UNIVERSIDAD DEL BÍO-BÍO
FACULTAD DE EDUCACIÓN Y HUMANIDADES
ESCUELA DE PEDAGOGÍA EN EDUCACIÓN MATEMÁTICA

Bases de Gröbner y Aplicaciones a Sistemas de Ecuaciones Polinomiales

AUTOR: Sebastián Alejandro Garrido Cruces
PROFESOR GUÍA: Edgardo Andrés Riquelme Faúndez

MEMORIA PARA OPTAR AL TÍTULO DE PROFESOR DE EDUCACIÓN MEDIA EN EDUCACIÓN MATEMÁTICA

CHILLÁN

Índice general

CAPÍTULO 1

Introducción

En ciertas ocasiones, la resolución de sistemas de ecuaciones polinomiales pueden conllevar más allá del tiempo esperado para su resolución, como lo puede ser en el caso del siguiente ejemplo:

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

Para la resolución del sistema de ecuaciones que se presenta se necesita tener un conocimiento de los conceptos primordiales del algebra abstracta, debido a que se le puede dar solución a estos casos mediante la utilización de Bases de Gröbner.

Las bases de Gröbner tiene como finalidad analizar el sistema de polinomios con más de una indeterminada a través de los conjuntos ideales al que pertenezcan estos polinomios, estas bases contendrán los divisores de los polinomios de un conjunto, de tal manera que todos y cada uno de los polinomios del conjunto se pueden dividir por los polinomios. Con este trabajo ya realizado, nuestro problema de sistema de ecuaciones polinomiales puede ser resuelto con mayor facilidad, puesto que, se puede reestructurar dicho sistema de ecuaciones con las ecuaciones que se obtuvieron en nuestra base de Gröbner.

El estudio de las bases de Gröbner es relativamente nuevo, su invención data de aproximadamente 1966, fue ahí cuando Bruno Buchberger cuando hizo lectura de su tesis "Encontrando una base del espacio vectorial cociente para el anillo de clases, módulo un ideal de polinomios cero dimensional", escrito originalmente en alemán, enunció esta directriz de estudio del álgebra abstracta, que fue nombrado así por quien fuese su profesor que lo dirigía, Wolfgang Gröbner.

El desarrollo de este tipo de ejercicios guarda un estrecho vínculo con ciertos contenidos que indica el Curriculum de matemática en primer año de la

Enseñanza Media, específicamente con el objetivo de desarrollar los productos notables, perteneciente al eje de Números, y de resolver sistemas de ecuaciones de 2x2. Con el primer objetivo se ve relacionado en el sentido de poder realizar la división de polinomios multivariables para reducir los términos, mientas que con el segundo guarda una relación más estrecha por ser la finalidad con la cual se estudiara las bases de Gröbner.

CAPÍTULO 2

Preliminares

2.1 Anillos y Polinomios

En el siguiente capítulo se presentará la definición de anillo, además de propiedades que presenta $K[x]$ donde K es un anillo, es decir, el conjunto de polinomios que tienen por variable a x y posee coeficientes pertenecientes a un cuerpo. Para ello se darán breves contextos históricos previos a desarrollar cada uno de los tópicos.

Definición de Grupo.

El concepto abstracto de grupo se propago rápidamente en la época de 1880 y 1890. Una de las maneras que se manifestó el punto de vista abstracto de los grupos fue a partir de conceptos y resultados introducidos y probados en el marco de grupos "concretos" que fueron reformulados y reprobado en un marco abstracto. Un ejemplo de aquello es la nueva demostración por parte de Frobenius, en un marco abstracto, del Teorema de Sylow, el cual fue probado por Sylow en 1872 para el grupo de permutaciones. Esta corrección fue realizada en 1887, en un paper titulado como "A new proof of Sylow's Proof theorem". A pesar de que Frobenius admitió el hecho de que cada grupo finito puede ser representado por un grupo de permutaciones prueba que el teorema de Sylow debe sostenerse para todos los grupos finitos. Él sin embargo deseaba establecer el teorema abstractamente.
Ya que el grupo simétrico, el cual es introducido en todas estas pruebas, es totalmente ajeno al contexto del teorema de Sylow, he intentado de encontrar una nueva derivación de esto. Hölder fue un contribuidor importante a la teoría abstracta de grupos, y fue responsable de introducir numerosos conceptos teóricos abstracto de grupo. Por ejemplo, en 1889 el definió la noción abstracta de

grupo cociente.

Definición 1. *Un grupo G es un conjunto con una operación binaria $\star$, definida dentro de G, tal que satisface lo siguiente:*

1. *La operación binaria $\star$ es asociativa*
2. *Existe un elemento e en G tal que $e \star x = x \star e = x$ para todas las $x \in G$. A este elemento e se le denomina* ***elemento identidad*** *de G.*
3. *Para cada a en G existe un elemento a' en G con la propiedad de que $a \star a' = a' \star a = e$. Dicho elemento a' es el inverso, respecto a la operación $\star$, de a.*

Teorema 1. *Si G es un grupo con una operación binaria $\star$, entonces las leyes de cancelación, por izquierda y por la derecha, se cumplen en G, es decir:*
$a \star b = a \star c$ implica $b = c$ y $b \star a = c \star a$ implica que $b = c$, para todo $a, b, c \in G$.

Ejemplo 1. *El conjunto $\mathbb{Z}$ con la operación $+$ es un grupo, dado que cumple con todas las condiciones. Mientras que, el mismo conjunto con la operación $\cdot$ no es grupo, dado que, no hay inverso dentro de este conjunto.*

Definición de Anillo

En la primera década del siglo veinte había teorías bien establecidas, prósperas y concretas para anillos conmutativos y no conmutativos y sus ideales. La primera definición abstracta de anillo fue dada por Fraenkel en un paper de 1914 titulado "On zero divisors and the descomposition of rings". La definición de Fraenkel quería abarcar tanto anillos conmutativos como no conmutativos. La definición de Fraenkel para anillo es cual se usa hoy en día. Él lo definió como "un sistema" con dos operaciones abstractas, a los cuales él le dio el nombre de adición y multiplicación. La teoría de los anillos, hecha en 1920 un concepto abstracto central en la algebra por Emmy Noether y Emil Artin, es el lugar de encuentro para elementos como la teoría de grupo, los análisis funcionales, la geometría algebraica, la aritmética, entre otros. Estos anillos son clasificados en dos categorías: conmutativos y no conmutativos, y sus teorías abstractas vienen de variadas fuentes y se desarrollan en diferentes direcciones. La primera clasificación guarda origen en la teoría de los números algebraicos, la geometría algebraica y la teoría de invariantes; mientras que la segunda comenzó con intentos de extender los números complejos a varios sistemas de numeración hipercomplejos. Algunos ejemplos pertenecientes a la teoría de los anillos son los enteros,

los polinomios, y las matrices. Los enteros $\mathbb{Z}$ son considerados como el subdominio apropiado del campo $\mathbb{Q}$ de racionales para hacer teorías de números. Los anillos polinomiales $R[x]$ y $R[x, y]$, de acuerdo a sus variables, constituyen un conjunto discreto de números reales o curvas algebraicas. Las matrices cuadradas $m \times m$, consisten en n-tuples R^n de números reales con sumas sabiamente coordinadas y multiplicaciones apropiadas, obteniendo como resultado un anillo.

Definición 2. *Un **anillo** R es un conjunto con dos operaciones $+$ y $\cdot$, llamados suma y multiplicación respectivamente, definidas en R tal que satisface lo siguiente:*

1. *R es abeliano respecto a la operación $+$.*
2. *$\cdot$ es asociativo sobre R.*
3. *La operación $\cdot$ es distributiva sobre la operación $+$ por la izquierda y por la derecha, o sea: $c \cdot (a + b) = c \cdot a + c \cdot b$ y $(a + b) * c = a \cdot c + b \cdot c$.*

*un anillo R se dice que es **conmutativo** si la operación $\cdot$ es conmutativa: $h \cdot g = g \cdot h$, con h y $g \in R$. Se dice **anillo con unitario** al anillo que tiene elemento identidad multiplicativa, dicho elemento recibe el nombre de **unitario**.*

Definición 3. *Sea R un anillo con unitario. Un elemento u en R es una unidad de R si tiene inverso multiplicativo en R. Si todo elemento distinto de cero en R es una unidad, entonces se dice que R es **anillo con división**. Un **cuerpo** es un anillo conmutativo con división.*

Ejemplo 2. *Para la suma y multiplicación usuales en $\mathbb{R}$, los siguientes anillos son conmutativos:*

1. *$(\mathbb{Z}, +.\cdot)$*
2. *$(\mathbb{Q}, +, \cdot)$*
3. *$R = \left\{a + b\sqrt{3} | a, b \in \mathbb{Z}\right\}$*

Polinomios

En esta sección se clarificará la noción de polinomios y la estructura de un anillo de polinomios, puesto que es una pieza fundamental de los sistemas de ecuaciones que serán estudiadas más adelante.

