UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA CIVIL Y ARQUITECTURA

ESCUELA PROFESIONAL DE CIENCIAS FÍSICO MATEMÁTICAS

BASES DE GRÖBNER Y SU APLICACIÓN EN LA SOLUCIÓN DE SISTEMAS POLINOMIALES

TESIS

PRESENTADA POR:

Bach. FLORES MAMANI LUIS CESAR

PARA OPTAR EL TÍTULO PROFESIONAL DE:

LICENCIADO EN CIENCIAS FÍSICO MATEMÁTICAS CON ESPECIALIDAD EN MATEMÁTICAS

PUNO – PERÚ

2021

DEDICATORIA

Dedico el presente trabajo, a mis queridos padres: Ernesto y Yolanda, por haberme guiado con amor y sabiduría, enseñarme con su ejemplo el significado de dedicación y esfuerzo, a mis hermanos Griselda, Aydón y Denis, que me acompañaron incondicionalmente; también quiero dedicar este trabajo, a mi amiga y compañera de vida, Hilda María Mendoza, que gracias a su apoyo he logrado culminar satisfactoriamente mi trabajo.

Luis Cesar.

AGRADECIMIENTO

En primer lugar, agradezco a mi padre celestial, quien me dio fuerza y paciencia para superar las adversidades de cada circunstancia en mi vida, quien me guía y me impulsa para forjar un camino de bien, haciendo de mi un testimonio de entrega y servicio. Gracias, señor.

En segundo lugar, agradezco a la directora de esta tesis, Lic. Fabiola Loayza Torreblanca, por la dedicación y el apoyo que me brindó a lo largo de la elaboración de este trabajo, le agradezco por el respeto a mis sugerencias e ideas. Así como también, haber sido paciente, al momento de acompañarme en la realización de mi trabajo, gracias por compartir conmigo su vocación de servicio y su conocimiento para así, poder culminar esta investigación.

También, agradezco a todos los docentes de la Escuela Profesional de Ciencias Físico Matemáticas, de la Universidad Nacional del Altiplano, por haber sido participes de mi formación académica. Finalmente doy las gracias a mis jurados, por haberse tomado el tiempo de leer mi trabajo, y hacer las observaciones correspondientes, para poder culminar mi trabajo con éxito.

Luis Cesar.

ÍNDICE GENERAL

Pág.

Área : Matemática
Tema : Bases de Gröbner y su aplicación en la solución de sistemas Polinomiales
Línea : Álgebra

FECHA DE SUSTENTACIÓN: 16 de noviembre de 2021.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ACRÓNIMOS

$\boldsymbol{\beta}$ **: El vector** $(\boldsymbol{\beta_1}, \ldots \boldsymbol{\beta_n}) \in \mathbb{N}^{\boldsymbol{n}}$

$K[x_1, \ldots x_n]$: Anillo de polinomios de n indeterminadas con coeficientes en K

$\mathbb{N}$: Conjunto de los números naturales incluido el cero

$\mathbb{Z}$: Conjunto de los números enteros

X^{β}: Al monomio ${x_1}^{\beta_1}, \ldots, {x_n}^{\beta_n}$

a/b: a divide a b

M_n: El conjunto de los Monomios $K[x_1, \ldots x_n]$

$cp(f)$: Coeficiente principal de f

$mp(f)$: Producto de potencia principal o monomio principal de f

$tp(f)$: término principal del polinomio f

mcd: Máximo común divisor

mcm: Mínimo común múltiplo

RESUMEN

Este trabajo de investigación tiene como objetivo encontrar las Bases de Gröbner y con ellas resolver sistemas de ecuaciones polinomiales, partiremos con conceptos del algebra abstracta tal como grupos, grupo abeliano, campo, espacios vectoriales, anillos, ideales etc. también hacemos un estudio de las ordenes monomiales dentro de ellas estudiamos el orden lexicográfico prioridad, el algoritmo de la división; seguidamente el algoritmo de Buchberger los cuales son necesarios para determinar las Bases de Gröbner, Gröbner fue un matemático alemán el cual dio un argumento que garantiza que todo ideal de un anillo de polinomios admite conjuntos finitos de generadores "especiales" llamados posteriormente por Bruno Buchberger "Bases de Gröbner" Los cuales posibilitan decidir si un elemento pertenece o no a un ideal dado. Las Bases de Gröbner son una herramienta que se aplica a diversas áreas, dentro de ellos a la solución de sistemas de ecuaciones Polinomiales, al ser este un proceso muy extenso se hace uso del software CoCoa versión 4.7.5 (Computación in Conmutativa Algebra) este nos permite obtener las bases las soluciones.

Palabras clave: Anillos, bases de Grobner, ideales, sistemas polinomiales, órdenes monomiales.

ABSTRACT

This research work aims to analyze the Bases of Gröbner and with them solve systems of polynomial equations, we will start with concepts of abstract algebra such as groups, abelian group, field, vector spaces, etc. We also do a study of monomial orders within them we study the lexicographic order with the highest priority, we study the rings, ideals, the algorithm of division; which are necessary for the analysis of Gröbner's Bases, then Buchberger's algorithm and Hilbert's Basis theorem.

Gröbner was a German mathematician who gave an argument that guarantees that every ideal of a ring of polynomials admits finite sets of "special" generators later called by Bruno Buchberger "Gröbner bases" which make it possible to decide whether or not an element belongs to a given ideal. The Gröbner Bases are a tool that is applied to various areas of many mathematical problems within them systems of polynomial equations, as this is a very extensive process, this work uses the Cocoa software version 4.7.5 (Computation in Commutative Algebra) This allows us to solve the calculations more quickly. We must take into account the importance of solving systems of polynomial equations since these are representations of real problems in different areas of our environment.

Key words: Rings, Grobner bases, ideals, polynomial systems, monomial orders.

CAPÍTULO I

INTRODUCCIÓN

En los años 60, Bruno Buchberger y Heisuke Hironaka introdujeron independientemente nuevos algoritmos para manipular sistemas de ecuaciones polinomiales que desembocaron en la creación de la teoría de bases de Grobner, también llamadas bases estándar en un contexto local (Giménez 2016). Gröbner fue un matemático alemán el cual dio un argumento que garantiza que todo ideal de un anillo de polinomios admite un conjunto finito de generadores "especiales" llamados, bases de Gröbner" por el matemático austriaco Bruno Buchberger quien además presento un algoritmo para el cálculo de estas, todo ello fue presentado en su tesis de doctorado el año de 1960 cuyo asesor fue justamente Grobner (Gonzáles 2014). Las bases de Gröbner son una herramienta que se aplica a diversas áreas, dentro de ellas a la solución de sistemas de ecuaciones Polinomiales, al ser este un proceso muy extenso se hace uso de paquetes de cálculo simbólico, en esta investigación se trabajó con el CoCoa versión 4.7.5 (Computación in Conmutativa Algebra) (Cifuentes, Patiño, y Pérez 2010) este nos permitió obtener de manera rápida las bases y soluciones de sistemas polinomiales.

El objetivo fundamental de la investigación es explicar que son y cómo obtener las Bases de Gröbner y para ello utilizar las ordenes monomiales, el algoritmo de la división, el algoritmo de Buchberger.

El trabajo se estructuró de la siguiente manera:

En el capítulo 1 se presenta la introducción, también se menciona los componentes del problema, la formulación del problema, las hipótesis, la justificación y los objetivos para el desarrollo de esta investigación.

En el capítulo 2 se muestra la revisión de literatura, en ella se encuentran los antecedentes que sustentan el desarrollo de esta investigación, el marco teórico en el que se enuncia a detalle todos los conceptos que serán necesarios para lograr el objetivo de la investigación.

En el capítulo 3, se encuentran los materiales y métodos.

En el capítulo 4 se encuentran los resultados y discusión, en ella presento ordenes monomiales, el algoritmo de la división, algoritmo de Buchberger, el teorema de los ceros de Hilbert y el proceso de la obtención de las bases de Grobner las cuales me sirvieron para determinar la solución de sistemas Polinomiales, por lo extenso del procedimiento se hizo necesario el uso de un software en este caso se trabajó con el software CoCoA. Finalmente, en el capítulo 5 y 6 se encuentran las conclusiones y las recomendaciones, en ellas explico lo que se logró en esta investigación y recomiendo posibles temas de investigación que han surgido del proceso de este.

1.1. PLANTEAMIENTO DE PROBLEMA

¿Cómo obtener bases de Gröbner, y de qué manera se pueden aplicar para en la resolución de sistemas Polinomiales?

1.2. FORMULACIÓN DEL PROBLEMA.

En la presente investigación titulada “Bases de Gröbner y su aplicación a la solución de sistemas Polinomiales” se plantea lo siguiente:

¿Qué son las Bases de Gröbner?

¿Cómo se obtienen las Bases de Gröbner para la solución de sistemas Polinomiales? ¿Cómo se clasifican las ordenes monomiales en $\boldsymbol{K[x_1, x_2, \ldots x_n.]}$ para desarrollar la base de Grobner?

1.3. HIPÓTESIS DE LA INVESTIGACIÓN

1.3.1. Hipótesis general

Las bases de Grobner permiten resolver sistemas de ecuaciones polinomiales

1.3.2. Hipótesis específicas

- Las órdenes monomiales intervienen en la determinación de una base de Grobner.
- En el proceso para determinar bases de Grobner interviene el algoritmo de la división.
- El algoritmo de Buchberger permiten determinar las bases de Grobner.

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

El estudio de las Bases de Gröbner para la solución de sistemas de ecuaciones Polinomiales es un tema se suma importancia dentro de las matemáticas en la línea del algebra y específicamente del algebra conmutativa, esta investigación nos lleva a profundizar conceptos que en muchos casos no le encontramos aplicación como son la teoría de grupos, campos, espacio vectorial, anillos, ideales etc. Lo más importante es que con ello encontramos una herramienta que nos va a permitir resolver sistemas de ecuaciones y otros como el problema de los colores etc. Muchos problemas reales en diferentes áreas se modelan y estas se representan en sistemas de ecuaciones, las más comunes son las ecuaciones lineales con dos variables con tres y para su solución sabemos que hay métodos como los de igualación, sustitución, gráficamente etc. pero a medida que los problemas se van tornando más complejos los sistemas ya no se pueden resolver fácilmente y se tiene que recurrir a otros métodos como el de Gauss Jordan etc. Aquí

surge la necesidad e importancia de este trabajo de investigación ya que este es un método novedoso e importante que nos va a permitir encontrar las raíces de sistemas de ecuaciones polinomiales; para problemas simples podemos operarlo manualmente, pero en muchos casos los problemas reales son complejos para lo que es necesario utilizar software como el CocoA, el Macaulay etc. Por todo lo mencionado este trabajo de investigación es importante para el desarrollo de las ciencias matemáticas y por ende va a dar luces a muchos investigadores tomarlo como herramienta útil para solucionar muchos problemas.

1.5. OBJETIVOS DE LA INVESTIGACIÓN

1.5.1. Objetivo general

Determinar Bases de Grobner y aplicar a la solución de un sistema de ecuación polinomial.

1.5.2. Objetivo específico

- Analizar las ordenes monomiales
- Analizar el algoritmo de la división
- Analizar el algoritmo de Buchberger

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. MARCO TEÓRICO

En esta sección se presenta definiciones, teoremas, lemas algoritmos que serán necesarios para lograr los propósitos de la investigación

Definición 2.1.1 Un grupo $(\boldsymbol{G}; \cdot)$ es un conjunto $\boldsymbol{G}$ provisto de una operación $\cdot : \boldsymbol{G} \times \boldsymbol{G} \rightarrow \boldsymbol{G}$ Que satisface las siguientes condiciones:

- Asociatividad: para todo $g_1, g_2, g_3 \in G, es$

$$(\boldsymbol{g_1}.\boldsymbol{g_2}).\boldsymbol{g_3} = \boldsymbol{g_1}.(\boldsymbol{g_2}.\boldsymbol{g_3})$$

- Elemento neutro: existe un único $\boldsymbol{e} \in \boldsymbol{G}$ tal que para todo

$$\boldsymbol{g} \in \boldsymbol{G}\ ,\ \boldsymbol{e}.\boldsymbol{g} = \boldsymbol{g} = \boldsymbol{g}.\boldsymbol{e}$$

- Inverso: para todo

$$g \in G, \exists!\ g'.g = e = g.g'$$

si además para todo par $g, h \in G$ es $g.h = h.g$ entonces el grupo se llama abeliano (conmutativo)

Definición 2.1.2 Un subconjunto no vacío $\boldsymbol{H}$ de un grupo $\boldsymbol{G}$ se llama subgrupo de $\boldsymbol{G}$, si $\boldsymbol{H}$ mismo forma un grupo relativo al producto de $\boldsymbol{G}$.

