Universidad Mayor de San Andrés
Facultad de Ciencias Puras y Naturales
Carrera de Matemática

Teorema de las bases de Gröbner

presentado en parcial cumplimiento de los requerimientos para optar al grado de licenciado en matemática

POSTULANTE:JHONNY CHAMBI MOLLERICONA
TUTOR: Dr. RAMIRO LAFUENTE RODRIGUEZ
TRIBUNALES:
LIC. MARIO F. PAZ BALLIVIÁN
LIC. ZENÓN CONDORI GONZALES

LA PAZ - BOLIVIA
2010

Dedicatoria

Dedico el presente trabajo

A mis queridos padres y hermanos

Tomás Chambi Ch. y Matilde Mollericona C.

Como a Bruno, Gonzalo, María Magdalena y Sara

Agradecimientos

En primer lugar agradecer al supremo creador por ser fuente de vida y guía en el camino de la humildad, sinceridad y justicia para con los que me rodean. En segundo lugar agradecer a mi familia por inculcarme todos los principios y valores para con la sociedad y por brindarme un apoyo incondicional en cada momento de mi vida. Por otro lado, un agradecimiento muy especial a mi consejero y tutor Dr. Ramiro Lafuente Rodriguez por ser más que todo un gran amigo y guía en este presente trabajo, al Lic. Mario Paz Ballivian por sus claras observaciones y sugerencias en cada capítulo de la presente tesis, y al Lic. Zenón Condori por su colaboración desinteresada y guía en las demostraciones matemáticas por ser parte de mi tribunal.

Además de esto, agradecer a todos y a cada uno de mis docentes de la carrera de Matemática, compañeros(as) y amigos(as) principalmente: Ronnald Alvaro Silva Guzmán, Viter Franco Rojas, Julio Jarandilla por estar siempre en los momentos más alegres y tristes de mi vida; y por ser más que todo, los mejores consejeros en la formación de mi persona, en fin un alto aprecio a todos. Por cuanto dedicó a mis amigos(as) profesores(as): Soledad C.,Norha R., Marleny N., Gabriela, William A.,Pedro D., Martha M., Delia C., Ximena, Norha, Ángela Vargas, Ruth Candida R., Rolando, F.,Pierre V.,Job V. Además de esto al Dr. Silverio Chavez, Lic. Ramiro Ramos, Lic Jaime Cazas, Lic José Luis Romero, Ing. Jhonny J., Lic. Huber Delboy y al Lic. Javier Rodolfo Quispe Colque.

Por último, un agradecimiento especial a las instituciones que me fortalecieron en mi vida profesional: U.M.S.A.; E.S.F.M.T.H.E.A.; U.P.E.A.; INS.PRO.IN.; C.E.P.E.C. y O.L.A.C.

Metas + Objetivos + Misión = Camino a la Visión
Jhonny Ch. M.

Resúmen General

En el presente trabajo de investigación (proyecto de grado) se analiza el algoritmo de la división, las cuales pueden ser extendidos de polinomios de una y varias variables utilizando criterios del algoritmo euclidiano y el de la división para polinomios.

Aunque estos resultados son elementales, fueron descubiertos recientemente, en 1965 por Bruno Buchberger en su trabajo matemático ya que el algebra siempre trata con algoritmos, pero el poder y lo bello del método axiomático ha dominado el temas desde Cayley y Dedekind en la segunda mitad del siglo XIX.

Después de la invención del transistor en 1948, el cálculo rápido y veloz llego hacer realidad y vieron algoritmos complicados y como también en algunos nuevos, podrían ser implementados; un orden superior ha ingresado en Algebra. Muy probablemente el desarrollo de las ciencias de la computación es una gran razón del por qué las generalizaciones de algoritmos clásicos de polinomios de una y varias variables han sido descubiertos; esta es una ilustración dramática del impacto de ideas externas sobre la matemática.

Por lo tanto lo que se espera de las Bases de Gröbner, es que se cada ideal que se tome se puede hallar una Base Gröbner ya sea de un dominio entero de una o varias variables con la restricción de que sea un campo; que fue tanto mecánico y engorroso en épocas pasadas de la historia que fue revolucionando la creación de algoritmos como el último fue de Buchberger con la optimización del algoritmo.

Índice general

1. Introducción **1**

1.1. Antecedentes 3

1.2. Planteamiento del Problema 5

1.2.1. Formulación del Problema 5

1.3. Objetivos: 5

1.3.1. Objetivo General: 5

1.3.2. Objetivos Específicos: 5

1.4. Justificación 6

1.5. Alcances y Limitaciones 6

2. Orden Monomiales **8**

2.1. Orden de Monomios en $F[x_1, x_2, ..., x_n]$ 8

2.2. Estructura de $F[x_1, x_2, ..., x_n]$ 15

3. Bases de Gröbner **19**

3.1. Los Anillos Noetherianos 19

3.2. Estructura de la Base Gröbner 23

3.3. Criterio de Bruno Buchberger 29

4. Aplicaciones de las bases de Gröbner **37**

4.1. Bases Gröbner- Resolución de Ecuaciones Algebraicas: Eliminación 37

5. Conclusiones **43**

A. Anexos **45**

A.1. Teoremas Básicos en el Anillo de Polinomios F[x] 45

A.2. Propiedades en el Anillo de Polinomios K[x] 47

A.3. Algoritmo de la División Generalizada 49

A.4. Biografía de: Wolfgang Gröbner 56

A.5. Biografía de: Bruno Buchberger 59

Bibliografía **62**

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

Capítulo 1

Introducción

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

En el presente trabajo de investigación nos basaremos en la teoría del Orden Monomiales en $F[x_1, x_2, ..., x_n]$ siendo un Dominio entero, para llegar al teorema de la base de Gröbner; hecho que es generalizado de la siguiente manera:

Teorema .- *Fije un orden monomial en* $F[x_1, x_2, ..., x_n]$ *y suponga que* $\{g_1, ..., g_m\}$ *es una* base Gröbner *para el ideal no cero* I *de* $F[x_1, x_2, ..., x_n]$. *Entonces:*

1. *Cada polinomio* $f \in F[x_1, x_2, ..., x_n]$ *puede ser escrito de modo único en la forma* $f = f_I + r$ *donde* $f_I \in I$ *y ningún término mónico no cero del resto* r *es divisible por*

cualquiera de los términos principales $LT(g_1), \ldots, LT(g_m)$.

2. *Ambos* f_I *y* r *pueden ser calculados por la división general de polinomios para* $g_1, .., g_m$ *y son independientes del orden en el cual estos son utilizados en la división.*

3. *El resto* r *da un único representante para la clase de* f *en el anillo cociente de polinomios* $F[x_1, x_2, ..., x_n]/I$. *En particular* $f \in I$ *si y solo si* $r = 0$.

Este razonamiento viene de la inducción (de manera particular) que si dados dos polinomios $f(x), g(x) \in F[x]$, con $g(x) \neq 0$, donde F es un campo; si nos preguntamos ¿Cuando $g(x)$ es un divisor de $f(x)$?.El algoritmo de la división nos dice que existen polinomios únicos $q(x)$,$r(x)$ en $F[x]$ tal que:

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

donde $r(x) = 0$ o $deg(r) < deg(g)$; además $g(x) \mid f(x)$ si y solo si el resto $r(x) = 0$, veamos este enunciado desde otro punto de vista diferente. Decir que $g \mid f$ es decir que $f \in (g)$, que es el ideal principal generado por $g(x)$. Así que el resto es la obstrucción para que esté en este ideal, esto es $f \in (g)$ si y solo si $r = 0$.

Ahora consideremos un problema más general, dados los polinomios

$$f(x), g_1(x), g_2(x), ..., g_n(x) \in F[x]$$

donde F es un campo; cuando es $d(x) = gcd\{g_1(x), g_2(x), .., g_n(x)\}$ un divisor de f ?. El algoritmo euclidiano encuentra d, y el algoritmo de la división determina si $d \mid f$. Es decir, dos algoritmos clásicos combinados nos dan un algoritmo para determinar si $f \in (g_1, g_2, .., g_n)$. En efecto un algoritmo de la división en $F[x]$ debería de ser un algoritmo que produzca $r(x), q_1(x), q_2(x), .., q_n(x) \in F[x]$ tal que:

$$f = g_1q_1 + ... + g_nq_n + r$$

ya que $(g_1, g_2, .., g_n)$ consiste de todas las combinaciones lineales de los g_i´s tal algoritmo de la división generalizado dice que el resto r es la obstrucción:$f \in (g_1, g_2, .., g_n)$ si y solo si $r = 0$. Finalmente mostraremos que ambos, el algoritmo de la división y el algoritmo

Euclidiano pueden ser extendidos al anillo de polinomios en n-variables(ver en Anexos). Entonces una base de Gröbner es la generalización de esta idea, es decir; una base de Gröbner $g_1, g_2, ..., g_n$ de un ideal $I = \langle g_1, g_2, .., g_n \rangle$ es una base tal que para cualquier n-tuple G formado por las g_i´s , el resto f modulo G es siempre la obstrucción de f para que se sitúe en I.

1.1. Antecedentes

El uso temprano de lo que equivale a la existencia de las Bases de Gröbner puede ser Gordan[1900]; quien uso Bases de Gröbner y la generación finita de ideales monomiales para deducir el teorema de las Bases de Hilbert. Un mayor paso hacia la teoría presentada en este trabajo fue tomando por Macaulay, quien introdujo órdenes totales del conjunto de monomiales de un anillo[1927] y los utilizó para caracterizar las posibles funciones de Hilbert de ideales graduados comparándolos con ideales monomiales.

Gröbner publicó aplicaciones de la idea de Macaulay de ordenes monomiales y encontrando explícitamente una base para un anillo factor zero dimensional a principios de 1939, aunque su uso va más a atrás quizá hasta 1932. En pasaje sobre su teoría de eliminación [1950], pero en 1965 Gröbner propuso a su estudiante Bruno Buchberger, calcular tales Bases como un problema de tesis doctoral; como parece haber sido de costumbre, él no mencionó a Buchberger que el ya tenía la solución al problema. Como Gröbner debe haber esperado la solución de Buchberger para su problema de tesis contenía ideas que estaba más allá del conocimiento de Gröbner.

La ciencia de la matemática ha dado y viene dando avances día a día en diferentes ramas y especialidades del desarrollo científico, una de ellas tiene que ver con la generalización del algoritmo de la división con relación a la Euclidiana, ya que nuestro interés de esta monografía es el estudio de polinomios en varias variables. Puesto que uno ve en geometría analítica que los polinomios corresponden a figuras geométricas; por ejemplo: la elipse $2x^2 + 2xy + y^2 - 2x - 2y = 0$ interseca al círculo $x^2 + y^2 = 1$ en dos puntos.

Para encontrarlos estas soluciones de los polinomios lineales de 2-variables fue una problemática en aquel tiempo donde Wolfgang Gröbner planteo una solución general. Viendo el ideal $I = \langle 2x^2 + 2xy + y^2 - 2x - 2y, x^2 + y^2 - 1\rangle \subset \mathbb{R}[x, y]$; y que además hay una fuerte conexión entre el anillo $F[x_1, x_2, ..., x_n]$, donde F es un campo, y la geometría de subconjuntos de F^n; viendo una perspectiva más allá de esto. Dado un conjunto de polinomios $f_1, .., f_n$ de $n - variables$ llamamos $V \subset F^n$ consistente de sus ceros(raíces-soluciones) comunes. Por supuesto uno puede estudiar variedades, por que las soluciones de sistemas de ecuaciones polinomiales(una obvia generalización de sistemas de ecuaciones lineales), es intrínsecamente interesante visto de otra forma.

Gröbner pudo presentar a Noether la solución (i.e. el boceto) de un problema sobre ideales irreducibles, que llegó a ser uno de los trabajos más importantes de Gröbner. Donde Bruno Buchberger fue uno de los estudiantes importantes de Wolfgang Gröbner; desde que en 1966 leyó su tesis encontrando una base del espacio vectorial cociente para el anillo de clases, módulo un ideal de polinomios cero dimensional (en alemán), bajo la dirección del profesor Wolfgang Gröbner, a Bruno se le considera el inventor de la teoría de bases de Gröbner. Su algoritmo ha sido estudiado, mejorado y generalizado en los últimos 30 años, y lo más importante, se han encontrado multitud de aplicaciones a las ramas más diversas, incluidas criptografía, física, ingeniería y robótica entre otras. La naturaleza constructiva y computacional de esos métodos, en la era de la informática, lo hacen líder de las aplicaciones en muchos campos. Su algoritmo ha sido implementado y forma parte de todos los sistemas o paquetes de cálculo simbólico actuales tales como Mathematica, Macsyma, Magma, Maple, Derive y Reduce.

En 1694, John Bernoulli conjeturo que la integral nació de a longitud de arco de una elipse que no pudiera ser integrada. Entonces en anillos conmutativos involucrado por el anillo de polinomios avanzando con la teoría de números, principalmente la divisibilidad entre dos enteros a y b con la pregunta ¿Cuándo $a \mid b$?, según la teoría de números nos indica: cuando b es múltiplo de a, luego se traslada la cuestión a ideal principal, $a \mid b$ si y solo si $(a) \subset (b)$. En general, obtener las cuestiones y operaciones que son:

- Decidir si un polinomio f pertenece a un ideal I (*ideal membership*)
- Decidir cuándo dos ideales son iguales
- Calcular la suma de ideales, Calcular el producto de ideales
- Calcular la intersección de ideales, Eliminar variables(ver en aplicaciones de las Bases de Gröbner)

1.2. Planteamiento del Problema

1.2.1. Formulación del Problema

Así, por todo lo expuesto anteriormente, el problema en que se basa el presente trabajo de investigación es el siguiente:

¿Cómo sistematizar la teoría relacionada de orden monomiales en $F[x_1, x_2, ..., x_n]$ ***para el desarrollo de las Bases de Gröbner?.***

1.3. Objetivos:

1.3.1. Objetivo General:

► *Desarrollar los teoremas de Orden Monomiales para polinomios de n-variables , el Teorema de las Bases de Gröbner y ver la optimización de Bruno Buchberger sobre tal teorema de Gröbner.*

1.3.2. Objetivos Específicos:

- Analizar la teoría de Orden Monomiales en el campo de n-variables $F[x_1, x_2, ..., x_n]$.
- Proponer la construcción de la estructura de $F[x_1, x_2, ..., x_n]$ de manera inductiva, por medio de la inducción efectiva.

- Determinar definiciones y teoremas con respecto sobre las principales características de una base de Gröbner.
- Describir la aplicación del teorema y las definiciones de la bases de Gröbner .

1.4. Justificación

Dado que el presente documento es realizado por que, se tiene mucha importancia e interés de mostrar a los demás la teoría, definiciones y la estructura que tiene una Base de Gröbner en $F[x_1, x_2, ..., x_n]$ y además la forma en que se divide polinomios en n-variables, es decir; la generalización del algoritmo de la división combinado con el algoritmo euclidiano en un campo de varias variables $F[x_1, x_2, ..., x_n]$(ver en Anexos) que es parte del algebra de anillos conmutativos, siendo una de las áreas más ricas para los estudios matemáticos - científicos.

Como ya se mencionó anteriormente, este documento será y servirá para todos los estudiantes egresados de la carrera de Matemática y estudiantes que cursan últimos semestres, como una fuente de información referido a la teoría de las Bases de las Gröbner principalmente y adicionando la división de polinomios.

El desarrollo y posterior implementación del teorema puede ser útil para la teoría de números y principalmente para el algebra abstracta, particularmente en los ejes temáticos sobre el anillo de polinomios, ideales, entre otros.

1.5. Alcances y Limitaciones

El Algoritmo de la División y la Euclidiana, analizado en el presente trabajo de investigación se limita al estudio de teoría de Polinomios en n-variables con coeficientes en un campo y no en un escenario donde se tenga una serie infinita de polinomios.

Lo que se hará es simplemente mostrar el desarrollo del teorema de las Bases Gröbner lo cual se limitará a demostrar el algoritmo de manera computacional ya que esto se realiza

en el area de computación informática. Se pretende llegar a los siguientes alcances:

1. Llegar solo hasta optimización de la bases Gröbner(Criterio de B.Buchberger).
2. Alcanzar a mostrar el desarrollo de teoremas, definiciones, corolarios de las bases de Gröbner
3. Que llegue el presente documento a estudiantes que gusten del area de algebra en la carrera de Matemática.