Definición 4. *Sea R un anillo, un polinomio de indeterminada x, escrito como $f(x)$, con coeficientes en R, es una suma formal infinita:*

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$$

en donde $a_i \in R$ *con* $a_i = 0, \forall i \in \mathbb{N}$*, a excepción de una cantidad finita de valores* a_i*- Los valores* a_i *serán los* ***coeficientes*** *de* $f(x)$*.*

Definición 5. *Si* $f(x)$ *es un polinomio descrito como suma formal infinita, entonces diremos que es cierto que* $a_i \neq 0$ *para alguna* $i > 0$*, el mayor de los valores de* i *es el grado de* $f(x)$ *y se escribe como* $gradf(x)$ *o* $\partial f(x)$*. En el caso que no exista un* $i > 0$*, el grado de* $f(x)$ *será cero.*

Observación 1. *Para el polinomio* $f(x) = 0$ *no se definirá su grado.*

Definición 6. *Un* ***polinomio constante*** *será todo* $f(x) \in F[x]$ *si* $f(x) = 0$ *o si* $\partial f(x) = 0$*.*
Para los polinomios con coeficientes en el anillo R*, los procedimientos de suma y multiplicación son como se expresan a continuación. Sea:*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$$

y

$$g(x) = b_0 + b_1 x + \ldots + b_n x^n + \ldots$$

la suma entre $f(x)$ *y* $g(x)$ *será lo siguiente:*

$$f(x) + g(x) \quad = c_0 + c_1 x + \ldots + c_n x^n + \ldots, \qquad con\ c_n = a_n + b_n$$

mientras que la multiplicación será descrita de la siguiente manera:

$$f(x) \cdot g(x) = d_0 + d_1 x + \ldots + d_n x^n + \ldots, \qquad con\ d_n = \sum_{i=0}^{n} a_i b_{n-i}$$

denotaremos como $F[x]$ *al conjunto formado por todos los polinomios de indeterminada* x *con coeficientes en un anillo* R*. Dicho conjunto es un anillo bajo la operación suma y multiplicación. La demostración para aquello resulta bastante extensa, es por ello que se omitirá.*

2.2 Estructura de $F[x]$

Ya revisado todo lo fundamental, en la presente sección se presentará diversas propiedades que posee un anillo concretamente

Definición 7. *Sea en* R *dos elementos* a *y* b *distintos de cero, si* $a * b = 0$*, entonces* a *y* b *son* ***divisores de cero***

Ejemplo 3. *En $\mathbb{Z}_6$, 2 y 3 son divisores de cero.*

Definición 8. *Se denominará un **dominio entero** D a un anillo conmutativo unitario que no contenga divisores de 0.*

Definición 9. *Un subanillo $(I,+,\cdot)$ del anillo $(R,+,\cdot)$ es un ideal sí y solo si $r \in R$ y $a \in I$ implica que $a * r \in I$ y $r * a \in I$.*

Así, sea cual sea el elemento en R, su producto por un elemento que pertenezca a I pertenecerá a I. En otro sentido, el producto es "absorbido" por I.

Definición 10. *Sea $(R,+\cdot)$ un anillo e I un subanillo no vacío de R. Entonces, $(I,+,\cdot)$ es un ideal de $(R,+,\cdot)$ sí y solo si:*

1. *$a,b \in I$ implica $a-b \in I$.*
2. *$r \in R$ y $a \in I$ implica que $r \cdot a \in I$ y $a \cdot r \in I$.*

En el caso de que A sea un anillo conmutativo, solo se requiere que $r \cdot a \in I$.

Ejemplo 4. *En cualquier anillo $(R,+,\cdot)$, los subanillos impropios $(R,+,\cdot)$ y $(\{0\},+,\cdot)$ son ideales.*

Ejemplo 5. *Los subanillos $(\mathbb{Z}_n,+,\cdot)$ con n cualquier entero par, son un ideal de $(\mathbb{Z},+,\cdot)$.*

División de polinomios en $F[x]$

*Una de los procesos más fundamentales al momento de realizar la búsqueda de las bases de Gröbner es la división de polinomios, pero **¿cómo se debe realizar una división de polinomios y qué se debe tener en cuenta al momento de realizarlo?**, esto será respondido en esta sección en la cual se revisará todo lo que rodea a la división de polinomios dentro de un anillo.*

Teorema 2. ***(Algoritmo de la división para** $F[x]$**)***Sean dos elementos de $F[x]$:*

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ y $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$, con a_n y b_n elementos distintos del cero de F y $m > 0$. Entonces, en $F[x]$, existen polinomios únicos $q(x)$ y $r(x)$ tal que:

$$f(x) = g(x)q(x) + r(x),$$

donde el $\partial r(x) < \partial g(x)$ o bien $\partial r(x) = 0$.

Demostración. *Considerar el conjunto* $M = \{f(x) - g(x)m(x) | m(x) \in F[x]\}$. *Si* $0 \in M$, *entonces, existe un* $m(x)$ *tal que* $f(x) - g(x)m(x) = 0$, *así* $f(x) = g(x)m(x)$. *Tomando* $q(x) = m(x)$ *y* $r(x) = 0$, *estaría listo. Por otro lado, sea r(x) un elemento de grado mínimo en M. Entonces*

$$f(x) = g(x)q(x) + r(x),$$

para algún $q(x) \in F[x]$. *Debemos mostrar que el grado de r(x) es menor que el grado de g(x). Suponemos que*

$$r(x) = c_t x^t + c_{t-1}x^{t-1} + \ldots + c_0,$$

con $c_j \in F$ *y* $c_t \neq 0$ *si* $t \neq 0$. *Si* $t \geq m$, *entonces*

$$f(x) - q(x)g(x) - \left(\frac{c_t}{b_m}\right) x^{t-m} g(x) = r(x) - \left(\frac{c_t}{b_m}\right) x^{t-m} g(x), \qquad (2.2.1)$$

la última parte vendría siendo de la forma

$$r(x) - \left(c_t x^t + \textit{términos de grado menor}\right)$$

lo cual es un polinomio con menor grado que $r(x)$, *o sea, menor que* t. *Sin embargo, el polinomio de la ecuación* (2.2.1) *puede escribirse de la siguiente forma*

$$f(x) = -g(x)\left[q(x) + \left(\frac{c_t}{b_m}\right) x^{t-m}\right],$$

de esta manera está en escritura perteneciente a M, *contradiciendo el hecho de que se haya seleccionado a* $r(x)$ *con grado minimal en* M. *Así el grado de* $r(x)$ *es menor que el grado de* $g(x)$.

Para la unicidad, si

$$f(x) = g(x)q_1(x) + r_1(x)$$

y

$$f(x) = g(x)q_2(x) + r_2(x)$$

de la sustracción de ambas

$$g(x)\left[q_2(x) - q_1(x)\right] = r_2(x) - r_1(x).$$

Porque ni $r_2(x) - r_1(x) = 0$ *ni el grado de* $r_2(x) - r_1(x)$ *es menor que el grado de* $g(x)$, *esto se sostiene si* $q_1(x) - q_2(x) = 0$ *o bien* $q_1(x) = q_2(x)$. *Entonces debemos tener que* $r_2(x) - r_1(x) = 0$ *o* $r_2(x) = r_1(x)$.

Ejemplo 6. *Trabajaremos con los polinomios en* $\mathbb{R}[x]$ *y la división de* $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ *por* $g(x) = x^2 - 2x + 3$ *para encontrar* $q(x)$ *y* $r(x)$ *tal como se indica en el Teorema 1.*

$$\begin{array}{r|l} & x^2 - x - 3 \\ \hline x^2 - 2x + 3 & x^4 - 3x^3 + 2x^2 + 4x - 1 \\ & -x^4 + 2x^3 - 3x^2 \\ \hline & \quad -x^3 - x^2 + 4x \\ & \quad x^3 - 2x^2 + 3x \\ \hline & \quad -3x^2 + 7x - 1 \\ & \quad 3x^2 - 6x + 9 \\ \hline & \quad x + 8 \end{array}$$

Así el polinomio cociente sería $q(x) = x^2 - x - 3$*, mientras que el polinomio resto o residuo es* $r(x) = x + 8$*.*

Observación 2. *Como más adelante se repetirá este tipo de escritura cabe clarificar que:*

El puesto que ocupa el polinomio $x^4 - 3x^3 + 2x^2 + 4x - 1$*, es el lugar en el que va los polinomios que se están dividiendo. Los polinomios que ocupen el lugar de* $x^2 - 2x + 3$ *serán de aquellos polinomios divisores. En el caso de los polinomios, como lo es* $x^2 - x - 3$*, son los polinomios cociente. Y los polinomios como* $x^4 - 2x^3 + 3x^2$ *y* $-x^3 + 2x^2 - 3x$ *son los polinomios resto o residuos, siendo el resto final* $x + 3$*.*

Corolario 1. ***(Teorema del Factor):*** *Un elemento* $a \in F$ *es un* ***cero*** *de* $f(x) \in F[x]$ *si y sólo sí* $x - a$ *es un factor de* $f(x)$ *en* $F[x]$*.*

Demostración. *Suponemos que para* $a \in F$ *tenemos que* $f(a) = 0$*. Por Teorema 1, existen* $q(x), r(x) \in F[x]$ *tal que*

$$f(x) = (x - a)q(x) + r(x),$$

donde $r(x) = 0$ *o el grado de* $r(x)$ *es menor que* 1*. Así debemos de tener que* $r(x) = c$ *para* $c \in F$*, entonces*

$$f(x) = (x - a)q(x) + c.$$

Aplicando la evaluación de homomorfismo $\phi_a : F[x] \longrightarrow F$*, damos con que:*

$$0 = f(a) = 0q(a) + c,$$

entonces debemos de tener que $c = 0$*. Luego* $f(x) = (x - a)q(x)$*, entonces* $x - a$ *es una factor de* $f(x)$*.*

Por el contrario, si $x - a$ es un factor de $f(x)$ en $F[x]$, donde $a \in F$, luego aplicando nuestra evaluación del homomorfismo ϕ_a para $f(x) = (x - a)q(x)$, tenemos que $f(a) = 0q(a) = 0$. □

Corolario 2. *Un polinomio distinto de cero $f(x) \in F[x]$ de grado n puede tener a lo más n ceros en un cuerpo F.*

Demostración. *El corolario anterior nos muestra que si $a_1 \in F$ es un cero de f(x), entonces*

$$f(x) = (x - a_1)q_1(x),$$

en donde, se tiene claro que, el grado de $q_1(x)$ es $n-1$. Un cero $a_2 \in F$ de $q_1(x)$ lo que resulta en la siguiente factorización:

$$f(x) = (x - a_1)(x - a_2)q_2(x).$$

Repitiendo dicho proceso, llegamos a que

$$f(x) = (x - a_1) \dots (x - a_r)q_r(x),$$

en donde $q_r(x)$ no tiene más ceros en F. Dado que el grado de f(x) es n, una gran parte de los n factores $(x - a_i)$, se da que $r \leq n$. También, sí $b \neq a_i$ para $i = 1, \dots, r$ y $b \in A$, entonces

$$f(b) = (b - a_1) \dots (b - a_r)q_r(b) \neq 0,$$

dado que en F no hay divisores de 0 y ni $b-a_i$ ni $q_r(b)$ son 0 mediante resolución. Por lo tanto los a_i, para $i = 1, \dots, r \leq n$ son todos 0 en F de $f(x)$. □

Polinomios Irreducibles

Dentro del álgebra, es posible factorizar ciertos polinomios a modo de facilitar la escritura, y también para que sea más sencillo a la vista. Así como existen polinomios que son posibles de factorizar, existen aquellos que no son posible de hacerlo y quedan expresados tal como están escritos, pero ***¿es posible que un polinomio se pueda factorizar sin importar en que conjunto se encuentre?****. La respuesta a esto será desarrollado dentro de este apartado, en el cual un mismo polinomio puede ser factorizable dentro de ciertos conjuntos y en otros no sea posible factorizarlos.*

Definición 11. *Un polinomio $f(x) \in F[x]$, que no sea constante, se dice que es* ***irreducible sobre*** *F o es un* ***polinomio irreducible en*** *$F[x]$ si $f(x)$ no puede ser expresada como un producto de dos polinomios $g(x)$ y $h(x)$, o sea $g(x)h(x)$, donde ambos polinomios pertenecen a $F[x]$ y son de grado menor que el grado de $f(x)$. Si $f(x) \in F[x]$ es un polinomio no constante que no es irreducible sobre F, entonces se dice que $f(x)$ es* ***reducible sobre*** *F.*
Hay que notar que se habla de polinomio irreducible sobre F, no que simplemente el polinomio sea irreducible. Además, un polinomio $f(x)$ que es irreducible sobre F, pero puede que no sea irreducible sobre B, donde B es un cuerpo más grande que contiene a F.