Definición 2.1.3 Un anillo $(\boldsymbol{A}, +, \cdot)$ es un conjunto no vacio en donde están definidas un par de operaciones llamadas suma y producto, las cuales denotamos por $+$ y $\cdot$ respectivamente.

Estas operaciones satisfacen cada una de las propiedades siguientes:

- **Cerradura respecto a la suma:** para todo $a, b \in A$, se tiene que $a + b \in A$.

- **Asociativa respecto a la suma:** para todo $a, b, c \in A$, se tiene que

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

- **Existencia del neutro aditivo**: existe un elemento neutro"0" en A, la cual llamaremos cero, tal que

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

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

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

- **Conmutativa respecto a la suma:** para todo a , b en A se tiene .

$$a + b = b + a$$

- **Cerradura respecto al producto:** para todo a , b en A se tiene se tiene que $a.b$ están en A.

- **Asociativa respecto al producto:** para todo a , b y c en A se satisface

$$a.(b.c) = (a.b)c$$

- **Existencia del neutro multiplicativo:** para todo a, existe un único elemento, e, en A que es neutro de la operación; es decir

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

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

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

$$(\boldsymbol{a+b})\cdot \boldsymbol{c} = \boldsymbol{a}\cdot\boldsymbol{c} + \boldsymbol{b}\cdot\boldsymbol{c}$$

Ejemplo 2.1.4. (de anillos)

$\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$

Si $\boldsymbol{R}$ es un anillo, entonces $\boldsymbol{R}[\boldsymbol{x}]$, $\boldsymbol{R}[\boldsymbol{x_1}, \dots, \boldsymbol{x_n}]$ también son anillos.

Definición 2.1.5 Un Monoide $(\boldsymbol{M}, \cdot)$ es una estructura algebraica en la que $\boldsymbol{M}$, es un conjunto y " $\cdot$ " es una operación binaria interna en $\boldsymbol{M}$, que cumple las siguientes propiedades.

1. **Operación interna**: para cualesquiera dos elementos del conjunto M operados bajo " $\cdot$ "; el resultado siempre pertenece al mismo semigrupo M. Es decir:

$$\forall x, y \in M : x \cdot y \in M$$

2. **Asociativa**: para cualquiera elemento del conjunto M no importa el orden en que se operen las parejas de elementos, mientras no se cambie el orden de los elementos siempre dará el mismo resultado. Es decir

$$\forall \boldsymbol{x, y, z} \in \boldsymbol{M} : \boldsymbol{x}\cdot(\boldsymbol{y}\cdot\boldsymbol{z}) = (\boldsymbol{x}\cdot\boldsymbol{y})\cdot\boldsymbol{z} \in \boldsymbol{M}$$

3. **Elemento neutro**: existe un único elemento, e, en M que es neutro de la operación " $\cdot$ " es decir: $\exists!\ e \in M, \forall x \in M : e \cdot x = x = x \cdot e$

Un monoide es conmutativo o abeliano si satisface la propiedad conmutativa.

Definición 2.1.6 Sea $\boldsymbol{K}$un conjunto no vacío, y sean $+$ $\boldsymbol{y}$ $\cdot$ dos operaciones internas sobre $\boldsymbol{K}$ el sistema $(\boldsymbol{K}, +, \cdot)$ es un campo si cumple**:**

- **Asociativa respecto a la suma:** para todo $a, b, c \in K$ se tiene que

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

- **Conmutativa respecto a la suma**: para todo $a, b \in K$ se tiene que

$$a + b = b + a$$

- **Existencia del neutro aditivo:** existe un elemento neutro 0 en K, el cual llamaremos cero, talque

$$a + 0 = a = 0 + a \text{ Para todo } a \in K.$$

- **Existencia del inverso aditivo**: para todo a en K, existe otro elemento en K, denotada por $-a$, el cual llamaremos el opuesto de a, el cual llamaremos el opuesto de a y que verifica

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

- **Asociativa respecto al producto:** para todo a, b en K satisface

$$a.(bc) = (ab).c$$

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

$$ab = ba$$

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

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

- **Existencia del elemento inverso multiplicativo:** para todo $a \in K, \exists\, a' \in K$, es decir: $a'.a = e$

- **Definición 2.1.7 (Espacio vectorial)** Sean dos conjuntos, no vacíos $\boldsymbol{V}$ **y** $\boldsymbol{K}$,donde $\boldsymbol{K}$ es un campo. En $\boldsymbol{V}$ se define las operaciones:

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

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

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

Definición 2.1.8 (Base y dimensión) Dado un subconjunto S de un espacio vectorial $\mathbb{V}$

S es una base de $\mathbb{V}$ si y solo si satisface las siguientes propiedades.

1) S es linealmente independiente

2) $\ell\{S\} = \mathbb{V}$, en otras palabras, para todo, $x \in \mathbb{V}, \sum_{i=1}^{n} c_i x_i \in S, 1 \leq i \leq n$

3) El número de elementos de la base se llama dimensión $\mathbb{V}$ $(dim\mathbb{V})$

Ejemplos 2.1.9.

Dado $S = \{(1,0),(0,1)\} \subset \mathbb{R}^2$

S es una base de $\mathbb{R}^2$, pues

1. es linealmente independiente

2. $\ell\{S\} = \mathbb{V}, \forall(x,y) = \mathrm{x}(1,0) + \mathrm{y}(0,1)$

3. $dim\mathbb{V}$=2

Ejemplo 2.1.10.

Dado $s_1 = \{(1,0,0),(0,1,0),(0,0,1)\} \subset \mathbb{R}^3$

S Es una base de $\mathbb{R}^3$, pues

1. es linealmente independiente

2. $\ell\{s_1\} = \mathbb{V},\ \forall(x,y,z) = \mathrm{x}(1,0,0) + \mathrm{y}(0,1,0), z(0,0,1)$

3. $dim\mathbb{V} = 3$

Teorema 2.1.11. ***(Teorema fundamental de algebra)***

Todo polinomio en una variable de grado $n \geq 1$ con coeficientes reales o complejos tiene al menos n raíces (reales o complejas).

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

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

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

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

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

$$\boldsymbol{f(x) = a_0(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2 \cdots}(x - \alpha_i)^{k_i}}$$

Donde

$$k_1 + k_2 + \cdots k_i = n \, , y \, \alpha_1 \neq \alpha_2 \neq \cdots \neq \alpha_i.$$

2.2 . POLINOMIOS EN VARIAS INDETERMINADAS (el anillo $K[x_1, \ldots, x_n]$)

Definición 2.2.1 Un monomio en $\boldsymbol{x_1, x_2, \ldots, x_n}$ es un producto de la forma

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

Donde todos los exponentes $\boldsymbol{\alpha_1, \alpha_2, \ldots, \alpha_n}$ son exponentes no negativos. El grado total de este monomio es la suma $\boldsymbol{|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n}$.

Notación: escribimos x^{α} por $x_1^{\alpha_1}.x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}$ donde $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ es una

n − upla de enteros no negativos. Si $\alpha = (0,0,\dots 0), x^{\alpha} = 1$ además,

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

Ejemplo 2.2.2. (monomios)

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

Ejemplos 2.2.3. (no monomios)

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

Definición 2.2.4 Sea K un campo. Un polinomio f en $x_1, x_2, \dots, x_n$ con coeficientes en K es una combinación lineal de un numero finito de monomios (con coeficientes en K). Se puede escribir de la siguiente forma:

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

Donde la suma se realiza sobre un número finito de $n - uplas\ \alpha = (\alpha_1, \alpha_2, \dots, \alpha_n.)$.

El conjunto de todos los polinomios en $x_1, x_2 \dots, x_n$ con coeficientes en K se denotará por $K[x_1, \dots, x_n]$ y cuando tratemos con polinomios en un número pequeño de variables, usualmente prescindiremos de los subíndices. De esta manera, polinomios en una, dos y tres variables pertenecerán a $K[x]$, $K[x,y]$ y $K[x,y,z]$ respectivamente.

(O'Shea, Ideals, Varieties, and Algorithms, 2010, pág. 02)

Ejemplo 2.2.5. sea f un polinomio.

$$f(x,y,z) = 2x^3y^5z^4 + 4xyz + xz$$

Es un polinomio en las variables x, y, z;

Pues es una combinación lineal de los términos $2x^3y^5z^4, 4xyz, xz$

Ejemplo 2.2.6. sea f un polinomio.

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

Es un polinomio $\mathbb{Q}[\boldsymbol{x,y,z}]$. Comúnmente se usa las letras de $\boldsymbol{f, g, h, p, q, r}$ para nombrar a los polinomios. Usaremos la siguiente terminología para tratar con ellos.

2.3. TÉRMINOS Y COEFICIENTES

Definición 2.3.1 Sea $\boldsymbol{f = \sum_\alpha a_\alpha x^\alpha}$ un polinomio en $\boldsymbol{K[x_1, \dots, x_n]}$.

i) Donde a_α es el coeficiente del monomio x^α.

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

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

Ejemplo 2.3.2. el polinomio dado anteriormente

$$f = 4x^3y^2z^2 + \frac{5}{2}y^3z^3 - 3xyz + y^2x^4z$$

Consta de 4 términos y grado 7. Se observa que hay 2 términos de grado total máximo, algo que no puede suceder para los polinomios en una variable.

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

$$\boldsymbol{\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha = \sum_\alpha (a_\alpha + b_\alpha) x^\alpha} \quad \boldsymbol{y}$$

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

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

Corolario 2.3.3. Si $\boldsymbol{K}$ es un campo, entonces todo ideal de $\boldsymbol{K[x]}$ se puede escribir de la forma $\boldsymbol{\langle f \rangle}$ para algún $\boldsymbol{f \in K[x]}$. Además, $\boldsymbol{f}$ es único salvo por un factor no nulo en $\boldsymbol{K}$.

Observación: Tenemos resultados interesantes si $\boldsymbol{d(x)}$ es el máximo común divisor de dos polinomios $\boldsymbol{f(x)\ y\ g(x)}$, existen polinomios $\boldsymbol{u(x)\ y\ v(x)}$ tales que los polinomios es una combinación lineal denotada como identidad de (Bezout) $\boldsymbol{f(x).u(x) + g(x).v(x) = d(x)}$, además si los grados de $\boldsymbol{f(x)\ y\ g(x)}$ son mayores que cero , entonces el grado de $\boldsymbol{u(x)}$ es menor que el grado de $\boldsymbol{g(x)}$, y el grado de $\boldsymbol{v(x)}$ es menor que el grado $\boldsymbol{f(x)}$.

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

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

¿Existe un algoritmo para decidir si un polinomio dado $\boldsymbol{f \in K[x]}$. Pertenece al ideal $\boldsymbol{\langle f_1, \dots, f_s \rangle}$? La respuesta es sí, y el algoritmo es fácil de escribir. El primer paso es usar $\boldsymbol{mcd}$ para encontrar un generador $\boldsymbol{h}$ de $\boldsymbol{\langle f_1, \dots, f_s \rangle}$. Entonces, puesto que $\boldsymbol{f \in \langle f_1, \dots, f_s \rangle}$ es equivalente a $\boldsymbol{f \in \langle h \rangle}$, solo necesitamos usar el algoritmo de la división para escribir

$\boldsymbol{f = gh + r}$, donde $\boldsymbol{grad(r) < grad(h)}$, se deduce que $\boldsymbol{f}$ pertenece al ideal si solo si $\boldsymbol{r = 0}$.

