucionar problemas de optimización de recursos.

- Utilizar el software CoCoA para la solución de sistemas de ecuaciones polinomiales.

9. Desarrollo del tema

9.1 Antecedentes

Presentaremos este trabajo, dando una pequeña historia de los orígenes del problema que aquí trataremos.

Una de las primeras civilizaciones en tratar problema del tipo algebraico fueron los egipcios, que en sus papiros hay una multitud de problemas matemáticos resueltos .La mayoría de ellos son aritméticos, pero también se encuentran problema del tipo algebraico. Conforme iba transcurriendo el tiempo se empezaron a descubrir nuevos métodos para resolver problemas algebraicos, uno de ellos fue el griego Thymarila (800 – A.C.) el cual había encontrado una fórmula para resolver un determinado sistema de n ecuaciones con n incógnitas.

Otro griego que se internó en la solución de sistemas de ecuaciones fue Diofanto de Alejandría, quien público su aritmética en la que por primera vez las matemáticas griegas eran tratadas de forma rigurosa. Estos métodos pasaron a los árabes los cuales lo extendieron a Europa… En el siglo IX el matemático y astrónomo musulmán Al-jwarizme investigo y escribió acerca de los números y métodos de cálculo, procedimientos algebraicos para resolver ecuaciones y sistemas de ecuaciones.

Un siglo después el matemático musulmán Abul-kamil continúo con los trabajos de Al-jwarizme, cuyos avances fueron aprovechados por el matemático italiano Fibonacci.

En el siglo XV el matemático Francés Nicolás Chuquet introdujo a Europa el uso de los números negativos y el matemático Alemán Christopher Rudolff introdujo el signo de la raíz cuadrada. Posteriormente entre 1545 y 1560 los matemáticos Italianos Grirolano Cardano y Rafael Bombilli, se dieron cuenta de la importancia de los números complejos para resolver sistemas de ecuaciones de segundo, tercer y cuarto

grado. En 1591 el matemático Francés François Vlite, desarrollo la notación algebraica más conocida y en 1637 Rene Descarte dio lugar a la geometría analítica y también introdujo la notación exponencial que se usa hoy en día.

Finalmente en el siglo XX el matemático Alemán Wolfgang Gröbner y el matemático Austriaco Bruno Buchberger, introdujeron un nuevo concepto conocido como bases de Gröbner, en honor al director de su tesis (Wolfgang- Gröbner) Su descubrimiento, es un conjunto especial de generadores para ideales en un anillo de polinomios en varias variables el cual nos permite resolver sistemas de ecuaciones Polinomiales, que a su vez son muy difíciles o imposibles de resolver mediante los métodos convencionales conocidos del álgebra lineal.

9.2 Marco teórico

9.2.1 Estructuras Algebraicas

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:

1. **Asociatividad:** para todo $g_1, g_2, g_3 \in G$, es
$$g_1 \cdot g_2 \cdot g_3 = g_1 \cdot g_2 \cdot g_3$$
2. **Elemento neutro:** existe un único $e \in G$ tal que para todo $g \in G$ es
$$e \cdot g = g = g \cdot e$$
3. **Inverso:** para todo $g \in G, \exists\, g' \in G$ tal que
$$g \cdot g' = e = g' \cdot g$$

Si además para todo par $g, \square \in G$ es $g \cdot \square = \square \cdot g$ entonces el grupo se llama abeliano o conmutativo.

Definición 2. 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:

1. **Cerradura respecto a la suma:** Para todo $a, b \in A$, se tiene que $a + b$ están en A.
2. **Asociatividad respecto a la suma:** Para todo $a, b, c \in A$ se tiene que
$$a + b + c = a + b + c$$
3. **Existencia del idéntico aditivo:** Existe un elemento neutro 0 en A, el cual llamaremos cero, tal que
$$a + 0 = a = 0 + a \text{ para todo } a \text{ en } A.$$

4. **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
$$a + -a = 0 = -a + a$$
5. **Conmutatividad respecto a la suma:** Para todo a, b en A se tiene
$$a + b = b + a$$
6. **Cerradura respecto al producto:** Para todo $a, b \in A$, se tiene que $a \cdot b$ están en A.

7. **Asociatividad respecto al producto:** Para todo a, b y c en A se satisface
$$a \cdot b \cdot c = (a \cdot b) \cdot c$$
8. **Existencia del idéntico multiplicativo:** Para todo a, existe un (único) elemento, e, en A que es neutro de la operación $\cdot$, es decir
$$\exists\, e \in A, \forall\, a \in A: e \cdot a = a = a \cdot e$$
9. **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 3. Sea K un conjunto no vacío, y sean $+$ y $\cdot$ dos operadores internas sobre K el sistema $K, +, \cdot$ es un **campo** si cumple:

1. **Asociatividad respecto a la suma:** Para todo $a, b, c \in K$ se tiene que
$$a + b + c = a + b + c$$
2. **Conmutatividad respecto a la suma:** Para todo a, b en K se tiene
$$a + b = b + a$$

3. **Existencia del idéntico aditivo:** Existe un elemento neutro 0 en K, el cual llamaremos cero, tal que
$$a + 0 = a = 0 + a \text{ para todo } a \text{ en } K.$$
4. **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
$$a + -a = 0 = -a + a$$
5. **Conmutatividad respecto a la suma:** Para todo a, b en K se tiene
$$a + b = b + a$$
6. **Asociatividad respecto al producto:** Para todo $a, b\, y\, c$ en K se satisface
$$a \cdot b \cdot c = a \cdot b \cdot c$$
7. **Conmutatividad respecto al producto :** Para todo a, b en K se tiene
$$a \cdot b = b \cdot a$$
8. **Existencia del idéntico multiplicativo:** Existe un (único) elemento $e \in K$, tal que para todo a es neutro de la operación $\cdot$, es decir
$$\exists\, e \in K, \forall\, a \in K : e \cdot a = a = a \cdot e$$
9. **Existencia de elementos inversos multiplicativo:** Para todo $a \in K, \exists\, a' \in K$, es decir:
$$a' \cdot a = e$$

Definición 4. Un **módulo** sobre un anillo R consiste en un grupo abeliano $M, +$, y la operación $R \times M \to M$ multiplicación escalar, estrictamente escrita solo por yuxtaposición, es decir como rx para r en R y x en M, tal que para todo r, s en r, x y en R tenemos:

1. $rs\ x = r\ sx$
2. $r + s\ x = rx + sx$
3. $r\ x + y = rx + ry$
4. $1.x = x$

Generalmente, escribimos simplemente “un R-módulo izquierdo M”.

Un R módulo derecho *M*, se define de forma semejante, sólo que el anillo actúa por la derecha, es decir tenemos una multiplicación escalar de la forma $M \times R \to M$, y los tres axiomas antedichos se escriben con los escalares $r\ y\ s$ a la derecha de $x\ e\ y$.

Si *R* es **conmutativo**, entonces los *R*-módulos a la izquierda son lo mismo que *R*-módulos a la derecha y se llaman simplemente *R*-módulos.

Definición 5. Dado un cuerpo K y un conjunto E, decimos que E se ha dotado de estructura de **espacio vectorial**, si en E están definidas las siguientes operaciones:

$$\begin{array}{ll} E \times E \to E & K \times E \to E \\ u, v \ \to u + v & (\lambda, u) \to \lambda \cdot u \end{array}$$

Que tiene las propiedades siguientes:

$$\forall\, u \in E, v \in E, w \in E \ \wedge\ \forall\, \lambda \in K, \mu \in K$$

1. $u + v + w = u + v + w$

2. $u + v = v + u$

3. $\exists 0 \in E / u + 0 = u$

4. $\exists\, u^{-1} \in E / u + u^{-1} = 0$

5. $\lambda + \mu \cdot u = \lambda \cdot u + \mu \cdot u$

6. $\lambda \cdot u + v = \lambda \cdot u + \lambda \cdot v$

7. $\lambda \cdot \mu \cdot a = \lambda \cdot \mu \cdot a$

8. $1 \cdot a = a$

Llamaremos un vector a todo elemento de un espacio vectorial.

Definición 6. Un **monomio** en $x_1, x_2, \cdots, x_n$ es un producto de la forma $x_1^{a_1}.x_2^{a_2} \cdots x_n^{a_n}$, donde todos los exponentes $a_1, a_2, \cdots, a_n$ son enteros no negativos. El grado total de este monomio es la suma $a_1, a_2, \cdots, a_n$.

Notación. Escribiremos x^{α} por $x_1^{\alpha_1}.x_2^{\alpha_2}\cdots x_n^{\alpha_n}$, donde $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_n$ es una n-uplas de enteros no negativos. Si $\alpha = 0,0,\cdots,0$, $x^{\alpha} = 1$. Además, $|\alpha| = \sum_{i=1}^{n} \alpha_i$ denota el grado total del monomio x^{α}.

Definición 7. Un **Ideal** es un subconjunto $I \subset K\ x_1, \cdots, x_n$ es un ideal si satisface:

1. $0 \in I$
2. Si $f, g \in I$, entonces $f + g \in I$
3. Si $f \in I\ y\ \square \in K\ x_1, \cdots, x_n$, $entonces\ \square f \in I$

9.2.2 El anillo de polinomios $K\ x_1, \cdots, x_n$

Definición 8. Sea **A** un anillo y denotemos $A^{\square}$ con la estructura de anillo definida anteriormente (definición 2):

1. Si acordamos que $x = \epsilon_1$, el anillo $A^{\square}$ será denominado **anillo polinomial** en la indeterminada x sobre A y denotada por $A\ x$. Este es un anillo conmutativo y cada elemento de $A\ x$ tiene una representación única

$$\sum_{i \in \square} a_i x^i$$

   Con $a_i \in A\ y\ a_i \neq 0$ únicamente para un número finito de índices $i \in \square$.

2. Para $n \geq 1$, definimos recursivamente

$$A\ x_1, \cdots, x_n = A\ x_1, \cdots, x_{n-1}\ \ x_n$$

   Y llamémoslo **anillo polinomial en n indeterminadas sobre A**.

3. Los elementos de un anillo polinomial se llaman polinomios. Con mucha frecuencia los polinomios en una indeterminada son llamados polinomios univariados, mientras los polinomios en varias indeterminadas, polinomios multivariados.

9.2.3 Ideales en el anillo $K\ x_1, \cdots, x_n$

Definición 9. Sea $I \subset K[x_1, \cdots, x_n]$ un subconjunto no vacío. I Se llama un **ideal polinomial** si:

1. $f + g \in I$ siempre que $f \in I$ y $g \in I$

2. $\rho f \in I$ siempre que $f \in I$ y $\rho \in K[x_1, \cdots, x_n]$ es un polinomio arbitrario.

Definición 10. Aritmética de Ideales. Las siguientes operaciones existen entre los Ideales I y J de anillos $K[x_1, \cdots, x_n]$, siendo K un número natural.

1. I + J = f + g / f ∈ I, g ∈ J

2. I · J = $\sum_{i=1}^{n} f_i g_i \ / \ f_i \in I \ , g_i \in J, \ n \in$?

3. I: J = $f \in K\ x_1, \cdots, x_n \ / f g \in I \ , \forall g \in J$

4. I ∩ J = $f \in K\ x_1, \cdots, x_n \ / f \in I \ , f \in J$

5. $I^k = \sum_{i=1}^{n} f_1 \ , f_2, \cdots, f_k \ / \ f_1, \cdots, f_k \in I$

Ideales principales e Ideales maximales.

El siguiente teorema nos dice que la intercepción de ideales de un anillo es también ideal.

Teorema 11. Si para cada $j \in J, I_j$ es un ideal entonces $I = \cup_{j \in J} I_j$ es un ideal.

Definición 12. Si $X \subset A$ llamamos **ideal generado** por X al ideal de A que contiene a X . Lo denotamos $\langle X \rangle$.

Si $X = a$ el ideal generado por x. Se llama ideal principal generado por a para ello basta considerar $\cap \ I = I \ es \ ideal \ de \ A \ \ y \ X \subseteq \ I$

Definición 13. Un **ideal** $M \in A$ se dice **máximal** si $M \neq A$ y $\forall N \in A$, si $M \subseteq A \rightarrow N = A$. En otras palabras un ideal es máximal si no está contenido en ningún otro ideal no trivial.

Ejemplo 14.

1. El ideal 3Z de Z es maximal.
2. El ideal $\langle x^2 + 1 \rangle$ de Q[x] es maximal.

9.2.4 Órdenes entre términos

Definición 15. Órdenes entre términos

Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio de $K\ x_1, \cdots, x_n$

1. Llamaremos a a_α el coeficiente del monomio x^α
2. Si $a_\alpha \neq 0$, $a_\alpha x^\alpha$ es un término de f
3. El grado total de f denotado $grad\,(f)$ es el máximo $|\alpha|$ entre todos los monomios cuyos coeficientes a_α son distintos de 0.

Definición 16. Términos principales

Dado un polinomio no nulo $f \in K[x]$, sea

$$f = a_0 x^m + a_1 x^{m-1} + \cdots + a_m$$

Donde $a_i \in K$ y $a_0 \neq 0$ (es decir $m = grad\,(f)$). Decimos entonces que $a_0 x^m$ es el termino principal de f y se escribe $t_p\,(f) = 2x^3$. Observe también que $f\ y\ g$ son polinomios no nulos, entonces

$$grad\ f \leq grad\ g \leftrightarrow t_p\ f \ / \ t_p\,(g)\,)$$

Definición 17. Órdenes Monomiales

Un **orden monomial** en $K\ x_1, \cdots, x_n$ es una relación $>$ en $Z_{\geq 0}^n$, o equivalentemente, una relación en el conjunto de monomios x^α, $\alpha \in Z_{\geq 0}^n$, que sastiface:

1. $>$ es un orden total o lineal $en\ Z_{\geq 0}^n$
2. $si\ \alpha > \beta$ y $\gamma \in Z_{\geq 0}^n$, Entonces $\alpha + \gamma > \beta + \gamma$
3. $>$ es un buen orden $en\ Z_{\geq 0}^n$. Esto significa que todo subconjunto no vacío de $Z_{\geq 0}^n$ tiene un elemento mínimo bajo $>$

Definición 18. Orden Lexicográfico

Sea $\alpha = (\alpha_1, \cdots, \alpha_n)$ y $\beta = \beta_1, \cdots, \beta_n \in Z_{\geq 0}^n$ Decimos que $\alpha >_{lex} \beta$ si, en la diferencia vectorial $\alpha - \beta \in \mathbb{Z}^n$ la primera componente no nula por la izquierda es positiva. Escribiremos $x^\alpha >_{lex} x^\beta$ si $\alpha >_{lex} \beta$

Ejemplo 19.

1. $1,2,0 >_{Lex} 0,3,4$ donde $\alpha - \beta = (1, -1, -4)$
2. $3,2,4 >_{Lex} (3,2,1)$ donde $\alpha - \beta = (0,0,3)$
3. Las variables $x_1, \cdots, x_n$ están ordenadas en el sentido usual por el orden Lex.

$$1,0,\cdots,0 >_{Lex} 0,1,0,\cdots,0 >_{Lex} \cdots >_{Lex} 0,\cdots,0,1$$

Así $x_1 >_{Lex} x_2 >_{Lex} \cdots >_{Lex} x_n$

En la práctica, cuando se trabaja con polinomios en dos o tres variables se utiliza x, y, z en vez de $x_1,\ x_2,\ x_3$. Se asume también el orden alfabético $x > y > z$.

El orden Lex es análogo al orden de las palabras usado en el diccionario (de aquí su nombre). Las componentes de las n-uplas $\alpha \in \mathbb{Z}_{\geq 0}^n$ o como una analogía en las letras de una palabra. Las letras están ordenadas alfabéticamente,

$$a > b > c > \cdots > x > y > z$$

Definición 20. Orden Lexicográfico Graduado

Sea $\alpha, \beta \in Z_{\geq 0}^n$ Decimos que $\alpha >_{lexgr} \beta$, Si $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ o $|\alpha| = |\beta|$ y $\alpha >_{lex} \beta$

Vemos que el orden Lexgr ordena con el grado total primero, luego cuando son iguales sumamos el orden Lex.

