UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS

Tesis

Sobre las Bases de Gröbner, los Sistemas de Ecuaciones Polinomiales y los Polinomios Simétricos

Para Obtener
el Título Profesional de
LICENCIADO EN MATEMÁTICA

Elaborado por:

Mark Leyva Sartori

Asesor

Mg. Manuel Teodosio Toribio Cangana

LIMA-PERÚ

2016

CIP - CATÁLOGO DE PUBLICACIÓN

Leyva Sartori, Mark

Sobre las Bases de Gröbner, los Sistemas de Ecuaciones Polinomiales y los Polinomios Simétricos / Mark Leyva Sartori – EPM - FC - UNI, 2016.

97 p.: il.

Tesis (Licenciatura)—Universidad Nacional de Ingeniería, Facultad de Ciencias, Escuela Profesional de Matemática, Lima, Diciembre 2016. Asesor: Mg. Manuel Teodosio Toribio Cangana.

Dedicatoria

A mis padres, Maximo Leyva Caballero y Fulgencia Sartori Obregón.

Agradecimientos

Agradezco a los docente y trabajadores de la Facultad de Ciencias de la UNI y al profesor Mg. Manuel Toribio Cangana que me asesoró para esta tesis.

Resumen

La presente tesis tiene como objetivo exponer la teoría de las Bases de Gröbner en el anillo de polinomios $k[x_1, \ldots, x_n]$ sobre un campo k, así como sus aplicaciones en la solución de sistemas de ecuaciones polinomiales no-lineales y los polinomios simétricos. Las Bases de Gröbner pueden ser vistas como una generalización multi-variable del algoritmo euclidiano para calcular el máximo común divisor de un conjunto de polinomios y el método de eliminación Gaussiana para resolver sistemas lineales. La teoría que expondremos a continuación es central en el estudio de muchos algoritmos en geometría algebraica y álgebra conmutativa, siendo el algoritmo de Buchberger de fundamental importancia en estas implementaciones.

Abstract

This thesis is about Gröbner Basis for ideals in the ring of polynomials $k[x_1, \ldots, x_n]$ over a field k, its use in solving systems of polynomial equations and representing symmetric polynomials. A Gröbner basis is a set of multivariate polynomials enjoying certain properties that allow simple algorithmic solutions for many fundamental problems in mathematics and natural and technical sciences with Buchberger's Algorithm being fundamental on this implementations.

Índice general

Lista de Símbolos

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

$k[x_1, \ldots, x_n]$: El Anillo de los polinomios en n indeterminadas con coeficientes en k.

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

$\mathbb{N}^n$: al producto cartesiano $\underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{n \text{ veces}}$.

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

$\boldsymbol{X}^{\boldsymbol{\beta}}$: al monomio $x_1^{\beta_1} \ldots x_n^{\beta_n}$.

$\vee$: o, disyunción lógica.

$\wedge$: y, conjunción lógica.

$a \mid b$: a divide a b.

$f \xrightarrow{g} h$: f se reduce a h módulo g.

M_n : El Conjunto de los Monomios de $k[x_1, \ldots, x_n]$.

$MO(M_n)$: El conjunto de los órdenes monomiales en M_n.

$Supp(p)$: El conjunto de los monomios o productos de potencia que aparecen en p.

$supp(p)$: Sub-conjunto de $\mathbb{N}^n$ que determina únicamente al polinomio $p \in k[x_1, \ldots, x_n]$.

$V(S)$: La variedad inducida por S.

$\mathrm{lc}(f)$: coeficiente principal de f.

lp(f) : producto de potencias principal o monomio principal de f.

lt(f) : término principal del polinomio f.

Lt(S) : ideal de los términos principales de polinomios en S.

mcd : máximo común divisor.

mcm : mínimo común múltiplo.

Lista de Algoritmos

Prólogo

Una Base de Gröbner es un conjunto de polinomios con ciertas propiedades que nos permiten obtener simples soluciones algorítmicas para muchos problemas fundamentales en las matemáticas, ciencias naturales y ciencias técnicas. Ejemplos de tales problemas son: la solución de sistemas de ecuaciones álgebraicas, control inteligente de plataformas de petróleo, búsqueda de relación genética entre especies, etc.

La primera sección del segundo cápitulo es una referencia a conceptos fundamentales del álgebra como anillos, ideales, dominios de integridad, etc. Lo más importante de esta primera sección es el Teorema de las Bases de Hilbert por el papel que cumple en las pruebas de los teoremas y proposiciones de las secciones posteriores.

El segundo cápitulo continua con un repaso del algoritmo de la división para polinomios en $k[x]$ y el algoritmo euclidiano para determinar el máximo común divisor de dos polinomios en $k[x]$. Luego sigue con la definición de órdenes monomiales en $k[x_1, \ldots, x_n]$ (por ejemplo *lex* y *deglex*) y el proceso de reducción, para así poder dar un algoritmo de la división en $k[x_1, \ldots, x_n]$. El cápitulo continúa con la definición de bases de Gröbner, es decir que condiciones deben cumplir un conjunto de polinomios en un ideal de $k[x_1, \ldots, x_n]$ para ser denominados una base de Gröbner, la definición de S-polinomios y la exposición de en que consiste el Algoritmo de Buchberger. El final de este cápitulo trata sobre las bases de Gröbner reducidas, las bases de Gröbner no son únicas pero las que están reducidas sí, syzygies y su aplicación para encontrar criterios que hagan más eficiente el algoritmo de Buchberger.

El tercer cápitulo trata sobre aplicaciones específicas de la teoría y algoritmos expuestos en el cápitulo dos. Como son: el problema de membresía a un ideal, la solución de sistemas de ecuaciones polinomiales, los polinomios simétricos, etc.

Se agrega un apéndice acerca de las Bases de Gröbner Universales, que son bases de

Gröbner que continúan siendo bases de Gröbner si se cambia el orden entre monomios.

Para todos los ejemplos de los algoritmos desarrollados en está tesis se muestran los cálculos explícitamente, con el fin de hacer una mejor exposición del proceso que sigue cada algoritmo. Mencionamos que existe software matemático (como CoCoA,Maple,Mathematica,etc) en el cual estos algoritmos ya están pre-programados.

Capítulo 1

Introducción

1.1 Generalidades

Dado un sistema de ecuaciones polinomiales en el anillo $\mathbb{R}[x_1, \ldots, x_n]$:

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

, resolver el sistema anterior implica hallar todas las n-tuplas $(a_1, \ldots, a_n) \in \mathbb{R}^n$ tales que se cumple

$$\begin{cases} f_1(a_1, \ldots, a_n) & = 0 \\ \vdots & \\ f_m(a_1, \ldots, a_n) & = 0 \end{cases}.$$

Si consideramos el ideal generado por estos polinomios, es decir $I = \langle f_1, \ldots, f_m \rangle$, podemos verficar fácilmente que para cualquier otro conjunto generador de este ideal digamos $I = \langle g_1, \ldots, g_s \rangle$ se cumple que las soluciones del sistema

$$\begin{cases} g_1(x_1, \ldots, x_n) & = 0 \\ \vdots & \\ g_m(x_1, \ldots, x_n) & = 0 \end{cases}$$

son equivalentes a las soluciones del sistema original. Luego todo sistema de ecuaciones polinomiales está asociado a un ideal. Además se demuestra (teorema 2.4) que

todos los ideales de $\mathbb{R}[x_1, \ldots, x_n]$ (y más generalmente de $k[x_1, \ldots, x_n]$) son finitamente generados, es decir todo ideal induce un sistema de ecuaciones polinomiales.

1.2 Problemática

El sistema anterior puede ser:

1. Compatible Determinado, en el caso tenga un número finito o numerable de soluciones.

2. Conmpatible Indeterminado, en el caso las soluciones formen un conjunto infinito no-numerable.

3. Incompatible, en el caso no tenga solución alguna.

Resolver sistemas de ecuaciones polinomiales no-lineales no es una tarea sencilla. Pero debido al descubrimiento de las Bases de Gröbner y el algoritmo de Buchgberger podemos encontrar, bajo ciertas condiciones en el ideal formado por los polinomios del sistema original, un sistema equivalente que sea más comodo de resolver.

1.3 Objetivos

Exponer el fundamento teórico de las Bases de Gröbner, mostrar detalladamente el funcionamiento del algoritmo de Buchberger y utilizarlo en la resolución de sistemas de ecuaciones polinomiales no-lineales, así como también aplicarlo en la representación de los polinomios simétricos, entre otras aplicaciones como por ejemplo el problema de membresía a un ideal.

Capítulo 2

Teoría de las Bases de Gröbner

El objetivo de este cápitulo será estudiar el algoritmo de Buchberger, el cual permite encontrar bases de Gröbner para ideales en el anillo de polinomios de varias indeterminadas.

2.1 Conceptos Preliminares

En esta sección se expondrá algunas definciones, proposiciones y teoremas bien conocidos (pero necesarios para las secciones posteriores) del Álgebra de pre-grado.

Denotaremos por $\mathbb{N}$ al conjunto de enteros no-negativos, es decir $\mathbb{N} = \{0, 1, 2, \dots\}$.

2.1.1 Anillos

Definición 2.1. A un conjunto no-vacío R junto con dos operaciones binarias $+, \cdot$ (usualmente referidas como adición y multipliación) se le llama anillo, si cumple las siguientes propiedades:

(i) $(R, +)$ es un grupo abeliano;

(ii) $(ab)c = a(bc)$, para todo $a, b, c \in R$ (asociatividad de la multipliación);

(iii) $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$.

Definición 2.2. Si en un anillo R se cumple $ab = ba$ para todo $a, b \in R$, se dice que R es un anillo conmutativo.

Definición 2.3. Si en un anillo R existe un elemento 1_R tal que $1_R a = a1_R$ para todo $a \in R$, se dice que R es un anillo con identidad.

Al elemento neutro aditivo de un anillo R usualmente se le denota por 0. Ahora sea $n \in \mathbb{Z}$ y $a \in R$, escribiremos

$$na = \underbrace{a + \cdots + a}_{n \text{ sumandos}}, \quad \text{si} \quad n > 0$$

, y

$$na = \underbrace{(-a) + \cdots + (-a)}_{n \text{ sumandos}}, \quad \text{si} \quad n < 0.$$

Teorema 2.1 (ref.[Hungerford T.],cáp.3,pág.115)**.** Sea R un anillo. Se cumple:

(i) $0a = a0 = 0$, $\forall a \in R$;

(ii) $(-a)b = a(-b) = -(ab)$, $\forall a, b \in R$;

(iii) $(-a)(-b) = ab$, $\forall a, b \in R$;

(iv) $(na)b = a(nb) = n(ab)$, $\forall n \in \mathbb{Z}$ y $a, b \in R$;

(v) $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$, $\forall a_i, b_j \in R$;

Definición 2.4. Sea S un sub-conjunto no-vacío de un anillo R que es cerrado bajo las operaciones de adición y multiplicación en R. Si S es en si mismo un anillo bajo esas operaciones se dice que S es un sub-anillo de R. Sea I un sub-anillo de R, se dice que I es un ideal a la izquierda de R, si cumple

$$\forall r \in R, x \in I \implies rx \in I$$

, respectivamente un ideal a la derecha de R, si cumple

$$\forall r \in R, x \in I \implies xr \in I.$$

I es un ideal de R si es que es ambos un ideal a la izquierda y a la derecha de R.

Teorema 2.2 (ref.[Hungerford T.],cáp.3,pág.123)**.** Un sub-conjunto no-vacío I de R es un ideal a la izquierda(resp. a la derecha) si, y sólo si para todo $a, b \in I$, $r \in R$:

(i) $a, b \in I \implies a - b \in I$ y;

(ii) $a \in I, r \in R \implies ra \in I$.

Corolario 2.1. Sea $\{A_i \mid i \in S\}$ una familia de ideales en un anillo R. Entonces $\bigcap_{i \in S} A_i$ también es un ideal.

Definición 2.5. Sea X un sub-conjunto del anillo R. Sea $\{A_i \mid i \in S\}$ la familia de todos los ideales en R que contienen a X. Al ideal $\bigcap_{i \in S} A_i$ se le dice el ideal generado por X, y es denotado por $\langle X \rangle$.

Proposición 2.1. Sea R un anillo conmutativo con unidad. Entonces para un sub-conjunto no vacío X de R se tiene que

$$\langle X \rangle = \{\sum_{i=1}^{n} r_i x_i, \quad \forall r_i \in R, x_i \in X, n \in \mathbb{N}\}.$$

2.1.2 Dominios de Integridad y Dominios de Factorización Única

Definición 2.6. Sea a un elemento no-nulo del anillo R. Se dice que a es un divisor izquierdo (resp. derecho) de cero, si existe un $0 \neq b \in R$ tal que $ab = 0$ (resp. $ba = 0$). Un divisor de cero de R es un elemento que cumple con ser ambos, un divisor izquierdo y derecho de cero.

Es fácil verificar que un anillo R no tiene divisores de cero si, y sólo si se cumple $\forall a, b, c \in R$ con $a \neq 0$

$$ab = ac \vee ba = ca \implies b = c$$

Definición 2.7. Un elemento a de un anillo con identidad R, se dice invertible a la izquierda (resp. a la derecha) si existe $c \in R$ tal que $ca = 1_R$ (resp. existe un $b \in R$ tal que $ab = 1_R$). Al elemento c se le llama una inversa a la izquierda (resp. a b una inversa a la derecha) de a. A un elemento a que es invertible a la izquierda y a la derecha se le dice invertible o que es una unidad.

Las inversas a la izquierda y a la derecha de una unidad necesariamente coinciden. Y el conjunto de las unidades de un anillo con identidad R forman un grupo bajo la multiplicación.

Definición 2.8. A un anillo conmutativo R con unidad $1_R \neq 0$ y sin divisores de cero, se le denomina dominio de integridad. A un anillo D con identidad $1_D \neq 0$ en el cual todo elemento no-nulo es una unidad se le denomina anillo de división. A un anillo conmutativo de división F se le denomina campo.

Nota 2.1. Todo campo F es un dominio de integridad.

Nota 2.2. A un ideal generado por un elemento se le llama ideal principal, y a un dominio de integridad en el cual todo ideal es principal se le llama dominio de ideales principales(DIP).

Definición 2.9. Sea a un elemento no-nulo y b un elemento de un anillo conmutativo R, se dice que $a \mid b$, a divide a b, si existe un $c \in R$ tal que $b = ac$. Dos elementos no-nulos $a, b \in R$ se dice que son asociados si $a \mid b$ y $b \mid a$.

Definición 2.10. Sea R un anillo conmutativo con unidad. A un elemento $c \in R$ se le llama irreducible si cumple

(i) c es no-nulo y no es una unidad.

(ii) si $c = ab$ entonces a es una unidad o b es una unidad.

A un elemento $p \in R$ se le dice primo si

(i) p es no-nulo y no es una unidad.

(ii) si $p \mid ab$ entonces $p \mid a \vee p \mid b$.

Definición 2.11. A un dominio de integridad D se le llama Dominio De Factorización Única (DFU), si cumple

(i) Todo elemento no-nulo y no-unidad a de R puede ser expresado como $a = c_1 \ldots . c_n$, con $c_1, \ldots, c_n$ irreducibles.

(ii) Si $a = c_1 \ldots c_n$ y $a = b_1 \ldots b_m$ con los c_i, b_i irreducibles, entonces $n = m$ y para alguna permutación σ de $\{1, \ldots, n\}$, c_i y $b_{\sigma(i)}$ son asociados para todo $1 \leq i \leq n$.

2.1.3 Módulos

Definición 2.12. Sea R un anillo. Un R-módulo es un grupo abeliano aditivo M junto con una función $R \times M \to M$ (la imagen de (r, m) siendo denotada por rm) tal que para todo $r, s \in R$ y $a, b \in M$:

(i) $r(a + b) = ra + rb$;

(ii) $(r + s)a = ra + sa$;

(iii) $r(sa) = (rs)a$;

(iv) $1_R a = a$.(en caso 1_R existe)

En caso R es un anillo de división, el R-módulo sera un espacio vectorial.

Definición 2.13. Sean A y B módulos sobre un anillo R. Una función $f : A \to B$ es un R-módulo homomorfismo si para todo $a, c \in A$ y $r \in R$:

$$f(a + c) = f(a) + f(c), \quad f(ra) = rf(a).$$

En caso R sea un anillo de división, un R-módulo homomorfismo sera una transformación lineal.

El núcleo de un R-morfismo $f : A \to B$, es el sub-módulo

$$Ker(f) = \{a \in A \mid f(a) = 0\}.$$

Teorema 2.3 (Primer Teorema de Isomorfismos de R-módulos, ref.[Hungerford T.],cáp.4,pág.172)**.** Sean R un anillo, M,N dos R-módulos, $f : M \to N$ un R-morfismo. Entonces existe un único R-isomorfismo $\phi : \frac{M}{Ker(f)} \to Imf$, definido por: $\forall \overline{m} \in \frac{M}{Ker(f)}$, $\phi(\overline{m}) = f(m)$.

Definición 2.14. Un sub-conjunto no-vacío S de un R-módulo M es una base de M si, y sólo si todo elemento de M puede ser expresado en forma única como una combinación lineal de elementos de S.

2.1.4 Teorema de las bases de Hilbert

Sea k un campo.

Teorema 2.4 (Teorema de las Bases de Hilbert, ref.[Adams W.],cáp.1,pág.5)**.** En el anillo $k[x_1, \ldots, x_n]$ se cumple lo siguiente:

(1) Si I es un ideal de $k[x_1, \ldots, x_n]$ entonces I es finitamente generado es decir existen polinomios $f_1, \ldots, f_s$ en $k[x_1, \ldots, x_n]$ tales que $I = \langle f_1, \ldots, f_s \rangle$.

(2) Si $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots I_n \subseteq \ldots$ es una cadena de ideales creciente en $k[x_1, \ldots, x_n]$ entonces existe N tal que $I_N = I_{N+1} = I_{N+2} = \ldots$.

Prueba. Será una consecuencia de los siguientes resultados. □

A todo anillo conmutativo que cumple (1) o (2) en el Teorema anterior se le dice Notheriano (ref.[Hungerford T.],cáp.6, pág.76).

Primero demostraremos que en un anillo conmutativo las dos afirmaciones del teorema anterior son equivalentes:

Teorema 2.5 ([Adams W.], cáp.1, pág.6)**.** Sea R un anillo conmutativo. Las siguientes dos condiciones son equivalentes:

(i) Todo ideal I de R es finitamente generado.

(ii) Si $I_1 \subseteq I_2 \subseteq \cdots I_n \subseteq \cdots$ es una cadena de ideales ascendente de R, entonces existe N tal que $I_N = I_{N+1} = I_{N+2} \cdots$.

Prueba. (i)⇒(ii). Consideremos

$$I = \bigcup_{n=1}^{\infty} I_n$$

claramente I es un ideal en R y entonces por hipótesis finitamente generado, es decir para algunos $f_1, \ldots, f_s$ en R podemos escribir $I = \langle f_1, \ldots, f_s \rangle$ luego para cada $f_i, i = 1, \ldots, s$ existe N_i tal que $f_i \in I_{N_i}$, si definimos $N = \max_{1 \leq i \leq s} N_i$ entonces $f_i \in I_N$ para todo $i = 1, \ldots, s$ y entonces $\langle f_1, \ldots, f_s \rangle \subseteq I_N$ luego $I = I_N$ y condición (ii) se cumple.

(ii)⇒(i). Supongamos que existe un ideal I en R que no puede ser finitamente generado. Sea $f_1 \in I$ entonces existe un $f_2 \in I$ tal que $f_2 \notin \langle f_1 \rangle$ asi $\langle f_1 \rangle \subsetneqq \langle f_1, f_2 \rangle$ continuando con el proceso tendremos una cadena de ideales en R estrictamente creciente lo que contradice la hipótesis (ii). □

Teorema 2.6 ([Adams W.], cáp. 1, pág.6-7)**.** Si R es un anillo Notheriano entonces también lo es $R[x]$.

Prueba. Sea J un ideal de $R[x]$. Por el Teorema anterior es suficiente con probar que J es finitamente generado. Para cada $n \geq 0$, definamos

$$I_n = \{r \in R \mid r \text{ es el coeficiente principal de un polinomio de grado } n \text{ en } J\}.$$

Claramente los I_n son ideales de R y $I_n \subseteq I_{n+1}$ para todo $n \geq 0$, luego por hipótesis existe N tal que $I_n = I_N, \forall n \geq N$ y podemos escribir $I_i = \langle r_{i1}, \ldots, r_{it_i} \rangle, i = 0, \ldots, N$. Sea f_{ij} un polinomio en J de grado i con coeficiente principal r_{ij} y denotemos

$$J^* = \langle f_{ij} \rangle \quad \text{para} \quad 0 \leq i \leq N, 1 \leq j \leq t_i.$$

Bastará con probar que $J^* = J$. Claramente $J^* \subseteq J$. Para la otra inclusión sea $f \in J$ de grado n con coeficiente principal r. Por inducción sobre n, si $n = 0$ entonces $f \in I_0$ y luego en J^*. Ahora sea $n > 0$ y asumamos que todos los polinomios en J hasta grado $n-1$ se encuentran en J^*. Si $n \leq N$ desde que $r \in I_n$ tenemos para algunos $s_j \in R$,

$$r = \sum_{j=1}^{t_n} s_j r_{nj}.$$

Entonces el polinomio

$$g = \sum_{j=1}^{t_n} s_j f_{nj}$$

tiene coeficiente principal r, es de grado n y se encuentra en J^*. La diferencia $f - g$ tiene grado a lo más $n-1$ y se encuentra en J luego por nuestra hipótesis inductiva también se encuentra en J^* así $f \in J^*$. Si $n > N$, entonces $r \in I_n = I_N$, y para algunos $s_j \in R$

$$r = \sum_{j=1}^{t_N} s_j r_{Nj}.$$

El polinomio

$$g = \sum_{j=1}^{t_N} s_j x^{n-N} f_{Nj}$$

tiene coeficiente principal r, es de grado n y está en J^*. Así $f - g$ es de grado a lo más $n-1$ y por inducción está en J^*. Se sigue que $f \in J^*$. □

Usando un simple proceso de inducción en n, el resultado anterior y considerando que $k[x_1,\ldots,x_n] \cong k[x_1,\ldots,x_{n-1}][x_n]$ (ref.[Hungerford T.], cáp.5, págs.153-154) se prueba que $k[x_1,\ldots,x_n]$ es notheriano (notar que el campo k es trivialmente notheriano). Es decir el Teorema 2.4 es verdadero.

2.2 El caso de los polinomios con una sola variable

Sea k un campo, revisaremos primero que ocurre con los ideales y el proceso de división en el anillo de los polinomios con una sola indeterminada, $k[x]$, para luego pasar al caso multi-variable.

Para $0 \neq f \in k[x]$, denotaremos por grado(f) al grado de f, lt(f) al término principal de f, lc(f) al coeficiente principal de f y por lp(f) al monomio principal o producto de potencias principal de f. En el caso de $f = 0$ podemos definir lt(0)=lp(0)=lc(0)=0 y grado(f)=0.
Por ejemplo si $f = 2x^5 + \frac{3}{7}x^2 + x - 5$ tenemos que $\text{lt}(f) = 2x^5, \text{lp}(f) = x^5, \text{lc}(f) = 2$ y grado(f)=5.

Teorema 2.7 (ref.[Adams W.], cáp. 1, págs. 11-12)**.** Sea g un polinomio no-nulo en $k[x]$. Entonces para todo $f \in k[x]$, existen q, r en $k[x]$ tales que

$$f = qg + r, \quad \text{donde} \quad r = 0 \quad \vee \quad \text{grado}(r) < \text{grado}(g).$$

además q,r son únicos (q es llamado cociente y r resto).

Prueba. La prueba es conocida como el algoritmo de la división:

Entrada: f,g$\in$ k[x] con g$\neq$0
Salida: q,r tales que f=qg+r y r=0 $\vee$ grado(r)<grado(g)
Inicio: q:=0, r:=f
Mientras: r$\neq$0 y grado(g)$\leq$grado(r)
Hacer
q:=q+$\frac{\text{lt}(r)}{\text{lt}(g)}$
r:=r$-\frac{\text{lt}(r)}{\text{lt}(g)}g$
Fin Mientras

Algoritmo 2.1: Algoritmo de la División para polinomios de una sola variable.

□

Si $f = a_n x^n + a_{n-1}x^{n-1} + \dots$ y $g = b_m x^m + b_{m-1}x^{m-1} + \dots$ con $b_m \neq 0$ y $n \geq m$ entonces el primer paso en la división es sustraer de f el producto $\frac{a_n}{b_m}x^{n-m}g = \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)}g$ entonces tenemos $h = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)}g$ como el primer resto. A h se le dice una reducción de f por g y al proceso de calcular h lo denotamos

$$f \xrightarrow{g} h.$$

Repetidos usos del proceso de reducción nos da el resto r.

Ejemplo 2.1. Sea $f = x^3 - 2x^2 + 2x + 8$, y $g = 2x^2 + 3x + 1$ en $\mathbb{Q}[x]$.
Inicio: $q := 0, r := f = x^3 - 2x^2 + 2x + 8$.
Primera iteración por el bucle mientras:
$q := 0 + \frac{x^3}{2x^2} = \frac{1}{2}x$
$r := (x^3 - 2x^2 + 2x + 8) - \frac{x^3}{2x^2}(2x^2 + 3x + 1) = -\frac{7}{2}x^2 + \frac{3}{2}x + 8$
Segunda iteración por el bucle mientras:
$q := \frac{1}{2}x + \frac{-\frac{7}{2}x^2}{2x^2} = \frac{1}{2}x - \frac{7}{4}$
$r := (-\frac{7}{2}x^2 + \frac{3}{2}x + 8) - \frac{-\frac{7}{2}x^2}{2x^2}(2x^2 + 3x + 1) = \frac{27}{4}x + \frac{39}{4}$
Fin del proceso mientras desde que grado(r)=1<2=grado(g), f queda expresado como $f = (\frac{1}{2}x - \frac{7}{4})(2x^2 + 3x + 1) + (\frac{27}{4}x + \frac{39}{4})$.

Ahora sea $I = \langle f, g\rangle$ y supongamos que $f \xrightarrow{g} h$. Entonces desde que $h = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)}g$ se ve fácilmente que $I = \langle h, g\rangle$ así podemos reemplazar f por h en el conjunto de generadores de I. Usando esta idea repetidamente podemos probar el siguiente resultado:

Teorema 2.8. [ref.[Adams W.], cáp.1, pág.13] Todo ideal de $k[x]$ es generado por un elemento. Es decir $k[x]$ es un DIP.

Prueba. Sea I un ideal no-nulo de $k[x]$. Sea $g \in I$ tal que $g \neq 0$ y de grado n mínimo. Para todo $f \in I$ haciendo uso del algoritmo de la división existen $q, r \in k[x]$ tales que $f = qg + r$, con $r = 0$ o grado(r)<grado(g)=n. Si $r \neq 0$, entonces $r = f - qg \in I$ lo cual contradice la elección de g. Por tanto $r = 0$, $f = qg$ y $I \subseteq \langle g\rangle$. La igualdad se sigue del hecho que g esta en I. □

El polinomio g en la prueba del teorema anterior es único excepto por la multiplicación de una constante. Esto se sigue del hecho que si $I = \langle g_1 \rangle = \langle g_2 \rangle$, entonces g_1 y g_2 son asociados es decir g_1 divide a g_2 y g_2 divide a g_1. También g es el *mejor* conjunto generador para el ideal $I = \langle f_1, \ldots, f_s \rangle$ por que por ejemplo el sistema de ecuaciones en $k[x]$

$$\begin{cases} f_1 & = 0 \\ f_2 & = 0 \\ & \vdots \\ f_s & = 0 \end{cases}$$

tiene precisamente el mismo conjunto de soluciones que la ecuación $g = 0$, donde $\langle f_1, \ldots, f_s \rangle = \langle g \rangle$.

Dada la importancia del polinomio g del teorema anterior, buscaremos calcularlo, enfocándonos primero en los ideales $I \subseteq k[x]$ generados por dos polinomios, digamos $I = \langle f_1, f_2 \rangle$, con alguno f_1, f_2 no-nulo. El máximo común divisor de f_1 y f_2 denotado por $\text{mcd}(f_1, f_2)$ es el polinomio g tal que:

1. g divide a f_1 y a f_2;

2. si $h \in k[x]$ divide a f_1 y f_2, entonces h divide a g;

3. $\text{lc}(g) = 1$ (es decir g es mónico).

Proposición 2.2. Sea $f_1, f_2 \in k[x]$, con al menos uno no-nulo. Entonces $\text{mcd}(f_1, f_2)$ existe y $\langle f_1, f_2 \rangle = \langle \text{mcd}(f_1, f_2) \rangle$.

Prueba. Por el teorema 2.8, existe $g \in k[x]$ tal que $\langle f_1, f_2 \rangle = \langle g \rangle$ y g es único salvo por una constante luego podemos asumir $\text{lc}(g) = 1$. Probaremos que $g = \text{mcd}(f_1, f_2)$. Desde que $f_1, f_2 \in \langle g \rangle$, g divide a f_1 y f_2. Ahora sea h en $k[x]$ tal que h divide a ambos f_1, f_2. Como g está en el ideal $\langle f_1, f_2 \rangle$, existen $u_1, u_2 \in k[x]$ tal que $g = u_1 f_1 + u_2 f_2$. Por tanto h divide a g y la prueba está completa. □

Como una consecuencia si tuvieramos un algoritmo para encontrar el $\text{mcd}(f_1, f_2)$ entonces tendríamos al solo generador del ideal $\langle f_1, f_2 \rangle$. El algoritmo para computar los mcd es llamado *algoritmo euclidiano*. Antes un lema que nos será útil en la construcción del algoritmo.

Lema 2.1. Sea $f_1, f_2 \in k[x]$ con no ambos nulos. Entonces mcd(f_1, f_2)=mcd$(f_1 - qf_2, f_2)$ para todo $q \in k[x]$.

Prueba. Es fácil ver que $\langle f_1, f_2\rangle = \langle f_1 - qf_2, f_2\rangle$, y por la proposición 2.2 tenemos

$$\langle \text{mcd}(f_1, f_2)\rangle = \langle f_1, f_2\rangle = \langle f_1 - qf_2, f_2\rangle = \langle \text{mcd}(f_1 - qf_2, f_2)\rangle.$$

Desde que el generador de un ideal principal es único excepto por una constante y que el mcd de dos polinomios tiene coeficiente principal 1, la prueba está completa. □

Con la notación del lema anterior, si q fuera el cociente en la división de f_1 por f_2 (si digamos grado(f_1)>grado(f_2)), obtendriámos mcd(f_1, f_2)=mcd(r, f_2) con r el resto de tal división. Desde que podemos seguir dividiendo hasta encontrar un resto que sea cero, esto nos lleva a definir el siguiente algoritmo:

Entrada: $f_1, f_2 \in k[x]$, con no ambos nulos.
Salida: $f = \text{mcd}(f_1, f_2)$
Inicio: $f := f_1, g := f_2$
Mientras $g \neq 0$ **Hacer**
    Calcular r como el resto de la división de f por g;
    $f := g$;
    $g := r$;
Fin Mientras
$f := \frac{1}{\text{lc}(f)} f$.

Algoritmo 2.2: Algoritmo Euclidiano.

Ejemplo 2.2. Inicio: $f := x^3 - 3x + 2, g := x^2 - 1$
Primera iteración por el bucle mientras:
$x^3 - 3x + 2 \xrightarrow{x^2-1} -2x + 2$, con $f = xg + (-2x + 2)$
$f := x^2 - 1$
$g := -2x + 2$
Segunda iteración por el bucle mientras:
$x^2 - 1 \xrightarrow{-2x+2} x - 1 \xrightarrow{-2x+2} 0$, con $x^2 - 1 = g + \frac{1}{2}x(-2x + 2)$
$f := -2x + 2$
$g := 0$

Fin mientras

$f := \frac{1}{\mathrm{lc}(f)} f = \frac{1}{-2} f = x - 1$

Obtenemos $\mathrm{mcd}(f_1, f_2) = x - 1$. También hemos encontrado los coeficientes polinomiales $u_1 = \frac{x}{2}$, $u_2 = -\frac{x^2}{2} + 1$ tales que $\mathrm{mcd}(f, g) = u_1 f + u_2 g$.

Generalizando la propiedad del máximo común divisor ahora para s polinomios $f_1, \ldots, f_s$, denotado $\mathrm{mcd}(f_1, \ldots, f_s)$, es el polinomio g tal que:

1. g divide a cada $f_i, i = 1, \ldots, s$;
2. si $h \in k[x]$ divide a cada $f_i, i = 1, \ldots, s$, entonces h divide a g;
3. $\mathrm{lc}(g) = 1$ (es decir g es mónico).

Proposición 2.3. Sean $f_1, \ldots, f_s$ polinomios en $k[x]$. Entonces

(i) $\langle f_1, \ldots, f_s \rangle = \langle \mathrm{mcd}(f_1, \ldots, f_s) \rangle$;

(ii) si $s \geq 3$, entonces $\mathrm{mcd}(f_1, \ldots, f_s) = \mathrm{mcd}(f_1, \mathrm{mcd}(f_2, \ldots, f_s))$.