Definición 2.2.4 (máximo común divisor generalizado) Un máximo común divisor de los polinomios $\boldsymbol{f_1, \dots, f_s \in K[x]}$ es un polinomio $\boldsymbol{h}$ tal que

- h divide a $f_1, \dots, f_s$
- Si p es otro polinomio que divide a $f_1, \dots, f_s$ luego p divide a h.
- cuando h tiene estas propiedades, escribimos $h = mcd(f_1, \dots, f_s)$

(O'Shea, Ideals, Varieties,and Algoritmhms, 2010, pág. 44)

Proposición 2.3.5. Sean $f_1, \dots, f_s \in K[x]$, donde s $\geq$ 2. Entonces:

i) $mcd(f_1, \dots, f_s) \in$ K[x] existe y es único salvo por la multiplicación de una constante no nula en K.

ii) $mcd(f_1, \dots, f_s) \in$ K[x] es un generador del ideal $\langle f_1, \dots, f_s \rangle$.

iii) Existe un algoritmo para calcular el $mcd(f_1, \dots, f_s)$.

Demostración:

Las pruebas de las partes (i) y (ii) son similares a las principales propiedades de los $\boldsymbol{mcd}$ y serán omitidas.

Probando (iii), sean $h = mcd(f_2, \dots f_s)$, probaremos que:

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

a) Probaremos que $\langle f_1, \dots, f_s \rangle \subset \langle f_1, h \rangle$.

sea
$$f_1 = f_1 + 0h$$
$$\vdots$$
$$f_i = m_i h_i \quad 2 \leq i \leq s,$$

Entonces $\boldsymbol{\langle f_1, \dots, f_s \rangle \in \langle f_1, h \rangle}$. por tanto $\boldsymbol{\langle f_1, \dots, f_s \rangle \subset \langle f_1, h \rangle}$. Sigamos con la otra inclusión

b) $\langle \boldsymbol{f_1}, \boldsymbol{h} \rangle \subset \langle \boldsymbol{f_1}, \dots, \boldsymbol{f_s} \rangle$ recordemos que $\boldsymbol{f_1} \in \langle \boldsymbol{f_1}, \dots, \boldsymbol{f_s} \rangle$ y que **h** puede ser expresado de la siguiente forma por (ii)

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

Entonces, $\boldsymbol{f_1}, \boldsymbol{h} \in \langle \boldsymbol{f_1}, \dots, \boldsymbol{f_s} \rangle$. De esto se deduce que $\langle \boldsymbol{f_1}, \boldsymbol{h} \rangle \subset \langle \boldsymbol{f_1}, \dots, \boldsymbol{f_s} \rangle$. Por tanto, $\langle \boldsymbol{f_1}, \boldsymbol{h} \rangle = \langle \boldsymbol{f_1}, \dots, \boldsymbol{f_s} \rangle$.

Por (ii) de esta proposición vemos que

$$\langle \boldsymbol{mcd}\langle \boldsymbol{f_1}, \boldsymbol{h} \rangle \rangle = \langle \boldsymbol{mcd}\langle \boldsymbol{f_1}, \dots, \boldsymbol{f_s} \rangle \rangle.$$

Entonces $\boldsymbol{mcd}(\boldsymbol{f_1}, \boldsymbol{h}) = \boldsymbol{mcd}(\boldsymbol{f_1}, \dots, \boldsymbol{f_s})$ resulta de la parte de la unidad de **corolario 2.3.3**, lo que prueba lo deseado.

Finalmente, necesitamos demostrar que existe un algoritmo para calcular $\boldsymbol{mcd}(\boldsymbol{f_1}, \dots, \boldsymbol{f_s})$. la idea básica es combinar la parte (iii) con el algoritmo de Euclides. Por ejemplo, supongamos que queremos calcular:

$$\boldsymbol{mcd}(\boldsymbol{f_1}, \boldsymbol{f_2}, \boldsymbol{f_3}, \boldsymbol{f_4})$$

$$mcd\left(f_1, mcd(f_2, f_3, f_4)\right)$$
$$mcd\left(f_1, mcd\left(f_2, mcd\ (f_3, f_4)\right)\right)$$

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

Ejemplo 2.3.6 Calcular el $\boldsymbol{m.c.d}$ de los polinomios $\boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h}, \boldsymbol{i} \in \boldsymbol{K}[\boldsymbol{x}]$.

Sean:

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

El comando del máximo común divisor en la mayoría de los sistemas del algebra computacional solo maneja dos polinomios a la vez. Por lo tanto, para trabajar más de

dos polinomios, tendrá que utilizar el método escrito en la demostración de la proposición anterior.

Consideremos el ideal:

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

Sabemos que $\boldsymbol{mcd(x^6 - 1, x^4 - 1, x^3 - 3x + 2, x^2 - 1)}$ es un generador. Además, se puede verificar que:

$$mcd(x^6 - 1, x^4 - 1, x^3 - 3x + 2, x^2 - 1)$$

$$mcd\big(mcd(x^6 - 1, x^4 - 1), mcd(x^3 - 3x + 2, x^2 - 1)\big)$$

Así se obtiene el máximo común divisor de dos polinomios.

$$mcd(x^2 - 1, x - 1)$$

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

Ahora encontramos en $\boldsymbol{m.c.d}$. Para estos nuevos polinomios por medio del algoritmo de la división tenemos:

$$mcd(x - 1)$$

Por algoritmo de Euclides tenemos el mcd de I es $x - 1$

2.4. IDEALES POLINOMIALES

Definición 2.4.1 Un ideal $I \subset K[x_1, \ldots, x_n]$ es un ideal monomial si existe un subconjunto $A \subseteq Z_{\geq 0}^n$ (posiblemente) finito tal que I esta formado por todos los polinomios que son sumas finitas de la forma:

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

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

Lema 2.4.2 Sea $I = \langle x^\alpha : \alpha \in A \rangle$ un ideal monomial. Entonces un monomio $x^\beta \in I$ si solo si x^β es divisible por x^α para algún $\alpha \in A$.

Demostración:

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

Lema 2.4.3 Sea I un ideal monomial, y sea $f \in K[x_1, \dots, x_n]$ las siguientes afirmaciones son equivalentes:

i) $f \in I$

ii) todo termino de f está en I.

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

Demostración:

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

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

Al desarrollar el producto $h_i x^{\alpha(i)}$ nos quedan términos de la forma $\alpha_j x^{\beta} x^{\alpha(i)} \in I$.(ii)⇐(iii). Para facilitar la demostración veamos que si un término pertenece a I el monomio respectivo pertenece a I.

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

Esto lo podemos hacer porque los coeficientes los tomamos del campo $\boldsymbol{I \subset K[x_1, \dots, x_n]}$.

Entonces podemos trabajar con monomios en $\boldsymbol{I}$ y luego pasarnos al término multiplicando por una constante adecuada al monomio respectivo.

Sea $\boldsymbol{f = \sum_{j=1}^{s} \alpha_{\beta(j)} x^{\beta(j)} \in K[x_1, \dots, x_n]}$, donde cada $\boldsymbol{\alpha_{\beta(j)} x^{\beta(j)} \in I}$. Entonces $\boldsymbol{x^{\beta(j)} \in I.}$

Por tanto. $\boldsymbol{f}$ es una $\boldsymbol{K}$ −combinacion de monomios en $\boldsymbol{I}$ (recuerde que esto significa que $\boldsymbol{f}$es una sumatoria de elementos del campo por monomios).

(iii)⇒(i). si f es una K −combinacion lineal de los monomios en I, f es de la forma:

$$f = \sum_{i=1}^{s} \alpha_{\alpha(i)} x^{\alpha(i)} \in I,$$

Donde $\boldsymbol{\alpha_{\alpha(i)} \in K}$ y $\boldsymbol{x^{\alpha(i)} \in I}$, entonces cada $\boldsymbol{\alpha_{\alpha(i)} x^{\alpha(i)} \in I}$, y como $\boldsymbol{f}$ es una sumatoria de elementos de $\boldsymbol{I}, \boldsymbol{f \in I}$.

Definición 2.4.4 Dado un subconjunto $I \subset K[x_1, \dots x_n]$ es un ideal si satisface:

1. $0 \in I$ (el polinomio constante cero pertenece a I)
2. Si $f, g \in I$, entonces $f + g \in I$ (si dos polinomios pertenecen a I, las sumas pertenecen a I)

3. Si $f \in I$ y $h \in K[x_1, \dots x_n]$, entonces $h.f \in I$. (el producto de un polinomio del ideal por un polinomio cualquiera, es otro polinomio que pertenece al ideal).

El conjunto de polinomios con varias variables $x_1, \dots, x_n$ y con coeficientes en K, siendo Kun cuerpo, forman el anillo de polinomios que denotaremos $K[x_1, \dots x_n]$.

Definición 2.4.5 Sea $\boldsymbol{I \subset K[x_1, \dots x_n]}$ un subconjunto no vacío. $\boldsymbol{I}$ se llama un ideal polinomial si:

a) $f + g \in I$ siempre que $f \in I \; y \; g \in I$

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

Definición 2.4.6 (Suma y producto de ideal)

Si $I \; y \; J$ son ideales, entonces los conjuntos

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

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

son ideales.

(O'Shea, 2010)

Lema 2.4.7. Si $f_1, \dots f_s \in K[x_1, \dots x_n]$ entonces

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

Es un ideal $K[x_1, \dots x_n]$ llamado el ideal generado por $f_1, \dots f_s$

Demostración:

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

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

Entonces.

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

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

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

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

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

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

Definición 2.4.8 Un ideal $\boldsymbol{I}$ es finitamente generado si existen $\boldsymbol{f_1, \dots, f_s} \in \boldsymbol{K[x_1, \dots x_n]}$ tales que

$$\boldsymbol{I} = \langle \boldsymbol{f_1, \dots, f_s} \rangle$$

En este caso decimos que $\boldsymbol{f_1, \dots, f_s}$ forman una base de $\boldsymbol{I}$.

Teorema 2.4.9 (Teorema de la base de Hilbert). El anillo A = $\boldsymbol{K[x_1, \dots x_n]}$ es noetheriano, es decir que satisface cualquiera de las dos condiciones equivalentes siguientes:

1. Todo ideal de A es finitamente generado.

2. Toda cadena ascendente de ideales de A estabiliza

Teorema 2.4.10 (Teorema de los ceros de Hilbert). Si K es un cuerpo algebraicamente cerrado, para todo ideal I de $K[x_1, \dots x_n]$ se tiene:

(versión débil) $V(I) = I,\ I = (1)$

(versión fuerte) $I(V(I)) = \sqrt{I}$

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. MATERIALES

Los materiales necesarios de acuerdo con el tiempo que se programó para este trabajo de investigación esta resumido en la tabla siguiente:

Actividad	Trimestres											
			M	A	M	J	J	A	S	O	N	D
Revisión Bibliográfica						x	x	x	x			
Redacción del proyecto						x						
Presentación del proyecto						x						
Revisión y Aprobación del proyecto						x						
Obtención del borrador de tesis								x				
Sustentación											x	

3.2.PRESUPUESTO

El recurso utilizado para el desarrollo de este proyecto de investigación se ha estimado de la siguiente manera.

Descripción	Costo Unitario (S/.)	Cantidad	Costo total (S/.)
Bibliografía	**60.00**	**10**	**2400.00**
Papel bond	**20.00**	**3 millares**	**60.00**
Fotocopias	**0.10**	**500**	**50.00**
Memoria USB	**30**	**1**	**50.00**
Impresión	**0.20**	**1000**	**100.00**
Uso de internet	**1.00**	**2.00**	**200.00**
otros			**100.00**
Costo total			**2960.00**

3.3. MÉTODOS

El método que se ha utilizado en la presente investigación es lectura, análisis, síntesis, justificación, interpretación y aplicación.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. ORDENES MONOMIALES

Un orden monomial es una ordenación de conjunto de monomios de un anillo de polinomios, se utiliza para poder establecer un algoritmo de división en polinomios, en una variable no se tiene mayor problema ya que se puede ordenar de mayor a menor los monomios del polinomio que queremos dividir y los del divisor, Pero cuando tenemos varias variables, sabemos que no hay una manera única de ordenar los monomios.

La relación de orden > sobre el conjunto de monomios que necesitamos para la división tiene que ser total, para ordenar los monomios de mayor a menor sin ninguna ambigüedad, Además tiene que ser compatible con el producto.