Finalmente implementar una propuesta para la demostración del problema. ♦

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

Capítulo 2

Orden Monomiales

2.1. Orden de Monomios en $F[x_1, x_2, ..., x_n]$

Para esta sección vamos a dar un orden a los términos de un polinomio. El caso para una variable es sencillo, pues tenemos el siguiente orden:

$$1 < x < x^2 < ... < x^m < x^{m+1} < ....$$

ya que el orden implícitamente es el grado del polinomio, esto es que si tenemos $f(x) = 4x^5 - 2x^3 + 2x - 5$ el término principal es $4x^5$ y el coeficiente principal es 4.

Pero dados los siguientes polinomios; $f(x, y) = 2x^2y + 4xy^2 + 8xy$ y $g(x, y, z) = 4x^2yz^3 - xy^3z^2 + 3y^3x^2z + 10$ como podemos ver el $deg(f) = 3$ y $deg(g) = 6$ pero no sabemos cual es el primer término principal de los polinomios $f \in F[x, y]$ y $g \in F[x, y, z]$ para resolver este problema definimos lo siguiente, que a posterior lo necesitamos para poder dividir

polinomios en varias variables con respecto a alguna variable.

Por lo cual es necesario definir un *orden* para las n variables digamos se tiene: $x_1 > x_2 > .... > x_n$ entonces nos reducimos a dar un orden total a $\mathbb{N}^n$ que cumpla: si $\mathbf{x}^\alpha \in F[x_1, x_2, ..., x_n]$, entonces $1 < \mathbf{x}^\alpha$ para todo monomio no constante y si $\mathbf{x}^\beta \geq \mathbf{x}^\gamma$ si y solo si $\mathbf{x}^{\beta+\alpha} \geq \mathbf{x}^{\gamma+\alpha}$ para toda $\alpha \in \mathbb{N}^n$, formalmente esto quiere decir en la siguiente definición.

Definición 2.1.1. Un *Orden Monomial* en el dominio entero $F[x_1, x_2, ..., x_n]$ es una relación de orden total "$\geq$" sobre los vectores $\alpha \in \mathbb{N}^n$ que satisface las dos siguientes condiciones:

1. Sean $\alpha = (a_1, a_2, ..., a_n)$ y $\beta = (b_1, b_2, ..., b_n) \in \mathbb{N}^n$, si $\alpha \geq \beta$ y $\gamma \in \mathbb{N}^n$, entonces $\alpha + \gamma \geq \beta + \gamma$

2. $\geq$ es un buen orden sobre $\mathbb{N}^n$. (Esto es, que cada subconjunto no vacío de $\mathbb{N}^n$ tiene un elemento mínimo bajo la relación de orden $\geq$)

El siguiente lema nos va ser de mucha ayuda para entender el verdadero significado de la condición 2) del buen orden.

Lema 2.1.2. *Una relación de orden $\gneq$ sobre $\mathbb{N}^n$ es un buen orden si y sólo si cada sucesión decreciente en $\mathbb{N}^n$*

$$\alpha_1 \gneq \alpha_2 \gneq \alpha_3 \gneq .....$$

eventualmente se estaciona.

Demostración.- La prueba será por contrapositiva, en efecto por probar que $\gneq$ no es un buen orden si y sólo si existe una sucesión infinita decreciente en $\mathbb{N}^n$.

Probaremos en el sentido $\Rightarrow$] Si $\gneq$ no es un buen orden, entonces algún subconjunto no vacío $N \subset \mathbb{N}^n$ no tiene elemento mínimo. Como $N \neq \emptyset$ entonces escójase un n-tuple $\alpha_1 \in N$, como α_1 no es elemento mínimo, podemos encontrar un $\alpha_2 \in N$ tal que $\alpha_1 \gneq \alpha_2$ en N. Ahora, como α_2 tampoco es elemento mínimo de N, entonces hay un $\alpha_3 \in N$ tal que

$\alpha_2 \gneq \alpha_3$ en N. Continuando de esta manera obtenemos una sucesión infinita decreciente;

$$\therefore \qquad \alpha_1 \gneq \alpha_2 \gneq \alpha_3 \gneq ..... \qquad\qquad Q.E.P.D. \quad \blacksquare$$

Ahora probaremos en el sentido $\Leftarrow]$ por hipótesis; existe un sucesión infinita decreciente $\alpha_1 \gneq \alpha_2 \gneq \alpha_3 \gneq .....$, entonces sea el conjunto formado por los elementos de la sucesión $\{\alpha_1, \alpha_2, \alpha_3, ...\}$ es un subconjunto no vacío de $\mathbb{N}^n$ sin elemento mínimo, ya que si fuera lo contrario, es decir que si existiera un elemento mínimo en $\{\alpha_1, \alpha_2, \alpha_3, ...\}$ la sucesión eventualmente terminaría en algún α_j en consecuencia seria finita la sucesión lo que entra en contradicción con la hipótesis. Por lo tanto no tiene elemento mínimo y con esto $\gneq$ no es buen orden. $Q.E.P.D.$ $\blacksquare$

► Notese que si I es un ideal en $F[x_1, x_2, ..., x_n]$ generado por un conjunto S (posiblemente infinito) de polinomios, por uno de los corolario a posterior se prueba que I es finitamente generado. La prueba del teorema de bases de Hilbert muestra que la colección de coeficientes principales de los polinomios en un ideal I de $K[x]$ forman un ideal extremadamente útil en K que pueden ser usados para entender I.
Esto sugiere estudiar *términos principales* en $F[x_1, x_2, ..., x_n]$, para hacer esto necesitamos especificar un orden total sobre los monomios para tener un orden en las n-variables, pues sin algún tipo de orden no podemos en general decir cual es el término principal de un polinomio. Implícitamente elegimos un orden tal en prueba inductiva del corolario anterior(Teorema de las Bases de Hilbert) como vimos un polinomio f como un polinomio en x_1 con coeficientes en $F[x_2, ..., x_n]$, digamos que vimos a su coeficiente principal en ahí como un polinomio en $F[x_3, x_4, ..., x_n]$, etc. Este es un ejemplo de un orden lexicográfico para monomios (*orden monomial lexicográfico*)en el anillo de polinomios $F[x_1, x_2, ..., x_n]$ que está definido claramente primero un orden en las variables, por ejemplo $x_1 > x_2 > .... > x_n$ y declarando el término monomio $Ax_1^{a_1}x_2^{a_2} \cdots {x_n}^{a_n}$ con exponentes $(a_1, a_2, ..., a_n)$ tiene un orden más alto que el término monomio $Bx_1^{b_1}x_2^{b_2} \cdots {x_n}^{b_n}$ con exponentes $(b_1, b_2, ..., b_n)$ si la primera componente donde las $n-tuples$ difieren, tiene $a_i > b_i$; esto es análogo al orden usado en un diccionario (de ahí el nombre), donde la letra a viene antes que la letra b, la

cual viene su vez antes que la letra c, etc. entonces *aarava* viene antes de *abaco*. Note que el orden esta definido solamente salvo multiplicación por unidades y que multiplicar dos monomios por el mismo monomio no cero no cambia su orden, esto puede ser formalizado en la siguiente manera:

Definición 2.1.3.(Orden Lexicográfico) Dados los n-tuples $(a_1, a_2, ..., a_n)$ y $(b_1, b_2, ..., b_n) \in \mathbb{N}^n$ diremos que $(a_1, a_2, ..., a_n) >_{lex} (b_1, b_2, ..., b_n)$, si en la diferencia vectorial $(a_1, a_2, ..., a_n) - (b_1, b_2, ..., b_n) \in \mathbb{Z}^n$, donde la coordenada no cero de izquierda a derecha es positiva.
Entonces escribiremos:

$$Ax_1^{a_1}x_2^{a_2}\cdot\cdot\cdot\cdot{x_n}^{a_n} >_{lex} Bx_1^{b_1}x_2^{b_2}\cdot\cdot\cdot\cdot{x_n}^{b_n} \qquad si \qquad (a_1, a_2, ..., a_n) >_{lex} (b_1, b_2, ..., b_n)$$

Ejemplo 2.1.4. Algunos ejemplos del Orden Lexicográfico son:

1. $(1, 2, 0) >_{lex} (0, 3, 4)$ puesto que $(1, 2, 0) - (0, 3, 4) = (1, -1, -4) \in \mathbb{Z}^3$
2. $(3, 2, 4) >_{lex} (3, 2, 1)$ puesto que $(3, 2, 4) - (3, 2, 1) = (0, 0, 3) \in \mathbb{Z}^3$
3. Las variables $x_1, x_2, ..., x_n$ están ordenados de la forma usual por el orden lexicográfico, puesto que:

   $$(1, 0, ..., 0) >_{lex} (0, 1, 0, ..., 0) >_{lex} \cdot\cdot\cdot\cdot >_{lex} (0, 0, ..., 1)$$

   por lo que;

   $$x_1 >_{lex} x_2 >_{lex}, ..., >_{lex} x_n$$

El nombre y la idea del Orden Lexicográfico proviene como lo hemos recalcado antes, por el orden análogo para las palabras usadas por los diccionarios.

Teorema 2.1.5. *El Orden lexicográfico sobre $\mathbb{N}^n$ es un Orden Monomial.*
Demostración.- (i) Como $>_{lex}$ es un orden(reflexiva, antisimétrica y transitiva) tal que si $\alpha >_{lex} \beta$ si la diferencia vectorial $\alpha - \beta \in \mathbb{Z}^n$ la primera entrada no cero de la izquierda

es positiva, como $\alpha - \beta = (\alpha + \gamma) - (\beta + \gamma)$ para todo $\gamma \in \mathbb{N}^n$, si la diferencia vectorial de $(\alpha + \gamma) - (\beta + \gamma) \in \mathbb{Z}^n$ la primera entrada no cero de la izquierda es positiva; es decir, $\alpha + \gamma >_{lex} \beta + \gamma$.

(ii) Supongamos por hipótesis que $>_{lex}$ no es un buen orden; entonces según el Lema 2.1.2. debe haber una sucesión infinita decreciente, $\alpha_1 >_{lex} \alpha_2 >_{lex} \alpha_3 >_{lex} ....$ de elementos de $\mathbb{N}^n$ o $\alpha_1 = \alpha_2 = \alpha_3 = ...$ Si hubiese el caso en que $\alpha_i = \alpha_j$ para algún $i < j$, entonces termina la sucesión lo que seria finita pero esto contradice a la hipótesis.

Supongamos que $\alpha_i \neq \alpha_j$ para todo $i < j$, entonces $\alpha_1 >_{lex} \alpha_2 >_{lex} \alpha_3 >_{lex} ....$, si $\alpha_i >_{lex} \alpha_j$ la diferencia vectorial $\alpha_i - \alpha_j \in \mathbb{Z}^n$ donde la primera entrada no cero de la izquierda es positiva, es decir, $a_{1i} - a_{1j} > 0$ para α_i, α_j respectivamente, esto significa que $a_{1i} > a_{1j}$ con $a_{1i}, a_{1j} \in \mathbb{N}$ por definición del orden lexicográfico estas primeras entradas forman una sucesión decreciente de números naturales no nulos; dado que $\mathbb{N}$ esta bien ordenado las primeras entradas de las α_i se deben estacionar eventualmente, es decir; existe k tal que todas las primeras entradas de las α_i, $i = 1, 2, 3....k$ con $i \geq k$ son iguales.

Las segundas entradas de $\alpha_k, \alpha_{k+1}, ...$ forman una sucesión decreciente, análogamente al anterior se estacionan eventualmente, considerando que para algunas l los $\alpha_l, \alpha_{l+1}, ...$ son iguales lo que contradice el hecho de que $\alpha_k >_{lex} \alpha_{k+1}$. ■

Definición 2.1.6. Sea $f = \sum_{\mathbf{a}} \alpha_{\mathbf{a}} \mathbf{x}_{\mathbf{a}} \in F[x_1, x_2, ..., x_n]$ tal que; $\mathbf{a} := (a_1, a_2, ..., a_n)$ y $\mathbf{x} := (x_1, x_2, ..., x_n)$ no nulo y " $>$ " un orden monomial en el Dominio entero $F[x_1, x_2, ..., x_n]$.

1. El multigrado de f es:

$$MGRAD(f) = \text{máx}\{\mathbf{a} \in \mathbb{N}^n / \alpha_{\mathbf{a}} \neq 0\}$$

2. El monomio Líder de f es:

$$LM(f) = \mathbf{x}^{MGRAD(f)}$$

3. El coeficiente Líder o principal de f es:

$$LC(f) = \alpha_{MGRAD(f)}$$

Y cuando $f = 0$ (es el polinomio nulo) tomaremos $LC(f) = 0$

4. El término Líder o principal de f es:

$$LT(f) = LC(f).LM(f)$$

Para ilustrar esta definición consideremos el polinomio $f = 4x^3y^2z + 8xy^3z^2 - 5x^5$ y sea $\geq$ denotando al orden lexicográfico $x >_{lex} y >_{lex} z$. Entonces:

$$MGRAD(f) = (5, 0, 0)$$

$$LM(f) = x^5$$

$$LC(f) = -5$$

$$LT(f) = LC(f).LM(f) = -5x^5$$

★ Es importante recalcar que hay varios órdenes lexicográficos, dependiendo de como estén ordenadas las variables, por ejemplo hemos usado el orden lexicográfico con el orden de las variables $x_1 > x_2 >, ..., > x_n$. En general para n variables existen $n!$ órdenes lexicográficos, uno para cada orden posible de las variables.

Definición 2.1.7. Fijamos un *orden monomial* en el Dominio entero de polinomios en n-variables $F[x_1, x_2, ..., x_n]$,

1. Sea I un ideal en $F[x_1, x_2, ..., x_n]$ el ideal de términos principales, denotado $LT(I)$, es el ideal generado por los términos principales de todos los elementos(polinomios) del ideal, es decir; $LT(I) = \langle LT(f)/f \in I\rangle$; donde:

$$I = \langle g_1, \ldots, g_n\rangle = \left\{ \sum_{i=1}^{m} g_i r_i \ / r_i \in F[x_1, \ldots, x_n] \right\}$$

$$LT(I) = \langle LT(g_1), \ldots, LT(g_n)\rangle = \left\{ \sum_{i=1}^{m} LT(g_i) f_i \ / f_i \in F[x_1, \ldots, x_n],\ g_i \in I \right\}$$

El término principal y el multigrado de un polinomio claramente dependen de la relación de orden.

Ejemplo 2.1.8. Sea $LT(2xy+y^3) = 2xy$ con multigrado $(1, 1)$ si $x > y$; pero $LT(2xy+y^3) = y^3$ con multigrado $(0, 3)$ si $y > x$. El término principal de un polinomio no necesita ser el

término de grado total más grande sino de la relación de orden de las variables. Similarmente el ideal de términos principales $LT(I)$ de un ideal I en general dependen del orden utilizado, note también que el multigrado de un polinomio satisface algunas condiciones interesante en el Lema 2.1.8. a continuación.

El ideal $LT(I)$ esta por definición generado por monomios, tales ideales son llamados *ideales de monomios* y son típicamente fáciles de trabajar que con ideales genéricos. Por ejemplo un polinomio está contenido en un ideal de monomios si y solo si cada uno de sus términos monomios es múltiplo de uno de los generadores del ideal.

Si el ideal $I = \langle f_1, ..., f_m \rangle$, entonces $LT(I)$ contiene los términos principales que estos son, $LT(f_1), ..., LT(f_m)$ de los generadores de I por definición, como $LT(I)$ es un ideal, contiene el ideal generado por estos términos principales:

$$\langle LT(f_1), ..., LT(f_m) \rangle \subseteq LT(I)$$

El primero de los ejemplos siguientes prueba que el ideal $LT(I)$ de términos principales puede en general ser estrictamente más grande que el ideal generado por los términos principales de algunos generadores de I.

Lema 2.1.9. *Sean f, $g \in F[x_1, x_2, ..., x_n]$ polinomios no nulos. Entonces:*

1. $MGRAD(fg) = MGRAD(f) + MGRAD(g)$
2. *Si $f + g \neq 0$, entonces $MGRAD(f + g) \leq$ máx$\{MGRAD(f), MGRAD(g)\}$. Si además $MGRAD(f) \neq MGRAD(g)$, entonces la igualdad se cumple.*

Ejemplo 2.1.10. Elija el orden lexicográfico $x > y$; en $F[x, y]$; dados los polinomios $f_1 = x^3y - xy^2 + 1$ y $f_2 = x^2y^2 - y^3 - 1$ son $LT(f_1) = x^3y$(Así el multigrado de f_1 es $MGRAD(f_1) = (3, 1)$) y $LT(f_2) = x^2y^2$(Así el multigrado de f_2 es $MGRAD(f_2) = (2, 2)$). Si $I = (f_1, f_2)$ es el ideal generado por f_1 y f_2, entonces el ideal de términos principales $LT(I)$ contiene $LT(f_1)$ $LT(f_2)$, así que $\langle x^3y, x^2y^2 \rangle \subseteq LT(I)$ como:

$$yf_1 - xf_2 = y(x^3y - xy^2 + 1) - x(x^2y^2 - y^3 - 1) = x + y$$

vemos que el polinomio $x + y$ es un elemento de I y así el ideal $LT(I)$ también contiene al término principal $LT(x + y) = x$ esto muestra que $LT(I)$ es estrictamente más grande que $\langle LT(f_1), LT(f_2)\rangle = \langle x^3y, x^2y^2\rangle$ tiene grado tal al menos 4; vemos después que en este caso $LT(I) = \langle x, y^4\rangle$.