Ejemplos 21:

1. $1,2,3 >_{Lexgr} 3,2,0$, ya que $|\ 1,2,3\ | = 6 > |\ 3,2,0\ | = 5$
2. $1,2,4 >_{Lexgr} 1,1,5$, $|(1,2,4)| = |(1,1,5)| = 7$ y $1,2,4 >_{Lex} 1,1,5$ donde $1,2,4 - 1,1,5 = (0,1,-4)$ se concluye que $1,2,4 >_{Lexgr} (1,1,5)$

Definición 22. Orden Lexicográfico Graduado Revertido

Sea $\alpha, \beta \in Z_{\geq 0}^n$. Decimos que $\alpha >_{lexgrev} \beta$, si $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ o $|\alpha| = |\beta|$ y en $\alpha - \beta \in$ ⍰^{n} , la primera componente no nula por la derecha es negativa.

Ejemplos 23:

1. $(4,7,1) >_{Lexgrv} (4,2,3)$ ya que $|(4,7,1)| = 12 > |(4,2,3)| = 9$
2. $(1,5,2) >_{Lexgrv} (4,1,3)$ ya que $|(1,5,2)| = |(4,1,3)| = 8$ y $1,5,2 - 4,1,3 = (-3,4,-1)$

Definición 24. Orden Lexicográfico Inverso.

Para $t_1, t_2 \in \mathbb{T}^n$ diremos que $t_1 >_{lexin} t_2$ si y solo si en la diferencia vectorial $\log(t_1) - \log(t_2)$, la primera componente no nula por la derecha es positiva, o bien si $t_1 = t_2$.

Ejemplo 25. En $K\ u,v,w$ con $u > v > w$ tenemos que:

1. $x^2y^2z^3 >_{Lexin} x^4yz^3$, dado que al hacer la diferencia $2,2,3 - 4,1,3 = -2,1,0$, la primera componente no nula por la derecha es positiva.
2. $y >_{Lexin} x^3$, dado que al hacer la diferencia $0,1,0 - 3,0,0 = -3,1.0$, la primera componente no nula por la derecha es positiva.

9.2.5 División en el anillo $K\ x_1,\cdots,x_n$

Para estudiar el problema de dividir un polinomio $K\ x_1,\cdots,x_n$ es más de un divisor, se planteara el algoritmo de la división para polinomios en $K\ x_1,\cdots,x_n$, la meta es dividir f por $g_1,\cdots,g_s \in K\ x_1,\cdots,x_n$, esto se puede expresar en la forma:

$$f = a_1g_1 + \cdots + a_sg_s + r$$

Donde los cocientes $a_1,\cdots,a_s\ y\ r \in K\ x_1,\cdots,x_n$, para caracterizar el residuo, será necesario usar los órdenes monomial definidos en el apartado 9.2.4

La idea básica del algoritmo de la División es cancelar el termino principal de f (con respecto al orden monomial fijado) multiplicando y dividiendo cierto g_i para un monomio apropiado. Entonces este monomio se convierte en un término correspondiente a_i.

Definición 26. Algoritmo de la división

Sea $s \geq 1$, y sean $f,g_1,\cdots,g_s \in K\ x_1,\cdots,x_n$ consideremos la siguiente secuencia de pasos.

1. Sea $q_1 = \cdots = q_s = 0, p = 0\ y\ v = f$
2. Encontrar el menor $i \in 1,\cdots,s$ tal que $tp(v)$ es un múltiplo de $tp(g_i)$, si tal i existe, reemplazar q_i por $q_i + \frac{mp(v)}{mp(g_i)}$ y v por $v - \frac{mp(v)}{mp(g_i)} \cdot g_i$.

3. Repetir el paso II hasta que no exista mas $i \in \{1, \cdots, s\}$ tal que $tp(v)$ es un múltiplo de $tp(g_i)$, entonces reemplazar p por $p + mp(v)$ y v por $v - mp(v)$.
4. Si ahora $v \neq 0$, inicial de nuevo con el paso II, si $v = 0$ regresar la tupla $(q_1, \cdots, q_s) \in p^s$ y el vector $p \in p^r$.

Este es un algoritmo que retorna vectores $(q_1, \cdots, q_s) \in p^s$ y $p \in p^r$ tales que:

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

Que satisfacen las condiciones siguientes:

1. Ningún elemento de p esta contenido en $\langle tp(g_1), \cdots, tp(g_s) \rangle$.
2. Ningún $q_i \neq 0$ para algún $i \in \{1, \cdots, s\}$ entonces $tp(q_i g_i) \leq tp(f)$.
3. Para todo índice $i \in \{1, \cdots, s\}$ y todo término $t \in q_i$, tenemos $t.tp(g_i) \notin \langle tp(g_i), \cdots, tp(g_{i-1}) \rangle$

Ejemplo 27:

Sea $f = x^2y + xy^2 - y^2$ y $F = \{y^2 - 1, xy - 1\}$, dividir $f\ entre\ F$ con el orden Lex.

$$\begin{array}{r} a_1: \\ a_2: \\ y^2 - 1 \\ xy - 1 \end{array} \overline{\big) x^2y + xy^2 - y^2} \quad \underline{\quad} \; \mathrm{r}$$

Podemos apreciar que solo hemos colocado cada elemento en su lugar. Ahora procedamos a sacar los términos principales de $f\ y\ F$ y verifiquemos si podemos hacer la división.

$tp(f) = x^2y, tp(F) = (y^2, xy)$. Como vemos el término que divide a $tp(f) = x^2y$ es xy por lo tanto procedemos hacer la división $\frac{x^2y}{xy} = x$ el cual es nuestro cociente a_2, ahora hacemos la resta $f - x(xy - 1) = f - x^2y + x$.

$$\begin{array}{r|l} & a_1: \\ & a_2: x \qquad\qquad\qquad\qquad r \\ y^2-1 \;\big)\; x^2y+xy^2-y^2 & \\ xy-1 \quad -x^2y+x & \\ \hline xy^2+x-y^2 \longrightarrow & xy^2+x-y^2 \end{array}$$

Ahora hacemos el mismo procedimiento y como se observa el término principal de F aun es divisible por xy, pero también es divisible por y^2 y como a_1 esta antes que a_2 por lo tanto se hace la división correspondiente $\frac{xy^2}{y^2}=x$ el cuál es nuestro nuevo cociente para a_1, se hace la resta de nuestro nuevo $f-x(y^2-1)$, el cual da como resultado lo siguiente.

$$\begin{array}{r|l} & a_1{:}x \\ & a_2{:}x \qquad\qquad r \\ y^2-1 \;\big)\; x^2y+xy^2-y^2 & \\ xy-1 \quad -x^2y+x & \\ \hline xy^2+x-y^2 & \\ -xy^2+x & \\ \hline 2x-y^2 \longrightarrow & 2x-y^2 \end{array}$$

Aquí como ni xy, y^2 dividen al término principal de nuestro nuevo $f=2x-y^2$, $tp(f)=(2x)$ se saca fuera al residuo, y queda de la siguiente forma.

$$
\begin{array}{r|l}
 & a_1{:}x \\
y^2-1 & a_2{:}x \qquad\qquad r \\
xy-1 & \overline{)\,x^2y+xy^2-y^2} \\
 & \underline{-x^2y+x} \\
 & xy^2+x-y^2 \\
 & \underline{-xy^2+x} \\
 & 2x-y^2 \\
 & \underline{\qquad\qquad} \\
 & -y^2 \longrightarrow 2x-y^2
\end{array}
$$

$f=-y^2$ y su $tp(f)=-y^2$, el cual es divisible por y^2, y se procede a realizar la división correspondiente $\frac{y^2}{-y^2}=-1$ el cual es el cociente para a_1, se efectúa la resta $-y^2-(-1)(y^2-1)=-1$, y nos queda de la siguiente forma.

$$
\begin{array}{r|l}
 & a_1{:}x\ -1 \\
y^2-1 & a_2{:}x \qquad\qquad r \\
xy-1 & \overline{)\,x^2y+xy^2-y^2} \\
 & \underline{-x^2y+x} \\
 & xy^2+x-y^2 \\
 & \underline{-xy^2+x} \\
 & 2x-y^2 \ \to 2x \\
 & \underline{-y^2} \\
 & y^2-1 \qquad -1
\end{array}
$$

Como -1 no es divisible por (y^2, xy), se saca al residuo y nos queda.

$$
\begin{array}{rl}
 & a_1 = x - 1 \\
 & a_2 = x \\
y^2 - 1 \;\; \overline{)\, x^2 y + x y^2 - y^2} \\
xy - 1 & \\
 & -x^2 y + x \\
 & \_\_\_\_\_ \\
 & xy^2 + x - y^2 \\
 & -xy^2 + x \\
 & \_\_\_\_\_ \\
 & 2x - y^2 \rightarrow 2x \\
 & -y^2 \\
 & y^2 - 1 \\
 & \_\_\_\_\_ \\
 & -1 \rightarrow 2x - y \\
 & \_\_\_\_\_ \\
 & 0 \longrightarrow \text{residuo}
\end{array}
$$

Después de todo este procedimiento llegamos a f puede ser escrito de la forma $f = a_1\,(y^2 - 1) + a_2\,(xy - 1) + r$, donde los valores para a_1, a_2, r son $a_1 = x - 1$, $a_2 = x$, $r = x + y - 1$, de lo cual se concluye que.

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

9.3 Metodología

9.3.1 Modalidad de investigación

El presente estudio, según el diseño es de tipo descriptivo, ya que describe los diversos tipos de órdenes monomiales, el algoritmo de la división para $K\ x_1, \cdots, x_n$, el algoritmo de Buchberger, las bases de Gröbner, el método de Autovalores, etc. Dando sus definiciones previas para realizar nuestro estudio.

Planteamos nuestra aplicación en conceptos científicos y en la problemática de la vida cotidiana en nuestro país.

9.3.2 Recursos computacionales

Utilizamos como herramienta el software CoCoA 4.7.5, el Mathematica, el Singular y el Scientific WorKPlace 5.5

Para hacer uso de énfasis en la parte algorítmica utilizamos el sistema de Álgebra Computacional. Se hace uso del SAC en casos, como verificación de algún cálculo, ejemplificación de algún algoritmo y en aquellos cálculos engorrosos donde solo interesa el resultado para el análisis de algún dato.

9.3.3 ¿Qué es CoCoA?

El SAC CoCoA es un software libre que puede ser descargado gratuitamente en URL:

http://cocoa.dima.unige.it

Es un programa especializado en álgebra conmutativa, de ahí su nombre “COMPUTATIONS IN Commutative Algebra”, contiene un listado con sus principales comandos ejemplificados como una herramienta para facilitar su uso.

Es un sistema de algebra computacional, desarrollado por Universidad de Génova y diseñado para hacer frente a los problemas de la teoría de números y especialmente de polinomios.

CoCoA presenta una interfaz de texto (también utilizado por temas) y una interfaz gráfica.

Todos los ejercicios citados en el documento están presentados con el CoCoA 4.7.4

9.3.4 ¿Qué es Singular?

Singular, es un sistema de algebra Computacional (SAC) para cálculos polinomicas con énfasis especial en las necesidades del algebra conmutativa, de geometría algebraica y de la teoría de singularidades. Como sistema especializado su objetivo no es proporcionar toda la funcionalidad de un SAC de proposición general.

Es un software libre que puede ser descargado gratuitamente en el URL:

http://www.singular.uni_kl.de

9.3.5 ¿Qué es Mathematica?

Mathematica, es un programa utilizado en áreas científicas, de ingenierías y áreas de computacionales. Originalmente fue concebido por Sthephen Wolfram, quien continúa como líder del grupo de matemáticos y programadores que desarrolla. El mathematica es considerado como un sistema poderoso de algebra computacional de propósito general.

Es un software libre que puede ser descargado gratuitamente en el URL:

http://www.softonic.com/s/programa-mathematica

9.4 Sistemas de Ecuaciones Polinomiales

Los sistemas de ecuaciones polinomiales son importantes dentro de la modelización de problemas reales. El estudio y el cálculo de sus soluciones exactas constituyen todo un campo de trabajo con diversas aplicaciones en la vida cotidiana así está plasmado en la economía, la ingeniería, informática, etc. Este campo se estudia dentro de las diversas ramas de la matemática.

9.4.1 Algoritmo de Buchberger y Bases de Gröbner

Definición 28. Términos principales de un Ideal

Sea $I \in K\ x_1, \cdots, x_n$ un ideal distinto de 0 .

1. Denotamos por $tp(I)$ al conjunto de todos los términos principales de los elementos de I asi,

$$\boldsymbol{tp\ I\ =\ cx^{a}}: \exists \boldsymbol{f} \in \boldsymbol{I} \text{ con } \boldsymbol{tp\ f\ =\ cx^{a}}$$

2. Denotamos por $\langle tp(I) \rangle$ al ideal generado por los elementos de $tp(I)$.

Esto brinda un importante detalle respecto a $\langle tp(I) \rangle$, es decir si tenemos un conjunto generador finito de $I = \langle f_1, \cdots, f_s \rangle$, entonces $\langle tp\ f_1\ , \cdots, tp(f_s) \rangle$ y $\langle tp(I) \rangle$ pueden ser ideales diferentes. Es cierto que $tp(f_i) \in tp(I) \subset \langle tp(I) \rangle$ por definición, lo que implica que $\langle tp\ f_1\ , \cdots, tp(f_s) \rangle \subset \langle tp(I) \rangle$. No obstante, $\langle tp(I) \rangle$ pueden ser estrictamente más grandes.

Ejemplo 29. Términos Principales del Ideal

Sea $I = \langle f_1, f_2 \rangle$, donde $f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x$, y usemos el orden $Lexgr$ en los monomios de $K\ x, y$. Entonces

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

De modo que $x^2 \in I$. Por tanto, $x^2 = tp\ x^2 \in \langle tp\ I \rangle$, sin embargo x^2 no es divisible ni por $tp(f_1) = x^3$, ni por $tp(f_2) = x^2y$ así que $x^2 \notin \langle tp\ f_1, tp(f_2) \rangle$

Proposición 30. Sea $I \subset K\ x_1 \cdots, x_n$ un ideal de términos principales. Entonces:

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

2. Existen $g_1, \cdots, g_t \in I$: $\langle tp\ I \rangle = \langle tp\ g_1, \cdots, tp(g_t) \rangle$

Teorema 31. Las bases de Hilbert. Todo ideal $I \subset K\ x_1, \cdots, x_n$ tiene un conjunto generador finito. Es decir $I = \langle g_1, \cdots, g_t \rangle$, para algunos $g_1, \cdots, g_t \in I$.

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 $g_1, \cdots, g_t$ para I de la siguiente manera: existen $g_1, \ldots, g_t \in I$ tal que $\langle tp\ I \rangle = \langle tp\ g_1, \cdots, tp(g_t) \rangle$. Afirmamos que $I = \langle g_1, \cdots, g_t \rangle$.

Es evidente que $\langle g_1, \cdots, g_t \rangle \subset I$ porque cada $g_i \subset I$. Para la otra inclusión, sea $f \in I$ un polinomio arbitrario. Si aplicamos el algoritmo de la división de la sección 9.2.5 para dividir f por $g_1, \cdots, g_t$, entonces obtenemos una expresión de la forma

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

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

$$r = f - a_1 f_1 - \cdots - a_s f_s \in I$$

Si $r \neq 0$, entonces $tp\ r \in \langle tp\ I \rangle = \langle tp\ g_1, \cdots, tp(g_t) \rangle$, por lo tanto $tp\ r$ 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,

$$f = a_1 f_1 + \cdots + a_s f_s + 0 \in \langle g_1, \cdots, g_t \rangle.$$

Lo cual deja de manifiesto que $I \subset \langle g_1, \cdots, g_t \rangle$, completandose asi la demostración. ■

Definición 32. Un conjunto finito $G = \{g_1, \cdots, g_t\}$ de un ideal I es una **Base de Gröbner** para I (o base estándar) si

$$\langle tp\ g_1, \cdots, tp\ g_t \rangle = \langle tp\ I \rangle$$

Un conjunto $G = \{g_1, \cdots, g_t\} \subset I$ es una **Base de Gröbner** de I si y sólo si el término principal de cualquier elemento de I es divisible por alguno de los $tp\ g_i$.