Prueba. La prueba de (i) es similar a la prueba de la proposición 2.2. Para probar (ii), sea $h = \mathrm{mcd}(f_2, \ldots, f_s)$. Entonces, por (i), $\langle f_2, \ldots, f_s \rangle = \langle h \rangle$, y $\langle f_1, \ldots, f_s \rangle = \langle f_1, h \rangle$. Otra vez por (i),

$$\mathrm{mcd}(f_1, \ldots, f_s) = \mathrm{mcd}(f_1, h) = \mathrm{mcd}(f_1, \mathrm{mcd}(f_2, \ldots, f_2)).$$

□

Ejemplo 2.3. Busquemos resolver el siguiente sistema de ecuaciones

$$\begin{cases} x^2 - 3x + 2 & = 0 \\ x^3 + x^2 + x - 3 & = 0 \\ 2x^4 - 3x^3 + x^2 + x - 1 & = 0 \end{cases}$$

Consideramos los polinomios $f_1 = x^2 - 3x + 2$, $f_2 = x^3 + x^2 + x - 3$ y $f_3 = 2x^4 - 3x^3 + x^2 + x - 1$. Desde que $\langle f_1, f_2, f_3 \rangle = \langle \mathrm{mcd}(f_1, f_2, f_3) \rangle$, cualquier solución de $\mathrm{mcd}(f_1, f_2, f_3) = 0$ es también una solución para el sistema de ecuaciones original (y viceversa). Luego calculamos $\mathrm{mcd}(f_1, f_2, f_3) = x - 1$ lo que nos da la solución única $x = 1$. Además si desearamos conocer si un polinomio $f \in k[x]$ se encuentra en el ideal $I = \langle f_1, f_2, f_3 \rangle$ bastaría con aplicar el algoritmo de la división a f y $x - 1$, es decir $f \in I \iff f \xrightarrow{x-1} 0$ (los múltiplos de $x - 1$).

2.3 Orden de Monomios en $k[x_1, \ldots, x_n]$

En el caso de polinomios de una variable los hemos ordenado de mayor a menor exponente de la indeterminada, esto nos fue útil para identificar el término principal, coeficiente principal, etc de los polinomios en $k[x]$. Para el caso de polinomios de varias variables definiremos un orden análogo.

Sea

$$M_n = \{x_1^{\beta_1} \cdots x_n^{\beta_n} \mid \beta_i \in \mathbb{N}, i = 1. \ldots, n\}$$

el conjunto de monomios o productos de potencias de $k[x_1, \ldots, x_n]$, a veces denotaremos $x_1^{\beta_1} \ldots x_n^{\beta_n}$ por $\boldsymbol{X}^{\boldsymbol{\beta}}$, donde $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. Hay muchas maneras de ordenar M_n pero es necesario que cumpla algunas propiedades similares al caso de polinomios en una variable como por ejemplo extender las relaciones de divisibilidad, ser un orden total (dados cualquier par de elementos x, y se debe cumplir una de las siguientes condiciones $x < y \vee x = y \vee x > y$) y estar bien ordenado.

Definición 2.15. [ref.[Adams W.], cáp.1, págs.18-19] Por un Orden Monomial en M_n nos referimos a un orden total $<$ que satisface las siguientes dos condiciones:

(i) $1 < \boldsymbol{X}^{\boldsymbol{\beta}}$ para todo $\boldsymbol{X}^{\boldsymbol{\beta}} \in M_n \setminus \{1\}$ (bien-fundado);

(ii) Si $\boldsymbol{X}^{\boldsymbol{\alpha}} < \boldsymbol{X}^{\boldsymbol{\beta}}$, entonces $\boldsymbol{X}^{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\gamma}} < \boldsymbol{X}^{\boldsymbol{\beta}}\boldsymbol{X}^{\boldsymbol{\gamma}}$, para todo $\boldsymbol{X}^{\boldsymbol{\gamma}} \in M_n$ (compatibilidad).

Al conjunto de todos los órdenes monomiales en M_n lo denotaremos por $MO(M_n)$.

El conjunto contable M_n es una base para el k-espacio vectorial $k[x_1, \ldots, x_n]$. Es decir cada polinomio no-nulo $p \in k[x_1, \ldots, x_n]$ puede ser escrito en forma cánonica como una suma

$$\sum_{v \in supp(p)} c_v \mathbf{X}^v$$

para un sub-conjunto finito únicamente determinado $supp(p)$ de $\mathbb{N}^n$ tal que $0 \neq c_v \in k$ para todo $v \in supp(p)$. Además para cada $p \in k[x_1, \ldots, x_n]$ definimos el conjunto

$$Supp(p) := \{\boldsymbol{X}^{\boldsymbol{v}} \in M_n \mid v \in supp(p)\}$$

de los monomios o productos de potencias que aparecen en p, el cual es llamado el soporte de p.

Proposición 2.4. Para $\boldsymbol{X^{\alpha}}, \boldsymbol{X^{\beta}} \in M_n$, si $\boldsymbol{X^{\alpha}}$ divide a $\boldsymbol{X^{\beta}}$ entonces $\boldsymbol{X^{\alpha}} \leq \boldsymbol{X^{\beta}}$.

Prueba. Existe un $\boldsymbol{X^{\gamma}} \in M_n$ tal que $\boldsymbol{X^{\beta}} = \boldsymbol{X^{\alpha}X^{\gamma}}$. Por la condición (i) en la definición 2.15 tenemos $\boldsymbol{X^{\gamma}} \geq 1$ y por la condición (ii) $\boldsymbol{X^{\beta}} = \boldsymbol{X^{\alpha}X^{\gamma}} \geq \boldsymbol{X^{\alpha}}$, lo que concluye la prueba. □

Teorema 2.9 (ref.[Adams W.],cáp.1,pág.21)**.** Todo orden monomial en M_n es un buen orden; es decir, para todo sub-conjunto A de M_n, existe $\boldsymbol{X^{\alpha}} \in A$ tal que para todo $\boldsymbol{X^{\beta}} \in A, \boldsymbol{X^{\alpha}} \leq \boldsymbol{X^{\beta}}$.

Prueba. Supongamos que el orden dado no es un buen orden. Entonces existen $\boldsymbol{X^{\alpha_i}} \in M_n, i = 1, 2, \ldots$ tales que

$$\boldsymbol{X^{\alpha_1}} > \boldsymbol{X^{\alpha_2}} > \boldsymbol{X^{\alpha_3}} > \cdots .$$

Esto define una cadena creciente de ideales en $k[x_1, \ldots, x_n]$

$$\langle \boldsymbol{X^{\alpha_1}} \rangle \subsetneqq \langle \boldsymbol{X^{\alpha_1}}, \boldsymbol{X^{\alpha_2}} \rangle \subsetneqq \langle \boldsymbol{X^{\alpha_1}}, \boldsymbol{X^{\alpha_2}}, \boldsymbol{X^{\alpha_3}} \rangle \subsetneqq \cdots .$$

Notemos que $\langle \boldsymbol{X^{\alpha_1}}, \ldots, \boldsymbol{X^{\alpha_i}} \rangle \neq \langle \boldsymbol{X^{\alpha_1}}, \ldots, \boldsymbol{X^{\alpha_{i+1}}} \rangle$, desde que si ocurriera la igualdad tendríamos

$$\boldsymbol{X^{\alpha_{i+1}}} = \sum_{j=1}^{i} u_j \boldsymbol{X^{\alpha_j}}$$

, donde u_j es un polinomio en $k[x_1, \ldots, x_n], j = 1, \ldots, i$. Si expandimos cada u_j como una combinación lineal de productos de potencia, vemos que cada término en el lado derecho es divisible por algún $\boldsymbol{X^{\alpha_j}}, 1 \leq j \leq i$, entonces $\boldsymbol{X^{\alpha_{i+1}}}$ también es divisible por algún $\boldsymbol{X^{\alpha_j}}$ y $\boldsymbol{X^{\alpha_{i+1}}} \geq \boldsymbol{X^{\alpha_j}}, 1 \leq j \leq i$ por la proposición 2.4 lo cual es una contradicción. Luego la cadena de ideales es estrictamente creciente contradiciendo que $k[x_1, \ldots, x_n]$ es notheriano. □

Definición 2.16 (ref.[Adams W.],cáp.1,pág.19)**.** Definimos el orden lexicográfico (lex) en M_n con $x_1 > x_2 > \cdots > x_n$ como sigue:

$$\text{Para} \quad \boldsymbol{X} = x_1 x_2 \ldots x_n, \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n), \boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$$

definimos $\boldsymbol{X^{\alpha}} < \boldsymbol{X^{\beta}} \iff$ las primeras coordenadas α_i y β_i en $\boldsymbol{\alpha}$ y $\boldsymbol{\beta}$ desde la izquierda que son diferentes cumplen $\alpha_i < \beta_i$.

Por ejemplo en el caso de dos variables x e y con $y > x$ tenemos

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

Definición 2.17 (ref.[Adams W.],cáp.1, pág.19)**.** Definimos el orden de grado lexicográfico (deglex) en M_n con $x_1 > x_2 > \cdots > x_n$ como sigue:

$$\text{Para} \quad \boldsymbol{X} = x_1x_2 \ldots x_n, \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n), \boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$$

definimos $\boldsymbol{X^\alpha} < \boldsymbol{X^\beta} \iff \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ ó $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ y $\boldsymbol{X^\alpha} < \boldsymbol{X^\beta}$ con respecto a lex con $x_1 > x_2 > \cdots > x_n$.

Usando el orden de grado lexicográfico en $k[x, y]$ con $x < y$, tenemos

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

Definición 2.18 (ref.[Adams W.],cáp.1,pág.20)**.** Definiremos el orden reverso de grado lexicográfico (degrevlex) en M_n con $x_1 > x_2 > x_3 > \cdots > x_n$ como sigue:

$$\text{Para} \quad \boldsymbol{X} = x_1x_2 \ldots x_n, \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n), \boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$$

definimos

$$\boldsymbol{X^\alpha} < \boldsymbol{X^\beta} \iff \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ \text{ó} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \quad \text{y las primeras coordenadas} \quad \alpha_i \quad \text{y} \quad \beta_i \quad \text{en} \\ \boldsymbol{\alpha} \quad \text{y} \quad \boldsymbol{\beta} \quad \text{desde la derecha, que son diferentes, satisfacen} \quad \alpha_i > \beta_i. \end{cases}$$

Ejemplo 2.4. En $k[x_1, x_2, x_3]$ con respecto a degrevlex y $x_1 > x_2 > x_3$, tenemos $x_1^2x_2x_3 < x_1x_2^3$.

Nota 2.3. Un polinomio $f \in k[x_1, \ldots, x_n]$ se dice homogéneo en caso el grado total de cada uno de sus términos es el mismo (ejem. $x^2y^2z + xy^4 - z^5$). Sea f un polinomio homogéneo, con el orden degrevlex y $x_1 > x_2 > \cdots > x_n$. Es fácil verificar que x_n divide a f si, y sólo si x_n divide a $\text{lt}(f)$. Además $f \in \langle x_i, \ldots, x_n \rangle$ si, y sólo si $\text{lt}(f) \in \langle x_i, \ldots, x_n \rangle$.

Nota 2.4. En $k[x, y]$, deglex y degrevlex son el mismo orden.

Ejemplo 2.5. Sea $f = 2x^2yz + 3xy^3 - 2x^3$:

1. Si el orden es lex con $x > y > z$, entonces $\mathrm{lt}(f) = -2x^3; \mathrm{lp}(f) = x^3; \mathrm{lc}(f) = -2$;

2. Si el orden es deglex con $x > y > z$, entonces $\mathrm{lt}(f) = 2x^2yz; \mathrm{lp}(f) = x^2yz; \mathrm{lc}(f) = 2$;

3. Si el orden es degrevlex con $x > y > z$, entonces $\mathrm{lt}(f) = 3xy^3; \mathrm{lp}(f) = xy^3; \mathrm{lc}(f) = 3$.

2.4 Algoritmo de la División en $k[x_1, \ldots, x_n]$

La idea básica del algoritmo será la misma que en el caso de los polinomios de una variable: cuando dividamos f por $f_1, \ldots, f_s$ queremos cancelar términos de f usando los términos principales de los $f_i's$ (con lo que los nuevos términos introducidos serían menores a los cancelados) y continuar con este proceso hasta que no sea posible más.

Definición 2.19 (ref.[Adams W.],cáp.1,pág.26)**.** Dados f, g, h en $k[x_1, \ldots, x_n]$, con $g \neq 0$ y fijemos un orden entre los monomios. Decimos que f se reduce a h módulo g en un paso y escribimos

$$f \xrightarrow{g} h,$$

si y sólo si $\mathrm{lp}(g)$ divide a algún término no-nulo X de f y $h = f - \frac{X}{\mathrm{lt}(g)}g$.

Ejemplo 2.6. Sean $f = 2x^3 + x^2y + y^3$, $g = x^2 - xy \in \mathbb{Q}[x, y]$, con el orden lex $x > y$. Escogemos el término $X = 2x^3$ en f y calculamos $h = f - \frac{X}{\mathrm{lt}(g)}g = 2x^3 + x^2y + y^3 - \frac{2x^3}{x^2}(x^2 - xy) = 3x^2y + y^3$.

Ejemplo 2.7. Sean $f = y^2x + 4yx - 3x^2$, $g = 2y + x + 1 \in \mathbb{Q}[x, y]$, con el orden deglex $y > x$. Entonces

$$f \xrightarrow{g} -\frac{1}{2}yx^2 + \frac{7}{2}yx - 3x^2 \xrightarrow{g} \frac{1}{4}x^3 + \frac{7}{2}yx - \frac{11}{4}x^2 \xrightarrow{g} \frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x.$$

En el último polinomio ningún término es divisible por $\mathrm{lp}(g) = y$ y entonces el proceso de división no puede continuar.

Definición 2.20 (ref.[Adams W.],cáp.1,pág.27)**.** Sea f, h, y $f_1, \ldots, f_s$ polinomios en $k[x_1, \ldots, x_n]$, con $f_i \neq 0, 1 \leq i \leq s$, y sea $F = \{f_1, \ldots, f_s\}$. Decimos que f se reduce a h módulo F, escribimos

$$f \xrightarrow{F} h,$$

si y sólo si existe una secuencia de indices $i_1, i_2, \ldots, i_t \in \{1, \ldots, s\}$ y una secuencia de polinomios $h_1, \ldots, h_{t-1} \in k[x_1, \ldots, x_n]$ tal que

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Proposición 2.5. Sea $f \in k[x_1, \ldots, x_n]$.

1. Si $f = 0$ entonces $f \xrightarrow{g} 0$ para todo polinomio no-nulo $g \in k[x_1, \ldots, x_n]$.
2. Sean $0 \neq c \in k$. Entonces $f \xrightarrow{c} 0$.
3. Dado $f \xrightarrow{F} h$ y un monomio X entonces $Xf \xrightarrow{F} Xh$.
4. Sea F un conjunto de polinomios no-nulos, $f \in F$ y $g \in k[x_1, \ldots, x_n]$. Entonces $fg \xrightarrow{F} 0$.

Prueba. (1) Convención.
(2) Desde que estamos considerando k un campo, cualquier término no-nulo en $k[x_1, \ldots, x_n]$ es dividido por c y luego f se reduce a cero usando el polinomio constante c.
(3) Prueba directa.
(4) Prueba directa. □

Ejemplo 2.8. Sean $f = xy^2 + xy + y^2$, $g = xy + y^2$, $\phi = x \in \mathbb{Q}[x, y]$, con el orden deglex $x > y$. Entonces $f \xrightarrow{\phi} xy + y^2 = r$ y $g \xrightarrow{\phi} y^2 = s$ pero $f + g \xrightarrow{\phi} 2xy + 2y^2 \neq r + s$.

Consideremos $f, g_1, g_2 \in k[x_1, \ldots, x_n]$, $G = \{g_1, g_2\}$, con g_1, g_2 no-nulos tales que

$$f \xrightarrow{g_1} h_1 \xrightarrow{g_2} h_2.$$

Entonces de la primera reducción tenemos:

$$h_1 = f - \frac{X_1}{\mathrm{lt}(g_1)} g_1$$

para algún término no-nulo X_1 de f, tal que $\mathrm{lp}(g_1)$ divide a X_1, con

$$\mathrm{lp}(f) = \max(\mathrm{lp}(h_1), \mathrm{lp}(\frac{X_1}{\mathrm{lt}(g_1)})\mathrm{lp}(g_1)).$$

Luego, de la segunda reducción:

$$h_2 = h_1 - \frac{X_2}{\mathrm{lt}(g_2)}g_2$$

para algún término no-nulo X_2 de h_1, tal que $\mathrm{lp}(g_2)$ divide a X_2 con

$$\mathrm{lp}(h_1) = \max(\mathrm{lp}(h_2), \mathrm{lp}(\frac{X_2}{\mathrm{lt}(g_2)})\mathrm{lp}(g_2)).$$

Combinando estas dos últimas expresiones obtenemos

$$f = \frac{X_1}{\mathrm{lt}(g_1)}g_1 + \frac{X_2}{\mathrm{lt}(g_2)}g_2 + h_2 = u_1g_1 + u_2g_2 + h_2,$$

con

$$\mathrm{lp}(f) = \max(\mathrm{lp}(u_1)\mathrm{lp}(g_1), \mathrm{lp}(u_2)\mathrm{lp}(g_2), \mathrm{lp}(h_2)),$$

es decir el proceso de reducción induce una división de f por G. En caso el polinomio h_2 cumpla ciertas condiciones lo llamaremos *resto* de la división de f por G o *reducido* respecto a G.

Definición 2.21 (ref.[Adams W.],cáp.1,pág.27)**.** Un polinomio r es llamado reducido con respecto a un conjunto de polinomios no-nulos $F = \{f_1, \ldots, f_s\}$ si $r = 0$ o ningún producto de potencias $X \in Supp(r)$ es divisible por algún $\mathrm{lp}(f_i), i = 1, \ldots, s$. En otras palabras r no puede reducirse módulo F a otro polinomio no-nulo.

Definición 2.22 (ref.[Adams W.],cáp.1,pág.27)**.** Si $f \xrightarrow{F} r$ y r es reducido respecto a F, entonces llamamos a r un resto para f con respecto a F.

El proceso de reducción ahora nos permite definir un algoritmo de la división que imite al caso de polinomios en una variable.(ref.[Adams W.], cáp.1, pág.28)

Entrada: $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ con $f_i \neq 0 (1 \leq i \leq s)$

Salida: $u_1, \ldots, u_s, r$ tal que $f = u_1f_1 + \cdots + u_sf_s + r$, r es reducido con respecto a $\{f_1, \ldots f_s\}$ y $\max(\mathrm{lp}(u_1)\mathrm{lp}(f_1), \ldots, \mathrm{lp}(u_s)\mathrm{lp}(f_s), \mathrm{lp}(r)) = \mathrm{lp}(f)$.

Inicio: $u_1 := 0, u_2 := 0, \ldots, u_s := 0, r := 0, h := f$

Mientras $h \neq 0$ **Hacer**

Si existen i tales que $\mathrm{lp}(f_i)$ divide a $\mathrm{lp}(h)$

Entonces

escoger alg\'un i

$u_i := u_i + \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_i)}$

$h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_i)} f_i$

Sino

$r := r + \mathrm{lt}(h)$

$h := h - \mathrm{lt}(h)$

Fin Si

Fin Mientras

Algoritmo 2.3: Algoritmo de la división para polinomios multivariables.

Ejemplo 2.9. Sea $F = \{f_1\}$, donde $f_1 = 2y + x + 1 \in \mathbb{Q}[x, y]$. El orden es deglex con $y > x$. Sea $f = y^2x + 4yx - 3x^2$.

Inicio: $u_1 := 0, r := 0, h := y^2x + 4yx - 3x^2$

Primera iteración en el bucle Mientras:

$y = \mathrm{lp}(f_1)$ divide a $\mathrm{lp}(h) = y^2x$

$u_1 := u_1 + \frac{y^2x}{2y} = \frac{1}{2}yx$

$h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_1)} f_1 = (y^2x + 4yx - 3x^2) - \frac{y^2x}{2y}(2y + x + 1)$

$= -\frac{1}{2}yx^2 + \frac{7}{2}yx - 3x^2$

Segunda iteración en el bucle Mientras:

$y = \mathrm{lp}(f_1)$ divide a $\mathrm{lp}(h) = yx^2$

$u_1 := u_1 + \frac{-\frac{1}{2}yx^2}{2y} = \frac{1}{2}yx - \frac{1}{4}x^2$

$h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_1)} f_1 = (-\frac{1}{2}yx^2 + \frac{7}{2}yx - 3x^2) - \frac{-\frac{1}{2}yx^2}{2y}(2y + x + 1)$

$= \frac{1}{4}x^3 + \frac{7}{2}yx - \frac{11}{4}x^2$

Tercera iteración en el bucle Mientras:

$y = \mathrm{lp}(f_1)$ no divide a $\mathrm{lp}(h) = x^3$

$r := r + \mathrm{lt}(h) = \frac{1}{4}x^3$

$h := h - \mathrm{lt}(h) = \frac{7}{2}yx - \frac{11}{4}x^2$

Cuarta iteración en el bucle Mientras:

$y = \mathrm{lp}(f_1)$ divide a $\mathrm{lp}(h) = yx$

$u_1 := u_1 + \frac{\frac{7}{2}yx}{2y} = \frac{1}{2}yx - \frac{1}{4}x^2 + \frac{7}{4}x$

$h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_1)} f_1 = (\frac{7}{2}yx - \frac{11}{4}x^2) - \frac{\frac{7}{2}yx}{2y}(2y + x + 1)$

$= -\frac{9}{2}x^2 - \frac{7}{4}x$

Quinta iteración en el bucle Mientras:

$y = \mathrm{lp}(f_1)$ no divide a $\mathrm{lp}(h) = x^2$

$r := r + \mathrm{lt}(h) = \frac{1}{4}x^3 - \frac{9}{2}x^2$

$h := h - \mathrm{lt}(h) = -\frac{7}{4}x$

Sexta iteración en el bucle Mientras:

$y = \mathrm{lp}(f_1)$ no divide a $\mathrm{lp}(h) = x$

$r := r + \mathrm{lt}(h) = \frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x$

$h := h - \mathrm{lt}(h) = 0$

El bucle Mientras termina, y tenemos

$$f \xrightarrow{F} \frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x$$

y

$$f = (\frac{1}{2}yx - \frac{1}{4}x^2 + \frac{7}{4}x)(2y + x + 1) + (\frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x).$$

Ejemplo 2.10. Sea $F = \{f_1, f_2\}$ donde $f_1 = yx - y$, $f_2 = y^2 - x \in \mathbb{Q}[x, y]$. El orden es deglex con $y > x$. Sea $f = y^2x$.

Inicio: $u_1 := 0; u_2 := 0; r := 0; h := y^2x$

Primera iteración a través del bucle Mientras:

$yx = \mathrm{lp}(f_1)$ divide a $\mathrm{lp}(h) = y^2x$

$u_1 := u_1 + \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_1)} = y$

$h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_1)} f_1 = y^2x - \frac{y^2x}{yx}(yx - y) = y^2$

Segunda iteración a través del bucle Mientras:

$yx = \mathrm{lp}(f_1)$ no divide al $\mathrm{lp}(h) = y^2$

$y^2 = \mathrm{lp}(f_2)$ divide a $\mathrm{lp}(h) = y^2$

$u_2 := u_2 + \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_2)} = 1$

$h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_2)} f_2 = y^2 - \frac{y^2}{y^2}(y^2 - x) = x$

Tercera iteración a través del bucle Mientras:

$yx = \mathrm{lp}(f_1)$ no divide al $\mathrm{lp}(h) = x$

$y^2 = \mathrm{lp}(f_2)$ no divide al $\mathrm{lp}(h) = x$

$r := r + \mathrm{lt}(h) = x$

$h := h - \mathrm{lt}(h) = 0$

Fin Mientras, y obtenemos $f \xrightarrow{F} x$ y $f = yf_1 + f_2 + x$.

Teorema 2.10. [ref.[Adams W.],cáp.1,pág.30] Dado un conjunto de polinomios no-nulos $F = \{f_1, \ldots, f_s\}$ y f en $k[x_1, \ldots, x_n]$, el algoritmo de la división produce polinomios $u_1, \ldots, u_s, r \in k[x_1, \ldots, x_n]$ tales que

$$f = u_1 f_1 + \cdots + u_s f_s + r,$$

con r reducido con respecto a F y

$$\mathrm{lp}(f) = \max(\max_{1 \leq i \leq s}(\mathrm{lp}(u_i)\mathrm{lp}(f_i)), \mathrm{lp}(r)).$$

Además este algoritmo es equivalente a $f \xrightarrow{F} r$.

Prueba. Observemos primero que el algoritmo termina. En cada iteración del algoritmo, el término principal de h es substraído hasta que ya no es más posible. Asi tenemos una secuencia $h_1, h_2, \ldots$ de los $h's$ en el algoritmo donde $\mathrm{lp}(h_{i+1}) < \mathrm{lp}(h_i)$ y, desde que el orden de los términos es bien ordenado, la lista de los h_i's es en realidad finita.

Desde que al comienzo $h = f$, tenemos que en cada iteración del algoritmo $\mathrm{lp}(h) \leq \mathrm{lp}(f)$. Ahora, para cada i, obtenemos u_i agregando términos $\frac{\mathrm{lt}(h)}{\mathrm{lt}(f_i)}$, entonces $\mathrm{lp}(u_i)\mathrm{lp}(f_i) \leq \mathrm{lp}(f)$. Además, r es obtenido al agregar $\mathrm{lt}(h)$ y entonces $\mathrm{lp}(r) \leq \mathrm{lp}(f)$, lo que concluye la prueba. □

Con f escrito como en el teorema anterior, tenemos $f - r \in \langle f_1, \ldots, f_s \rangle$. Luego, si $r = 0$, entonces $f \in \langle f_1, \ldots, f_s \rangle$. Sin embargo el recíproco no es necesariamente cierto; es decir f puede estar en el ideal $\langle f_1, \ldots, f_s \rangle$ pero el resto de la división de f por $f_1, \ldots, f_s$ no ser cero como comprobaremos en el siguiente ejemplo.

Ejemplo 2.11. Sea $f = y^2x - x \in \mathbb{Q}[x, y]$, y el ideal $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y]$, donde $f_1 = yx - y, f_2 = y^2 - x$. Sea $F = \{f_1, f_2\}$. Usando el orden deglex con $y > x$ y el algoritmo de la división, vemos que $f \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0$, es decir, $f \xrightarrow{F} 0$ y, $f = yf_1 + f_2 \in I$. Sin embargo si usamos f_2 primero en el algoritmo de la división entonces $f \xrightarrow{f_2} x^2 - x$, y $x^2 - x$ es reducido con respecto a F. Luego el resto de la división de f por F es no-nulo, pero f si está en el ideal $\langle f_1, f_2 \rangle$.

Esta dificultad ya se presentaba en el caso de polinomios de una sola indeterminada. Por ejemplo, si $f = x, f_1 = x^2$ y $f_2 = x^2 - x$, entonces f es reducido con respecto a $\{f_1, f_2\}$, con $f = f_1 - f_2 \in \langle f_1, f_2 \rangle$. Esto se resolvió encontrando un mejor generador para el ideal $\langle f_1, f_2 \rangle$, es decir $x = \text{mcd}(x^2, x^2 - x)$. Para el caso de un ideal en $k[x_1, \ldots, x_n]$ su mejor conjunto generador será definido como una base de Gröbner.

2.5 Bases de Gröbner

En esta sección definiremos el objeto más importante de la presente tesis, las bases de Gröbner. Esta definición está inspirada en el último comentario de la sección anterior, es decir la existencia de restos no-nulos producidos por el algoritmo 2.3.

Definición 2.23. [ref.[Adams W.],cáp.1,pág.32] Un conjunto de polinomios no-nulos $G = \{g_1, \ldots, g_t\}$ contenidos en un ideal I, es llamado una base de Gröbner[1] para I si y sólo si para todo $0 \neq f \in I$ existe $i \in \{1, \ldots, t\}$ tal que $\text{lp}(g_i)$ divide a $\text{lp}(f)$.

En otras palabras, si G es una base de Gröbner para I, entonces el único polinomio en I reducido respecto a G es 0.

Proposición 2.6. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para un ideal I.

1. Para cualquier sub-conjunto finito de polinomios no-nulos F de I , $G \cup F$ también es una base de Gröbner de I.

2. Sean $c_1, \ldots, c_t \in k$ arbitrarios pero no-nulos. Se cumple que $\{c_1 g_1, \ldots, c_t g_t\}$ también es una base de Gröbner para I.

Prueba. Se sigue directamente de la definición 2.23. □

Para un sub-conjunto no vacío S de $k[x_1, \ldots, x_n]$, definimos el ideal de términos principales de S como el ideal

$$\text{Lt}(S) = \langle \text{lt}(s) \mid s \in S \rangle.$$

[1] También denominada Base Standard.

Teorema 2.11. [ref.[Adams W.],cáp.1,pág.32-33] Sea I un ideal no-nulo de $k[x_1, \ldots, x_n]$. Los siguientes enunciados son equivalentes para un conjunto de polinomios no-nulos $G = \{g_1, \ldots, g_t\} \subset I$.

(i) G es una base de Gröbner para I.

(ii) $f \in I$ si y sólo si $f \xrightarrow{G} 0$.

(iii) $f \in I$ si y sólo si $f = \sum_{i=1}^{t} h_i g_i$, con $\mathrm{lp}(f) = \max_{1 \leq i \leq t}(\mathrm{lp}(h_i)\mathrm{lp}(g_i))$.

(iv) $\mathrm{Lt}(G) = \mathrm{Lt}(I)$.

Prueba. $(i) \implies (ii)$. Sea $f \in k[x_1, \ldots, x_n]$. Entonces por el Teorema 2.10 existe $r \in k[x_1, \ldots, x_n]$ reducido con respecto a G, tal que $f \xrightarrow{G} r$. Si $f \in I$, $r \in I$, $r = 0$ y si $r = 0$, $f \in I$.
$(ii) \implies (iii)$. Desde que el algoritmo de la división esta basado en el proceso de reducción.
$(iii) \implies (iv)$. Por hipótesis tenemos

$$\mathrm{lt}(f) = \sum_i \mathrm{lt}(h_i)\mathrm{lt}(g_i),$$

donde la suma es sobre los i tales que $\mathrm{lp}(f) = \mathrm{lp}(h_i)\mathrm{lp}(g_i)$.
$(iv) \implies (i)$ Sea $f \in I$. Entonces

$$\mathrm{lt}(f) = \sum_{i=1}^{t} h_i \mathrm{lt}(g_i),$$

para algunos $h_i \in k[x_1, \ldots, x_n]$. Si expandimos los términos a la derecha notaremos que cada término es divisible por algún $\mathrm{lp}(g_i)$, por tanto $\mathrm{lp}(f)$ también es divisible por algún $\mathrm{lp}(g_i)$. □

Corolario 2.2. Si $G = \{g_1, \ldots, g_t\}$ es una base de Gröbner para el ideal I, entonces $I = \langle g_1, \ldots, g_t \rangle$.

Lema 2.2 (Dickson)**.** Sea I un ideal generado por un conjunto S de términos no-nulos, y sea $f \in k[x_1, \ldots, x_n]$. Entonces f está en I si y sólo si para todo término X que aparece en f existe un $Y \in S$ tal que Y divide a X. Además, existe un sub-conjunto finito S_0 de S tal que $I = \langle S_0 \rangle$.

Prueba. Si $f \in I$, entonces

$$f = \sum_{i=1}^{l} h_i X_i,$$

donde $h_i \in k[x_1, \ldots, x_n]$ y $X_i \in S$, para $i = 1, \ldots, l$. Expandiendo el lado derecho vemos que cada término que aparece será divisible por algún X_i y entonces también cada término en f.

Conversamente si para cada término X de f es dividido por algún $Y \in S$, entonces claramente $f \in \langle S \rangle = I$.

Para probar la última afirmación, desde que $k[x_1, \ldots, x_n]$ es notheriano I tiene un conjunto finito que lo genera. Luego por la primera parte del lema cada término de cada uno de los miembros de este conjunto finito es divisible por algún elemento de S. Sea S_0 el conjunto finito de estos divisores, entonces $I = \langle S_0 \rangle$. □

Corolario 2.3. Todo ideal no-nulo I de $k[x_1, \ldots, x_n]$ tiene una base de Gröbner.

Prueba. Por el lema anterior el ideal de términos principales $\mathrm{Lt}(I)$ tiene un conjunto finito que lo genera, escribamos $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)$ con $g_1, \ldots, g_t \in I$. Sea $G = \{g_1, \ldots, g_t\}$, entonces $\mathrm{Lt}(G) = \mathrm{Lt}(I)$ lo que concluye la prueba por la parte (iv) del teorema 2.11. □

Definición 2.24. Decimos que un sub-conjunto $G = \{g_1, \ldots, g_t\}$ de $k[x_1, \ldots, x_n]$ es una base de Gröbner si y sólo si es una base Gröbner para el ideal que genera $\langle G \rangle$.