Definición 4.1.1 El conjunto de todos los monomios será denotado por M_n, es decir,

$$\mathrm{M}_n = \left\{ \prod_{i=1}^{n} {x_i}^{\alpha_i}; \alpha_1, \dots, \alpha_n \in \mathbb{N} \right\}$$

En lo que sigue, consideramos $\mathbf{M_n}$ las órdenes que tienen ciertas propiedades. **(Hernandesi, 2010, pág. 9)**

Definición 4.1.2 Una relación de orden $>$ sobre el conjunto de los monomios de A = $\boldsymbol{K[x_1, \dots x_n]}$ es un orden monomial si:

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

(ii) Si $\alpha > \beta$ y $\gamma \in \mathrm{Z}_{\geq 0}^{\mathrm{n}}$, entonces $\alpha + \gamma > \beta + \gamma$.

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

Lema 4.1.3 Una relación de orden $>$ en $\boldsymbol{Z_{\geq 0}^{n}}$ es un buen orden si y solo si toda sucesión estrictamente es decreciente en $\boldsymbol{Z_{\geq 0}^{n}}$

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

es finita.

(O'Shea, Ideals, Varieties,and Algorithms, 2010, pág. 56)

Demostración:

Probaremos esto con el contra reciproco: $>$ no es un buen orden si y solo si existe una sucesión estrictamente decreciente infinita en $\boldsymbol{Z_{\geq 0}^{n}}$.

($\Longrightarrow$) Si $>$ no es un buen orden, entonces algún subconjunto no vacío $\boldsymbol{S} \subset \boldsymbol{Z_{\geq 0}^{n}}$.

No tiene elemento mínimo. Escojamos $\boldsymbol{\alpha(1)} \in \boldsymbol{S}$. Como $\boldsymbol{\alpha(1)}$ no es elemento mínimo, de modo que existe un $\boldsymbol{\alpha(2)} \in \boldsymbol{S}$ con $\boldsymbol{\alpha(1)} > \boldsymbol{\alpha(2)}$. Pero $\boldsymbol{\alpha(2)}$ no es el elemento mínimo, de modo que existe un $\boldsymbol{\alpha(3)} \in \boldsymbol{S}$ son $\boldsymbol{\alpha(2)} > \boldsymbol{\alpha(3)}$. Continuando de esta manera, obtenemos una sucesión estrictamente decreciente;

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

($\Longleftarrow$) Dada una sucesión infinita estrictamente decreciente.

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

Entonces $\{\boldsymbol{\alpha(1)}, \boldsymbol{\alpha(2)}, \boldsymbol{\alpha(3)}, \ldots\}$. Es un subconjunto no vacío de $\boldsymbol{Z_{\geq 0}^{n}}$. Que no tiene elementos mínimos. Por tanto $>$ no es un buen orden.

Definición 4.1.4 (Orden lexicográfico)

Dado dos monomios $\mathbf{x^{\alpha}, x^{\beta}} \in \mathbf{K[x_1, \dots, x_n]}$con $\boldsymbol{\alpha = (\alpha_1, \dots, \alpha_n)}$ y $\boldsymbol{\beta = (\beta_1, \dots, \beta_n)} \in \mathbf{Z^n_{\geq 0}}$.

Decimos que $\boldsymbol{\alpha >_{lex} \beta}$ sí, en la diferencia vectorial $\boldsymbol{\alpha - \beta \in Z^n_{\geq 0}}$. La primera componente sea distinta de cero, de izquierda a derecha es positiva. Entonces este caso escribiremos $\boldsymbol{x^{\alpha} >_{lex} x^{\beta}}$ si $\boldsymbol{\alpha >_{Lex} \beta}$.

(O'Shea, Ideals, Varieties,and Algorithms, 2010, pág. 56)

Ejemplo 4.1.5. Comparación de monomios $\boldsymbol{K[x_1, \dots, x_n]}$ con orden lexicográfico.

Sea $\boldsymbol{xy^2z^2 <_{lex} x^2yz}$ este orden se distingue muy fácilmente, solo hay que fijarse que la primera variable tenga menor grado en el monomio menor. En caso de que la primera variable tenga el mismo grado en ambos monomios, nos fijaremos en que la segunda variable tenga menor grado en el monomio menor y así sucesivamente.

Ejemplo 4.1.6. sea:

$$\boldsymbol{x^3y^3 >_{lex} xy^6, x^5y^3z >_{lex} x^5y^2z^2 \text{ , etc.}}$$

Nota: el orden lexicográfico resulta un orden monomial $K[x_1, \dots, x_n]$

Si $n = 3$ considerando $x_1 > x_2 > x_3$*:*

$$x_1{}^{77} > x_1{}^{76}x_2{}^{666}x_3{}^{666}$$

Proposición 4.1.7 El orden lexicográfico en $Z_{\geq 0}^{n}$. Es un orden monomial

Demostración:

i) Que $>_{lex}$ es un orden total se deduce directamente de la definición y del hecho que el orden numérico usual en $Z_{\geq 0}^{n}$. Es un orden total.

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

iii) Supongamos que $>_{lex}$ no fuera un buen orden. Entonces por el lema (4.1.3), existiría una sucesión estrictamente decreciente finita

$$\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \ldots >$$

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

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

Comenzando en $\alpha(k)$, la segunda y la subsiguiente componente entran en juego en determinar el orden lexicográfico. Las segundas componentes de $\alpha(k)$, $\alpha(k+1)$, ..., forman una sucesión decreciente. Por el mismo razonamiento de antes, las segundas componentes también se "estabilizan "en algún momento. Continuando de la misma

manera, vemos que para algún I, de las $\alpha(I) > \alpha(I+1)$, son todas iguales. Esto contradice el hecho que $\alpha(I) >_{lex} \alpha(I+1)$.

Ejemplo 4.1.8. dado dos polinomios f y g.

$$K[x,y,z], x > y > z;$$

Tenemos los monomios

$$f(x,y,z) = x^6y^3z^2$$

$$g(x,y,z) = x^3y^4z$$

Vamos a ordenar estos monomios según el orden lexicográfico

$$\text{Si } f(x,y,z) >_{lex} g(x,y,z)$$

$$x^6y^3z^2 >_{lex} x^3y^4z$$

$$(6,3,2) - (3,4,1) = (3,-1,1)$$

Por lo tanto $x^6y^3z^2 >_{lex} x^3y^4z$,

Ejemplo 4.1.9.

Sea el polinomio $\boldsymbol{f(x,y,z) = 2xyz^2 + 3z^3 + 5x^3 - y^3z \in K[x,y,z]}$

Escribimos el polinomio de la siguiente manera:

$$f(x,y,z) = 5x^3 + 2xyz^2 - y^3z + 3z^3$$

Sea el polinomio: $\boldsymbol{f(x,y,z) = 5xy^2z + 5z^2 - 6x^3 + 8x^2z^2 \in K[x,y,z]}$

Orden $\boldsymbol{f(x,y,z) = -6x^3 + 8x^2z^2 + 5xy^2z + 5z^2}$

Ejemplo 4.1.10.

Sea el polinomio: $\boldsymbol{g(x,y,z) = x^2y + y + y^3 - x - 1 + xy^2 \in K[x,y,z]}$

Orden $\boldsymbol{g(x,y,z) = x^2y + xy^2 - x + y^3 + y - 1}$

Definición 4.1.11 (Orden lexicográfico graduado).

Dado dos monomios $\boldsymbol{x^{\alpha}, x^{\beta} \in K[x_1, \dots, x_n]}$con $\boldsymbol{\alpha = (\alpha_1, \dots, \alpha_n)}$ y $\boldsymbol{\beta = (\beta_1, \dots, \beta_n) \in Z^n_{\geq 0}}$. diremos que $\boldsymbol{\alpha >_{DegLex} \beta}$ si $\boldsymbol{|\alpha| > |\beta|}$, o en caso de ser $\boldsymbol{|\alpha| = |\beta|}$,si $\boldsymbol{\alpha > deglex \beta}$, donde para un monomio cualquiera $\boldsymbol{\theta}$ las barras,$\boldsymbol{|\theta|}$, denotan el orden de $\boldsymbol{\theta}$, o sea la suma $\boldsymbol{\theta_1 +, \dots + \theta_n}$.

Sea $\alpha . \beta \in \boldsymbol{Z^n_{\geq 0}}$. decimos que $\alpha >_{DegLex} \beta$, si

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

Vemos que el orden lexicográfico graduado ordena con el grado total luego cuando son iguales usaremos el orden lexicográfico,

Ejemplo 4.1.12.

Sea $\boldsymbol{xy^2z^2 >_{DegLex} x^2yz}$ por que $\boldsymbol{|(1,2,2)| = 5 > 4 = |(2,1,1)|}$. En este orden en lo primero que hay que fijarse es en el grado total del monomio. Y será menor el monomio con menor grado.

Ejemplo 4.1.13.

Sea; $\boldsymbol{K[x,y,z], x > y > z}$; Tenemos los monomios

$$f(x,y,z) = x^6y^3z^2$$

$$g(x,y,z) = x^3y^4z$$

Vamos a ordenar estos monomios según el orden lexicográfico graduado entonces:

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

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

Por lo tanto $x^6y^3z^2 >_{DegLex} x^3y^4z$

Ejemplo 4.1.14.

Sea el polinomio $\boldsymbol{f(x,y,z) = 2xyz^2 + 3z^3 + 5x^3 - y^3z \in k[x,y,z]}$

$$\boldsymbol{f(x,y,z) = 2xyz^2 - y^3z + 5x^3 + 3z^3}$$

Sea el polinomio: $f(x,y,z) = 5xy^2z + 5z^2 - 6x^3 + 8x^2z^2 \in k[x,y,z]$

Orden $f(x,y,z) = 8x^2z^2 + 5xy^2z - 6x^3 + 5z^2.$

Ejemplo 4.1.15.

Sea el polinomio: $\boldsymbol{g(x,y,z) = x^2y + y + y^3 - x - 1 + xy^2 \in K[x,y,z]}$

$g(x,y,z) = x^2y + xy^2 + y^3 - x + y - 1.$

Definición 4.1.16 (Orden Lexicográfico Graduado Invertido)

Sea $\boldsymbol{\alpha.\beta \in \mathbf{Z}^n_{\geq 0}}$. decimos que $\boldsymbol{\alpha >_{DegRevLex} \beta}$, *si*

$\boldsymbol{|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i}$, $\boldsymbol{o|\alpha| = |\beta|}$ *Y en* $\boldsymbol{\alpha - \beta \in Z^n_{\geq 0}}$, la primera componente no nula por la derecha es negativa.

Ejemplo 4.1.17.

Si $\boldsymbol{x^2yz^2 >_{DegRevLex} xy^3z}$ pues el grado total de los monomios es el mismo, pero,

Si $\boldsymbol{x^2yz^2 >_{DegRevLex} xy^3z}$ ya que $(\mathbf{2},\mathbf{1},\mathbf{2})-(\mathbf{1},\mathbf{3},\mathbf{1})=(\mathbf{1},-\mathbf{2},\mathbf{1})$ que tiene el primer elemento no nulo por la derecha es negativa. En este orden, en caso de que los grados totales de los monomios sean los mismos, los comparamos siguiendo el orden lexicográfico.

Ejemplo 4.1.18.

Si el anillo de polinomios es $K[x,y,z], x>y>z$;Tenemos los monomios

$$f(x,y,z)=x^6y^3z^2$$

$$g(x,y,z)=x^3y^5z^3$$

Vamos a ordenar estos monomios según el orden lexicográfico graduado Invertido

$$x^6y^3z^2 >_{DegRevLex} x^3y^5z^3$$

$$|(6+3+2)|=11 \text{ y } |(3+5+3)|=11$$

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

Entonces

$$x^6y^3z^2 >_{DegRevLex} x^3y^5z^3$$

$$(6,3,2)-(3,5,3)=(3,-2,-1)$$

Por lo tanto $x^6y^3z^2 >_{DegRevLex} x^3y^5z^3$

Ejemplo 4.1.19.