Ejemplo 2.1.11. Con respecto al orden lexicográfico $y > x$ los términos principales de f_1 y f_2 en el ejemplo anterior son $LT(f_1) = -xy^2$ (que se puede escribir como $-y^2x$ para enfatizar el orden elegido) y $LT(f_2) = -y^3$ vemos después que en este orden $LT(I) = \langle x^4, y\rangle$, el cual es un ideal diferente al ideal $LT(I) = \langle x, y^4\rangle$ del ejemplo anterior con el orden $x > y$, y es otra vez estrictamente más grande que $\langle LT(f_1), LT(f_2)\rangle$.

Ejemplo 2.1.12. Elijamos cualquier orden en $F[x, y]$ y sea $f = f(x, y)$ cualquier polinomio no cero; el término principal de cada elemento del ideal principal $I = \langle f\rangle$ es entonces un múltiplo del término principal de f, así en este caso $LT(I) = \langle LT(f)\rangle$.

2.2. Estructura de $F[x_1, x_2, ..., x_n]$

Definición 2.2.1..- Sea el anillo de polinomios en dos variables x_1, x_2 con coeficientes en F, denotado por $F[x_1, x_2]$ es definido por: $F[x_1, x_2] := F[x_1][x_2]$.
Esta definición quiere decir que podemos considerar a los polinomios en dos variables con coeficientes en F simplemente como polinomios en una variable (digamos x_2) pero con coeficientes que son ellos mismos en una variable(x_1).
Esto quiere decir que un polinomio;

$$f \in F[x_1, x_2] \Leftrightarrow f(x_1, x_2) \in F[x_1][x_2]$$

es decir;

$$f(x_1, x_2) = b_0 + (b_1)(x_2)^1 + ... + (b_{m-1})(x_2)^{m-1} + (b_m)(x_2)^m = \sum_{i=0}^{m}(b_i)(x_2)^i$$

tal que $b_i \in F[x_1]$ con $i = 0, 1, 2, ..., m$, como b_i es un polinomio en $F[x_1]$ por ejemplo:

$$b_0(x_1) = a_{00} + a_{10}x_1^1 + ... + a_{n0}x_1^{n0}$$

$$b_1(x_1) = a_{01} + a_{11}x_1^1 + ... + a_{n1}x_1^{n1}$$

$$b_2(x_1) = a_{02} + a_{12}x_1^1 + ... + a_{n2}x_1^{n2}$$

$$\vdots$$

$$b_i(x_1) = a_{0i} + a_{1i}x_1^1 + ... + a_{ni}x_1^{ni}$$

donde cada $a_{ji} \in F$ tal que $i = 0, 1, 2, ...m$ y $j = 0, 1, 2, ...n$

En una formulación un poco más concreta, un polinomio no cero en x_1, x_2 con coeficientes en F es una suma finita de términos monomio no cero, es decir; una suma finita de elementos de la forma $ax_1^{d_1}x_2^{d_2}$ donde $a \in K$ (el coeficiente del término) y los d_i son enteros no negativos. El exponente d_i es llamado el grado en x_i con $i = 1, 2$ del término y la suma $d = d_1 + d_2$ es llamado grado del término(conocido como grado absoluto); pero esto no nos servirá como definición para extender a más de dos variables, entonces el bi-tuple ordenado (d_1, d_2) es el multigrado del término.

Definición 2.2.2. El grado de un polinomio no cero en $F[x_1, x_2]$ es el grado más grande de todos sus términos *monomio*. Un polinomio es llamado homogéneo o una forma si todos sus términos tienen el mismo grado. Si f es un polinomio no cero en dos variables, la suma de todos los términos monomio en f de grado m es llamada la *componente homogénea* de f de grado n. Damos una descripción de la extensión natural de anillos de polinomios en varias variables que para esto tomamos un simple ejemplo en el anillo de polinomios $\mathbb{Z}[x, y]$ en dos variables x e y con coeficientes enteros de todas las sumas finitas de términos ***monomio*** de la forma ax^iy^j (de grado i+j).

Ejemplo 2.2.3.; Sean $p(x, y) = 2x^3 + xy - y^2$ y $q(x, y) = -2xy + 3y^2 + x^2y^3$ ambos elementos son de $\mathbb{Z}[x, y]$, de grados 3 y 5 respectivamente, tenemos que:

$$p(x, y) + q(x, y) = 2x^3 - xy + 2y^2 + x^2y^3$$

y además,

$$p(x,y).q(x,y) = -4x^4y + 6x^3y^2 + 2x^5y^3 - 2x^2y^2 + 5xy^3 + x^3y^4 - 3y^4 - x^2y^5$$

un polinomio de grado 8. Para ver este polinomio, como un polinomio en la variable y con coeficientes en $\mathbb{Z}[x]$ escribimos el polinomio en la forma siguiente:

$$(-4x^4)y + (6x^3 - 2x^2)y^2 + (2x^5 + 5x)y^3 + (x^3 - 3)y^4 - (x^2)y^5$$

Las componentes homogéneas no cero de $f(x,y) := p(x,y).q(x,y)$ son los polinomios:

$$f_4 = -2x^2y^2 + 5xy^3 - 3y^4$$

$$f_5 = -4x^4y + 6x^3y^2$$

$$f_7 = x^3y^4 - x^2y^5$$

$$f_8 = 2x^5y^3$$

Por consiguiente definimos de manera natural e inductivamente las definiciones provisionales para fines consiguientes en el temas de estudio de las bases de Gröbner.

Definición 2.2.4. El anillo de polinomios en varias variables $x_1, x_2, ..., x_n$ con coeficientes en F, denotado por $F[x_1, x_2, ..., x_n]$ es definido inductivamente por: $F[x_1, x_2, ..., x_n] := F[x_1, x_{2,...,x_{n-1}}][x_n]$. Esta definición quiere decir que podemos considerar a los polinomios en n variables con coeficientes en F simplemente como polinomios en una variable (digamos x_n) pero con coeficientes que son ellos mismos en $n-1$ variables.

Definición 2.2.5. En general si f es un polinomio no cero en n variables, la suma de todos los términos monomio en f de grado m es llamada la *componente homogénea* de f de grado n. En general si f tiene grado d, entonces f puede ser de modo único como la suma $f_0 + f_1 + ... + f_{d-1} + f_d$ donde f_j es la componente homogénea de f de grado j, para $0 \leq j \leq d$ donde algún f_j puede ser cero.

Finalmente, para definir un anillo de polinomios en un número arbitrario de variables con coeficientes en F tomamos sumas finitas de términos monomio del tipo indicado arriba (pero donde las variables no están restringidas a solo $x_1, x_2, ..., x_n$) con la adición y multiplicación naturales tales que podemos definir este anillo como la union de todos los anillos de polinomios en un número finito de las variables que estén siendo consideradas.

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

Capítulo 3

Bases de Gröbner

3.1. Los Anillos Noetherianos

En esta sección consideramos polinomios en n variables sobre un campo F y además por conveniencia el anillo R siempre será un anillo conmutativo con identidad $1 \neq 0$. El anillo de polinomios $R[x]$ en la indeterminada x de una sola variable con coeficientes en R; para esto daremos a conocer algunas definiciones y resultados sumamente interesantes.

Definición 3.1.1. Un subconjunto $I \subset R$ del anillo, es un ideal de R si cumple las siguientes condiciones:

1. $(I,+) \preceq (R,+)$ *esto es* :

   a) $0 \in I \neq \emptyset$

   b) $Sif, g \in I$, entonces $f - g \in I$

2. $Si f \in I$ y $g \in R$, entonces $gf \in I$

A continuación vemos una forma de construir ideales.

Definición 3.1.2. Un anillo conmutativo R con $1 \neq 0$, es llamado *Noetheriano* si cada ideal de R es finitamente generado.

Los *anillos Noetherianos* serán estudiados con mayor detalle por otro investigador matemático; en esta sección desarrollaremos algo de la teoría básica y algoritmos resultantes para trabajar con ideales(finitamente generados) en $F[x_1, x_2, ..., x_n]$, como vimos en la anterior sección, un anillo de polinomios en n variables puede ser considerado como un anillo de polinomios en una variable con coeficientes en un anillo de polinomios en $n-1$ variables; donde podemos deducir que $F[x_1, x_2, ..., x_n]$ es Noetheriano del siguiente resultado más general.

Definición 3.1.3. Sea un subconjunto $I \subset R$ del anillo, el ideal I es finitamente generado en R, si existen $a_1, ..., a_n \in I$ tal que:

$$I = \langle a_1, .., a_n \rangle = \left\{ \sum_{i=1}^{n} r_i a_i / \qquad r_i \in R \right\}$$

donde cada suma contiene una cantidad finita de términos.

Teorema 3.1.4.*Sea R es un Anillo. Las siguientes condiciones son equivalentes;*

1. *R es Noetheriano*

2. *R cumple la Condición de la cadena ascendente esto significa: (Para toda cadena ascendente $I_1 \subset I_2 \subset I_3 \subset ....$ de ideales en R, existe $N \geq 1$ tal que $I_N = I_{N+1} = ...$ en este caso se dice que la cadena se estaciona).*

Prueba.(1)⇒(2) Sea $I_1 \subset I_2 \subset I_3 \subset ....$ una cadena de ideales en R; probaremos que cumple c.c.a. para esto consideremos $I = \bigcup_{i \in J} I_i$ donde J es el conjunto de indices $J = \{1, 2, 3, ...\}$; probemos que I es un ideal también de R. Para esto debe cumplirse lo siguiente:

1. $(I,+) \preceq (R,+)$ *esto es* :

   a) $0 \in I \neq \emptyset$ ya que $0 \in I_i \subset \bigcup_{i \in J} I_i = I$

   b) $Sif, g \in I$, entonces (P.D.) $f - g \in I$

   En efecto, si $Sif, g \in I$ entonces existen $j, k \in J$ tal que $f \in I_j$ y $g \in I_k$ ahora suponemos que $k > j$, entonces $f \in I_k$, entonces $f - g \in I_k$ pues I_k es uno de los ideales de R así, existe $k \in J$ tal que $f - g \in I_k$ esto es por definición $f - g \in I$

2. $Sif \in I$ y $r \in R$, entonces (P.D.) $rf \in I$

   Si $f \in I$ entonces existe $j \in J$ tal que $f \in I_j$ y $r \in R$ entonces $rf \in I_j$ puesto que I_j es uno de los ideales de R así por definición; existe $j \in J$ tales que $rf \in I_j$, entonces $rf \in I$.

En consecuencia I es finitamente generado pues por hipótesis R es Noetheriano; así por la definición 3.1.3. existen $f_1, ..., f_n \in I$ entonces tomemos $N = máx\{f_1, ..., f_n\}$ donde para algún $f_i \in I_{j_i}$ sea $N > j_i$ como los I_j forman sucesión ascendente de ideales se tiene que $\langle f_1, ..., f_n \rangle \subset I_N \subset I_{N+1} \subset ... \subset I = \langle f_1, ..., f_n \rangle$ de ahí se cierra la igualdad concluyendo que si existe $N \geq 1$ tal que $I_N = I_{N+1} = ...$ en este caso se dice que la cadena se estaciona.

Prueba.(2)⇒(1) Supongamos que R no es Noetheriano entonces probaremos que R no cumple la condición de cadena ascendente.

Sea I un ideal de R que no admite un conjunto finito de generadores es decir para todo $f_1, f_2, ...$ no generan I. Por construcción sea un $f_1 \in I$ donde el ideal generado por f_1 es $\langle f_1 \rangle \precneqq I$ donde se da $\neq$ pues $f_1 \in I - \langle f_1 \rangle$ similarmente tómese un elemento $f_2 \in I$ tal que $\langle f_1 \rangle \precneqq \langle f_1, f_2 \rangle \precneqq I$ pues $f_2 \in I - \langle f_1, f_2 \rangle$ así sucesivamente extendiendo la secuencia de ideales infinitamente,

$$\langle f_1 \rangle \precneqq \langle f_1, f_2 \rangle \precneqq \langle f_1, f_2, f_3 \rangle \precneqq .....$$

tal ninguno de los ideales puede ser todo I pues es infinito, por lo tanto R no cumple la condición de cadena ascendente. ■

Teorema 3.1.5. (***Hilbert's basis theorem***) *Si K es un Anillo Noetheriano, entonces $K[x]$ también es Noetheriano.*

Prueba.- Sea I un ideal en $K[x]$ y sea L el conjunto de todos los coeficientes principales de los elementos de I. Probamos primero que L es un ideal de K, en efecto como I contiene al polinomio cero, $0 \in L$. Sean $f = ax^d + \cdots$ y $g = bx^e + \cdots$ polinomios en I de grados d, e y coeficientes principales $a, b \in K$ entonces para cada $r \in K$, $ra - b = 0$ o el coeficiente principal es el polinomio $rx^e f - x^d g$. Como este polinomio está en I tenemos que $ra - b \in L$ lo cual prueba que L es un ideal de K.

Ahora como K es asumido Noetheriano, el ideal L en K es finitamente generado, digamos por $a_1 a_2, ..., a_n$ tal que $a_i \in K$ para cada $i = 1, 2, ..., n$; sea f_i un elemento de I cuyo coeficiente principal es a_i donde e_i denota el grado de f_i para cada $i = 1, 2, ..., n$ tal que;

$$N = máx\{deg(f_1), deg(f_2), ..., deg(f_n)\} = máx\{e_1, e_2, ..., e_n\}$$

Para cada $d \in \{0, 1, 2, ..., N-1\}$ sea L_d el conjunto de todos los coeficientes principales de polinomios en I de grado d junto con el cero. Un argumento similar como en el L se prueba que cada L_d es también un ideal de K, de nuevo L_d es finitamente generado pues K es Noetheriano; ahora para cada L_d sea $b_{d,1}, b_{d,2}, ..., b_{d,n_d} \in K$ un conjunto de generadores para L_d, y sea $f_{d,i}$ un polinomio en I de grado d con coeficiente principal así $b_{d,i}$.

Probamos ahora que los polinomios $f_1, f_2, ..., f_n$ junto con todos los polinomios $f_{d,i}$ para todos los ideales no cero L_d son un conjunto de generadores para I, es decir; que

$$I' = (\{f_1, f_2, ..., f_n\} \cup \{f_{d,i} \,/\, 0 \leq N < d,\ 1 \leq i \leq n_d\})$$

Por construcción el ideal I' está contenido en I pues todos los generadores fueron elegidos en I. Si $I' \neq I$, existe un polinomio no cero $f \in I$ de grado mínimo tal que f no esta en I'. Sean $deg(f) = d$ y a el coeficiente principal de f.

Supongamos primero que $d \geq N$, como $a \in L$ podemos escribir a como una combinación $K - lineal$ de los generadores de L, esto es: $a = r_1 a_1 + r_2 a_2 + ... + r_n a_n$; entonces $g = r_1 x^{d-e_1} f_1 + r_2 x^{d-e_2} f_2 + ... + r_n x^{d-e_n} f_n$ es un elemento de I' con el mismo grado d y el

mismo coeficiente principal a de f. Entonces $f - g \in I$de grado más pequeño que f, por su minimalidad debemos tener que $f - g = 0$, así $f = g \in I'$ lo cual es una contradicción.

Ahora supongamos que $d < N$ en este caso $a \in L_d$ para algún $d < N$, así que podemos escribir $a = r_1 b_{d,1} + r_2 b_{d,2} + ... + r_{n_d} b_{d,n_d}$ para algunos $r_i \in K$. Entonces $g = r_1 f_{d,1} + \cdots + r_{n_d} f_{d,n_d}$ es un polinomio en I' con el mismo grado d y el mismo coeficiente principal a de f y tenemos una contradicción como antes. Así tenemos que $I = I'$ es finitamente generado, como I fue arbitrario esto completa la prueba que $K[x]$ es Noetheriano. ■ Q.E.P.D.