Ejemplo 7. *En $\mathbb{Q}[x]$ el polinomio $x^2 - 2$ no tiene soluciones. Esto nos muestra que $x^2 - 2$ es un polinomio irreducible sobre $\mathbb{Q}$. Mientras tanto, $x^2 - 2$ visto en $\mathbb{R}[x]$ no es un polinomio irreducible sobre $\mathbb{R}$, porque $x^2 - 2$ se factoriza como $(x - \sqrt{2})(x + \sqrt{2})$.*

Teorema 3. *Sea $f(x) \in F[x]$, y sea $f(x)$ de grado 2 o 3. Entonces $f(x)$ es reducible sobre F si y sólo sí tiene un cero en F.*

Demostración. *Si $f(x)$ es reducible eso quiere decir que $f(x) = g(x)h(x)$, donde el grado de $g(x)$ y el grado de $h(x)$ son ambos menores al grado de $f(x)$, entonces desde que $f(x)$ es cualquiera cuadrática o cúbica, cualquiera sea, $g(x)$ o $h(x)$ es de grado 1. Si el grado de $g(x)$ es 1, entonces, exceptuando un posible factor en F, $g(x)$ es de la forma $x - a$. Entonces, $g(a) = 0$, lo cual implica que $f(a) = 0$, de este modo $f(x)$ tiene un cero en F. Por otro lado, el Corolario 1 nos muestra que si $f(a)$ resulta ser cero, para un $a \in F$, entonces, $x - a$ es un factor de $f(x)$, de esta manera, $f(x)$ es reducible.* □

Estructura de Ideal en F[x]

Hilbert, Lasker y Macauley cambiaron todo lo anterior de finales del siglo diecinueve y principios del siglo XX con el estudio en profundidad de ideales en anillos de polinomios para así iluminar las variedades algebraicas. El mayor resultado obtenido por Lasker fue la "descomposición primaria" de los ideales.

Definición 12. *Si R es un anillo conmutativo con la unidad y $a \in R$, el ideal $\{ra | r \in R\}$ de todos los múltiplos de a es el* ***ideal principal generado por a*** *y se denota por $\langle a \rangle$. Un ideal N de R es un* ***ideal principal*** *si $N = \langle a \rangle$ para alguna $a \in R$.*

Ejemplo 8. *En $F[x]$ el ideal generado por $\langle x \rangle$ serían todos los polinomios en $F[x]$ que tengan término constante cero.*

El siguiente teorema es una aplicación importante del algoritmo de la división para $F[x]$. La demostración de dicho teorema es el algoritmo de la división en $F[x]$ para probar que un subgrupo de un grupo cíclico es cíclico es debido al algoritmo de la división en $\mathbb{Z}$.

Teorema 4. *Si F es un cuerpo, cada ideal en $F[x]$ es principal.*

Demostración. *Sea N un ideal de $F[x]$. Si $N = \{0\}$, entonces $N = \langle a \rangle$. Supongamos que $N \neq \{0\}$, y sea $g(x)$ un elemento de menor grado, distinto de cero, de N. Si el grado de $g(x)$ es 0, entonces $g(x) \in F$ y es una unidad, así $N = F[x] = \langle 1 \rangle$, de esto se desprende que N es ideal principal. Si el grado de $g(x)$ es mayor o igual a 1, sea $f(x)$ cualquier elemento de N, entonces por el Algoritmo de la División, $f(x) = g(x)q(x)+r(x)$, donde $r(x) = 0$ ó grad$(r(x)) <$ grad$(g(x))$. Al tener $f(x) \in N$ y $g(x) \in N$ implica que $f(x) - g(x)q(x) = r(x)$ está en N por definición de ideal. Ya que $g(x)$ es un elemento de menor grado, distinto de cero, de N, debemos tener $r(x) = 0$. Así $f(x) = g(x)q(x)$ y $N = \langle g(x) \rangle$* □

Para continuar con nuestro trabajo, en el Teorema 6, antes debemos de definir lo que es maximal ideal de un anillo. Además de agregar más definiciones que serán utilizados más adelante, incluyendo un teorema y un corolario.

Definición 13. *Un **ideal maximal** de un anillo R es un ideal M, diferente de R, tal que no existe ningún ideal propio N de R que contenga propiamente a M.*

Definición 14. *Un ideal $N \neq R$ en un anillo conmutativo R es un **ideal primo** si $ab \in N$ implica que $a \in N$ o $b \in N$ para $a, b \in A$.*

Teorema 5. *Sea R un anillo conmutativo con unidad, y sea $N \neq R$ un ideal en R. Entonces R/N es un dominio integral si y solo sí N es un ideal primo en R.*

Corolario 3. *Cada ideal maximal en un anillo conmutativo con la unidad R es un ideal primo.*

Ya una vez revisado lo anterior, se continuará con el objetivo de mostrar cuando un polinomio P es irreducible sobre $F[x]$.

Teorema 6. *Un ideal $\langle p(x) \rangle \neq \{0\}$ de $F[x]$ es un maximal si y solo sí $p(x)$ es irreducible sobre $F[x]$.*

Demostración. *Suponer que $\langle p(x) \rangle \neq \{0\}$ es un ideal maximal de $F[x]$. Entonces $\langle p(x) \rangle \neq \{F[x]\}$, así $p(x) \notin F$. Sea $p(x) = f(x)g(x)$ una factorización de*

$p(x)$ en $F[x]$. Ya que $\langle p(x)\rangle$ es un ideal maximal y, por lo tanto, también es un primo ideal, $(f(x)g(x)) \in \langle p(x)\rangle$ implica que $f(x) \in \langle p(x)\rangle$ o $g(x) \in \langle p(x)\rangle$, es decir, $f(x)$ o $g(x)$ tiene a $p(x)$ como factor. Pero, entonces, no podemos tener que los grados de $f(x)$ y $g(x)$ sean menores al grado de $p(x)$. Esto nos muestra que $p(x)$ es irreducible sobre F.

Por el contrario, si $p(x)$ es irreducible sobre F, suponemos que N es un ideal tal que $\langle p(x)\rangle \subseteq N \subseteq F[x]$. Ahora N es un ideal principal por el Teorema 3, así $N = \langle g(x)\rangle$ para algún $g(x) \in N$. Entonces $p(x) \in N$ implica que $p(x) = g(x)q(x)$ para algún $q(x) \in F[x]$. Pero $p(x)$ es irreducible, lo cual implica que el grado de $g(x)$ o $q(x)$ es 0. Si el grado de $g(x)$ es 0, es decir, es una constante distinta de cero en F, entonces $g(x)$ es una unidad en $F[x]$, así $\langle g(x)\rangle = N = F[x]$. Si $q(x)$ es de grado 0, entonces $q(x) = c$, donde $c \in F$, y $g(x) = (1/c)p(x)$ es un $\langle p(x)\rangle$, así $N = \langle p(x)\rangle$. Así $\langle p(x)\rangle \subset N \subset F[x]$ es imposible, así $\langle p(x)\rangle$ es maximal. □

Otro elemento que hay que tener en consideración para el trabajo de varias demostraciones que se realizarán más adelante dentro de este documento, es el concepto de ideal monomial.

Definición 15. *Un ideal $I \subseteq k[x_1, \ldots, x_n]$ es un **ideal monomial** si es un subconjunto $F \subseteq \mathbb{Z}^n_{\geq 0}$ (posiblimente infinito) tal que I consiste de todos los polinomios los cuales son sumas finitas de la forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, donde $h_\alpha \in k[x_!, \ldots, x_n]$. En estos casos, escribimos $I = \langle x^\alpha | \alpha \in R\rangle$. Un ejemplo de ideal monomial esta dado por $I = \langle x^4y^2, x^3y^4, x^2y^5\rangle \subseteq k[x, y]$.*

Lema 1. *Sea $I = \langle x^\alpha | \alpha \in R\rangle$ un polinomio monomial. Entonces un monomio x^β está en I si y solo si x^β es divisible por x^α para algún $\alpha \in R$.*

Aplicación de la Factorización Única en $F[x]$

Como fue visto con anterioridad, existe una única manera de factorizar un polinomio dentro de un anillo, lo que trae consigo un aplicación que es importante de revisar.

Teorema 7. *Sea $p(x)$ un polinomio irreducible en $F[x]$. Si $p(x)$ divide a $r(x)s(x)$ para $r(x), s(x) \in F[x]$, entonces $p(x)$ divide a $r(x)$ o $p(x)$ divide a $s(x)$.*

Demostración. *Suponemos que $p(x)$ divide a $r(x)s(x)$. Entonces $r(x)s(x) \in \langle p(x)\rangle$, el cual es maximal por Teorema 4. Por lo tanto, $\langle p(x)\rangle$ es un primo ideal por Corolario 3. Por tanto $r(x)s(x) \in \langle p(x)\rangle$ implica que $r(x) \in \langle p(x)\rangle$, lo que daría que $p(x)$ divide $r(x)$, o que $s(x) \in \langle p(x)\rangle$, lo que daría que $p(x)$ divide a $s(x)$.* □

2.3 Sistema de Ecuaciones Polinomiales

Existen casos en que los sistemas de ecuaciones pasan a un nivel mayor en cuanto a la complejidad de su resolución, esto sucede cuando el sistema de ecuaciones está conformado por ecuaciones polinomiales, en aquellos casos no se puede llegar a conocer las soluciones exactas asociadas al sistema. Un sistema de ecuaciones polinomiales luciría de la siguiente forma:

$$p_1(x_1, \ldots, x_n) = 0$$

$$p_2(x_1, \ldots, x_n) = 0$$

$$\vdots$$

$$p_n(x_1, \ldots, x_n) = 0$$

en donde los polinomios poseen varias indeterminadas, o variables. Como mencionamos no se puede obtener soluciones explicitas del sistema, pero si podemos considerar lo que menciona la siguiente definición.