Sea el polinomio: $\boldsymbol{f(x,y,z) = 5xy^2z + 5z^2 - 6x^3 + 8x^2z^2 \in k[x,y,z]}$

Orden $\boldsymbol{f(x,y,z) = 5xy^2z + 5x^2z^2 - 6x^3 + 5z^2}$

Definición 4.1.20. (Orden Lexicográfico Inverso)

Sea $\boldsymbol{\alpha.\beta \in Z^n_{\geq 0}}$. decimos que $\boldsymbol{\alpha >_{Lexin} \beta}$, si solo si en la diferencia vectorial $\boldsymbol{\alpha - \beta \in Z^n}$, la primera componente no nula por la derecha es positiva.

Ejemplo 4.1.21.

Si $\boldsymbol{xy^3z >_{Lexin} x^2yz^2}$pues el grado total de los monomios es el mismo, pero,

$\boldsymbol{(1,3,1) - (2,1,2) = (-1,2,-1)}$ cuando los grados totales de los monomios coinciden, los comparamos siendo el monomio menor el que tenga grado mayor en la última variable, será menor el que tenga grado mayor en la penúltima variable y así sucesivamente.

Ejemplo 4.1.22.

sí; $\boldsymbol{K[x,y,z], x > y > z}$;

Tenemos los monomios

$$f(x,y,z) = x^6y^3z^2$$

$$g(x,y,z) = x^3y^5z^3$$

Vamos a ordenar estos monomios según el orden lexicográfico inverso

$$x^6y^3z^2 >_{Lexin} x^3y^5z^3$$

$$x^6y^3z^2 > lex\ graduado\ \ invertido\ x^3y^5z^3$$

$$(6,3,2) - (3,5,3) = (3,-2,-1)$$

Por lo tanto $x^6y^3z^2 >_{Lexin} x^3y^5z^3$.

Ejemplo 4.1.23.

Sea el polinomio: $\boldsymbol{f(x,y,z) = 5xy^2z + 5z^2 - 6x^3 + 8x^2z^2 \in k[x,y,z]}$

Orden

$f(x,y,z) = 8x^2z^2 + 5z^2 + 5xy^2z - 6x^3$.

Observación:

Para aclarar la relación entre el orden lexicográfico graduado con el orden lexicográfico graduado Invertido, observe que ambos usan el grado total del mismo modo. Pero la diferencia está en qué el orden lexicográfico graduado usa orden lexicográfico, es decir, observa la variable (mayor o) más a la izquierda y escoge la **mayor potencia. En** cambio, cuando en el DegReglex coinciden los grados totales, observa la variable (menor o) más a la derecha y escoge la menor potencia.

Definición 4.1.24 (coeficiente, Monomios Principal)

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

El multigrado de $\boldsymbol{f}$ es

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

(El máximo es tomado respecto a $>$).

El coeficiente principal de f = coeficiente líder de f es

$$\boldsymbol{cp(f) = cl(f) = a_{multigrad(f)} \in K.}$$

El monomio principal = monomio líder de f es

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

El término principal= término líder de $\boldsymbol{f}$ es

$$tp(f) = tl(f) = cl(f).ml(f)$$

sea $\boldsymbol{f(x,y,z) = 6xy^3z + 3y^2z - 7x^4 - 8x^2y^3}$ y sea $>$ el orden lexicográfico.

Entonces:

Ordenamos lexicográficamente el polinomio

$multigrad(f) = (4,0,0)$	$cl(f) = -7$	$ml(f) = x^4$	$tl(f) = 7x^4$

Lema 4.1.25

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

Entonces:

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

2) *si* $f + g \neq 0$, entonces

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

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

4.2. ALGORITMO DE LA DIVISIÓN

4.2.1 Teorema (algoritmo de la división) dado $g(x) \in \mathbb{K}[x] \setminus \{0\}$, para cualquier $f(x) \in \mathbb{K}[x]$ existen $q(x), r(x) \in \mathbb{K}[x]$ únicamente determinados con las condiciones:

$$f = qg + r, \text{ con } r(x) = 0 \text{ o } gr(r(x)) < gr(g(x))$$

Demostración

(Existencia) sean $f(x)$ y $g(x)$ polinomios tales que $g(x) \neq 0$ en $f(x)$; si $f(x) = 0$ entonces tomemos $q(x) = r(x) = 0$ tal que: $f(x) = g(x)q(x) + r(x)$ con $r(x) = 0$

Ahora si $f(x) \neq 0$ vamos proceder la demostración por inducción en $gr(f)$.

Si $gr(f) < gr(g)$, entonces tomamos $q = 0$ e $r = f$ tenemos $.g + f$ e obtenemos lo deseado.

Por otro lado, si $gr(f) \geq gr(g)$, entonces $tl(g)$ divide a $tl(f)$ es así,

$$tl(f) = \frac{tl(f)}{tl(g)} tl(g).$$

Si $tl(f) = \frac{tl(f)}{tl(g)}(g) = 0$, entonces tomamos $q = \frac{tl(f)}{tl(g)}$ e $r = 0$ obtenemos lo deseado.

Si $f - \frac{tl(f)}{tl(g)}(g) \neq 0$,entonces

$$gr\left(f - \frac{tl(f)}{tl(g)} g\right) < gr(f)$$

Por hipótesis de la inducción, existen polinomios $q_1, r_1 \in \mathbb{K}[x]$ tal que

$$f - \frac{tl(f)}{tl(g)} g = q_1 g + r_1,$$

Como $r_1 = 0$ o $gr(r_1) < gr(g)$así.

$$f = \left(\frac{tl(f)}{tl(g)} + q_1\right) g + r_1.$$

Ahora, tomando $q = \frac{tl(f)}{tl(g)} + q_1$ y $r_1 = r$ tenemos lo deseado.

Supongamos que existen $q_1, q_2, r_1, r_2 \in \mathbb{K}[x]$tale que

$$f = q_1 g + r_1 \quad \text{e} \quad f = q_2 g + r_2$$

Con $r_i = 0$ o $gr(r_1) < gr(g)$ para $i \in \{1,2\}$. Así, podemos afirmar que

$gr(g) > max\{gr(r_1), gr(r_2)\}$. Sigue que

$$0 = f - f = (q_1 - q_2)g + (r_1 - r_2)$$

O sea,

$$r_2 - r_1 = (q_1 - q_2)g$$

Si $r_2 \neq r_1$, entonces

$$gr(g) > max\{gr(r_1), gr(r_2)\} \geq gr(r_2 - r_1) = gr\big((q_1 - q_2)g\big) \geq gr(g).$$

¡Absurdo!

Si, $r_2 = r_1$ y $(q_1 - q_2)$. Como $\mathbb{K}[x]$ es un dominio y $g \neq 0$,

Se sigue que $q_1 - q_2 = 0$ entonces obviamente $q_1 = q_2$. Probado.

Teorema 4.2.2 Algoritmo de la división multivariada

La meta de esta sección es generalizar el algoritmo de la división de polinomios en una variable a polinomios en varias $(\boldsymbol{n})$variables, también llamado proceso de reducción. la principal diferencia es que usamos un algoritmo que divide un polinomio por un conjunto de polinomios; este algoritmo es esencial para obtención de Bases de Grobner de un conjunto de polinomios.

Fijemos un orden monomial $>$ en $\boldsymbol{Z^n_{>0}}$, considere $\boldsymbol{F} = (\boldsymbol{f_1}, \dots, \boldsymbol{f_s})$ una S-uplas ordenada de polinomios en $\mathbf{K}[\mathbf{x_1}, \dots \mathbf{x_n}]$. Entonces cada $\boldsymbol{f} \in \mathbf{K}[\mathbf{x_1}, \dots \mathbf{x_n}]$ puede ser escrito en forma:

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

donde los "coeficientes" $\boldsymbol{a_1}, \dots, \boldsymbol{a_s}$, y el resto $\boldsymbol{r}$ pertenece $\boldsymbol{K}[\boldsymbol{x_1}, \dots \boldsymbol{x_n}]$ la idea básica del algoritmo es cancelar el término principal de $\boldsymbol{f}$ usando el termino principal de

algún $\boldsymbol{f_i}$ y repetir este proceso hasta que no se pueda hacer, y $\boldsymbol{r = 0}$ o $\boldsymbol{r}$ es una combinación lineal de monomios (con coeficientes en $\boldsymbol{K}$), ninguno de los cuales es divisible por alguno de $\boldsymbol{tl(f_1), \dots, tl(f_s)}$.

Llamaremos a $\boldsymbol{r}$ un residuo de la división de $\boldsymbol{f}$ por $\boldsymbol{F}$ y se denota por $\overline{\boldsymbol{f}}^{\boldsymbol{F}}$. Además, si $\boldsymbol{a_i f_i \neq 0}$, entonces tenemos $\boldsymbol{multigrad(f) \geq multigrad(a_i f_i)}$. Veremos un ejemplo**.**

Ejemplo 4.2.3. Dividir $\boldsymbol{f}$ por $\boldsymbol{F = (g(x), h(x))}$**.**

Para ilustrar el algoritmo de la división en $\boldsymbol{K[x_1, \dots x_n]}$**.**

Dados:

$$f(x) = 3x^3 - 4x^2 - 5x - 2$$

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

$$\boldsymbol{h(x) = x - 2}$$

Dividiendo f por g y h obtenemos:

Por tanto:

$$\begin{array}{r|l} 3x^3 - 4x^2 - 5x - 2 & x^2 - 1 \;;\; x - 2 \\ \cline{2-2} -3x^3 \quad + 3x & 3x - 4 \;;\; -2 \\ \cline{1-1} -4x^2 - 2x - 2 & \\ 4x^2 \quad - 4 & \\ \cline{1-1} -2x - 6 & \\ 2x - 4 & \\ \cline{1-1} -10 & \end{array}$$

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

Ejemplo 4.2 4.

Queremos dividir $\boldsymbol{f(x,y) = x^2y + xy^2 + y^2}$ entre $\boldsymbol{g(x,y) = xy - 1}$ y $\boldsymbol{h(x,y) = y^2 - 1}$ usaremos el orden lexicográfico con $\boldsymbol{x > y}$ como $\boldsymbol{ml(f)}$ es múltiplo de $\boldsymbol{ml(g)}$ primero dividiremos entre $\boldsymbol{g}$.

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

Como $\boldsymbol{x + y + 1}$ no son divisibles por $\boldsymbol{ml(f)}$ ni por $\boldsymbol{ml(g)}$ por tanto queda como resto, y termina la división.

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

Ejemplo 4.2.5.

$\boldsymbol{f(x) = x^2y + xy^2 + y^2 \in R[x,y]}$ $\boldsymbol{y}$ $\{\boldsymbol{xy - 1, y^2 - 1}\} \subset \mathbb{R}[\boldsymbol{x,y}]$, Respecto al orden lexicográfico $(\mathbf{y \leq x})$ tenemos

$$
\begin{array}{l|l|l}
x^2y + xy^2 + y^2 & xy - 1, y^2 - 1 & x \\
\underline{-x^2y + x} & x + y \quad 1 & y + 1 \\
xy^2 + x + y^2 & & \\
\underline{-xy^2 \quad + \quad y} & & \\
x + y^2 + y & & \\
\underline{-x} & & \\
y^2 + y & & \\
\underline{-y^2 + 1} & & \\
Y + 1 & &
\end{array}
$$

Al final de la división tenemos $f = (x + y)(xy - 1) + (y^2 - 1) + (x + y + 1)$

Ejemplo 4.2.6.

Sea en $\boldsymbol{K[x, y]}$ con el orden lexicográfico $\mathbf{x > y}$, dividimos $\boldsymbol{f = xy^2 + 1}$ entre $\boldsymbol{f_1 = xy + 1}$ y $\boldsymbol{f_2 = y + 1}$

$$
\begin{array}{l|ll}
xy^2 + 1 & xy + 1, \ y + 1 & \\
\underline{-xy^2 - y} & y \quad -1 & \\
-y + 1 & & \\
\underline{+y + 1} & & \\
2 & &
\end{array}
$$

Por tanto:

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

Definición 4.2.7 Sea $I \subset K[x_1, \ldots x_n]$ un ideal distinto de cero $\{0\}$.

Sea $I \subset K[x_1, \ldots x_n]$ un ideal distinto de cero $\{0\}$.

