Universidad de Granada
Facultad de Ciencias
Máster de Matemáticas

Aplicaciones de las bases de Gröbner a interpolación y teoría de grafos

Flavia María Romero Camacho

(TRABAJO FIN DE MÁSTER)

Dirigido por: Pascual Jara

Granada–2012

INTRODUCCIÓN

Las bases de Gröbner fueron introducidas por Bruno Buchberger en su tesis doctoral en 1965, realizada bajo la dirección de Wolfgang Gröbner. Los principios básicos subyacentes a la noción de bases de Gröbner se remontan al fin del siglo XIX, pero la contribución principal de Buchberger ha sido la de idear un algoritmo finito que transforma un sistema de generadores dados de un ideal en una base de Gröbner del ideal. Este algoritmo está actualmente implementado en muchos sistemas de álgebra computacional (MAPLE, MATHEMATICA, REDUCE, AXIOM, MACAULAY, COCOA, GROBNER, etc.).

El algoritmo de Buchberger para el cálculo de Bases Gröbner se ha convertido en una poderosa herramienta para la solución aquellos problemas que se pueden expresar en términos de la teoría de ideales de polinomios con coeficientes en un cuerpo; en esta teoría los ideales son finitamente generados como consecuencia del Teorema de la Base de Hilbert.

Si I es un ideal de un anillo de polinomios $K[X_1, ..., X_n]$ con coeficientes en un cuerpo, una base de Gröbner de I es un conjunto finito de elementos no nulos, $\mathbb{G} = \{G_1, \ldots, G_t\} \subseteq I$, verificando que

$$Exp(I) = exp(G_1), ..., exp(G_t) + \mathbb{N}^n = Exp(G) + \mathbb{N}^n$$

respecto de un orden monomial admisible. De forma esquemática la importancia de las bases de Gröbner radica en que se asocia a cada ideal un sistema de generadores, la base de Gröbner, de forma única; pudiendo entonces operar con este ideal considerando únicamente la base de Gröbner. El uso de elementos accesorios, como el orden monomial elegido permiten, en ciertos casos, la simplificación de los elementos a considerar.

Las bases de Gröbner pueden ser utilizadas para resolver el problema de la pertenencia de un polinomio a un ideal dado, la intersección y cociente de ideales y otras operaciones aritméticas sobre ideales. Sin embargo un aspecto esencial en las aplicaciones actuales de la matemática se basa en el uso de las bases de Gröbner, ya que al dar una interpretación de problemas en términos de ideales de anillos de polinomios; los algoritmos que involucran a bases de Gröbner tiene aplicación directa a la resolución

de estos problemas. En este trabajo tratamos algunos de estos problemas; aquellos que tratan de interpolación y otros relacionados con teoría de grafos.

Este trabajo está dividido en tres capítulos. Comenzamos dando al lector los conceptos necesarios para la comprensión de la teoría de anillos de polinomios que nos permitan tratar con ideales y polinomios de forma sencilla; de particular importancia es el problema de representar cada elemento. polinomio, de forma única, para lo que es necesario introducir los órdenes monomiales. El principal resultado es el Teorema de Dickson que es un resultado sobre finitud similar al Teorema de la base de Hilbert, y el principal algoritmo es el algoritmo de la división de un polinomio por un conjunto finito de polinomios.

En el Capítulo dos tratamos específicamente con bases de Gröbner y estudiamos el algoritmo de Buchberger que nos permite calcular una base de Gröbner de un ideal dado por un conjunto finito de generadores. La obtención de una base de Gröbner reducida asociada a un ideal es de particular importancia para el desarrollo posterior de la teoría.

Tratamos en el Capítulo tres de la resolución de tres problemas utilizando como herramienta la teoría de bases de Gröbner. El primero trata con el problema de interpolación multivariante; se estudian los métodos de interpolación de Lagrange, y Hermite. Ilustrando su aplicación con ejemplos variados como también la aplicación a la teoría de grafos y su desarrollo utilizando el software Mathematica 8. El segundo problema tratado es el del coloreado de grafos y su tratamiento algebraico. Estudiamos en particular el uso de cuerpos finitos que permite obtener de forma más eficiente la solución teórica, si bien para determinar cada posible solución sería necesario desarrollar otros métodos. El tercer problema trata de aplicar la aritmética a grafos; estudiamos el problema de determinar ciclos en grafos y también el problema de la existencia de caminos de una longitud dada.