Corolario 33. Todo ideal $I \neq \{0\} \subset K[x_1, \cdots, x_n]$ tiene una Base de Gröbner. Además toda Base de Gröbner de un ideal I es una base de I.

Demostración. Dado un ideal I no nulo, el conjunto $G = \{g_1, \cdots, g_t\}$ construido con la demostración del teorema es una Base de Gröbner por definición. Respecto a la segunda afirmación observamos que si

$$\langle tp\ I \rangle = \langle tp\ g_1, \cdots, tp\ g_t \rangle,$$

Entonces el argumento dado en el teorema prueba que $I = \{g_1, \cdots, g_t\}$ de modo que G es una base para I. ■

Definición 34. S-polinomio

Sea $f, g \in K[x_1, \cdots, x_n]$, polinomios no nulos

1. Si el multigrado $f = \alpha$ y el multigrado $g = \beta$ entonces $\rho = (\rho_1, \cdots, \rho_n)$ donde $p_i = Max(\alpha_i \beta_i)$ para cada i. Llamamos x^p al m.c.m. de $m\rho\ f$, $m\rho\ g$, y escribimos

$$x^p = \text{m.c.m.}\ (m\rho\ f, m\rho\ g)$$

2. El S- polinomio de f, g es la combinación.

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

Ejemplo 35. Calcule el $S\ f,g$ usando el orden $DegRevLex$. Para los los polinomios

$$f = 4x^2z - 7y^2 \text{ y } g = xyz^2 + 3xz^4$$

El primer paso es encontrar el multigrado de $f\ y\ g$, a los cuales designaremos por $\alpha\ y\ \beta$ respectivamente.

El multigrado de f es $\alpha = (2,0,1)$ y el multigrado de g es $\beta = (1,0,4)$, lo que implica que $\rho = (2,0,4)$, por ende $x^\rho = x^2z^4$, aplicando la fórmula para calcular el S-polinomio obtenemos:

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

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

Ahora resolveremos el mismo ejemplo utilizando CoCoA 4.7.4

Use R ::= QQ[x,y,z],DegRevLex;

f1:= 4x^2z-7y^2;

F2:= xyz^2+3xz^4;

TP1:=LT(4x^2z-7y^2);

TP2:=LT(xyz^2+3xz^4);

M:=LCM(TP1,TP2);

SPOLY:=(M/TP1)*(F1)-(M/TP2)*(F2);

Print "El S-polinomio es:";

SPOLY;

El S-polinomio es:

-(7y^2 z^3)/4-(x^2 yz^2)/3

Definición 36. Algoritmo de Buchberger

Sea K un campo, sea $n \geq 1$, sea $p = K[x_1, \cdots, x_n]$ un anillo polinomial, sea $r \geq 1$, y sea σ un orden de términos sobre el módulo $\mathbb{T}^n\langle e_1, \cdots, e_r\rangle$. Nuestra meta es calcular una $\sigma-$base de Gröbner de un P-submódulo $M \subseteq p^r$ el cual esta explícitamente dado por un sistema de generadores $G = \{g_1, \cdots, g_s\} \subseteq p^r \setminus \{0\}$. Sea $\mathcal{G}$ la tupla $(g_1, \cdots, g_s)$. Iniciemos escribiendo $mp_\sigma(g_i) = c_i t_i e_{\gamma_i}$ con $c_i \in K \setminus \{0\}, t_i \in \mathbb{T}^n, y\, \gamma_i \in \{1, \cdots, r\}$ para $i = 1, \cdots, s$.

Definición 37. Criterio de Buchberger

Sea $M \subseteq p^r$ un P-submódulo generado por $G = \{g_1, \cdots, g_s\} \subseteq p^r \setminus \{0\}$ y sea

$\mathcal{G} = (g_1, \cdots, g_s)$. Entonces las siguientes condiciones son equivalentes.

1. El conjunto G es una $\sigma-$base de Gröbner de M.
2. $\forall (i, j) \in \mathbb{B}$, tenemos $RN_{\sigma,\mathcal{G}}(S_{i,j}) = 0$.

Teorema 38. Algoritmo de Buchberger

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

1. Sea $s' = s$ y $B = \mathbb{B} = \{(i, j) \mid 1 \leq i < j \leq s', \gamma_i = \gamma_j\}$.
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

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

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 $g_s = RN_{\sigma,G}(S_{i,j})$ a G y el conjunto de pares

$i, j \mid 1 \leq i < j \leq s, \gamma_i = \gamma_j$ 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-upla G de vectores los cuales forman una $\sigma -$ base de Gröbner de M.

Ejemplo 39. Bases de Gröbner

Calcular la Base de Gröbner del ideal respecto al orden monomial lexicográfico con $x > y > z$.

$$I = \langle -z^4 + x, -z^5 + y \rangle$$

Sabemos que nuestro Ideal no es una base de Gröbner, como el ejercicio nos lo están pidiendo con el orden monomial lexicográfico ya se encuentra ordenado.

Encontraremos el S-Polinomio:

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

$$x^\rho = z^5 \text{ en } \langle f_1, f_2 \rangle$$

$$S(f_1, f_2) = \frac{z^5}{-z^4}(-z^4 + x) - \frac{z^5}{-z^5}(-z^5 + y)$$

$$S(f_1, f_2) = -z(-z^4 + x) - z^5 + y$$

$$S(f_1, f_2) = z^5 - xz - z^5 + y$$

$$S(f_1, f_2) = -xz + y$$

$$S(f_1, f_2)^F = f_3$$

Comprobaremos con el algoritmo de la división si nuestro f_3 pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{rl}
 & a_1{:}0 \\
 & a_2{:}0 \qquad\qquad r \\
f_1 = -z^4 + x \;\big)\; & -xz + y \\
f_2 = -z^5 + y \;\big)\; & 0 \\
\hline
 & -xz + y \longrightarrow -xz + y
\end{array}
$$

Como el residuo no es cero entonces $f_3 = -xz + y$ pasa a ser parte de la base.

$$F = \{-z^4 + x, -z^5 + y, -xz + y\}$$

Ahora encontraremos el S-Polinomio de f_1, f_3 con $x^\rho = xz^4$

$$S(f_1, f_3) = \left[\frac{xz^4}{-z^4}\right](-z^4 + x) - \left[\frac{xz^4}{-xz}\right](-xz + y)$$

$$S(f_1, f_3) = (-x)(-z^4 + x) - (-z^3)(-xz + y)$$

$$S(f_1, f_3) = xz^4 - x^2 - xz^4 + yz^3$$

$$S(f_1, f_3) = -x^2 + yz^3$$

$$S(f_1, f_3) = yz^3 - x^2$$

$$\overline{S(f_1, f_3)}^F = f_4$$

Comprobaremos con el algoritmo de la división si nuestro f_4 pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l|l}
 & a_1: -x \\
 & a_2: 0 \\
 & a_3: z^3 \qquad\qquad r \\
f_1 = -z^4 + x & \overline{\qquad\qquad\qquad} \\
f_2 = -z^5 + y & yz^3 - x^2 \\
f_3 = -xz + y & \underline{-yz^3 + xz^4} \\
 & xz^4 - x^2 \\
 & \underline{-xz^4 + x^2} \\
 & 0 \longrightarrow 0
\end{array}
$$

$f_4 = yz^3 - x^2$ Pasa a ser parte de la base

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2\}$$

Ahora encontraremos el S-Polinomio de f_2, f_3 con $x^\rho = xz^5$

$$S(f_2, f_3) = \left[\frac{xz^5}{-z^5}\right](-z^5 + y) - \left[\frac{xz^5}{-xz}\right](-xz + y)$$

$$S(f_2, f_3) = (-x)(-z^5 + y) - (-z^4)(-xz + y)$$

$$S(f_2, f_3) = xz^5 - xy - xz^5 + yz^4$$

$$S(f_2, f_3) = yz^4 - xy = (-y)f_1$$

$$S(f_2, f_3)^F = 0$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l}
f_1 = -z^4 + x \\
f_2 = -z^5 + y \\
f_3 = -xz + y \\
f_4 = yz^3 - x^2
\end{array}
\qquad
\begin{array}{l}
a_1{:}0 \\
a_2{:}0 \\
a_3{:}x \\
a_4{:}\ z
\end{array}
\qquad
\begin{array}{|l}
\hline
yz^4 - xy \\
-yz^4 - x^2z \\
\hline
-x^2z - xy \\
x^2z - xy \\
\hline
-2xy \longrightarrow
\end{array}
\qquad
\begin{array}{l}
r \\
\\
\\
\\
\\
\\
-2xy
\end{array}
$$

Por lo tanto

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2\}$$

Ahora encontraremos el S-Polinomio de f_1, f_4 con $x^\rho = yz^4$

$$S(f_1, f_4) = \left[\frac{yz^4}{-z^4}\right](-z^4 + x) - \left[\frac{yz^4}{yz^3}\right](yz^3 - x^2)$$

$$S(f_1, f_4) = (-y)(-z^4 + x) - (z)(yz^3 - x^2)$$

$$S(f_1, f_4) = yz^4 - xy - yz^4 + x^2z$$

$$S(f_1, f_4) = x^2z - xy = (-x)f_3$$

$$S(f_1, f_4)^F = 0$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

a_1:0
a_2:0
a_3: $-x$
a_4: 0 $\quad r$

$f_1 = -z^4 + x$
$f_2 = -z^5 + y$
$f_3 = -xz + y$
$f_4 = yz^3 - x^2$

$x^2z - xy$
$-x^2z + xy$
$0 \longrightarrow 0$

Por lo tanto

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2\}$$

Ahora encontraremos el S-Polinomio de f_2, f_4 con $x^\rho = -yz^5$

$$S(f_2, f_4) = \left[\frac{-yz^5}{-z^5}\right](-z^5 + y) - \left[\frac{-yz^5}{yz^3}\right](yz^3 - x^2)$$

$$S(f_2, f_4) = (y)(-z^5 + y) - (-z^2)(yz^3 - x^2)$$

$$S(f_2, f_4) = -yz^5 + y^2 + yz^5 - x^2z^2$$

$$S(f_2, f_4) = -x^2z^2 + y^2 = (xz + y)f_3$$

$$S(f_2, f_4)^F = 0$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l}
f_1 = -z^4 + x \\
f_2 = -z^5 + y \\
f_3 = -xz + y \\
f_4 = yz^3 - x^2
\end{array}
\qquad
\begin{array}{l}
a_1{:}0 \\
a_2{:}0 \\
a_3{:}xz + y \\
a_4{:}\ 0 \\
\hline
x^2z^2 + y^2 \\
\underline{-x^2z^2 - xyz} \\
-xyz + y^2 \\
\underline{xyz - y^2} \\
0 \longrightarrow
\end{array}
\qquad
\begin{array}{l}
r \\
\hline
\\
\\
\\
\\
0
\end{array}
$$

Por lo tanto

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2\}$$

Ahora encontraremos el S-Polinomio de f_3, f_4 con $x^\rho = xyz^3$

$$S(f_3, f_4) = \left[\frac{xyz^3}{-xz}\right](-xz + y) - \left[\frac{xyz^3}{yz^3}\right](yz^3 - x^2)$$

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

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

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

$$S(f_3, f_4)^F = f_5$$

Comprobaremos con el algoritmo de la división si nuestro f_5 pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l}
f_1 = -z^4 + x \\
f_2 = -z^5 + y \\
f_3 = -xz + y \\
f_4 = yz^3 - x^2
\end{array}
\qquad
\begin{array}{l}
a_1{:}0 \\
a_2{:}0 \\
a_3{:} -yz^2 \\
a_4{:}\ -x \qquad\qquad r \\
\hline
-y^2z^2 + x^3 \\
\underline{y^2z^2 - xyz^3} \\
x^3 - xyz^3 \\
\underline{-x^3 + xyz^3} \\
0 \longrightarrow 0
\end{array}
$$

$f_5 = -y^2z^2 + x^3$ Pasa a ser parte de la base.

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2, -y^2z^2 + x^3\}$$

Ahora encontraremos el S-Polinomio de f_1, f_5 con $x^\rho = -y^2z^4$

$$S(f_1, f_5) = \left[\frac{-y^2z^4}{-z^4}\right](-z^4 + x) - \left[\frac{-y^2z^4}{-y^2z^2}\right](-y^2z^2 + x^3)$$

$$S(f_1, f_5) = (y^2)(-z^4 + x) - (z^2)(-y^2z^2 + x^3)$$

$$S(f_1, f_5) = -y^2z^4 + xy^2 + y^2z^4 - x^3z^2$$

$$S(f_1, f_5) = -x^3z^2 + xy^2 = (x^2z + xy)f_3$$

$$[illegible]^F = 0$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

a_1:0
a_2:0
a_3:$x^2z + xy$
a_4: 0
a_5: 0 r

$f_1 = -z^4 + x$
$f_2 = -z^5 + y$
$f_3 = -xz + y$
$f_4 = yz^3 - x^2$
$f_5 = -y^2z^2 + x^3$

$-x^3z^2 + xy^2$
$x^3z^2 - x^2yz$
$-x^2yz + xy^2$
$x^2yz - xy^2$
$0 \longrightarrow 0$

Por lo tanto

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2, -y^2z^2 + x^3\}$$

Ahora encontraremos el S-Polinomio de f_2, f_5 con $x^\rho = y^2z^5$

$$S(f_2, f_5) = \left[\frac{y^2z^5}{-z^5}\right](-z^5 + y) - \left[\frac{y^2z^5}{-y^2z^2}\right](-y^2z^2 + x^3)$$

$$S(f_2, f_5) = (-y^2)(-z^5 + y) - (-z^3)(-y^2z^2 + x^3)$$

$$S(f_2, f_5) = y^2z^5 - y^3 - y^2z^5 + x^3z^3$$

$$S(f_2, f_5) = x^3z^3 - y^3 = (x^2z^2 + xyz + y^2)f_3$$

$$S(f_2, f_5)^F = 0$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

a_1:0
a_2:0
a_3: $-x^2z^2 - xyz - y^2$
a_4: 0
a_5: 0 $\quad r$

$f_1 = -z^4 + x$
$f_2 = -z^5 + y$
$f_3 = -xz + y$
$f_4 = yz^3 - x^2$
$f_5 = -y^2z^2 + x^3$

$$x^3z^3 - y^3$$
$$-x^3z^3 + x^2yz^2$$
$$x^2yz^2 - y^3$$
$$-x^2yz^2 + xy^2z$$
$$xy^2z - y^3$$
$$-xy^2z + y^3$$
$$0 \longrightarrow 0$$

Por lo tanto

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2, -y^2z^2 + x^3\}$$

Ahora encontraremos el S-Polinomio de f_3, f_5 con $x^\rho = xy^2z^2$

$$S(f_3, f_5) = \left(\frac{xy^2z^2}{-xz}\right)(-xz + y) - \left(\frac{xy^2z^2}{-y^2z^2}\right)(-y^2z^2 + x^3)$$

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

$$S(f_3, f_5) = xy^2z^2 - y^3z - xy^2z^2 + x^4$$

$$S(f_3, f_5) = x^4 - y^3z$$

$$\overline{S(f_3, f_5)}^F = f_6$$

Comprobaremos con el algoritmo de la división si nuestro f_6 pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l}
f_1 = -z^4 + x \\
f_2 = -z^5 + y \\
f_3 = -xz + y \\
f_4 = yz^3 - x^2 \\
f_5 = -y^2z^2 + x^3
\end{array}
\qquad
\begin{array}{r|l}
 & a_1:0 \\
 & a_2:0 \\
 & a_3:-y^2z \\
 & a_4:\ 0 \\
 & a_5:\ x \qquad\qquad r \\
\hline
x^4 - y^3z & \\
y^3z - xy^2z^2 & \\
\hline
x^4 - xy^2z^2 & \\
-x^4 + xy^2z^2 & \\
\hline
0 \longrightarrow & 0
\end{array}
$$

Por lo tanto $f_6 = x^4 - y^3z$ pasa a ser parte de la base.