Puesto que un campo claramente es Noetheriano, el teorema de las Bases de Hilbert y la inducción dan como resultado lo siguiente:

Corolario 3.1.6. *Cada ideal en el dominio entero de polinomios $F[x_1, x_2, ..., x_n]$ con coeficientes en un campo F es finitamente generado.*

3.2. Estructura de la Base Gröbner

A través de este capítulo vamos a estudiar las bases de Gröbner, que nos van a permitir resolver problemas sobre ideales polinomiales, de una manera algorítmica. Las bases de Gröbner se usan en muchos sistemas algebraicos computacionales poderoso para estudiar ideas especificas ideas polinomiales que aterrizan en diversas aplicaciones.

Definición 3.2.1. Una *base Gröbner* para un ideal I en el anillo de polinomios $F[x_1, ..., x_n]$ es un conjunto finito de generadores $\{g_1, ..., g_m\}$ para I cuyos términos principales generan el ideal de todos los términos principales en I, es decir;

$$I = \langle g_1, ..., g_m \rangle \quad y \quad LT(I) = \langle LT(g_1), ..., LT(g_m) \rangle$$

donde I y $LT(I)$ son;

$$I = \left\{ \sum_{i=1}^{m} g_i r_i \,/ r_i \in F[x_1, \ldots, x_n] \right\}$$

$$LT(I) = \left\{ \sum_{i=1}^{m} LT(g_i) f_i \,/ f_i \in F[x_1, \ldots, x_n],\ g_i \in I \right\}$$

Observación 3.2.2. Notese que una *base Gröbner* es de hecho un conjunto de generadores para I (que depende de la elección del orden), es decir; cada elemento en I es una combinación lineal de los generadores, pero no es una base en el sentido de espacios vectoriales (donde la combinación lineal podría ser única).
Una de las propiedades más importantes de una *base Gröbner* es que cada polinomio g puede ser escrito de modo único como la suma de elementos en I y un resto r obtenido por una división general de polinomios. En particular vemos que g es un elemento de I si y solo si $r = 0$, ya que si no utilizamos una *base Gröbner* la unicidad es perdida, pues existen términos principales no considerados por los términos principales de los generadores.

Teorema 3.2.3. *Fije un orden monomial en* $F[x_1, x_2, ..., x_n]$ *y suponga que* $\{g_1, ..., g_m\}$ *es una* base Gröbner *para el ideal no cero* I *de* $F[x_1, x_2, ..., x_n]$. *Entonces:*

1. *Cada polinomio* $f \in F[x_1, x_2, ..., x_n]$ *puede ser escrito de modo único en la forma* $f = f_I + r$ *donde* $f_I \in I$ *y ningún término mónico no cero del resto* r *es divisible por cualquiera de los términos principales* $LT(g_1), ..., LT(g_m)$.

2. *Ambos* f_I *y* r *pueden ser calculados por la división general de polinomios para* $g_1, ..., g_m$ *y son independientes del orden en el cual estos son utilizados en la división.*

3. *El resto* r *da un único representante para la clase de* f *en el anillo cociente de polinomios* $F[x_1, x_2, ..., x_n]/I$. *En particular* $f \in I$ *si y solo si* $r = 0$.

$$\frac{F[x_1, \ldots, x_n]}{I} = \{f(x_1, \ldots, x_n) + I \,/ f \in F[x_1, \ldots, x_n]\}$$

donde esto significa:

$$f(x_1, \ldots, x_n) + I = \{f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n) \,/ g \in I\}$$

Demostración(1).-Supongamos que $\{g_1, ..., g_m\}$ es una *base Gröbner* para el ideal no cero I, realizando $f_I = g_1q_1 + ... + g_mq_m \in I$ en la división general de polinomios f por $g_1, ..., g_m$ inmediatamente da una descomposición $f = f_I + r$ para cualesquiera generadores $g_1, ..., g_m$;

sean $f = f_I + r$ y $f = f'_I + r'$, entonces se tiene: $f_I + r = f'_I + r'$ esto significa que $r - r' = f'_I - f_I \in I$ así su término principal $LT(r - r')$ es un elemento de $LT(I)$ que es el ideal $\langle LT(g_1), ..., LT(g_m)\rangle$ pues $\{g_1, ..., g_m\}$ es una *base Gröbner* para I. Donde cada elemento de este ideal es una suma de múltiplos de los términos monomios $LT(g_1), ..., LT(g_m)$, así es una suma de términos cada uno de los cuales es divisible por uno de los $LT(g_i)$. Además r y r' por tanto $r - r'$ son sumas de términos monomios ninguno de los cuales es divisible por $LT(g_1), ..., LT(g_m)$, lo cual es una contradicción a menos de que $r - r' = 0$ es decir; $r = r'$ es único, por tanto así es $f_I = f - r$. ■

Demostración(2).- Como f_I y r pueden ser calculados algorítmicamente por la división de polinomios, y la unicidad en (1) implica que r es independiente del orden en el cual los polinomios $g_1, ..., g_m$ son usados en la división, como $f_I = g_1q_1 + ... + g_mq_m$ está determinado de manera única(aún cuando los cocientes individuales q_i no son en general únicos) de manera independiente, lo cual prueba (2). ■

Demostración(3).- Si tomamos $r = 0$, entonces por (1) $f = f_I \in I$; recíprocamente si $f \in I$ entonces $f = f + 0$ y por la unicidad de r implica que $r = 0$. ■

Corolario 3.2.4. *El resto al dividir por una* base Gröbner *es único.(que satisface las propiedades del algoritmo de la división generalizada)*

Demostración.- Sea $G = \{g_1, ..., g_m\}$ una *base Gröbner* para el ideal no cero I, y

$$f = g_1q_1 + ... + g_mq_m + r = g_1q'_1 + ... + g_mq'_m + r'$$

donde ningún termino de r y r' es divisible por $LT(g_i)$ así pasa lo mismo con los términos de $r - r'$. Ahora consideremos el polinomio;

$$h = g_1q_1 + ... + g_mq_m - (g_1q'_1 + ... + g_mq'_m) = r - r' \qquad (\bigstar)$$

como $h \in I$ y G es una *base Gröbner* si tenemos el caso en que $h \neq 0$ entonces $LT(h)$ es divisible por algún $LT(g_i)$ y esto llega a contradecir ya que $r - r'$ no es divisible por $LT(g_i)$; entonces $h = 0$ así en $(\bigstar)$ se tiene por lo tanto $r = r'$. ■

Proposición 3.2.5. *Fije un orden monomial en $F[x_1, x_2, ..., x_n]$ y sea I un ideal no cero en $F[x_1, x_2, ..., x_n]$.*

1. *Si $g_1, ..., g_m$ son elementos cualesquiera de I tales que $LT(I) = \langle LT(g_1), ..., LT(g_m)\rangle$, entonces $\{g_1, ..., g_m\}$ es una base Gröbner para I.*

2. *El ideal I tiene una base Gröbner.*

Demostración (1).-(Por Inducción efectiva) Supongase que $g \in I$ tal que $LT(I) = \langle LT(g)\rangle$ por demostrar que: $I = \langle g\rangle$,esto es equivalente a probar $f \notin \langle g\rangle \Leftrightarrow f \notin I$.

Sea $f \in F[x_1, x_2, ..., x_n]$ aplicando el algoritmo de la división generalizada con el polinomio dado g se tiene que $f = gq + r$ con $g \in I$ y por hipotesis $r \neq 0$ pues $f \notin \langle g\rangle$, donde $LT(g)|r_1$ y $LT(g)|r_2$ y supongamos que $r = r_1 + r_2$ tal que r_i son términos no ceros de r. Además $r \in I$ o $r \notin I$, en efecto si $r \in I$ entonces directamente $LT(r) \in \langle LT(g)\rangle$ esto implica que $LT(r) = f_k.LT(g)$ con $f_k \in F[x_1, x_2, ..., x_n]$ es decir; $LT(g)|LT(r)$ sin perdida de generalidad $LT(r) = r_i$ para algún $i = 1, 2$ lo que es una contradicción, por lo tanto $r \notin I$, luego $f \in I$ entonces $r \in I$ lo que es una contradicción. Así que $r = 0$ en tal efecto $f = gq$ es decir $f \in \langle g\rangle$ por lo tanto $I \subset \langle g\rangle$. ■

Aplicando la inducción efectiva se tendra que si tenemos $g_1, ..., g_m$ son elementos cualesquiera de I tales que $LT(I) = \langle LT(g_1), ..., LT(g_m)\rangle$, entonces $\{g_1, ..., g_m\}$ es una base Gröbner para I. ♦ Q.E.P.D.

Demostración (2).- Ahora para que el ideal I tenga una base Gröbner, simplemente tomamos el ideal $LT(I)$ de términos principales de cualesquiera ideal de I, es generado por todos los términos principales de los polinomios en I y por (1) ya demostrado obtenemos un número finitos de esos términos principales es suficiente para generar $LT(I)$,digamos $LT(I) = \langle LT(h_1), ..., LT(h_k)\rangle$ para $h_1, ..., h_k \in I$ y por (1) los polinomios $h_1, ..., h_k$ son una base de Gröbner de I. ■

Observación 3.2.6. $LT(I)$ es, por construcción, un ideal monomial (es decir un ideal generado por monomios; un polinomio está en un ideal monomial si y solo si todo término suyo está en el ideal).

Observación 3.2.7. Es fácil ver que $g_1, ..., g_m \in I$ es una base de Gröbner si y solo si $LT(g_1), ..., LT(g_m)$ generan el ideal inicial I.

★ La Proposición 3.2.5. prueba que siempre existen bases Gröbner; a continuación probaremos un criterio que determina si un conjunto dado de generadores de un ideal I es una base Gröbner, que usamos para dar un algoritmo para hallar una base Gröbner, la idea es: elementos adicionales en $LT(I)$ pueden aparecer tomando combinaciones lineales de generadores que cancelan términos principales, como vimos al tomar $yf_1 - xf_2$ en el ejemplo 2.1.9., en general si f_1 y f_2 son dos polinomios en $F[x_1, x_2, ..., x_n]$ y M es el mínimo común múltiplo mónico de los términos monomios $LT(f_1)$ y $LT(f_2)$ esto es: $M = mcm[LT(f_1), LT(f_2)]$, entonces podemos cancelar los términos principales tomando la diferencia;

$$S(f_1, f_2) = \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2$$

Esto nos indica la siguiente definición;

Definición 3.2.8. Sean f, $g \in F[x_1, x_2, ..., x_n]$ polinomios no cero,

1. Si $MGRAD(f) = \alpha = (a_1, ..., a_n)$ y $MGRAD(g) = \beta = (b_1, ..., b_n)$, entonces definimos $\gamma = (c_1, ..., c_n)$ con $c_i = máx\{a_i, b_i\}$ para cada i. Llamamos al monomio $\mathbf{x}^\gamma$ el *mínimo común múltiplo* de $LT(f)$ y $LT(g)$, denotado por: $M = mcm[LT(f), LT(g)]$

2. Definimos al *S-polinomio* de f y g como la combinación;

$$S(f, g) = \frac{M}{LT(f)}.f - \frac{M}{LT(g)}.g$$

Un *S-polinomio* de f y g $S(f, g)$ está diseñado para cancelar los términos iniciales entre f y g. De hecho el siguiente lema prueba que esta combinación lineal elemental cuenta

para todas las combinaciones de términos principales de polinomios del mismo multigrado(MGRAD).

Lema 3.2.9. *Suponga que $f_1, ..., f_m \in F[x_1, x_2, ..., x_n]$ son polinomios con el mismo multigrado α y que la combinación lineal $h = a_1f_1 + ... + a_mf_m$ con constantes $a_i \in F$ tiene multigrado estrictamente más pequeño. Entonces $h = \sum_{i=2}^{m} b_iS(f_{i-1}, f_i)$ para algunas constantes $b_i \in F$.*

Prueba .-Sea $f_i = c_if_i'$ para todo $i = 1, 2, ..., m$ sustituyendo en la combinación lineal $h = a_1f_1 + ... + a_mf_m$ con constantes $a_i \in F$, tal que f_i' es un polinomio mónico de multigrado α y $c_i \in F$, así tenemos:

$$\Rightarrow h = a_1f_1 + ... + a_mf_m = a_1c_1f_1' + ... + a_mc_mf_m'$$

tomando la ideal del siguiente truco matemático(sumar un cero adecuado) para $m = 3$;

$$\Rightarrow h = a_1f_1 + a_2f_2 + a_mf_m = a_1c_1f_1' + a_2c_2f_2' + a_3c_3f_3' =$$

$$= a_1c_1f_1' + a_2c_2f_2' + a_3c_3f_3' + \{a_1c_1(f_2' + f_3') + a_2c_2f_3'\} - \{a_1c_1(f_2' + f_3') + a_2c_2f_3'\} =$$

Reordenando tenemos lo siguiente:

$$\Rightarrow h = a_1f_1 + a_2f_2 + a_mf_m = a_1c_1(f_1' - f_2') + (a_1c_1 + a_2c_2)(f_2' - f_3') + (a_1c_1 + a_2c_2 + a_3c_3)(f_3')$$

Llevando esta idea de manera general se tiene:

$$h = a_1c_1(f_1' - f_2') + (a_1c_1 + a_2c_2)(f_2' - f_3') + ... + (a_1c_1 + ... + a_mc_m)(f_m')$$

★ Note que $f_{i-1}' - f_i' = S(f_{i-1}, f_i)$, entonces como h y cada $f_{i-1}' - f_i'$ tiene multigrado estrictamente pequeño que α, tenemos $a_1c_1 + ... + a_mc_m = 0$ así el último término del lado derecho de la suma en h es 0, es decir;

$$h = a_1c_1S(f_1, f_2) + (a_1c_1 + a_2c_2)S(f_2, f_3) + ... + (a_1c_1 + ... + a_mc_m)S(f_{m-1}, f_m) + (0)(f_m')$$

esto es:

$$h = a_1c_1S(f_1, f_2) + (a_1c_1 + a_2c_2)S(f_2, f_3) + ... + (a_1c_1 + ... + a_mc_m)S(f_{m-1}, f_m)$$

Por lo tanto se concluye la prueba,

$$\triangleright \quad h = \sum_{i=2}^{m} b_i S(f_{i-1}, f_i) \quad \textit{donde} \quad b_i = (a_1c_1 + ... + a_{i-1}c_{i-1}) \in F \quad .\blacksquare$$

La proposición siguiente prueba que un conjunto de generadores $g_1, ..., g_m$ es una base Gröbner si no existen nuevos términos principales entre las diferencias $S(g_i, g_j)$ no contadas por los g_i. Este resultado provee el ingrediente principal en un algoritmo para construir una base Gröbner.