Granada, 20 de junio de 2012

Índice general

Capítulo 1

POLINOMIOS E IDEALES

En este capítulo recordaremos algunos conceptos sobre anillos e ideales y los trasladaremos al anillo de polinomios en un cuerpo K.

1.1. Ideales en $K[X_1, \ldots, X_n]$

Sea K un cuerpo, $X_1, \ldots, X_n$ indeterminadas sobre K y $K[X_1, \ldots, X_n]$ el anillo de los polinomios en $X_1, \ldots, X_n$ con coeficientes en K.

Definición 1.1. *Un **monomio** en las indeterminadas $X_1, \ldots, X_n$ es un producto de la forma*

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n},$$

*donde todos los exponentes $\alpha_1, \ldots, \alpha_n$ son números naturales. El **grado total** del monomio $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ es $|\alpha| = \alpha_1 + \ldots + \alpha_n$.*

Podemos simplificar la notación para monomios del siguiente modo. Si $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ es una n-upla de números naturales, entonces escribimos $X^\alpha = X_1^{\alpha_1} \cdots X_n{}^{\alpha_n}$.

Definición 1.2. *Un **polinomio** $F \in K[X_1, \ldots, X_n]$ es una combinación lineal finita de monomios con coeficientes en K, y lo escribimos de la siguiente manera:*

$$F = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$$

Ésta es la representación distributiva de F. El problema de esta notación es que no es única en el sentido de que aunque las expresiones $X_1X_2^5 + X_2$ y $X_2 + X_1X_2^5$ se refieren al mismo polinomio son distintas, vamos a buscar criterios para asociar a cada polinomio una expresión única que nos permita compararlos de forma sencilla y poder desarrollar algoritmos sobre los mismos.

Definición 1.3. *Un conjunto $I \subset K[X_1, \ldots, X_n]$ es un **ideal** si satisface*

i. $0 \in I$.

ii. Si $F, G \in I$ *entonces* $F + G \in I$.

iii. Si $F \in I$ *y* $H \in K[X_1, \ldots, X_n]$ *entonces* $HF \in I$

De particular interés son los ideales generados por un número finito de polinomios.

Definición 1.4. *Sean $F_1, \ldots, F_s$ polinomios en $K[X_1, \ldots, X_n]$. Entonces*

$$\langle F_1, \ldots, F_s \rangle = \left\{ \sum_{i=1}^{s} H_i F_i | H_1, \ldots, H_s \in K[X_1, \ldots, X_n] \right\}.$$

Lema 1.5. *Si $F_1, \ldots, F_s \in K[X_1, \ldots, X_n]$, entonces $\langle F_1, \ldots, F_s \rangle$ es un ideal de $K[X_1, \ldots, X_n]$ y lo llamaremos el ideal generado por $F_1, \ldots, F_s$.*

Demostración. Primero, $0 = \sum_{i=1}^{s} 0 \cdot F_i$, luego $0 \in \langle F_1, \ldots, F_s \rangle$.
Suponga $F = \sum_{i=1}^{s} P_i F_i$ y $G = \sum_{i=1}^{s} QiF_i$ entonces

$$F + G = \sum_{i=1}^{s} (P_i + Q_i) F_i$$

Por último, sea $H \in K[X_1, \ldots, X_n]$,

$$HF = \sum_{i=1}^{s} (HP_i) F_i.$$

Queda demostrado que $\langle F_1, \ldots, F_s \rangle$ es un ideal.

1.2. Lema de Dickson. Órdenes Monomiales

Algunas herramientas algebraicas son necesarias para el tratamiento simbólico y computacional de los polinomios multivariados. En primer lugar, estudiaremos la manera de ordenar los términos $aX_1^{\alpha_1} \cdots X_n^{\alpha_1}$, con $a \in K$ un escalar, $X_1, \ldots, X_n$ indeterminadas, y $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. Como queremos que el escalar a no influya en el orden de los términos; fijada una ordenación de las indeterminadas, bastará con ordenar los exponentes $\alpha = (\alpha_1 \ldots \alpha_n) \in \mathbb{N}^n$.