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2, -y^2z^2 + x^3, x^4 - y^3z\}$$

Ahora encontraremos el S-Polinomio de f_4, f_5 con $x^\rho = y^2z^3$

$$S(f_4, f_5) = \left[\frac{y^2z^3}{yz^3}\right](yz^3 - x^2) - \left[\frac{y^2z^3}{-y^2z^2}\right](-y^2z^2 + x^3)$$

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

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

$$S(f_4, f_5) = x^3z - x^2y = (-x^2)f_3$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

a_1:0
a_2:0
a_3: $-x^2$
a_4: 0
a_5:0
a_6: 0

$f_1 = -z^4 + x$
$f_2 = -z^5 + y$
$f_3 = -xz + y$
$f_4 = yz^3 - x^2$
$f_5 = -y^2z^2 + x^3$
$f_6 = x^4 - y^3z$

$x^3z - x^2$
$-x^3z + x^2$
0 → 0 r

$(0,0,0,0,0,0)^F = 0$ no pasa a ser parte de la base

Ahora encontraremos el S-Polinomio de f_1, f_6 con $x^\rho = x^4z^4$

$$S(f_1, f_6) = \left[\frac{x^4z^4}{-z^4}\right](-z^4 + x) - \left[\frac{x^4z^4}{x^4}\right](x^4 - y^3z)$$

$$S(f_1, f_6) = (-x^4)(-z^4 + x) - (z^4)(x^4 - y^3z)$$

$$S(f_1, f_6) = x^4z^4 - x^5 - x^4z^4 + y^3z^5$$

$$S(f_1, f_6) = -x^5 + y^3z^5$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l|l|l}
 & a_1{:}0 & \\
 & a_2{:}0 & \\
 & a_3{:}-x^2 & \\
 & a_4{:}\ 0 & \\
 & a_5{:}0 & \\
 & a_6{:}\ -z^4 & r \\
\hline
f_1 = -z^4 + x & -x^5 + y^3 z^5 & \\
f_2 = -z^5 + y & x^5 - x^4 z^4 & \\
\cline{2-2}
f_3 = -xz + y & -x^4 z^4 + y^3 z^5 & \\
f_4 = yz^3 - x^2 & x^4 z^4 - y^3 z^5 & \\
\cline{2-2}
f_5 = -y^2 z^2 + x^3 & 0 \longrightarrow & 0 \\
f_6 = x^4 - y^3 z & &
\end{array}
$$

$\overline{(\ldots)}^F = 0$ no pasa a ser parte de la base.

Ahora encontraremos el S-Polinomio de f_2, f_6 con $x^\rho = x^4 z^5$

$$S(f_2, f_6) = \left[\frac{x^4 z^5}{-x^5}\right](-z^5 + y) - \left[\frac{x^4 z^5}{x^4}\right](x^4 - y^3 z)$$

$$S(f_2, f_6) = (-x^4)(-z^5 + y) - (z^5)(x^4 - y^3 z)$$

$$S(f_2, f_6) = x^4 z^5 - x^4 y - x^4 z^5 + y^3 z^6$$

$$S(f_2, f_6) = -x^4 y + y^3 z^6 = y(-x^4 + y^2 z^6) = y(-x^2 - yz^3) f_4$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l}
f_1 = -z^4 + x \\
f_2 = -z^5 + y \\
f_3 = -xz + y \\
f_4 = yz^3 - x^2 \\
f_5 = -y^2z^2 + x^3 \\
f_6 = x^4 - y^3z
\end{array}
\qquad
\begin{array}{l}
a_1 : -x^3y \\
a_2 : 0 \\
a_3 : x^2yz^3 \\
a_4 : y^2z^3 \\
a_5 : 0 \\
a_6 : 0
\end{array}
\qquad
\begin{array}{|l}
\hline
-x^4y + y^3z^6 \\
\underline{x^4y - x^3yz^4} \\
y^3z^6 - x^3yz^4 \\
\underline{-y^3z^6 + x^2y^2z^3} \\
-x^3yz^4 + x^2y^2z^3 \\
\underline{x^3yz^4 - x^2y^2z^3} \\
0 \longrightarrow 0
\end{array}
\qquad r
$$

$\overline{S(f_3,f_6)}^F = 0$ no pasa a ser parte de la base.

Ahora encontraremos el S-Polinomio de f_3, f_6 con $x^\rho = x^4z$

$$S(f_3,f_6) = \left[\frac{x^4z}{-xz}\right](-xz+y) - \left[\frac{x^4z}{x^4}\right](x^4 - y^3z)$$

$$S(f_3,f_6) = (-x^3)(-xz+y) - (z)(x^4 - y^3z)$$

$$S(f_3,f_6) = x^4z - x^3y - x^4z + y^3z^2$$

$$S(f_3,f_6) = -x^3y + y^3z^2$$

$$S(f_3,f_6) = y(-x^3 + y^2z^2) = yf_5$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

a_1:0
a_2:0
a_3:0
a_4:0
a_5:$-y$
a_6: 0

$f_1 = -z^4 + x$
$f_2 = -z^5 + y$
$f_3 = -xz + y$
$f_4 = yz^3 - x^2$
$f_5 = -y^2z^2 + x^3$
$f_6 = x^4 - y^3z$

r

$-x^3y + y^3z$
$x^3y - y^3z$
0 → 0

$\overline{(f_4,f_6)}^F = 0$ no pasa a ser parte de la base.

Ahora encontraremos el S-Polinomio de f_4, f_6 con $x^\rho = x^4yz^3$

$$S(f_4,f_6) = \left[\frac{x^4yz^3}{yz^3}\right](yz^3 - x^2) - \left[\frac{x^4yz^3}{x^4}\right](x^4 - y^3z)$$

$$S(f_4,f_6) = (x^4)(yz^3 - x^2) - (yz^3)(x^4 - y^3z)$$

$$S(f_4,f_6) = x^4yz^3 - x^6 - x^4yz^3 + y^4z^4$$

$$S(f_4,f_6) = -x^6 + y^4z^4$$

$$S(f_4,f_6) = (-x^3 - y^2z^2)f_5$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l}
f_1 = -z^4 + x \\
f_2 = -z^5 + y \\
f_3 = -xz + y \\
f_4 = yz^3 - x^2 \\
f_5 = -y^2z^2 + x^3 \\
f_6 = x^4 - y^3z
\end{array}
\qquad
\begin{array}{l}
a_1{:}0 \\
a_2{:}0 \\
a_3{:}0 \\
a_4{:}0 \\
a_5{:} -x^3 - y^2z^2 \\
a_6{:}\ 0 \qquad\qquad r \\
\hline
-x^6 + y^4z^4 \\
\underline{x^6 - x^3y^2z^{\,2}} \\
-x^3y^2z^2 + y^4z^4 \\
\underline{x^3y^2z^2 - y^4z^4} \\
0 \longrightarrow\ 0
\end{array}
$$

$(\quad)^F = 0$ no pasa a ser parte de la base.

Ahora encontraremos el S-Polinomio de f_5, f_6 con $x^\rho = x^4y^2z^2$

$$S(f_5, f_6) = \left[\frac{x^4y^2z^2}{-y^2z^2}\right](-y^2z^2 + x^3) - \left[\frac{x^4y^2z^2}{x^4}\right](x^4 - y^3z)$$

$$S(f_5, f_6) = (-x^4)(-y^2z^2 + x^3) - (y^2z^2)(x^4 - y^3z)$$

$$S(f_5, f_6) = x^4y^2z^2 - x^7 - x^4y^2z^2 + y^5z^3$$

$$S(f_5, f_6) = -x^7 + y^5z^3$$

Comprobaremos con el algoritmo de la división si pasa a ser parte de la Base de Gröbner.

$$
\begin{array}{l}
f_1 = -z^4 + x \\
f_2 = -z^5 + y \\
f_3 = -xz + y \\
f_4 = yz^3 - x^2 \\
f_5 = -y^2z^2 + x^3 \\
f_6 = x^4 - y^3z
\end{array}
\qquad
\begin{array}{l}
a_1{:}0 \\
a_2{:}0 \\
a_3{:}0 \\
a_4{:}0 \\
a_5{:} -x^4 \\
a_6{:}\, y^2z^2 \qquad\qquad r \\
\hline
-x^7 + y^5z^3 \\
x^7 - x^4y^2z^2 \\
\hline
-x^4y^2z^2 + y^5z^3 \\
x^4y^2z^2 - y^5z^3 \\
\hline
0 \longrightarrow 0
\end{array}
$$

$F = 0$ no pasa a ser parte de la base.

$$F = \{-z^4 + x, -z^5 + y, -xz + y, yz^3 - x^2, -y^2z^2 + x^3, x^4 - y^3z\}$$

Esta es mi Base de Gröbner.

Comprobando el ejemplo en el CoCoA:

```
Use R ::= QQ[x,y,z];

I := Ideal(x-z^4,y-z^5);

Describe I;

GBasis(I);
```

```
Record[Type := IDEAL, Value := Record[Gens := [-z^4 + x, -z^5 + y]]]

[-z^4 + x, -xz + y, yz^3 - x^2, -y^2z^2 + x^3, x^4 - y^3z]
```

9.4.2 Ceros de Hilbert

Definición 40. Los Ceros de Hilbert

Sea una variedad $V \subseteq K^n$ y un ideal I, consideremos

$$\begin{array}{ccc} Varieda\,afines & & Ideales \\ V & \longmapsto & I(V) \end{array}$$

Recíprocamente dado un ideal $I \subseteq K[x_1, \cdots, x_n]$, definimos el conjunto;

$$V(I) = \{x \in K^n : f(x) = 0 \ \forall f \in I\}$$

El teorema de la Base de Hilbert asegura que $V(I)$ es una variedad afin por que existe un conjunto finito de polinomios $f_1, \cdots, f_s \in I : I = \langle f_1, \cdots, f_s \rangle$, donde $V(I)$ es el conjunto de raíces comunes de estos polinomios por consiguiente tenemos el mapeo:

$$\begin{array}{ccc} Ideales & & Variedades\,afín \\ I & \longmapsto & V(I) \end{array}$$

Los mapeos anteriores dan una correspondencia entre Ideales y Variedades, pero dicho mapeo no es uno a uno, es decir Ideales diferentes pueden corresponder a la misma variedad.

Ejemplo 41.

Si $\langle x \rangle, \langle x^2 \rangle$ son ideales diferentes en $K[x]$ que tienen la misma variedad $V(x) = V(x^2) = \{0\}$, ahora consideremos $1, 1 + x^2, 1 + x^2 + x^4 \in K[x]$ que generan ideales diferentes.

$$I_1 = \langle 1 \rangle = R[x] , I_2 = \langle 1 + x^2 \rangle, I_3 = \langle 1 + x^2 + x^4 \rangle$$

Pero cada polinomio no tiene raíces reales, siendo sus variedades correspondientes vacías.

$$V\ I_1\ = V\ I_2\ = V\ I_3\ = \square$$

En cualquier anillo de polinomios, basta la clausura algebraica para garantizar que el único ideal que representa la variedad vacía es el mismo anillo. Esto es el **Nullstellensatz Débil**, el cual es base de unos de los resultados matemáticos más celebrado del siglo XIX. **El Nullstellensatz de Hilbert,** tal fue su impacto que aún se usa la palabra típica en Alemán **Null (=cero), Stellen (=lugares), Satz (=Teorema).**

9.4.3 Sistemas de Ecuaciones Polinomiales y Variedades

Teorema 42. Los ceros de Hilbert (El Nullstellensatz de Hilbert)

El teorema de los cero de Hilbert representa el borde de la moneda cuyas caras son el álgebra conmutativa y la Geometría Algebraica, es la herramienta fundamental para el traslado de la Geometría Algebraica al lenguaje de Algebra Conmutativa y viceversa. Este Teorema prevé la conexión entre las variedades de un conjunto de polinomios y el ideal polinomial definidos por ellos.

Teorema 43. El Nullstellensatz Débil

Sea K un campo algebraicamente cerrado e I, un ideal con $V\ I\ = \square$, entonces $I = K\ x_1, \cdots, x_n$.

Demostración. Para probar que $I = K\ x_1, \cdots, x_n$ la estrategia es mostrar que el polinomio constante 1 está en I, porque si $1 \square I$, entonces por la definición de ideal $f = f \cdot 1 \square I \square f \square K\ x_1, \cdots, x_n$. Entonces saber que $1 \square I$ es suficiente para probar que I es $t \square K\ x_1, \cdots, x_n$ todo el anillo.

La prueba es por inducción sobre n, el número de variables. Si $n = 1$, $I \subset K[x]$ satisface que $V(I) = \emptyset$.

Supongamos ahora que se cumple para el anillo de polinomios en $n-1$ variables en $K[x_1, \cdots, x_n]$. Sea $I = \langle f_1, \ldots, f_s \rangle$ un ideal en $K[x_1, \cdots, x_n]$ con $V(I) = \emptyset$. Asumamos que f_1 no es constante porque de lo contrario no habría nada que probar. Supongamos que el grado total de f_1 es $N \geq 1$, podemos asumir también f_1 tiene la forma:

$$f_1(x_1, \cdots, x_n) = cx_1^N + \text{términos en } x_1 \text{ con grado } < N,$$

Donde $c \neq 0$ es una constante. Consideremos el cambio lineal de coordenadas

$$\begin{aligned} x_1 &= \bar{x}_1 \\ x_2 &= \bar{x}_2 + a_2\bar{x}_1 \\ &\vdots \\ x_n &= \bar{x}_n + a_n \end{aligned}$$

Donde los a_i son constante en K que deben determinarse. Si sustituimos $x_1, \ldots, x_n, f_1$ adquiere la forma.

$$\begin{aligned} f_1(x_1, \cdots, x_n) &= f_1(\bar{x}_1, \bar{x}_2 + a_2\bar{x}_1, \cdots, \bar{x}_n + a_n\bar{x}_1 \\ &= c(a_1, \cdots, a_n)\bar{x}_1^N + \text{términos en } x_1 \text{con grado} < N \end{aligned}$$

Donde $c(a_1, \cdots, a_n)$ es una expresión polinomial no nula en $a_1, \cdots, a_n$, por definición de polinomios antes de proseguir probemos que K es un campo algebraicamente cerrado es infinito.

Sea K un campo algebraicamente cerrado. Supongamos que K es finito, digamos $K = \{a_1, \cdots, a_n\}$, formemos el siguiente sistema de polinomios de $K[x]$.

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) + 1$$

Observemos que el polinomio así formado no tiene ninguna raíz en K puesto que:

$$f(\alpha_1) = (\alpha_1 - \alpha_1)(\alpha_1 - \alpha_2)\cdots(\alpha_1 - \alpha_n) + 1$$

$$f(\alpha_1) = 0\,(\alpha_1 - \alpha_2)\cdots(\alpha_1 - \alpha_n) + 1 = 0 + 1 = 1 \neq 0$$

$$f(\alpha_2) = (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_2)\cdots(\alpha_2 - \alpha_n) + 1$$

$$f(\alpha_2) = (\alpha_2 - \alpha_1)\,0\cdots(\alpha_2 - \alpha_n) + 1 = 0 + 1 = 1 \neq 0$$

$$f(\alpha_n) = (\alpha_n - \alpha_1)(\alpha_n - \alpha_2)\cdots(\alpha_n - \alpha_n) + 1$$

$$f(\alpha_n) = (\alpha_n - \alpha_1)(\alpha_n - \alpha_2)\cdots 0 + 1 = 0 + 1 = 1 \neq 0$$

Lo cual contradice el hecho de que K es algebraicamente cerrado. Por tanto K es infinito, así podemos tomar $(a_1, \cdots, a_n)$ con $c(a_1, \cdots, a_n) \neq 0$.