Proposición 2.7. Para $\{g_1, \ldots, g_t\} \subseteq k[x_1, \ldots, x_n]$ y $0 \neq h \in k[x_1, \ldots, x_n]$, se tiene que $\{g_1, \ldots, g_t\}$ es una base de Gröbner si y sólo si $\{hg_1, \ldots, hg_t\}$ es una base de Gröbner.

Prueba. Se sigue directamente de la definición 2.23. □

Teorema 2.12. [ref.[Adams W.],cáp.1,pág.34] Sea $G = \{g_1, \ldots, g_t\}$ un conjunto de polinomios no-nulos en $k[x_1, \ldots, x_n]$. Entonces G es una base de Gröbner si y sólo si para todo $f \in k[x_1, \ldots, x_n]$, el resto de la división de f por G es único.

Prueba. Primero asumamos que G es una base de Gröbner. Sea $f \xrightarrow{G} r_1$ y $f \xrightarrow{G} r_2$ con r_1 y r_2 reducidos con respecto a G. Desde que $f - r_1$ y $f - r_2$ están ambos en $\langle G \rangle$, también $r_1 - r_2$. Además $r_1 - r_2$ es reducido con respecto a G, luego $r_1 - r_2 = 0$.

Conversamente, asumamos que los restos de las divisiones por G son únicos. Probaremos la condición (ii) en el Teorema 2.11.

Sea $f \in \langle G \rangle$, supongamos que $f \xrightarrow{G} r$ tal que r es reducido.

Afirmación: Si $c \in k$ es no-nulo, $X \in M_n$ un producto de potencias, y $g \in k[x_1, \ldots, x_n]$ es tal que $g \xrightarrow{G} r$, donde r es reducido, entonces, para cada $i \in 1, \ldots, t, \quad g - cXg_i \xrightarrow{G} r$.

Veamos que si nuestra afirmación es verdadera la prueba estaría completa. Desde que $f \in \langle G \rangle$ podemos escribir $f = \sum_{v=1}^{l} c_v X_v g_{i_v}$, donde los c_v son no-nulos y están en k y $X_v \in M_n$ y $i_v \in 1, \ldots, t$. Entonces aplicamos nuestra afirmación con $g = f$, $f - c_1 X_1 g_{i_1} \xrightarrow{G} r$. Luego para $g = f - c_1 X_1 g_{i_1}$ en nuestra afirmación, $f - c_1 X_1 g_{i_1} - c_2 X_2 g_{i_2} \xrightarrow{G} r$. Continuando con este procedimiento, $0 = f - \sum_{v=1}^{l} c_v X_v g_{i_v} \xrightarrow{G} r$. Por tanto $r = 0$.

Prueba de la afirmación: Definamos d tal que $d\mathrm{lc}(g_i)$ sea el coeficiente de $X\mathrm{lp}(g_i)$ en g.

Caso 1. $d = 0$.Entonces el coeficiente de $X\mathrm{lp}(g_i)$ en $g - cXg_i$ es $-c\mathrm{lc}(g_i) \neq 0$ y entonces $g = (g - cXg_i) - (-cXg_i) = (g - cXg_i) - \frac{Y}{\mathrm{lt}(g_i)} g_i$ donde $Y = -c\mathrm{lc}(g_i) X\mathrm{lp}(g_i)$, es decir $g - cXg_i \xrightarrow{g_i} g \xrightarrow{G} r$.

Caso 2. $d = c$. Asumamos $g - cXg_i \xrightarrow{G} r_1$ con r_1 reducido. Entonces, desde que $d = c \neq 0$ tenemos $g \xrightarrow{g_i} g - cXg_i \xrightarrow{G} r_1$. Luego $r = r_1$.

Caso 3. $d \neq 0$ y $d \neq c$. Sea $h = g - dXg_i$. Entonces el coeficiente de $X\mathrm{lp}(g_i)$ en h es 0. Desde que $d \neq 0$, $g \xrightarrow{g_i} h$. También, desde que $d \neq c$ tenemos $g - cXg_i \xrightarrow{g_i} h$. Luego si $h \xrightarrow{G} r_2$ con r_2 reducido, $g \xrightarrow{g_i} h \xrightarrow{G} r_2$ y entonces $r = r_2$. Finalmente $g - cXg_i \xrightarrow{g_i} h \xrightarrow{G} r$.

□

De la prueba del teorema anterior notamos que dados $f \in k[x_1, \ldots, x_n]$ y G_1, G_2 dos bases de Gröbner para un ideal I se cumple $f \xrightarrow{G_1} r_1$ y $f \xrightarrow{G_2} r_2$ implica $r_1 = r_2$.

Ejemplo 2.12. Sea $f = y^2x - x$, $f_1 = yx - y$ y $f_2 = y^2 - x$. Sea $F = \{f_1, f_2\}$. Usaremos el orden deglex con $y > x$. Entonces (ejemplo 2.11) $f \xrightarrow{F} 0$ y $f \xrightarrow{F} x^2 - x$, el último resto siendo reducido respecto a F. Así por el teorema 2.12, F no es una base de Gröbner. Podemos verificar esto de otra manera. Desde que $f = yf_1 + f_2 \in \langle f_1, f_2 \rangle$ y $f \xrightarrow{F} x^2 - x$ tenemos que $x^2 - x \in \langle f_1, f_2 \rangle$. Pero $x^2 = \mathrm{lp}(x^2 - x)$ no es divisible por $\mathrm{lp}(f_1) = xy$ ni por $\mathrm{lp}(f_2) = y^2$. Así por la defínción 2.23, F no es una base de Gröbner.

Ejemplo 2.13. Consideremos los polinomios $g_1 = z + x$, $g_2 = y - x \in \mathbb{Q}[x, y, z]$. Sea $G = \{g_1, g_2\}$, $I = \langle g_1, g_2 \rangle$. Usaremos el orden lex en $\mathbb{Q}[x, y, z]$ con $z > y > x$. Probaremos que G es una base de Gröbner para I. Supongamos por el contrario que existe un $f \in I$ tal que $\mathrm{lt}(f) \notin \langle \mathrm{lt}(g_1), \mathrm{lt}(g_2) \rangle = \langle z, y \rangle$. Entonces, z e y no dividen al $\mathrm{lt}(f)$ y, por el orden lex $z > y > x$, $f \in \mathbb{Q}[x]$. Sea $f = (z + x)h_1 + (y - x)h_2$, donde $h_1, h_2 \in \mathbb{Q}[x, y, z]$. Haciendo $y = x$, $f = (z + x)h_1(x, x, z)$, luego $(z + x)$ divide a f lo cual es una contradicción.

Ejemplo 2.14. Con el orden lex y con $x > y > z$ en el ejemplo 2.13, tenemos que $\{g_1, g_2\}$ no forman una base de Gröbner para I. Desde que $g_1 + g_2 = z + y \in I$ no es divisible por $\mathrm{lp}(g_1) = \mathrm{lp}(g_2) = x$.

2.6 S-Polinomios y El Algoritmo de Buchberger

En esta sección finalmente expondremos el algoritmo de Buchberger para calcular bases de Gröbner. Con el fin de entender mejor el funcionamiento de este algoritmo, para los ejemplos de esta sección (así como en toda esta tesis) los cálculos son realizados explícitamente sin necesidad de recurrir a algún software matemático (Como por ejemplo Maple,CoCoA,Macaulay2,etc).

Definamos el mínimo común múltiplo **mcm** y el máximo común divisor **mcd** de dos monomios $X = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ e $Y = x_1^{\beta_1} \dots x_n^{\beta_n}$ en $k[x_1, \dots, x_n]$, de la siguiente forma:

$$\mathrm{mcm}(X, Y) = x_1^{\gamma_1} \dots x_n^{\gamma_n},$$

$$\mathrm{mcd}(X, Y) = x_1^{\delta_1} \dots x_n^{\delta_n},$$

donde $\gamma_i = \max(\alpha_i, \beta_i)$, $\delta_i = \min(\alpha_i, \beta_i)$ para todo $i \in \{1, \dots, n\}$. En caso dos monomios X e Y cumplen $\mathrm{mcd}(X, Y) = 1$ se les llama relativamente primos.

Definición 2.25 (ref.[Adams W.],cáp.1,pág.40)**.** Sean $f, g \in k[x_1, \dots, x_n] \setminus \{0\}$, y $L = \mathrm{mcm}(\mathrm{lp}(f), \mathrm{lp}(g))$. Al polinomio

$$S(f, g) = \frac{L}{\mathrm{lt}(f)} f - \frac{L}{\mathrm{lt}(g)} g$$

se le llama S-polinomio de f y g.

En la división de un polinomio f por $f_1, \ldots, f_s$, puede ocurrir que un término X de f sea divisible por $\mathrm{lp}(f_i)$ y $\mathrm{lp}(f_j)$ para $i \neq j$ (luego X es divisible por $L = \mathrm{mcm}(\mathrm{lp}(f_i), \mathrm{lp}(f_j)))$. Si reducimos f usando f_i obtenemos $h_1 = f - \frac{X}{\mathrm{lt}(f_i)} f_i$ y si reducimos f usando f_j obtenemos $h_2 = f - \frac{X}{\mathrm{lt}(f_j)} f_j$. La ambigüedad introducida puede ser escrita $h_2 - h_1 = \frac{X}{\mathrm{lt}(f_i)} f_i - \frac{X}{\mathrm{lt}(f_j)} f_j = \frac{X}{L} S(f_i, f_j)$.

Ejemplo 2.15. Sea $f = 2yx - y$, $g = 3y^2 - x \in \mathbb{Q}[x, y]$, con el orden deglex con $y > x$. Entonces $L = y^2x$, y $S(f, g) = \frac{y^2x}{2yx} f - \frac{y^2x}{3y^2} g = \frac{1}{2} yf - \frac{1}{3} xg = -\frac{1}{2} y^2 + \frac{1}{3} x^2$. Además $\mathrm{lp}(\frac{1}{2} yf) = y^2x = \mathrm{lp}(\frac{1}{3} xg)$ se han cancelado en $S(f, g)$.

Ejemplo 2.16. Sea $f = y^2x + 1, f_1 = yx - y, f_2 = y^2 - x \in \mathbb{Q}[x, y]$ con el orden deglex con $y > x$. Consideremos el término $X = y^2x$ en f. Tenemos que $f \xrightarrow{f_1} y^2 + 1 = f - yf_1$, y $f \xrightarrow{f_2} x^2 + 1 = f - xf_2$. Notemos que $X = L = \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_2)) = y^2x$, y que la ambigüedad introducida es $-y^2 + x^2 = yf_1 - xf_2 = S(f_1, f_2)$. También notemos que $S(f_1, f_2) \in \langle f_1, f_2 \rangle$, y que puede ser reducido: $S(f_1, f_2) \xrightarrow{f_2} x^2 - x$. El polinomio $x^2 - x$ es reducido con respecto a $\{f_1, f_2\}$, pero no es cero.

Proposición 2.8. Se cumple:

1. En caso f y g son dos términos no-nulos, es decir $0 \neq f = \mathrm{lt}(f)$ y $0 \neq g = \mathrm{lt}(g)$, entonces $S(f, g) = 0$.

2. Sean $f, g \in k[x_1, \ldots, x_n]/\{0\}$. Entonces $S(f, g) = S(f, -g)$.

Lema 2.3. Sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ tales que $\mathrm{lp}(f_i) = X \neq 0$ para todo $i = 1, \ldots, s$. Sea $f = \sum_{i=1}^{s} c_i f_i, \quad c_i \in k, i = 1, \ldots, s$. Si $\mathrm{lp}(f) < X$, entonces f es una combinación lineal, con coeficientes en k, de los $S(f_i, f_j), 1 \leq i < j \leq s$.

Prueba. Escribamos $f_i = a_i X$+términos de menor grado, $a_i \in k$. Desde que $\mathrm{lp}(f) < X$, tenemos $\sum_{i=1}^{s} c_i a_i = 0$. Ahora $S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j$. Así

$$
\begin{aligned}
f &= c_1 f_1 + \cdots + c_s f_s \\
&= c_1 a_1 (\frac{1}{a_1} f_1) + \cdots + c_s a_s (\frac{1}{a_s} f_s) \\
&= c_1 a_1 (\frac{1}{a_1} f_1 - \frac{1}{a_2} f_2) + (c_1 a_1 + c_2 a_2)(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3) + \cdots + (c_1 a_1 + \cdots \\
&\cdots + c_{s-1} a_{s-1})(\frac{1}{a_{s-1}} f_{s-1} - \frac{1}{a_s} f_s) + (c_1 a_1 + \cdots + c_s a_s) \frac{1}{a_s} f_s
\end{aligned}
$$

$$= c_1a_1S(f_1, f_2) + (c_1a_1 + c_2a_2)S(f_2, f_3) + \cdots + (c_1a_1 + \cdots + c_{s-1}a_{s-1})S(f_{s-1}, f_s).$$

□

Teorema 2.13 (Buchberger)**.** [ref.[Adams W.],cáp.1,pág.40] Sea $G = \{g_1, \ldots, g_t\}$ un conjunto de polinomios no-nulos en $k[x_1, \ldots, x_n]$. Entonces G es una base de Gröbner para el ideal $I = \langle g_1, \ldots, g_t\rangle$ si y sólo si para todo $i \neq j$,

$$S(g_i, g_j) \xrightarrow{G} 0.$$

Prueba. ($\Longrightarrow$) Desde que los $S(g_i, g_j)$ están en I y por el teorema 2.11.
($\Longleftarrow$) Usaremos (iii) del teorema 2.11 para probar que G es una base de Gröbner para I. Sea $f \in I$. Entonces f puede ser expresado de muchas maneras como una combinación lineal de los g_i's. Escogemos $f = \sum_{i=1}^{t} h_i g_i$, con

$$X = \max_{1\leq i\leq t} \mathrm{lp}(h_i)lp(g_i)$$

mínimo (por la propiedad del buen-orden). Si $X = \mathrm{lp}(f)$ la prueba está completa. Asumamos, $\mathrm{lp}(f) < X$. Encontraremos una representación para f con un menor X lo cual será una contradicción. Sea $S = \{i \mid \mathrm{lp}(h_i)\mathrm{lp}(g_i) = X\}$. Para $i \in S$, escribamos $h_i = c_iX_i +$ términos de menor grado, donde $X_i = \mathrm{lp}(h_i)$ y los c_i están en k. Sea $g = \sum_{i\in S} c_iX_ig_i$. Entonces, $\mathrm{lp}(X_ig_i) = X$, para todo $i \in S$, y $\mathrm{lp}(g) < X$ (desde que $\mathrm{lp}(g) = X$ implica $\mathrm{lp}(f) = X$). Por el lema 2.3, existen $d_{ij} \in k$ tales que

$$g = \sum_{i,j\in S, i\neq j} d_{ij}S(X_ig_i, X_jg_j).$$

Ahora, se tiene $\mathrm{mcm}(\mathrm{lp}(X_ig_i), \mathrm{lp}(X_jg_j)) = X$, entonces

$$\begin{aligned} S(X_ig_i, X_jg_j) &= \frac{X}{\mathrm{lt}(X_ig_i)}X_ig_i - \frac{X}{\mathrm{lt}(X_jg_j)}X_jg_j \\ &= \frac{X}{\mathrm{lt}(g_i)}g_i - \frac{X}{\mathrm{lt}(g_j)}g_j = \frac{X}{X_{ij}}S(g_i, g_j), \end{aligned}$$

donde $X_{ij} = \mathrm{mcm}(\mathrm{lp}(g_i), \mathrm{lp}(g_j))$. Luego por hipótesis, $S(X_ig_i, X_jg_j) \xrightarrow{G} 0$. Esto nos da una representación

$$S(X_ig_i, X_jg_j) = \sum_{v=1}^{t} h_{ijv}g_v,$$

donde por el teorema 2.10,

$$\max_{1\leq v\leq t}(\mathrm{lp}(h_{ijv})\mathrm{lp}(g_v)) = \mathrm{lp}(S(X_ig_i, X_jg_j))$$

$$= \mathrm{lp}(\frac{X}{\mathrm{lt}(X_i g_i)} X_i g_i - \frac{X}{\mathrm{lt}(X_j g_j)} X_j g_j) < X$$

Substituyendo estas expresiones en $g = \sum_{i \in S} c_i X_i g_i$ y luego en $f = \sum_{i \in S} h_i g_i +$ términos de menor orden que X, obtenemos $f = \sum_{i=1}^{t} h'_i g_i$, con $\max_{1 \leq i \leq t}(\mathrm{lp}(h'_i)\mathrm{lp}(g_i)) < X$. □

Corolario 2.4. Sea $G = \{g_1, \ldots, g_t\}$ con $g_i \neq 0, 1 \leq i \leq t$. Entonces G es una base de Gröbner si y sólo si para todo $i \neq j, \quad 1 \leq i, j \leq t$, tenemos

$$S(g_i, g_j) = \sum_{v=1}^{t} h_{ijv} g_v, \quad \text{donde} \quad \mathrm{lp}(S(g_i, g_j)) = \max_{1 \leq v \leq t}(\mathrm{lp}(h_{ijv})\mathrm{lp}(g_v)).$$

Prueba. De $S(X_i g_i, X_j g_j) = \frac{X}{X_{ij}} S(g_i, g_j)$ en la prueba del teorema anterior. □

El teorema 2.13 nos da una estrategia para calcular bases de Gröbner para un ideal a partir de cualquier conjunto finito de generadores de este. Es decir, calcular los S-polinomios de los polinomios en el conjunto generador, reducirlos y si el resto es no-nulo, agregarlo a la lista de polinomios en el conjunto generador; repetir esto hasta que hayan suficientes polinomios tales que todos los S-polinomios correspondientes se reducen a cero.

Entrada: $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$ con $f_i \neq 0, 1 \leq i \leq s$
Salida: $G = \{g_1, \ldots, g_t\}$ una base de Grobner para $\langle f_1, \ldots, f_s \rangle$
Inicio: $G := F, \quad \mathcal{G} := \{\{f_i, f_j\} \mid f_i \neq f_j \in G\}$
Mientras $\mathcal{G} \neq \emptyset$ **Hacer**
    Escoger cualquier par $\{f, g\} \in \mathcal{G}$
    $\mathcal{G} := \mathcal{G} - \{\{f, g\}\}$
    $S(f, g) \xrightarrow{G} h$, donde h es reducido respecto a G
    Si $h \neq 0$ **Entonces**
        $\mathcal{G} := \mathcal{G} \cup \{\{u, h\} \mid \forall u \in G\}$
        $G := G \cup \{h\}$
    Fin Si
Fin Mientras

Algoritmo 2.4: Algoritmo de Buchberger para calcular Bases de Gröbner.

Teorema 2.14 (ref.[Adams W.],cáp.1,pág.42)**.** Dado $F = \{f_1, \ldots, f_s\}$ con $f_i \neq 0, \forall 1 \leq i \leq s$. El algoritmo de Buchberger produce una base de Gröbner para el ideal $I = \langle f_1, \ldots, f_s \rangle$.

Prueba. Empezemos por probar que el algoritmo termina. Cada G_i es obtenido de G_{i-1} al agregar un $h \in I$ a G_{i-1}, donde h es la reducción no-nula, con respecto a G_{i-1}, de un S-polinomio de dos elementos de G_{i-1}. Desde que h es reducido con respecto a G_{i-1}, tenemos que $\mathrm{lt}(h) \notin \mathrm{Lt}(G_{i-1})$. Así, en caso el algoritmo fuera infinito:

$$\mathrm{Lt}(G_1) \subsetneqq \mathrm{Lt}(G_2) \subsetneqq \mathrm{Lt}(G_3) \subsetneqq \ldots.$$

sería una cadena de ideales estrictamente creciente contradiciendo el hecho que $k[x_1, \ldots, x_n]$ es notheriano.
Ahora $F \subseteq G \subseteq I$, luego $I = \langle f_1, \ldots, f_s \rangle \subseteq \langle g_1, \ldots, g_t \rangle \subseteq I$. Además si g_i, g_j son polinomios en G, entonces $S(g_i, g_j) \xrightarrow{G} 0$ por construcción. □

Ejemplo 2.17. Sea $f_1 = xy - x$,$f_2 = -y + x^2 \in \mathbb{Q}[x, y]$ con el orden lex, $x < y$.
Inicio: $G := \{f_1, f_2\}, \mathcal{G} := \{\{f_1, f_2\}\}$
Primera iteración a través del bucle Mientras
$\mathcal{G} := \emptyset$
$S(f_1, f_2) = (xy - x) - \frac{xy}{-y}(-y + x^2) = x^3 - x = h$ (reducido con respecto a G)
Desde que $0 \neq h$, sea $f_3 := x^3 - x$
$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$
$G := \{f_1, f_2, f_3\}$
Segunda iteración a través del bucle Mientras
$\mathcal{G} := \{\{f_2, f_3\}\}$
$S(f_1, f_3) = x^2(xy - x) - y(x^3 - x) = xy - x^3 \xrightarrow{f_2} 0$
$S(f_1, f_3) \xrightarrow{G} 0 = h$
Tercera iteración a través del bucle Mientras
$\mathcal{G} := \emptyset$
$S(f_2, f_3) = \frac{x^3 y}{-y}(-y + x^2) - y(x^3 - x) = xy - x^5 \xrightarrow{f_2} -x^5 + x^3 \xrightarrow{f_3} 0$
Fin Mientras, desde que $\mathcal{G} = \emptyset$.
Así $\{xy - x, -y + x^2, x^3 - x\}$ es una base de Gröbner para el ideal $\langle xy - x, -y + x^2 \rangle$.

Ejemplo 2.18. Sea $f_1 = y^2 + yx + x^2$, $f_2 = y + x$, y $f_3 = y \in \mathbb{Q}[x, y]$. Usaremos el orden lex con $y > x$ para computar una base de Gröbner para $I = \langle f_1, f_2, f_3 \rangle$.

Inicio: $G := \{f_1, f_2, f_3\}$

$\mathcal{G} := \{\{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}\}$

Primera iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$S(f_1, f_2) = (y^2 + yx + x^2) - y(y + x) = x^2$ (reducido con respecto a $\{f_1, f_2, f_3\}$)

Sea $f_4 := x^2$

$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$G := \{f_1, f_2, f_3, f_4\}$

Segunda iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$S(f_1, f_3) = (y^2 + yx + x^2) - y(y) = yx + x^2 \xrightarrow{f_2} 0$

Tercera iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$S(f_2, f_3) = (y + x) - x = x$ reducido con respecto a G

$f_5 := x$

$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$G := \{f_1, f_2, f_3, f_4, f_5\}$

Cuarta iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$S(f_1, f_4) = x^2(y^2 + yx + x^2) - y^2(x^2) = x^3y + x^4 \xrightarrow{f_2} 0$

Quinta iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$S(f_2, f_4) = x^2(y + x) - y(x^2) = x^3 \xrightarrow{f_5} 0$

Desde que f_3, f_4, f_5 son monomios, entonces $S(f_3, f_4) = S(f_3, f_5) = S(f_4, f_5) = 0$.

$S(f_1, f_5) = x(y^2 + yx + x^2) - y^2(x) = yx^2 + x^3 \xrightarrow{f_3} x^3 \xrightarrow{f_4} 0$

$S(f_2, f_5) = x(y + x) - y(x) = x^2 \xrightarrow{f_4} 0$

Así $\{y^2 + yx + x^2, y + x, y, x^2, x\}$ es una base de Gröbner para el ideal $\langle y^2 + yx + x^2, y + x, y \rangle$.

Ejemplo 2.19. En este ejemplo consideraremos el campo $k = \mathbb{Z}_5 = \mathbb{Z}/5\mathbb{Z}$. Sean

$f_1 = x^2 + y^2 + 1$ y $f_2 = x^2y + 2xy + x$ en $\mathbb{Z}_5[x, y]$. Usaremos el orden lex con $x > y$ para computar las bases de Gröbner para $I = \langle f_1, f_2 \rangle \subsetneqq \mathbb{Z}_5[x, y]$.

Inicio: $G := \{f_1, f_2\}$,$\mathcal{G} := \{\{f_1, f_2\}\}$

Primera iteración a través del bucle Mientras

$\mathcal{G} := \emptyset$

$S(f_1, f_2) = yf_1 - f_2 = 3xy + 4x + y^3 + y$ reducido con respecto a G.

Sea $f_3 := 3xy + 4x + y^3 + y$

$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$G := \{f_1, f_2, f_3\}$

Segunda iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_2, f_3\}\}$

$$\begin{aligned} S(f_1, f_3) = yf_1 - 2xf_3 &= 2x^2 + 3xy^3 + 3xy + y^3 + y \\ &\xrightarrow{f_1} 3xy^3 + 3xy + y^3 - 2y^2 + y - 2 \\ &\xrightarrow{f_3} 6xy^2 + 3xy - y^5 - 2y^2 + y - 2 \\ &\xrightarrow{f_3} 4y^5 + 3y^4 + y^2 + y + 3 \end{aligned}$$

Sea $f_4 := 4y^5 + 3y^4 + y^2 + y + 3$ reducido con respecto a G

$\mathcal{G} := \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$G := \{f_1, f_2, f_3, f_4\}$.

Tercera iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$$\begin{aligned} S(f_2, f_3) &= (x^2y + 2xy + x) - \frac{x}{3}(3xy + 4x + y^3 + y) \\ &= -\frac{4}{3}x^2 - \frac{1}{3}xy^3 + \frac{5}{3}xy + x = -3x^2 - 2xy^3 + x \\ &\xrightarrow{f_1} -2xy^3 + x + 3y^2 + 3 \\ &\xrightarrow{f_3} -4xy^2 + x - y^5 - y^3 + 3y^2 + 3 \\ &\xrightarrow{f_3} -8xy + x - y^5 - 2y^4 - y^3 + y^2 + 3 \\ &\xrightarrow{f_3} -y^5 - 2y^4 + y^2 + y + 3 \xrightarrow{f_4} 0 \end{aligned}$$

Cuarta iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_2, f_4\}, \{f_3, f_4\}\}$

$$S(f_1, f_4) = y^5(x^2 + y^2 + 1) - \frac{1}{4}x^2(4y^5 + 3y^4 + y^2 + y + 3)$$

$$
\begin{aligned}
&= -\frac{3}{4}x^2y^4 - \frac{1}{4}x^2y^2 - \frac{1}{4}x^2y - \frac{3}{4}x^2 + y^7 + y^5 \\
&= -2x^2y^4 + x^2y^2 + x^2y - 2x^2 + y^7 + y^5 \\
&\xrightarrow{f_1} x^2y^2 + x^2y - 2x^2 + y^7 - 3y^6 + y^5 - 3y^4 \\
&\xrightarrow{f_1} x^2y - 2x^2 + y^7 - 3y^6 + y^5 - 4y^4 - y^2 \\
&\xrightarrow{f_1} -2x^2 + y^7 - 3y^6 + y^5 - 4y^4 - y^3 - y^2 - y \\
&\xrightarrow{f_1} y^7 - 3y^6 + y^5 - 4y^4 - y^3 + y^2 - y + 2 \\
&\xrightarrow{f_4} y^5 - 3y^4 + 4y^2 - y + 2 \xrightarrow{f_4} 0.
\end{aligned}
$$

Quinta iteración a través del bucle Mientras

$\mathcal{G} := \{\{f_3, f_4\}\}$

$$
\begin{aligned}
S(f_2, f_4) &= y^4(x^2y + 2xy + x) - \frac{1}{4}x^2(4y^5 + 3y^4 + y^2 + y + 3) \\
&= 3x^2y^4 + x^2y^2 + x^2y + 3x^2 + 2xy^5 + xy^4 \\
&\xrightarrow{f_1} x^2y^2 + x^2y + 3x^2 + 2xy^5 + xy^4 - 3y^6 - 3y^4 \\
&\xrightarrow{f_1} x^2y + 3x^2 + 2xy^5 + xy^4 - 3y^6 - 4y^4 - y^2 \\
&\xrightarrow{f_1} 3x^2 + 2xy^5 + xy^4 - 3y^6 - 4y^4 - y^3 - y^2 - y \\
&\xrightarrow{f_1} 2xy^5 + xy^4 - 3y^6 - 4y^4 - y^3 - 4y^2 - y - 3 \\
&\xrightarrow{f_4} 7xy^4 + 2xy^2 + 2xy + 6x - 3y^6 - 4y^4 - y^3 - 4y^2 - y - 3 \\
&\xrightarrow{f_3} 4xy^3 + 2xy^2 + 2xy + 6x - 2y^6 - 3y^4 - y^3 - 4y^2 - y - 3 \\
&\xrightarrow{f_3} 2xy + 6x - 2y^6 + 2y^5 - 3y^4 + y^3 - 4y^2 - y - 3 \\
&\xrightarrow{f_3} -2y^6 + 2y^5 - 3y^4 + 2y^3 - 4y^2 - 3 \\
&\xrightarrow{f_4} y^5 - 3y^4 - y^2 - y - 3 \xrightarrow{f_4} 0.
\end{aligned}
$$

Finalmente calculamos:

$$
\begin{aligned}
S(f_3, f_4) &= \frac{1}{3}y^4(3xy + 4x + y^3 + y) - \frac{1}{4}x(4y^5 + 3y^4 + y^2 + y + 3) \\
&= 3xy^4 + 2y^7 + 2y^5 + 3xy^4 + xy^2 + xy + 3x \\
&= xy^4 + xy^2 + xy + 3x + 2y^7 + 2y^5 \\
&\xrightarrow{f_3} 2xy^3 + xy^2 + xy + 3x + 2y^7 + 3y^6 + 2y^5 + 3y^4 \\
&\xrightarrow{f_3} xy + 3x + 2y^7 + 3y^6 + 3y^5 + 3y^4 + y^3 \\
&\xrightarrow{f_3} 2y^7 + 3y^6 + 3y^5 + 3y^4 + 4y^3 + 3y
\end{aligned}
$$

$$\xrightarrow{f_4} -y^6 + 3y^5 + y^3 + y^2 + 3y \xrightarrow{f_4} 0.$$

Así $G = \{x^2 + y^2 + 1, x^2y + 2xy + x, 3xy + 4x + y^3 + y, 4y^5 + 3y^4 + y^2 + y + 3\}$ forma una base de Gröbner para el ideal $\langle x^2 + y^2 + 1, x^2y + 2xy + x\rangle \subseteq \mathbb{Z}_5[x, y]$.

2.7 Bases de Gröbner Reducidas

Las Bases de Gröbner obtenidas empleando el algoritmo de Buchberger no necesariamente son únicas. En el ejemplo 2.18 si hubieramos computado $S(f_2, f_3) = x$ primero, el S-polinomio $S(f_1, f_2)$ se hubiera reducido a cero y entonces no habría aparecido en la base de Gröbner, obteniendo asi una base de Gröbner diferente.
Demostraremos en esta sección que poniendo ciertas condiciones a los polinomios que forman una base de Gröbner obtendremos unicidad.

Definición 2.26 (ref.[Adams W.],cáp.1,pág.47)**.** Una base de Gröbner $G = \{g_1, \ldots, g_t\}$ es llamada mínima si para todo i, $\mathrm{lc}(g_i) = 1$ y para todo $i \neq j$, $\mathrm{lp}(g_i)$ no divide a $\mathrm{lp}(g_j)$.

Lema 2.4. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para el ideal I. Si $\mathrm{lp}(g_2)$ divide a $\mathrm{lp}(g_1)$, entonces $\{g_2, \ldots, g_t\}$ es también una base de Gröbner para I.

Corolario 2.5. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para el ideal I. Para obtener una base de Gröbner mínima eliminamos todos los g_i para los cuales existe un $j \neq i$ tal que $\mathrm{lp}(g_j)$ divide al $\mathrm{lp}(g_i)$, y luego dividimos los restantes g_i por su $\mathrm{lc}(g_i)$.

Proposición 2.9. Si $G = \{g_1, \ldots, g_t\}$ y $F = \{f_1, \ldots, f_s\}$ son bases de Gröbner mínimas para un ideal I, entonces $s = t$, y $\mathrm{lt}(f_i) = \mathrm{lt}(g_i), \forall i = 1, \ldots, t$. (reenumerando de ser necesario)

Prueba. Para $\mathrm{lp}(f_1)$ existe un i tal que $\mathrm{lp}(g_i)$ divide al $\mathrm{lp}(f_1)$. Podemos asumir que $i = 1$. Ahora para $\mathrm{lp}(g_1)$ existe un j tal que $\mathrm{lp}(f_j)$ divide al $\mathrm{lp}(g_1)$, luego $\mathrm{lp}(f_j)$ divide a la $\mathrm{lp}(f_1)$ y entonces $j = 1$, $\mathrm{lp}(f_1) = \mathrm{lp}(g_1)$.
Ahora existe un i tal que $\mathrm{lp}(g_i)$ divide al $\mathrm{lp}(f_2)$, $i \neq 1$, y reenumerando se ser necesario podemos asumir $i = 2$, $\mathrm{lp}(f_2) = \mathrm{lp}(g_2)$. El proceso continúa hasta completar la prueba.