Cuando trabajamos con polinomios en una indeterminada nos interesamos por su grado, que es un número natural, y el conjunto $\mathbb{N}$ de los números naturales es un conjunto

bien ordenado, pero con polinomios multivariados, no es tan obvio qué debiera ser el grado, y, de hecho, puede haber varias alternativas. Una razón fundamental es que el conjunto que indexa los monomios es ahora

$$\mathbb{N}^n = \{(\alpha_1, \ldots, \alpha_n) : \alpha_1, \ldots, \alpha_n \in \mathbb{N}\},$$

para $n > 1$, y en contraste con el caso $n = 1$, hay una infinidad de maneras distintas de ordenar $\mathbb{N}^n$. Además, con objeto de poder hacer argumentos de teoría de anillos, habremos de usar órdenes que proporcionen buenas ordenaciones. El resultado que asegurará que esto va a ser posible se llama Lema de Dickson, y comenzaremos discutiéndolo.

Lema 1.6. ***(Lema de Dickson)*** *Sea $S \subseteq \mathbb{N}^n$ un subconjunto no vacío, entonces existe un subconjunto finito $G \subseteq S$ tal que para cada $\alpha \in S$ existen $\beta \in G$ y $\gamma \in \mathbb{N}^n$ tales que $\alpha = \beta + \gamma$.*

Se dice que G genera a S.

Demostración. Hacemos inducción sobre n. Si $n = 1$, entonces $S \subseteq \mathbb{N}$ y podemos tomar $G = \{\beta\}$, siendo β el primer elemento de S. Supongamos que $n > 1$. Tomamos $\beta \in S$, si existe $\alpha \in S$ tal que $\alpha \notin \beta + \mathbb{N}^n$, entonces existe un índice i tal que $\alpha_i < \beta_i$, y en particular α pertenece a uno de los siguientes subconjuntos:

$$S_{ij} = \{\alpha \in S | \alpha_i = j\};\ i = 1, \ldots, n;\ j = 0, \ldots, \beta_i - 1,$$

Definimos nuevos subconjuntos

$$S'_{ij} = \{\alpha \in \mathbb{N}^n | \alpha_i = 0 \text{ y } (\alpha_1, \ldots, \alpha_{i-1}, j, \alpha_{i+1}, \ldots, \alpha_n) \in S_{ij}\}$$

Podemos considerar $S'_{ij} \subseteq \mathbb{N}^{n-1}$. Por la hipótesis de inducción, existe $G'_{ij} \subseteq S'_{ij}$ finito que genera S'_{ij}. Definimos entonces

$$G_{ij} = \{(\alpha_1, \ldots, \alpha_{i-1}, j, \alpha_{i+1}, \ldots, \alpha_n) \in S_{ij} | (\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) \in G'_{ij}\}.$$

Resulta que G_{ij} es un subconjunto finito que genera S_{ij}, luego $\{\beta\} \cup (\bigcup_{ij} G_{ij})$ es un conjunto finito que genera a S.

Cada $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ determina un monomio estándar $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_1}$ en el anillo de polinomios $K[X_1, \ldots, X_n]$. Entonces decimos que todo conjunto A de monomios estándar contiene un subconjunto finito B tal que cada monomio de A es múltiplo de alguno de B.

Ordenar el conjunto $\{X^\alpha | \alpha \in \mathbb{N}^n\}$ de monomios del anillo de polinomios $K[X_1, \ldots, X_n]$ es equivalente a ordenar $\mathbb{N}^n$. Los órdenes que nos interesarán en la práctica serán del tipo de los descritos en la siguiente definición.

Definición 1.7. *Un* ***orden monomial*** $\preceq$ *en* $K[X_1, \ldots, X_n]$ *es una relación* $\preceq$ *en* $\mathbb{N}^n$*, o de forma equivalente, una relación en el conjunto de los monomios* $\{X^\alpha | \alpha \in \mathbb{N}^n\}$*, que satisface:*

i. $\preceq$ *es un orden total en* $\mathbb{N}^n$*.*

ii. Si $\alpha \preceq \beta$ *y* $\gamma \in \mathbb{N}^n$*, entonces* $\alpha + \gamma \preceq \beta + \gamma$*.*

iii. $\preceq$ *es un buen orden en* $\mathbb{N}^n$*. Esto es, todo subconjunto no vacío de* $\mathbb{N}^n$ *tiene un primer elemento.*