3.3. Criterio de Bruno Buchberger

Teorema 3.3.1.(Criterio de Buchberger) *Sea $F[x_1, ..., x_n]$ fijado un orden monomial sobre este. Si $I = (g_1, ..., g_m)$ es un ideal no cero en $F[x_1, ..., x_n]$, entonces $G = \{g_1, ..., g_m\}$ es una base Gröbner para I si y solo si $S(g_i, g_j) \equiv 0(modG)$ para $1 \leq i < j \leq m$.*

Prueba $\Rightarrow\rfloor$ Si $\{g_1, ..., g_m\}$ es una base Gröbner para el ideal I, entonces se concluye que $S(g_i, g_j) \equiv 0(modG)$ esto es inmediato por el teorema 5.1 puesto que cada,

$$S(g_i, g_j) = \frac{M}{LT(g_i)} g_i - \frac{M}{LT(g_j)} g_j \in I$$

tal que $M = mcm[LT(g_i), LT(g_j)]$. ■

Prueba $\Leftarrow\rfloor$ Supongamos ahora que $S(g_i, g_j) \equiv 0(modG)$ para $1 \leq i < j \leq m$ y tomemos cualquier elemento $f \in I$; para ver que G es una base Gröbner necesitamos ver que $\langle LT(g_1), ..., LT(g_m)\rangle$ contiene a $LT(f)$; entonces como $f \in I$ podemos escribir $f = \sum_{i=1}^{m} h_i g_i$ para algunos $h_1, ..., h_m$ tal representación no es única. Entre todas esas elija una para la cual el multigrado más grande de cualquier sumando es decir, sea $\alpha = máx\{MGRAD(h_i g_i)\}$ que es minimal. Es claro que el multigrado de f no es menor que el multigrado más grande de todos los sumandos $h_i g_i$, así $MGRAD(f) \leq \alpha$, escribamos:

$$f = \sum_{i=1}^{m} h_i g_i = \sum_{MGRAD(h_i g_i)=\alpha} h_i g_i + \sum_{MGRAD(h_i g_i)<\alpha} h_i g_i$$

$$= \sum_{MGRAD(h_i g_i)=\alpha} LT(h_i)g_i + \sum_{MGRAD(h_i g_i)=\alpha} (h_i - LT(h_i))g_i + \sum_{MGRAD(h_i g_i)<\alpha} h_i g_i \qquad (\bigstar)$$

Si el $MGRAD(f) < \alpha$, entonces como el multigrado de las segundas dos sumas es también estrictamente más pequeña que α; se sigue que el multigrado de la primera suma es estrictamente más pequeña que α. Si $a_i \in F$ denota el coeficiente del término monomio $LT(h_i)$, implica que $LT(h_i) = a_i h_i'$ donde h_i' es un monomio, aplicando el Lema 3.1.8. a $\sum_i a_i(h_i' g_i)$ para escribir la primera suma como:

$$\sum_i b_i S(h_{i-1}' g_{i-1}, h_i' g_i) \qquad con \qquad MGRAD(h_{i-1}' g_{i-1}) = MGRAD(h_i' g_i) = \alpha$$

Sea el mínimo común múltiplo mónico de $LT(g_{i-1})$ y $LT(g_i)$ denotado por:

$$\beta_{i-1,i} = MGRAD\,\{mcm[LT(g_{i-1}), LT(g_i)]\}$$

Entonces un cálculo fácil prueba que $S(h_{i-1}' g_{i-1}, h_i' g_i)$ es precisamente $S(g_{i-1}, g_i)$ multiplicado por el monomio de multigrado $\alpha - \beta_{i-1,i}$. El polinomio $S(g_{i-1}, g_i)$ tiene multigrado menor que $\beta_{i-1,i}$ y por hipótesis $S(g_{i-1}, g_i) \equiv 0(mod G)$. Esto significa que después de la división general de polinomios de $S(g_{i-1}, g_i)$ por $g_1, ..., g_m$, cada $S(g_{i-1}, g_i)$ puede ser escrito como una suma $\sum_j g_j q_j$ con $MGRAD(g_j q_j) < \beta_{i-1,i}$, en consecuencia cada $S(h_{i-1}' g_{i-1}, h_i' g_i)$ es una suma $\sum_j g_j q_j'$ con,

$$MGRAD(g_j q_j') < \alpha$$

.

Pero entonces todas las sumas del lado derecho de la ecuación ($\bigstar$) pueden ser escritas como una suma de de términos de la forma $p_i g_i$ con polinomios satisfaciendo $MGRAD(p_i g_i) < \alpha$. Esto contradice la minimalidad de α y prueba que de hecho,

$$MGRAD(f) = \alpha$$

es decir el término principal de f tiene multigrado α.

Si tomamos ahora los términos en la ecuación ($\bigstar$) de multigrado α vemos que:

$$LT(f) = \sum_{MGRAD(h_i g_i)=\alpha} LT(h_i) \cdot LT(g_i),$$

Así $LT(f) \in \langle LT(g_1), ..., LT(g_m)\rangle$. Por tanto $\{g_1, ..., g_m\}$ es una base Gröbner. ■

El *criterio de Bruno Buchberger* puede ser utilizado para construir un algoritmo que permita encontrar una base Gröbner para I, como sigue: Si $I = \langle g_1, ..., g_m\rangle$ y cada $S(g_i), g_j$ deja un resto cero cuando es dividido por $\{g_1, ..., g_m\}$ utilizando la división general de polinomios, entonces $\{g_1, ..., g_m\}$ es una base Gröbner. En otro caso, si $S(g_i), g_j$ no deja un resto cero, incrementamos a $\{g_1, ..., g_m\}$ adicionando el polinomio $g_{m+1} = r$, luego será $\{g_1, ..., g_m, g_{m+1}\}$ y comenzamos otra ves (note que este es de nuevo un conjunto de generadores para I, pues $g_{m+1} \in I$). No es difícil verificar que este procedimiento termina después de un número finito de pasos en un conjunto generador $\{g_1, ..., g_m\}$ que satisface el criterio de B. Buchberger; por lo tanto es una base Gröbner para I.

(★) Note que cuando $S(g_i, g_j)$ da un resto 0 después de la división por los polinomios en $\{g_1, ..., g_m\}$, también da un resto cero cuando polinomios adicionales son anexados a $\{g_1, ..., g_m\}$.

Si $\{g_1, ..., g_m\}$ es una base Gröbner para el ideal I y $LT(g_j)$ es divisible por $LT(g_i)$ para algún $j \neq i$, entonces $LT(g_i)$ no es necesario como un generador para $LT(I)$.

Por el Teorema 3.2.6. podemos por lo tanto eliminar g_j y aún tener una base Gröbner para I; podríamos también asumir que sin perdida que el término principal de cada g_i es mónico.

Una base de Gröbner $\{g_1, ..., g_m\}$ para I donde cada $LT(g_i)$ es mónico y donde $LT(g_j)$ no es divisible por $LT(g_i)$ para $j \neq i$, es llamada una base Gröbner minimal no es única, el número de elementos y sus términos principales son únicos.

Problemas Fijamos un orden monomial lexicográfico $>_{lex}$ sobre $F[x, y]$ de las siguientes formas:

Ejemplo 3.3.2. Fijando orden lexicográfico $x > y$ sobre $F[x, y]$ y consideremos el ideal I generado por $f_1 = x^3y - xy^2 + 1$ y $f_2 = x^2y^2 - y^3 - 1$, para verificar si $G = \{f_1, f_2\}$ es una base Gröbner, calculamos $S(f_1, f_2) = yf_1 - xf_2 = x + y$, el cual es su resto cuando es dividido por $G = \{f_1, f_2\}$ así no es una base Gröbner para I. Sea $r_1 = x+y$ e incremente el conjunto generador $G' = \{f_1, f_2, r_1\}$. Ahora $S(f_1, f_2) \equiv 0(modG')$ y un calculo breve da:

$$S(f_1, r_1) = f_1 - x^2yr = -x^2y^2 + xy^2 + 1 \equiv 0(modG')$$

$$S(f_2, r_1) = f_2 - xy^2r = -xy^3 - xy^3 - 1 \equiv y^4 - y^3 - 1(modG')$$

Sea $r_2 = y^4 - y^3 - 1$ e incremente al conjunto generador a G' para obtener $G'' = \{f_1, f_2, r_1, r_2\}$; el resto es aún cero y ahora $S(f_2, r_1) \equiv 0(modG'')$ por la elección de r_2.

Un calculo adicional produce:

$$S(f_1, r_2) = S(f_2, r_2) = S(r_1, r_2) \equiv 0(modG'')$$

Así;

$$\{x^3y - xy^2 + 1; x^2y^2 - y^3 - 1; x + y; y^4 - y^3 - 1\} \quad \text{es base de Gröbner para } I$$

En particular $LT(I)$ es generado por los términos principales de estos cuatro polinomios, así $LT(I) = \langle x^3y; x^2y^2; x; y^4\rangle = \langle x; y^4\rangle$ como se menciona previamente. Entonces $x + y$ o $y^4 - y^3 - 1$ en I tienen términos principales que generan a $LT(I)$, por el Teorema 5.1.4. $\{x + y; y^4 - y^3 - 1\}$ da una base Gröbner minimal para I,

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

De hecho esta descripción es mucho más simple que:

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

Ejemplo 3.3.3. Elijamos el orden lexicográfico $y > x$ sobre $F[x, y]$ y consideremos el ideal I del ejemplo previo. En este caso $S(f_1, f_2)$ produce un resto $r_1 = -x - y$; entonces $S(f_1, r_1)$ produce un resto $r_2 = -x^4 - x^3 + 1$, entonces todos los restos son cero "0çon respecto a la base Gröbner

$$\{x^3y - xy^2 + 1; x^2y^2 - y^3 - 1; -x - y; -x^4 - x^3 + 1\}$$

aquí

$$LT(I) = \langle LT(f_1), LT(f_2), LT(r_1), LT(r_2)\rangle = \langle -xy^2, -y^3, -y, -x^4\rangle = \langle y, x^4\rangle$$

como se mencionó previamente, y $\{x + y, x^4 + x^3 - 1\}$ da una base Gröbner minimal para I con respecto a este orden:

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

una descripción más simple y diferente de I.

★ En el ejemplo 3.1.10. previo es fácil de verificar que:

$$\{x + y + y^4 - y^3 - 1, y^4 - y^3 - 1\} = \{r_1 + r_2, r_2\}$$

es otra vez una base Gröbner minimal para I. Esto nos indica que aún con un orden monomial fijado en $F[x_1, ..., x_n]$ una base de Gröbner minimal para un ideal I no es única. Podemos obtener una propiedad importante de unicidad fortaleciendo la condición de divisibilidad por términos principales de la base.

Definición 3.3.4. Fije un orden monomial sobre $F[x_1, .., x_n]$. Una base Gröbner $\{g_1, .., g_m\}$ para el ideal no cero I en $F[x_1, ..., x_n]$ es llamada base Gröbner reducida si:

- Cada g_i tiene término principal mónico, es decir; $LT(g_i)$ es mónico para $i = 1, 2, ..., m$
- Ningún término en g_j es divisible por $LT(g_i)$ para $j \neq i$

Note que una base Gröbner reducida es, en particular una base Gröbner minimal. Si $G = \{g_1, ..., g_m\}$ es una base Gröbner minimal para I, entonces el término principal $LT(g_i)$ para cualquier $j \neq i$. Como un resultado, si usamos la división de polinomios para dividir g_j por los otros polinomios en G obtenemos un resto g'_j en el ideal I con el mismo término principal que g_j (con resto g'_j no depende del orden de los polinomios usados en la división por el inciso (2) del Teorema 3.2.4.) por la proposición 3.1.4. reemplazando g_j por g'_j en G otra vez da una base de Gröbner minimal para I, y en esta base ningún término de g'_j es divisible por $LT(g_i)$ para cualquier $i \neq j$. Reemplazando cada elemento en G por su resto después de la división por los otros elementos en G obtendremos una base Gröbner reducida para I. La importancia de las bases Gröbner reducidas es que son únicas (para un orden monomial dado), como el resultado siguiente prueba.

Observación 3.3.5. Fije un orden monomial sobre $F[x_1, ..., x_n]$.

- Pruebe que $\{g_1, ..., g_m\}$ es una base Gröbner minimal para el ideal I de $F[x_1, ..., x_n]$ si y solo si $\{LT(g_1), ..., LT(g_m)\}$ es un conjunto generador minimal para $LT(I)$.
- Pruebe que los términos principales de una base Gröbner minimal para el ideal I están determinados de modo único y el número de elementos en cualesquiera dos bases Gröbner minimales para I es el mismo.

Teorema 3.3.6. *Fije un orden monomial sobre $F[x_1, ..., x_n]$. Entonces existe una única base Gröbner reducida para cada ideal no cero I de $F[x_1, ..., x_n]$.*

Demostración.- Utilizando la observación 3.3.4., dos bases reducidas tienen el mismo número de elementos y los mismos términos principales pues las bases reducidas son también bases minimales. Si $G = \{g_1, ..., g_m\}$ y $G' = \{g'_1, ..., g'_m\}$ son dos bases reducidas para el mismo ideal no cero I, entonces después de un posible reacomodo podemos asumir $LT(g_i) = LT(g'_i) = h_i$ para $i = 1, 2, ..., m$. Para cualquier i fijo, considere el polinomio $f_i = g_i - g'_i$. Si f_i no es cero, entonces como $f_i \in I$ su término principal debe ser divisible

por algún h_j. Por definición de un base Gröbner reducida, h_j para $j \neq i$ no divide a cada uno de los términos en g_i o en g_i' por lo tanto no divide a $LT(f_i)$. Pero h_i no divide a $LT(f_i)$ pues todos los términos en f_i tienen multigrado estrictamente más pequeño, esto obliga a que $f_i = 0$ es decir $g_i = g_i'$ para cada i, así $G = G'$. ■

Una aplicación de la unicidad de las bases Gröbner reducida es un método computacional para determinar cuando dos ideales en un anillo de polinomios son iguales.

Corolario 3.3.7. *Sean I, J dos ideales en $F[x_1, ..., x_n]$. Entonces $I = J$ si y solo si I, J tienen la misma base Gröbner reducida con respecto a cualquier orden monomial fijado sobre $F[x_1, ..., x_n]$.*

Ejemplo 3.3.8. Considere el ideal $I = \langle h_1, h_2, h_3\rangle$ con $h_1 = x^2+xy^5+y^4$, $h_2 = xy^6-xy^3+y^5-y^2$, y $h_3 = xy^5-xy^2$ en $F[x, y]$. Usando el orden lexicográfico $x > y$ encontramos;

$$S(h_1, h_2) \equiv S(h_1, h_3) \equiv 0 \mod\{h_1, h_2, h_3\} \quad y$$

$$S(h_2, h_3) \equiv y^5 - y^2 \mod\{h_1, h_2, h_3\}$$

Si hacemos $h_4 = y^5 - y^2$ hallamos;

$$S(h_i, h_j) \equiv 0 \mod\{h_1, h_2, h_3, h_4\}$$

para $1 \leq i < j \leq 4$ así; el conjunto $\{h_1, h_2, h_3, h_4\}$ es una base Gröbner para I. Los términos principales de esta base son:x^2, xy^6, xy^5, y^5 como y^5 divide a xy^6 y a xy^5, podemos eliminar el segundo y tercero generadores para obtener una base Gröbner minimal $\{h_1, h_4\} = \{x^2 + xy^5 + y^4; y^5 - y^2\}$ para I. El segundo término en el primer generador es divisible por el término principal y^5 del segundo generador así esta no es una base Gröbner reducida. Reemplazando $x^2 + xy^5 + y^4$ por su resto $x^2 + xy^2 + y^4$ después de la división por los otros polinomios en la base (que en este caso es solo el

polinomio y^5-y^2) hemos quedado con la base Gröbner reducida $\{x^2+xy^2+y^4; y^5-y^2\}$ para I.

Ahora consideremos el ideal $J = \langle h_1, h_2, h_3\rangle$ con $h_1 = xy^3 + y^3 + 1$, $h_2 = x^3y - x^3 + 1$ y $h_3 = x + y$ en $F[x, y]$. Usando el orden lexicográfico $x > y$ encontramos;

$$S(h_1, h_2) \equiv 0 \quad mod\{h_1, h_2, h_3\} \quad y$$

$$S(h_1, h_3) \equiv y^4 - y^3 - 1 \quad mod\{h_1, h_2, h_3\}$$

haciendo $h_4 = y^4 - y^3 - 1$ hallamos;

$$S(h_i, h_j) \equiv 0 \quad mod\{h_1, h_2, h_3, h_4\}$$

para $1 \leq i < j \leq 4$ así; el conjunto $\{h_1, h_2, h_3, h_4\}$ es una base Gröbner para J. Los términos principales de esta base son: xy^3, x^3y, x, y^4 así $\{x + y, y^4 - y^3 - 1\}$ es una base Gröbner minimal para J en este caso ninguno de los términos en $y^4 - y^3 - 1$ son divisibles por el término principal de $x + y$ y ninguno de los términos principales en $x+y$ son divisibles por el término principal en $y^4 - y^3 - 1$ así $\{x+y, y^4 - y^3 - 1\}$es la base Gröbner reducida para J; pero esta es la base para el ideal I del ejemplo anterior, por lo tanto por el criterio de Buchberger del Teorema 4.2.11. estos dos ideales son iguales:

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

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

Capítulo 4

Aplicaciones de las bases de Gröbner

4.1. Bases Gröbner- Resolución de Ecuaciones Algebraicas: Eliminación

La teoría de las Bases de Gröbner es muy útil para resolver explícitamente sistema de ecuaciones algebraicas y es esa la base por la cual programas de algebra para la computadora intentan resolver sistema de ecuaciones. Suponga que $S = \{f_1, ..., f_m\}$ es una colección de polinomios en n variables $x_1, ..., x_n$ y que estamos intentando encontrar las soluciones del sistema de ecuaciones $f_1 = 0$; $f_2 = 0$; ...; $f_m = 0$,es decir el conjunto común de ceros de los polinomios en S.

Si $(a_1, ..., a_n)$ es cualquier solución a este sistema, entonces cada elemento del ideal I generado por S también satisface $f(a_1, ..., a_n) = 0$. Además es un ejercicio fácil ver que si $S' = \{g_1, ..., g_s\}$ es cualquier conjunto de generadores para el ideal I, entonces el conjunto

de soluciones al sistema $g_1 = 0$, $g_2 = 0$,...., $g_s = 0$ es el mismo que el conjunto solución original.