Con esta escogencia de $(a_1, \cdots, a_n)$ bajo el cambio de coordenadas todo polinomio $f \in K[x_1, \cdots, x_n]$ se trasformara en el polinomio $\bar{f} \in K[\bar{x}_1, \cdots, \bar{x}_n]$, $0 \in \bar{I}$ por como I es un ideal $0 \in I$, y el polinomio que le corresponda a este mediante el cambio de coordenadas es el polinomio $\sum_\alpha 0_\alpha \bar{x}^\alpha$ y este polinomio nulo del anillo $K[\bar{x}_1, \cdots, \bar{x}_n]$, a saber el polinomio 0 sea $\bar{f} \in \bar{I}$ y $\bar{g} \in \bar{I}$.

Sean ahora $\bar{f} \in \bar{I}$ y $\bar{g} \in K[\bar{x}_1, \cdots, \bar{x}_n]$, implica que $f \in I$ y $g \in K[x_1, \cdots, x_n]$ como I es un ideal de $K[x_1, \cdots, x_n]$ tenemos que $fg \in I$ y asi $\overline{fg} = \bar{f}\bar{g} \in \bar{I}$. Observamos que todavía $V(\bar{I}) = \emptyset$ por que si las ecuaciones tuviesen solución también tendrían las originales. Además si podemos probar que $1 \in \bar{I} \Longrightarrow 1 \in I$ se seguirá del hecho de que las constante no son afectadas por la operación $\bar{\cdot}$

De ahí es suficiente probar que $1 \in \bar{I}$, $f_1 \in I$ se trasforma en $\bar{f}_1 \in \bar{I}$ con la propiedad que:

$$\bar{f}_1(\bar{x}_1, \cdots, \bar{x}_n) = c(a_1, \cdots, a_n)\,\bar{x}_1^N + \text{términos en } x_1 \text{ con grado} < N$$

Donde $c\ a_1, \cdots, a_n \neq 0$. Esta observación nos permite relacionar $V\ \bar{I}$ con su proyección en el subespacio de K^n con coordenadas $\bar{x_1}, \cdots, \bar{x_n}$. Sea

$$\pi_1 = K^n \rightarrow K^{n-1}$$

El mapeo sobre las últimas $n-1$ componentes, si hacemos $\bar{I}_1 \cap K\ \bar{x_2}, \cdots, \bar{x_n}$ se establece que:

$$V\ I_1 = \pi_1(V\ \bar{I}_1)$$

Esto implica que:

$$V\ \bar{I}_1 = \pi_1\ V\ \bar{I}_1 = \square$$

Por la hipótesis de inducción se sigue que $\bar{I}_1 = K\ \bar{x_2}, \cdots, \bar{x_n}$, pero esto implica que $1 \square \bar{I}_1 \square \bar{I}_1$ por tanto $I = K\ x_1, \cdots, x_n$.

Inspirados por el **Nullstellensatz Débil** uno podría esperar que la correspondencia entre ideales y variedades a fines de uno a uno si nos restringimos solamente a los campos algebraicamente cerrados. En el ejemplo de $V\ x = V\ x^2 = 0$ es válido en cualquier campo, similarmente los ideales $\square x^2, y\square, \square x, y\square$ (y el caso más general $\square x^n, y^m\square\ \square n, m \square$ $\square_{>1}$) son diferentes pero definen la misma variedad: $0,0 \square k^n$. Estos ejemplos ilustran una razón básica del porque ideales diferentes pueden definir la misma variedad porque una potencia de un polinomio se anula en el mismo conjunto que el polinomio original.

El Nullstellensatz de Hilbert establece que en un campo algebraicamente cerrado, esta es la única razón para que ideales diferentes den la misma variedad: si un polinomio f se anula en todos los puntos de una variedad $V(I)$, entonces alguna potencia de f debe pertenecer a I.

Teorema 44. El Nullstellensatz de Hilbert.

Sea K un campo algebraicamente cerrado. Si $f_1, \cdots, f_s \in K[x_1, \cdots, x_n]$ son tales que $f \in I(V(f_1, \cdots, f_s))$, entonces existe un entero $m \geq 1$ tal que:

$$f^m \in \langle f_1, \cdots, f_s \rangle$$

(y recíprocamente).

Definición 45. Espacio afín

Sea K un campo y $n \in \mathbb{Z}^+$, entonces definimos el **espacio afín** $n-$dimencional sobre K como $K^n = \{(a_1, \cdots, a_n) : a_1, \cdots, a_n \in K\}$.

Los polinomios pueden expresarse también como funciones, estableciéndose una conexión interesante entre los polinomios y el espacio afín. Si $f = \sum_{\alpha \in \mathbb{Z}^+ n} c_\alpha t_\alpha$ pertenece al anillo de polinomios $K[x_1, \cdots, x_n]$ sobre un campo K, podemos evaluar f en cada punto de K^n obteniendo una función $f: K^n \to K$, definida así: $(a_1, \cdots, a_n) \in K^n$, reemplazamos cada x_i por a_i en la expresión para f. Como todos los coeficientes de f pertenecen a K, entonces $f(a_1, \cdots, a_n) \in K$.

El hecho de considerar a un polinomio como una función es lo que hace posible establecer relaciones entre el álgebra y la geometría.

Definición 46. Variedades Algebraicas

Dado un conjunto de polinomios $A = \{f_i\}_{i \in I} \subseteq R = K[x_1, \cdots, x_n]$, la variedad algebraica determinada por A, $V(A) \subseteq K^n$, se define como el conjunto de todas aquellas n- uplas que son ceros comunes a todos los polinomios de A. Es decir

$$V(A) = \{\alpha = (\alpha_1, \cdots, \alpha_n) \in K^n : f_i(\alpha) = 0, \forall f_i \text{ en } A\}.$$

Observaciones 47.

1. $V(A) = V(I)$ donde I es el ideal de R generado por A. Primero, observemos que si $A \subseteq B$ entonces se tiene que $V(B) \subseteq V(A)$. En el caso en el que $B = I$ se tiene también la contención en el sentido contrario ya que si α es un cero común de todos los polinomios de A también lo es de cualquier elemento que sea una combinación lineal de elementos de A con coeficiente en R.

2. Para todo par de ideales $I, J \text{ en } R$ se tiene que $V(I) \cap V(J) = V(I \cdot J)$ y que $V(I) \cup V(J) = V(I + J)$. Aquí I, J denota el conjunto de todos los elementos que son sumas de productos de elementos de I y J. Como I, J está incluido en I, y en J entonces $V(I, J)$ deberá estar incluido en $V(I)$ y en $V(J)$. Esto prueba la inclusión $V(I) \cap V(J) \subseteq V(I \cdot J)$. Ahora si $\theta \in V(I) \cap V(J)$ se tiene que θ debe ser un cero común a todos los elementos de I y J, y por lo tanto de cualquier suma $\sum = \sum f_i g_i \text{ con } f_i \in I \text{ y } g_i \in J$. Esto demuestra la otra inclusión. La demostración de la otra igualdad es similar.

3. Por el teorema de la Base de Hilbert vemos que existen $f_1, \cdots, f_n \in I$ tales que $V(A) = V(f_1, \cdots, f_n) = V(f_1) \cap V(f_2) \cap \cdots \cap V(f_n)$, de donde se ve que cada variedad algebraica se puede expresar la intersección de hipersuperficies en K^n.

Teorema 48. Sea $X \subseteq K^n$ una variedad algebraica. Entonces X es irreducible si y solo si su anillo coordenado, $K[X]$ es un dominio entero.

Demostración:

Supongamos que X esta definida como el conjunto de ceros de un cierto ideal $I \subseteq R = K[x_1, \cdots, x_n]$, y que X es irreducible. Sean $f, g \in K[X]$ dos funciones polinomicas tales que $f \cdot g = 0$ en $K[X]$. Definamos $X_1 = V(I + Rf)$ y $X_1 = V(I + Rg)$. Para cada $\alpha \in X$ se tiene que $f(\alpha) = 0$ o $g(\alpha) = 0$, luego $\alpha \in X_1$ o $\alpha \in X_2$, de donde se deduce que X es la unión de X_1 y X_2. Como X es irreducible se tiene que $X_1 = X$ o $X_2 = X$. La primera igualdad nos dice que f es idénticamente cero sobre X, es decir, $f = 0$ en $K[X]$ es un dominio entero. ■

Definición 49. Variedad afín

El conjunto de todas las soluciones simultáneas $a_1, \cdots, a_n \in K^n$ del sistema de ecuaciones:

$$\begin{matrix} f_1\ x_1, \cdots, x_n = 0 \\ f_2\ x_1, \cdots, x_n = 0 \\ \vdots \\ f_s\ x_1, \cdots, x_n = 0 \end{matrix},$$

Recibe el nombre de **variedad afín** definida por $f_1, \cdots, f_s$, y se denota por $V\ f_1, \cdots, f_s$. Un subconjunto $V \subset K^n$ es una variedad afín si $V = V\ f_1, \cdots, f_s$ para alguna colección de polinomios $f_i \in K\ x_1, \cdots, x_n$ esto es,

$$V\ f_1, \cdots, f_s = a_1, \cdots, a_n \in K^n : f\ a_1, \cdots, a_n = 0, 1 \leq i \leq s\ .$$

Una variedad puede describirse por diferentes sistemas de ecuaciones. Observemos que si

$g = p_1 f_1 + p_2 f_2 + \cdots + p_s f_s$ donde $p_i \in K\ x_1, \cdots, x_n$, $1 \leq i \leq s$,

Son polinomios cualesquiera, entonces $g\ a_1, \cdots, a_n = 0$ para todo $a_1, \cdots, a_n \in V\ f_1, \cdots, f_s$. Así, dado cualquier conjunto de ecuaciones que definen una variedad, podemos siempre producir un número infinito de polinomios adicionales que también se anulara en dicha variedad. Estos polinomios adicionales, como en el caso de g, son elementos del ideal $\langle f_1, \cdots, f_s \rangle$. Además una colección de estos nuevos polinomios puede definir la misma variedad que los $f_1, \cdots, f_s$.

Tomando en cuenta lo anterior, junto con el teorema de las Bases de Hilbert, podemos pensar en una variedad como algo definido por un ideal en $K\ x_1, \cdots, x_n$, más que por un sistema especifico de ecuaciones. Si queremos pensar en una variedad en el sentido anterior, la podemos denotar por $V = V\ I$, donde $I \subset K\ x_1, \cdots, x_n$ es el ideal en consideración.

Ahora, dada una variedad $V \subseteq K^n$, podemos también tratar de regresarnos en la construccuion de la variedad V de un ideal, considerando la colección entera de polinomios que se anula en cada punto de V.

El conjunto de $K^n = \{(a_1, \cdots, a_n) : a_1, \cdots, a_n \in K\}$ el espacio afin $n-$dimensional sobre K, y vimos que cada polinomio $f \in K[x_1, \cdots, x_n]$ define una función $f: K^n \to K$. Es decir al evaluar f en $(a_1, \cdots, a_n) \in K^n$, por la sustitución de $x_i = a_i$, la expresión que resulta esta en K.

Notemos que cualquier ecuación $p = q$, donde $p = q \in K[x_1, \cdots, x_n]$, puede ser reescrita como $p - q = 0$, así que es usual escribir todas las ecuaciones en la forma $f = 0$ Y siempre haremos esto. Para generalizar, podríamos considerar las ecuaciones simultáneas de un sistema de ecuaciones Polinomiales.

Ideales y variedades afines

Tratemos ahora de establecer la relación que existe entre ideales y variedades a fines.

Una variedad puede describirse por diferentes tipos de ecuaciones. Observemos que si $g = p_1 f_1 + p_2 f_2 + \cdots + p_s f_s$, donde $p_i \in K[x_1, \cdots, x_n], 1 \leq i \leq s$, son polinomios cualquiera, entonces $g(a_1, \cdots, a_n) = 0$ para todo $(a_1, \cdots, a_n) \in v(f_1, \cdots, f_s)$. Así, dado cualquier conjunto de ecuaciones que definen una variedad, podemos siempre producir un número infinitos de polinomios adicionales que también se anularan en dicha variedad. Estos polinomios adicionales como en el caso de g, son elementos de ideal $\langle f_1, \cdots, f_s \rangle$. Ademas una colección de estos nuevos polinomios puede definir la misma variedad de los $f_1, \cdots, f_s$.

Tomando en cuenta lo anterior, junto con el teorema de las Bases de Hilbert, podemos pensar como en una variedad algo definido por un ideal en $I \subseteq K[x_1, \cdots, x_n]$, más que por un sistema específico de ecuaciones. Si queremos pensar en una variedad en el sentido anterior, la podemos denotar por $v = V(I)$, donde $I \subseteq K[x_1, \cdots, x_n]$ es el ideal en consideración.

Proposición 50.

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

a) $V \subseteq W$ si y solo si $I(V) \supseteq I(W)$

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

Observaciones 51. Las primeras claves en la relación entre ideales y variedades están resumidas en los siguientes teoremas:

a) Versión fuerte de los ceros de Hilbert: Si K es un campo algebraicamente cerrado e I es un ideal en $K[x_1, \cdots, x_n]$, entonces $I(V(I)) = \sqrt{I}$.

b) Correspondencia ideal -Variedad : Sea K un campo arbitrario los mapeos

Variedad afines $\rightarrow$ **Ideales** (I)

e

Ideales $\rightarrow$ **Variedades a fines** (V)

Invierte las inclusiones y $I(V(I)) = V$ para toda variedad afin V. Si K es algebraicamente cerrado entonces

Variedad afines $\rightarrow$ **Ideales Radicales** (I)

e

Ideales Radicales $\rightarrow$ **Variedades a fines** (V)

Invierte las funciones (como una función uno a uno) y son inversos mutuamente.

Propiedades 52. Sea K un campo algebraicamente cerrado $V, W \subseteq K^n$ variedades y sean $I, J \subseteq K[x_1, \cdots, x_n]$ 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. $V(I \cap J) = V(I) \cup V(J)$

4. $V(I \cap J) = V(I) \cap V(J)$

5. $I(I \cap J) = I(I) \cap I(J)$

6. $I(I \cap J) = \sqrt{I(I) + I(J)}$

9.4.4 Número de soluciones

Los sistemas de ecuaciones polinomiales aparecen en muchos modelos matemáticos de sistemas físicos, en el estudio de estructuras algebraicas y en la descripción algebraica de objetos geométricos, robótica.

Es ahí donde radica la importancia de resolver dichos sistemas, pero antes de entrar al método de solución, necesitamos saber el límite de soluciones distintas y el número exacto de soluciones. Para ello introduciremos un nuevo concepto de algebra cociente.

Básicamente lo que se pretende hacer es que, dado un ideal I y la Base de Gröbner G asociada a dicho ideal, el número de soluciones distintas es la cardinalidad del conjunto $B = \{x^\alpha : x^\alpha \notin \langle tp(I) \rangle\}$.

Lema 53. Lema de Dickson: Sea $n \geq 1$, y sea $t_1, t_2, \cdots$ una sucesión de términos en $\mathbb{T}^n$. Entonces existe un número $N > 0$ tal que para $i > N$ el termino t_i es un múltiplo de uno de los términos $t_1, \cdots, t_N$, es decir, el monoideal $\langle t_1, \cdots, t_N \rangle \subseteq \mathbb{T}^n$ es generado por $t_1, \cdots, t_N$.

En particular, para cada anillo A, el ideal $\langle t_1, \cdots, t_N \rangle \subset A[x_1, \cdots, x_n]$ es finitamente generado.