A continuación daremos algunos ejemplos de órdenes monomiales en $\mathbb{N}^n$

Definición 1.8. ***(Orden Lexicográfico)*** *Sea* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *y* $\beta = (\beta_1 \ldots, \beta_n) \in \mathbb{N}^n$*. Decimos* $\beta \preceq_{lex} \alpha$ *si en el vector diferencia* $\alpha - \beta \in \mathbb{N}^n$*, el primer elemento distinto de cero, de izquierda a derecha, es positivo. Escribiremos* $X^\beta \preceq_{lex} X^\alpha$ *si* $\beta \preceq_{lex} \alpha$*.*

Ejemplo 1.1.

a. $(1, 3, 0) \succeq_{lex} (1, 2, 4)$ *ya que* $(1, 3, 0) - (1, 2, 4) = (0, 1, -4)$*.*

b. Las variables $X_1, \ldots, X_n$ *se ordenan conforme el orden lexicográfico de la siguiente manera:*

$$(1, 0, \ldots, 0) \succeq_{lex} (0, 1, 0, \ldots, 0) \succeq_{lex} \cdots \succeq_{lex} (0, 0, \ldots, 1)$$

entonces $X_1 \succeq_{lex} X_2 \succeq_{lex} \cdots \succeq_{lex} X_n$*. De forma natural esta es la ordenación de las variables que permite asociar a un monomio* $X^\alpha = X_1^{\alpha_1} \cdots X^{\alpha_n}$ *la* n*–upla* $(\alpha_1, \ldots, \alpha_n)$*.*

Definición 1.9. ***(Orden Lexicográfico Graduado)*** *Sean* $\alpha, \beta \in \mathbb{N}^n$*. Decimos* $\beta \preceq_{grlex} \alpha$ *si*

$$|\beta| = \sum_{i=1}^{n} \beta_i < |\alpha| = \sum_{i=1}^{n} \alpha_i$$

o si $|\alpha| = |\beta|$ *y* $\beta \preceq_{lex} \alpha$

Ejemplo 1.2.

a. $(1, 2, 3) \succeq_{grlex} (2, 3, 0)$ *ya que* $|(1, 2, 3)| = 6 > |(2, 3, 0)| = 5$*.*

b. $(1, 5, 4) \succeq_{grlex} (1, 3, 6)$ *ya que* $|(1, 5, 4)| = |(1, 3, 6)|$ *y* $(1, 5, 4) \succeq_{lex} (1, 3, 6)$*.*

Definición 1.10. ***(Orden Lexicográfico Graduado Inverso)*** *Sean $\alpha, \beta \in \mathbb{N}^n$. Decimos $\beta \preceq_{grevlex} \alpha$ si*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$$

o si $|\alpha| = |\beta|$ y en $\alpha - \beta \in \mathbb{Z}^n$ el primer elemento distinto de cero de derecha a izquierda es negativo.

Ejemplo 1.3.

a. $(4,7,1) \succeq_{grevlex} (4,2,3)$ *ya que* $|(4,7,1)| = 12 > |(4,2,3)| = 9$.

b. $(1,5,2) \succeq_{grevlex} (4,1,3)$ *ya que* $|(1,5,2)| = |(4,1,3)|$ *y* $(1,5,2) - (4,1,3) = (-3,4,-1)$.

Con el objeto de fijar notación, a la hora de tratar con polinomios, definiremos los siguientes términos

Definición 1.11. *Sea $F = \sum_\alpha a_\alpha X^\alpha$ un polinomio distinto de cero en $K[X_1, \ldots, X_n]$ y sea $\preceq$ un orden monomial*

i. *El* ***diagrama de Newton*** *de F es $\mathcal{N}(F) = \{\alpha \in \mathbb{N}^n | a_\alpha \neq 0\}$.*

ii. *El* ***exponente*** *de F es exp(F)*$= \max\{\alpha \in \mathbb{N}^n | \alpha \in \mathcal{N}(F)\}$.

iii. *El* ***grado*** *de F es grad(F)* $= \max\{|\alpha| : \alpha \in \mathcal{N}(F)\}$.