□

Definición 2.27 (ref.[Adams W.],cáp.1,pág.48)**.** Una base de Gröbner $G = \{g_1, \ldots, g_t\}$ es llamada una base de Gröbner reducida si y sólo si para todo $1 \leq i \leq t$, $\mathrm{lc}(g_i) = 1$ y g_i es reducido con respecto a $G - \{g_i\}$. Es decir, para todo i, ningún término no-nulo en g_i es divisible por $\mathrm{lp}(g_j)$ para todo $j \neq i$.

Notar que toda base de Gröbner reducida también es mínima. Ahora veamos que las bases de Gröbner reducidas existen.

Corolario 2.6. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner mínima para el ideal I. Consideremos el siguiente proceso de reducción:
$g_1 \xrightarrow{H_1} h_1$, donde h_1 es reducido con respecto a $H_1 = \{g_2, \ldots, g_t\}$
$g_2 \xrightarrow{H_2} h_2$, donde h_2 es reducido con respecto a $H_2 = \{h_1, g_3, \ldots, g_t\}$
$g_3 \xrightarrow{H_3} h_3$, donde h_3 es reducido con respecto a $H_3 = \{h_1, h_2, g_4, \ldots, g_t\}$

$\vdots$

$g_t \xrightarrow{H_t} h_t$, donde h_t es reducido con respecto a $H_t = \{h_1, h_2, \ldots, h_{t-1}\}$.
Entonces $H = \{h_1, \ldots, h_t\}$ es una base de Gröbner reducida para I.

Prueba. Desde que $\mathrm{lp}(g_1) = \max_{2 \leq i \leq t}(\mathrm{lp}(u_i g_i), \mathrm{lp}(h_1))$ para algunos $u_i \in k[x_1, \ldots, x_n]$ y de manera similar para $\mathrm{lp}(g_2), \ldots, \mathrm{lp}(g_t)$ obtenemos $\mathrm{lp}(h_i) = \mathrm{lp}(g_i)$ para cada $i = 1, \ldots, t$. Luego H es también una base de Gröbner para I (y mínima). Además por definición de los h_i's y el hecho que $\mathrm{lp}(h_i) = \mathrm{lp}(g_i)$ se ve fácilmente que h_i's son reducidos respecto a $H - \{h_i\}$. □

Teorema 2.15 (Buchberger)**.** [ref.[Adams W.],cáp.1,pág.48] Fijado un orden de términos. Entonces todo ideal no-nulo I tiene una única base de Gröbner reducida respecto a ese orden.

Prueba. El corolario anterior nos da la existencia, sólo resta probar la unicidad. Sean $G = \{g_1, \ldots, g_t\}$ y $H = \{h_1, \ldots, h_t\}$ bases de Gröbner reducidas para I. Luego podemos asumir por el hecho de ser mínimas para cada i que $\mathrm{lt}(g_i) = \mathrm{lt}(h_i)$, y entonces $\mathrm{lp}(g_i - h_i) < \mathrm{lp}(h_i)$. Supongamos $g_i \neq h_i$, como $g_i - h_i \in I$ existe j tal que $\mathrm{lp}(h_j)$ divide al $\mathrm{lp}(g_i - h_i)$, $\mathrm{lp}(h_j) \leq \mathrm{lp}(g_i - h_i)$ luego $j \neq i$ pero $\mathrm{lp}(h_j) = \mathrm{lp}(g_j)$ dividirá a algún término de g_i o h_i lo cual contradice el hecho de que G y H sean reducidas. Por tanto $g_i = h_i$. □

Ejemplo 2.20. Para el ejemplo 2.18. Una base de Gröbner mínima puede ser obtenida de $\{y^2 + yx + x^2, y + x, y, x^2, x\}$ removiendo $y^2 + yx + x^2, y + x, x^2$ o removiendo $y^2 + yx + x^2, y, x^2$, es decir $\{y, x\}$ y $\{y + x, x\}$ son ambas bases de Gröbner mínimas para el mismo ideal. Además $\{y, x\}$ es claramente reducida, pero $\{y + x, x\}$ no, desde que $y + x \xrightarrow{x} y$.

Ejemplo 2.21. Del ejemplo 2.19 sea $G = \{x^2 + y^2 + 1, x^2y + 2xy + x, 3xy + 4x + y^3 + y, 4y^5 + 3y^4 + y^2 + y + 3\}$ una base de Gröbner para el ideal $I = \langle x^2 + y^2 + 1, x^2y + 2xy + x\rangle \subseteq \mathbb{Z}_5[x, y]$ con respecto al orden lex con $x > y$. Por el corolario 2.5, $\{x^2+y^2+1, xy+3x+2y^3+2y, y^5+2y^4+4y^2+4y+2\}$ es una base de Gröbner mínima para I. Y de hecho se verifica fácilmente que también es reducida.

2.8 Syzygies

En esta sección se definirá al syzygy de un conjunto de polinomios. Sus propiedades, conceptos y resultados son necesarios para introducir un criterio que reduzca el cálculo y reducción de S-polinomios en el algoritmo de Buchberger.

La palabra syzygy es usada en astronomía para indicar alineación de planetas u otros cuerpos celestiales. De hecho la denominación S-polinomio es una abreviación para *syzygy polinomial*. Denotaremos por A a $k[x_1, \ldots, x_n]$. Sea $I = \langle f_1, \ldots, f_s\rangle$ un ideal de A. Definamos el homomorfismo de A-módulos $\phi : A^s \to I$ por $(h_1, \ldots, h_s) \to \sum_{i=1}^{s} h_i f_i$. Donde $I \cong \frac{A^s}{ker(\phi)}$, como A-módulos.

Definición 2.28 (ref.[Adams W.],cáp.3,pág.118)**.** Al núcleo de la aplicación ϕ se le llama módulo syzygy de la $1 \times s$ matriz $[f_1, \ldots, f_s]$, y se le denota por $\mathrm{Syz}(f_1, \ldots, f_s)$. A un elemento $(h_1, \ldots, h_s)$ de $\mathrm{Syz}(f_1, \ldots, f_s)$ es llamado un syzygy de $[f_1, \ldots, f_s]$ y satisface $h_1f_1 + \cdots + h_sf_s = 0$.

En otras palabras $\mathrm{Syz}(f_1, \ldots, f_s)$ es el conjunto de todas las soluciones de la sola ecuación lineal con coeficientes polinomiales (los $f_i's$), $f_1\mathcal{X}_1 + \cdots + f_s\mathcal{X}_f = 0$, donde las soluciones $\mathcal{X}_i$ también son polinomios en A.

La aplicación ϕ también puede ser vista como una multiplicación de matrices:

$$\phi(h_1, \ldots, h_s) = [f_1, \ldots, f_s] \begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix} = \sum_{i=1}^{s} h_i f_i.$$

Es decir, si F es la $1 \times s$ matriz $[f_1, \ldots, f_s]$, y

$$\mathbf{h} = \begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix} \in A^s$$

, entonces $\phi(h_1, \ldots, h_s) = F\mathbf{h}$ y $\mathrm{Syz}(f_1, \ldots, f_s)$ es el conjunto de todas las soluciones $\mathbf{h}$ de la ecuación lineal $F\mathbf{h} = 0$.

Ejemplo 2.22. Sea $A = \mathbb{Q}[x, y, z, w]$, y $I = \langle x^2 - yw, xy - wz, y^2 - xz \rangle$. El mapa $\phi : A^3 \to I$ es dado por $(h_1, h_2, h_3) \to h_1(x^2 - yw) + h_2(xy - wz) + h_3(y^2 - xz)$. Entonces $(y, -x, w)$ y $(-z, y, -x)$ son ambos syzys de $[x^2 - yw, xy - wz, y^2 - xz]$, desde que $y(x^2 - yw) - x(xy - wz) + w(y^2 - xz) = 0$ y $-z(x^2 - yw) + y(xy - wz) - x(y^2 - xz) = 0$.

Nota 2.5. $\mathrm{Syz}(f_1, \ldots, f_s)$ forma un sub-módulo de A^s y es finitamente generado (ref.[Adams W.],cáp.3,pág.115).

Proposición 2.10. Sean $c_1, \ldots, c_s \in k \setminus \{0\}$ y los monomios $X_1, \ldots, X_s$ en A. Para $i \neq j \in \{1, \ldots, s\}$, definimos $X_{ij} = \mathrm{mcm}(X_i, X_j)$. Entonces el módulo $\mathrm{Syz}(c_1X_1, \ldots, c_sX_s)$ es generado por

$$\{\frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j \in A^s \mid 1 \leq i < j \leq s\},$$

donde $e_1, \ldots, e_s$ forman la base standard de A^s.(Es decir $e_1 = (1, 0, \ldots, 0), \ldots, e_s = (0, \ldots, 0, 1)$)

Prueba. Desde que $[c_1X_1, c_2X_2, \ldots, c_sX_s](0, \ldots, 0, \frac{X_{ij}}{c_iX_i}, 0, \ldots, 0, -\frac{X_{ij}}{c_jX_j}, 0, \ldots, 0)^t = 0$, tenemos que $\frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j$ es un syzygy de $[c_1X_1, c_2X_2, \ldots, c_sX_s]$. Luego

$$\langle \frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j \mid 1 \leq i < j \leq s \rangle \subseteq \mathrm{Syz}(c_1X_1, \ldots, c_sX_s).$$

Para probar la otra inclusión, sea $(h_1, \ldots, h_s)$ tal que $h_1c_1X_1 + \cdots + h_sc_sX_s = 0$. Si X es cualquier monomio, entonces el coeficiente de X en $h_1c_1X_1 + \cdots + h_sc_sX_s$ es

0. Expresando los h_i en su forma canonica notamos que es suficiente con considerar el caso en que los $h_i = c'_i X'_i, i = 1, \ldots, s$, y donde $c'_i = 0$ o $X_i X'_i = X$ para un monomio fijo X. Sean $c'_{i_1}, \ldots, c'_{i_t}$, con $i_1 < i_2 < \cdots < i_t$, no-nulos. Entonces tenemos $c'_1 c_1 + \ldots c'_s c_s = c'_{i_1} c_{i_1} + \cdots + c'_{i_t} c_{i_t} = 0$. Por tanto

$$\begin{aligned}
(h_1, \ldots, h_s) =& (c'_1 X'_1, \ldots, c'_s X'_s) = c'_{i_1} X'_{i_1} e_{i_1} + \cdots + c'_{i_t} X'_{i_t} e_{i_t} \\
=& c'_{i_1} c_{i_1} \frac{X}{c_{i_1} X_{i_1}} e_{i_1} + \cdots + c'_{i_t} c_{i_t} \frac{X}{c_{i_t} X_{i_t}} e_{i_t} \\
=& c'_{i_1} c_{i_1} \frac{X}{X_{i_1 i_2}} \left(\frac{X_{i_1 i_2}}{c_{i_1} X_{i_1}} e_{i_1} - \frac{X_{i_1 i_2}}{c_{i_2} X_{i_2}} e_{i_2}\right) \\
&+ (c'_{i_1} c_{i_1} + c'_{i_2} c_{i_2}) \frac{X}{X_{i_2 i_3}} \left(\frac{X_{i_2 i_3}}{c_{i_2} X_{i_2}} e_{i_2} - \frac{X_{i_2 i_3}}{c_{i_3} X_{i_3}} e_{i_3}\right) + \ldots \\
&+ (c'_{i_1} c_{i_1} + \cdots + c'_{i_{t-1}} c_{i_{t-1}}) \frac{X}{X_{i_{t-1}} i_t} \left(\frac{X_{i_{t-1} i_t}}{c_{i_{t-1}} X_{i_{t-1}}} e_{i_{t-1}} - \frac{X_{i_{t-1} i_t}}{c_{i_t} X_{i_t}} e_{i_t}\right) \\
&+ (c'_{i_1} c_{i_1} + \cdots + c'_{i_t} c_{i_t}) \frac{X}{c_{i_t} X_{i_t}},
\end{aligned}$$

□

Si $c_1 X_1, \ldots, c_s X_s$ son los términos principales de los polinomios $f_1, \ldots, f_s$ y si $(h_1, \ldots, h_s) \in \mathrm{Syz}(c_1 X_1, \ldots, c_s X_s)$, entonces $\sum_{i=1}^{s} h_i f_i$ tiene una potencia principal estrictamente menor que $\max_{1 \le i \le s} \mathrm{lp}(h_i)\mathrm{lp}(f_i)$. En particular el syzygy $\frac{X_{ij}}{c_i X_i} e_i - \frac{X_{ij}}{c_j X_j} e_j$ de $[c_1 X_1 \ldots c_s X_s]$ genera al S-polinomio de f_i y f_j, desde que

$$[f_1 \ldots f_s]\left(\frac{X_{ij}}{c_i X_i} e_i - \frac{X_{ij}}{c_j X_j} e_j\right) = \frac{X_{ij}}{c_i X_i} f_i - \frac{X_{ij}}{c_j X_j} f_j = S(f_i, f_j). \tag{2.1}$$

Definición 2.29. Sean $X_1, \ldots, X_s$ monomios y $c_1, \ldots, c_s \in k \setminus \{0\}$. Entonces para un monomio X, decimos que un syzygy $\mathbf{h} = (h_1, \ldots, h_s) \in \mathrm{Syz}(c_1 X_1, \ldots, c_s X_s)$ es homogéneo de grado X si es que cada h_i es un término (es decir $\mathrm{lt}(h_i) = h_i$ para todo i) y $X_i \mathrm{lp}(h_i) = X$ para todo i tal que $h_i \neq 0$. Decimos que $\mathbf{h}$ es homogéneo si es homogéneo de grado X para algún monomio X.

Nota 2.6. El conjunto generador dado en la proposición 2.10 es un conjunto finito de syzygy's homogéneos.

Teorema 2.16. [ref.[Adams W.],cáp.3,pág.121] Sea $G = \{g_1, \ldots, g_t\}$ un conjunto de polinomios no-nulos en A. Sea B un conjunto generador homogéneo de $\mathrm{Syz}(\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t))$. Entonces G es una base de Gröbner si y sólo si para todo $(b_1, \ldots, b_t) \in B$, se cumple $b_1 g_1 + \cdots + b_t g_t \xrightarrow{G} 0$.

Prueba. ($\Longrightarrow$) Por el teorema 2.11 desde que $h_1g_1 + \cdots + h_tg_t \in \langle G \rangle$.

($\Longleftarrow$) Sea $g \in \langle G \rangle$, luego podemos escribir $g = u_1g_1 + \cdots + u_tg_t$, tal que $X = \max_{1\leq i\leq t}(\mathrm{lp}(u_i)\mathrm{lp}(g_i))$ es mínimo. Si $\mathrm{lp}(g) = X$ la prueba está completa. Asumamos $\mathrm{lp}(g) < X$ y consideremos el conjunto $S = \{i \in \{1, \ldots, t\} \mid \mathrm{lp}(u_i)\mathrm{lp}(g_i) = X\}$, tenemos que $\sum_{i\in S} \mathrm{lt}(u_i)\mathrm{lt}(g_i) = 0$. Ahora sea

$$\mathbf{h} = \sum_{i\in S} \mathrm{lt}(u_i)e_i, \tag{2.2}$$

,donde $e_1, \ldots, e_t$ es la base standar de A^t. Entonces $\mathbf{h} \in \mathrm{Syz}(\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t))$ y $\mathbf{h}$ es homogéneo de grado X. Si $B = \{h_1, \ldots, h_l\}$ es un conjunto generador homogéneo para el $\mathrm{Syz}(\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t))$ donde para cada $j = 1, \ldots, l$, $h_j = (h_{1j}, \ldots, h_{tj})$, con $\mathrm{lp}(h_{1j})\mathrm{lp}(g_1) = \cdots = \mathrm{lp}(h_{tj})\mathrm{lp}(g_t)$. Entonces, para algunos polinomios a_j,

$$\mathbf{h} = \sum_{j=1}^{l} a_jh_j = (a_1h_{11} + a_2h_{12} + \cdots + a_lh_{1l}; \ldots; a_1h_{t1} + a_2h_{t2} \cdots + a_lh_{tl}),$$

y por la ecuación 2.2

$$\sum_{j=1}^{l} a_jh_{ij} = \begin{cases} \mathrm{lt}(u_i), & i \in S \\ 0, & i \notin S. \end{cases}$$

Si digamos $1, 2 \in S$ y $\mathrm{lp}(a_1)\mathrm{lp}(h_{11}) > \mathrm{lp}(u_1)$ (análogamente para el caso $<$) entonces $\mathrm{lp}(a_1)\mathrm{lp}(h_{21}) > \mathrm{lp}(u_2)$ desde que $\mathrm{lp}(h_{11})\mathrm{lp}(g_1) = \mathrm{lp}(h_{21})\mathrm{lp}(g_2)$. Luego podemos omitir los términos no-relevantes que aparecen en los a_j y sólo considerar los a_j's como términos tales que $\mathrm{lp}(a_j)\mathrm{lp}(h_{ij})\mathrm{lp}(g_i) = X$ para todo i, j tales que $a_jh_{ij} \neq 0$. Por hipótesis, para cada j, $\sum_{i=1}^{t} h_{ij}g_i \xrightarrow{G} 0$. Por el teorema 2.10 tenemos $\sum_{i=1}^{t} h_{ij}g_i = \sum_{i=1}^{t} v_{ij}g_i$ para cada $j = 1, \ldots, l$, tal que $\max_{1\leq i\leq t} \mathrm{lp}(v_{ij})\mathrm{lp}(g_i) = \mathrm{lp}(\sum_{i=1}^{t} h_{ij}g_i) < \max_{1\leq i\leq t} \mathrm{lp}(h_{ij})\mathrm{lp}(g_i)$. La última desigualdad es estricta debido a que $\sum_{i=1}^{t} h_{ij}\mathrm{lt}(g_i) = 0$. Así,

$$\begin{aligned} g = u_1g_1 + \cdots + u_tg_t &= \sum_{i\in S} \mathrm{lt}(u_i)g_i + \text{términos de menor orden que X} \\ &= \sum_{i=1}^{t}\sum_{j=1}^{l} a_jh_{ij}g_i + \text{términos de menor orden que X.} \\ &= \sum_{j=1}^{l} a_j \sum_{i=1}^{t} h_{ij}g_i + \text{términos de menor orden que X.} \\ &= \sum_{j=1}^{l}\sum_{i=1}^{t} a_jv_{ij}g_i + \text{términos de menor orden que X.} \end{aligned}$$

Tenemos que $\max_{i,j} \mathrm{lp}(a_j)\mathrm{lp}(v_{ij})\mathrm{lp}(g_i) < \max_{i,j} \mathrm{lp}(a_j)\mathrm{lp}(h_{ij})\mathrm{lp}(g_i) = X$. Esto es una representación de g como combinación lineal de los g_i's tal que la potencia principal de cada sumando es menor a X. □

De la proposición 2.10 junto con la ecuación 2.1 y el teorema anterior vemos que, durante el algoritmo de Buchberger, sólo es necesario calcular los S-polinomios para aquellos pares que corresponden a generadores del syzygy.

2.9 Un par de criterios para reducir el cálculo de S-polinomios en el Algoritmo de Buchberger

En esta sección expondremos dos criterios que buscan disminuir el cálculo y reducción de S-polinomios que ocurren durante el algoritmo de Buchberger.

Desde que si k es un D.F.U, también $k[x_1, \ldots, x_n]$ lo es (ref.[Hungerford T.],cáp.3,pág.164). Por tanto la existencia y unicidad del máximo común divisor para dos o más polinomios en $k[x_1, \ldots, x_n]$ está asegurada.

Lema 2.5. Sean $f, g \in k[x_1, \ldots, x_n]$, no-nulos, y sea $d = \mathrm{mcd}(f, g)$. Las siguientes condiciones son equivalentes:
(i) $\mathrm{lp}(\frac{f}{d})$ y $\mathrm{lp}(\frac{g}{d})$ son relativamente primos;
(ii) $S(f, g) \xrightarrow{\{f,g\}} 0$.
En particular, $\{f, g\}$ es una base de Gröbner si y sólo si $\mathrm{lp}(\frac{f}{d})$ y $\mathrm{lp}(\frac{g}{d})$ son relativamente primos.

Prueba. $(i) \implies (ii)$. Asumamos primero que

$$d = \mathrm{mcd}(f, g) = 1.$$

Escribamos

$$f = aX + f',$$

$$g = bY + g',$$

donde $\mathrm{lt}(f) = aX$, $\mathrm{lt}(g) = bY$, $a, b \in k \setminus \{0\}$, y X, Y monomios. Entonces

$$X = \frac{1}{a}(f - f'),$$

$$Y = \frac{1}{b}(g - g').$$

Caso 1. $f' = g' = 0$. Entonces $S(f, g) = 0$.

Caso 2. $f' = 0$ y $g' \neq 0$. Entonces $S(f, g) = \frac{1}{a}Yf - \frac{1}{b}Xg = \frac{1}{ab}(g - g')f - \frac{1}{ab}fg = -\frac{1}{ab}g'f \xrightarrow{f} -\frac{1}{ab}f(g' - \mathrm{lt}(g'))$ y sucesivamente hasta reducirse a 0.

Caso 3. $f' \neq 0$ y $g' = 0$. Similar al Caso2.

Caso 4. $f' \neq 0$ y $g' \neq 0$. Tenemos $S(f, g) = \frac{1}{a}Yf - \frac{1}{b}Xg = \frac{1}{ab}(g - g')f - \frac{1}{ab}(f - f')g = \frac{1}{ab}(f'g - g'f)$. Si $\mathrm{lp}(f'g) = \mathrm{lp}(g'f)$, entonces $\mathrm{lp}(f')\mathrm{lp}(g) = \mathrm{lp}(g')\mathrm{lp}(f)$, y desde que asumimos $d = 1$ por (i) tenemos $\mathrm{lp}(f)$ divide a $\mathrm{lp}(f')$ y $\mathrm{lp}(g)$ divide a $\mathrm{lp}(g')$, lo cual es una contradicción ya que $\mathrm{lp}(f') < \mathrm{lp}(f)$ y $\mathrm{lp}(g') < g$. Por tanto $\mathrm{lp}(f'g) \neq \mathrm{lp}(g'f)$, y el término principal de $\frac{1}{ab}(f'g - g'f)$ aparece en $f'g$ o $g'f$ y así es un múltiplo de $\mathrm{lp}(f)$ o $\mathrm{lp}(g)$. Si $\mathrm{lp}(f'g) > \mathrm{lp}(g'f)$, entonces

$$S(f, g) \xrightarrow{g} \frac{1}{ab}((f' - \mathrm{lt}(f'))g - g'f).$$

Si $\mathrm{lp}(f'g) < \mathrm{lp}(g'f)$, entonces

$$S(f, g) \xrightarrow{f} \frac{1}{ab}(f'g - (g' - \mathrm{lt}(g'))f).$$

Usando un argumento similar, el término principal de $\frac{1}{ab}((f' - \mathrm{lt}(f'))g - g'f)$ o $\frac{1}{ab}(f'g - (g' - \mathrm{lt}(g')f))$ es un múltiplo de $\mathrm{lp}(f)$ o $\mathrm{lp}(g)$. El proceso de reducción continua, en cada paso el resto tendrá un término principal que es múltiplo de $\mathrm{lp}(f)$ o $\mathrm{lp}(g)$, hasta llegar a 0, es decir, $S(f, g) \xrightarrow{\{f,g\}} 0$.

Ahora asumamos que $d = \mathrm{mcd}(f, g) \neq 1$. Entonces $\mathrm{mcd}(\frac{f}{d}, \frac{g}{d}) = 1$. Por (i) $\mathrm{mcd}(\mathrm{lp}(\frac{f}{d}), \mathrm{lp}(\frac{g}{d})) = 1$, luego por el caso anterior $\{\frac{f}{d}, \frac{g}{d}\}$ es una base de Gröbner. Así $\{d\frac{f}{d}, d\frac{g}{d}\}$ es también una base de Gröbner, y $S(f, g) \xrightarrow{\{f,g\}} 0$.

$(ii) \implies (i)$. Asumamos primero que $\mathrm{mcd}(f, g) = 1$. Sea $\mathrm{lp}(f) = DX$ y $\mathrm{lp}(g) = DY$, donde D,X y Y son monomios en $k[x_1, \ldots, x_n]$, con $\mathrm{mcd}(X, Y) = 1$. Entonces $S(f, g) = \frac{Y}{\mathrm{lc}(f)}f - \frac{X}{\mathrm{lc}(g)}g$. Por hipótesis $S(f, g) \xrightarrow{\{f,g\}} 0$, luego existen $u, v \in k[x_1, \ldots, x_n]$ tales que $S(f, g) = uf + vg$, donde $\mathrm{lp}(uf) \leq \mathrm{lp}(S(f, g))$ y $\mathrm{lp}(vg) \leq \mathrm{lp}(S(f, g))$. Obtenemos $(\frac{X}{\mathrm{lc}(g)} + v)g = (\frac{Y}{\mathrm{lc}(f)} - u)f$. Y, desde que f y g son relativamente primos, f divide a $\frac{X}{\mathrm{lc}(g)} + v$, y g divide a $\frac{Y}{\mathrm{lc}(f)} - u$. También

$$\mathrm{lp}(u)DX = \mathrm{lp}(uf) \leq \mathrm{lp}(S(f, g)) < X\mathrm{lp}(g) = Y\mathrm{lp}(f) = DXY.$$

Así, $\mathrm{lp}(u) < Y$, luego $\mathrm{lp}(\frac{Y}{\mathrm{lc}(f)} - u) = Y$. Pero g divide a $(\frac{Y}{\mathrm{lc}(f)} - u)$, entonces $\mathrm{lp}(g) = DY$ divide a $\mathrm{lp}(\frac{Y}{\mathrm{lc}(f)} - u) = Y$, y luedo $D = 1$. Por tanto $\mathrm{lp}(f)$ y $\mathrm{lp}(g)$ son relativamente

primos.

Ahora asumamos que $d = \text{mcd}(f, g) \neq 1$. Entonces $\text{mcd}(\frac{f}{d}, \frac{g}{d}) = 1$. Fácilmente se prueba que si $S(f, g) \xrightarrow{\{f,g\}} 0$, entonces $\frac{1}{d}S(f, g) \xrightarrow{\{\frac{f}{d}, \frac{g}{d}\}} 0$. Además desde que d es mónico $\frac{1}{d}S(f, g) = S(\frac{f}{d}, \frac{g}{d})$. Utilizando el caso anterior tenemos que $\text{lp}(\frac{f}{d})$ y $\text{lp}(\frac{g}{d})$ son relativamente primos. □

Corolario 2.7. Desde que $\text{mcd}(\text{lp}(f), \text{lp}(g)) = 1$ implica $d = \text{mcd}(f, g) = 1$ tenemos, por el lema anterior, que la condición $\text{mcd}(\text{lp}(f), \text{lp}(g)) = 1$ es un criterio para mejorar el algoritmo de Buchberger **crit1** y disminuir el cálculo y las reducciones de S-polinomios.

El siguiente lema nos brindará un segundo criterio **crit2**:

Lema 2.6. Sean $X_1, X_2, \ldots, X_s$ productos de potencias en $A = k[x_1, \ldots, x_n]$ y sean $c_1, \ldots, c_s \in k \setminus \{0\}$. Para $i, j = 1, \ldots, s$, definamos $X_{ij} = \text{mcm}(X_i, X_j)$ y sea

$$\tau_{ij} = \frac{X_{ij}}{c_i X_i} e_i - \frac{X_{ij}}{c_j X_j} e_j \in \text{Syz}(c_1 X_1, \ldots, c_s X_s) \subseteq A^s,$$

donde $e_1, \ldots, e_s$ es la base standard para A^s. Para cada $i, j, l = 1, \ldots, s$ sea $X_{ijl} = \text{mcm}(X_i, X_j, X_l)$. Entonces tenemos que

$$\frac{X_{ijl}}{X_{ij}}\tau_{ij} + \frac{X_{ijl}}{X_{jl}}\tau_{jl} + \frac{X_{ijl}}{X_{li}}\tau_{li} = 0.$$

Además, si X_l divide a X_{ij}, entonces τ_{ij} esta en el sub-módulo de A^s generado por τ_{jl} y τ_{li}.

Prueba. Tenemos que

$$\frac{X_{ijl}}{X_{ij}}\tau_{ij} + \frac{X_{ijl}}{X_{jl}}\tau_{jl} + \frac{X_{ijl}}{X_{li}}\tau_{li} =$$

$$\frac{X_{ijl}}{X_{ij}}\left(\frac{X_{ij}}{c_i X_i} e_i - \frac{X_{ij}}{c_j X_j} e_j\right) + \frac{X_{ijl}}{X_{jl}}\left(\frac{X_{jl}}{c_j X_j} e_j - \frac{X_{jl}}{c_l X_l} e_l\right) + \frac{X_{ijl}}{X_{li}}\left(\frac{X_{li}}{c_l X_l} e_l - \frac{X_{li}}{c_i X_i} e_i\right)$$

$$= \frac{X_{ijl}}{c_i X_i} e_i - \frac{X_{ijl}}{c_j X_j} e_j + \frac{X_{ijl}}{c_j X_j} e_j - \frac{X_{ijl}}{c_l X_l} e_l + \frac{X_{ijl}}{c_l X_l} e_l - \frac{X_{ijl}}{c_i X_i} e_i = 0.$$

Ahora si X_l divide a X_{ij}, entonces $X_{ijl} = X_{ij}$, y tenemos que

$$\tau_{ij} + \frac{X_{ij}}{X_{jl}}\tau_{jl} + \frac{X_{ij}}{X_{li}}\tau_{li} = 0.$$

Luego τ_{ij} esta en el sub-módulo de A^s generado por τ_{jl} y τ_{li}. □

Corolario 2.8. Con la notación del lema anterior. Sea $\mathcal{B} \subseteq \{\tau_{ij} \mid 1 \leq i < j \leq s\}$ un conjunto generador para $\mathrm{Syz}(c_1X_1, \ldots, c_sX_s)$. Supongamos que tenemos tres indices distintos i, j, l tal que $\tau_{il}, \tau_{jl}, \tau_{ij} \in \mathcal{B}$, y tal que X_l divide a $X_{ij} = \mathrm{mcm}(X_i, X_j)$. Entonces $\mathcal{B} - \{\tau_{ij}\}$ es también un conjunto generador para $\mathrm{Syz}(c_1X_1, \ldots, c_sX_s)$.

El corolario 2.8 será considerado el segundo criterio de elminación de pares **crit2** para mejorar el algoritmo de Buchberger(ref.[Adams W.],cáp.3,pág.129). Este **crit2** será aplicado de forma intuitiva, es decir sin seguir necesariamente algun orden específico.

Entrada: $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$ con $f_i \neq 0 (1 \leq i \leq s)$
Salida: Una base de Grobner G para $\langle f_1, \ldots, f_s \rangle$
Inicio: $G := F, C := \emptyset, NC := \{\{1, 2\}\}, i := 2$
Mientras $i < s$ Hacer
$NC := NC \cup \{\{j, i+1\} \mid 1 \leq j \leq i\}$
$NC := crit2(NC, C)$
$i := i + 1$
FinMientras
Mientras $NC \neq \emptyset$ **Hacer**
Elegimos $\{i, j\} \in NC$
$NC := NC - \{\{i, j\}\}$
$C := C \cup \{\{i, j\}\}$
Si $crit1(i, j)$=Falso **Entonces**
$S(f_i, f_j) \xrightarrow{G} h$, donde h es reducido respecto a G
Si $h \neq 0$ **Entonces**
$f_{s+1} := h$
$G := G \cup \{f_{s+1}\}$
$s := s + 1$
$NC := NC \cup \{\{i, s\} \mid 1 \leq i \leq s - 1\}$
$NC := crit2(NC, C)$
FinSi
FinSi
FinMientras

Algoritmo 2.5: Algoritmo Mejorado de Buchberger.