Demostración. Debemos probar que el monoideal $\langle t_1, \cdots, t_N \rangle \subset \mathbb{T}^n$ es finitamente generado, para ello verificamos primero que el mapeo $log: \mathbb{T}^n \to \mathbb{Z}^n$ dado por $x_1^{\alpha_1}, \cdots, x_n^{\alpha_n} \mapsto (\alpha_1, \cdots, \alpha_n)$ es un isomorfismo de monoides. La inyectividad del mapeo log se sigue claramente del hecho de que dos términos t_α y t_β en $\mathbb{T}^n$ son distintos si y solo si α y β son distintos. Por otro lado, para todo elemento $(\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n$ existe un único elemento t_α en $\mathbb{T}^n$, con lo cual se hace obvia la sobreyectividad de log. Observemos ahora que el monoideal $\langle log\ t_1, log\ t_2, \cdots \rangle \subset \mathbb{Z}^n$ es finitamente generado, dado que el monoide $(\mathbb{Z}^n, +)$ es notheriano. Entonces existe un número $N > 0$ tal que $\langle log\ t_1, log\ t_2, \cdots \rangle$ es generado por $log\ t_1, \cdots, log\ t_n$. En consecuencia, por la isomorfía $\mathbb{T}^n \cong \mathbb{Z}^n$, el monoideal $\langle t_1, \cdots, t_N \rangle \subset \mathbb{T}^n$ es generado por $t_1, \cdots, t_N$. ■

Ejemplo 54.

Sea $I = \langle xy^3 - x^2, x^3y^2 - y^1 \rangle \subset \mathbb{Z}[x, y]$ y usemos el orden Lexicográfico Graduado. Encontramos que

$$G = \{x^3y^2 - y^1, x^4 - y^2, xy^3 - x^2, y^4 - xy\}$$

Es una Base de Gröbner para I. En consecuencia $\langle tp(I) \rangle = \langle x^3y^2, x^4, xy^3, y^4 \rangle$, donde

$$\alpha(1) = (3,2) \quad \alpha(3) = (4,0)$$
$$\alpha(2) = (1,3) \quad \alpha(4) = (0,4)$$

Donde $\alpha(1), \alpha(2), \alpha(3), \alpha(4)$ son los grados de los términos principales de la base, ahora podemos graficar estos puntos en el plano cartesiano.

Este ejemplo esta construido manualmente y también utilizando los software Singular y Mathematica, también el CoCoA nos permite ver el límite de soluciones y el número de soluciones.

La salida del Singular

```
> LIB''graphics.lib'';

Ring r0=0,(x,y),ls;

Ideal I=x3y2,x4,xy3,y4;

Ataircase('' '',std(I));
```

Nos dará la entrada del Mathematica para obtener la grafica.

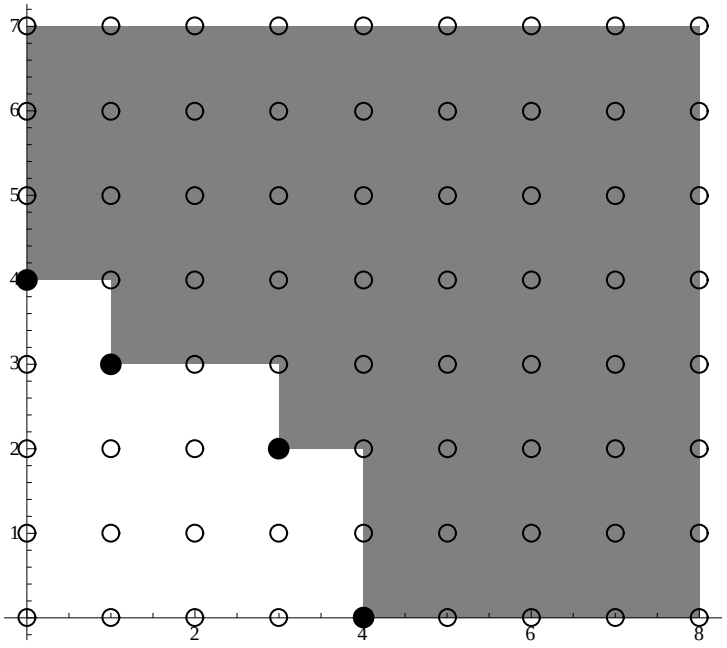
```
Show[Graphics[{{GrayLevel[0.5],

Map[Rectangle[#,{8,7}]&,{{3,2},{4,0},{1,3},{0,4}}]},

 PointSize 0.03 ,Map Point,  3,2 ,  4,0 ,  1,3 ,  0,4    ,

Table[Circle[{i,j},0.1],{i,0,8},{j,0,7}]},

Axes → True,AspectRatio → Automatic]]
```



Los elementos que están por debajo del área sombreada son todos los puntos que no pertenecen al ideal formado por los términos principales de I.

Dado cualquier $f \in \mathbb{K}[x,y]$, y por la proposición anterior tenemos que el residuo f^{-G} será una $\mathbb{K}-$combinacion lineal de los 12 monomios $1, x, x^2, x^3, y, xy, x^2y, x^3y, y^2, xy^2, x^2y^2, y^4$, lo cuales son los elementos que están por debajo del área sombreada. Se observa que todos los residuos pertenecen a un subespacio vectorial de $\mathbb{K}[x,y]$ de dimensión finita.

Lo que implica que el conjunto $B = \{1, x, x^2, x^3, y, xy, x^2y, x^3y, y^2, xy^2, x^2y^2, y^4\}$, este conjunto nos servirá para encontrar el límite de soluciones distintas.

Definición 55. Sea A un anillo, $n > 1$, $P = A[x_1, \cdots, x_n]$ un anillo polinomial y $r \geq 1$. Un P-submódulo $M \subseteq P^r$ es un **módulo monomial**, si tiene un sistema de generadores compuestos por elementos de $\mathbb{T}^n(e_1, \cdots, e_r)$. Un sub módulo monomial de P será denominado un **ideal monomial** de P.

Observación 56. Para ideales monomiales $I \subseteq A[x_1, \cdots, x_n]$, podemos ilustrar el conjunto de términos en I de la siguiente manera: Un término $x_1^i x_2^j \in \mathbb{T}^2$ se representan por medio del punto $(i,j) \in \mathbb{N}^2$. Entonces, para cada término $x_1^i x_2^j \in I$, el cuadrante $\{x_1^k, x_2^l \mid k \geq i, l \geq j\}$ está contenido en I.

Proposición 57. Limite para el número de soluciones Sean $f_1, \cdots, f_s \in P$-polinomios que generan al ideal cero-dimensional $I = \langle f_1, \cdots, f_s \rangle$. Entonces el sistema de ecuaciones $f_1(x_1, \cdots, x_n) = \cdots = f_s(x_1, \cdots, x_n) = 0$ tiene a lo sumo $dim_K\, P/I$ soluciones en $\overline{K}^n$.

Demostración. Dado $\bar{P} = \bar{K}\ x_1, \cdots, x_n$, las soluciones del sistema de ecuaciones polinomiales S se corresponden una a una con los ideales maximales en $\bar{P}$ que contienen a I$\bar{P}$. Sean $m_1, \cdots, m_t$ estos ideales son maximales. Asi podemos decir que

De donde obtenemos

$$dim_{\bar{K}}(\bar{P}/I\bar{P}) \geq dim_{\bar{K}}(\bar{P}/(m_1 \cap \cdots \cap m_t))$$

Para seguir con la demostración es necesario enunciar un teorema muy importante.

Teorema 58. Chino del Residuo.

Sea R un anillo y sean $I_1, \cdots, I_t$ ideales en R.

1. El mapeo canónico R-lineal $\varphi: R/(I_1, \cdots, I_t) \longrightarrow \prod_{i=1}^{t} R/I_i$ es inyevtivo.
2. Si los ideales $I_1, \cdots, I_t$ son maximales en pareja, es decir, si $I_i + I_j = R$ para $i \neq j$, entonces el mapeo φ es un isomorfismo de R- modulos.

Ahora podemos proseguir con la demostración. Por el teorema chino del residuo 1. Sabemos que

$$\bar{P}/(m_1 \cap \cdots \cap m_t) \square \prod_{i=1}^{t} \bar{P}/m_i,$$

Y además tenemos $\bar{P}/m_i \square \bar{K}$ para $i = 1, \cdots, t$. Finalmente obtenemos que

$$dim_{\bar{K}}(\bar{P}/I\bar{P}) \geq dim_{\bar{K}}(P/I).$$

En conjunto hemos conseguido

$$t = dim_{\bar{K}} \prod_{i=1}^{t} \bar{P}/m_i = dim_{\bar{K}}(\bar{P}/(m_1 \cap \cdots \cap m_t)) \leq dim_{\bar{K}}(\bar{P}/I\bar{P}) = dim_{\bar{K}}(P/I)$$

De donde

$$t \leq dim_K(P/I)$$

Que era la desigualdad que se quería llegar. ■

Ejemplo 59. Consideremos el siguiente sistema y encontremos el límite para el número de soluciones.

$$x^2 + y + z = 1$$
$$x + y^2 + z = 1$$
$$x + y + z^2 = 1$$

Para calcular el límite para el número de soluciones utilizaremos el CoCoA 4.7.4

Use R ::= QQ[x,y,z],DegRevLex;

I := Ideal(x^2+y+z-1,x+y^2+z-1,x+y+z^2-1);

J := Ideal (I);

Print "El ideal de términos principales es:";

LT(I);

Print "La base del módulo cociente está formada por:";

QuotientBasis(LT(J));

Print "Por tanto la dimensión del módulo cociente es:";

Len(QuotientBasis(LT(J)));

El ideal de términos principales es:

Ideal(z^2, y^2, x^2)

La base del módulo cociente está formada por:

[1, z, y, yz, x, xz, xy, xyz]

Por tanto la dimensión del módulo cociente es:

8

Donde el ideal de términos principales es $tp\ I = \langle z^2, y^2, x^2 \rangle$, asi que la dimensión $dim_{\mathbb{Q}}\ P/I = card\ B_{p/I} = cad\ \{1, z, y, yz, x, xz, xy, xyz\} = 8$, por lo tanto, 8 es el límite superior para el número de soluciones del sistema.

Definición 60. Radical de un ideal: Sea $I \subset K[x_1, \cdots, x_n]$ un ideal. El radical de I es el conjunto:

$$\sqrt{I} = \{g \in K[x_1, \cdots, x_n] : g^m \in I \ para\ algun\ m \geq 1\}$$

Un ideal se denomina un ideal radical si $\sqrt{I} = I$.

Teorema 61. Número exacto de soluciones

Sea I un ideal radical cero-dimensional en P, sea $\overline{K}$ la cerradura algebraica de K, y sea $\bar{P} = \overline{K}[x_1, \cdots, x_n]$. Si K es un campo perfecto, el número de soluciones del sistema de ecuaciones S es igual al número de ideales maximales de $\bar{P}$ que contiene a $I\bar{P}$, y este número es precisamente $dim_K\ P/I$.

Demostración. Podemos escribir $I = m_1 \cap \cdots \cap m_t$ con ideales maximales $m_1, \cdots, m_t$ de P, y escribimos también $m_i\bar{P} = \overline{m}_{i1} \cap \cdots \cap \overline{m}_{it}$, con ideales maximales $\overline{m}_{i1}, \cdots, \overline{m}_{it}$ de $\bar{P}$ para $i = 1, \cdots, t$. Entonces el Teorema chino del residuo tenemos

$$dim_K\ P/I = \sum_{i=1}^{t} dim_K\ P/m_i = \sum_{i=1}^{t} dim_{\overline{K}}\ \bar{P}/m\bar{P}$$

$$dim_K\ P/I = \sum_{i=1}^{t}\sum_{i=1}^{t} dim_{\overline{K}}(\bar{P}/\overline{m}_{ij}) = \sum_{i=1}^{t}\mu_i.$$

El número $\sum_{i=1}^{t}\mu_i$ es exactamente el número de ideales maximales de $\bar{P}$ que contienen a $I\bar{P}$, es decir, el número de soluciones de S. ■

Ejemplo 62. Retomemos el sistema de ecuaciones polinomiales del ejemplo 59:

$$x^2 + y + z = 1$$
$$x + y^2 + z = 1$$
$$x + y + z^2 = 1$$

Utilizaremos el CoCoA 4.7.4 para encontrar el número exacto de soluciones.

Use R ::= QQ[x,y,z],DegRevLex;

I := Ideal(x^2+y+z-1,x+y^2+z-1,x+y+z^2-1);

Print "El radical del ideal I es:";

Radical(I);

Print "La Base de Gröbner del radical de I es:";

RADI := Radical(I);

GBasis(RADI);

Print "El ideal de términos principales del radical de I es:";

LT(RADI);

Print "La base del módulo cociente está formada por:";

L := GBasis(RADI);

J := Ideal(L);

QuotientBasis(LT(J));

Print "Por tanto la dimensión del módulo cociente es:";

Len(QuotientBasis(LT(J)));

El radical del ideal I es:

Ideal(x^2 + y + z - 1, y^2 + x + z - 1, z^2 + x + y - 1, x^4 + x^3 - 3x^2 + x)

La Base de Gröbner del radical de I es:

[z^2 + x + y - 1, y^2 + x + z - 1, x^2 + y + z - 1, xy + xz - 2yz, -2xz + 2yz]

El ideal de términos principales del radical de I es:

Ideal(z^2, y^2, x^2, xy, xz)

La base del módulo cociente está formada por:

[1, z, y, yz, x]

Por tanto la dimensión del módulo cociente es:

5

Se observa que el número exacto de soluciones es 5.

9.4.5 Método de Autovalores

El problema central del trabajo se basa en encontrar las soluciones del sistema de ecuaciones polinomiales $f_1 = f_2 = \cdots = f_s = 0$. Sobre $\mathbb{K}$, es decir, encontrar los puntos de la variedad $V\ I$, donde I es el ideal generado por $f_1, \ldots, f_s$.

Dado un polinomio $f \in K\ x_1, \cdots, x_n$, podemos usar la multiplicación para definir un mapeo lineal m_f de $A = K\ x_1, \cdots, x_n\ /\ I$ en sí mismo. Mas precisamente, dado f y su clase $f \in A$, definimos $m_f : A \to A$ por la regla: si $g \in A$, entonces

$$m_f\ g = f \cdot g = fg \in A$$

Algunas propiedades de m_f están dadas de la siguiente proposición.

Proposición 63. Mapeo Lineal Sea $f \in \mathbb{K}\ x_1, \cdots, x_n$ entonces

1. El mapeo m_f es un **mapeo lineal** de A en A.
2. $m_f = m_g$ exactamente cuando $f - g \in I$. Por consiguiente, dos polinomios dan el mismo mapeo lineal si y sólo si difieren por un solo elemento de I. En particular, m_f es el mapeo nulo precisamente cuando $f \in I$.

Demostración. Para probar la parte a) usaremos la ley distributiva de la multiplicación sobre la adicción en el anillo A.

Si g , $\square \in A$ y $c \in \mathbb{K}$, entonces

$$m_f\ c\ f + \square = f \cdot c\ f + \square$$
$$m_f\ c\ f + \square = c\ f\ g + f\ \square$$
$$m_f\ c\ f + \square = cm_f\ f + m_f\ \square$$

Para la pate b) supongamos que $m_f = m_g$. Puesto que 1 es el idéntico multiplicativo en A, entonces

$$f = f \cdot 1 = m_f\ 1 = m_f\ 1 = g \cdot 1 = g$$

Por lo tanto $f = g$. ■

Puesto que A es un espacio vectorial sobre $\mathbb{K}$ de dimensión finita, podemos representar a m_f mediante una matriz con respecto a una base. Denotaremos esta matriz también como m_f.

Proposición 64. Sean $f, g \in A$. Entonces:

1. $m_{f+g} = m_f + m_g$
2. $m_{f \cdot g} = m_f \cdot m_g$ (donde el producto al lado derecho es la composición de operadores lineales o la matriz multiplicación).