iv. *El* ***coeficiente líder*** *de F, $lc(F) = a_{exp(F)}$.*

v. *El* ***término líder*** *de F, $lt(F) = a_{exp(F)} X^{exp(F)}$.*

vi. *El* ***monomio líder*** *de F, $lm(F) = X^{exp(F)}$.*

Lo siguiente es también notación. Si $\alpha(1), \ldots, \alpha(t) \in \mathbb{N}^n$, es una lista de elementos de $\mathbb{N}^n$, definimos:

$$\begin{aligned}
\Delta^1 &= \alpha(1) + \mathbb{N}^n, \\
\Delta^2 &= (\alpha(2) + \mathbb{N}^n) \setminus \Delta^1, \\
&\vdots \\
\Delta^t &= (\alpha(t) + \mathbb{N}^n) \setminus \bigcup_{i<t} \Delta^i, \\
\overline{\Delta} &= \mathbb{N}^n \setminus \bigcup_{i \leq t} \Delta^i
\end{aligned}$$

Lema 1.12. *Para cada lista de elementos de $\mathbb{N}^n$, por ejemplo $\alpha(1), \ldots, \alpha(t)$, tenemos que $\{\Delta^1, \Delta^2, \ldots, \Delta^t, \overline{\Delta}\}$ es una partición de $\mathbb{N}^n$, cuando eliminamos los conjuntos vacíos.*

Como consecuencia, de este resultado, tenemos el siguiente algoritmo de la división en el anillo $K[X_1, \ldots, X_n]$.

Teorema 1.13. *Dado un orden monomial en $\mathbb{N}^n$, para cada lista finita de polinomios no nulos*

$$G_1, \ldots, G_t \in K[X_1, \ldots, X_n],$$

consideramos la partición de $\mathbb{N}^n$ determinada por la lista

$$exp(G_1), \ldots, exp(G_t).$$

Se verifica entonces que para cada $0 \neq F \in K[X_1, \ldots, X_n]$ existen elementos $Q_1, \ldots, Q_t$ y $R \in K[X_1, \ldots, X_n]$, únicos, cumpliendo las propiedades siguientes:

i. $F = \Sigma_{i=1}^t Q_i G_i + R$;

ii. $R = 0$ *ó* $\mathcal{N}(R) \subseteq \overline{\Delta}$;

iii. Para cada índice i se verifica: $exp(G_i) + \mathcal{N}(Q_i) \subseteq \Delta^i$. *Como consecuencia, si* $Q_i G_i \neq 0$, *se tiene* $exp(Q_i G_i) \preceq exp(F)$ *y si* $R \neq 0$, *entonces* $exp(R) \preceq exp(F)$.

1.3. Ideales Monomiales

Un ideal I de $K[X_1, \ldots, X_n]$ se llama **monomial** si tiene un sistema de generadores formado por monomios.

Lema 1.14. *Si I es un ideal monomial con un sistema de generadores formado por monomios $\{X^\alpha | \alpha \in A \subseteq \mathbb{N}^n\}$, para cada monomio $X^\beta \in K[X_1, \ldots, X_n]$ son equivalentes:*

i. $X^\beta \in I$.

ii. Existe $F \in K[X_1, \ldots, X_n]$ *tal que* $X^\beta = F X^\alpha$, *para algún* $\alpha \in A$.

Además este F se puede tomar monomial.

Lema 1.15. *Sea I un ideal monomial y sea F un elemento de $K[X_1, \ldots, X_n]$. Son equivalentes los siguientes enunciados:*

i. $F \in I$.

ii. Todo monomio de F *pertenece a* I.

iii. F *es una combinación* K*-lineal de monomios de* I.

Si I es un ideal definimos:

$$Exp(I) = \{exp(F) | 0 \neq F \in I\}.$$

Un subconjunto $E \subseteq \mathbb{N}^n$ se llama un **monoideal**, si para cada $\gamma \in E$ y cada $\alpha \in \mathbb{N}^n$ se tiene $\gamma + \alpha \in E$, esto es, $E = E + \mathbb{N}^n$

Lema 1.16. *Para cada ideal* I *de* $K[X_1, \ldots, X_n]$ *se tiene que* $Exp(I)$ *es un monoideal de* $\mathbb{N}^n$.

Lema 1.17. ***(Lema de Dickson para ideales monomiales)*** *Si* I *es un ideal monomial, entonces* I *tiene un sistema finito de generadores formado por monomios.*

Proposición 1.18. *Cada ideal monomial tiene un sistema finito mínimo de generadores.*

Demostración. Sean G y G' dos sistemas de generadores. Para cada $g \in G$ existe $g' \in G'$ tal que $g'|g$, luego $(G \setminus \{g\}) \cup \{g'\}$ es un nuevo sistema de generadores que ocupa el lugar de G. Si realizamos este proceso para cada sistema de generadores G', llegamos a un sistema de generadores mínimo.