Ejemplo 2.23. Consideremos los polinomios $f_1 = x^2y^2 - z^2$, $f_2 = xy^2z - xyz$, y $f_3 = xyz^3 - xz^2$ en $\mathbb{Q}[x, y, z]$. Usaremos el orden deglex con $z > y > x$.
Empezamos con

$$G = \{f_1, f_2, f_3\},$$

$$C = \emptyset, NC = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}.$$

Vemos que $\text{lp}(f_2) = xy^2z$ divide a $x^2y^2z^3 = \text{mcm}(\text{lp}(f_1), \text{lp}(f_3))$, entonces $NC = crit2(NC) = \{\{1, 2\}, \{2, 3\}\}$. Notando que τ_{13} ha sido removido del conjunto de generadores del Syzygie, podemos registrar este par en el conjunto

$$PU = \{\tau_{13}\}.$$

Elegimos el par $\{1, 2\}$, cambiando NC a $\{\{2, 3\}\}$ y C a $\{\{1, 2\}\}$, y calculamos

$$S(f_1, f_2) = z(x^2y^2 - z^2) - x(xy^2z - xyz) = x^2yz - z^3$$

reducido respecto a G. Así agregamos $f_4 = x^2yz - z^3$ a G y actualizamos:

$$NC = \{\{2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}\}$$

Vemos que $\text{lp}(f_1) = x^2y^2$ divide a $\text{mcm}(\text{lp}(f_2), \text{lp}(f_4)) = x^2y^2z$ y actualizamos

$$NC = \{\{2, 3\}, \{1, 4\}, \{3, 4\}\}.$$

$$PU = \{\tau_{13}, \tau_{24}\}.$$

Elegimos el par $\{1, 4\}$, cambiando

$$NC = \{\{2, 3\}, \{3, 4\}\}, C = \{\{1, 2\}, \{1, 4\}\},$$

y calculamos

$$f_5 = S(f_1, f_4) = z(x^2y^2 - z^2) - y(x^2yz - z^3) = yz^3 - z^3$$

reducido respecto a G. Luego

$$NC = \{\{2, 3\}, \{3, 4\}, \{1, 5\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}.$$

Aplicando el **crit2**:

$$\text{lp}(f_2) = xy^2z \mid x^2y^2z^3 = \text{mcm}(\text{lp}(f_1), \text{lp}(f_5)),$$

$$\mathrm{lp}(f_3) = xyz^3 \mid xy^2z^3 = \mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_5)),$$
$$\mathrm{lp}(f_3) = xyz^3 \mid x^2yz^3 = \mathrm{mcm}(\mathrm{lp}(f_4), \mathrm{lp}(f_5)).$$

obtenemos

$$NC = \{\{2,3\},\{3,4\},\{3,5\}\}.$$
$$PU = \{\tau_{13}, \tau_{24}, \tau_{15}, \tau_{25}, \tau_{45}\}.$$

Elegimos el par $\{3,5\}$, ahora

$$NC = \{\{2,3\},\{3,4\}\}, \quad C = \{\{1,2\},\{1,4\},\{3,5\}\},$$

y calculamos

$$f_6 = S(f_3, f_5) = (xyz^3 - xz^2) - x(yz^3 - z^3) = xz^3 - xz^2$$

reducido respecto a G. Agregamos a

$$NC = \{\{1,6\},\{2,6\},\{3,6\},\{4,6\},\{5,6\},\{2,3\},\{3,4\}\}.$$

Aplicamos **crit2**:
$\mathrm{lp}(f_2) = xy^2z$ divide al $\mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_6)) = x^2y^2z^3$,
$\mathrm{lp}(f_3) = xyz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_6)) = xy^2z^3$,
$\mathrm{lp}(f_3) = xyz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_4), \mathrm{lp}(f_6)) = x^2yz^3$,
$\mathrm{lp}(f_3) = xyz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_5), \mathrm{lp}(f_6)) = xyz^3$.
Notando que de haber eliminado τ_{26} primero no hubiera sido posible eliminar τ_{16} del conjunto generador. Además al eliminar τ_{56} imposibilita eliminar τ_{36} utilizando $lp(f_5)$. Actualizamos

$$NC = \{\{2,3\},\{3,4\},\{3,6\}\}.$$
$$PU = \{\tau_{13}, \tau_{24}, \tau_{15}, \tau_{25}, \tau_{45}, \tau_{16}, \tau_{26}, \tau_{46}, \tau_{56}\}.$$

Elegimos el par $\{3,6\}$, $NC = \{\{2,3\},\{3,4\}\}$ y $C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\}\}$. Calculamos

$$f_7 = S(f_3, f_6) = (xyz^3 - xz^2) - y(xz^3 - xz^2) = xyz^2 - xz^2$$

reducido respecto a G. Agregamos

$$NC = \{\{2,3\},\{3,4\},\{1,7\},\{2,7\},\{3,7\},\{4,7\},\{5,7\},\{6,7\}\}.$$

Aplicamos **crit2**:

$\mathrm{lp}(f_2) = xy^2z$ divide al $\mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_7)) = x^2y^2z^2$,

$\mathrm{lp}(f_3) = xyz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_6), \mathrm{lp}(f_7)) = xyz^3$,

$\mathrm{lp}(f_7) = xyz^2$ divide al $\mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_3)) = xy^2z^3$,

$\mathrm{lp}(f_7) = xyz^2$ divide al $\mathrm{mcm}(\mathrm{lp}(f_3), \mathrm{lp}(f_4)) = x^2yz^3$.

Y actualizamos

$$NC = \{\{2,7\},\{3,7\},\{4,7\},\{7,8\}\}.$$

$$PU = \{\tau_{13}, \tau_{24}, \tau_{15}, \tau_{25}, \tau_{45}, \tau_{16}, \tau_{26}, \tau_{46}, \tau_{56}, \tau_{17}, \tau_{67}, \tau_{23}, \tau_{34}\}.$$

Elegimos $\{4,7\}$,

$$C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\},\{6,7\},\{4,7\}\},$$

y calculamos $f_8 = S(f_4, f_7) = z(x^2yz - z^3) - x(xyz^2 - xz^2) = -z^4 + x^2z^2$ reducido respecto a G. Actualizamos

$$NC = \{\{2,7\},\{3,7\},\{1,8\},\{2,8\},\{3,8\},\{4,8\},\{5,8\},\{6,8\},\{7,8\}\}.$$

Aplicando el **crit1** para $\mathrm{mcd}(\mathrm{lp}(f_1), \mathrm{lp}(f_8)) = 1$. Luego aplicamos **crit2**

$\mathrm{lp}(f_5) = yz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_3), \mathrm{lp}(f_8)) = xyz^4$,

$\mathrm{lp}(f_5) = yz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_7), \mathrm{lp}(f_8)) = xyz^4$,

$\mathrm{lp}(f_3) = xyz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_5), \mathrm{lp}(f_7)) = xyz^3$.

Desde que ha quedado claro el procedimiento que se está siguiendo dejaremos de actualizar el conjunto PU. Además

$$S(f_2, f_7) = z(xy^2z - xyz) - y(xyz^2 - xz^2) = 0$$
$$S(f_3, f_7) = (xyz^3 - xz^2) - z(xyz^2 - xz^2) = xz^3 - xz^2 \xrightarrow{f_6} 0.$$

Luego

$$NC = \{\{2,8\},\{4,8\},\{5,8\},\{6,8\}\}.$$

Luego para el par $\{6,8\}$,

$$C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\},\{4,7\},\{2,7\},\{3,7\},\{6,8\}\},$$

calculamos

$$f_9 = S(f_6, f_8) = z(xz^3 - xz^2) + x(-z^4 + x^2z^2) = x^3z^2 - xz^3$$

reducido respecto a G. Aplicamos **crit2**:

$\mathrm{lp}(f_2) = xy^2z$ divide al $\mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_9)) = x^3y^2z^2$,

$\mathrm{lp}(f_4) = x^2yz$ divide al $\mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_9)) = x^3y^2z^2$,

$\mathrm{lp}(f_4) = x^2yz$ divide al $\mathrm{mcm}(\mathrm{lp}(f_3), \mathrm{lp}(f_9)) = x^3yz^3$,

$\mathrm{lp}(f_4) = x^2yz$ divide al $\mathrm{mcm}(\mathrm{lp}(f_7), \mathrm{lp}(f_9)) = x^3yz^2$,

$\mathrm{lp}(f_6) = xz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_8), \mathrm{lp}(f_9)) = x^3z^4$,

$\mathrm{lp}(f_6) = xz^3$ divide al $\mathrm{mcm}(\mathrm{lp}(f_5), \mathrm{lp}(f_9)) = x^3yz^3$.

Notando que pudimos no eliminar los $\tau_{24}, \tau_{34}, \tau_{56}$ hasta despúes de eliminar $\tau_{29}, \tau_{34}, \tau_{59}$. Actualizamos

$$NC = \{\{2,8\},\{4,8\},\{5,8\},\{4,9\},\{6,9\}\}.$$

Calculamos los S-polinomios restantes:

$$\begin{aligned}
S(f_2, f_8) &= z^3(xy^2z - xyz) - (-xy^2)(-z^4 + x^2z^2) = x^3y^2z^2 - xyz^4 \xrightarrow{f_1} \\
&\quad - xyz^4 + xz^4 \xrightarrow{f_5} 0. \\
S(f_4, f_8) &= z^3(x^2yz - z^3) - (-x^2y)(-z^4 + x^2z^2) = x^4yz^2 - z^6 \xrightarrow{f_4} \\
&\quad - z^6 + x^2z^4 \xrightarrow{f_8} 0. \\
S(f_5, f_8) &= z(yz^3 - z^3) - (-y)(-z^4 + x^2z^2) = x^2yz^2 - z^4 \xrightarrow{f_4} 0. \\
S(f_4, f_9) &= xz(x^2yz - z^3) - y(x^3z^2 - xz^3) = -xz^4 + xyz^3 \xrightarrow{f_6} xyz^3 - xz^3 \xrightarrow{f_3} \\
&\quad - xz^3 + xz^2 \xrightarrow{f_6} 0. \\
S(f_6, f_9) &= x^2(xz^3 - xz^2) - z(x^3z^2 - xz^3) = xz^4 - x^3z^2 \xrightarrow{f_6} -x^3z^2 + xz^3 \xrightarrow{f_9} 0. \\
C =& \{\{1,2\},\{1,4\},\{3,5\},\{3,6\},\{4,7\},\{2,7\},\{3,7\},\{6,8\},\{2,8\},\{4,8\}, \\
&, \{5,8\},\{4,9\},\{6,9\}\}.
\end{aligned}$$

Así $G = \{x^2y^2 - z^2, xy^2z - xyz, xyz^3 - xz^2, x^2yz - z^3, yz^3 - z^3, xz^3 - xz^2, xyz^2 - xz^2, -z^4 + x^2z^2, x^3z^2 - xz^3\}$ es una base de Gröbner para $I = \langle x^2y^2 - z^2, xy^2z - xyz, xyz^3 - xz^2\rangle$. Fue necesario calcular 13 S-polinomios aplicando el **crit2**, de las $36 = \frac{9\times 8}{2}$ posibles.

Ejemplo 2.24. Sean los polinomios $f_1 = x^2y + z$, $f_2 = xz + y$, $f_3 = y^2z + 1 \in \mathbb{Q}[x, y, z]$ usando el orden lex con $x > y > z$. Calcularemos una base de Gröbner para el ideal generado por estos polinomios. Desde que $\mathrm{lp}(f_2) = xz$ divide al $\mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_3)) = x^2y^2z$, $NC = \{\{1,2\},\{2,3\}\}$. Calculamos $S(f_1, f_2) = z(x^2y + z) - xy(xz + y) = -xy^2 +$

$z^2 = f_4$ reducido con respecto a $G = \{f_1, f_2, f_3\}$ luego se agrega a $G = \{f_1, f_2, f_3, f_4\}$ y se actualiza

$$C = \{\{1, 2\}\}, \quad NC = \{\{2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}\}.$$

Aplicamos **crit2** en NC:
$\text{lp}(f_3) = y^2z$ divide al $\text{mcm}(\text{lp}(f_2), \text{lp}(f_4)) = xy^2z$.
Entonces $NC = \{\{2, 3\}, \{1, 4\}, \{3, 4\}\}$. Elegimos $\{2, 3\}$,y calculamos $S(f_2, f_3) = y^2(xz + y) - x(y^2z + 1) = -x + y^3 = f_5$ reducido. Agregamos a

$$G = \{f_1, f_2, f_3, f_4, f_5\}.$$

$$NC = \{\{1, 4\}, \{1, 5\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}.$$

$$C = \{\{1, 2\}, \{2, 3\}\}.$$

y aplicamos el **crit2**:
$\text{lp}(f_2) = xz$ divide al $\text{mcm}(\text{lp}(f_3), \text{lp}(f_5)) = xy^2z$,
$\text{lp}(f_5) = x$ divide al $\text{mcm}(\text{lp}(f_1), \text{lp}(f_4)) = x^2y^2$.

$$NC = \{\{1, 5\}, \{2, 5\}, \{4, 5\}\},$$

y calculamos:

$$S(f_1, f_5) = (x^2y + z) - (-xy)(-x + y^3) = xy^4 + z \xrightarrow{f_4} y^2z^2 + z \xrightarrow{f_3} 0,$$
$$S(f_2, f_5) = (xz + y) - (-z)(-x + y^3) = y^3z + y \xrightarrow{f_3} 0,$$
$$S(f_4, f_5) = -(-xy^2 + z^2) - (-y^2)(-x + y^3) = y^5 - z^2 = f_6.$$

f_6 reducido, actualizamos:

$$C = \{\{1, 2\}, \{2, 3\}, \{1, 5\}, \{2, 5\}, \{4, 5\}\}.$$

$$NC = \{\{1, 6\}, \{2, 6\}, \{3, 6\}, \{4, 6\}, \{5, 6\}\}.$$

Aplicando el **crit2**:
$\text{lp}(f_5) = x$ divide al $\text{mcm}(\text{lp}(f_1), \text{lp}(f_6)) = x^2y^5$,
$\text{lp}(f_3) = y^2z$ divide al $\text{mcm}(\text{lp}(f_2), \text{lp}(f_6)) = xy^5z$,

$\mathrm{lp}(f_5) = x$ divide al $\mathrm{mcm}(\mathrm{lp}(f_4), \mathrm{lp}(f_6)) = xy^5$,

Luego

$$NC = \{\{3,6\},\{5,6\}\}.$$

Calculamos $S(f_3, f_6) = y^3(y^2z+1) - z(y^5 - z^2) = y^3 + z^3 = f_7$ reducido. Actualizamos:

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7\}.$$

$$C = \{\{1,2\},\{2,3\},\{1,5\},\{2,5\},\{4,5\},\{3,6\}\}.$$

$$NC = \{\{5,6\},\{1,7\},\{2,7\},\{3,7\},\{4,7\},\{5,7\},\{6,7\}\}.$$

$\mathrm{lp}(f_4) = xy^2$ divide al $\mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_7)) = x^2y^3$, eliminando este par τ_{17} antes que el par τ_{14},

$\mathrm{lp}(f_3) = y^2z$ divide al $\mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_7)) = xy^3z$,

$\mathrm{lp}(f_5) = x$ divide al $\mathrm{mcm}(\mathrm{lp}(f_4), \mathrm{lp}(f_7)) = xy^3$.

Entonces resta calcular

$$NC = \{\{3,7\},\{5,7\},\{6,7\}\}.$$

$$S(f_3, f_7) = y(y^2z+1) - z(y^3 + z^3) = y - z^4 = f_8,$$

$$\mathrm{mcd}(\mathrm{lp}(f_5), \mathrm{lp}(f_7)) = \mathrm{mcd}(x, y^3) = 1,$$

$$S(f_6, f_7) = (y^5 - z^2) - y^2(y^3 + z^3) = -y^2z^3 - z^2 \xrightarrow{f_3} 0.$$

Actualizamos

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}.$$

$$NC = \{\{1,8\},\{2,8\},\{3,8\},\{4,8\},\{5,8\},\{6,8\},\{7,8\}\}.$$

$$C = \{\{1,2\},\{2,3\},\{1,5\},\{2,5\},\{4,5\},\{3,6\},\{3,7\},\{6,7\}\}.$$

Aplicamos **crit2**:

$$\mathrm{lp}(f_5) = x \mid \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_8)) = x^2y,$$

$$\mathrm{lp}(f_5) = x \mid \mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_8)) = xyz,$$

$$\mathrm{lp}(f_5) = x \mid \mathrm{mcm}(\mathrm{lp}(f_4), \mathrm{lp}(f_8)) = xy^2,$$

$$\mathrm{lp}(f_7) = y^3 \mid \mathrm{mcm}(\mathrm{lp}(f_6), \mathrm{lp}(f_8)) = y^5.$$

Calculamos los S-polinomios restantes:

$$S(f_3, f_8) = (y^2z+1) - yz(y - z^4) = yz^5 + 1 \xrightarrow{f_8} z^9 + 1 = f_9 \quad \text{reducido},$$

$$\text{mcd}(\text{lp}(f_5), \text{lp}(f_8)) = mcd(x, y) = 1.$$

$$S(f_7, f_8) = (y^3 + z^3) - y^2(y - z^4) = y^2z^4 + z^3 \xrightarrow{f_3} 0.$$

Actualizamos:

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9\}.$$

$$C = \{\{1,2\},\{2,3\},\{1,5\},\{2,5\},\{4,5\},\{3,6\},\{3,7\},\{6,7\},\{3,8\},\{7,8\}\}.$$

$$NC = \{\{1,9\},\{2,9\},\{3,9\},\{4,9\},\{5,9\},\{6,9\},\{7,9\},\{8,9\}\}.$$

Aplicando el **crit1**:

$$\begin{aligned}
\text{mcd}(\text{lp}(f_1), \text{lp}(f_9)) &= \text{mcd}(x^2y, z^9) = 1,\\
\text{mcd}(\text{lp}(f_4), \text{lp}(f_9)) &= \text{mcd}(xy^2, z^9) = 1,\\
\text{mcd}(\text{lp}(f_5), \text{lp}(f_9)) &= \text{mcd}(x, z^9) = 1,\\
\text{mcd}(\text{lp}(f_6), \text{lp}(f_9)) &= \text{mcd}(y^5, z^9) = 1,\\
\text{mcd}(\text{lp}(f_7), \text{lp}(f_9)) &= \text{mcd}(y^3, z^9) = 1,\\
\text{mcd}(\text{lp}(f_8), \text{lp}(f_9)) &= \text{mcd}(y, z^9) = 1.
\end{aligned}$$

Aplicando el **crit2**:

$$\text{lp}(f_5) = x \mid \text{mcm}(\text{lp}(f_2), \text{lp}(f_9)) = xz^9,$$

$$\text{lp}(f_8) = y \mid \text{mcm}(\text{lp}(f_3), \text{lp}(f_9)) = y^2z^9.$$

Con lo que obtenemos la base de Gröbner $G = \{x^2y+z, xz+y, y^2z+1, -xy^2+z^2, -x+y^3, y^5-z^2, y^3+z^3, y-z^4, z^9+1\}$ para el ideal $\langle x^2y+z, xz+y, y^2z+1\rangle$. La correspondiente Base de Gröbner reducida es $G_R = \{x - yz^8, y - z^4, z^9 + 1\}$. Fue necesario calcular 10 S-polinomios de los $36 = \frac{9\times 8}{2}$ posibles.

Capítulo 3

Aplicaciones para las bases de Gröbner

En este cápitulo expondremos aplicaciones para la teoría desarrollada en el cápitulo anterior, es decir ahora que se conoce como calcular bases de Gröbner de una forma aceptablemente eficiente, procedemos a mostrar como se utiliza en la solución de distintos problemas.

3.1 Aplicaciones Elementales

Sea $I = \langle f_1, \ldots, f_s \rangle$ un ideal $k[x_1, \ldots, x_n]$. Consideremos los siguientes problemas:

(i) Sea $f \in k[x_1, \ldots, x_n]$, determinar si es que $f \in I$ y de ser así encontrar los $v_1, \ldots, v_s \in k[x_1, \ldots, x_n]$ tales que $f = v_1 f_1 + \cdots + v_s f_s$;

(ii) Determinar si es que dos ideales $I, J \in k[x_1, \ldots, x_n]$ son iguales.

(iii) Encontrar representantes de clase para cada elemento de $k[x_1, \ldots, x_n]/I$;

(iv) Encontrar una base para el k-espacio vectorial $k[x_1, \ldots, x_n]/I$;

(v) Determinar las operaciones en $k[x_1, \ldots, x_n]/I$;

(vi) Encontrar inversas en $k[x_1, \ldots, x_n]/I$ si es que existen.

Empezaremos con (i). Sea $F = \{f_1 \ldots, f_s\}$ y sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para $I = \langle f_1, \ldots, f_s \rangle$ con respecto a un orden de términos fijo. Por el teorema 2.11

$$f \in I \iff f \xrightarrow{G} 0.$$

Además aplicando el algoritmo de la división a $f \in I$ obtenemos $u_1, \ldots, u_t$ tales que

$$f = u_1 g_1 + \cdots + u_t g_t. \tag{3.1}$$

También el algoritmo de Buchberger puede ser utilizado para registrar las combinaciones lineales de los f_i's que generan a los g_j's. Para ver esto recordemos que durante el algoritmo de Buchberger para la computación de una base de Gröbner, un nuevo polinomio g es agregado a la base si es el resto no-nulo de la división de un S-polinomio por la base obtenida hasta ese momento, digamos $\{h_1, \ldots, h_l\}$. Es decir

$$g = S(h_v, h_u) - \sum_{i=1}^{l} w_i h_i,$$

para algunos $v, u \in \{1, 2, \ldots, l\}$ y algunos polinomios w_i que son explícitamente calculados por el algoritmo de la división. Así podemos obtener como salida del algoritmo de Buchberger no sólo la base de Gröbner $\{g_1, \ldots, g_t\}$ pero también una matriz M de dimensiones $t \times s$ cuyos elementos son polinomios tales que

$$\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_t \end{bmatrix} = M \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_s \end{bmatrix}.$$

Así la ecuación 3.1 puede ser transformada para darnos f como una combinación lineal de los polinomios originales $f_1, \ldots, f_s$:

$$f = v_1 f_1 + \cdots v_s f_s.$$

Ejemplo 3.1. [ref.[Adams W.],cáp.2,pág.54] Sean $f_1 = x^2y - y + x, f_2 = xy^2 - x$ en $\mathbb{Q}[x, y]$ y $I = \langle f_1, f_2 \rangle$. Usaremos el orden deglex con $y > x$. Aplicando el algoritmo de Buchberger y registrando las combinaciones lineales pertinentes:

Inicio: $G := \{f_1, f_2\}, \mathcal{G} := \{\{f_1, f_2\}\}$.

Primera Iteración:

$\mathcal{G} := \emptyset$

$S(f_1, f_2) = yf_1 - xf_2 = -y^2 + xy + x^2$ (reducido con respecto a G)

Sea $f_3 := -y^2 + xy + x^2$

Notemos que $f_3 = yf_1 - xf_2$

$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$G := \{f_1, f_2, f_3\}$

Segunda Iteración:

$\mathcal{G} := \{\{f_2, f_3\}\}$

$S(f_1, f_3) = yf_1 + x^2 f_3 = x^3y + x^4 - y^2 + xy$

$\xrightarrow{f_1} x^4 - y^2 + 2xy - x^2$

$\xrightarrow{f_3} x^4 + xy - 2x^2$ (reducido con respecto a G)

Sea $f_4 := x^4 + xy - 2x^2$

Notar que $f_4 = (yf_1 + x^2 f_3) - xf_1 - f_3 = (x^2y - x)f_1 + (-x^3 + x)f_2$

$\mathcal{G} := \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$G := \{f_1, f_2, f_3, f_4\}$

Tercera Iteración:

$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$S(f_2, f_3) = f_2 + xf_3 = x^2y + x^3 - x \xrightarrow{f_1} x^3 + y - 2x$ (reducido con respecto a G)

Sea $f_5 := x^3 + y - 2x$

Notar que $f_5 = (f_2 + xf_3) - f_1 = (xy - 1)f_1 + (-x^2 + 1)f_2$

$$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}.$$

$$G := \{f_1, f_2, f_3, f_4, f_5\}.$$

$$\begin{aligned} S(f_1, f_4) &= x^2(x^2y - y + x) - y(x^4 + xy - 2x^2) \\ &= -xy^2 + yx^2 + x^3 \\ &\xrightarrow{f_2} yx^2 + x^3 - x \\ &\xrightarrow{f_1} x^3 + y - 2x \xrightarrow{f_5} 0 \\ S(f_2, f_4) &= x^3(xy^2 - x) - y^2(x^4 + xy - 2x^2) \\ &= -y^3x + 2y^2x^2 - x^4 \\ &\xrightarrow{f_2} 2y^2x^2 - x^4 - yx \end{aligned}$$

$$\begin{aligned}
&\xrightarrow{f_2} -x^4 - yx + 2x^2 \xrightarrow{f_4} 0 \\
\operatorname{mcd}(\operatorname{lp}(f_3), \operatorname{lp}(f_4)) &= \operatorname{mcd}(y^2, x^4) = 1 \\
S(f_1, f_5) &= x(x^2y - y + x) - y(x^3 + y - 2x) \\
&= -y^2 + xy + x^2 \xrightarrow{f_3} 0 \\
S(f_2, f_5) &= x^2(xy^2 - x) - y^2(x^3 + y - 2x) \\
&= -y^3 + 2xy^2 - x^3 \\
&\xrightarrow{f_3} xy^2 - x^2y - x^3 \\
&\xrightarrow{f_2} -x^2y - x^3 + x \\
&\xrightarrow{f_1} -x^3 - y + 2x \xrightarrow{f_5} 0 \\
\operatorname{mcd}(\operatorname{lp}(f_3), \operatorname{lp}(f_5)) &= mcd(y^2, x^3) = 1 \\
S(f_4, f_5) &= (x^4 + xy - 2x^2) - x(x^3 + y - 2x) = 0.
\end{aligned}$$

Luego $G = \{f_1, f_2, f_3, f_4, f_5\}$ es una base de Gröbner para I. Ahora desde que $\operatorname{lp}(f_2) = xy^2$ es divisible por $\operatorname{lp}(f_3) = y^2$ y $\operatorname{lp}(f_4) = x^4$ es divisible por $\operatorname{lp}(f_5) = x^3$, pueden ser omitidos para formar

$$\{f_1, f_3, f_5\} = \{x^2y - y + x, -y^2 + xy + x^2, x^3 + y - 2x\}$$

una base de Gröbner para I con respecto al orden deglex con $y > x$. Y como hemos registrado las combinaciones lineales de f_1 y f_2 que generan a f_3 y f_5 tenemos que:

$$\begin{bmatrix} f_1 \\ f_3 \\ f_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ y & -x \\ xy - 1 & -x^2 + 1 \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix}. \tag{3.2}$$

Para el polinomio

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

Veamos (notando que si X es un término, entonces $f \xrightarrow{X,g} h$ quiere decir $h = f + Xg$) que $f \in I$:

$$\begin{aligned}
f &\xrightarrow{-x^2, f_1} -2x^5 + 2x^2y^2 - 2x^3y - 2x^4 - 2y^3 + 4xy^2 - 2x^2y + x^3 - y + 2x \\
&\xrightarrow{2x^2, f_5} 2x^2y^2 - 2x^3y - 2x^4 - 2y^3 + 4xy^2 - 3x^3 - y + 2x
\end{aligned}$$

$$\xrightarrow{-2y,f_1} -2x^3y - 2x^4 - 2y^3 + 4xy^2 - 3x^3 + 2y^2 - 2xy - y + 2x$$
$$\xrightarrow{2y,f_5} -2x^4 - 2y^3 + 4xy^2 - 3x^3 + 4y^2 - 6xy - y + 2x$$
$$\xrightarrow{2x,f_5} -2y^3 + 4xy^2 - 3x^3 + 4y^2 - 4xy - 4x^2 - y + 2x$$
$$\xrightarrow{-2y,f_3} 2xy^2 - 2x^2y - 3x^3 + 4y^2 - 4xy - 4x^2 - y + 2x$$
$$\xrightarrow{2x,f_3} -x^3 + 4y^2 - 4xy - 4x^2 - y + 2x$$
$$\xrightarrow{1,f_5} 4y^2 - 4xy - 4x^2$$
$$\xrightarrow{4,f_3} 0.$$

Luego

$$\begin{aligned} f &= x^2 f_1 - 2x^2 f_5 + 2y f_1 - 2y f_5 - 2x f_5 + 2y f_3 - 2x f_3 - f_5 - 4 f_3 \\ &= (x^2 + 2y) f_1 + (2y - 2x - 4) f_3 + (-2x^2 - 2y - 2x - 1) f_5. \end{aligned}$$

Usando la ecuación (3.2) obtenemos

$$\begin{aligned} f =& (x^2 + 2y) f_1 + (2y - 2x - 4)(y f_1 - x f_2) \\ &+ (-2x^2 - 2y - 2x - 1)((xy - 1) f_1 + (-x^2 + 1) f_2) \\ =& (-2x^3 y - 2xy^2 - 2x^2 y + 2y^2 - 3xy + 3x^2 + 2x + 1) f_1 \\ &+ (2x^4 + 2x^2 y + 2x^3 - 2xy + x^2 - 2y + 2x - 1) f_2. \end{aligned}$$

El segundo problema (ii), determinar si es que dos ideales I, J son iguales, es una consecuencia del teorema 2.15. Es decir, $I = J$ si y sólo si I y J tienen la misma base de Gröbner reducida. En particular $I = k[x_1, \ldots, x_n]$ si y sólo si la base de Gröbner reducida para I es $\{1\}$. Alternativamente, $I = \langle f_1, \ldots, f_s \rangle \subseteq J$ si y sólo si $f_1, \ldots, f_s \in J$, y sabemos como determinar eso; entonces para ver si $I = J$ bastaría con verificar $I \subseteq J$ y $J \subseteq I$.

Consideremos ahora el problema (iii), encontrar representantes de clase para cada elemento de $k[x_1, \ldots, x_n]/I$, $I = \langle G \rangle$, donde $G = \{g_1, \ldots, g_t\}$ es una base de Gröbner para I. Sabemos que para todo $f \in k[x_1, \ldots, x_n]$ existe un único elemento $r \in k[x_1, \ldots, x_n]$, reducido con respecto a G, tal que $f \xrightarrow{G} r$.

Definición 3.1. Al elemento r anterior se le llama la forma normal de f con respecto a G, y es denotado por $N_G(f)$.

Proposición 3.1. Sean $f, g \in k[x_1, \ldots, x_n]$. Entonces

$$(f - g \in I) f \equiv_I g \iff N_G(f) = N_G(g).$$

Por tanto $\{N_G(f) \mid f \in k[x_1, \ldots, x_n]\}$ es un conjunto de representantes de clase para $k[x_1, \ldots, x_n]/I$. Además, la aplicación $N_G : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$ es k-lineal.

Prueba. Sean $f_1, f_2 \in k[x_1, \ldots, x_n]$, podemos escribir $f_1 = \sum_i u_i g_i + N_G(f_1)$, $f_2 = \sum_i v_i g_i + N_G(f_2)$ y $f_1 + f_2 = \sum_i w_i g_i + N_G(f_1 + f_2)$ entonces combinando estas ecuaciones

$$N_G(f_1 + f_2) - N_G(f_1) - N_G(f_2) \in I \implies N_G(f_1 + f_2) = N_G(f_1) + N_G(f_2)$$

, claramente se puede generalizar a $N_G(c_1 f_1 + c_2 f_2) = c_1 N_G(f_1) + c_2 N_G(f_2)$ con $c_1, c_2 \in k$.
$(\implies)$ Existe $q \in I$ tal que $f = q + g$. Así $N_G(f) = N_G(q) + N_G(g) = N_G(g)$.
$(\impliedby)$ Si $N_G(f) = N_G(g)$, entonces $f - g = (f - N_G(f)) - (g - N_G(g)) \in I$. □

Ejemplo 3.2. Del ejemplo 3.1, $I = \langle f_1, f_3, f_5 \rangle = \langle x^2y - y + x, -y^2 + xy + x^2, x^3 + y - 2x \rangle$ forman un base de Gröbner. Notamos que

$$x^3 = f_5 - y + 2x.$$

Desde que $-y + 2x$ es reducido, tenemos $N_G(x^3) = -y + 2x$. También,

$$x^2y + y = f_1 + 2y - x.$$

Desde que $2y - x$ es reducido, tenemos $N_G(x^2y + y) = 2y - x$. Luego $N_G(x^3) \neq N_G(x^2y + y)$, entonces $\overline{x^3} \neq \overline{x^2y + y} \pmod{I}$.

Consideremos ahora el problema (iv), es decir deseamos determinar una base para el k-espacio vectorial $k[x_1, \ldots, x_n]/I$.

Proposición 3.2. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I. Una base para el k-espacio vectorial $k[x_1, \ldots, x_n]/I$ consiste de las clases de todos los productos de potencias $X \in M_n$ tales que $\mathrm{lp}(g_i)$ no divide a X para todo $i = 1, 2, \ldots, t$.

Prueba. Para todo $f \in k[x_1, \ldots, x_n]$, $\overline{f} = \overline{N_G(f)}$. Desde que $N_G(f)$ es reducida con respecto a G, es por definición una k-lineal combinación de productos de potencia X tales que los $\mathrm{lp}(g_i)$'s no dividen a X. Finalmente $c_1X_1 + \cdots + c_nX_n \in I$ con los X_i's reducidos implica $c_1X_1 + \cdots + c_nX_n = 0$ luego los c_i's son todos nulos (identidad de polinomios). □

Ejemplo 3.3. Del ejemplo 3.1. Una base de Gröbner para I con respecto al orden deglex con $x < y$ es $G = \{x^2y - y + x, -y^2 + xy + x^2, x^3 + y - 2x\}$. Luego una base para $\mathbb{Q}[x, y]/I$ consiste de las clases de $1, x, y, x^2, xy$ y $dim(\mathbb{Q}[x, y]/I) = 5$.