Denotamos por $\boldsymbol{tl(I)}$ al conjunto de todos los términos principales de los elementos de $\boldsymbol{I}$. Así

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

Denotado por $\langle \boldsymbol{tp(I)} \rangle$. Al ideal generado por los elementos $\boldsymbol{tp(I)}$.

Proposición 4.2.8. Sea $\boldsymbol{I \subset K[x_1, \dots x_n]}$ un ideal $\langle \boldsymbol{tp(I)} \rangle$. Es un ideal monomial.

Existe $\boldsymbol{g_1, \dots, g_t \epsilon I}$ tal que $\langle \boldsymbol{tp(I)} \rangle = \langle \boldsymbol{tp(g_1)} \rangle, \dots, \langle \boldsymbol{tp(g_t)} \rangle$.

4.3 BASES DE GROBNER

Definición 4.3.1 Fijado un orden monomial en $\boldsymbol{K[x_1, \dots x_n]}$, un conjunto finito $\boldsymbol{G = \{g_1, \dots, g_t\}}$ de un ideal $\boldsymbol{I \subset K[x_1, \dots x_n]}$ es una Base de Grobner para $\boldsymbol{I}$ si

$$\langle \boldsymbol{tp(g_1)} \rangle, \dots, \langle \boldsymbol{tp(g_t)} \rangle = \langle \boldsymbol{tp(I)} \rangle$$

Equivalentemente, un conjunto $\boldsymbol{G = \{g_1, \dots, g_t\} \subset I}$ es una base de Grobner de $\boldsymbol{I}$ si solo si el término principal de cualquier elemento de $\boldsymbol{I}$ es divisible por uno de los $\boldsymbol{tp(g_i)}$.

Corolario 4.3.2.

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

Propiedades de las bases de Grobner

Proposición 4.3.3

Sea $\boldsymbol{G = \{g_1, \dots, g_t\}}$ una base de Grobner para un ideal $\boldsymbol{I \subset K[x_1, \dots x_n]}$, y sea $\boldsymbol{f \in K[x_1, \dots x_n]}$ entonces existe un único $\boldsymbol{r \in K[x_1, \dots x_n]}$ con las siguientes propiedades:

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

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

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

Observación:

El residuo de $\boldsymbol{r}$ es a veces llamado la forma normal de $\boldsymbol{f}$ y sus propiedades de unicidad serán exploradas en los ejercicios. En realidad, las bases de Grobner pueden ser caracterizadas por la unicidad del residuo.

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

Corolario 4.3.4.

Sea $\boldsymbol{G = \{g_1, \dots, g_t\}}$ una base de Grobner para un ideal $\boldsymbol{I \subset K[x_1, \dots x_n]}$. Sea $\boldsymbol{f \in K[x_1, \dots x_n]}$. Entonces $\boldsymbol{f \in I}$ sí y solo si el residuo de la división de $\boldsymbol{f}$ por $\boldsymbol{G}$ es cero.

Definición 4.3.5 Denotaremos por $\boldsymbol{\bar{f}^F}$ al residuo que resulta de dividir $\boldsymbol{f}$ por la S-upla ordenada $\boldsymbol{F = (f_1, \dots, f_s)}$. Si $\boldsymbol{F}$ es una base de Grobner para $\boldsymbol{\langle f_1, \dots, f_s \rangle}$, entonces podemos considerar a $\boldsymbol{F}$ como un conjunto (sin orden en particular).

Ejemplo 4.3.6.

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

Si tenemos los siguientes polinomios: f dividido por g.

$$g(x;y) = x^3y^2 - y^3$$

$$h(x;y) = x^5y^3 - y^3$$

$$\begin{array}{r|l} x^6y^2 & x^3y^2-y^3;\ x^5y^3-y^3 \\ \underline{-x^6y^2+x^3y^2} & x^3+y \\ x^3y^2 & \\ \underline{-x^3y^2+y^4} & \\ y^4 & \end{array}$$

Entonces tenemos el resto de la división: y^4

Entonces $\bar{f}^F = r = \overline{x^6y^2}^{\{x^3y^2-y^3, x^5y^3-y^3\}} = y^4$

Puesto que con el algoritmo de la división produce

$$\boldsymbol{x^6y^2 = (x^3+y)(x^3y^3-y^3) + 0\left(x^5y^3-y^3\right) + y^4}$$

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

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

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

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

Así su término principal está en $\langle \boldsymbol{tp}(\boldsymbol{I}) \rangle$.

Definición 4.3.8 $(\boldsymbol{S-polinomio})$ Sean $\boldsymbol{f, g} \in \boldsymbol{k}\ [\boldsymbol{x_1}, \dots, \boldsymbol{x_n}]$ polinomios no nulos.

Si el $\boldsymbol{multigrad\,(f) = \alpha\ y\ el\ multigrad\,(g) = \beta, entonces\ \rho =}$ $(\boldsymbol{y_1, \dots, y_n})$ donde $\boldsymbol{p_i = max\,(\alpha_i, \beta_i)}$ para cada $\boldsymbol{I}$. llamamos a $\boldsymbol{x^{\rho}}$ el mínimo común múltiplo del $\boldsymbol{mp\,(f)\ y\ mp(g), y}$ escribimos.

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

Un $S-$ polinomio f y g es la combinación

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

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

Ejemplo 4.3.9

Calcular el $\boldsymbol{S-polinomio}$ $\boldsymbol{f(x,y,z) = (4x^2z - 7y^2), g(x,y,z) = (xyz^2 + 3xz^2)} \in \mathbf{R}[\boldsymbol{x,y}]$ con el orden $\boldsymbol{lex}$.

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

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

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

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

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

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

Ordenando según $\boldsymbol{lex}$.

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

Lema 4.3.10. Supongamos que tenemos una suma $\sum_{i=1}^{s} \boldsymbol{c_i f_i}$, donde $\boldsymbol{c_i} \in \boldsymbol{K}$ y el $\boldsymbol{multigrad}\,(\boldsymbol{f_i}) = \boldsymbol{\delta} \in \mathbb{Z}_{\geq 0}^{n}$ para todo $\boldsymbol{i}$. Si el $\boldsymbol{multigrad}(\sum_{i=1}^{s} \boldsymbol{c_i f_i}) < \boldsymbol{\delta}$, entonces $(\sum_{i=1}^{s} \boldsymbol{c_i f_i})$ es una combinación lineal. Con coeficientes en K, de los:

$\boldsymbol{S - polinomio\ S(f_j, f_k)}$ para $\boldsymbol{1 \leq jk \leq s}$. Además cada $\boldsymbol{S(f_j, f_k)}$ tiene $\boldsymbol{multigrad < \delta}$..

4.4. ALGORITMO DE BUCHBEGER

Teorema 4.4.1. (Criterio de los S −pares de Buchberger)

Sea $\boldsymbol{I}$ un ideal polinomial. Entonces una base $\boldsymbol{G} = \{\boldsymbol{g_1}, \ldots, \boldsymbol{g_t}\}$ de $\boldsymbol{I}$ es una base de Grobner de $\boldsymbol{I}$ si y solo si para toda la pareja $\boldsymbol{i \neq j}$, el residuo de la división de $\boldsymbol{S(g_i, g_j)}$ por $\boldsymbol{G}$ (listado en cierto orden) son cero.

Demostración:

⇒ Si $\boldsymbol{G}$ es una base de Grobner, entonces, dado que $\boldsymbol{S(g_i, g_j)} \in \boldsymbol{I}$, el residuo de la división por $\boldsymbol{G}$ es cero por **corolario 4.3.4**.

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

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

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

Del lema 2.4.2, se sigue que

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

Si la igualdad no ocurre, entonces alguna cancelación entre los términos principales de (2) debe ocurrir. **el lema 4.3.10**. nos permitirá rescribir esto en términos de los $\boldsymbol{S-polinomios}$. Entonces nuestra suposición de que $\boldsymbol{S-polinomios}$ tiene residuo cero permitirá reemplazar los $\boldsymbol{S-polinomios}$ por extensiones para $\boldsymbol{f}$ que tenga menos cancelaciones de términos principales. Continuando de esta manera, encontramos eventualmente una expresión (2) para $\boldsymbol{f}$ donde la igualdad ocurre en (3). Entonces

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

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

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

Entonces la desigualdad (3) se vuelve

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

Ahora consideremos todas las posibles maneras en que $\boldsymbol{f}$ puede ser de la forma (2). Para cada una de estas expresiones, obtenemos posiblemente un $\boldsymbol{\delta}$ deferente. Ya que un orden monomial es un buen orden, podemos seleccionar una expresión (2) para $\boldsymbol{f}$ tal que $\boldsymbol{\delta}$ sea mínimo.

Mostraremos que una vez que este $\boldsymbol{\delta}$ mínimo es escogido, tenemos $\boldsymbol{multigrad\,(f) = \delta}$. Entonces la igualdad ocurre en (3), y como observamos, se sigue $\boldsymbol{tp(f) \in \langle tp(g_1), \ldots, tp(g_t)\rangle}$ esto probara el teorema.

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

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

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

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

Tiene exactamente la forma $\boldsymbol{f_i = x^{\alpha(i)} g_i}$. así el **lema (4.3.10)** implica esta suma es una combinación lineal de los $\boldsymbol{S - polinomios}$. $\boldsymbol{S\big(x^{\alpha(j)} g_j\,,\ x^{\alpha(k)} g_k\big)}$. Sin embargo,

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

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

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

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

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

Donde $\boldsymbol{x^{\gamma_{jk}} = mcm(mp(g_i), mp(g_k))}$. Así existe la constante $\boldsymbol{c_{jk} \in K}$ tales que

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

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

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

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

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

Para todo $\boldsymbol{i, j, k}$ ver **teorema (4.2.2.).** Intuitivamente, esto dice que cuando el residuo es cero, podemos encontrar una expresión para los $\boldsymbol{S(g_j, g_k)}$ en términos de $\boldsymbol{G}$ donde los términos principales no todos se cancelan.

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

Donde $\boldsymbol{b_{ijk} = x^{\delta-\gamma_{jkS}} a_{ijk}}$. Entonces (7) y el **lema (4.2.10)** implica que

$$multigrad(b_{ijk} g_i) \leq multigrad\left(x^{\delta-\gamma_{jkS}} S(g_j, g_k)\right) < \delta \qquad (8)$$

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

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

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

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

Para el paso final de la prueba, sustituyamos $\sum_{\boldsymbol{m(i)=\delta}} \boldsymbol{tp(h_i)g_i} = \sum_{\boldsymbol{i}} \boldsymbol{\bar{h}_i g_i}$ en la ecuación (4)

Para obtener una expresión para $\boldsymbol{f}$ como una combinación polinomica de los $\boldsymbol{g_i}$ donde todos los términos tienen $\boldsymbol{multigrad < \delta}$ esto contradice la minimalidad de $\boldsymbol{\delta}$ y completa la prueba de teorema.

Teorema 4.4.2 (Algoritmo de Buchberger)

Sea $\boldsymbol{I \subset K[x_1, \dots, x_n]}$ un ideal. Entonces una base de Gröbner $\boldsymbol{G = \{g_1, \dots, g_t\}}$ de $\boldsymbol{I}$ es una base de Grobner de $\boldsymbol{I}$ si solo si para cada par $\boldsymbol{i \neq j}$, el resto de la división de $\boldsymbol{S(g_i, g_j)}$ entre $\boldsymbol{G}$ es cero.

Ejemplo 4.4.3.

Encontrar una base de Gröbner para el ideal $\boldsymbol{I}$.

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

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

$$f(x, y, z) = x^2y^2 - z$$

$$g(x, y, z) = \ xy^2z - xyz$$

Ahora encontraremos $\boldsymbol{S - polinomios}$ para $\boldsymbol{f_1, f_2}$, tenemos la fórmula.

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

$$x^p = x^2y^2z$$

$$tp(f_1) = x^2y^2$$

$$tp(f_2) = x^2y^2z$$

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

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

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

Ordenamos de forma $lexicográfica$.

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

Aplicando el algoritmo de la división para $\boldsymbol{S(f_1, f_2)}$ por $\boldsymbol{f_1 \quad y \quad f_2}$.