Es claro que existe una biyección entre ideales monomiales de $K[X_1, \ldots, X_n]$ y monoideales de $\mathbb{N}^n$. En esta biyección a cada ideal I le corresponde el monoideal $Exp(I)$, y a cada monoideal $E \subseteq \mathbb{N}^n$, con sistema de generadores G le corresponde el ideal monomial con sistema de generadores $\{X^\gamma | \gamma \in G\}$. En ambos casos los sistemas de generadores pueden ser tomados finitos.

Lema 1.19. *Sea* I *un ideal no nulo de* $K[X_1, \ldots, X_n]$. *Si* $A \subseteq \mathbb{N}^n$ *es un sistema finito de generadores de* $Exp(I)$, *para cada conjunto de polinomios* $\{F_\alpha | \alpha \in A\} \subseteq I$ *tales que* $exp(F_\alpha) = \alpha$ *para cada* $\alpha \in A$, *se tiene que* $\{F_\alpha | \alpha \in A\}$ *es sistema de generadores de* I *como ideal.*

Capítulo 2

BASES DE GRÖBNER

Estamos ya preparados para manejar sistemas de generadores de ideales de anillos de polinomios con coeficientes en un cuerpo. La primera observación que necesitamos es la siguiente. Seguimos denotando por $K[X_1, \ldots, X_n]$ el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en K, y por $\preceq$ un orden admisible sobre $\mathbb{N}^n$.

Si I es un ideal de $K[X_1, \ldots, X_n]$, una **base de Gröbner** de I es un conjunto finito de elementos no nulos, $G = \{G_1, \ldots, G_t\} \subseteq I$, verificando que

$$Exp(I) = \{exp(G_1), \ldots, exp(G_t)\} + \mathbb{N}^n = Exp(G) + \mathbb{N}^n.$$

respecto de un orden monomial admisible.

Corolario 2.1.

i. Cada ideal no nulo de $K[X_1, \ldots, X_n]$ tiene una base de Groebner.

ii. Toda base de Groebner de un ideal no nulo es un sistema de generadores.

iii. ***Teorema de la base de Hilbert.*** *Todo ideal de $K[X_1, \ldots, X_n]$ es finitamente generado.*

2.1. Algoritmo de Buchberger

Aunque sabemos que cada ideal de $K[X_1, \ldots, X_n]$ tiene una base de Gröbner, aún no tenemos un procedimiento para calcularla. Normalmente, un ideal vendrá dado por un conjunto finito de generadores. Presentaremos el Algoritmo de Buchberger, que permite calcular una base de Gröbner a partir de un sistema de generadores dado. Durante el desarrollo de esta sección, consideraremos un orden admisible $\preceq$ sobre $\mathbb{N}^n$.

Vamos a introducir la notación necesaria para su desarrollo.

Si X^α y X^β son dos monomios, vamos a definir su mínimo común múltiplo. Sea

$$\gamma_i = \text{máx}\{\alpha_i, \beta_i\}, 1 \leq i \leq n.$$

Sea $\gamma = (\gamma_1, \cdots, \gamma_n) \in \mathbb{N}^n$, entonces llamamos a X^γ el **mínimo común múltiplo** de X^α y X^β. Tenemos que X^γ es realmente un múltiplo ya que se verifica:

$$X^\gamma = X^{\gamma-\alpha}X^\alpha.$$

Y el resultado es análogo para X^β.

Representaremos el mínimo común múltiplo por m.c.m$\{X^\alpha, X^\beta\}$. Con esto definiremos las **semisicigias** ó **s–polinomios**s–polinomios. Dados $F, G \in K[X_1, \ldots, X_n]$, con $exp(F) = \alpha$ y $exp(G) = \beta$, el s–polinomio definido por F y G es:

$$S(F,G) = \frac{1}{lc(F)}X^{\gamma-\alpha}F - \frac{1}{lc(G)}X^{\gamma-\beta}G$$

Lema 2.2. *Se considera la expresión $\sum_i c_i X^{\alpha(i)}F_i$, en donde, los F_i son elementos de $K[X_1, \ldots, X_n]$, $c_i \in K$, y $\alpha(i) \in \mathbb{N}^n$, verificando:*

$$exp(\sum_i c_i X^{\alpha(i)}F_i) < \delta = exp(X^{\alpha(i)}F_i),$$

para cada índice i. Entonces existen elementos $c_{jk} \in K$ tales que :

$$\sum_i c_i X^{\alpha(i)}F_i = \sum_{jk} c_{jk}X^{\delta-\gamma(jk)}S(F_j, F_k), \text{ y } exp(X^{\delta-\gamma(jk)}S(F_j, F_k)) < \delta,$$

en donde $X^{\gamma(jk)} = m.c.m.\{X^{exp(F_j)}, X^{exp(F_k)}\}$.