Ahora ya podemos resolver el problema (v), es decir dar una tabla de multiplicación para $k[x_1, \ldots, x_n]/I$.

$$\overline{f}\,\overline{g} = \overline{N_G(fg)}$$

$$(f + I)(g + I) = N_G(fg) + I$$

Ejemplo 3.4. Para el ejemplo 3.1, $(y+I)(xy+I) = N_G(xy^2)+I$. Desde que $xy^2 \xrightarrow{G} x$ con x reducido respecto a G, $N_G(xy^2) = x$ y entonces $(y+I)(xy+I) = x+I$. El resto de productos son calculados de una manera similar para obtener la siguiente tabla de multiplicación para la $\mathbb{Q}$-base $\{1 + I, x + I, y + I, x^2 + I, xy + I\}$ de $\mathbb{Q}[x, y]/I$.

$\times$	1	x	y	x^2	xy
1	1	x	y	x^2	xy
x	x	x^2	xy	$-y + 2x$	$y - x$
y	y	xy	$xy + x^2$	$y - x$	x
x^2	x^2	$-y + 2x$	$y - x$	$-xy + 2x^2$	$xy - x^2$
xy	xy	$y - x$	x	$xy - x^2$	x^2

Por ejemplo para el producto, $(2x^2 + y)(3xy - 5) = 6x^3y - 10x^2 + 3xy^2 - 5y \equiv 6(xy - x^2) - 10x^2 + 3x - 5y = 6xy - 16x^2 - 5y + 3x \pmod{I}$.

El problema (vi), determinar si un elemento $f + I \in k[x_1, \ldots, x_n]/I$ tiene una inversa, y calcularla. Dado una k-base finita y una tabla de multiplicación como en el ejemplo anterior, el problema se traduce en resolver un sistema de ecuaciones lineales.

Ejemplo 3.5. Para el ejemplo 3.1, queremos determinar si $y+x+1+I$ es invertible,y si es, calcular su inversa. Entonces buscamos $a, b, c, d, e \in \mathbb{Q}$ tales que

$$(axy + bx^2 + cy + dx + e)(y + x + 1) \equiv_I 1.$$

Ahora,

$$(axy + bx^2 + cy + dx + e)(y + x + 1)$$

$$= axy^2 + ax^2y + axy + bx^2y + bx^3 + bx^2 + cy^2 + cxy$$

$$
\begin{aligned}
&+ cy + dxy + dx^2 + dx + ey + ex + e \\
\equiv_I &ax + a(y - x) + axy + b(y - x) + b(-y + 2x) + bx^2 \\
&+ c(xy + x^2) + cxy + cy + dxy + dx^2 + dx + ey + ex + e \\
=&(a + 2c + d)xy + (b + c + d)x^2 + (a + c + e)y + (b + d + e)x + e.
\end{aligned}
$$

Luego $(axy + bx^2 + cy + dx + e)(y + x + 1) \equiv_I 1$ si y sólo si

$$
\begin{cases}
a + 2c + d = 0 \\
b + c + d = 0 \\
a + c + e = 0 \\
b + d + e = 0 \\
e = 1
\end{cases}
$$

desde que las clases de $1, x, y, x^2, xy$ forman una base del $\mathbb{Q}$-espacio vectorial $\mathbb{Q}[x, y]/I$. Estas ecuaciones se resuelven fácilmente para obtener $a = -2, b = -1, c = 1, d = 0, e = 1$. Por tanto $(-2xy - x^2 + y + 1) + I$ es una inversa de $y + x + 1 + I$ en $\mathbb{Q}[x, y]/I$. Por supuesto si hubieramos empezado con un elemento no invertible, estas ecuaciones no tendrían solución.

Un método alternativo que no requiere que $k[x_1, \ldots, x_n]/I$ tenga una k-base finita, es reconocer que $f + I$ tiene una inversa en $k[x_1, \ldots, x_n]/I$ si y sólo si el ideal $\langle I, f\rangle$ es, de hecho, todo $k[x_1, \ldots, x_n]$, desde que $fg - 1 \in I$ si y sólo si $1 \in \langle I, f\rangle$. Así dado un ideal $I = \langle f_1, \ldots, f_s\rangle$ y un polinomio $f \in k[x_1, \ldots, x_n]$, primero calculamos la base de Gröbner reducida H para el ideal $\langle f_1, \ldots, f_s, f\rangle$. Si $H \neq \{1\}$, entonces $f + I$ no posee una inversa en $k[x_1, \ldots, x_n]/I$. Si $H = \{1\}$, entonces, como en la solución del problema (i),podemos expresar

$$1 = h_1 f_1 + \cdots + h_s f_s + gf.$$

El polinomio obtenido g es la inversa de f.

Ejemplo 3.6. Otra vez en el ejemplo 3.1, deseamos conocer la inversa del polinomio $y + x + 1$. Primero calculamos una base de Gröbner para el ideal $\langle f_1, f_3, f_5, y + x + 1\rangle$,

donde $f_1 = x^2y - y + x$, $f_3 = -y^2 + xy + x^2$, $f_5 = x^3 + y - 2x$, con respecto al orden deglex con $y > x$, registrando los multiplicadores como en el ejemplo 3.1. Escribiendo $f_6 = y + x + 1$ calculamos

$$\begin{aligned}
S(f_1, f_6) &= f_1 - x^2 f_6 = -x^3 - x^2 - y + x \\
&\xrightarrow{f_5} -x^2 - x = f_7 \\
&\boxed{f_7 = f_1 - x^2 f_6 + f_5} \\
S(f_3, f_6) &= -f_3 - y f_6 = -2yx - x^2 - y \\
&\xrightarrow{2x, f_6} x^2 - y + 2x \\
&\xrightarrow{1, f_7} -y + x \xrightarrow{1, f_6} 2x + 1 = f_8 \\
f_8 &= -f_3 - y f_6 + 2x f_6 + f_7 + f_6 \\
f_8 &= -f_3 + (-y + 2x + 1) f_6 + f_1 - x^2 f_6 + f_5 \\
&\boxed{f_8 = f_1 - f_3 + f_5 + (-x^2 - y + 2x + 1) f_6} \\
\mathrm{mcd}(\mathrm{lp}(f_5), \mathrm{lp}(f_6)) &= \mathrm{mcd}(x^3, y) = 1 \\
\mathrm{mcd}(\mathrm{lp}(f_3), \mathrm{lp}(f_7)) &= \mathrm{mcd}(y^2, x^2) = 1 \\
\mathrm{mcd}(\mathrm{lp}(f_6), \mathrm{lp}(f_7)) &= \mathrm{mcd}(y, x^2) = 1 \\
\mathrm{mcd}(\mathrm{lp}(f_3), \mathrm{lp}(f_8)) &= \mathrm{mcd}(y^2, x) = 1 \\
\mathrm{mcd}(\mathrm{lp}(f_6), \mathrm{lp}(f_8)) &= \mathrm{mcd}(y, x) = 1 \\
\mathrm{lp}(f_6) &= y \mid x^2 y = \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_7)) \\
\mathrm{lp}(f_8) &= x \mid x^3 = \mathrm{mcm}(\mathrm{lp}(f_5), \mathrm{lp}(f_7)) \\
\mathrm{lp}(f_6) &= y \mid x^2 y = \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_8)) \\
S(f_5, f_8) &= f_5 - \frac{x^2}{2} f_8 = -\frac{x^2}{2} + y - 2x \\
&\xrightarrow{-\frac{1}{2}, f_7} y - \frac{3x}{2} \\
&\xrightarrow{-1, f_6} -\frac{5x}{2} - 1 \\
&\xrightarrow{\frac{5}{4}, f_8} \frac{1}{4} = f_9 \\
S(f_7, f_8) &= -f_7 - \frac{x}{2} f_8 = \frac{x}{2} \\
&\xrightarrow{-\frac{1}{4}, f_8} -\frac{1}{4} \xrightarrow{f_9} 0
\end{aligned}$$

Luego todos los otros S-polinomios se reducen a cero utilizando el polinomio $f_9 = \frac{1}{4}$. Del proceso de reducción para llegar a f_9 tenemos:

$$\begin{aligned}1 &= 4f_5 - 4f_6 - 2f_7 - (2x^2 - 5)f_8 \\ &= 4f_5 - 4f_6 - 2(f_1 - x^2 f_6 + f_5) - (2x^2 - 5)(f_1 - f_3 + f_5 + (-x^2 - y + 2x + 1)f_6) \\ &= (-2x^2 + 3)f_1 + (2x^2 - 5)f_3 + (-2x^2 + 7)f_5 + (2x^4 + 2x^2 y - 4x^3 - 5x^2 - 5y + 10x + 1)f_6,\end{aligned}$$

obtenemos la inversa $(2x^4 + 2x^2y - 4x^3 - 5x^2 - 5y + 10x + 1) + I$, y usando la tabla del ejemplo 3.4, $= (2(-xy + 2x^2) + 2(y - x) - 4(-y + 2x) - 5x^2 - 5y + 10x + 1) + I = (-2xy - x^2 + y + 1) + I$ llegando al mismo resultado que en el ejemplo 3.5.

3.2 Resolución de Sistemas de Ecuaciones Polinomiales

En el caso de sistemas de ecuaciones lineales, tenemos el método de eliminación gaussiana o eliminación por filas para obtener sus soluciones. En esta sección se expondrá un método similar, basado en la teoría de bases de Gröbner, para resolver sistemas de ecuaciones polinomiales no-lineales. Veamos un ejemplo:

Ejemplo 3.7. Sean $f_1 = x + 2y + z$, $f_2 = x + 3y + 2z$ y $f_3 = 3x + 6y + z$ polinomios lineales en $\mathbb{R}[x, y, z]$. Consideremos el sistema:

$$\begin{aligned}x + 2y + z &= 0 \\ x + 3y + 2z &= 0 \\ 3x + 6y + z &= 0\end{aligned}$$

Y el proceso de reducción por fila correspondiente:

$$\begin{bmatrix}1 & 2 & 1 \\ 1 & 3 & 2 \\ 3 & 6 & 1\end{bmatrix} \xrightarrow{f_3 - 3f_1} \begin{bmatrix}1 & 2 & 1 \\ 1 & 3 & 2 \\ 0 & 0 & -2\end{bmatrix} \xrightarrow{f_2 - f_1} \begin{bmatrix}1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -2\end{bmatrix}.$$

Así la solución única es: $x = y = z = 0$. La intersección de tres planos en $\mathbb{R}^3$ que pasan por el origen.

Ahora aplicaremos la teoría de las Bases de Gröbner para el siguiente ejemplo:

Ejemplo 3.8. Queremos resolver el sistema:

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

La base de Gröbner del ideal $I = \langle x^2+y^2+z^2-1, x^2+z^2-y, x-y\rangle$ con respecto al orden lex $x > y > z$ es $g_1 = x-y$, $g_2 = -2y+z^2+1$, $g_3 = z^4+4z^2-1$, desde que

$$\begin{aligned} f_1 &= x^2+y^2+z^2-1 \\ f_2 &= x^2+z^2-y \\ f_3 &= x-y \\ S(f_1,f_2) &= y^2+y-1 = f_4 \\ S(f_2,f_3) &= xy-y+z^2 \\ &\xrightarrow{f_3} y^2-y+z^2 \\ &\xrightarrow{f_4} -2y+z^2+1 = f_5 \\ S(f_1,f_3) &= xy+y^2+z^2-1 \\ &\xrightarrow{f_3} 2y^2+z^2-1 \\ &\xrightarrow{f_4} -2y+z^2+1 \\ &\xrightarrow{f_5} 0 \\ \mathrm{mcd}(\mathrm{lp}(f_1),\mathrm{lp}(f_4)) &= \mathrm{mcd}(x^2,y^2) = 1 \\ \mathrm{mcd}(\mathrm{lp}(f_2),\mathrm{lp}(f_4)) &= \mathrm{mcd}(x^2,y^2) = 1 \\ \mathrm{mcd}(\mathrm{lp}(f_3),\mathrm{lp}(f_4)) &= \mathrm{mcd}(x,y^2) = 1 \\ \mathrm{mcd}(\mathrm{lp}(f_1),\mathrm{lp}(f_5)) &= \mathrm{mcd}(x^2,y) = 1 \\ \mathrm{mcd}(\mathrm{lp}(f_2),\mathrm{lp}(f_5)) &= \mathrm{mcd}(x^2,y) = 1 \\ \mathrm{mcd}(\mathrm{lp}(f_3),\mathrm{lp}(f_5)) &= \mathrm{mcd}(x,y) = 1 \\ S(f_4,f_5) &= \frac{yz^2}{2}+\frac{3y}{2}-1 \\ &\xrightarrow{f_5} \frac{3y}{2}+\frac{z^4}{4}+\frac{z^2}{4}-1 \\ &\xrightarrow{f_5} \frac{z^4}{4}+z^2-\frac{1}{4} = f_6, \end{aligned}$$

el resto de S-polinomios se reducen a cero aplicando el **crit1**. Notamos que $lp(f_3) = x$ divide a $lp(f_1) = lp(f_2) = x^2$ y $lp(f_5) = y$ divide a $lp(f_4) = y^2$ lo que nos permite reducir la base de Gröbner al conjunto $\{f_3, f_5, f_6\}$. Sabemos que si $I = \langle g_1, g_2, g_3 \rangle$, las soluciones del sistema:

$$\begin{cases} x - y & = 0 \\ -2y + z^2 + 1 & = 0 \\ z^4 + 4z^2 - 1 & = 0 \end{cases}$$

son equivalentes a las soluciones del sistema original y resolver el sistema en los polinomios de la base de Gröbner resulta más conveniente. En el caso de nuestro ejemplo implica resolver primero la ecuación en una sola variable z: $z^4 + 4z^2 - 1 = 0$ y luego reemplazar en $x = y$ e $y = \frac{z^2+1}{2}$. Desde que

$$(-2 + \sqrt{5})^2 + 4(-2 + \sqrt{5}) - 1 = 9 - 4\sqrt{5} - 8 + 4\sqrt{5} - 1 = 0$$

obtenemos $z = \pm\sqrt{-2 + \sqrt{5}}$ dos raíces reales para el polinomio $z^4 + 4z^2 - 1 = 0$ y además de

$$(-2 - \sqrt{5})^2 + 4(-2 - \sqrt{5}) - 1 = 9 + 4\sqrt{5} - 8 - 4\sqrt{5} - 1 = 0$$

obtenemos $z = \pm\sqrt{-2 - \sqrt{5}} = \pm\sqrt{2 + \sqrt{5}}i$ dos raíces complejas para el polinomio $z^4 + 4z^2 - 1 = 0$. Luego hemos encontrado las soluciones para el sistema

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

las cuales son las siguientes

$$\begin{aligned} (x_1, y_1, z_1) &= (\frac{-1 + \sqrt{5}}{2}, \frac{-1 + \sqrt{5}}{2}, \sqrt{-2 + \sqrt{5}}) \\ (x_2, y_2, z_2) &= (\frac{-1 + \sqrt{5}}{2}, \frac{-1 + \sqrt{5}}{2}, -\sqrt{-2 + \sqrt{5}}) \\ (x_3, y_3, z_3) &= (\frac{-1 - \sqrt{5}}{2}, \frac{-1 - \sqrt{5}}{2}, \sqrt{2 + \sqrt{5}}i) \\ (x_4, y_4, z_4) &= (\frac{-1 - \sqrt{5}}{2}, \frac{-1 - \sqrt{5}}{2}, -\sqrt{2 + \sqrt{5}}i) \end{aligned}$$

Así la teoría de las Bases de Gröbner nos brinda un método más formal al simple tanteo y reemplazo, además de ser un método directamente programable.

No siempre el nuevo sistema a resolver en los polinomios de la base de Gröbner resultará más conveniente, pero elegiendo un orden monomial adecuado y bajo ciertas hipótesis podemos reducir el problema a resolver un sistema *triangular*. Para esto será necesario definir lo que es una variedad y su relación con los sistemas de ecuaciones polinomiales:

Definición 3.2. Sea S un conjunto de polinomios en $k[x_1, \ldots, x_n]$. Definimos la variedad $V(S)$ en K^n como:

$$V(S) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0, \forall f \in S\}.$$

La variedad en k definida por un conjunto de polinomios $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ es el conjunto de soluciones en k^n del sistema de ecuaciones polinomiales $f_1 = 0, \ldots, f_s = 0$ y claramente coincide con la variedad del ideal generado por estos polinomios y por tanto con la variedad de cualquier conjunto de generadores de dicho ideal. También dado un sub-conjunto $V \subseteq k^n$ podemos definir el ideal

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

A continuación se probará un conocido teorema utilizando la teoría de las bases de Gröbner.

Teorema 3.1 (Hilbert Nullstellensatz débil)**.** [ref.[Cox D.],cáp.4,pág.177-178] Sea I un ideal en $k[x_1, \ldots, x_n]$ y consideremos k algebraicamente cerrado. Entonces $V(I) = \emptyset$ si, y sólo si $I = k[x_1, \ldots, x_n]$.

Prueba. Probaremos que

$$I \subsetneqq k[x_1, \ldots, x_n] \implies V(I) \neq \emptyset.$$

Dado $a \in k$ y $f \in k[x_1, \ldots, x_n]$. Sea $f' = f(x_1, \ldots, x_{n-1}, a) \in k[x_1, \ldots, x_{n-1}]$ y el siguiente ideal de $k[x_1, \ldots, x_{n-1}]$

$$I_{x_n=a} = \{f' \mid f \in I\}$$

Afirmación. Si k es algebráicamente cerrado y $I \subsetneqq k[x_1, \ldots, x_n]$ entonces existe $a \in k$ tal que

$$I_{x_n=a} \subsetneqq k[x_1, \ldots, x_{n-1}]$$

Una vez probada esta afirmación un simple proceso de inducción nos da $a_1, \ldots, a_n \in k$ tales que $I_{x_1=a_1,\ldots,x_n=a_n} \subsetneqq k$, entonces $I_{x_1=a_1,\ldots,x_n=a_n} = \{0\}$. Lo que implica $(a_1, \ldots, a_n) \in V(I)$, y concluimos que $V(I) \neq \emptyset$.

Para probar la afirmación consideraremos los siguientes dos casos:

Caso 1. $I \cap k[x_n] \neq \{0\}$.

Sea $f \in I \cap k[x_n]$ no-nulo. Notemos que f es no-constante ya que de otra manera se tendría $1 \in I \cap k[x_n] \subseteq I$ lo que contradice $I \neq k[x_1, \ldots, x_n]$.

Desde que k es algebráicamente cerrado podemos escribir

$$f = c\prod_{i=1}^{r}(x_n - b_i)^{m_i}$$

donde $c, b_1, \ldots, b_n \in k$ y $c \neq 0$. Supongamos que $I_{x_n=b_i} = k[x_1, \ldots, x_{n-1}]$ para todo $i = 1, \ldots, r$. Entonces para todo i existe $B_i \in I$ con $B_i(x_1, \ldots, x_{n-1}, b_i) = 1$. Esto implica que

$$1 = B_i(x_1, \ldots, x_{n-1}, b_i) = B_i(x_1, \ldots, x_{n-1}, x_n - (x_n - b_i)) = B_i + A_i(x_n - b_i),$$

para algunos $A_i \in k[x_1, \ldots, x_n]$. Luego

$$1 = \prod_{i=1}^{r}(A_i(x_n - b_i) + B_i)^{m_i} = A\prod_{i=1}^{r}(x_n - b_i)^{m_i} + B,$$

donde $A = \prod_{i=1}^{r} A_i^{m_i}, B \in I$. Además $\prod_{i=1}^{r}(x_n - b_i)^{m_i} = c^{-1}f \in I$ lo que implica $1 \in I$, contradiciendo $I \neq k[x_1, \ldots, x_n]$. Así tenemos $I_{x_n=b_i} \neq k[x_1, \ldots, x_{n-1}]$ para algún i, y podemos tomar $a = b_i$.

Caso 2. $I \cap k[x_n] = \{0\}$. Sea $\{g_1, \ldots, g_t\}$ una base de Gröbner para I para el orden lex con $x_1 > x_2 > \cdots > x_n$ y escribamos

$$g_i = c_i(x_n)\boldsymbol{X}^{\boldsymbol{\alpha_i}} + \text{ términos} < \boldsymbol{X}^{\boldsymbol{\alpha_i}} \tag{3.3}$$

,donde $c_i(x_n) \in k[x_n]$ es no-nulo y $\boldsymbol{X}^{\boldsymbol{\alpha_i}}$ es un monomio en $x_1, \ldots, x_{n-1}$. Desde que los campos algebráicamente cerrados son infinitos podemos encontrar un $a \in k$ tal que $c_i(a) \neq 0$ para todo $i = 1, \ldots, r$. Se verifica fácilmente que los polinomios

$$g_i' = g_i(x_1, \ldots, x_{n-1}, a)$$

generan al ideal $I_{x_n=a}$. Luego, desde que $c_i(a) \neq 0$, sustituyendo $x_n = a$ en la ecuación (3.3) se tiene $\mathrm{lt}(g_i') = c_i(a)\boldsymbol{X}^{\boldsymbol{\alpha_i}}$. En caso $\boldsymbol{X}^{\boldsymbol{\alpha_i}} = 1$, se tendría $g_i = c_i \in I \cap k[x_n] = \{0\}$, por tanto $\boldsymbol{X}^{\boldsymbol{\alpha_i}} \neq 1$. Es decir $\mathrm{lt}(g_i')$ es no-constante para cada $i = 1, \ldots, r$. Veamos que los g_i' forman una base de Gröbner para $I_{x_n=a}$. Sea $f' \in I_{x_n=a}$, es decir $f' = f(x_1, \ldots, x_{n-1}, a)$ con $f \in I$. Luego para algún $1 \leq i \leq r$, se tiene $\mathrm{lp}(g_i) = \mathrm{lp}(c_i(x_n))\boldsymbol{X}^{\boldsymbol{\alpha_i}}$ divide a $\mathrm{lp}(f)$ y desde que $\mathrm{lp}(g_i') = \boldsymbol{X}^{\boldsymbol{\alpha_i}} \neq 1$ se cumple $\mathrm{lp}(g_i') \mid \mathrm{lp}(f')$ (expresando a f como en la ecuación (3.3)). Finalmente $1 \notin I_{x_n=a}$ ya que ningún $\mathrm{lp}(g_i')$ divide a 1. Así $I_{x_n=a} \neq k[x_1, \ldots, x_{n-1}]$. □

Y como consecuencia directa se obtiene el siguiente resultado:

Proposición 3.3. Sea I un ideal en $k[x_1, \ldots, x_n]$ y G una base de Gröbner reducida para I. $V_{\overline{k}}(I) = \emptyset$ si, y sólo si $1 \in G$. Y entonces si $I = \langle f_1, \ldots, f_s \rangle$: el sistema de ecuaciones $f_1 = \cdots = f_s = 0$ no tiene soluciones en $\overline{k}^n \iff G = \{1\}$.

Prueba. La prueba es directa utilizando el teorema anterior. □

Por ejemplo para $k = \mathbb{C}$ podemos reformular la proposición anterior como *el teorema fundamental del álgebra para polinomios multivariables* - todo sistema de polinomios que generen un ideal estrictamente menor a $\mathbb{C}[x_1, \ldots, x_n]$ tienen una raíz común en $\mathbb{C}^n$ (ref.[Cox D.],cáp.4,pág.178).

Es interesante resaltar la siguiente propiedad de $I(V)$:

Lema 3.1. Sea V una variedad. Si $f^m \in I(V)$, entonces $f \in I(V)$.

Prueba. Desde que para $a \in V$, $f^m(a) = 0$ implica $f(a) = 0$. □

Si generalizamos la propiedad anterior para ideales en $k[x_1, \ldots, x_n]$ obtenemos:

Definición 3.3. Para un ideal I de $k[x_1, \ldots, x_n]$. Definimos el ideal radical de I por

$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid f^m \in I, \quad \text{para algún} \quad m \in \mathbb{N}\}$$

Y la importancia de la definición anterior se formula en el siguiente resultado:

Teorema 3.2. [Hilbert Nullstellensatz Fuerte] Si consideramos k algebráicamente cerrado. Para todo ideal I de $k[x_1, \ldots, x_n]$ se cumple

$$I(V(I)) = \sqrt{I}.$$

Prueba. ref. [Cox D.], cáp.4, pág.183. □

El siguiente teorema relaciona la cardinalidad de la variedad de un ideal con la forma de los polinomios de la base de Gröbner y con la dimensión del espacio cociente inducido:

Teorema 3.3. [ref.[Adams W.],cáp.2,pág.63] Sea $G = \{g_1 \dots, g_t\}$ una base de Gröbner para el ideal $I \subset k[x_1, \dots, x_n]$. Las siguientes afirmaciones son equivalentes:

(i) La variedad $V_{\overline{k}}(I)$ es finita.

(ii) Para cada $i = 1, \dots, n$, existe un $j \in \{1, \dots, t\}$ tal que $\mathrm{lp}(g_j) = x_i^m$ para algún $m \in \mathbb{N}$.

(iii) La dimensión del k-espacio vectorial $\frac{k[x_1,\dots,x_n]}{I}$ es finita.

Prueba. $(i) \implies (ii)$. Podemos asumir que $V_{\overline{k}}(I)$ es no-vacío. Fijamos $i \in \{1, \dots, n\}$. Sean $a_{ij}, j = 1, \dots, l$ las distintas i-ésimas coordenadas de los puntos en $V_{\overline{k}}(I)$. Para cada $j, 1 \leq j \leq l$, sea $f_j \in k[x_i]$ no-nulo tal que $f_j(a_{ij}) = 0$. Consideremos

$$f = f_1 f_2 \dots f_l \in k[x_i] \subseteq k[x_1, \dots, x_n].$$

Claramente $f \in I(V_{\overline{k}}(I))$, y por el teorema 3.2 existe $m \in \mathbb{N}$ tal que $f^m \in I$. Luego $\mathrm{lp}(f^m)$ es una potencia de solamente x_i y es divisible por algún $\mathrm{lp}(g_s)$.

$(ii) \implies (iii)$. Directamente por la proposición 3.2.

$(iii) \implies (i)$. Tomemos cualquier $1 \leq i \leq n$. Por hipótesis el siguiente conjunto $\{1, x_i, x_i^2, \dots\}$ es linealmente dependiente módulo I, es decir podemos escribir para constantes no todas nulas $c_j \in k, 0 \leq j \leq m$:

$$\sum_{j=0}^{m} c_j x_i^j \in I.$$

El polinomio anterior posee solamente un número finito de raíces en $\overline{k}$, lo que implica que existen solamente un número finito de valores diferentes para las i-ésimas coordenadas de puntos en $V_{\overline{k}}(I)$. □

Un ideal $I \neq k[x_1, \dots, x_n]$ que satisface cualquiera de las condiciones en el teorema anterior es llamado cero-dimensional (debido a la finitud del conjunto $V_{\overline{k}}(I)$). De la

parte (ii) en el teorema anterior se sigue que podemos reordenar los g_j tal que $\mathrm{lp}(g_j)$ es una potencia de x_j y además si consideramos el orden monomial lex $x_1 < x_2 < \cdots < x_n$, las únicas variables que aparecen en g_j serián $x_1, x_2, \ldots, x_j$. Esto nos lleva al siguiente corolario:

Corolario 3.1. Sea I un ideal cero-dimensional y $G = \{g_1, \ldots, g_t\}$ la base de Gröbner reducida para I con respecto al orden monomial lex con $x_1 < x_2 < \cdots < x_n$. Entonces se puede reordenar $g_1, \ldots, g_t$ tal que g_1 contiene sólo las variables x_1, g_2 contiene sólo las variables x_1, x_2 y $\mathrm{lp}(g_2)$ es una potencia de x_2, g_3 contiene sólo las variables x_1, x_2, x_3 y $\mathrm{lp}(g_3)$ es una potencia de x_3, y así sucesivamente hasta g_n.

Es decir: Para un ideal cero-dimensional podemos encontrar una base de Gröbner que esté en forma triangular.

Ejemplo 3.9. Sea el sistema en $\mathbb{Q}[x, y]$:

$$\begin{cases} x^2y - y + x & = 0 \\ xy^2 - x & = 0 \end{cases}$$

En el ejemplo 3.1, para el ideal $I = \langle x^2y - y + x, xy^2 - x\rangle$, calculamos la siguiente base de Gröbner con respecto al orden monomial deglex, $x < y$, $G = \{x^2y - y + x, -y^2 + xy + x^2, x^3 + y - 2x\}$. Desde que x^3 e y^2 aparecen como potencias principales de elementos de G, se sigue del teorema anterior que I es cero-dimensional y que $V_{\overline{\mathbf{Q}}}(I)$ es finito. La base de Gröbner reducida con respecto a lex, $x < y$, para I

$$\begin{aligned} f_1 &= x^2y - y + x \\ f_2 &= xy^2 - x \\ S(f_1, f_2) &= y(x^2y - y + x) - x(xy^2 - x) \\ &= -y^2 + yx + x^2 = f_3 \\ \mathrm{lp}(f_2) &= xy^2 \mid x^2y^2 = \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_3)) \\ S(f_2, f_3) &= (xy^2 - x) - (-x)(-y^2 + yx + x^2) \\ &= yx^2 + x^3 - x \\ &\xrightarrow{f_1} y + x^3 - 2x = f_4 \\ \mathrm{lp}(f_3) &= y^2 \mid xy^2 = \mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_4)) \end{aligned}$$

$$
\begin{aligned}
S(f_1, f_4) &= (x^2y - y + x) - x^2(y + x^3 - 2x) \\
&= -y - x^5 + 2x^3 + x \\
&\xrightarrow{f_4} -x^5 + 3x^3 - x = f_5 \\
S(f_3, f_4) &= -(-y^2 + yx + x^2) - y(y + x^3 - 2x) \\
&= -yx^3 + yx - x^2 \\
&\xrightarrow{f_4} yx + x^6 - 2x^4 - x^2 \\
&\xrightarrow{f_4} x^6 - 3x^4 + x^2 \\
&\xrightarrow{f_5} 0 \\
\mathrm{mcd}(\mathrm{lp}(f_3), \mathrm{lp}(f_5)) &= \mathrm{mcd}(\mathrm{lp}(f_4), \mathrm{lp}(f_5)) = 1 \\
\mathrm{lp}(f_1) &= x^2y \mid x^5y^2 = \mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_5)) \\
\mathrm{lp}(f_4) &= y \mid x^5y = \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_5))
\end{aligned}
$$

es $G_R = \{x^5 - 3x^3 + x, y + x^3 - 2x\}$ y resolviendo este sistema triangular

$$
\begin{cases}
y + x^3 - 2x & = 0 \\
x^5 - 3x^3 + x & = 0
\end{cases}
$$

obtenemos el conjunto solución

$$
\left\{(0,0), (\frac{1+\sqrt{5}}{2}, -1), (\frac{-1+\sqrt{5}}{2}, 1), (\frac{1-\sqrt{5}}{2}, -1), (\frac{-1-\sqrt{5}}{2}, 1)\right\}.
$$

Ejemplo 3.10. Consideremos la intersección del círculo $f_1 = (x-1)^2 + y^2 - 1 = 0$ con la elipse $f_2 = 4(x-1)^2 + y^2 + xy - 2 = 0$, es decir el sistema:

$$
\begin{cases}
x^2 - 2x + y^2 & = 0 \\
4x^2 + xy - 8x + y^2 + 2 & = 0
\end{cases}
$$

con el orden lex, $x > y$, tenemos

$$
\begin{aligned}
S(f_1, f_2) &= (x^2 - 2x + y^2) - \frac{1}{4}(4x^2 + xy - 8x + y^2 + 2) \\
&= -\frac{xy}{4} + \frac{3y^2}{4} - \frac{1}{2} = f_3 \\
\mathrm{lp}(f_1) &= x^2 \mid x^2y = \mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_3))
\end{aligned}
$$

$$
\begin{aligned}
S(f_1, f_3) &= y(x^2 - 2x + y^2) - (-4x)(-\frac{xy}{4} + \frac{3y^2}{4} - \frac{1}{2}) \\
&= -2xy + y^3 + 3xy^2 - 2x \\
&\xrightarrow{f_3} -2xy - 2x + 10y^3 - 6y \\
&\xrightarrow{f_3} -2x + 10y^3 - 6y^2 - 6y + 4 = f_4 \\
\mathrm{lp}(f_1) &= x^2 \mid xy = \mathrm{mcm}(\mathrm{lp}(f_3), \mathrm{lp}(f_4)) \\
\mathrm{lp}(f_2) &= x^2 \mid x^2 = \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_4)) \\
S(f_2, f_4) &= \frac{1}{4}(4x^2 + xy - 8x + y^2 + 2) - (-\frac{x}{2})(-2x + 10y^3 - 6y^2 - 6y + 4) \\
&= 5xy^3 - 3xy^2 - \frac{11xy}{4} + \frac{y^2}{4} + \frac{1}{2} \\
&\xrightarrow{f_3} -3xy^2 - \frac{11xy}{4} + 15y^4 - \frac{39y^2}{4} + \frac{1}{2} \\
&\xrightarrow{f_3} -\frac{11xy}{4} + 15y^4 - 9y^3 - \frac{39y^2}{4} + 6y + \frac{1}{2} \\
&\xrightarrow{f_3} 15y^4 - 9y^3 - 18y^2 + 6y + 6 = f_5.
\end{aligned}
$$

Luego una base de Gröbner para el ideal $I = \langle f_1, f_2 \rangle$, es

$$G = \{g_1, g_2\} = \{x - 5y^3 + 3y^2 + 3y - 2, 5y^4 - 3y^3 - 6y^2 + 2y + 2\}.$$

Y pasamos al sistema:

$$
\begin{cases}
x - 5y^3 + 3y^2 + 3y - 2 & = 0 \\
5y^4 - 3y^3 - 6y^2 + 2y + 2 & = 0
\end{cases}
$$

Desde que $\mathrm{lp}(g_1) = x$ y $\mathrm{lp}(g_2) = y^4$, el teorema 3.3 afirma que el número de puntos en la intersección es finito. Geométricamente se nota que a lo más 4, lo que coincide con que $g_2(y) = 0$ tiene a lo más 4 soluciones:

$$y = \{-0.76019682, -0.56730707, 0.92750389, 1\},$$

cada una de estas nos da sólo una solución para x en $g_1(x, y) = 0$:

$$
\begin{aligned}
(x_1, y_1) &= (0.3503071535, -0.76019682) \\
(x_2, y_2) &= (1.82350633, -0.56730707) \\
(x_3, y_3) &= (0.626186512, 0.92750389) \\
(x_4, y_4) &= (1, 1).
\end{aligned}
$$

Ejemplo 3.11. Resolvamos el sistema en $\mathbb{Z}_5[x, y]$:

$$\begin{cases} x^2 + y^2 + 1 & = 0 \\ x^2y + 2xy + x & = 0 \end{cases}$$

En el ejemplo 2.19, calculamos para el ideal $I = \langle x^2 + y^2 + 1, x^2y + 2xy + x\rangle$, su base de Gröbner reducida $G_R = \{x^2 + y^2 + 1, xy + 3x + 2y^3 + 2y, y^5 + 2y^4 + 4y^2 + 4y + 2\}$ respecto al orden lex con $x > y$. Desde que x^2 e y^5 aparecen como potencias principales de elementos de G, $V_{\overline{\mathbb{Z}_5}}(I)$ es finito. Luego tenemos

$$\begin{cases} x^2 + y^2 + 1 & = 0 \\ xy + 3x + 2y^3 + 2y & = 0 \\ y^5 + 2y^4 + 4y^2 + 4y + 2 & = 0 \end{cases}$$

Resolviendo la última ecuación:

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

si $y = 2 \quad \text{o} \quad y = -2 \implies x = 0$, es decir el conjunto solución en $\mathbb{Z}_5$ sólo consta de $\{(0, 2), (0, -2)\}$ ya que las soluciones de $y^3 + 2y^2 - y + 2 = 0$ no se encuentran en $\mathbb{Z}_5$.