En la situación donde $f_1, ..., f_m$ son polinomios lineales, una solución al sistema de ecuaciones puede ser obtenida eliminando sucesivamente las variables $x_1, ..., x_n$ por medios elementales usando combinaciones lineales de las ecuaciones originales para eliminar la variable x_1, luego usar estas ecuaciones originales para eliminar x_2, así sucesivamente produciendo un sistema de ecuaciones que puede ser fácilmente resuelto (esto es "Gauss-Jordan elimination.[en] algebra lineal).

El encontrar ecuaciones que provenían del sistema de ecuaciones en S, es decir; encontrar elementos del ideal I que no involucren algunas de las variables, es referido como la teoría de eliminación. Los polinomios en I que no involucran las variables $x_1, ..., x_n$ esto es $I \cap F[x_{i+1}, ..., x_n]$ y tiene un nombre.

Definición 4.1.1. Si I es un ideal en $F[x_1, ..., x_n]$ entonces $I_i = I \cap F[x_{i+1}, ..., x_n]$ es llamado el i-ésimo ideal eliminación de I con respecto al orden $x_1 > .... > x_n$.

El éxito de utilizar eliminación para resolver un sistema de ecuaciones depende de la capacidad para determinar los ideales eliminación. La siguiente proposición fundamental prueba que si el orden lexicográfico $x_1 > .... > x_n$ es usado para computar una base Gröbner para I, entonces los elementos en la base resultante que no involucran las variables $x_1, ..., x_i$ no solo determinan el i-ésimo ideal eliminación, de hecho dan una base Gröbner para el i-ésimo ideal eliminación de I.

Proposición 4.1.2.(Eliminación) *Suponga que $G = \{g_1, ..., g_m\}$ es una base Gröbner para el ideal no cero I de $F[x_1, ..., x_n]$ con respecto al orden monomial lexicográfico $x_1 > .... > x_n$. Entonces $G \cap F[x_{i+1}, ..., x_n]$ es una base Gröbner del i-ésimo ideal eliminación $I_i = I \cap F[x_{i+1}, ..., x_n]$ de I. En particular $I \cap F[x_{i+1}, ..., x_n] = 0$ si y solo si $G \cap F[x_{i+1}, ..., x_n] = \emptyset$.*

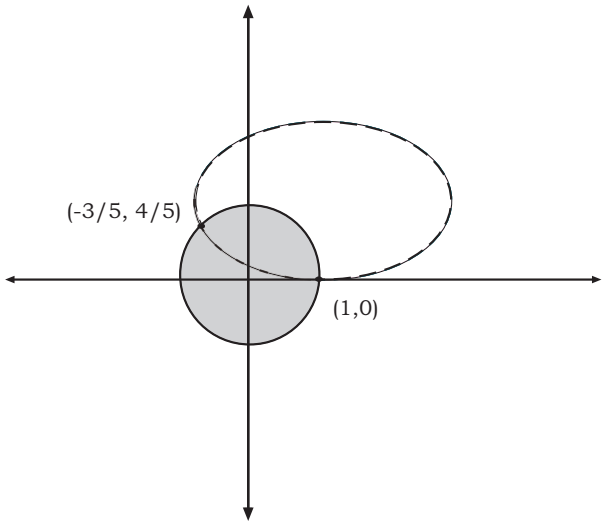
Demostración.- Sea denotado $G_i = G \cap F[x_{i+1}, ..., x_n]$, entonces $G_i \subseteq I_i$ así por la Proposición 4.2.6., para ver que G_i es una base Gröbner de I_i es suficiente ver que $LT(G_i)$, los términos principales de los elementos en G_i, generan $LT(I_i)$ como un ideal en $F[x_{i+1}, ..., x_n]$. Ciertamente $\langle LT(G)_i \rangle \subseteq LT(I_i)$ como ideales en $F[x_{i+1}, ..., x_n]$. Para probar la otra inclusión tómese $f \in I_i$, entonces $f \in I$ y como G es una base Gröbner para I tenemos:

$$LT(f) = a_1(x_1, ..., x_n)LT(g_1) + ... + a_m(x_1, ..., x_n)LT(g_m)$$

para algunos polinomios $a_1, ..., a_n \in F[x_1, ..., x_n]$. Escribiendo cada polinomio a_i como una suma de términos monomio vemos que $LT(f)$ es una suma de términos monomio de la forma $ax^{s_1}x^{s_2} \cdots x^{s_n}LT(g_i)$, como $LT(f)$ involucra solo las variables $x_{i+1}, ..., x_n$ la suma de esos términos conteniendo cualquiera de las variables $x_1, ..., x_i$ debe ser cero "0", así $LT(f)$ es también la suma de aquellos términos monomio que solo involucran $x_{i+1}, ..., x_n$. En consecuencia $LT(f)$ puede ser escrito como una $F[x_{i+1}, ..., x_n]$ - combinación lineal de algunos términos monomio $LT(g_t)$ donde $LT(g_t)$ no involucra las variables $x_1, ..., x_i$; pero por la elección del orden, si $LT(g_t)$ no involucra a $x_1, ..., x_i$, entonces ninguno de sus otros términos lo hace, es decir; $g_t \in G_i$, por lo tanto $LT(f)$ puede ser escrito como una combinación $F[x_{i+1}, ..., x_n]$ - lineal de elementos de $LT(G_i)$ esto significa que $f \in G_i$ lo que completa la prueba. ■

Note que una base Gröbner puede ser usada para eliminar cualquier variable usando simplemente un orden monomial apropiado.

Ejemplo 4.1.3. la elipse $2x^2 + 2xy + y^2 - 2x - 2y = 0$ intersecta el círculo $x^2 + y^2 = 1$ en dos puntos. Para encontrarlos computamos una base Gröbner para el ideal $I = \langle 2x^2 + 2xy + y^2 - 2x - 2y, x^2 + y^2 - 1 \rangle \subset \mathbb{R}[x, y]$ usando el orden monomial lexicográfico $x > y$ para eliminar x, obteniendo $g_1 = 2x + y^2 + 5y^3 - 2$ y $g_2 = 5y^4 - 4y^3$, hacemos $g_i = 0$ para cada $i = 1, 2$ primero si $g_2 = 0$ entonces $5y^4 = 4y^3$ de ahí que $y = 0$ o $y = 4/5$ para luego sustituir estos valores en $g_1 = 0$ resolviendo para x encontramos que los dos puntos de intersección son (1, 0) y (-3/5, 4/5).



Ejemplo 4.1.4. En el previo ejemplo las soluciones también podrían haber sido encontradas por medio elementales. Considere ahora las soluciones en $\mathbb{C}$ al sistema de dos ecuaciones $f_1 = x^3 - 2xy + y^3$ y $f_2 = x^5 - 2x^2y^2 + y^5$ calculamos una base Gröbner para el ideal generado por f_1 y f_2 con respecto al orden monomial lexicográfico $x > y$ obtenemos la base por cálculos;

$$\begin{aligned} g_1 &= x^3 - 2xy + y^3 \\ g_2 &= 200xy^2 + 193y^9 + 158y^8 - 45y^7 - 456y^6 + 50y^5 - 100y^4 \\ g_3 &= y^{10} - y^8 - 2y^7 + 2y^6 \end{aligned}$$

Cualquier solución a nuestras ecuaciones originales tendría que satisfacer $g_1 = g_2 = g_3 = 0$ como $g_3 = y^6(y-2)^2(y^2+2y+2)$ tenemos $y = 0$, $y = 1$ o $y = -1 \pm i$. como $g_1(x, 0) = x^3$ y $g_2(x, 0) = 0$ vemos que (0,0) es la única solución con $y = 0$, pero como $g_1(x, 1) = x^3 - 2x + 1$ y $g_2(x, 1) = 200(x - 1)$ tiene solo $x = 1$ como un cero común, la única solución con $y = 1$ es (1,1), finalmente $g_1(x, -1 \pm i) = x^3 + 2(\mp 2i)x + 2(\pm 2i)$; $g_2(x, -1 \pm i) = -400i(x + 1 \pm i)$ y una verificación rápida prueba que $x = -1 \mp i$ es cero común cuando $y = -1 \pm i$ respectivamente, por lo tanto hay cuatro soluciones al par de ecuaciones originales, a saber; $(x, y) = (0, 0)$, $(1, 1)$, $(-1 + i, -1 - i)$ o $(-1 - i, -1 + i)$.

Como los ejemplos previos muestran, el estudio de soluciones a sistemas de ecuaciones

polinomiales $f_1 = 0, f_2 = 0, ..., f_m = 0$ está íntimamente relacionado al estudio del ideal $I = \langle f_1, f_2, ..., f_m\rangle$ que dichos polinomios generan en $F[x_1, ..., x_n]$. Esta conexión fundamental es el punto de inicio para la importante y activa rama de la matemática llamada "Geometría Algebraica".

Las operaciones (conjuntistas) básicas de suma, producto e intersección de ideales en el anillo de polinomios son definidos por: Dados los ideales $I = \langle f_1, ..., f_m\rangle$ y $J = \langle h_1, ..., h_t\rangle$ en $F[x_1, ..., x_n]$ se tiene;

$$I + J = \langle f_1, ..., f_m, h_1, ..., h_t\rangle$$
$$IJ = \langle f_1h_1, ..., f_mh_t\rangle$$

La proposición siguiente muestra como calcular la intersección de dos ideales cualesquiera.

Proposición 4.1.5. *Si I y J son dos ideales cualesquiera en $F[x_1, ..., x_n]$ entonces $tI + (1-t)J$ es un ideal en $F[t, x_1, ..., x_n]$ y $I \cap J = \langle tI + (1-t)J\rangle \cap F[x_1, ..., x_n]$. en particular, $I \cap J$ es el primer ideal eliminación de $tI + (1-t)J$ con respecto al orden $t > x_1 > .... > x_n$.*

Demostración.- Primeramente tI y $(1-t)J$ son ideales en el anillo de polinomios en n-variables, así su suma $tI + (1-t)J$ es un ideal en $F[t, x_1, ..., x_n]$. Si $f \in I \cap J$, entonces $f = tf + (1-t)f$ lo cual prueba que $I \cap J \subseteq \langle tI + (1-t)J\rangle \cap F[x_1, ..., x_n]$.

Recíprocamente, supongamos que $f = tf_1 + (1-t)f_2$ es un elemento de $F[x_1, ..., x_n]$, donde $f_1 \in I$ y $f_2 \in J$, entonces $t(f_1 - f_2) = f - f_2 \in F[x_1, ..., x_n]$ lo cual prueba que $f_1 - f_2 = 0$ y $f = f_2$ así $f = f_1 = f_2 \in I \cap J$, como $I \cap J = \langle tI + (1-t)J\rangle \cap F[x_1, ..., x_n]$, $I \cap J$ es el primer ideal de eliminación de $tI + (1-t)J$ con respecto al orden $t > x_1 > .... > x_n$. Tenemos $tI + (1-t)J = \langle tf_1, ..., tf_m, (1-t)h_1, ..., (1-t)h_t\rangle$ por la proposición 4.1.2.(Eliminación) los elementos no involucran t en una base Gröbner para este ideal en $F[t, x_1, ..., x_n]$ calculada para el orden monomial lexicográfico $t > x_1 > .... > x_n$ lo cual da una base Gröbner para el ideal $I \cap J$ en $F[x_1, ..., x_n]$. ■

Ejemplo 4.1.6. Sea $I = \langle x^2, xy, y^2 \rangle$ y sea $J = \langle x \rangle$, para el orden monomial lexicográfico $t > x > y$ y la base Gröbner reducida para $tI + (1-t)J$ en $F[t, x, y]$ es $\{tx - x, ty^2, x^2, xy\}$ y así $I \cap J = \langle x^2, xy \rangle$. ★.

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

Capítulo 5

Conclusiones

► En el estudio de las bases de Gröbner se tiene dos formas de ver: la matemática y la computacional, construyendo un conjunto manejable, en el sentido de que no se puede visualizarlo fácilmente ya que el cálculo de las bases de Gröbner es bastante costoso debido a la resolución de polinomios multivariados (sobre un cuerpo finito) donde Bruno Buchberger introdujo un criterio para eliminar términos redundantes dentro del algoritmo; la base de esta optimización es saber qué se debe agregar al conjunto de generadores del ideal en cuestión para obtener de ahí una base Gröbner, estos son un subconjunto(restos) de sizigias particulares que dan una optimización del algoritmo.

Además de obtener las cuestiones y operaciones que son:

- Decidir si un polinomio pertenece a un ideal I (*ideal membership*)
- Decidir cuándo dos ideales son iguales

- Calcular la suma de ideales
- Calcular el producto de ideales
- Calcular la intersección de ideales
- Eliminar variables

Las cuales son conocidos para aquellos que posean unas nociones básicas sobre anillos pero vistas desde otro punto de vista.

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

Apéndice A

Anexos

A.1. Teoremas Básicos en el Anillo de Polinomios F[x]

Ahora consideramos con más cuidado la situación donde el anillo de coeficientes es un campo F, podemos definir una norma sobre $F[x]$ haciendo $N(f(x)) =$ grado de$f(x)$ (donde N(0)=0). Del algebra elemental sabemos que podemos dividir un polinomio con coeficientes racionales por otro polinomio no cero con coeficientes racionales para obtener un cociente y un resto. Lo mismo es verdad sobre cualquier campo; por conveniencia denotaremos el grado de $f(x)$ como $deg(f)$.

Teorema A.1.1..- *Sea F un campo. El anillo de polinomios $F[x]$ es un dominio euclidiano, específicamente si $f(x)$ y $g(x)$ son dos polinomios en $F[x]$ con $g(x)$ distinto de cero, entonces existen $q(x)$ y $r(x)$ únicos en $F[x]$ tal que: $f(x) = g(x)q(x) + r(x)$ con $r(x) = 0$*

o $deg(r) < deg(g)$.

Prueba.- ***(Demostración para la Existencia)*** Sean $f(x)$ y $g(x)$ polinomios tal que $g(x) \neq 0$ en $F[x]$; Si $f(x) = 0$ entonces tómese $q(x) = r(x) = 0$ tal que: $f(x) = g(x)q(x) + r(x)$ con $r(x) = 0$. $\square$

Ahora si $f(x) \neq 0$ entonces tiene grado, es decir $deg(f) = n$ aplicaremos el segundo principio de inducción sobre n la existencia de $q(x)$ y $r(x)$; como $g(x) \neq 0$ entonces tiene grado sea $deg(g) = m$ para esto consideramos dos casos:

(CASO I) Si $deg(f) = n < m = deg(g)$ tómese $q(x) = 0$ y $r(x) = f(x)$ tal que $f(x) = g(x)q(x) + r(x)$ con $deg(r) = deg(f) < deg(g)$, es decir; con $deg(r) < deg(g)$. $\square$

(CASO II) Si $deg(f) = n \geq m = deg(g)$ donde:

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad y \qquad g(x) = \sum_{i=0}^{m} b_i x^i$$

entonces $a_n \neq 0$ y $b_m \neq 0$ como estamos en un campo $\exists\ b_m^{-1}$ entonces $\exists\ a_n b_m^{-1}$ que esta en F, como $n - m \geq 0$ entonces existe el monomio $x^{n-m} \in F[x]$, implica que $\exists\ a_n b_m^{-1} x^{n-m}$ luego de ahí que: $(\frac{a_n}{b_m})x^{n-m}g(x) \in F[x]$, es decir; $f(x) - (\frac{a_n}{b_m})x^{n-m}g(x) \in F[x]$ que tiene grado menor de $deg(f)$ sea el polinomio;

$$f'(x) = f(x) - (\frac{a_n}{b_m})x^{n-m}g(x) \qquad (\bigstar)$$

que hemos hecho simplemente arreglos para sustraer el término principal de $f(x)$ note que el polinomio $f'(x)$ está bien definido ya que los coeficientes son tomados en un campo.

Hipótesis de inducción: $\exists\ q'(x)$ y $r(x)$ tal que, $f'(x) = g(x)q'(x) + r(x)$ con $r(x) = 0$ o $deg(r) < deg(g)$.

Tesis de inducción: $\exists\ q(x)$ y $r(x)$ tal que, $f(x) = g(x)q(x) + r(x)$ con $r(x) = 0$ o $deg(r) < deg(g)$.