Esta proposición dice que el mapeo que envía a $f \in K[x_1, \cdots, x_n]$ a la matriz m_f define un homomorfismo de anillos $\varphi \in K[x_1, \cdots, x_n]$ al anillo $M_{dxd}(K)$ de las matrices dxd, donde d es la dimensión de A como K-espacio vectorial.

Demostración. El homomorfismo de anillo está definido de la siguiente manera.

$$\varphi: K[x_1, \cdots, x_n] \longrightarrow M_{dxd}(K)$$

$$f \longrightarrow m_f$$

Por consiguiente,

$$m_{f+g} = \varphi(f + g) = \varphi(f) + \varphi(g) = m_f + m_g$$

Análogamente,

$$m_{f \cdot g} = \varphi(f \cdot g) = \varphi(f) \cdot \varphi(g) = m_f \cdot m_g \quad \blacksquare$$

Sea $x \in K[x] = \sum_{i=0}^{m} c_i x^i \in K[x]$ un polinomio. La expresión $f \in K[x_1, \cdots, x_n] = \sum_{i=0}^{m} c_i f^i$ es un elemento de $K[x_1, \cdots, x_n]$. Similarmente $m_f \in M_{dxd}(K) = \sum_{i=0}^{m} c_i (m_f)^i$ es una matriz bien definida, donde el término c_0 podría ser interpretado como $c_0 I$, donde I es la matriz identidad.

Corolario 65. Sea □ t y $f \in K[x_1, \cdots, x_n]$, entonces.

$$m_{h(f)} = \sqrt{(m_f)}$$

Donde el polinomio $f \in K[x_1, \cdots, x_n]$ da la clase f de A. Puesto que A es de dimensión finita, el conjunto $1, f, f^2, \cdots$ debe ser linealmente dependiente en la estructura de espacio vectorial de A, es decir existe una combinación lineal.

$$\sum_{i=0}^{m} c_i f^i = 0$$

En A, donde los $c_i \in K$ no son todos nulos. Por la definición de **anillo cociente**, esto es equivalente a decir que:

$$\sum_{i=0}^{m} c_i f^i \in I$$

Por lo tanto, $\sum_{i=0}^{m} c_i f^i$ se anula en cada punto de $V(I)$.

Sea $\sqrt{(t)} \in K[t]$ y sea $f \in K[x_1, \cdots, x_n]$. Por el corolario tenemos que,

$\sqrt{m_f} = 0 \Leftrightarrow \sqrt{f} = 0$

En A.

Los polinomios $\sqrt{}$ tales que $\sqrt{m_f} = 0$ forman un ideal en $K[t]$.

Dada una matriz M, dxd, con elementos en un campo K, consideremos la colección I_M de polinomios $\sqrt{(t)}$ tal que $\sqrt{M} = 0$, entonces I_M es un ideal en $K[t]$.

El generador monomico no nulo $\sqrt{}_M$ del ideal I_M se llama **polinomio mínimo** de M, si $\sqrt{}$ es cualquier polinomio con $\sqrt{M} = 0$, entonces el polinomio mínimo $\sqrt{}_M$ divide a$\sqrt{}$. En

particular χ_M divide al polinomio característico de M. Además todos los valores propios de M son también raíces del polinomio mínimo.

χ_f denota el polinomio mínimo del operador multiplicación m_f en A.

Tenemos tres conjuntos interesantes de números:

1. Las raíces de la ecuación $\chi_f(t)$.
2. Los Autovalores de la matriz m_f.
3. Los valores de la función f en $V(I)$.

Teorema 66. Sea $I \subset K[x_1, \cdots, x_n]$ cero-dimensional, $f \in K[x_1, \cdots, x_n]$ y χ_f el polinomio minimo de m_f en $A = K[x_1, \cdots, x_n]/I$. Entonces, para $\lambda \in K$, son equivalentes:

1. λ es una raíz de la ecuación $\chi_f(t) = 0$
2. λ es un valor propio de la matriz m_f
3. λ es un valor de la función f en $V(I)$

Demostración. Sabemos que si λ es una raíz de la ecuación $\chi_f(t) = 0$, entonces λ es un auto valor de la matriz m_f, el reciproco también se cumple, habiéndose probado $a) \Longrightarrow b)$, probemos ahora $b) \Longrightarrow c)$: sea λ un valor propio de m_f. Entonces existe un auto vector correspondiente $z \neq 0 \in A$. Eso es, dado $V(I) = \{p_1, \cdots, p_m\}$, supongamos que $f(p_i) \neq \lambda$ para todo $i = 1, \cdots, m$.

Para continuar con la demostración es necesario enunciar el siguiente Lema.

Lema 67. Sea $S = \{p_1, \cdots, p_m\}$ un subconjunto a fin de $\mathbb{C}^n$. Existen polinomios $g_i \in K[x_1, \cdots, x_n]$, $i = 1, \cdots, m$ tal que

$$g_i(p_j) = \begin{cases} 0 \text{ si } i \neq j \\ 1 \text{ si } i = j \end{cases}$$

Sea $g = f - \lambda$, así que $g\ p_j \neq 0 \forall i$. Por el Lema anterior existen polinomios g_i tal que $g_i\ p_j = 0\ si\ i \neq j$ y $g_i\ p_j = 1\ si\ i = j$. Consideremos el polinomio $g = \sum_{i=1}^{m} 1/g(p_i)g_i$. Sucede que $g\ p_i\ g\ p_i = 1 \forall i$, y por consiguiente $1 - g\,g \in \mathcal{I}(V\ I)$. Por el teorema de los ceros de Hilbert, $1 - g\,g^{\ l} \in I$ para algún $l \geq 1$. Desarrollando la última expresión por el teorema del binomio y agrupando términos que contienen a g como factor, obtenemos que $1 - \breve{g}g \in I$ para algún $\breve{g} \in K\ x_1, \cdots, x_n$. En A, esta última inclusión implica que $1 = \breve{g}\ g$; por consiguiente g tiene un inverso multiplicativo $\breve{g} \in A$.

Pero $g\ z = f - \lambda\ z = 0 \in A$. Multiplicando ambos lados por $\breve{g}$, obtenemos $z = 0$. Lo cual es una contradicción. Por lo tanto λ debe ser un valor de f en $V(I)$.

Solo falta probar $c) \Longrightarrow a)$: Sea $\lambda = f(p)$ para $p \in V(I)$. Puesto que $\mathcal{I}_f\ m_f = 0$ por el corolario poner número muestra que $\mathcal{I}_f\ f = 0$, y entonces esto implica que $\mathcal{I}_f\ f \in I$. Esto significa $\mathcal{I}_f\ f$ se anula en cada punto de $V(I)$, así que

$$\mathcal{I}_f\ \lambda = \mathcal{I}_f\ f\ p = 0. \quad \blacksquare$$

Ejemplo 68.

Consideremos el sistema de ecuaciones polinomiales:

$$x^2 + y + z = 1$$
$$x + y^2 + z = 1$$
$$x + y + z^2 = 1$$

Este sistema nos genera el ideal $I = \langle f_1, f_2, f_3 \rangle = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$, encontraremos las soluciones en $\mathbb{Q}\ x, y, z$.

Usando el orden DegRevLex, la Base de Gröbner para I es, G= [z^2 + x + y - 1, y^2 + x + z - 1, x^2 + y + z - 1]. Los monomios que no son divisibles por los términos principales del ideal forman la base monomial o módulo cociente $B = 1, z, y, yz, x, xz, xy, xyz$. Luego procedemos a calcular m_f, para $f = x, f = y, f = z$. Los cálculos se harán e el SCA CoCoA, luego se utilizara elScientific WorkPlace para calcular los valores propios de m_f.

Usando CoCoA 4.7.4, Calculemos m_x

Use R ::= QQ[x,y,z],DegRevLex;

I := Ideal(x^2+y+z-1,x+y^2+z-1,x+y+z^2-1);

Print "Este es el mapeo m_x:";

A:=x;

B:=xz;

C:=xy;

D:=xyz;

E:=x^2;

F:=x^2z;

G:=x^2y;

H:=x^2yz;

Print "L es la base de Gröbner encontrada para el ideal formado por el sistema polinomial:";

L:=[z^2 + x + y - 1, y^2 + x + z - 1, x^2 + y + z - 1];

Print "las divisiones algebraicas del mapeo m_x con la base de Grobner:";

DivAlg(A,L);

DivAlg(B,L);

DivAlg(C,L);

DivAlg(D,L);

DivAlg(E,L);

DivAlg(F,L);

DivAlg(G,L);

DivAlg(H,L);

Este es el mapeo m_x:

L es la base de Gröbner encontrada para el ideal formado por el sistema polinomial:

----

las divisiones algebraicas del mapeo m_x con la base de Gröbner:

Record[Quotients := [0, 0, 0], Remainder := x]

Record[Quotients := [0, 0, 0], Remainder := xz]

Record[Quotients := [0, 0, 0], Remainder := xy]

Record[Quotients := [0, 0, 0], Remainder := xyz]

Record[Quotients := [0, 0, 1], Remainder := -y - z + 1]

Record[Quotients := [-1, 0, z], Remainder := -yz + x + y + z - 1]

Record[Quotients := [0, -1, y], Remainder := -yz + x + y + z - 1]

Record[Quotients := [-y + 1, -z + 1, yz], Remainder := xy + xz + yz - 2x - 2y - 2z + 2]

Luego m_x es;

$$m_x = \begin{matrix} 0 & 0 & 0 & 0 & 1 & -1 & -1 & 2 \\ 0 & 0 & 0 & 0 & -1 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 & -1 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 & -1 & -1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & -2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{matrix}$$

Y sus Autovalores son:

$$\sqrt{2} - 1, -\sqrt{2} - 1, 0, 1$$

Calculemos m_y obtenemos:

Use R ::= QQ[x,y,z],DegRevLex;

I := Ideal(x^2+y+z-1,x+y^2+z-1,x+y+z^2-1);

Print "Este es el mapeo m_y:";

A:=y;

B:=yz;

C:=y^2;

D:=y^2z;

E:=xy;

F:=xyz;

G:=xy^2;

H:=xy^2z;

Print "L es la base de Gröbner encontrada para el ideal formado por el sistema polinomial:";

L:=[z^2 + x + y - 1, y^2 + x + z - 1, x^2 + y + z - 1];

Print "las divisiones algebraicas del mapeo m_y con la base de Gröbner:";

DivAlg(A,L);

DivAlg(B,L);

DivAlg(C,L);

DivAlg(D,L);

DivAlg(E,L);

DivAlg(F,L);

DivAlg(G,L);

DivAlg(H,L);

Este es el mapeo m_y:

L es la base de Gröbner encontrada para el ideal formado por el sistema polinomial:

---

las divisiones algebraicas del mapeo m_y con la base de Grobner:

Record[Quotients := [0, 0, 0], Remainder := y]

Record[Quotients := [0, 0, 0], Remainder := yz]

Record[Quotients := [0, 1, 0], Remainder := -x - z + 1]

Record[Quotients := [-1, z, 0], Remainder := -xz + x + y + z - 1]

Record[Quotients := [0, 0, 0], Remainder := xy]

Record[Quotients := [0, 0, 0], Remainder := xyz]

Record[Quotients := [0, x, -1], Remainder := -xz + x + y + z - 1]

Record[Quotients := [-x + 1, xz, -z + 1], Remainder := xy + xz + yz - 2x - 2y - 2z + 2]

Luego m_y es:

$$m_y = \begin{matrix} 0 & 0 & 1 & -1 & 0 & 0 & -1 & 2 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & -2 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & -2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}$$

Y sus valores propios son:

$$\sqrt{2} - 1, -\sqrt{2} - 1, 0, 1$$

Análogamente m_z es:

```
Use R ::= QQ[x,y,z],DegRevLex;

I := Ideal(x^2+y+z-1,x+y^2+z-1,x+y+z^2-1);
```

Print "Este es el mapeo m_z:";

A:=z;

B:=z^2;

C:=yz;

D:=yz^2;

E:=xz;

F:=xz^2;

G:=xyz;

H:=xyz^2;

Print "L es la base de Gröbner encontrada para el ideal formado por el sistema polinomial:";

L:=[z^2 + x + y - 1, y^2 + x + z - 1, x^2 + y + z - 1];

Print "las divisiones algebraicas del mapeo m_z con la base de Gröbner:";

DivAlg(A,L);

DivAlg(B,L);

DivAlg(C,L);

DivAlg(D,L);

DivAlg(E,L);

DivAlg(F,L);

DivAlg(G,L);

DivAlg(H,L);

Este es el mapeo m_z:

L es la base de Gröbner encontrada para el ideal formado por el sistema polinomial:

las divisiones algebraicas del mapeo m_z con la base de Gröbner:

Record[Quotients := [0, 0, 0], Remainder := z]

Record[Quotients := [1, 0, 0], Remainder := -x - y + 1]

Record[Quotients := [0, 0, 0], Remainder := yz]

Record[Quotients := [y, -1, 0], Remainder := -xy + x + y + z - 1]

Record[Quotients := [0, 0, 0], Remainder := xz]

Record[Quotients := [x, 0, -1], Remainder := -xy + x + y + z - 1]

Record[Quotients := [0, 0, 0], Remainder := xyz]

Record[Quotients := [xy, -x + 1, -y + 1], Remainder := xy + xz + yz - 2x - 2y - 2z + 2]

Obteniendo que m_z:

$$m_z = \begin{matrix} 0 & 1 & 0 & -1 & 0 & -1 & 0 & 2 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & -2 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{matrix}$$

Y sus Autovalores son:

$$\sqrt{2}-1,-\sqrt{2}-1,0,1$$

Finalmente al sustituirlos los Autovalores dentro del sistema vemos que de las 64 posibles combinaciones sólo 5 son solución del sistema:

$$VI = \begin{matrix} 0,0,1\ ,\ 0,1,0\ ,\ 1,0,0\ ,\ -1-\sqrt{2},-1-\sqrt{2},-1-\sqrt{2}\ , \\ -1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2} \end{matrix}$$

9.5 Aplicación de esta teoría

En un sistema de ecuaciones lineales es un caso particular de sistemas polinomiales en el que los polinomios involucrados son de grado 1. Para dichos sistemas sabemos que el algebra lineal da respuestas sencillas.

9.5.1 Optimización de recursos

En las diferentes organizaciones siendo estas pequeñas, medianas incluso las grandes empresas tienen a su disposición una serie de recursos, sin estos pues estas no pudieran persistir, como son por ejemplo: las personas, materia prima, etc. Llevar a cabo el proceso de las prácticas administrativas para el manejo de los recursos de vital importancia, ya que de esta forma se garantiza un adecuado manejo de estos.

Es por ello que el método abordado en este trabajo resulta de mucha importancia, ya que tiene la capacidad de resolver sistemas que son muy complicados de resolver, por los métodos convencionales de Álgebra Lineal y Análisis Numérico.

Aquí presentamos un modelo general de optimización, en el cual se puede observar que las restricciones son lineales y polinómicas de grado mayor que uno, a como estamos acostumbrados a tratar en los modelos lineales.

$$minimizar; f\ x,y,z\ = x^2 + 3y^2 + 5xz^2$$

$$sujeta\ a:$$

$$g_1\ x,y,z\ = xz + 2y + y^2 - 11;$$

$$g_2\ x,y,z\ = x^2 + 2xy + z^2 - 14;$$

$$g_3\ x,y,z\ = x^2 + 2y + z - 8.$$

Solución:

Para agilizar los cálculos serán hechos con el software CoCoA 4.7.4

Usando el orden entre términos DegRevLex (Léxico graduado revertido por sus siglas en ingles), usando el CoCoA 4.7.4 obtenemos el siguiente resultado.