Ejemplo 3.12. Para el sistema de ecuaciones:

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

Sea el ideal $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1\rangle$, entonces

$$\begin{aligned} f_1 &= x^2 + y + z - 1 \\ f_2 &= x + y^2 + z - 1 \\ f_3 &= x + y + z^2 - 1 \\ S(f_1, f_2) &= (x^2 + y + z - 1) - x(x + y^2 + z - 1) \\ &= -xy^2 - xz + x + y + z - 1 \\ &\xrightarrow{f_3} -xz + x + y^3 + y^2z^2 - y^2 + y + z - 1 \end{aligned}$$

$$\xrightarrow{f_2} x + y^3 + z^2y^2 + zy^2 - y^2 + y + z^2 - 1$$
$$\xrightarrow{f_3} y^3 + z^2y^2 + zy^2 - y^2 = f_4$$
$$\text{lp}(f_2) = x \mid x^2 = \text{mcm}(\text{lp}(f_1), \text{lp}(f_3))$$
$$\text{mcd}(\text{lp}(f_1), \text{lp}(f_4)) = \text{mcd}(\text{lp}(f_2), \text{lp}(f_4)) = \text{mcd}(\text{lp}(f_3), \text{lp}(f_4)) = 1$$
$$S(f_2, f_3) = (x + y^2 + z - 1) - (x + y + z^2 - 1)$$
$$= y^2 - y - z^2 + z = f_5$$
$$\text{mcd}(\text{lp}(f_1), \text{lp}(f_5)) = \text{mcd}(\text{lp}(f_2), \text{lp}(f_5)) = \text{mcd}(\text{lp}(f_3), \text{lp}(f_5)) = 1$$
$$S(f_4, f_5) = (y^3 + z^2y^2 + zy^2 - y^2) - y(y^2 - y - z^2 + z)$$
$$= z^2y^2 + zy^2 + z^2y - zy$$
$$\xrightarrow{f_5} zy^2 + 2z^2y - zy + z^4 - z^3$$
$$\xrightarrow{f_5} 2z^2y + z^4 - z^2 = f_6$$
$$\text{mcd}(\text{lp}(f_1), \text{lp}(f_6)) = \text{mcd}(\text{lp}(f_2), \text{lp}(f_6)) = \text{mcd}(\text{lp}(f_3), \text{lp}(f_6)) = 1$$
$$\text{lp}(f_5) = y^2 \mid y^3z^2 = \text{mcm}(\text{lp}(f_4), \text{lp}(f_6))$$
$$S(f_5, f_6) = z^2(y^2 - y - z^2 + z) - \frac{y}{2}(2z^2y + z^4 - z^2)$$
$$= -\frac{yz^4}{2} - \frac{yz^2}{2} - z^4 + z^3$$
$$\xrightarrow{f_6} -\frac{yz^2}{2} + \frac{z^6}{4} - \frac{5z^4}{4} + z^3$$
$$\xrightarrow{f_6} \frac{z^6}{4} - z^4 + z^3 - \frac{z^2}{4} = f_7$$
$$\text{mcd}(\text{lp}(f_1), \text{lp}(f_7)) = \text{mcd}(\text{lp}(f_2), \text{lp}(f_7)) = \text{mcd}(\text{lp}(f_3), \text{lp}(f_7)) = 1$$
$$\text{lp}(f_5) = y^2 \mid y^3z^6 = \text{mcm}(\text{lp}(f_4), \text{lp}(f_7))$$
$$\text{lp}(f_6) = z^2y \mid y^2z^6 = \text{mcm}(\text{lp}(f_5), \text{lp}(f_7))$$
$$S(f_6, f_7) = \frac{z^4}{2}(2z^2y + z^4 - z^2) - 4y(\frac{z^6}{4} - z^4 + z^3 - \frac{z^2}{4})$$
$$= 4z^4y - 4z^3y + z^2y + \frac{z^8}{2} - \frac{z^6}{2}$$
$$\xrightarrow{f_6} -4z^3y + z^2y + \frac{z^8}{2} - \frac{5z^6}{2} + 2z^4$$
$$\xrightarrow{f_6} z^2y + \frac{z^8}{2} - \frac{5z^6}{2} + 2z^5 + 2z^4 - 2z^3$$
$$\xrightarrow{f_6} \frac{z^8}{2} - \frac{5z^6}{2} + 2z^5 + \frac{3z^4}{2} - 2z^3 + \frac{z^2}{2}$$
$$\xrightarrow{f_7} -\frac{z^6}{2} + 2z^4 - 2z^3 + \frac{z^2}{2} \xrightarrow{f_7} 0$$

Luego una base de Gröbner G para I con respecto al orden lex $x > y > z$, es:

$$G = \{x + y + z^2 - 1, y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2\}.$$

Resolviendo este sistema:

$$\begin{cases} x + y + z^2 - 1 & = 0 \\ y^2 - y - z^2 + z & = 0 \\ 2yz^2 + z^4 - z^2 & = 0 \\ z^6 - 4z^4 + 4z^3 - z^2 & = 0 \end{cases}$$

notando que $z^6-4z^4+4z^3-z^2 = z^2(z-1)^2(z^2+2z-1)$ obtenemos el conjunto solución:

$$\{(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})\}.$$

3.3 Aplicaciones a los Polinomios Simétricos

En esta sección se verá la relación entre las bases de Gröbner y las funciones simétricas elementales.

Los polinomios simétricos surgen naturalmente cuando se estudian raíces de polinomios. Por ejemplo consideremos el siguiente polinomio mónico cúbico de grado 3, $f = x^3 + bx^2 + cx + d$ y denotemos sus raíces por $\alpha_1, \alpha_2, \alpha_3$. Entonces

$$x^3 + bx^2 + cx + d = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Expandiendo el lado derecho de esta ecuación obtenemos

$$x^3 + bx^2 + cx + d = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3,$$

y así,

$$\begin{aligned} b &= -(\alpha_1 + \alpha_2 + \alpha_3), \\ c &= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3), \\ d &= -\alpha_1\alpha_2\alpha_3. \end{aligned}$$

Esto muestra que los coeficientes de f son polinomios en sus raíces y además permutando el orden de estas raíces no afecta a f, a dichos polinomios se les denomina simétricos.

Definición 3.4. Un polinomio $f \in k[x_1, \ldots, x_n]$ es simétrico si

$$f(x_{\phi(1)}, \ldots, x_{\phi(n)}) = f(x_1, \ldots, x_n)$$

para cualquier permutación ϕ del conjunto $\{1, \ldots, n\}$.

Por ejemplo los polinomios constantes y $x^2+y^2+z^2$, xyz, $xy+yz+xz$, $x+y+z \in \mathbb{Q}[x, y, z]$ son simétricos. También se nota que los polinomios simétricos forman un sub-anillo de $k[x_1, \ldots, x_n]$. Existe un conjunto especial de polinomios simétricos tales que todo polinomio simétrico puede ser expresado como un polinomio en elementos de dicho conjunto. A los elementos de este conjunto se les denomina los polinomios simétricos elementales.

Definición 3.5. Definamos los polinomios simétricos elementales $\sigma_1, \ldots, \sigma_n \in k[x_1, \ldots, x_n]$ por las fórmulas:

$$\begin{aligned}
\sigma_1 &= x_1 + \cdots + x_n \\
&\vdots \\
\sigma_r &= \sum_{i_1 < i_2 < \cdots < i_r} x_{i_1} x_{i_2} \ldots x_{i_r} \\
&\vdots \\
\sigma_n &= x_1 x_2 \ldots x_n.
\end{aligned}$$

Teorema 3.4 (Teorema Fundamental de los Polinomios Simétricos)**.** [ref.[Sturmfels B.],cáp.1,págs.2-3] Sea $f \in k[x_1, \ldots, x_n]$ un polinomio simétrico. Entonces f puede ser escrito únicamente como un polinomio en los polinomios simétricos elementales $\sigma_1, \ldots, \sigma_n$.

Prueba. Sea $f \in k[x_1, \ldots, x_n]$ un polinomio simétrico entonces el siguiente algoritmo reescribe f únicamente como un polinomio en las funciones simétricas elementales $\sigma_1, \ldots, \sigma_n$.
Usaremos el orden deglex con $x_1 > x_2 > \cdots > x_n$. Luego como f es simétrico podemos escribir $\mathrm{lt}(f) = cx_1^{\gamma_1} \ldots x_n^{\gamma_n}$ con $\gamma_1 \geq \gamma_2 \geq \ldots \gamma_n$.
Reemplazamos f por un nuevo polinomio simétrico

$$\widetilde{f} = f - c\sigma_1^{\gamma_1 - \gamma_2} \sigma_2^{\gamma_2 - \gamma_3} \ldots \sigma_{n-1}^{\gamma_{n-1} - \gamma_n} \sigma_n^{\gamma_n},$$

en caso $\widetilde{f} \neq 0$ se repiten los pasos. Notamos que

$$\begin{aligned}
\mathrm{lp}(\sigma_1^{\gamma_1-\gamma_2}) &= x_1^{\gamma_1-\gamma_2} \\
\mathrm{lp}(\sigma_2^{\gamma_2-\gamma_3}) &= x_1^{\gamma_2-\gamma_3} x_2^{\gamma_2-\gamma_3} \\
&\vdots \\
\mathrm{lp}(\sigma_{n-1}^{\gamma_{n-1}-\gamma_n}) &= x_1^{\gamma_{n-1}-\gamma_n} \dots x_{n-1}^{\gamma_{n-1}-\gamma_n} \\
\mathrm{lp}(\sigma_n^{\gamma_n}) &= x_1^{\gamma_n} \dots x_{n-1}^{\gamma_n} x_n^{\gamma_n}
\end{aligned}$$

lo que implica

$$\mathrm{lt}(f) = \mathrm{lt}(c\sigma_1^{\gamma_1-\gamma_2}\sigma_2^{\gamma_2-\gamma_3} \dots \sigma_{n-1}^{\gamma_{n-1}-\gamma_n}\sigma_n^{\gamma_n}).$$

Así $\mathrm{lp}(\widetilde{f}) < \mathrm{lp}(f)$ y el algoritmo termina.

Para probar la unicidad supongamos $p(y_1, \dots, y_n)$ un polinomio no-nulo tal que $p(\sigma_1, \dots, \sigma_n) = 0$. Sea $y_1^{\alpha_1} \dots y_n^{\alpha_n}$ un monomio en p. Encontramos que

$$\mathrm{lp}(\sigma_1^{\alpha_1} \dots \sigma_n^{\alpha_n}) = x_1^{\alpha_1+\dots+\alpha_n} x_2^{\alpha_2+\dots+\alpha_n} \dots x_n^{\alpha_n},$$

y desde que la aplicación lineal

$$(\alpha_1, \dots, \alpha_n) \mapsto (\alpha_1 + \dots + \alpha_n, \alpha_2 + \dots + \alpha_n, \dots, \alpha_n),$$

es inyectiva, si consideramos el máximo $\alpha_1+\dots+\alpha_n$ sobre los monomios que conforman p, tenemos que $x_1^{\alpha_1+\dots+\alpha_n} x_2^{\alpha_2+\dots+\alpha_n} \dots x_n^{\alpha_n}$ con el orden lex $x_1 > x_2 > \dots > x_n$ nunca se cancela lo que contradice $p(\sigma_1, \dots, \sigma_n) = 0$. □

Ejemplo 3.13.

$$\begin{aligned}
f &= \underline{x_1^3} + x_2^3 = \sigma_1^3 + (f - \sigma_1^3) \\
&= \sigma_1^3 - \underline{3x_1^2 x_2} - 3x_1 x_2^2 \\
&= \sigma_1^3 - 3\sigma_1\sigma_2 + (-3x_1^2 x_2 - 3x_1 x_2^2 - (-3\sigma_1\sigma_2)) \\
&= \sigma_1^3 - 3\sigma_1\sigma_2
\end{aligned}$$

Proposición 3.4. En el anillo $k[x_1, \dots, x_n, y_1, \dots, y_n]$, fijado un orden monomial donde cualquier monomio que involucre a una de las variables $x_1, \dots, x_n$ sea mayor que todos los monomios en $k[y_1, \dots, y_n]$. Sea G una base de Gröbner para $\langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle \subseteq k[x_1, \dots, x_n, y_1, \dots, y_n]$, donde los $\sigma_1, \dots, \sigma_n \in k[x_1, \dots, x_n]$. Dado $f \in k[x_1, \dots, x_n]$, sea $f \xrightarrow{G} r$ con r reducido respecto a G. Entonces:

(i) f es simétrico si y sólo si $r \in k[y_1, \ldots, y_n]$.

(ii) Si f es simétrico, entonces $f = r(\sigma_1, \ldots, \sigma_n)$ es la expresión única de f como un polinomio en los polinomios simétricos elementales $\sigma_1, \ldots, \sigma_n$.

Prueba. (i) ($\Longleftarrow$) Sea $f = u_1 g_1 + \cdots + u_n g_n + r$, evaluando los y_i's por los σ_i's, esto no afecta a $f \in k[x_1, \ldots, x_n]$, obtenemos $f = r(\sigma_1, \ldots, \sigma_n)$, y entonces f es simétrico. (i) ($\Longrightarrow$) Sea $f = r(\sigma_1, \ldots, \sigma_n)$, para algún $r \in k[y_1, \ldots, y_n]$. Probaremos que r es el resto de la división de f por G. Primero notemos que en $k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ los monomios en $\sigma_1, \ldots, \sigma_n$ pueden ser escritos como

$$\begin{aligned} \sigma_1^{\alpha_1} \ldots \sigma_n^{\alpha_n} &= (y_1 + (\sigma_1 - y_1))^{\alpha_1} \ldots (y_n + (\sigma_n - y_n))^{\alpha_n} \\ &= y_1^{\alpha_1} \ldots y_n^{\alpha_n} + B_1(\sigma_1 - y_1) + \cdots + B_n(\sigma_n - y_n), \end{aligned}$$

para algunos $B_1, \ldots, B_n$ en $k[x_1, \ldots, x_n, y_1, \ldots, y_n]$. Se sigue que

$$r(\sigma_1, \ldots, \sigma_n) = r(y_1, \ldots, y_n) + C_1(\sigma_1 - y_1) + \cdots + C_n(\sigma_n - y_n),$$

donde $C_1, \ldots, C_n$ son polinomios en $k[x_1, \ldots, x_n, y_1, \ldots, y_n]$, y desde que $f = r(\sigma_1, \ldots, \sigma_n)$ obtenemos

$$f = C_1(\sigma_1 - y_1) + \cdots + C_n(\sigma_n - y_n) + r(y_1, \ldots, y_n).$$

Ahora supongamos que existe i tal que $\mathrm{lp}(g_i)$ divide a algún monomio en $r \in k[y_1, \ldots, y_n]$, esto implica que, por el orden entre monomios que estamos utilizando, $g_i \in k[y_1, \ldots, y_n]$ y si evaluamos $g_i \in \langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle$ en $\sigma_1, \ldots, \sigma_n$ tenemos que $g_i(\sigma_1, \ldots, \sigma_n) = 0$ y entonces por la parte de la unicidad en la prueba del teorema anterior $g_i = 0$.

□

Ejemplo 3.14. Para $x_1^3 + x_2^3$. Consideramos el ideal $I = \langle f_1, f_2 \rangle = \langle x_1 + x_2 - y_1, x_1 x_2 - y_2 \rangle$ y aplicamos el algoritmo de Buchberger con el orden lex $x_1 > x_2 > y_1 > y_2$:

$$S(x_1 + x_2 - y_1, x_1 x_2 - y_2) = x_2(x_1 + x_2 - y_1) - (x_1 x_2 - y_2) = x_2^2 - x_2 y_1 + y_2 = f_3,$$

reducido respecto a $\{f_1, f_2\}$, luego

$$S(f_1, f_3) = x_2^2(x_1 + x_2 - y_1) - x_1(x_2^2 - x_2 y_1 + y_2)$$

$$
\begin{aligned}
&= x_2^3 - x_2^2 y_1 + x_1 x_2 y_1 - x_1 y_2 \\
&\xrightarrow{f_2} -x_1 y_2 + x_2^3 - x_2^2 y_1 + y_1 y_2 \\
&\xrightarrow{f_1} x_2^3 - x_2^2 y_1 + y_2 x_2 \xrightarrow{f_3} 0. \\
S(f_2, f_3) &= x_2(x_1 x_2 - y_2) - x_1(x_2^2 - x_2 y_1 + y_2) \\
&= x_1 x_2 y_1 - x_1 y_2 - x_2 y_2 \\
&\xrightarrow{f_2} -x_1 y_2 - x_2 y_2 + y_1 y_2 \xrightarrow{f_1} 0.
\end{aligned}
$$

Entonces, y desde que $\mathrm{lp}(f_1) = x_1$ divide a $\mathrm{lp}(f_2) = x_1 x_2$, $G = \{f_1, f_3\} = \{x_1 + x_2 - y_1, x_2^2 - x_2 y_1 + y_2\}$ es una base de Gröbner para I. Luego dividimos $x_1^3 + x_2^3$ por G:

$$
\begin{aligned}
x_1^3 + x_2^3 &\xrightarrow{f_1} -x_1^2 x_2 + x_1^2 y_1 + x_2^3 \\
&\xrightarrow{f_1} x_1^2 y_1 + x_1 x_2^2 - x_1 x_2 y_1 + x_2^3 \\
&\xrightarrow{f_1} x_1 x_2^2 - 2 x_1 x_2 y_1 + x_1 y_1^2 + x_2^3 \\
&\xrightarrow{f_1} -2 x_1 x_2 y_1 + x_1 y_1^2 + x_2^2 y_1 \\
&\xrightarrow{f_1} x_1 y_1^2 + 3 x_2^2 y_1 - 2 x_2 y_1^2 \\
&\xrightarrow{f_1} 3 x_2^2 y_1 - 3 x_2 y_1^2 + y_1^3 \\
&\xrightarrow{f_3} y_1^3 - 3 y_1 y_2.
\end{aligned}
$$

Y aplicando la proposición anterior obtenemos:

$$x_1^3 + x_2^3 = \sigma_1^3 - 3\sigma_1\sigma_2.$$

Ejemplo 3.15. Buscamos expresar $x^4 + y^4$ como combinación de los polinomios $x + y$ e xy. Primero calculamos una base de Gröbner para el ideal $\langle t_1 - x - y, t_2 - xy \rangle$ con respecto al orden lex $x > y > t_1 > t_2$,

$$
\begin{aligned}
f_1 &= -x - y + t_1 \\
f_2 &= -xy + t_2 \\
S(f_1, f_2) &= -y(-x - y + t_1) + (-xy + t_2) \\
&= y^2 - y t_1 + t_2 = f_3 \\
\mathrm{mcd}(\mathrm{lp}(f_1), \mathrm{lp}(f_3)) &= \mathrm{mcd}(x, y^2) = 1 \\
\mathrm{lp}(f_1) &= x \mid xy^2 = \mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_3))
\end{aligned}
$$

esta es $G = \{-x-y+t_1, y^2-yt_1+t_2\}$. Luego haciendo uso del algoritmo de la división dividimos x^4+y^4 por G

$$\begin{aligned}
x^4+y^4 &\xrightarrow{f_1} -yx^3+t_1x^3+y^4\\
&\xrightarrow{f_1} t_1x^3+y^2x^2-t_1yx^2+y^4\\
&\xrightarrow{f_1} y^2x^2-2t_1yx^2+t_1^2x^2+y^4\\
&\xrightarrow{f_1} -2t_1yx^2+t_1^2x^2-y^3x+t_1y^2x+y^4\\
&\xrightarrow{f_1} t_1^2x^2-y^3x+3t_1y^2x-2t_1^2yx+y^4\\
&\xrightarrow{f_1} -y^3x+3t_1y^2x-3t_1^2yx+t_1^3x+y^4\\
&\xrightarrow{f_1} 3t_1y^2x-3t_1^2yx+t_1^3x+2y^4-t_1y^3\\
&\xrightarrow{f_1} -3t_1^2yx+t_1^3x+2y^4-4t_1y^3+3t_1^2y^2\\
&\xrightarrow{f_1} t_1^3x+2y^4-4t_1y^3+6t_1^2y^2-3t_1^3y\\
&\xrightarrow{f_3} 2y^4-4t_1y^3+6t_1^2y^2-4t_1^3y+t_1^4\\
&\xrightarrow{f_3} -2t_1y^3+6t_1^2y^2-4t_1^3y+t_1^4-2y^2t_2\\
&\xrightarrow{f_3} 4t_1^2y^2-4t_1^3y+t_1^4-2y^2t_2+2t_1t_2y\\
&\xrightarrow{f_3} t_1^4-2y^2t_2+2t_1t_2y-4t_1^2t_2\\
&\xrightarrow{f_3} t_1^4-4t_1^2t_2+2t_2^2
\end{aligned}$$

lo que nos da el resto $t_1^4-4t_1^2t_2+2t_2^2$. Así

$$x^4+y^4=(x+y)^4-4(x+y)^2xy+2x^2y^2.$$

Vemos, de los dos ejemplos anteriores, que se presenta una dificultad en encontrar la base de Gröbner para el ideal $\langle\sigma_1-y_1,\ldots,\sigma_n-y_n\rangle$ en la proposición 3.4. La siguiente proposición determina la base de Gröbner para este ideal sin necesidad de hacer los cálculos del algoritmo de Buchberger.

Dadas las variables $z_1,\ldots,z_t$, definimos

$$h_j(z_1,\ldots,z_t)=\sum_{|\alpha|=j}\boldsymbol{z}^{\boldsymbol{\alpha}},$$

la suma de todos los monomios en $z_1,\ldots,z_t$ de grado total $j\geq 0$ (Denotando $h_0=1$).

Proposición 3.5 (ref.[Cifuentes] págs.8-9)**.** Fijado el orden lex (o deglex) con $x_1 > x_2 > \cdots > x_n > y_1 > \cdots > y_n$ en el anillo $k[x_1,\ldots,x_n,y_1,\ldots,y_n]$. Entonces los

polinomios

$$g_j = h_j(x_j, \ldots, x_n) + \sum_{i=1}^{j} (-1)^i h_{j-i}(x_j, \ldots, x_n) y_i,$$

$j = 1, \ldots, n$, forman una base de Gröbner para el ideal $\langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle$.

Prueba. Primero probaremos la identidad:

$$0 = \sum_{i=0}^{k} (-1)^i h_{k-i}(x_1, \ldots, x_n) \sigma_i(x_1, \ldots, x_n). \tag{3.4}$$

Dado un monomio $\boldsymbol{X}^{\boldsymbol{\alpha}}$ en $k[x_1, \ldots, x_n]$ de a distintas variables y grado total k. Para $i \leq a$, existen $\binom{a}{i}$ monomios en σ_i que involucran las variables que aparecen $\boldsymbol{X}^{\boldsymbol{\alpha}}$. Luego este monomio aparecerá $\binom{a}{i}$-veces en el polinomio $h_{k-i}(x_1, \ldots, x_n)\sigma_i(x_1, \ldots, x_n)$. El coeficiente de $\boldsymbol{X}^{\boldsymbol{\alpha}}$ en

$$\sum_{i=0}^{k} (-1)^i h_{k-i}(x_1, \ldots, x_n) \sigma_i(x_1, \ldots, x_n)$$

es $\sum_{i=0}^{a} (-1)^i \binom{a}{i}$. Y por el teorema del binomio, se cumple la siguiente identidad:

$$0 = (-1+1)^a = \sum_{i=0}^{a} \binom{a}{i} (-1)^i (1)^{(a-i)} = \sum_{i=0}^{a} \binom{a}{i} (-1)^i.$$

Con lo que queda probada la ecuación (3.4).

El siguiente paso será probar que (denotando $\sigma_0 = 1$):

$$0 = \sum_{i=0}^{k} (-1)^i h_{k-i}(x_k, \ldots, x_n) \sigma_i(x_1, \ldots, x_n). \tag{3.5}$$

Sea $A = \{1, \ldots, k-1\}$ y $H = \{S \mid S \subseteq A\}$. Denotemos por X_S al monomio que involucra las variables correspondientes a los índices que aparecen en S y por $y = (x_k, \ldots, x_n)$. Mostraremos que para $1 \leq i \leq k-1$ se cumple:

$$\sum_{S \in H} X_S \sigma_{i-|S|}(y) = \sigma_i(x_1, \ldots, x_n). \tag{3.6}$$

En efecto:

$$\begin{aligned} \sum_{S \in H} X_S \sigma_{i-|S|}(y) = {} & \sigma_i(y) + x_1 \sigma_{i-1}(y) + \cdots + x_{k-1} \sigma_{i-1}(y) + \\ & + x_1 x_2 \sigma_{i-2}(y) + \cdots + x_{k-2} x_{k-1} \sigma_{i-2}(y) + \cdots + \sum_{|S|=i} X_S. \end{aligned}$$

Luego podemos encontrar cualquier monomio de $\sigma_i(x_1,\ldots,x_n)$ en el desarrollo de la expresión anterior y viceversa, con lo que queda probada la ecuación (3.6).
Ahora si desarrollamos la parte derecha en la ecuación (3.5):

$$\begin{aligned}\sum_{i=0}^{k}(-1)^i h_{k-i}(y)\sigma_i(x_1,\ldots,x_n) &= \sum_{i=0}^{k} h_{k-i}(y)\sum_{S\in H} X_S\sigma_{i-|S|}(y)\\ &= h_k(y)\sum_{S\in H} X_S\sigma_{0-|S|}(y) - h_{k-1}(y)\sum_{S\in H} X_S\sigma_{1-|S|}(y)+\ldots\\ &\cdots+(-1)^k h_0(y)\sum_{S\in H} X_S\sigma_{k-|S|}(y)\\ &= \sum_{S\in H} X_S[\sum_{i=|S|}^{k}(-1)^i h_{k-i}(y)\sigma_{i-|S|}(y)] = 0.\end{aligned}$$

En efecto, haciendo el cambio de variable $j = i- \mid S \mid$ se tiene

$$\sum_{i=|S|}^{k}(-1)^i h_{k-i}(y)\sigma_{i-|S|}(y) = (-1)^{|S|}\sum_{j=0}^{k-|S|}(-1)^j h_{(k-|S|)-j}(y)\sigma_j(y) = 0,$$

debido a la identidad probada en la ecución (3.4). Con lo que queda probada la ecuación (3.5).
Ahora mostraremos que:

$$\langle g_1,\ldots,g_n\rangle = \langle \sigma_1 - y_1,\ldots,\sigma_n - y_n\rangle.$$

Substrayendo (3.5) de la definición de los g_k obtenemos:

$$g_k = \sum_{i=1}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)(y_i-\sigma_i),$$

por tanto $\langle g_1,\ldots,g_n\rangle \subseteq \langle \sigma_1 - y_1,\ldots,\sigma_n - y_n\rangle$. Para probar la otra inclusión notemos que para $1 \le k \le n$:

$$g_k = (-1)^k(y_k-\sigma_k) + \sum_{i=1}^{k-1}(-1)^i h_{k-i}(x_k,\ldots,x_n)(y_i-\sigma_i),$$

$$g_1 = \sigma_1 - y_1.$$

Por último calculemos $\mathrm{lp}(g_k)$, teniendo en cuenta el orden entre monomios lex (o deglex) con $x_1 > \cdots > x_n > y_1 > \cdots > y_n$:

$$\mathrm{lp}(g_k) = \mathrm{lp}(h_k(x_k,\ldots,x_n) + \sum_{i=1}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)y_i) = x_k^k,$$

luego se tiene $\text{mcd}(\text{lp}(g_i), \text{lp}(g_j)) = 1$ para todos $i \neq j$ en $\{1, \ldots, n\}$, y entonces (por el corolario 2.7) $\{g_1, \ldots, g_n\}$ forma una base de Gröbner para el ideal $\langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle$. □

Ejemplo 3.16. Para el ideal $I = \langle x_1 + x_2 - y_1, x_1x_2 - y_2 \rangle$ aplicamos la proposición anterior:

$$g_1 = h_1(x_1, x_2) - h_0(x_1, x_2)y_1 = x_1 + x_2 - y_1,$$
$$g_2 = h_2(x_2) + \sum_{i=1}^{2} (-1)^i h_{2-i}(x_2)y_i = x_2^2 - x_2y_1 + y_2,$$

entonces $G = \{x_1 + x_2 - y_1, x_2^2 - x_2y_1 + y_2\}$ es una base de Gröbner para I.

Ejemplo 3.17. Si se considera el grupo $S_n \subseteq GL(n, k)$ de matrices de permutación, entonces

$$k[x_1, \ldots, x_n]^{S_n} = \{p \in k[x_1, \ldots, x_n] \mid p \quad \text{es simétrico}\}.$$

Y por los resultados mostrados en está sección,

$$k[x_1, \ldots, x_n]^{S_n} = k[\sigma_1, \ldots, \sigma_n].$$

Es decir, cualquier invariante puede ser escrito como un polinomio en las funciones simétricas elementales siendo está representación única y construida explicítamente.

3.4 Coloreado de un grafo

En esta sección expondremos una última aplicación a la teoría de las bases de Gröbner y el algoritmo de Buchberger, el coloreado de un grafo.

Dado un grafo $\mathcal{G}$ con n vértices y con a lo más un borde, línea o arco entre cualesquiera dos vértices (por ejemplo un mapa con sus regiones siendo representandas por los vértices y las fronteras entre las regiones por los bordes). Se quiere colorear los vértices de tal manera que sólo 3 colores son usados y que ningún par de vértices que estén conectados por un borde sean del mismo color. Si $\mathcal{G}$ puede ser coloreado de está manera, $\mathcal{G}$ es llamado 3-coloreable.