En efecto, por $(\bigstar)$ y la hipótesis tenemos:

$$f(x) - (\frac{a_n}{b_m})x^{n-m}g(x) = q'(x)g(x) + r(x)$$

en consecuencia tenemos que $\exists\, q(x) = q'(x) + (\frac{a_n}{b_m})x^{n-m}$ tenemos así $f(x) = g(x)q(x) + r(x)$ con $r(x) = 0$ o $deg(r) < deg(g)$ completando la inducción. ■

(Demostración para la unicidad) Sean:$q_1(x), r_1(x), q_2(x), r_2(x)$ que satisfacen las condiciones del teorema;

$$f(x) = g(x)q_1(x) + r_1(x) \qquad y \qquad f(x) = g(x)q_2(x) + r_2(x)$$

realizando la diferencia de las dos igualdades se tiene:

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x) \qquad (\bigstar)(\bigstar)$$

Supongamos que $q_1(x) \neq q_2(x)$, entonces al estar en un Dominio integral $deg[g(q_1 - q_2)] = deg(g) + deg(r_2 - r_1)$ como $deg(r_2 - r_1) \geq 0$ implica que $deg(g) \leq deg(r_2 - r_1) + deg(g)$ y $deg(r_2 - r_1) < deg(g)$ de estas dos relaciones se da que: $deg(g) \leq deg(r_2 - r_1) < deg(g)$ llegando a una contradicción. Entonces $q_1(x) - q_2(x) = 0$ es decir; $q_1(x) = q_2(x)$ de ahí que $r_1(x) = r_2(x)$ completando la prueba.■

A.2. Propiedades en el Anillo de Polinomios K[x]

Primeramente, por conveniencia el anillo K siempre será un anillo conmutativo con identidad $1 \neq 0$. El anillo de polinomios $K[x]$ en la indeterminada x de una sola variable con coeficientes en K es el conjunto de todas las sumas formales: $a_0 + a_1x^1 + ... + a_{n-1}x^{n-1} + a_nx^n = \sum_{i=0}^{n} a_ix^i$ con $n \geq 0$ y cada $a_i \in K$. Si $a_n \neq 0$ entonces el polinomio es de grado n, a_nx^n es el termino principal y a_n es el coeficiente principal (donde el coeficiente principal del polinomio cero es definido como 0). El polinomio es *mónico* si $a_n = 1$. La adición de polinomios es çomponente a componente":

$$\sum_{i=0}^{n} a_ix^i + \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{n} (a_i + b_i)x^i$$

Notese que aquí tanto a_n como b_n pueden ser ceros para que la adición de polinomios de grados diferentes esté definida. La multiplicación es llevando a cabo definiendo primero

$(ax^i)(bx^j) = abx^{i+j}$, extendiendo entonces a todos los polinomios por medio de las leyes distributivas de modo que en general es:

$$\left(\sum_{i=0}^{n} a_i x^i\right) \times \left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k$$

En esta forma $K[x]$ es un anillo conmutativo con identidad (la identidad 1 de K) en el cual identificamos K con el subanillo de polinomios constantes.
Notemos que si K es un *dominio integral* entonces el termino principal de un producto de polinomios es el producto de los términos principales de los factores.

Teorema A.2.1..- *Sea K un dominio integral, entonces:*

1. *$deg(p(x)q(x)) = deg(p(x)) + deg(q(x))$ si $p(x)$, $q(x)$ son distintos de cero.*
2. *Las unidades de $K[x]$ son precisamente las unidades de K.*
3. *$K[x]$ es un dominio integral*

Recuerde que si K es un dominio integral, el campo cociente de $K[x]$ consiste en todos los polinomios cocientes $\frac{p(x)}{q(x)}$ donde $q(x)$ no es el polinomio cero (se llama el campo de funciones racionales en x con coeficientes en K). El resultado siguiente describe una relación entre los ideales de K y los de $K[x]$.

Teorema A.2.2..- *Sea I un ideal del anillo K y $(I) = I[x]$ denota el ideal de $K[x]$ generado por I (el conjunto de polinomios con coeficiente en I). Entonces:*

$$K[x]/(I) \cong (K/I)[x]$$

En particular, si I es un ideal primo de K, entonces (I) es un ideal de $K[x]$.

Demostración.- Sea la función natural $\varphi : K[x] \to (K/I)[x]$ dada por reducción de cada uno de los coeficientes de un polinomio modulo I. La definición de adición y multiplicación en estos dos anillos prueba que φ es un homomorfismo de anillos. El kernel es precisamente el conjunto de polinomios, cada uno de cuyos coeficientes es un elemento de I, es decir

$ker\varphi = I[x] = (I)$, probando así la primera parte de la proposición, la ultima afirmación se sigue de la proposición 1, pues si I es un ideal primo en K, entonces K/I es un dominio integral, por tanto también $(K/I)[x]$ es un dominio integral. Esto prueba que si I es un ideal primo de K; entonces (I) es un ideal primo de $K[x]$. ■

Ejemplo A.2.3. Sea $K = \mathbb{Z}$ y considere el ideal $n\mathbb{Z}$ de $\mathbb{Z}$, entonces el homomorfismo de la proposición 2 puede ser escrito como:

$$\mathbb{Z}[x]/n\mathbb{Z}[x] \cong (\mathbb{Z}/n\mathbb{Z})[x]$$

y la función proyección natural de $\mathbb{Z}[x]$ a $(\mathbb{Z}/n\mathbb{Z})[x]$ que reduce los coeficientes modulo n, es un homomorfismo de anillos. Si n es compuesto, entonces el anillo cociente no es un dominio integral. No obstante si n es un primo p, entonces $\mathbb{Z}/p\mathbb{Z}$ es un campo y así es $\mathbb{Z}/p\mathbb{Z}[x]$ es un dominio integral(de hecho un dominio euclidiano).

A.3. Algoritmo de la División Generalizada

Fije un orden monomial sobre $F[x_1, x_2, ..., x_n]$ y supongamos que $g_1, ..., g_m$ es un conjunto de polinomios distintos de cero en $F[x_1, x_2, ..., x_n]$. Si f es cualquier polinomio en $F[x_1, x_2, ..., x_n]$, comencemos con un conjunto de cocientes $q_1, ..., q_m$ y un resto r inicialmente todos iguales a cero y sucesivamente verificamos si el término principal del dividendo f es divisible por los términos principales de los divisores $g_1, ..., g_m$ en ese orden. Entonces:

(i) Si $LT(f)$ es divisible por $LT(g_i)$, digamos esto como: $LT(f) = a_i LT(g_i)$, sume a_i al cociente q_i, reemplazamos f por el dividendo $f - a_i g_i$ (un polinomio con término principal con orden más bajo) y repetimos este proceso consecuentemente.

(ii) Si el término principal del dividendo f no es divisible por cualquiera de los términos principales de $LT(g_1), ..., LT(g_m)$, adicionamos el término principal de f al resto r, reemplace f por el dividendo $f - LT(f)$ (es decir; quitamos el término principal de f) para luego siguiendo el proceso de división.

El proceso termina cuando el dividendo es cero y da por resultado un conjunto de cocientes $g_1, ..., g_m$ y un resto r con:

$$f = g_1q_1 + ... + g_mq_m + r$$

donde cada $MGRAD(g_iq_i) \leq MGRAD(f)$ y resto r tiene la propiedad que cada término distinto de cero en r no es divisible por cualquiera de los términos principales de $LT(g_1), ..., LT(g_m)$ (pues solo los términos con esta propiedad son adicionados a r en (ii)).

► Para los siguientes ejemplos fijamos un orden lexicográfico $x > y$ en $F[x, y]$.

Ejemplo A.3.1. Suponga que $f = 5x^3y^3 + 10x^2y^4$ y $g = xy^4$ donde $LT(f) = 5x^3y^3$ lo cual no es divisible por g, así $5x^3y^3$ es adicionado al resto r (ahora $r = 5x^3y^3$) y f es reemplazado por $f - LT(f) = xy^4$ y comenzamos de nuevo, como $10x^2y^4$ es divisible por $LT(g) = xy^4$, con cociente $a = 10x$; adicionamos $10x$ al cociente q (así $q = 10x$)y reemplazamos $10x^2y^4$ por $10x^2y^4 - a.LT(g) = 0$, aquí termina el proceso cuyo resultado es $q = 10x$ y resto $r = 5x^3y^3$ tal que:

$$f = gq + r = (xy^4)(10x) + 5x^3y^3$$

Ejemplo A.3.2. Sea $f = x^2 + x - y^2 + y$ y sean $g_1 = xy + 1$ y $g_2 = x + y$.

Iteracción 1 Como $LT(f) = x^2$ que no es divisible por $LT(g_1)$ pero si por el $LT(g_2)$ así $q_2 = x$ y el dividendo f es reemplazado por $f - xg_2 = -xy + x - y^2 + y$.

Iteracción 2 Como $LT(f - xg_2) = -xy$ que es divisible por $LT(g_1)$ con cociente $q_1 = -1$ y el dividendo es reemplazado por $f - xg_2 - q_1g_1 = x - y^2 + y + 1$.

Iteracción 3 Ahora $LT(f-xg_2-q_1g_1) = x$ que no es divisible por $LT(g_2)$ pero si por el $LT(g_1)$ así 1 es adicionado a q_2 ahora tenemos $q_2 = x+1$ y el dividendo se convierte en $(x-y^2+y+1)-(1)(x+y) = -y^2+1$. el término principal de $LT(-y^2+1) = -y^2$ que no es divisible por $LT(g_1)$ pero tampoco por $LT(g_2)$, así que $-y^2$es adicionado al resto r y el dividendo se convierte simplemente en 1. Finalizando 1 no es divisible por $LT(g_1)$ ni por $LT(g_2)$, así es adicionado al resto r ahora termina el proceso de

dividir lo que queda es $r = -y^2 + 1$. Entonces:

$f = x^2 + x - y^2 + y = (xy + 1)(-1) + (x + y)(x + 1) + (-y^2 + 1) = g_1q_1 + g_2q_2 + r$

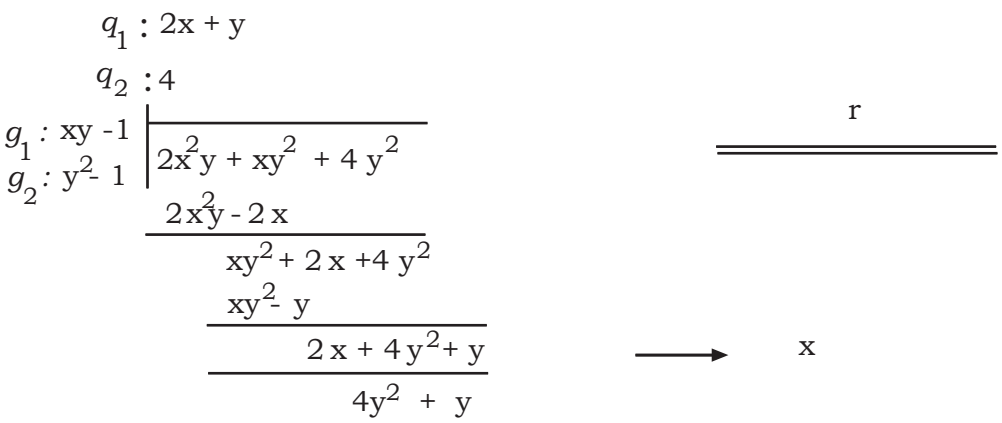
Ejemplo A.3.3. Tomando el mismo ejemplo anterior $f = x^2 + x - y^2 + y$ tan solamente intercambiando los divisores $g_1 = x + y$ y $g_2 = xy + 1$ el calculo fácil nos da $q_1 = x - y + 1$, $q_2 = 0$ y $r = 0$ donde:

$f = x^2 + x - y^2 + y = (x + y)(x - y + 1) + (xy + 1)(0) + 0 = g_1q_1 + g_2q_2 + r$ probando que los cocientes q_i y el resto r no son en general únicos, ya que dependen del orden de los divisores $g_1, ..., g_m$

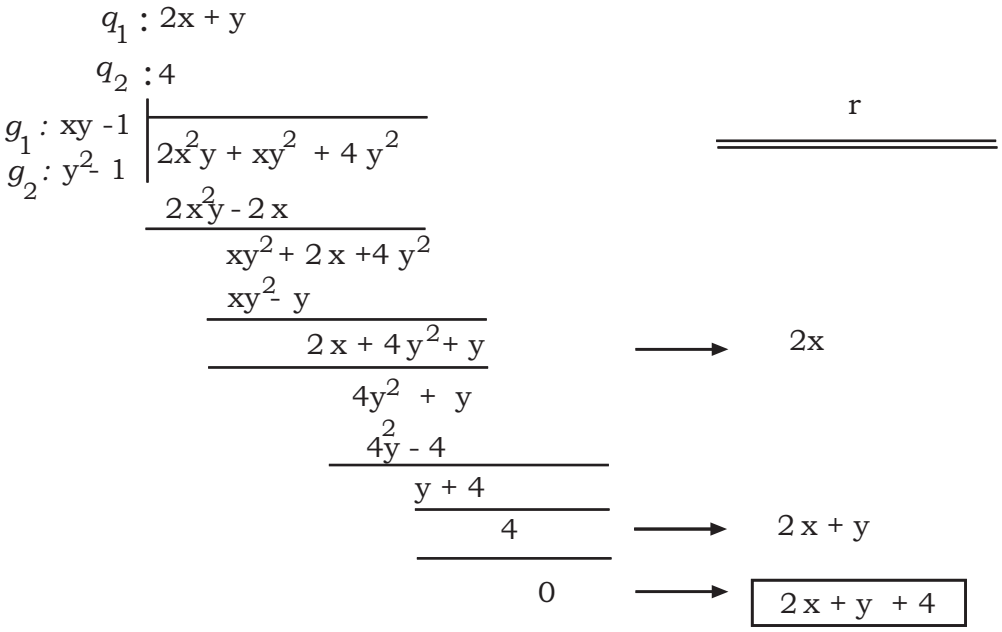
Ejemplo A.3.4. Para poder visualizarlo muy bien el algoritmo de la división veamos este ejemplo donde utilizamos el orden lexicográfico $x > y$ en $F[x, y]$ y además consideremos los polinomios $f = 2x^2y + xy^2 + 4y^2$ que lo dividiremos por: $g_1 = xy - 1$ y $g_2 = y^2 - 1$ entonces se obtendrán cocientes $q_1 = 2x + y$ y $q_2 = 4$ y un resto $r = 2x + y + 4$ (no necesariamente único) de la siguiente forma:

$$
\begin{array}{rl}
 & q_1 : 2x + y \\
 & q_2 : 4 \\
g_1 : xy - 1 \\
g_2 : y^2 - 1 & \left| \overline{2x^2y + xy^2 + 4y^2} \right. \\
 & \underline{2x^2y - 2x} \\
 & \quad xy^2 + 2x + 4y^2 \\
 & \quad \underline{xy^2 - y} \\
 & \quad\quad 2x + 4y^2 + y
\end{array}
$$

Puesto que $LT(g_1) = xy$ ni $LT(g_2) = y^2$ no dividen a $LT(2x + 4y^2 + y) = 2x$ ya no podemos seguir dividiendo; pero observe que no podemos escribir a $2x + 4y^2 + y$ como residuo, por que $LT(g_2) = y^2$ divide a $4y^2$, así es que si mandamos a $2x$ al residuo podemos seguir dividiendo. Para implementar esta idea creamos la columna r a la derecha de la división en donde pondremos los términos que pertenezcan al residuo. Al polinomio bajo el radical lo llamaremos dividendo intermedio, continuamos dividiendo hasta que el dividendo intermedio sea cero.



Si podemos dividir entre $LT(g_1) = xy$ o $LT(g_2) = y^2$ continuamos con la división usual, y si ninguno de ellos lo divide, entonces lo mandamos al residuo el término inicial del dividendo intermedio; presentamos a continuación el resto de la división finalizada.



Observe que el residuo es la suma de monomios $r = 2x + y + 4$, de los cuales ninguno es divisible entre $LT(g_1) = xy$ ni $LT(g_2) = y^2$

Además el calculo en el Ejemplo 3.3. muestra que f es un elemento de $I = \langle x + y, xy + 1\rangle$ pues el residuo obtenido en este caso fue 0 de hecho f un múltiplo del primer generador in-

dica el Teorema 4.1.3 y Ejemplo 3.4. muestra de manera similar que $f \in I = \langle xy-1, y^2-1\rangle$ si y solo si $r = o$; si utilizamos una *base Gröbner* para el ideal I, entonces estas dificultades no aparecen, pues obtenemos un resto único, lo cual puede ser usado para determinar si un polinomio f es un elemento del ideal I.