Use R ::= QQ[x,y,z], DegRevLex;

I := Ideal(xz+2y+y^2-11,x^2+2xy+z^2-14,x^2+2y+z-8);

Describe I;

GBasis(I);

Record[Type := IDEAL, Value := Record[Gens := [y^2 + xz + 2y - 11, x^2 + 2xy + z^2 - 14, x^2 + 2y + z - 8]]]

[Use R ::= QQ[x,y,z], DegRevLex;

I := Ideal(xz+2y+y^2-11,x^2+2xy+z^2-14,x^2+2y+z-8);

Describe I;

GBasis(I);

La Base de Gröbner para el ideal formado por las ecuaciones del sistema es:

GBasis(I)= [x^2 + 2xy + z^2 - 14, y^2 + xz + 2y - 11, -2xy - z^2 + 2y + z + 6, -1/2yz^2 - xz - 3/2yz - 2z^2 - 11x + 3y + 9z + 17, -1/2xz^2 - 3/2xz + yz - 1/2z^2 + 3x - 11y + 1/2z + 25, 1/2z^4 + z^3 + 32xz - 4yz + 5/2z^2 + 32x + 132y - 22z - 392]

Para aplicar el método necesitamos encontrar la base B formada por los elementos que no son divisibles por el ideal formado por los términos principales del ideal. Dicho ideal esta dado por $tp(I) = \langle x^2, y^2, xy, yz^2, xz^2, z^4 \rangle$, la base B la encontraremos usando CoCoa 4.7.4.

Use R ::= QQ[x,y,z],DegRevLex;

I := Ideal(xz+2y+y^2-11,x^2+2xy+z^2-14,x^2+2y+z-8);

QuotientBasis(LT(I));

[1, z, z^2, z^3, y, yz, x, xz]

De aquí se observa que $B = \langle 1, z, z^2, z^3, y, yz, x, xz \rangle$, según la **proposición 63 y el corolario 66** podemos encontrar la solución a este problema encontrando los valores propios asociados a la matriz generada por cada uno de los mapeos m_{x_i}.

Primero encontremos la matriz generada por el mapeo $m_x = x$, esto se hace multiplicando x con cada término de la base B y luego haciendo la división algebraica por la Base de Gröbner, luego de efectuar dicha división la matriz se obtiene con los coeficientes de los residuos.

Use R ::= QQ[x,y,z],DegRevLex;

A:=x;

B:=xz;

C:=xz^2;

D:=xz^3;

E:=xy;

F:=xyz;

G:=x^2;

H:=x^2z;

L:=[x^2 + 2xy + z^2 - 14, y^2 + xz + 2y - 11, -2xy - z^2 + 2y + z + 6, -1/2yz^2 - xz - 3/2yz - 2z^2 - 11x + 3y + 9z + 17, -1/2xz^2 - 3/2xz + yz - 1/2z^2 + 3x - 11y + 1/2z + 25, 1/2z^4 + z^3 + 32xz - 4yz + 5/2z^2 + 32x + 132y - 22z - 392];

DivAlg(A,L);

DivAlg(B,L);

DivAlg(C,L);

DivAlg(D,L);

DivAlg(E,L);

DivAlg(F,L);

DivAlg(G,L);

DivAlg(H,L);

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := x]

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := xz]

Record[Quotients := [0, 0, 0, 0, -2, 0], Remainder := -3xz + 2yz - z^2 + 6x - 22y + z + 50]

Record[Quotients := [0, 0, 0, -4, -2z + 6, 0], Remainder := -z^3 + 11xz - 34yz - 4z^2 - 62x + 78y + 83z - 82]

Record[Quotients := [0, 0, -1/2, 0, 0, 0], Remainder := -1/2z^2 + y + 1/2z + 3]

Record[Quotients := [0, 0, -1/2z, 0, 0, 0], Remainder := -1/2z^3 + yz + 1/2z^2 + 3z]

Record[Quotients := [1, 0, 1, 0, 0, 0], Remainder := -2y - z + 8]

Record[Quotients := [z, 0, z, 0, 0, 0], Remainder := -2yz - z^2 + 8z]

Lo que implica que:

$$m_x = \begin{matrix} 0 & 0 & 50 & -82 & 3 & 0 & 8 & 0 \\ 0 & 0 & 1 & 83 & 1/2 & 3 & -1 & 8 \\ 0 & 0 & -1 & -4 & -1/2 & 1/2 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 & -1/2 & 0 & 0 \\ 0 & 0 & -22 & 78 & 1 & 0 & -2 & 0 \\ 0 & 0 & 0 & -34 & 0 & 1 & 0 & -2 \\ 1 & 0 & 1 & -62 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 11 & 0 & 0 & 0 & 0 \end{matrix}$$

Del Álgebra Lineal sabemos que los valores propios asociados a esta matriz, son las raíces del polinomio resultante que sale de calcular el determinante de $|m_x - aI|$ donde I es la matriz identidad. Usaremos el CoCoA 4.7.4 para calcular el polinomio característico y para calcular los valores propios usaremos en Scientific WorkPlace 5.5 .

Use R ::= QQ[x],DegRevlex;

CharPoly(Mat([[0,0,0,0,0,0,1,0],[0,0,0,0,0,0,0,1],[50,1,-1,0,-22,0,1,-3],[-82,83,-4,-1,78,-34,-62,11],[3,1/2,-1/2,0,1,0,0,0],[0,3,1/2,-1/2,0,1,0,0],[8,-1,0,0,-2,0,0,0],[0,8,-1,0,0,-2,0,0]]), x);

----

x^8 - 49x^6 + x^5 + 693x^4 - 389x^3 - 3122x^2 + 3402x + 568

---

y los valores propios asociados a la matriz (raíces del polinomio) será:

$$5.6188, 2.8057, 1.0 + 8.1879 \times 10^{-2}\, i, 1.9544 - 8.1879 \times 10^{-2}\, i, -0.14747, -3.0574, -4.5642 + 0.22752\, i, -4.5642 - 0.22752\, i$$

para calcular m_y se hace un proceso análogo por lo tanto:

Use R ::= QQ[x,y,z],DegRevLex;

A:=y;

B:=yz;

C:=yz^2;

D:=yz^3;

E:=y^2;

F:=y^2z;

G:=xy;

H:=xyz;

L:=[x^2 + 2xy + z^2 - 14, y^2 + xz + 2y - 11, -2xy - z^2 + 2y + z + 6, -1/2yz^2 - xz - 3/2yz - 2z^2 - 11x + 3y + 9z + 17, -1/2xz^2 - 3/2xz + yz - 1/2z^2 + 3x - 11y + 1/2z + 25, 1/2z^4 + z^3 + 32xz - 4yz + 5/2z^2 + 32x + 132y - 22z - 392];

DivAlg(A,L);

DivAlg(B,L);

DivAlg(C,L);

DivAlg(D,L);

DivAlg(E,L);

DivAlg(F,L);

DivAlg(G,L);

DivAlg(H,L);

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := y]

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := yz]

Record[Quotients := [0, 0, 0, -2, 0, 0], Remainder := -2xz - 3yz - 4z^2 - 22x + 6y + 18z + 34]

Record[Quotients := [0, 0, 0, -2z + 6, 4, 0], Remainder := -4z^3 - 10xz + 11yz + 32z^2 + 54x + 26y - 22z - 202]

Record[Quotients := [0, 1, 0, 0, 0, 0], Remainder := -xz - 2y + 11]

Record[Quotients := [0, z, 0, 0, 2, 0], Remainder := 3xz - 4yz + z^2 - 6x + 22y + 10z - 50]

Record[Quotients := [0, 0, -1/2, 0, 0, 0], Remainder := -1/2z^2 + y + 1/2z + 3]

Record[Quotients := [0, 0, -1/2z, 0, 0, 0], Remainder := -1/2z^3 + yz + 1/2z^2 + 3z]

La matriz asociada es:

$$m_y = \begin{matrix} 0 & 0 & 34 & -202 & 11 & -50 & 3 & 0 \\ 0 & 0 & 18 & -22 & 0 & 10 & 1/2 & 3 \\ 0 & 0 & -4 & 32 & 0 & 1 & -1/2 & 1/2 \\ 0 & 0 & 0 & -4 & 0 & 0 & 0 & -1/2 \\ 1 & 0 & 6 & 26 & -2 & 22 & 1 & 0 \\ 0 & 1 & -3 & 11 & 0 & -4 & 0 & 1 \\ 0 & 0 & -22 & 54 & 0 & -6 & 0 & 0 \\ 0 & 0 & -2 & -10 & -1 & 3 & 0 & 0 \end{matrix}$$

El polinomio característico es:

Use R ::= QQ[y],DegRevLex;

CharPoly(Mat([[0,0,0,0,1,0,0,0],[0,0,0,0,0,1,0,0],[34,18,-4,0,6,-3,-22,-2],[-202,-22,32,-4,26,11,54,-10],[11,0,0,0,-2,0,0,-1],[-50,10,1,0,22,-4,-6,3],[3,1/2,1/2,0,1,0,0,0],[0,3,1/2,-1/2,0,1,0,0]]), y);

----

y^8 + 14y^7 + 36y^6 – 246y^5 – 1219y^4 + 4074y^3 + 1930y^2 – 11722y + 6156

---

y los valores propios son:

$$2.6703, 2.1531, 2.0, 0.69301, -1.8564, -5.1815 + 4.2322i, -5.1815 - 4.2322i, -9.297$$

calculemos m_z.

Use R ::= QQ[x,y,z],DegRevLex;

A:=z;

B:=z^2;

C:=z^3;

D:=z^4;

E:=yz;

F:=yz^2;

G:=xz;

H:=xz^2;

L:=[x^2 + 2xy + z^2 - 14, y^2 + xz + 2y - 11, -2xy - z^2 + 2y + z + 6, -1/2yz^2 - xz - 3/2yz - 2z^2 - 11x + 3y + 9z + 17, -1/2xz^2 - 3/2xz + yz - 1/2z^2 + 3x - 11y + 1/2z + 25, 1/2z^4 + z^3 + 32xz - 4yz + 5/2z^2 + 32x + 132y - 22z - 392];

DivAlg(A,L);

DivAlg(B,L);

DivAlg(C,L);

DivAlg(D,L);

DivAlg(E,L);

DivAlg(F,L);

DivAlg(G,L);

DivAlg(H,L);

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := z]

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := z^2]

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := z^3]

Record[Quotients := [0, 0, 0, 0, 0, 2], Remainder := -2z^3 - 64xz + 8yz - 5z^2 - 64x - 264y + 44z + 784]

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := yz]

Record[Quotients := [0, 0, 0, -2, 0, 0], Remainder := -2xz - 3yz - 4z^2 - 22x + 6y + 18z + 34]

Record[Quotients := [0, 0, 0, 0, 0, 0], Remainder := xz]

Record[Quotients := [0, 0, 0, 0, -2, 0], Remainder := -3xz + 2yz - z^2 + 6x - 22y + z + 50]

Esto implica que:

$$m_z = \begin{matrix} 0 & 0 & 0 & 784 & 0 & 34 & 0 & 50 \\ 1 & 0 & 0 & 44 & 0 & 18 & 0 & 1 \\ 0 & 1 & 0 & -5 & 0 & -4 & 0 & -1 \\ 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -264 & 0 & 6 & 0 & -22 \\ 0 & 0 & 0 & 8 & 1 & -3 & 0 & 2 \\ 0 & 0 & 0 & -64 & 0 & -22 & 0 & 6 \\ 0 & 0 & 0 & -64 & 0 & -3 & 1 & -3 \end{matrix}$$

Y el polinomio característico asociado será:

Use R ::= QQ[x],DegRevlex;

CharPoly(Mat([[0,1,0,0,0,0,0,0],[0,0,1,0,0,0,0,0],[0,0,0,1,0,0,0,0],[784,44,-5,-2,-264,8,-64,-64],[0,0,0,0,0,0,1,0,0],[34,18,-4,0,6,-3,-22,-2],[0,0,0,0,0,0,0,0,1],[0,1,-1,0,-22,2,6,-3]]), x);

----

x^8 + 8x^7 + 18x^6 - 80x^5 - 3387x^4 + 3104x^3 + 20768x^2 - 27072x + 249504

y las raíces del polinomio son:

$$4.9484, 3.0, 2.4756, -3.491 \times 10^{-29}, -2.1209 + 5.8876\,i, -2.1209 - 5.8876\,i, -2.2467, -9.2944$$

Como el problema se trata de minimizar, se excluyen todos los valores propios negativos e imaginarios por lo tanto el punto óptimo que minimiza la función objetivo y satisface las condiciones es:

$$x, y, z = 1, 2, 3$$

9.5.2 Otras Aplicaciones

En nuestro trabajo presentamos algunas aplicaciones en la geometría algebraica, la teoría de ideales polinomiales, álgebra conmutativa y no conmutativa.

Así también encontramos información en más aplicaciones como lo es la teoría de códigos, combinatoria, criptografía, teoría de invariantes, programación entera, teoría de grafos, ecuaciones diferenciales, etc.

Una aplicación muy interesante es la de un condensador de energía eléctrica que nos permite reusar la energía utilizada, ya que en nuestro país los marcadores de energía contabilizan la energía que entra así también la energía utilizada.

10. Conclusiones

10.1 En relación a los objetivos de la investigación

- La resolución de los sistemas de ecuaciones polinomiales nos permiten analizar resultados utilizando las Bases de Gröbner.
- Conocimos procesos interesantes y nomenclaturas que para nosotros eran desconocidos así profundizamos en el análisis de las diversas definiciones, teoremas, lemas, formulas utilizadas, etc.

10.2 En relación a la metodología aplicada

- Practicamos y analizamos los resultados presentados por el software CoCoA en nuestra metodología utilizada.
- Planteamos nuestra aplicación en un sistema de ecuaciones multivariado pero de grado 1, probando que el método de Autovalores también nos permite ver el número de soluciones en estos sistemas.
- La optimización de recursos resulta imprescindible para la industria y empresa moderna he ahí donde radica la importancia de resolver los sistemas de ecuaciones polinomiales.

10.3 Perspectivas de futuro (Recomendaciones)

- Se recomienda implementar en el laboratorio de matemática la facilidad hacia los estudiantes en el estudio y practica de los software CoCoA 4.7.4, Singular y Mathematica.
- Analizar más a fondo las aplicaciones ya que pueden ser útiles en nuestro país resolviendo problemáticas necesarias para mejorías en nuestro entorno.

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 algebra*. New York: Springer-Verlag.

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

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

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

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

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

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

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

Handy, A. Taha. (2004). Investigación de Operaciones, 7ma. Edición. México: Pearson Educación.

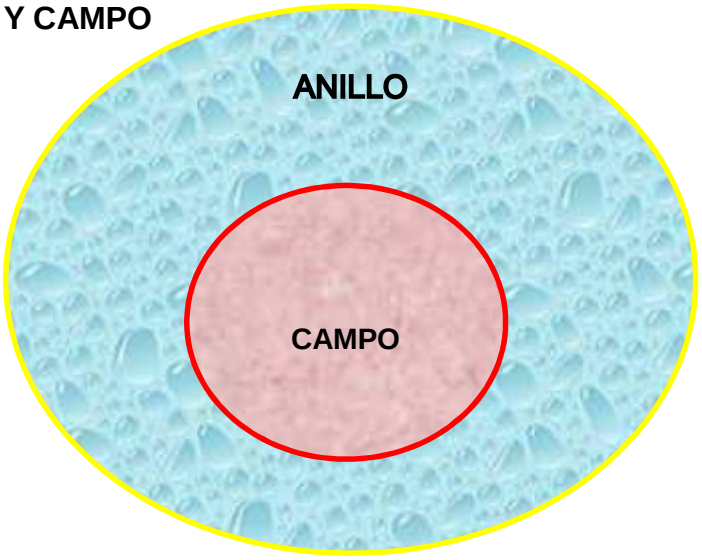
12. Anexos

I. Sistemas de computación algebraica usados

En el presente trabajo utilizamos el software CoCoA 4.7.4, el Scientific Word Place, Singular y el Mathematica. Se hizo uso de estos software para hacer los cálculos algebraicos más rápidos y menos tediosos.

II.Gráficas

ANILLO Y CAMPO



MÓDULO Y ESPACIOS VECTORIAL