Representaremos los 3 colores por las 3 distintas raíces cúbicas de la unidad $1, \xi, \xi^2$, donde $\xi = e^{\frac{2\pi i}{3}}$. A cada vértice se le asigna un color, esto puede ser representado por las ecuaciones

$$x_i^3 - 1 = 0, 1 \leq i \leq n.$$

Ahora para 2 vértices x_i, x_j conectados por un borde, deben ser de diferente color, es decir $x_i \neq x_j$. De la ecuación $x_i^3 = x_j^3$ obtenemos $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$. Por tanto, x_i e x_j serán de diferente color si, y sólos si

$$x_i^2 + x_i x_j + x_j^2 = 0.$$

Si consideramos el ideal $I = \langle x_i^3 - 1, x_i^2 + x_i x_j + x_j^2 \rangle$ en $\mathbb{C}[x_1, \ldots, x_n]$, notamos que se cumple lo siguiente:
El grafo $\mathcal{G}$ es 3-coloreable si, y sólo si $V(I) \neq \emptyset$. Para determinar si $V(I) = \emptyset$, haremos uso de la proposición 3.3. Es decir, calculamos una base de Gröbner reducida G para I. Si $1 \in G$, entonces $V(I) = \emptyset$ de otra manera $V(I) \neq \emptyset$.

Ejemplo 3.18 (ref.[Adams W.],cáp.2,págs.103-104)**.** Consideremos el siguiente grafo:

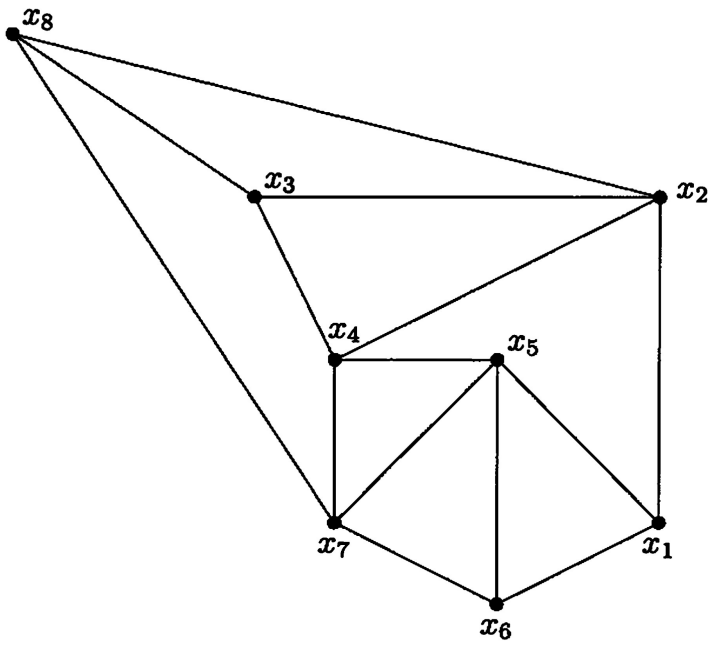

Figura 3.1: **El grafo $\mathcal{G}$**

Sea I el ideal formado por los polinomios $x_i^3 - 1$, con $1 \leq i \leq 8$ y los polinomios:

$$x_i^2 + x_i x_j + x_j^2$$

para los pares

$$(i,j) \in \{(1,2),(1,5),(1,6),(2,3),(2,4),(2,8),(3,4),(3,8),(4,5),(4,7),(5,6),(5,7),(6,7),(7,8)\}.$$

Considerando el teorema 3.3 y el corolario 3.1 utilizamos el orden lex $x_1 > x_2 > \cdots > x_8$, para calcular una base de Gröbner G para I. Denotamos:

$$f_1 = x_1^3 - 1, f_2 = x_2^3 - 1, f_3 = x_3^3 - 1, f_4 = x_4^3 - 1$$
$$f_5 = x_5^3 - 1, f_6 = x_6^3 - 1, f_7 = x_7^3 - 1, f_8 = x_8^3 - 1$$
$$f_9 = x_1^2 + x_1x_2 + x_2^2, f_{10} = x_1^2 + x_1x_5 + x_5^2$$
$$f_{11} = x_1^2 + x_1x_6 + x_6^2, f_{12} = x_2^2 + x_2x_3 + x_3^2$$
$$f_{13} = x_2^2 + x_2x_4 + x_4^2, f_{14} = x_2^2 + x_2x_8 + x_8^2$$
$$f_{15} = x_3^2 + x_3x_4 + x_4^2, f_{16} = x_3^2 + x_3x_8 + x_8^2$$
$$f_{17} = x_4^2 + x_4x_5 + x_5^2, f_{18} = x_4^2 + x_4x_7 + x_7^2$$
$$f_{19} = x_5^2 + x_5x_7 + x_7^2, f_{20} = x_5^2 + x_5x_6 + x_6^2$$
$$f_{21} = x_6^2 + x_6x_7 + x_7^2, f_{22} = x_7^2 + x_7x_8 + x_8^2$$

Eliminando pares debido al **crit1** nos quedan los siguientes:

$$\{(1,9),(1,10),(1,11),(2,12),(2,13),(2,14),(3,15),(3,16),(4,17),(4,18)$$
$$,(5,19),(5,20),(6,21),(7,22),(9,10),(9,11),(10,11),(12,13),(12,14),(13,14)$$
$$,(15,16),(17,18),(19,20)\}$$

Aplicamos el **crit2**:

$$\mathrm{lp}(f_{10}) = x_1^2 \mid x_1^3 = \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_9))$$
$$\mathrm{lp}(f_{11}) = x_1^2 \mid x_1^3 = \mathrm{mcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_{10}))$$
$$\mathrm{lp}(f_{13}) = x_2^2 \mid x_2^3 = \mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_{12}))$$
$$\mathrm{lp}(f_{14}) = x_2^2 \mid x_2^3 = \mathrm{mcm}(\mathrm{lp}(f_2), \mathrm{lp}(f_{13}))$$
$$\mathrm{lp}(f_{16}) = x_3^2 \mid x_3^3 = \mathrm{mcm}(\mathrm{lp}(f_3), \mathrm{lp}(f_{15}))$$
$$\mathrm{lp}(f_{18}) = x_4^2 \mid x_4^3 = \mathrm{mcm}(\mathrm{lp}(f_4), \mathrm{lp}(f_{17}))$$
$$\mathrm{lp}(f_{20}) = x_5^2 \mid x_5^3 = \mathrm{mcm}(\mathrm{lp}(f_5), \mathrm{lp}(f_{19}))$$
$$\mathrm{lp}(f_{11}) = x_1^2 \mid x_1^2 = \mathrm{mcm}(\mathrm{lp}(f_9), \mathrm{lp}(f_{10}))$$
$$\mathrm{lp}(f_{14}) = x_2^2 \mid x_2^2 = \mathrm{mcm}(\mathrm{lp}(f_{12}), \mathrm{lp}(f_{13}))$$

Ahora restan calcular los pares:

$$\{(1,11),(2,14),(3,16),(4,18),(5,20),(6,21),(7,22),(9,11),(10,11),(12,14)$$

$, (13,14), (15,16), (17,18), (19,20)\}$

$$
\begin{aligned}
S(f_1, f_{11}) &= (x_1^3 - 1) - x_1(x_1^2 + x_1x_6 + x_6^2) \\
&= -x_1^2x_6 - x_1x_6^2 - 1 \\
&\xrightarrow{f_{11}} x_6^3 - 1 \xrightarrow{f_6} 0 \\
S(f_2, f_{14}) &= (x_2^3 - 1) - x_2(x_2^2 + x_2x_8 + x_8^2) \\
&= -x_2^2x_8 - x_2x_8^2 - 1 \\
&\xrightarrow{f_{11}} x_8^3 - 1 \xrightarrow{f_8} 0 \\
S(f_3, f_{16}) &= (x_3^3 - 1) - x_3(x_3^2 + x_3x_8 + x_8^2) \\
&= -x_3^2x_8 - x_3x_8^2 - 1 \\
&\xrightarrow{f_{16}} x_8^3 - 1 \xrightarrow{f_8} 0 \\
S(f_4, f_{18}) &= (x_4^3 - 1) - x_4(x_4^2 + x_1x_7 + x_7^2) \\
&= -x_4^2x_7 - x_4x_7^2 - 1 \\
&\xrightarrow{f_{18}} x_7^3 - 1 \xrightarrow{f_7} 0 \\
S(f_5, f_{20}) &= (x_5^3 - 1) - x_5(x_5^2 + x_5x_6 + x_6^2) \\
&= -x_5^2x_6 - x_5x_6^2 - 1 \\
&\xrightarrow{f_{20}} x_6^3 - 1 \xrightarrow{f_6} 0 \\
S(f_6, f_{21}) &= (x_6^3 - 1) - x_6(x_6^2 + x_6x_7 + x_7^2) \\
&= -x_6^2x_7 - x_6x_7^2 - 1 \\
&\xrightarrow{f_{21}} x_7^3 - 1 \xrightarrow{f_7} 0 \\
S(f_7, f_{22}) &= (x_7^3 - 1) - x_7(x_7^2 + x_7x_8 + x_8^2) \\
&= -x_7^2x_8 - x_7x_8^2 - 1 \\
&\xrightarrow{f_{22}} x_8^3 - 1 \xrightarrow{f_8} 0 \\
S(f_9, f_{11}) &= (x_1^2 + x_1x_2 + x_2^2) - (x_1^2 + x_1x_6 + x_6^2) \\
&= x_1x_2 - x_1x_6 + x_2^2 - x_6^2 \\
&\xrightarrow{f_{14}} x_1x_2 - x_1x_6 - x_2x_8 - x_6^2 - x_8^2 \\
&\xrightarrow{f_{21}} x_1x_2 - x_1x_6 - x_2x_8 + x_6x_7 + x_7^2 - x_8^2 \\
&\xrightarrow{f_{22}} x_1x_2 - x_1x_6 - x_2x_8 + x_6x_7 - x_7x_8 - 2x_8^2 = f_{23}
\end{aligned}
$$

Continuando de esta manera (el resto de los cálculos son bastante extensos y se recomienda utilizar algún software matemático como CoCoA, Xcas o Maple para verificar el resultado final) se obtiene la base de Gröbner Reducida

$$G = \{x_1 - x_7, x_2 + x_7 + x_8, x_3 - x_7, x_4 - x_8, x_5 + x_7 + x_8, x_6 - x_8, x_7^2 + x_7x_8 + x_8^2, x_8^3 - 1\}.$$

Desde que $1 \notin G$ sabemos que $V(I) \neq \emptyset$ y que $V(I)$ es finito. Luego el grafo $\mathcal{G}$ es 3-coroleable. Asumamos que los colores a utilizar sean azul, rojo y verde y solucionemos el sistema de ecuaciones formado por los polinomios en G. De la ecuación $x_8^3 - 1 = 0$ elijamos un color para x_8 digamos rojo. Debemos elegir un color diferente para x_7, digamos azul, debido a que x_7 y x_8 están conectados por un borde. Luego $x_1 = x_7$, $x_3 = x_7$ implican que x_1 y x_3 deben ser azul, y $x_4 = x_8$, $x_6 = x_8$ implican que x_4 y x_8 deben ser rojo. Finalmente de las ecuaciones $x_2 + x_7 + x_8 = x_5 + x_7 + x_8 = 0$, obtenemos x_2 y x_5 deben ser del mismo color pero diferentes a x_7 y x_8 por el borde que los une, entonces x_2 y x_5 son verdes, con lo que completamos una solución. De manera similar se obtiene el resto de las soluciones al coloreado del grafo $\mathcal{G}$.

Conclusiones

Primero resaltar la importancia de que $k[x_1, \ldots, x_n]$ sea notheriano para probar la finitud de los algoritmos presentados. El algoritmo 2.4 junto con los ejemplos 2.17, 2.18 y 2.19 explican paso por paso que ocurre durante el algoritmo de Buchberger para encontrar bases de Gröbner. Así como la teoría de Syzygies, el lema 2.5, el corolario 2.8 y los ejemplos 2.23, 2.24 lo hacen en el proceso para hacerlo más eficiente obteniendo el algoritmo mejorado 2.5.

El estudio de los sistemas de ecuaciones polinomiales nos conduce al concepto de variedades. El teorema 3.1, y su demostración, junto con la proposición 3.3 relacionan la teoría de las bases de Gröbner con las variedades. En los ejemplos 3.8, 3.9, 3.10, 3.11 y 3.12 se muestra la utilidad de estos resultados en la solución de sistemas de ecuaciones polinomiales multi-variables no-lineales reduciendo este sistema al problema de calcular raíces de polinomios en una sola indeterminada.

La proposición 3.4 y su prueba relaciona las bases de Gröbner con la representación de polinomios simétricos. Y en el ejemplo 3.17 se utiliza esta relación para determinar los invariantes de $k[x_1, \ldots, x_n]^{S_n}$.

El desarrollo de la teoría de las bases de Gröbner nos muestra que es posible ahondar mucho más en el tema (por ejemplo bases de Gröbner en anillos no conmutativos o para módulos, etc), así como mostrar otras aplicaciones (ej. encriptación). Por tanto el objetivo de la tesis se considera cumplido pero el tesista espera continuar en este tema para futuras investigaciones.

Recomendaciones

Para iniciarse en el tema de las Bases de Gröbner y la solución de sistemas de ecuaciones polinomiales se recomienda consultar [Adams W.], [Cox D.] y [Cox, Little, O'shea] en la bibliografía.

Y para profundizar más en la parte teórica, implementación y eficiencia de los algoritmos, así como diferentes aplicaciones no mencionadas en la presente tesis, se recomiendan los siguientes textos:

1. *Gröbner Bases, Statistics and Software Systems*, por Takayuki Hibi, Springer 2010.

2. *Gröbner Bases, Coding and Cryptography*, por Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, Carlo Traverso, Springer 2009.

3. *Solving Polynomial Equations Systems I-II*, por Teo Mora, Cambridge 2005.

Apéndice A

Bases de Gröbner Universales

Como se mostro en el ejemplo 2.14, puede ocurrir que una base de Gröbner con respecto a un orden de términos no siga siendo una base de Gröbner con respecto a otro orden términos.

Definición A.1. A un conjunto F que cumple en ser una base de Gröbner para un ideal I con respecto a cualquier orden de términos se le denomina base de Gröbner universal para ese ideal.

Nuestro objetivo en este apéndice sera demostrar que todo ideal en $k[x_1, \ldots, x_n]$ posee una base de Gröbner universal.

A.1 Espacios Topológicos de ordenes totales de conjuntos

Sea S un conjunto.

Definición A.2. Un orden total en S es una relación binaria $\preceq$ en S tal que para todo $a, b, c \in S$ se cumple antisimetría: $a \preceq b \wedge b \preceq a \implies a = b$, transitividad: $a \preceq b \wedge b \preceq c \implies a \preceq c$, totalidad: $a \preceq b \vee b \preceq a$. Totalidad implica reflexividad: $a \preceq a$ para todo $a \in S$. El conjunto no-vacío de todos los ordenes totales en S es denotado por $TO(S)$.

Dado un par ordenado $(a, b) \in S \times S$, sea $\mathfrak{U}_{(a,b)}$ el conjunto de todos los ordenes totales $\preceq$ en S para los cuales $a \preceq b$. Denotemos $\mathcal{U}$ la topología para la cual $\{\mathfrak{U}_{(a,b)} \mid$

$(a,b) \in S \times S\}$ es una sub-base es decir los conjuntos abiertos en $\mathcal{U}$ son las uniones de intersecciones finitas de conjuntos de la forma $\mathfrak{U}_{(a,b)}$. Observamos que $\mathfrak{U}_{(a,a)} = TO(S)$ y que $\mathfrak{U}_{(a,b)} = TO(S) \backslash \mathfrak{U}_{(b,a)}$ si $a \neq b$, así los conjuntos abiertos $\mathfrak{U}_{(a,b)}$ también son cerrados.

Sea $\mathbf{S}$ una filtración exhaustiva de S, es decir una familia $\mathbf{S} := (S_i)_{i\in\mathbb{N}}$ de sub-conjuntos S_i de S con $S_0 = \emptyset$, $S_i \subseteq S_{i+1}$ para todo $i \in \mathbb{N}$ y $S = \bigcup_{i\in\mathbb{N}} S_i$. Definamos la función $d_{\mathbf{S}} : TO(S) \times TO(S) \to \mathbb{R}$ por $d_{\mathbf{S}}(\preceq', \preceq'') := 2^{-r}$ con $r := sup\{i \in \mathbb{N} \mid \preceq' \restriction_{S_i} = \preceq'' \restriction_{S_i}\}$, donde $\restriction$ significa restricción. Se cumple $0 \subseteq Im(d_{\mathbf{S}}) \subseteq [0,1]$. Como S es exhaustivo, tenemos $d_{\mathbf{S}}(\preceq', \preceq") = 0$ si y sólo si $\preceq' = \preceq"$. Obviamente, $d_{\mathbf{S}}(\preceq', \preceq'') = d_{\mathbf{S}}(\preceq'', \preceq')$. Finalmente $d_{\mathbf{S}}(\preceq', \preceq''') \leq d_{\mathbf{S}}(\preceq', \preceq'') + d_{\mathbf{S}}(\preceq'', \preceq''')$, por que $d_{\mathbf{S}}(\preceq', \preceq''') \leq max\{d_{\mathbf{S}}(\preceq', \preceq''), d_{\mathbf{S}}(\preceq'', \preceq''')\}$. Así $d_{\mathbf{S}}$ es una métrica en $TO(S)$, dependiente de la elección de la filtración $\mathbf{S}$ de S.

Teorema A.1 (ref.[Boldini R.],pág.1)**.** Sea $\mathbf{S} = (S_i)_{i\in\mathbb{N}}$ cualquier filtración exhaustiva de S tal que cada uno de los S_i es finito. Sea $\mathcal{N}$ la topología de TO(S) inducida por la métrica $d_{\mathbf{S}}$, es decir $\Omega \in \mathcal{N}$ si y sólo si Ω es una unión de intersecciones finitas de conjuntos de la forma $\Omega_r(\preceq) := \{\preceq' \in TO(S) \mid d_{\mathbf{S}}(\preceq, \preceq') < 2^{-r}\}$ con $r \in \mathbb{N}$ y $\preceq \in TO(S)$. Entonces $\mathcal{N} = \mathcal{U}$, en particular la topología $\mathcal{N}$ es independiente de la elección de la filtración exhaustiva $\mathbf{S}$ de S.

Prueba. Sea $r \in \mathbb{N}$ y $\preceq \in TO(S)$. Afirmamos que $\Omega_r(\preceq) \in \mathcal{U}$. Sea $\mathfrak{U} := \cap_{(a,b)}\mathfrak{U}_{(a,b)}$, donde la intersección es sobre todos los $(a,b) \in S_{r+1} \times S_{r+1}$ con $a \preceq b$. Entonces $\preceq \in \mathfrak{U} \in \mathcal{U}$. Luego $\preceq' \in \Omega_r(\preceq)$ si y sólo si $\preceq' \restriction_{S_{r+1}} = \preceq \restriction_{S_{r+1}}$, y este es el caso si y sólo si se cumple $a \preceq' b \iff a \preceq b$ para todo $(a,b) \in S_{r+1} \times S_{r+1}$, lo cual es cierto si y sólo si $\preceq' \in \mathfrak{U}$. Así $\Omega_r(\preceq) = \mathfrak{U}$, y esto muestra que $\mathcal{N} \subseteq \mathcal{U}$.

Por otro lado, sea $(a,b) \in S \times S$ cualquier par ordenado. Afirmamos que el conjunto $\mathfrak{U}_{(a,b)}$ es abierto respecto a la métrica $d_{\mathbf{S}}$. Sea $\preceq \in \mathfrak{U}_{(a,b)}$, así $a \preceq b$. Escojamos $r \in \mathbb{N}$, tal que $(a,b) \in S_{r+1} \times S_{r+1}$. Si $\preceq' \in \Omega_r(\preceq)$, entonces $\preceq' \restriction_{S_{r+1}} = \preceq \restriction_{S_{r+1}}$, en particular $a \preceq' b$, entonces $\preceq' \in \mathfrak{U}_{(a,b)}$, así $\Omega_r(\preceq) \subseteq \mathfrak{U}_{(a,b)}$. Por tanto $\mathfrak{U}_{(a,b)}$ es abierto respecto a $\mathcal{N}$, y concluimos que $\mathcal{U} \subseteq \mathcal{N}$. □

De ahora en adelante *Espacio topológico TO(S)*, hará referencia a la topología $\mathcal{U}$.

Teorema A.2. [ref.[Boldini R.],pág.2] Si el conjunto S es contable, entonces el espacio topológico TO(S) es compacto.

Prueba. Desde que S es contable, encontramos una filtración exhaustiva $\mathbf{S} = (S_i)_{i\in\mathbb{N}}$ de S que consiste de subconjuntos finitos. Desde que TO(S) es un espacio métrico con respecto a la métrica $d_{\mathbf{S}}$, es suficiente con probar que cada secuencia de elementos de TO(S) admite una subsecuencia convergente en TO(S). Sea $(\preceq_j)_{j\in\mathbb{N}}$ cualquier secuencia de ordenes totales en S. Sin pérdida de generalidad podemos asumir que los $\preceq_j$ son distintos entre sí.

Como existen sólo un número finito de órdenes totales en S_0, encontramos una subsecuencia infinita $(\preceq_{j_k^0})_{k\in\mathbb{N}}$ de $(\preceq_j)_{j\in\mathbb{N}}$ cuyos miembros coinciden en S_0. Como existen sólo un número finito de órdenes totales distintos en S_1, encontramos una secuencia infinita $(\preceq_{j_k^1})_{k\in\mathbb{N}}$ de $(\preceq_{j_k^0})_{k\in\mathbb{N}}$ cuyos miembros todos coinciden en S_1. Continuando de está manera, construimos una familia $((\preceq_{j_k^i})_{k\in\mathbb{N}})_{i\in\mathbb{N}}$ de secuencias infinitas de órdenes totales en S tal que para cada i los miembros de $(\preceq_{j_k^i})_{k\in\mathbb{N}}$ coinciden todos en S_i y $(\preceq_{j_k^{i+1}})_{k\in\mathbb{N}}$ es una subsecuencia de $(\preceq_{j_k^i})_{k\in\mathbb{N}}$. Escribiendo $\preceq^i := \preceq_{j_i^i}$, hemos obtenido una subsecuencia $(\preceq^i)_{i\in\mathbb{N}}$ de $(\preceq_j)_{j\in\mathbb{N}}$.

Ahora sea $\preceq^\infty$ una relación binaria en S definida por $a \preceq^\infty b \iff a \preceq^i b$ para casi todos los i. Se verifica fácilmente la anti-simetría y la transitividad. Sea $a, b \in S$. Encontramos $r \in \mathbb{N}$ con $a, b \in S_r$. Se cumple $a \preceq^r b$ o $b \preceq^r a$, digamos $a \preceq^r b$. Como $\preceq^{r+1}$ es un miembro de la subsecuencia $(\preceq_{j_k^{r+1}})_{k\in\mathbb{N}}$ de la secuencia $(\preceq_{j_k^r})_{k\in\mathbb{N}}$ que contiene a $\preceq^r$ y cuyos miembros todos coinciden en S_r, se sigue $a \preceq^{r+1} b$, e inductivamente $a \preceq^i b$ para todo $i \geq r$, así $a \preceq^\infty b$. Luego $\preceq^\infty$ es un orden total en S.

Para todo $r \in \mathbb{N}$ y todo $i \geq r+1$ se cumple $\preceq^i \in \Omega_r(\preceq^\infty)$. En efecto, sea $r \in \mathbb{N}$ y sea $i \geq r+1$. Es suficiente con mostrar que $\preceq^i$ y $\preceq^\infty$ coinciden en S_{r+1}. Sea $a, b \in S_{r+1}$. Como hemos visto antes tenemos $a \preceq^i b \implies a \preceq^{i+1} b \implies a \preceq^{i+2} b \implies \ldots$, y por ende $a \preceq^i b \implies a \preceq^\infty b$. Por otro lado asumamos que $a \preceq^\infty b$. Si no se cumple $a \preceq^i b$, entonces $b \preceq^i a$ por totalidad, se sigue que $b \preceq^\infty a$, y $a = b$ por anti-simetría, y entonces $a \preceq^i a = b$ por reflixividad, lo cual es una contradicción. Así $\preceq^i$ y $\preceq^\infty$ coinciden en S_{r+1}. Por tanto $\preceq^i \to \preceq^\infty$ para $i \to \infty$. □

Teorema A.3 (ref.[Boldini R.],pág.2)**.** Para cada $a \in S$ el conjunto $SO_a(S) := \{\preceq \in TO(S) \mid \forall b \in S : a \preceq b\}$ es cerrado en TO(S). Luego, si S es contable, entonces el subespacio topológico $SO_a(S)$ de TO(S) es compacto.

Prueba. Se cumple $SO_a(S) = \cap_{b\in S}\mathfrak{U}_{(a,b)} = \cap_{b\in S\setminus\{a\}}\mathfrak{U}_{(a,b)} = TO(S)\setminus \cup_{b\in S\setminus\{a\}} \mathfrak{U}_{(b,a)}$, así

$SO_a(S)$ es cerrado en TO(S). Si S es contable, entonces TO(S) es compacto por el teorema A.2, así siendo $SO_a(S)$ cerrado en TO(S) implica que $SO_a(S)$ con la topología relativa es compacto. □

A.2 Bases de Gröbner universales en $k[x_1, \ldots, x_n]$

Sea $M := \{X^v \mid v \in \mathbb{N}^n\}$ el conjunto contable de monomios de $k[x_1, \ldots, x_n]$. Para cada $p \in k[x_1, \ldots, x_n]$ puede ser expresado únicamente en forma canónica como $\sum_{v \in supp(p)} c_v X^v$ con $supp(p) \subseteq \mathbb{N}^n$ y $c_v \in K \backslash \{0\}$ para todo $v \in supp(p)$. Definimos $Supp(p) := \{X^v \in M \mid v \in supp(p)\}$ el soporte de p, y para un sub-conjunto U de $k[x_1, \ldots, x_n]$ escribimos $Supp(U) := \cup_{u \in U} Supp(u)$.

Teorema A.4 (ref.[Boldini R.],pág.3)**.** $MO(M)$ es un sub-conjunto cerrado de $SO_1(M)$. Luego $MO(M)$ es un sub-espacio topológico compacto de $SO_1(M)$.

Prueba. $MO(M)$ es por supuesto un sub-conjunto de $SO_1(M)$. Sea $(S_i)_{i \in \mathbb{N}}$ una filtración exhaustiva de M con conjuntos finitos S_i. Sea $\leq \in SO_1(M)$ un punto de acumulación de MO(M). Entonces para cada $r \in \mathbb{N}$ existen $\leq_r \in MO(M) \backslash \{\leq\}$ con $\leq_r \in \Omega_r(\leq) \cap SO_1(M)$, así $\leq_r$ y $\leq$ coinciden en S_{r+1}. Elegimos cualesquiera $u, v, \gamma \in \mathbb{N}^n$ y asumamos que $X^u \leq X^v$. Encontramos $r \in \mathbb{N}$ tal que $X^u, X^v, X^{u+\gamma}, X^{v+\gamma} \in S_{r+1}$. Existe $\leq_r$ tal que $X^u \leq_r X^v$. Desde que $\leq_r$ es un orden de monomios se sigue que $X^{u+\gamma} \leq_r X^{v+\gamma}$, y por tanto $X^{u+\gamma} \leq X^{v+\gamma}$. Así $\leq \in MO(M)$. Entonces, MO(M) es cerrado en $SO_1(M)$, que es compacto. □

Proposición A.1. Sea I un ideal de $k[x_1, \ldots, x_n]$, $\leq$ un orden de monomios de $k[x_1, \ldots, x_n]$ y B una base de Gröbner de I con respecto a $\leq$. Sea $\leq'$ un orden de monomios de $k[x_1, \ldots, x_n]$ tal que $\leq' \restriction_{Supp(B)} = \leq \restriction_{Supp(B)}$. Entonces B es una base de Gröbner para I con respecto a $\leq'$.

Prueba. Sea $p \in I$ no-nulo, dividiendo p por B con respecto a $\leq'$ tenemos $p = \sum_{b \in B} q_b b + r$ para algunos elementos $q_b \in k[x_1, \ldots, x_n]$ y r en I reducido. Supongamos $r \neq 0$. Entonces existe un $b \in B$ tal que $lp_{\leq}(b) \mid lp_{\leq}(r)$. Desde que $\leq$ y $\leq'$ coinciden en $Supp(B)$, tenemos $lp_{\leq'}(b) = lp_{\leq}(b)$, por tanto $lp_{\leq'}(b) \mid lp_{\leq}(r)$ lo cual es una contradicción. Por tanto $r = 0$ y, por el teorema 2.11 parte (ii), B es una base de Gröbner de I con respecto a $\leq'$. □

Lema A.1. Sea I un ideal $k[x_1, \ldots, x_n]$ y F un sub-conjunto finito de I. Entonces el conjunto $\mathfrak{U}_I(F)$ de todos los ordenes de monomios $\leq$ para los cuales F es una base de Gröbner de I respecto a $\leq$ es abierto en $MO(M)$.

Prueba. Sin pérdida de generalidad podemos asumir que $\mathfrak{U}_I(F) \neq \emptyset$. Sea $\leq \in \mathfrak{U}_I(F)$. Entonces F es una base de Gröbner para I con respecto a $\leq$. Sea $(S_i)_{i\in\mathbb{N}}$ una filtración exhaustiva de M consistiendo de conjuntos finitos S_i. Encontramos $r \in \mathbb{N}$ tal que cada monomio perteneciente a los elementos de F se encuentra en S_{r+1}. Consideremos la vecindad abierta $\Omega_r(\leq) \cap MO(M)$ de $\leq$ en $MO(M)$ y sea $\leq' \in \Omega_r(\leq) \cap MO(M)$. Entonces $\leq'$ y $\leq$ coinciden en S_{r+1}, se sigue que F es una base de Gröbner de I con respecto a $\leq'$, así $\leq' \in \mathfrak{U}_I(F)$. Por tanto $\Omega_r(\leq) \cap MO(M) \subseteq \mathfrak{U}_I(F)$, y luego $\mathfrak{U}_I(F)$ es abierto en $MO(M)$. □

Nota A.1. Sea I un ideal de $k[x_1, \ldots, x_n]$. Para cada $\leq \in MO(M)$ podemos elegir una base de Gröbner B de I con respecto a $\leq$. Por supuesto $\leq \in \mathfrak{U}_I(B_\leq)$. Por tanto $(\mathfrak{U}_I(B_\leq))_{\leq\in MO(M)}$ es un cubrimineto abierto de $MO(M)$.

Teorema A.5 (ref.[Boldini R.],pág.4)**.** Todo ideal I de $k[x_1, \ldots, x_n]$ admite una base de Gröbner universal.

Prueba. Podemos escoger un cubrimiento abierto $(\mathfrak{U}_I(B_\leq))_{\leq\in MO(M)}$ de $MO(M)$ donde cada $B_\leq$ es una base de Gröbner para I con respecto a $\leq$. Ahora desde que $MO(M)$ es compacto tenemos un sub-cubrimiento finito $(\mathfrak{U}_I(B_{\leq_k}))_{1\leq k\leq t}$ con $t \in \mathbb{N}$. Afirmamos que $U := \cup_{1\leq k\leq t} B_{\leq_k}$ es una base de Gröbner universal de I. En efecto, sea $\leq_0 \in MO(M)$. Como $MO(M) = \cup_{1\leq k\leq t}\mathfrak{U}_I(B_{\leq_k})$, tenemos $\leq_0 \in \mathfrak{U}_I(B_{\leq_k})$ para algún $k \in \{1, \ldots, t\}$. Luego $B_{\leq_k}$ es una base de Gröbner de I con respecto a $\leq_0$ y se sigue que U es una base de Gröbner de I con respecto a $\leq_0$. Como la elección de $\leq_0$ en $MO(M)$ fue arbitraria, concluimos que U es una base de Gröbner universal de I. □

Bibliografía

[Adams W.] Adams W., Loustaunau P., *An Introduction to Gröbner Bases*. American Mathematical Society, 1994.

[Atiyah M.F] Atiyah M.F., Macdonald I.G., *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[Boldini R.] Boldini R., *Universal Gröbner bases in polynomial rings*. Notes, 2009.

[Cox D.] Cox D. A., Little J.,OShea D., *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2015.

[Cifuentes] Cifuentes V., Patiño B., Pérez H., *Las Bases de Gröbner en el estudio de los polinomios simétricos*. Revista Tumbaga, 2010.

[Cox, Little, O'shea] Cox D. A., Little J.,OShea D., *Using Algebraic Geometry*. Graduate Texts in Mathematics, 2005.

[Fulton W.] Fulton W., *Algebraic Curves, An Introduction to Algebraic Geometry*. Addison-Wesley, 1974.

[Hungerford T.] Hungerford T., *Algebra*. Springer, 1974.

[Scholarpedia] Scholarpedia (visto en agosto 2016) `http://www.scholarpedia.org/article/groebner_basis`.

[Sturmfels B.] Sturmfels B., *Algorhitms in invariant theory*. SpringerWienNewYork, 2008.

[University of Kent] University of Kent (visto en junio 2016) `https://www.kent.ac.uk/smsas/personal/gdb/MA574`.

[Wikilibros] Wikilibros (visto en setiembre 2016) https://es.wikibooks.org/wiki/Manual_de_LaTeX.