Definición 16. *Sea S un subconjunto de $F[x]$. La* ***variedad algebraica*** *$V(S)$ en F^n es el conjunto de todas las soluciones en F^n de los polinomios en S.*

CAPÍTULO 3

Bases de Gröbner

En esta sección tenemos como principal objetivo el modificar, lo mayormente posible, una base de un ideal I en $F[x]$ y para así determinar una nueva base para el conjunto y asociarlo a la variedad algebraica V(I). Para ello trabajaremos de acuerdo a lo que nos indica el siguiente teorema.

Ahora nos vemos en la necesidad de poder encontrar un base adecuada para un ideal I' en I en $F[x] = F[x_1, x_2, \ldots, x_n]$. Para poder ilustrar dichas bases es conveniente reemplazar los polinomios de la base por polinomios de menor grado, o que contengan menos indeterminadas. Es por ello que primero debemos darles un orden a los polinomios en la base.

3.1 Orden de polinomios

Para poder darle un cierto orden a los polinomios que trabajaremos, debemos tener en consideración los grados que posean estos mismos. En nuestro caso, los polinomios en $F[x]$ tienen términos de la forma $ax_1^{m_1}x_2^{m_2}\ldots x_n^{m_n}$ donde $a \in R$, por lo anterior tendremos en consideración el producto potencia en $F[x]$, que estará dado por la expresión:

$$P = x_1^{m_1}x_2^{m_2}\ldots x_n^{m_n} \text{ para todo } m_i \geq 0 \text{ en } \mathbb{Z}$$

Existen propiedades en torno al ordenar productos potencias, que son las siguientes:

1. *$1 < P$ para todos los productos potencias $P \neq 1$.*
2. *Para cualquier dos productos potencias P_i y P_j, se cumple una de las siguientes relaciones: $P_i < P_j$, $P_i = P_j$, $P_i > P_j$.*
3. *Si $P_i < P_j$ y $P_j < P_k$, entonces $P_i < P_k$.*

4. Si $P_i < P_j$, entonces $PP_i < PP_j$ para cualquier producto potencia P.

Hay que notar que todos los x_i están presentes, algunos presentes con exponente 0. Así en Fx, y, z debemos escribir xz^2 como xy^0z^2 para ser producto potencia. Lo que queremos es describir un orden total ¡dentro del conjunto de todos los productos potencias, de esa manera podemos conocer que es lo queremos decir con $P_i < P_j$ para dos productos potencias, proporcionándonos la noción del tamaño relativo de los productos potencias. Entonces podemos intentar cambiar una base ideal de una manera sistemática para crear con polinomios que tenga términos a_iP_i con el "menor" producto potencia P_i como sea posible. Denotaremos por 1 al producto potencia con todos los productos potencia con exponente 0 y requiere del orden de los productos potencia que se describieron con anterioridad. Suponiendo que tal orden es descrito como $P_i \neq P_j$ y que P_i divide a P_j, luego tenemos que $P_j = PP_i$ donde $1 < P$. Por la Propiedad 4, entonces tenemos $1P_j < PP_i = P_j$, entonces $P_i < P_j$. Así P_i divide a P_j implica que $P_i < P_j$.

En $F[x]$ con x como única indeterminada, hay un único ordenamiento de producto potencia, para la Propiedad 1, tenemos que $1 < x$. Multiplicando repetidamente por x y haciendo uso de la Propiedad 4, tenemos $x < x^2$, $x^2 < x^3$, $x^3 < x^4$, etc. La Propiedad 3 luego nos muestra que $1 < x < x^2 < x^3 < \ldots$ es el único orden posible.

Hay un número de posibles ordenamientos para los productos potencia en $F[x]$ con n indeterminadas. Para este caso solo se presentará uno, el ***orden lexicográfico****, que se denota como "lex". En el orden lexicográfico definiremos*

$$x_1^{s_1}x_2^{s_2}\ldots x_n^{s_n} < x_1^{t_1}x_2^{t_2}\ldots x_n^{t_n}$$

si y sólo si $s_i < t_i$ para el primer subíndice i leyendo de izquierda a derecha, tal que $s_i \neq t_i$. Así en $F[x, y]$, si escribimos los productos potencia en el orden x^ny^m, tendremos $y = x^0y^1 < x^1 = x$ y $xy < xy^2$. Usando lex, el orden de n indeterminadas es dado por $1 < x_n < x_{n-1} < \ldots < x_2 < x_1$. Para el caso de dos indeterminadas con $y < x$, esquemáticamente el orden lex completo es

$$1 < y < y^2 < y^3 < \ldots < x < xy < xy^2 < xy^3 < \ldots < x^2 < x^2y^2 < \ldots$$

Un ordenamiento de producto potencias P induce un ordenamiento obvio de términos aP de un polinomio en $F[x]$, que nos referiremos como orden de término. Desde ahora, dado un ordenamiento de producto potencia, consideraremos cada polinomio f en $F[x]$ será escrito en orden decreciente de los términos, así el término que lidera (primero) tendrá el orden mayor. Denotaremos

por $LT(f)$ el término líder de f y por $LP(f)$ el producto potencia del término líder. Si f y g son polinomios en $F[x]$ tal que $LP(g)$ divide $LP(f)$, entonces podemos realizar una división de f por g para obtener que $f(x) = g(x)q(x) + r(x)$ donde $LP(r) < LP(f)$. Notar que no indicamos que $LP(r) < LP(g)$, esto será ilustrado mediante un ejemplo.

Ejemplo 9. *Mediante división, reducir la base $xy^2, y^2 - y$ para el ideal $I = \langle xy^2, y^2 - y\rangle$ en $\mathbb{R}[x, y]$ a uno con menos términos posibles, asumiendo el orden lex $y < x$. Notamos que y^2 divide xy^2 y procedemos*

$$\begin{array}{rl} & x \\ \underline{y^2 - y)} & \overline{xy^2} \\ & \underline{xy^2 - xy} \\ & \quad xy \end{array}$$

porque y^2 no divide a xy, no podemos continuar con la división. Notar que $LP(xy) = xy$ no es menor que $LP(y^2 - y) = y^2$. Sin embargo, tenemos que $LP(xy) < LP(xy^2)$. Entonces nuestra nueva base para I es $\{xy, y^2 - y\}$.

Observación 3. *El orden lexicográfico posee dos ordenamientos más:*

1. *Orden Lexicográfico Graduado(grlex): Los monomios se ordenan por grado total, y las igualdades se resuelven por orden lexicográfico. Es decir, $q \prec p$ si $\sum a_i > \sum b_i$ o $\sum a_i = \sum b_i$ y en $(a_1, \ldots, a_n) - (b_1, \ldots, b_n)$ el primer término distinto de cero de izquierda a derecha es positivo.*

2. *Orden Lexicográfico Graduado Inverso(grevlex): : Los monomios se ordenan por grado total, y las igualdades se resuelven usando el orden lexicográfico inverso. Es decir, $q \prec p$ si $\sum a_i > \sum b_i$, o $\sum a_i = \sum b_i$ y en $(a_1, \ldots, a_n) - (b_1, \ldots, b_n)$ el primer término distinto de cero de derecha a izquierda es negativo.*

3.2 Nociones previas a las Bases de Gröbner

Proposición 1. *Sea $I \subseteq F[x_1, x_2, \ldots, x_n]$ un ideal. Entonces:*

1. *$\langle LT(I)\rangle$ es un ideal monomial.*

2. *Existen $x_1, x_2, \ldots, x_n \in I$ tales que $\langle LT(I)\rangle = \langle LT(x_1), LT(x_2), \ldots, LT(x_n)\rangle$. Es decir $\langle LT(I)\rangle$ posee un número finito de generadores.*

Con esta proposición podemos enunciar un teorema importante para el desarrollo del trabajo.

Teorema 8. ***Teorema de la Base de Hilbert*** *Cada ideal I en $F[x_1, x_2, \ldots, x_n]$ es finitamente generado. En otras palabras, $I = \langle x_1, x_2, \ldots, x_n \rangle$ para algún $x_1, x_2, \ldots, x_n \in I$.*

Demostración. *Si $I = 0$, nuestro grupo será generado por 0, el cual es ciertamente finito. Si I contiene algún polinomio distinto de cero, luego un grupo generador $x_1, x_2, \ldots, x_n$ para I puede ser construido de la siguiente manera. Por la Proposición 1 existen $x_1, x_2, \ldots, x_n \in I$ tales que $\langle LT(I) \rangle = \langle LT(x_1), LT(x_2), \ldots, LT(x_n) \rangle$. Veamos que $I = \langle x_1, x_2, \ldots, x_n \rangle$. Tenemos que $\langle x_1, x_2, \ldots, x_n \rangle \subseteq I$ ya que cada $g_i \in I$. Sea $f \in I$ cualquier elemento de I. Si aplicamos el algoritmo de la división, dividiendo f por $x_1, x_2, \ldots x_n$ obtenemos lo siguiente:*

$$f = a_1x_1 + a_2x_2 + \ldots + a_nx_n + r$$

En donde ningún término r es divisible por $LT(x_1), LT(x_2), \ldots, LT(x_n) \in I$. Si $r \neq 0$, entonces $LT(r) \in \langle LT(I) \rangle = \langle LT(x_1), LT(x_2), \ldots, LT(x_n) \rangle$, para este caso tenemos que $LT(r)$ debe ser divisible por algún $LT(x_i)$ Esto contradice que r pueda considerarse resto y por tanto r debe ser 0. Así

$$f = a_1x_1 + a_2x_2 + \ldots + a_nx_n \in \langle x_1, x_2, \ldots, x_n \rangle,$$

lo cual demuestra que $I \subseteq \langle x_1, x_2, \ldots, x_n \rangle$. □

El teorema de las bases de Hilbert muestra que, de hecho, hace sentido hablar de que una variedad algebraica es definida por un ideal $I \subseteq k[x, \ldots, x_n]$.