Bueno esta división tiene residuo es: $\boldsymbol{x^2yz - z^2}$ entonces incluimos al generador

$$\begin{array}{l|ll} x^2yz - z^2 & x^2y^2 - z,\ xy^2z - xyz & \\ \hline 0 & 0 & 0 \\ \hline x^2yz - z^2 & & \\ 0 & & \\ \hline x^2yz - z^2 & & \end{array}$$

Entonces $f_3 = x^2yz - z^2$

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

Luego obtenemos $\overline{s(f_1, f_2)}^F$

$$\begin{array}{l|lll} yz^2 - z^2 & x^2y^2 - z\ , xy^2z - xyz\ , x^2yz - z^2 & & \\ \hline 0 & 0 & 0 & 0 \\ \hline yz^2 - z^2 & & & \\ \hline 0 & & & \\ \hline yz^2 - z^2 & & & \\ \hline 0 & & & \\ \hline yz^2 - z^2 & & & \end{array}$$

Por lo tanto, el residuo es: $\overline{s(f_1,f_2)}^{F} = 0$

Encontramos S-polinomio $s(f_1,f_3)$

$$x^p = x^2y^2z$$

$$tpf_1 = x^2y^2$$

$$tpf_3 = x^2y\mathbf{z}$$

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

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

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

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

Ordenando de forma $Lexicográfico$.

Obtenemos

$$\boldsymbol{s(f_1,f_3) = yz^2 - z^2}$$

Luego usamos el algoritmo de la división para $s(f_1,f_3)$para F

Ya que nuestro residuo no es nulo agregamos a nuestro generador

$$f_4 = yz^2 - z^2$$

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

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

$$\begin{array}{l|l} yz^2 - z^2 & x^2y^2 - z \;,\; xy^2z - xyz \;,\; x^2yz - z^2 \;,\; yz^2 - z^2 \\ \hline 0 & 0 \qquad 0 \qquad 0 \qquad 1 \\ \hline yz^2 - z^2 & \\ \hline 0 & \\ \hline yz^2 - z^2 & \\ \hline 0 & \\ \hline yz^2 - z^2 & \\ \hline -yz^2 + z^2 & \\ \hline 0 & \end{array}$$

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

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

$$\boldsymbol{x^{\rho} = x^2y^2y^2}$$

$$\boldsymbol{tp(f_1) = x^2y^2}$$

$$\boldsymbol{tp(f_4) = yz^2}$$

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

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

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

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

Ordenamos el polinomio de forma $lexicográfica$

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

$$x^2yz^2 - yz^2 \;\big|\; \underline{x^2y^2 - z,\ xy^2z - xyz,\ x^2yz - z^2,\ yz^2 - z^2}$$

$$\underline{x^2yz - z^2} \qquad 0 \qquad 0 \qquad -1 \qquad 1$$

$$yz^2 - z^2$$

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

$$0$$

Ya que nuestro residuo es cero. Por lo tanto, no debemos incluir al conjunto generador.

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

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

$$\boldsymbol{x^{\rho} = x^2y^2z^2}$$

$$\boldsymbol{tp(f_1) = x^2y^2}$$

$$\boldsymbol{tp(f_4) = yz^2}$$

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

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

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

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

Según el orden $\boldsymbol{lexicográfico}$.

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

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

$$x^2yz^2 - z^3 \quad \left| \underline{x^2y^2 - z, xy^2z - xyz, x^2yz - z^2, yz^2 - z^2} \right.$$

$$\underline{-x^2yz^2 + z^3} \qquad 0 \qquad 0 \qquad 0 \qquad 0$$

$$0$$

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

$\boldsymbol{x^p} = x^2y^2z$ *de término lideres*

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

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

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

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

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

Luego utilizando el algoritmo de la división para $\boldsymbol{S(f_2, f_3)}$ por F

$$-x^2yz + yz^2 \quad \left| \underline{x^2y^2 - z\,, xy^2z - xyz\,, x^2yz - z^2, yz^2 - z^2} \right.$$

$$\underline{0} \qquad 0 \qquad 0 \qquad -1 \qquad 1$$

$$-x^2yz + yz^2$$

$$\underline{0}$$

$$-x^2yz + yz^2$$

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

$$yz^2 - z^2$$

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

$$0$$

Ya nuestro residuo es cero no debemos incluir en nuestro conjunto generador

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

Encontrando *S*-polinomios $S(f_2, f_4)$

$$\boldsymbol{x^p = xy^2z^2}$$

$$\boldsymbol{tp(f_2) = xy^2z}$$

$$\boldsymbol{tp(t_4) = yz^2}$$

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

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

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

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

Ya qué nuestro s-polinomio es cero. Por tanto, F no tiene ningún cambio.

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

Encontremos *S*-polinomio $\boldsymbol{S(f_3, f_4)}$

$$\boldsymbol{x^p = x^2yz^2}$$

$$\boldsymbol{tp(f_3) = x^2yz}$$

$$\boldsymbol{tp(f_4) = yz^2}$$

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

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

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

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

Ordenando según $\boldsymbol{lex}$

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

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

$$x^2z^2 - z^3 \quad \left| \begin{matrix} x^2y^2 - z\,,\, xy^2z - xyz\,,\, x^2yz - z^2, yz^2 - z^2 \end{matrix} \right.$$

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 \end{matrix}$$

$$x^2z^2 - z^3$$

$$0$$

$$x^2z^2 - z^3$$

$$0$$

$$x^2z^2 - z^3$$

$$0$$

$$x^2z^2 - z^3$$

Nuestro residuo no es nulo. Por tanto, incluimos nuestro residuo en nuestro conjunto generador $\boldsymbol{f_5 = x^2z^2 - z^3}$.entonces

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

Luego determinamos $\overline{s(f_3, f_4)}^F$ obtenemos*:*

$$x^2z^2 - z^3 \quad \left| x^2y^2 - z \;, xy^2z - xyz \,, x^2yz - z^2, yz^2 - z^2, x^2z^2 - z^3 \right.$$

$$0 \qquad 0 \qquad 0 \qquad 0 \qquad 0 \qquad 1$$

$$x^2z^2 - z^3$$

$$0$$

$$x^2z^2 - z^3$$

$$0$$

$$x^2z^2 - z^3$$

$$0$$

$$x^2z^2 - z^3$$

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

$$0$$

Entonces tenemos

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

Encontrar S- polinomio de $\overline{s(f_3,f_5)}^F$

$$\boldsymbol{x^{\rho} = x^2yz^2}$$

$$\boldsymbol{tp(f_3) = x^2yz}$$

$$\boldsymbol{tp(f_5) = x^2z^2}$$

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

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

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

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

Ordenamos de forma ***lexicográfica***.

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

Luego utilizamos el algoritmo de la división para $\boldsymbol{S(f_3, f_5)}$ por $\boldsymbol{F}$

$$
\begin{array}{l|llllll}
yz^3 - z^3 & x^2y^2 - z\,,\, xy^2z - xyz\,,\, x^2yz - z^2, yz^2 - z^2, x^2z^2 - z^3 \\
\underline{\quad 0 \quad} & 0 & 0 & 0 & 0 & 1 \\
yz^3 - z^3 & & & & & \\
\underline{\quad 0 \quad} & & & & & \\
yz^3 - z^3 & & & & & \\
\underline{\quad 0 \quad} & & & & & \\
yz^3 - z^3 & & & & & \\
\underline{\quad 0 \quad} & & & & & \\
yz^3 - z^3 & & & & &
\end{array}
$$

Nuestro residuo de la división es cero. Por tanto, no incluimos a nuestro conjunto generador. Por tanto, no tenemos cambios de $\boldsymbol{F}$

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

Encontramos S – polinomios $S(f_4, f_5)$

$$\boldsymbol{x^{\rho} = x^2yz^2}$$

$$\boldsymbol{tp(f_3) = yz^2}$$

$$\boldsymbol{tp(f_5) = x^2z^2}$$

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

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

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

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

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

$$
\begin{array}{l|llllll}
-x^2z^2+yz^3 & x^2y^2-z\,, xy^2z-xyz\,, x^2yz-z^2, yz^2-z^2, x^2z^2-z^3 \\
\hline
0 & 0 & 0 & 0 & z & -1 \\
\hline
-x^2z^2+yz^3 & & & & & \\
\hline
0 & & & & & \\
\hline
-x^2z^2+yz^3 & & & & & \\
\hline
0 & & & & & \\
\hline
-x^2z^2+yz^3 & & & & & \\
\hline
x^2z^2-z^3 & & & & & \\
\hline
yz^3-z^3 & & & & & \\
\hline
-yz^3+z^3 & & & & & \\
\hline
0 & & & & &
\end{array}
$$

Por tanto, nuestro residuo es cero no debemos incluir a nuestro conjunto generador. Por tanto, $\boldsymbol{F}$ no tiene ningún cambio.

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

$$= \{x^2y^2 - z\,, xy^2z - xyz\,, x^2yz - z^2, yz^2 - z^2, x^2z^2 - z^3\}$$

Encontramos S – polinomios $S(f_1, f_5)$

$$\boldsymbol{x^{\rho} = x^2y^2z^2}$$

$$\boldsymbol{tp(f_1) = x^2y^2}$$

$$\boldsymbol{tp(f_5) = x^2z^2}$$

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

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

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

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

Ordenamos según lex.

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

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

$$\begin{array}{l|l} y^2z^3 - z^3 & x^2y^2 - z\,,\, xy^2z - xyz\,,\, x^2yz - z^2, yz^2 - z^2, x^2z^2 - z^3 \\ \hline 0 \qquad 0 \qquad 0 \qquad 0 \qquad yz + z \qquad 0 \end{array}$$

$$y^2z^3 - z^3$$

$$0$$

$$y^2z^3 - z^3$$

$$0$$

$$y^2z^3 - z^3$$

$$-y^2z^2 + yz^3$$

$$yz^3 - z^3$$

$$-yz^3 + z^3$$

$$0$$

Nuestro residuo es cero. Por tanto, no se incluye a nuestro conjunto generador.

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

$$= \{x^2y^2 - z\,,\, xy^2z - xyz\,,\, x^2yz - z^2, yz^2 - z^2, x^2z^2 - z^3\}$$

Encontramos *S- polinomio* $S(f_2, f_5)$

$$\boldsymbol{x^{\rho} = x^2y^2z^2}$$

$$\boldsymbol{tp(f_2) = xy^2z}$$

$$\boldsymbol{tp(f_5) = x^2z^2}$$

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

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

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

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

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

$$-x^2yz^2 + y^2z^3 \,\big|\, \underline{x^2y^2 - z\,,\, xy^2z - xyz\,,\, x^2yz - z^2,\, yz^2 - z^2,\, x^2z^2 - z^3}$$

$$0 \qquad 0 \qquad 0 \qquad 0 \qquad yz \qquad -y$$

$$-x^2yz^2 + y^2z^3$$

$$\underline{\quad 0 \quad}$$

$$-x^2yz^2 + y^2z^3$$

$$\underline{\quad 0 \quad}$$

$$-x^2yz^2 + y^2z^3$$

$$\underline{x^2yz^2 - yz^3}$$

$$y^2z^3 - yz^3$$

$$\underline{-y^2z^3 + yz^3}$$

$$0$$

Ya que nuestro residuo es cero. Por tanto, no debemos incluir al conjunto generador. Por tenemos.

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

Ya concluimos todas las combinaciones podemos observar que

$$\overline{s(f_v, f_J)}^{\{f_1, f_2, f_3, f_4, f_5\}} = 0 \;\; \forall\, i > j,$$

Y así finalmente se tiene que

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

$$F = \{x^2y^2 - z\,, xy^2z - xyz\,, x^2yz - z^2, yz^2 - z^2, x^2z^2 - z^3\}.$$

Es una base de Gröbner.

Ejemplo 4.4.4.

Usando la aplicación (COCOA)

Encontrar una base de Gröbner para el ideal I

$$I = \langle f, g\rangle = \langle x^2y^2 - z, xy^2z - xyz\rangle$$

```
Use R: = QQ [X, Y, Z], Lex;

G: = GBasis (Ideal (X^2*Y^2-Z, X* Y^2*Z-X*Y*Z));

G;

[x* Y^2*Z- X*Y*Z, X^2*Y^2-Z, - X^2*Y*Z+Z^2, Y* Z^2-Z^2, X^2* Z^2- Z^3]
```

Ejemplo 4.4.5. Resolver sistema de ecuaciones

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

$$x^2 + z^2 - 2 = 0$$

$$x - y + 2z = 0$$

Sea el ideal

$$I = \langle x^2 + y^2 + z^2 - 3 = 0, x^2 + z^2 - 2, x - y + 2z\rangle,$$

Resolvemos el sistema de ecuaciones por medio de software COCOA.