Teorema A.3.5. *Fije un orden monomial $\geq$ y sean $g_1, ..., g_m$ una m-ada ordenada de polinomios en $F[x_1, x_2, ..., x_n]$. Entonces para cada $f \in F[x_1, x_2, ..., x_n]$ puede ser escrito como:*

$$f = g_1q_1 + ... + g_mq_m + r$$

donde $q_i, r \in F[x_1, x_2, ..., x_n]$ y $r = 0$ o r es la combinación lineal con coeficientes en F de monomios tal que ningún es divisible entre los $LT(g_1), ..., LT(g_m)$.

Demostración.-(Existencia) Para esto tomamos el siguiente algoritmo de la división para polinomios en n variables;

Input:$g_1, ..., g_m, f$
Ouput:$q_1, ..., q_m, r$
$q_1 := 0; ...; q_m := 0, r := 0$
$p := f$
WHILE $p \neq 0$ DO
    $i := 1$
    divisionocurred:= $false$
    WHILE $i \leq s$ AND divisionocurred:= $false$ DO
        IF $LT(f_i)$ divides $LT(p)$ THEN
            $a_i := a_i + \frac{LT(p)}{LT(f_i)}$
            $p := p - (\frac{LT(p)}{LT(f_i)})f_i$
            divisionocurred:= $true$
        ELSE

$$i = i + 1$$

IF divisionocurred:= $false$ THEN

$$r := r + LT(p)$$

$$p := p - LT(p)$$

Podemos ver que este algoritmo es parecido al Ejemplo 3.4., pero con la diferencia que agregamos la variable p quien representa el dividendo intermedio en cada paso, la variable r representa la columna del lado derecho, y las variables $q_1, ..., q_m$ representan los cocientes listados encima de la división.

La variable *divisionocurred* nos dice cuando algún $LT(g_i)$ divide al cociente inicial del dividendo intermedio. Es claro que si está adentro del bucle principal $WHILE...DO$, precisamente ocurre dos cosas:

- (Paso de la división) Si algún $LT(g_i)|LT(p)$, entonces el algoritmo procede como en el caso de una variable.

- (Paso del residuo) Si ningún $LT(g_i)|LT(p)$, entonces el algoritmo manda $LT(p)$ al residuo.

Estos pasos corresponden al Ejemplo A.3.4.; vamos a probar que la igualdad;

$$f = g_1q_1 + ... + g_mq_m + p + r \qquad (1)$$

Supongamos que se cumple en cada etapa en efecto, para los valores iniciales de $g_1, ..., g_m$,p y r donde se cumple (1) en uno de los pasos del algoritmo. Si estamos en el paso de la división, entonces algún $LT(g_i)|LT(p)$ y se tendrá:

$$g_iq_i + p = \left(g_i + \frac{LT(p)}{LT(g_i)}\right) g_i + \left(p - \left(\frac{LT(p)}{LT(g_i)}\right) g_i\right)$$

nos muestra que permanece intacto $g_iq_i + p$. Dado que las otras variables no son afectadas, (1) sigue siendo cierta en este caso. Por otro lado si estaríamos en el paso del residuo,

entonces p y r serán sustituidos, pero la suma $p + r$ permanece intacta puesto que:

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

y como antes la igualdad (1) se preserva. Ahora observe que el algoritmo se detiene si $p = 0$, en esta situación (1) se convierte en:

$$f = g_1 q_1 + ... + g_m q_m + r \qquad (1)$$

Dado que se añaden términos a r sólo cuando no son divisibles por ninguno de los $LT(g_i)$, aquí se sigue que de aquí se sigue que $g_1, ..., g_m$ y r tienen las propiedades que deseamos cuando el algoritmo termina.

Por último debemos probar que el algoritmo eventualmente termina, observe que cuando se redefine la variable p, o se hace 0, o su multigrado disminuye; para probar esto supongase que durante el Paso de la División, p es redefinido como:

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

por uno de los lemas tenemos que

$$MGRAD\left(\frac{LT(p)}{LT(f_i)} f_i\right) = MGRAD\left(\frac{LT(p)}{LT(f_i)}\right) + MGRAD(f_i)$$

este se obtiene de fijarse en el multigrado del producto de los dos términos iniciales, de aquí se sigue la siguiente igualdad,

$$LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \left(\frac{LT(p)}{LT(f_i)} LT(f_i)\right) = LT(p)$$

con lo que p y $\frac{LT(p)}{LT(f_i)} f_i$ tienen el mismo término inicial, se sigue entonces que su diferencia, p' cancela el término inicial de p y por consiguiente p' tiene grado estrictamente menor cuando $p' \neq 0$.

Ahora supongase que estamos en el Paso del Residuo, p es redefinido como:

$$p' = p - LT(p)$$

aquí claramente $MGRAD(p') < MGRAD(p)$ cuando $p' \neq 0$ entonces en cualquiera de los casos, el multigrado debe disminuir. Si el algoritmo nunca terminará, entonces podríamos encontrar una sucesión decreciente infinita de multigrados; pero como el Lema 2.1.2. establece que $\geq$ es un Buen Orden si y solo si, toda sucesión decreciente debe terminar, lo que muestra que esta sucesión de multigrados no puede tomarse; con esto eventualmente debe ser $p = 0$, así el algoritmo termina después de un número finito de pasos.

La relación de los multigrados entre $MGRAD(f)$ y $MGRAD(g_i q_i)$. Todo término en q_i es de la forma $\frac{LT(p)}{LT(f_i)}$ para algún valor de la variable p. El algoritmo inicia con $p = f$ pero como ya hemos probado que el multigrado de p decrece, entonces $LT(p) \leq LT(f)$ de esto se sigue que;

$$MGRAD(g_i q_i) \leq MAGRAD(p) \leq MGRAD(f) \quad \text{, cuando } g_i q_i \neq 0$$

■ *Q.E.P.D.*

► Notese que no se demuestra la unicidad ya que un polinomio puede tener dos restos diferentes, por ejemplo tomando los polinomios simples en $Z[x, y]$ con el orden monomial lexicográfico $x >_{lex} y$; $f = xy^2$, $g_1 = xy + 1$ y $g_2 = y^2 - 1$, donde $LT(g_1) \mid LT(f)$ y $LT(g_2) \mid LT(f)$ así operando el algoritmo se hallan $q_1 = y$; $q_2 = 0$ y $r = -x - y \neq 0$ y por otro lado $q_1' = 0$ $q_2' = x$ y $r' = 0$ tal que:

$$f = (y)g_1 + (0)g_2 + (-x - y) \quad y \quad f = (0)g_1 + (x)g_2 + (0)$$

A.4. Biografía de: Wolfgang Gröbner

Matemático computacional (1899, Südtirol-Italia, 1980)

Wolfgang Gröbner nació el 11 de febrero de 1899, en Gossensass, en el Tyrol italiano y

murió en la misma ciudad el 20 de agosto de 1980. Creció y se educó con cuatro hermanos. El internado de los jesuitas en Feldkirch influyó mucho su vida posterior. En 1917 tuvo que ir al frente italiano y después de la guerra empezó sus estudios de construcción mecánica en la universidad técnica de Graz.

Hacia el final de sus estudios secundarios, una desventura le hizo cambiar el rumbo y su visión de la vida: un domingo, uno de sus hermanos tuvo un accidente con la moto sin haber asistido a una misa. Como Gröbner creía que su hermano iba a ser condenado para siempre, entró en crisis. Dejó sus estudios y rompió con la Iglesia católica. Diez años más tarde describió su búsqueda de una religiosidad sin ataduras en su primer libro *Der Weg aufwärts.* (El camino hacia arriba).

Otra consecuencia fue -que después de su matrimonio- empezó sus estudios en el area de matemática de la universidad de Viena (Austria), entre otros motivos porque "no hay ninguna autoridad aparte de tu propia razón". Sus profesores eran entre otros W. Wirtinger y Ph. Furtwängler. A Wirtinger le dió una buena impresión. En su trabajo *Eine Determinantenidentität und ihre Anwendungen.* (Una identidad de determinantes y aplicaciones) Wirtinger resaltó el importante aporte de Gröbner en el seminario de 1933/34. La tesis doctoral de Gröbner en 1932, supervisada por Furtwängler, se titula *Ein Beitrag zum Problem der Minimalbasen.* (Una contribución al problema de las bases minimales).

Como Furtwängler se lo había recomendado, Gröbner se fue inmediatamente después de su promoción a Göttingen para asistir a las lecciones de Emmy Noether. Ya antes de navidad Gröbner pudo presentar a Noether la solución (i.e. el boceto) de un problema sobre ideales irreducibles, que llegó a ser uno de los trabajos más importantes de Gröbner.

En enero de 1933 volvió a Austria por motivos económicos. Como no logró encontrar un trabajo en una universidad, trabajó por libre y construyó pequeñas centrales eléctricas en Gossensass, donde encontró al Prof M. Picone, quien estaba de vacaciones en el hotel del padre de Gröbner. Picone le empleó en su instituto de matemáticas aplicadas en Roma. En 1939 tuvo que irse de Roma a causa de la situación militar en Alemania. Trabajó una temporada para la Academia prusiana de ciencias antes de su nombramiento como *Extraor-*

dinarius (extraordinario) en la universidad de Viena el día 31 de octubre de 1941. Poco después tuvo que asistir al servicio militar, donde se dedicó a partir del 19.06.1942 a la constitución de un instituto de fuerza aérea para la aplicación de métodos matemáticos avanzados a problemas aeronáuticos. El instituto estaba en Braunschweig y el director del projecto se llamaba G. Doetsch, un matemático de Freiburg.

En 1945, Gröbner se refugió en el Tirol donde vivía su familia, pero después del fin de la guerra no logró volver a Viena inmediatamente y en 1947 se fue a Innsbruck a trabajar en la universidad de allí. Caracterizó la estructura de los ideales primarios por condiciones diferenciales. La idea es muy simple y consiste en expresar la multiplicidad de una raíz de un polinomio por su derivada. Sobre estos ideales primarios trata su segundo trabajo en 1938, Sobre una nueva fundación ideal teorética de geometría algebraica. M.G. Marinari, H.M. Möller, T. Mora lo llaman l*a dualidad de Gröbner*, en su libro *On multiplicities in polynomial system solving* de 1996. Hacia 1958, Gröbner se concentró en la solución sistemática de las ecuaciones diferenciales no lineales. El método de Gröbner de series de Lie es un método numérico de gran precisión para ecuaciones diferenciales ordinarias. En 1980, su método de series de Lie fue generalizado al caso de variables no communitativas por M. Fliess.

Sus alumnos de doctorado más famosos son: Heinrich Reitberger, Bruno Buchberger y G. Sonderegger. Precísamente, en el verano de 1964, Gröbner dio un seminario sobre la D*imensionstheorie der Polynomideale* (teoría de la dimensión de ideales de polinomios). B. Buchberger incluyó en su tesis ese método de Gröbner y se concentró en el problema de la terminación de ese método. Buchberger encontró la condición de terminación y desarrolló un algoritmo que hoy día lleva su nombre y produce una base del ideal y la llamó *base de Gröbner*. También inició, junto con un físico F. Cap, un programa de investigación subvencionado por la NASA y la US Army y consiguió la demostración de una famosa fórmula, la *Störungsformel*. En 1978, escribió un libro sobre teoría de Galois, *Die Galoistheorie*. En 1993, H. Hauser y G. Müller definieron la correspondencia de Gröbner, una asignación entre subvariedades del espacio afín y subálgebras geométricas del álgebra de Lie de todos los

campos vectoriales.

Gröbner no fue miembro de la NSDAP (partido político de Hitler) y se dice que no tenía una opinión nacionalista. Aún así - según una carta que escribió a Doetsch - le importaba mucho el triunfo de Alemania, lo cual según él era muy probable. Trabajó hasta 1970 en Innsbruck y murió en 1980 después de haber sufrido un ataque de apoplejía (síntoma neurológica).

A.5. Biografía de: Bruno Buchberger

Matemático computacional (1942, Innsbruck, Tyrol, Austria)

Bruno Buchberger nació en 1942, en Innsbruck, la capital del Tyrol austríaco. Se educó en su ciudad natal, entrando en la universidad de Innsbruck para estudiar matemáticas en 1960. Ya en 1966, consigue su doctorado (Ph.D.) en esa especialidad. También en el periodo 1964-66, trabaja como programador para el Computing Center, de la universidad de Innsbruck. Desde 1966 hasta 1973, trabaja como Profesor Ayudante en dicho centro. Después en el periodo 1973-74, ya como Docente en el mismo centro.

En 1974, se traslada a Linz, también Austria, como Full profesor de Ciencias de la Computación, en la Universidad Johannes Kepler. Fue Decano de la Escuela de Ciencias Naturales y Técnicas de la Johannes Kepler, de 1979 a 1981. En 1987, fue fundador del RISC (Research Institute for Symbolic Computation), en la Johannes Kepler, Linz, Austria. Donde fue Director hasta 1999. También en 1985, fue fundador del Journal for Symbolic Computation, Academic Press, London, del cual fue también editor jefe hasta 1995. También en 1991, fue fundador y director del Software Park Hagenberg de Austria, que implica a 25 compañías o grupos académicos diferentes, 200 personas en su staff de personal invertidos en trabajar sobre varios aspectos de investigación del software y su desarrollo. El paeque también incluye un College for Software Engineering que tiene entre 300-400 entre el profesorado y estudiantes.

Desde que en 1966 leyó su tesis encontrando una base del espacio vectorial cociente para

el anillo de clases, módulo un ideal de polinomios cero dimensional (en alemán), bajo la dirección del profesor Wolfgang Gröbner, a Bruno se le considera el inventor de la teoría de bases de Gröbner. Su algoritmo ha sido estudiado, mejorado y generalizado en los últimos 30 años, y lo más importante, se han encontrado multitud de aplicaciones a las ramas más diversas, incluidas criptografía, física, ingeniería y robótica entre otras. La naturaleza constructiva y computacional de esos métodos, en la era de la informática, lo hacen líder de las aplicaciones en muchos campos. Su algoritmo ha sido implementado y forma parte de todos los sistemas o paquetes de cálculo simbólico actuales tales como Mathematica, Macsyma, Magma, Maple, Derive y Reduce.

Su investigación desde 1995, se centró en el proyecto Theorema, un sistema para la exploración de las teorías matemáticas asistidas por ordenador. El proyecto Theorema forma del SFB (Special Research Consortium) "Scientific Computing"de la universidad de Linz, esponsorizado por la FWF (Austrian National Science Foundation). Trata de desarrollar un sistema de software que simule formas humanas de demostración en matemáticas, sistema que el profesor Buchberger explica en su curso titulado T*hinking, Speaking, Writing*. Más generalmente, Theorema es un entorno uniforme de lógica y software para simular todas las fases de un ciclo de exploración matemático: formalización, prueba, resolución y cálculo.

El sistema se ha programado en el paquete Mathematica y consiste de varias partes: un analizador sintáctico que acepta fórmulas de dimensión dos en una notación muy cercana la usual en matemáticas, un mecanismo para expresar funtores, un lenguaje formal que permite construir jerarquías de fórmulas etiquetadas en bases estructuradas de conocimiento, varios probadores para la generación automática de demostraciones para varias clases de fórmulas matemáticas (e.g. fórmulas de lógica de predicados, igualdades sobre los números naturales y otros dominios inductivos, combinaciones booleanas de igualdades sobre números complejos, fórmulas de teoría de conjuntos, etc., post-procesadores que presentan las demostraciones en varios lenguajes naturales (por el momento Inglés y Japonés, interfaces para enviar fórmulas y bases de conocimiento desde Theorema a varios probadores externos como Otter etc. y para trasladar el output de estos probadores de vuelta hacia la

sisntasis de Theorema, un mecanismo para acceder a todas las funciones de Mathematica dentro de Theorema. Recientemente, Buchberger ha introducido la noción de símbolos lexicográficos que abren nuevas posibilidades para combinar el razonamiento formal con la intuición gráfica.

Bibliografía

Libros de Consulta:

[1] Becker,T. and Weispfenning, V.: *Grobner Bases: a Computacional Aproach to Conmutative Algebra*, Editorial: Springer-Velar, New York, 1993.

[2] D. Cox, J. Little, O'Shea: *Ideals, varieties, Algorithms-Introduction and computational algebraic geometry and commutative algebra* , Third edition. Undergraduate Texts in Mathematics.Springer New York-2007.

[3] Herstein, I.: *Topic in Algebra, 1ra. edición*, Editorial: Wiley, New York, 1975.

[4] Hungerford: *Abstract Algebra*, Editorial:x, New York, 1998.

Publicaciones en Internet:

Habraham Martín del Campo; Optimización del Algoritmo de Buchberger
http:// www.maths.psu.edu/pub/optimización-pdf/2007

Santiago Laplagne; Algoritmos de Descomposición primaria
http:// www.maths.org.edu/pub/algotim-pdf/2004