Definición 17. *Sea $I \subseteq k[x, \ldots, x_n]$ un ideal. Denotaremos por $V(I)$ al conjunto*

$$V(I) = \{(a_1, \ldots, a_n) \in k^n | f(a_1, \ldots, a_n) = 0 \forall f \in I)\}$$

Incluso si un ideal distinto de cero I siempre contiene infinitos polinomios diferentes, el conjunto $V(I)$ puede estar siempre definido por un conjunto finito de ecuaciones polinomiales.

Proposición 2. *$V(I)$ es una variedad algebraica. En particular, si $I = \langle f_1, \ldots, f_s \}$, entonces $V(I) = V(f_1, \ldots, f_s)$.*

Demostración. *Por teorema de las bases de Hilbert, $I = \langle f_1, \ldots, f_s \rangle$, para un conjunto generado de manera finita.*
Con el teorema que viene a continuación nos provee una herramienta para lograr la tarea que nos encomendamos en un inicio. En dicho teorema se entrega una información que no fue entregada en el teorema de Algoritmo de la División para $F[x]$, usaremos la notación normal de dicho teorema, con la diferenciación que x será reemplazada por x. Y además si se tiene que $f(x) = g(x)h(x)$ en $F[x]$, entonces $g(x)$ y $h(x)$ serán llamados ***divisores o factores de f(x)****.*

Teorema 9. ***Propiedad del Algoritmo de la División:*** *Sean $f(x), g(x), q(x)$ y $r(x)$ polinomios en $F[x]$ tal que $f(x) = g(x)q(x) + r(x)$. Los ceros comunes en F^n de $f(x)$ y $g(x)$ son los mismos ceros comunes de $g(x)$ y $r(x)$. Además, los divisores comunes de $f(x)$ y $g(x)$ son los mismos divisores comunes de $g(x)$ y $r(x)$.*
Si $f(x)$ y $g(x)$ son dos miembros de una base para un ideal I de $F[x]$, entonces reemplazando $f(x)$ por $r(x)$ en la base, esta sigue funcionando como base para I.

Demostración. *Si $a \in F^n$ es una solución de $g(x)$ y $r(x)$, luego aplicando ϕ_a a ambos lados de la ecuación $f(x) = g(x)q(x) + r(x)$, obtenemos lo siguiente:*

$$f(a) = g(a)q(a) + r(a) = 0q(a) + 0 = 0, \textit{así a es una solución de f(x) y g(x)}$$

Si $b \in F[x]$ es una solución de f(x) y g(x), luego aplicando phi_b funciona lo siguiente $f(b) = g(b)q(b) + r(b)$ así $0 = 0q(b) + r(b)$ y notamos que $r(b) = 0$ así como $g(b)$.

La demostración que concierne a los divisores comunes es esencialmente la misma, por lo que será omitido en este caso.

Finalmente, sea B una base para el ideal I, sea $f(x), g(x) \in B$ y sea $f(x) = g(x)q(x)+r(x)$. Sea B' el conjunto obtenido por reemplazar $f(x)$ por $r(x)$ en B, y sea I' el ideal que tiene a B' como base. Sea S el conjunto que se obtiene de B al adjuntar $r(x)$ a B. Notar que S también se puede obtener de adjuntar $f(x)$ a B'. La ecuación $f(x) = g(x)q(x)+r(x)$ muestra que $f(x) \in I'$, entonces tenemos que $B' \subseteq S \subseteq I'$. Así S es una base para I'. La ecuación $r(x) = f(x) - q(x)g(x)$ muestra que $r(x) \in I$, así tenemos que $B \subseteq S \subseteq I$. Así S es base para I. Por lo tanto, $I = I'$ y B' es una base para I. □

Cuando tratamos con más de una indeterminada, es a menudo más fácil realizar la reducción de base multiplicando un polinomio base g(x) por un polinomio –$q(x)$ y sumándolo a un polinomio $f(x)$ para obtener $r(x)$, a medida que realizamos una reducción matricial en álgebra lineal, que a escribir la división como fue ejemplificado anteriormente. Comenzando con los polinomios bases xy^2 y $y^2 - y$, podemos reducir el xy^2 por la multiplicación de $y^2 - y$ por $-x$, y sumando el resultado $-xy^2 + xy$ a xy^2,obteniendo el reemplazo de xy. Procedimiento que se puede realizar de manera mental y escribir el resultado directamente.

Refiriéndonos nuevamente al Ejemplo 9, declararemos que más adelante que cualquier polinomio $f(x, y) = c_1(x, y)(xy) + c_2(x, y)(y^2 - y)$ en $\langle xy, y^2 - y\rangle$, ya sea xy o y^2 dividirá a $lp(f)$. Esto define la propiedad de las ***Bases de Gröbner****.*

Definición 18. *Un conjunto* $\{g_1, g_2, \ldots, g_r\}$ *de polinomios distintos de cero en* $F[x_1, x_2, \ldots, x_n]$*, con el ordenamiento de términos* $<$*, es una Base de Gröbner para el ideal* $I = \langle g_1, g_2, \ldots, g_r\rangle$ *si y sólo sí, para cada* f *distinto de cero en* I*, existe algún* i *donde* $1 \leq i \leq r$ *tal que* $lp(g_i)$ *divide a* $lp(f)$*.*

El método para lograr aquello consiste en la multiplicación de algún polinomio en la base por cualquier polinomio en $F[x]$ *y sumándole el resultado a otro polinomio en la base de manera que se reduzca el tamaño de los productos potencia. Por ejemplo, si dos elementos en la base son* $xy - y^3$ *y* $y^2 - 1$*, podemos multiplicar* $y^2 - 1$ *por* y *y sumarle el resultado a* $xy - y^3$*, reduciendo* $xy - y^3$ *a* $xy - y$*.*

Uno podría esperarse como cualquier base $\{g_1, g_2, \ldots, g_r\}$ *podría fallar con ser una base de Gröbner para para* $I = \{g_1, g_2, \ldots, g_r$ *porque, cuando se forma un elemento* $c_1g_1 + c_2g_2 + \cdots + c_rg_r$ *en* I*, se ve que* $1p(g_i)$ *divide a* $lp(c_ig_i)$ *para* $i = 1, 2, \ldots, r$*. Sin embargo, la cancelación de productos potencias puede ocurrir en la adición, como será ilustrado en el siguiente ejemplo.*

Ejemplo 10. *Considerar el ideal* $I = \langle x^2y-2, xy^2-y\rangle$ *en* $\mathbb{R}[x, y]$*. Los polinomios en la base nos muestra que no pueden ser reducidos más allá de lo que ya está. Sin embargo, el ideal* I *contiene* $y(x^2y - 2) - x(xy^2 - y) = xy - 2y$*, el término producto potencia que lidera,* xy*, no es divisible por ninguno de los productos potencia líderes, ya sea el ya sea el* x^2y *o* xy^2*, dados en la base. Así* $\{x^2y - 2, xy^2 - y\}$ *no es una base de Gröbner para* I *acorde a lo mostrado en la definición18.*

¿Qué ocurre cuando nos resulta lo mostrado en el ejemplo anterior? Ya se sabe que una base de Gröbner debe contener algún polinomio con un producto potencia de menor orden que lo dado en la base. Sean f *y* g *polinomios en la base dada. Tal como se trabajó en el 10, se puede multiplicar* f *y* g *por los productos potencias lo más pequeño posible, de tal manera que los dos productos potencias resultantes sean iguales, el mínimo común múltiplo entre* $lp(f)$ *y* $lp(g)$*, y luego restando o sumando los coeficientes apropiados de* F *se obtenga cancelación por resultado. Anotaremos al polinomio formado de la siguiente manera* $S(f, g)$*. Visto de otra manera sería lo siguiente*

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

Por ejemplo, sea $f = x^3y^2 - x^2y^3 + x$ *y* $g = 3x^4y + y^2$ *en* $\mathbb{R}[x, y]$*. Entonces*

$\gamma = (4, 2)$ *y*

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

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

Ahora se entablará un teorema, sin probar, que puede ser usado para poner a prueba si una base es una base de Gröbner.

Teorema 10. *Una base $G = \{g_1, g_2, \ldots, g_r\}$ es una base de Gröbner para el ideal $\langle g_1, g_2, \ldots, g_r\rangle$ sí y solo si, para todo $i \neq j$, el polinomio $S(g_i, g_j)$ puede ser reducido a cero mediante dividir repetidamente los restos por elementos de G, usando el algoritmo de la división.*

Como se mencionó anteriormente, la reducción de $S(g_1, g_2)$ es preferible realizarla mediante una secuencia consistentes en adicionar (o sustraer) múltiples polinomios en G, a comparación de realizar la división.

Ahora se puede indicar como obtener una base de Gröbner a partir de una base dada. Primero, se reduce los polinomios en la base entre ellos tanto como sea posible. Luego elegir polinomios g_i y g_j en la base, con ellos formar el polinomio $S(g_i, g_j)$. Ver si $S(g_i, g_j)$ puede ser reducido a cero como fue descrito. Si lo hace, elegir un par de polinomios diferentes, y repetir el procedimiento con aquellos polinomios. Si $S(g_i, g_j)$ no puede ser reducido a cero como fue descrito anteriormente, aumentar la base dada con estos $S(g_i, g_j)$, y comenzar todo desde el inicio, reduciendo la base lo mayormente posible. Por 10 cuando cada polinomio $S(g_i, g_j)$, para todo $i \neq j$, puede ser reducido a cero usando polinomios de la última base, hemos logrado obtener una base de Gröbner. Esta idea será vista en el siguiente ejemplo.