Obtenemos las bases de Grobner

$$G = \{1 - 26z^2 + 25z^4, 4y + 21z - 25z^3, 4x + 29z - 25z^3\}.$$

Entonces tenemos,

$1-26z^2+25z^4=0$ y $4y+21z-25z^3=0$ y $4x+29z-25z^3$=0

Obtenemos

$$y=-1\,,z=-1;$$

$$y=-1\,,z=\frac{1}{5};$$

$$y=1\,,z=-\frac{1}{5};$$

$$y=1\,,z=1.$$

$$x=\frac{-7}{5}$$

$$x=1$$

$$x=\frac{7}{5}.$$

Ejemplo 4.4.6. solución de sistema de ecuación lineal por método de Gauss Jordan

$$\begin{cases} \boldsymbol{2x+3y+z=0} \\ \boldsymbol{x+y+2z=1} \\ \boldsymbol{x-y-z=-1} \end{cases}$$

Solución:

La matriz ampliada del sistema es

$$A_1=\begin{pmatrix} 2 & 3 & 1 & 0 \\ 1 & 1 & 2 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix}\frac{f_1-2f_3}{f_2-f_3}A_2=\begin{pmatrix} 0 & 5 & 3 & 2 \\ 0 & 2 & 3 & 2 \\ 1 & -1 & -1 & -1 \end{pmatrix}f_1-f_2$$

$$A_3=\begin{pmatrix} 0 & 3 & 0 & 0 \\ 0 & 2 & 3 & 2 \\ 1 & -1 & -1 & -1 \end{pmatrix}\frac{f_1}{f_3}A_4=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 2 & 3 & 2 \\ 1 & -1 & -1 & -1 \end{pmatrix}\frac{f_3+f_1}{f_2-2f_1}$$

$$A_5=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 2 \\ 1 & 0 & -1 & -1 \end{pmatrix}\frac{f_2}{f_3}A_6=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \frac{2}{3} \\ 1 & 0 & -1 & -1 \end{pmatrix}f_3+f_2$$

$$A_7 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \frac{2}{3} \\ 1 & 0 & 0 & \frac{-1}{3} \end{pmatrix}$$

Reordenamos las tres filas obtenemos

$$A_8 = \begin{pmatrix} 1 & 0 & 0 & \frac{-1}{3} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \frac{2}{3} \end{pmatrix}$$

Ya tenemos resultados de nuestro sistema

$$x = \frac{-1}{3}, \qquad y = 0, \qquad z = \frac{2}{3}$$

resolvamos el mismo sistema de ecuación, haciendo el uso de las bases de Gröbner

Ejemplo 4.4.7.

Resolvemos el sistema de ecuaciones por medio de software COCOA.

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

Inicialmente encontramos las bases de Gröbner

```
Use R:: = QQ[X,Y,Z],Lex;

G := GBasis (Ideal(2*X+3*Y+Z,X+Y+2*Z-1,X-Y-Z+1));

G;

[X +1/3, Y,Z-2/3]
```

Por tanto, tenemos las raíces de las variables

$$x = \frac{-1}{3} \ , \ y = 0 \ , \ z = \frac{2}{3}$$

Ejemplo 4.4.8. Grafique los conjuntos algebraicos:

$x^2 + y^2 + (z-1)^2 - 4\,, x^2 + z^2 - 1 \in \mathbb{R}^3$ es el conjunto de los ceros de

$$x^2 + y^2 + (z-1)^2 - 4 = 0$$

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

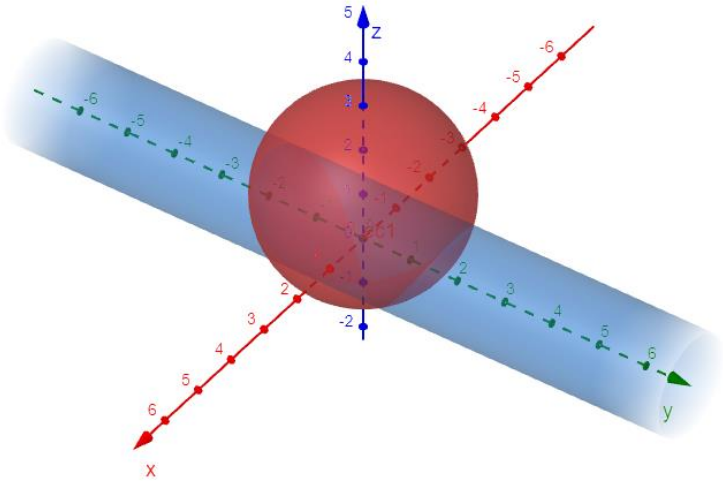

Figura 1. La curva de intersección de la esfera de centro $(0,0,1)$ y de radio 2 y el cilindro circular de radio 1 con el eje Y

Usamos COCOA para hallar las bases de Grobner del ideal generado por los polinomios dados:

```
Use R: = QQ [X, Y, Z], Lex;
G: = GBasis (Ideal(X^2+Y^2+(Z-1) ^2-4, X^2+Z^2-1);
G;
[X^2+Z^2-1, Y^2-2Z-2]
```

Obtenemos: $G = \{x^2 + z^2 - 1, y^2 - 2z - 2\}$

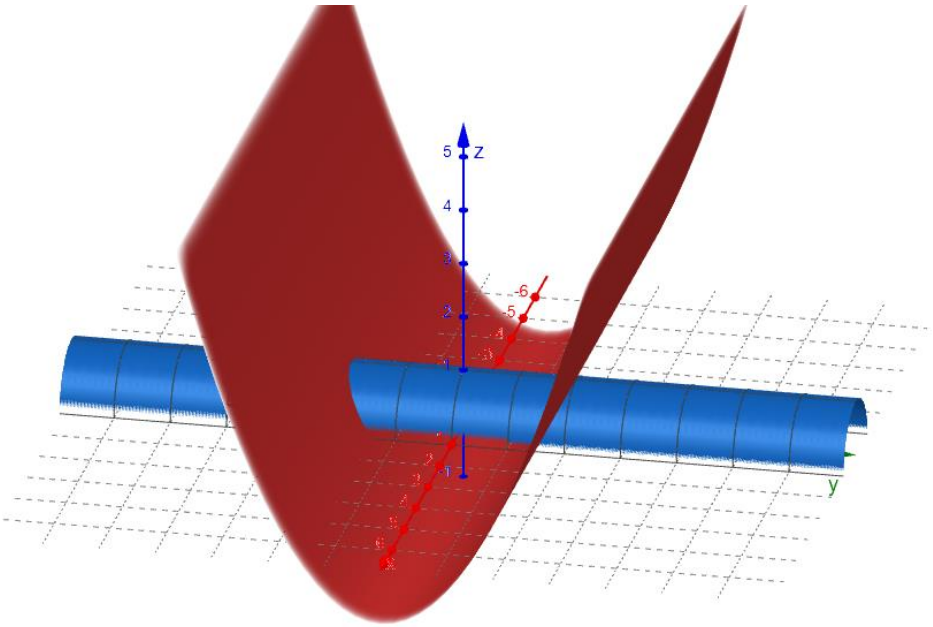

Figura 2. Es la intersección de los cilindros $y^2 - 2z - 2 = 0$ y $x^2 + z^2 - 1 = 0$

Ejemplo 4.4.9.

$x^2 + y^2 - z = 0$ o $z + 2 = 0$, este es un conjunto algebraico no irreductible y por tanto no es una variedad afín

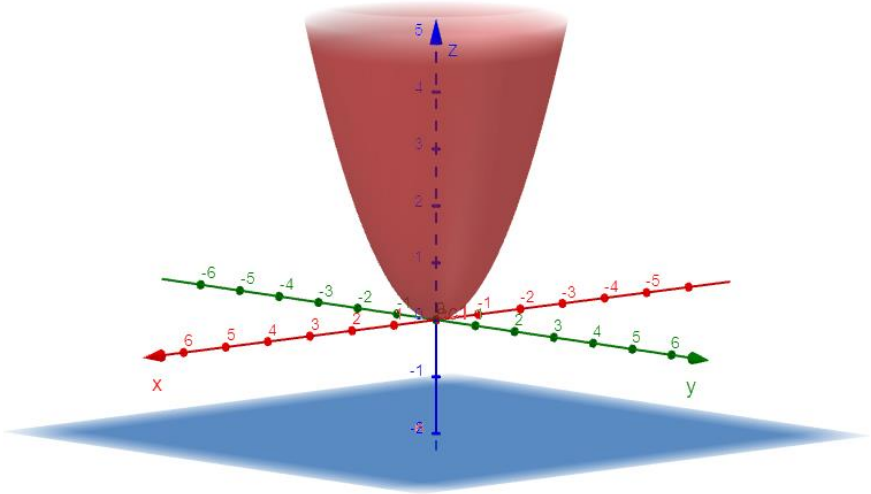

Figura 3. Conjunto algebraico no irreductible y por tanto no es una variedad afín

V. CONCLUSIONES

- Se logró desarrollar todo el proceso para determinar las Bases de Grobner y aplicar estas para encontrar la solución de sistemas de ecuaciones polinomiales, de tal manera que podemos concluir que con las bases de Grobner se pueden resolver sistemas de ecuaciones polinomiales.
- Se logró analizar de manera íntegra las órdenes monomiales, llegando a la conclusión que es importante e influyen en la determinación de una Base de Grobner.
- Se ha logrado analizar y demostrar el algoritmo de la división, concluyendo que esta es una herramienta central para la obtención de las bases de Grobner
- Se ha logrado analizar el algoritmo de Buchberger, encontrando que esta nos lleva a determinar las bases de Grobner utilizando herramientas computacionales.

VI. RECOMENDACIONES

- A los docentes de departamento, se les ínsita fomentar en los estudiantes de matemática la investigación no solo en temas de matemática teórica sino ella como herramienta para la matemática aplicada.

- A los estudiantes de matemática, utilizar el presente documento como base para estudios futuros acerca del tema y profundizar sobre las aplicaciones de bases de Grobner. Como solución de sistemas de ecuaciones polinomiales en varias variables, relación de las variedades algebraicas con los ideales de polinomios, solución del problema de los tres colores, solución de problemas de optimización con restricciones polinomiales en varias variables y solución de problemas de programación entera.

- Instar a los estudiantes del departamento de Matemática investigar sobre el uso de nuevos métodos para la solución de sistema de ecuaciones Polinomiales.

- Experimentar más sobre el uso de softwares que permitan determinar bases como el COCOA, SINGULAR, MACAULAY etc. Ya que son herramientas fundamentales para el desarrollo de muchas investigaciones.

VII. REFERENCIAS BIBLIOGRÁFICAS

Beshenov, A. (2018). Álgebra.1ra Edición. Editorial Usl. El Salvador 457pp.

Cadavid, C. (2005). Una Primera Lección de Geometría Algebraica. *Ingeniería y Ciencia*, 67–81.

Cifuentes, V., Patiño,B y Pérez, H. (2010). Las Bases de Gröbner en el Estudio de Los Polinomios Simétricos. *Tumbaga*,195–210.

Cox, D. (2010). Ideals, Varieties,and Algorithms.

Giménez, Philippe. (2016). Una Introducción a Las Bases de Gröbner y Algunas de Sus Aplicaciones.*VI Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA* 137-178.

Gómez, Vinicio. (2017). Una Introduccion a Las Bases de Groebner." *Revista Electrónica de Matemáticas*,18-34

Gonzáles, J. (2014). Algebra Conmutativa Básica.1ra.Edicion.Editorial Bajamoz.España 481pp.

Lopez, L., Ruiz, C. (2015). Resolución de Ecuaciones Polinomiales Aplicando Bases de Grobner y Teoría de Eliminación.*Seminario de graduación* 1-100

Thomas, W. (2017) Algebra abstracta. 2da Edición. Editorial Brooks Cole