Ejemplo 11. *Continuando con el ejemplo 10, sea $g_1 = x^2y - 2, g_2 = xy^2 - y$, y sea $I = \langle g_1, g_2\rangle$ en $\mathbb{R}^2$. En el ejemplo 10 se obtuvo el polinomio $S(g_i, g_j) = xy - 2y$, el cual no puede ser reducido a cero usando g_1 y g_2. Ahora se puede*

reducir la base $\{x^2y-2, xy^2-y, xy-2y\}$*, indicando cada paso.*

$\{x^2y-2, xy^2-y, xy-2y\}$	*base aumentada*
$\{2xy-2, xy^2-y, xy-2y\}$	*por sumar (-x)(tercera) a la primera*
$\{2xy-2, 2y^2-y, xy-2y\}$	*por sumar (-y)(tercera) a la segunda*
$\{4y-2, 2y^2-y, xy-2y\}$	*por sumar (-2)(tercera) a la primera*
$\{4y-2, 0, xy-2y\}$	*por sumar -(1/2)(primera) a la segunda*
$\{4y-2, 0, \frac{1}{2}x-2y\}$	*por sumar -(x/4)(primera) a la tercera*
$\{4y-2, 0, \frac{1}{2}x-1\}$	*por sumar (1/2)(primera) a la tercera*

Claramente, $\{y-\frac{1}{2}, x-2\}$ *es una base de Gröbner. Notar que si* $f=y-\frac{1}{7}$ *y* $g=x-2$*, entonces* $S(f,g)=xf-yg=(xy-\frac{x}{2})-(xy-2y)=-\frac{x}{2}+2y$*, lo cual puede ser reducido fácilmente a cero sumándole* $\frac{1}{2}(x-2)$ *y* $-2(y-\frac{1}{2})$*.*

De la base de Gröbner, notamos que la variedad algebraica $V(I)$ *contiene un único punto,* $(2, \frac{1}{2})$*, en* $\mathbb{R}^2$*.* □

Definición 19. *Ajustado a un orden monomial en el anillo polinómico* $k[x_1, \ldots, x_n]$*. Un subconjunto finito* $G=\{g_1, \ldots g_t$ *de un ideal* $I \subseteq k[x_1, \ldots, x_n]$ *diferente* $\{0\}$ *se dice que es base de Gröbner si*

$$\langle LT(g_1), \ldots, LT(g_t)\rangle = \langle LT(I)\rangle.$$

Equivalentemente, per de manera más informal, un conjunto $\{g_1, \ldots g_t\} \subseteq I$ *es una base de Gröbner de* I *si y solo si el término líder de cualquier elemento de* I *es divisible por uno de los* $LT(g_i)$*. La demostración al Teorema 8 también establece lo siguiente.*

Corolario 4. *Ajustado al orden monomial. Entonces cada ideal* $I \subseteq k[x_1, \ldots, x_n]$ *tiene una base de Gröbner. Además, cualquier base de Gröbner para un ideal* I *es una base de* I*.*

Demostración. *Dado un ideal distinto de cero, el conjunto* $G=\{g_1, \ldots, g_t\}$ *construido en la demostración del Teorema 8 es una base de Gröbner por definición. Para el segundo enunciado, notar que si* $\{LT(I)\}=\{LT(g_1), \ldots, LT(g_t)\}$*, entonces el argumento dado en el Teorema 8 muestra que* $I=\langle g_1, \ldots, g_t\rangle$*, así da que* G *es una base para* I*.* □

3.3 Algoritmo de Buchberger

Ya teniendo conocimiento de lo que son las bases de Gröbner nos queda saber ***¿cómo se puede construir una base de Gröbner para un ideal*** I***?****, es*

por ello que ahora revisaremos el algoritmo de Buchberger, que debe su nombre a Bruno Buchberger, autor que fue nombrado al inicio de este trabajo. Dicho algoritmo nos permitirá construir las bases de Gröbner a partir de un conjunto ideal previamente dado.

Ejemplo 12. *Considerar el anillo* $\mathbb{Q}[x, y]$ *con orden lex, y sea* $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. *Recordar que* $\{f_1, f_2\}$ *no es una base de Gröbner para* I *dado que* $LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2)\rangle$. *Para producir una base de Gröbner, una idea natural sería primeramente intentar de extender el conjunto generador original a una base de Gröbner añadiendo más polinomios en* I. *En un sentido, esto no añade nada nuevo, e incluso introduce un elemento de redundancia. Sin embargo, la información extra que obtenemos de una base de Gröbner más que compensa esto.*
¿Qué nuevos generadores deberíamos agregar? Por lo que se habló anteriormente sobre el S-polinomio, lo siguiente no debería ser una sorpresa. Tenemos que $S(f_1, f_2) = -x^2 \in I$, *y su resto al dividirlo por* $F = (f_1, f_2)$ *is* $-x^2$, *el cual es distinto de cero. Por lo tanto, deberíamos incluir dicho resto en el conjunto generador, como un nuevo generador* $f_3 = -x^2$. *Si definimos el conjunto* $F = (f_1, f_2, f_3)$, *podemos usar el Teorema 10 para comprobar si este nuevo conjunto es una base de Gröbner para* I.

$$\begin{aligned} S(f_1, f_2) &= f_3, \text{ entonces} \\ \overline{S(f_1, f_2)}^F &= 0, \\ S(f_1, f_3) &= (x^3 - 2xy) - (-x)(-x^2) = -2xy, \text{ pero} \\ \overline{S(f_1, f_3)}^F &= -2xy \neq 0. \end{aligned}$$

Así, debemos añadir $f_4 = -2xy$ *a nuestro conjunto generador. Si dejamos* $F = (f_1, f_2, f_3, f_4)$, *entonces tenemos que*

$$\begin{aligned} \overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = 0, \\ S(f_1, f_4) &= y(x^3 - 2xy) - (1/2)x^2(-2xy) = -2xy^2 = yf_4, \text{ entonces} \\ \overline{S(f_1, f_4)}^F &= 0, \\ S(f_2, f_3) &= (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \text{ pero} \\ \overline{S(f_2, f_3)}^F &= -2y^2 + x \neq 0. \end{aligned}$$

Por lo tanto, debemos añadir también $f_5 = -2y^2 + x$ *al conjunto generador. Ajustando* $F = (f_1, f_2, f_3, f_4, f_5)$, *se puede calcular*

$$\overline{S(f_i, f_j)}^F = 0 \text{ para todo } 1 \leq i < j \leq 5.$$

Por el Teorema 10, se sigue que una base de Gröbner para I esta dado por

$$\{f_{1,f}\,2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

El ejemplo anterior sugiere que en general, se debería intentar ampliar una base F a una base de Gröbner mediante la adición sucesiva de restos distintos de cero $\overline{S(f_i, f_j)}^F$ de F. Esta idea es una consecuencia natural de lo mostrado en el Teorema 10 y conlleva al siguiente algoritmo dado por Buchberger para calcular una base de Gröbner.

Teorema 11. ***Algoritmo de Buchberger*** *Sea $I = \langle f_1, \ldots, f_s\rangle \neq \{0\}$ un ideal polinomial. Entonces una base de Gröbner para I puede ser construido con un finito número de pasos dados por el siguiente algoritmo:*

Input: $F = (f_1, \ldots f_s)$
Output: una base de Gröbner $G = (g_1, \ldots, g_t)$ para I, con $F \subseteq G$
$G := F$
REPEAT
  $G' := G$
  FOR cada par $\{p, q\}$, $p \neq q$ en G' DO
    $r := \overline{S(p, q)}^{G'}$
    IF $r \neq 0$ THEN $G := G \cup \{r\}$
UNTIL $G = G'$
RETURN G

Demostración. *Comenzamos con una notación usada frecuentemente. Si $G = \{g_1, \ldots, g_t\}$, entonces $\langle G\rangle$ y $\langle LT\rangle$ será denotado por los siguientes ideales:*

$$\langle G\rangle = \langle g_1, \ldots, g_t\rangle,$$
$$\langle LT(G)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle.$$

Volviendo a la prueba del teorema, primero mostraremos que $G \subseteq I$ se mantiene en cada paso del algoritmo. Esto es cierto inicialmente, y cada vez que ampliamos G, lo hacemos agregando el resto $r = \overline{S(p, q)}^{G'}$ para $p, q \in G' \subseteq G$. Así, si $G \subseteq I$, entonces p, q y, por lo tanto, $S(p, q)$ están en I, y dado que estamos dividiendo por $G' \subseteq I$, obtenemos $G \cup \{r\} \subseteq I$. También debemos notar que G contiene la base dada F de I, así que G actualmente es una base de I.
El algoritmo termina cuando $G = G'$, lo que significa que $r = \overline{S(p, q)}^{G'} = 0$ para todo $p, q \in G$. Así que G es una base de Gröbner de $\langle G\rangle = I$ por el Teorema 10.

Aún falta por probar que el algoritmo se acaba en cierto punto. Se necesita considerar que es lo que ocurre después de cada paso a través del bucle principal. El conjunto G consiste de G' (el antiguo G) junto a los restos distintos de cero de los S-polinomios de los elementos de G'. Entonces

$$\langle LT(G')\rangle \subseteq \langle LT(G)\rangle \tag{3.3.1}$$

dado $G' \subseteq G$. Además, si $G' \neq G$, afirmamos que $\langle LT(G')\rangle$ es estrictamente más pequeño que $\langle LT(G)\rangle$. Para ver esto, suponer que un resto distinto de cero r de un S-polinomio ha sido unido a G. Dado que r es un resto de la división por G', $LT(r)$ no es divisible por los términos líderes de G', y así $LT(r) \notin \langle LT(G')\rangle$ por el Lema 1. Pero $LT(r) \in \langle LT(G)\rangle$, lo cual comprueba nuestra afirmación. Por (3.3.1)*, los ideales $\langle LT(G')\rangle$ que se obtienen de las sucesivas iteraciones del bucle, forman una cadena ascendente de ideales en $k[x_1, \ldots, x_n]$. Así, la condición de cadena ascendente, implica que después de un cierto número finito de iteraciones la cadena se estabilizará, así que $\langle LT(G')\rangle = \langle LT(G)\rangle$ terminará eventualmente ocurriendo. Gracias al párrafo anterior, esto implica que $G' = G$, así que el algoritmo deberá terminar después de realizar un número finito de pasos.* □

CAPÍTULO 4

Aplicaciones de las Bases de Gröbner

4.1 Pertenencia de f a un ideal

Teorema 12. *Sea $G = \{f_1, \ldots, f_s\}$ una base de Gröbner de un ideal I de $k[x_1, \ldots, x_n]$ y $f \in k[x_1, \ldots, x_n]$. Entonces, existe un único $r \in k[x_1, \ldots, x_n]$ con las dos propiedades siguientes:*

1. *Si $r \neq 0$, entonces ningún término de r está en $\langle LT(f_1), \ldots, LT(f_s)\rangle$*
2. *Existe $g \in I$ tal que $f = g + r$*

En particular, r es el resto que produce el algoritmo de división de f entre G sin importar como se ordenen los elementos de G.

Demostración. *Para demostrar la existencia de r usamos el algoritmo de la división en $k[x_1, \ldots, x_n]$. Tenemos que $f = g_1 f_1 + \ldots + g_s f_s + r$, para ciertos $g_i \in k[x_1, \ldots, x_n]$, con $i \in \{1, \ldots, s\}$, y $r \in k[x_1, \ldots, x_n]$ que verifican la primera condición.*

Para la unicidad, sean $r, r' \in k[x_1, \ldots, x_n]$ tales que $f = g + r, f = q' + r'$, verificando $i)$ y $ii)$. Entonces $r - r' = g - g' \in I$. Si $r \neq r'$, se tiene que $LT(r -' r) \in \langle LT(I)\rangle = \langle LT(f_1), \ldots, LT(f_s)\rangle$. Esto implica que algún término de r o de r' es divisible por algún $LT(f_i)$, con $i \in \{1, \ldots, s\}$, lo cual contradice $i)$. Luego, $r = r'$ y de aquí se deduce también la última parte del teorema. □

A partir del teorema anterior se deduce una condición para la pertenencia de un polinomio de $k[x_1, \ldots, x_n]$ en un ideal.

Corolario 5. *Sean $G = \{f_1, \ldots, f_s\}$ una base de Gröbner de un ideal $I \subset$*

$k[x_1, \ldots, x_n]$ *y* $f \in k[x_1, \ldots, x_n]$. *Entonces,* $f \in I$ *si y sólo si el resto de la división de* f *entre* G *es cero.*

4.2 El problema de resolver Ecuaciones Polinomiales

Todo lo explorado hasta ahora nos sirve de base para lo que se desarrollará en esta sección. Aquí daremos respuesta a como resolver sistemas de ecuaciones polinomiales mediante el uso de las bases de Gröbner. Para dar inicio a esta sección comenzaremos revisando unos ejemplos en especifico.

Ejemplo 13. *Considerar las ecuaciones*

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

en $\mathbb{C}^3$. *Estas ecuaciones determinan* $I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z \rangle \subseteq \mathbb{C}[x, y, z]$, *y se quiere encontrar todos los puntos en* $V(I)$. *La Preposición 2 implica que podemos escribir* $V(I)$ *usando cualquier base de* I. *Así que veremos que ocurre cuando usamos bases de Gröbner.*
Aunque aún no hay necesidad de hacerlo por el momento, escribiremos una base reducida de Gröbner de I *con el orden Lex respectivo. La base es*

$$\begin{aligned} g_1 = &\quad x - z, \\ g_2 = &\quad y - 2z^2, \\ g_3 = &\quad z^4 + (1/2)z^2 - 1/4. \end{aligned} \tag{4.2.1}$$

Si examinamos detenidamente los polinomios, se podrá encontrar algo destacable. Primero, el polinomio g_3 *depende solamente de* z. *Para encontrar las raíces, resolvemos para* z^2 *por la fórmula cuadrática y obtener las raíces cuadradas. Esto nos da cuatro valores para* z*:*

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5} - 1}$$

Después, cuando los valores de z *son reemplazados en las ecuaciones* $g_2 = 0$ *y* $g_1 =$, *esas dos ecuaciones pueden ser resueltas únicamente para* y *y* x, *respectivamente. Así, hay cuatro soluciones en conjunto para* $g_1 = g_2 = g_3 = 0$, *dos reales y dos complejas. Dado que* $V(I) = V(g_1, g_2, g_3)$ *por la Preposición 2, ya hemos encontrado todas las soluciones de las ecuaciones originales* (4.2.1).
El ejemplo 13 indica como encontrando una base de Gröbner para un ideal con respecto al orden lex simplifica la forma de las ecuaciones considerablemente.

En particular, hemos visto que obtener ecuaciones donde las variables son eliminadas sucesivamente. Además, notar que el orden de eliminación parece ser que corresponde al orden de las variables.
Un sistema de ecuaciones de esta forma es fácil de resolver, especialmente cuando la última ecuación contiene solo una variable. Se puede aplicar técnicas de una variable única para probar y encontrar las raíces, luego sustituir para resolver las otras variables, usando un procedimiento similar al ejemplo que se encuentra anteriormente. Así el lector debería notar la analogía entre el procedimiento de resolver sistemas polinomiales y el método de sustitución usado para resolver sistemas lineales triangularizados.

4.3 Multiplicadores de Lagrange

En la siguiente sección se revisará como las bases de Gröbner pueden ser utilizadas para resolver sistemas de ecuaciones obtenidos al usar multiplicadores de Lagrange, pero ***¿en qué consiste el método de multiplicadores de Lagrange?****.*
El método de multiplicadores de Lagrange consiste en calcular los mínimos y máximos de una función cuando está se encuentra bajo una condición que viene dada por una ecuación. Así, se lograr encontrar los puntos en los cuales la función y la ecuación sean tangentes. En términos de escritura, se habla de la función de Lagrange a lo siguiente

$$L(x, y, \lambda) = f(x, y) + \lambda g(x, y)$$

en donde $f(x, y)$ es la función que será optimizada, $g(x, y)$ es la ecuación condición dada igualada a 0 y λ es el multiplicador de Lagrange.
Una vez se reemplaza ambas funciones en la función de Lagrange, esta se debe derivar en cada de las variables, además de λ, e igualar dichas derivadas a 0. Realizando lo anteriormente señalado obtenemos el siguiente sistema de ecuaciones

$$\begin{aligned} \frac{\partial L}{\partial x} &= 0 \\ \frac{\partial L}{\partial y} &= 0 \\ \frac{\partial L}{\partial \lambda} &= 0 \end{aligned}$$

Una vez obtenido el sistema de ecuaciones, se resuelve para las incógnitas, lo que indicará una coordenada, el cuál será el máximo o un mínimo, para determinar esto último se debe evaluar dichas coordenadas a fin de determinar si son un punto máximo o mínimo. El procedimiento de saber cuando una coordenada

corresponde a un máximo o un mínimo se deja como tarea al lector.
A continuación, en el ejemplo se verá como emplear las bases de Gröbner en un sistema de ecuaciones que se obtiene al utilizar los multiplicadores de Lagrange.

Ejemplo 14. *Sea el siguiente sistema de ecuaciones polinomiales obtenido de aplicar multiplicadores de Lagrange para encontrar los valores mínimos y máximos de $x^3 + 2xyz - z^2$ sujeto a la condición $x^2 + y^2 + z^2 = 1$:*

$$\begin{aligned} 3x^2 + 2yz - 2x\lambda &= 0, \\ 2xz - 2y\lambda &= 0, \\ 2xy - 2z - 2z\lambda &= 0, \\ x^2 + y^2 + z^2 - 1 &= 0. \end{aligned}$$

Con esto, comenzaremos a calcular una base de Gröbner para el ideal $\mathbb{R}[x, y, z, \lambda]$, usando el orden lex con $\lambda > x > y > z$. De esta manera encontraremos la siguientes bases de Gröbner:

$$\begin{aligned} &\lambda - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 + \frac{36717}{590}z^4 - \frac{134419}{7670}z^2, \\ &x^2 + y^2 + z^2 - 1, \\ &xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z, \\ &xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z, \\ &y^3 + yz^2 - y - \frac{9216}{2825}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z, \\ &y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z, \\ &yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2, \\ &z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z. \end{aligned} \tag{4.3.1}$$

A primera vista, este conjunto de polinomios luce horrendo, además los coeficientes que se presentan en la base de Gröbner son significativamente más "dispersos" en comparación a los del conjunto generador original. Sin embargo, podemos notar que el último polinomio depende únicamente de la variable z. En el proceso de encontrar la base de Gröbner debemos "eliminar"las otras variables. Resolviendo primeramente el polinomio mencionado anteriormente igualado a cero se obtiene las siguientes raíces:

$$z = 0, \pm 1, \pm 2/3, \pm\sqrt{11}/8\sqrt{2}.$$

Si igualamos z a cada uno de los valores obtenidos, las ecuaciones restantes pueden resolverse para y, x (y λ, el cual es irrelevante para nuestros propósitos).

Obteniendo las siguientes soluciones:

$$
\begin{aligned}
&z = 0;\ y = 0;\ x = \pm 1,\\
&z = 0;\ y = \pm 1;\ x = 0,\\
&z = \pm 1;\ y = 0;\ x = 0,\\
&z = 2/3;\ y = 1/3;\ x = -2/3,\\
&z = -2/3;\ y = -1/3;\ x = -2/3,\\
&z = \sqrt{11}/8\sqrt{2};\ y = -3\sqrt{11}/8\sqrt{2};\ x = -3/8,\\
&z = -\sqrt{11}/8\sqrt{2};\ y = 3\sqrt{11}/8\sqrt{2};\ x = -3/8.
\end{aligned}
$$

De aquí es sencillo determinar los valores mínimos y máximos.
Encontrar la base de Gröbner de un ideal con respecto a un orden lex simplifica la forma de las ecuaciones considerablemente. En particular, parece que tenemos ecuaciones en donde las variables son eliminadas de manera sucesiva. Además, notar que el orden de eliminación parece corresponder al orden de las variables, para este ejemplo tenemos que las variables están en el orden $\lambda > x > y > z$, y si volvemos a revisar la base de Gröbner (4.3.1)*, se nota que λ se elimina primero, x segundo y así sucesivamente.*
Un sistema de ecuaciones así es fácil de resolver, especialmente cuando en la ultima ecuación posee solo una variable. Podemos aplicar técnicas de una variable y encontrar las raíces, luego substituir en las otras ecuaciones dentro del sistema y resolverlo para las otras variables.

Tanto el ejemplo 13 como el ejemplo 14 fueron extraídos del libro "Ideals, Varieties, and Algorithms"de Cox, Little & O'Shea.

4.4 Ecuaciones Diferenciales Parciales

Las bases de Gröbner también cumplen un gran papel para la resolución de sistemas con ecuaciones diferenciales parciales, más concretamente aquellos sistemas homogéneos, es decir, un sistema en el cual ambas ecuaciones están igualadas a 0. Esto será a visto con mayor desarrollo con el siguiente ejemplo.

Ejemplo 15. *Sea el siguiente sistema de ecuaciones diferenciales parciales:*

$$
\begin{aligned}
\frac{\partial^2 f(x,y)}{\partial x^2} + \frac{\partial^2 f(x,y)}{\partial y^2} - 25 f(x,y) = 0,\\
\frac{\partial^2 f(x,y)}{\partial x \partial y} - f(x,y) = 0.
\end{aligned}
\tag{4.4.1}
$$

Reemplazando $f(x,y)$ por 1, $\frac{\partial^2 f(x,y)}{\partial x^2}$ por x, $\frac{\partial^2 f(x,y)}{\partial x \partial y}$ por xy y así. Entonces la

ecuación (4.4.1) *se vuelve en el siguiente sistema algebraico:*

$$\begin{aligned} x^2 + y^2 - 25 = 0, \\ xy - 1 = 0. \end{aligned} \tag{4.4.2}$$

Ahora, si tomamos la derivada $\frac{\partial}{\partial x}$ *de la segunda ecuación en* (4.4.1)*, obtenemos:*

$$\frac{\partial^3 f(x,y)}{\partial x \partial y} - \frac{\partial^2 f(x,y)}{\partial x} = 0,$$

lo cual corresponde a

$$x^2 y - x = 0.$$

Así, tomando la derivada $\frac{\partial}{\partial x}$ *induce la multiplicación del polinomio correspondiente a* x*, y así se continua. Por lo tanto, el mismo método de Buchberger que simplifica ecuaciones algebraicas también ayuda a simplificar ecuaciones diferenciales parciales. Entonces la ecuación* (4.4.1) *es equivalente a*

$$\begin{aligned} \frac{\partial f(x,y)}{\partial y} - \frac{\partial^3 f(x,y)}{\partial x^3} - 25\frac{\partial f(x,y)}{\partial x} = 0, \\ \frac{\partial^4 f(x,y)}{\partial x^4} - 25\frac{\partial^2 f(x,y)}{\partial x^2} + 1 = 0 \quad . \end{aligned} \tag{4.4.3}$$

La segunda ecuación puede ser sustancialmente simplificado vía $g(x,y) := \frac{\partial^2 f(x,y)}{\partial y^2}$*, ya que esto da*

$$\frac{\partial^2 g(x,y)}{\partial x^2} = 25 g(x,y) - 1,$$

y entonces el sistema puede ser resuelto. El sistema "extendido"

$$\begin{aligned} \frac{\partial^2 f(x,y)}{\partial x^2} + \frac{\partial^2 f(x,y)}{\partial y^2} - 25 f(x,y) = 0, \\ \frac{\partial^2 f(x,y)}{\partial x \partial y} - f(x,y) = 0, \\ \frac{\partial^2 f(x,y)}{\partial x^2} - \frac{\partial^2 f(x,y)}{\partial y^2} - f(x,y) = 0. \end{aligned}$$

tiene solamente la solución trivial $f = 0$*. Esto podemos notarlo más fácilmente en la figura 4.1 que se mostrará a continuación, que sería el resultado de graficar el sistema anteriormente escrito* (4.4.2)*, donde podemos apreciar que la primera ecuación de dicho sistema es una circunferencia, mientras que la segunda ecuación grafica unas asíntotas a los ejes.*

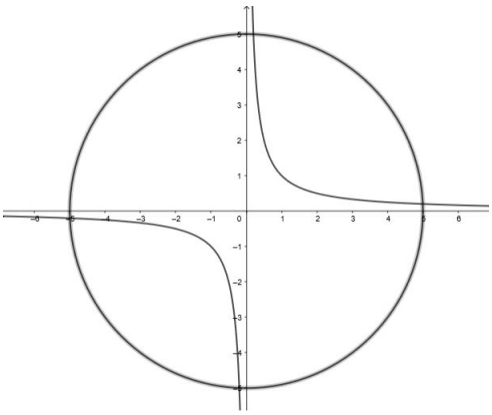

Figura 4.1: Figura 1.

Gracias a la figura, tenemos conocimiento que el sistema no tiene soluciones no triviales. Para un desarrollo más en profundidad, visto desde otros ámbitos de la matemática, se sugiere revisar la Sección 38, capítulo 7 del texto "Applied Abstract Algebra" de Lidl y Pilz, .

CAPÍTULO 5

Introducción a Magma

En este anexo presentamos al lector una breve introducción a las funciones del sistema de algebra computacional Magma y como algunas de estas pueden usarse en criptografía.
Magma es un sistema de álgebra computacional diseñado para realizar cálculos en álgebra, teoría de números, geometría algebraica y combinatoria algebraica.
En esta anexo, nos concentraremos en el uso de algunos comandos de Magma en Teoría de Números elemental y su uso en criptografía.
Existe una versión disponible online de magma en
http://magma.maths.usyd.edu.au/calc/

5.1 Ideas básicas

Para usar Magma:

1. *Tipear un comando o expresión después del prompt >.*
2. *No olvidar colocar una semicolon (;) al final de la linea.*
3. *Luego, presione la tecla enter .*

Ejemplo 16.

```
> 2+2;
4
> 3-5;
-2
> 2*3;
6
```

Cargar un archivo

Existe la opción para cargar el contenido de un archivo en Magma. Para esto debe tipear el nombre del archivo

```
> load "nombrearchivo";
```

Ayuda en Magma

Es posible obtener información acerca de las funciones. Hay que tipear ? seguido por el comando que se desea conocer.

```
> ?load

 5 matches:
       1   0   /system/database
       2   0   /system/library
       3   0   /system/loadn
       4   S   language/IO/load
       5   I   language/IO/load/load
To view an entry, type ? followed by the number next to it
```

Esta entrega una visión general sobre "load". Para leer específicamente sobre algún punto debes tipear por ejemplo:

```
> ?5
================================================================================
PATH: /language/IO/load/load
KIND: Intrinsic
================================================================================
load "filename";

    Input the file with the name specified by the string. The file will
    be read in, and the text will be treated as Magma input. Tilde
    expansion of file names is allowed.
================================================================================
```

5.2 Bases de Gröbner

A lo largo del presente texto se ha trabajado con diversos niveles de estructuras, más específicamente con cuerpos, anillos de polinomios e ideales. Para ello, en esta sección se revisará como definir cada uno de estos en el sistema Magma

y el como ordenar al sistema que entregue las bases de Gröbner para un cierto ideal.

Cuerpos

Inicialmente hay que definir un cuerpo dentro del sistema, por ello se debe hacer uso del siguiente comando

```
> Q:=Rationals();
> Q;
Rational Field
```

Así estamos definiendo que $\mathbb{Q}$ es un cuerpo compuesto por los números racionales.

Para definir cuerpos finitos, se debe ingresar lo siguiente

```
> F:=FiniteField(13);
> F;
Finite field of size 13
```

Así definimos un cuerpo finito de tamaño 13.

Anillos de Polinomios e Ideales

A continuación, se revisará como definir un anillo de polinomios, pieza elemental a definir para realizar el trabajo con bases de Gröbner. Por ejemplo, si se quiere definir un anillo de polinomios con coeficientes en $\mathbb{F}_4$.

```
> P<x>:=PolynomialRing(GF(5));
> P;
Univariate Polynomial Ring in x over GF(5)
```

En este caso, se está definiendo un anillo de polinomios que solo contiene una variable, como en el trabajo de las bases de Gröbner se utilizan anillos de polinomios que son de carácter multivariable. Para ello se deben realizar unas modificaciones al comando anteriormente escrito

```
> P<x,y>:=PolynomialRing(GF(5),2);
> P;
Polynomial ring of rank 2 over GF(5)
Order: Lexicographical
Variables: x, y
```

Al realizar los cambios al comando para obtener un anillo de polinomios multivariable, el sistema además de indicar el anillo, también nos entrega el orden con el se trabaja (orden lex) y las variables definidas dentro del comando x e y. Las bases de Gröbner trabajan esencialmente con los ideales de los anillos de polinomios, para ello es que deberemos definir los ideales de un anillo de poli-

nomios de la siguiente manera

```
> Q:=Rationals();
> P<x,y>:=PolynomialRing(Q,2);
> f:=x^2 * y - 2;
> g:=x * y^2 - y;
> I:=ideal<P|f,g>;
> I;
Ideal of Polynomial ring of rank 2 over Rational Field
Order: Lexicographical
Variables: x, y
Basis:
[
    x^2 * y - 2
    x * y^2 - y
]
```

Así, mediante estos comandos obtenemos lo que sería un ideal de un anillo de polinomios que está generado por los polinomios f y g que se encuentra definido en lo escrito.

Bases de Gröbner

Revisado todo lo anterior, ahora podemos trabajar con las bases de Gröbner dentro del sistema Magma. Para realizar esto, se debe acudir a todos los comandos anteriormente definidos, utilizándolos de la siguiente manera

```
> Q:=RationalField();
> P<x,y,z>:=PolynomialRing(Q,2,"lex");
> f:=x^2 + y^2 + z^2 - 1;
> g:=x^2 + z^2 - y;
> g:=x - z;
> I:=ideal<P|f,g,h>;
> B:=GroebnerBasis(I);
> B;
[
 x - z,
 y - 2 * z^2
 z^4 + 1/2 * z^2 - 1/4
]
```

podemos notar que los comandos aluden al ejemplo 13, con el detalle que se define como los racionales el cuerpo sobre el cual se trabajará. Magma nos dará

por resultado los polinomios $x - z$, $y - 2z^2$ *y* $z^4 + 1/2z^2 - 1/4$, *los cuales corresponden a los polinomios que se obtienen en* (4.2.1), *que son los que forman la base de Gröbner obtenido en el ejemplo anteriormente mencionado.*

Bibliografía

[1] Cox, D. A., Little, J., & O'Shea, D. (2015). Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra (Undergraduate Texts in Mathematics) (English Edition) (4.a ed.). Springer. https://doi.org/10.1007/978-3-319-16721-3

[2] Dummit, D. S., & Foote, R. M. (2003). Abstract Algebra (3.a ed.). Wiley.

[3] Fraleigh, J. B. A first course in abstract algebra. Reading, Mass: Addison-Wesley Pub. Co. (1982).

[4] Gathen, J., Gerhard, J., & von zur Gathen, J. (2013). Modern Computer Algebra (3.a ed.). Cambridge University Press.

[5] Lidl, R., & Pilz, G. (1998). Applied Abstract Algebra (2.a ed.). Springer Publishing.

[6] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.16 (2010)