Demostración. Supongamos que $exp(F_i) = \beta(i)$, entonces $\alpha(i) + \beta(i) = \delta$. Hacemos el siguiente desarrollo:

$$\sum_i c_i X^{\alpha(i)}F_i = \sum_i c_i lc(F_i)\frac{X^{\alpha(i)}F_i}{lc(F_i)} = \sum_i c_i lc(F_i)H_i$$

donde $\frac{X^{\alpha(i)}F_i}{lc(F_i)} = H_i$. Podemos completar este desarrollo de la siguiente forma:

$$\begin{aligned}\sum_i c_i X^{\alpha(i)} F_i &= \sum_i c_i lc(F_i) H_i = \\ &= c_1 lc(F_1)(H_1 - H_2) + (c_1 lc(F_1) + c_2 lc(F_2))(H_2 - H_3) + \cdots \\ &+ (c_1 lc(F_1) + \cdots c_{t-1} lc(F_{t-1}))(H_{t-1} - H_t) + \\ &+ (c_1 lc(F_1) + \cdots + c_t lc(F_t)) H_t.\end{aligned}$$

Consideramos ahora el producto $X^{\delta-\gamma(jk)} S(F_j, F_k)$. Vamos a desarrolllarlo y así obtener un múltiplo de $H_j - H_k$.

$$\begin{aligned}& X^{\delta-\gamma(jk)} S(F_j, F_k) = \\ = \; & X^{\delta-\gamma(jk)} \Big(\frac{1}{lc(F_j)} X^{\gamma(jk)-\beta(j)F_j} - \frac{1}{lc(F_k)} X^{\gamma(jk)-\beta(k)F_k} \Big) \\ = \; & \frac{1}{lc(F_j)} X^{\delta-\gamma(jk)} X^{\gamma(jk)-\beta(j)F_j} - \frac{1}{lc(F_k)} X^{\delta-\gamma(jk)} X^{\gamma(jk)-\beta(k)F_k} \\ = \; & \frac{1}{lc(F_j)} X^{\delta-\beta(j)} F_j - \frac{1}{lc(F_k)} X^{\delta-\beta(k)} F_k \\ = \; & \frac{X^{\alpha(i)} F_j}{lc(F_j)} - \frac{X^{\alpha(k)} F_k}{lc(F_k)} \\ = \; & H_j - H_k.\end{aligned}$$

Entonces tenemos

$$X^{\delta-\gamma(jk)} S(F_j, F_k) = H_j - H_k.$$

Ahora como $\sum c_i lc(F_i) = 0$, tenemos:

$$\begin{aligned}\sum c_i X^{\alpha(i)F_i} &= c_1 lc(F_1) X^{\delta-\gamma(12)} S(F_1, F_2) + \\ &+ (c_1 lc(F_1) + c_2 lc(F_2)) X^{\delta-\gamma(23)} S(F_2, F_3) + \cdots \\ &+ (c_1 lc(F_1) + \cdots + c_{t-1} lc(F_{t-1})) X^{\delta-\gamma(t-1,t)} S(F_{t-1}, F_t)\end{aligned}$$

Y hemos demostrado la primera parte del enunciado. Para la segunda parte tenemos en cuenta que cada H_i es un polinomio mónico con $exp(H_i) = \delta$, entonces $exp(H_i - H_j) < \delta$ y tenemos el resultado.

Teorema 2.3. ***(Teorema de Buchberger)*** *Sea G un conjunto finito de generadores de un ideal I de $K[X_1, \ldots, X_n]$. Entonces $\mathbb{G}$ es una base de Gröbner para I si, y sólo si, $R(S(G_i, G_j) : \mathbb{G}) = 0$ para todo $G_i, G_j \in \mathbb{G}$. Entiéndase $R(S(G_i, G_j) : \mathbb{G}) = 0$ como que el resto de aplicar el Algoritmo de la División para dividir $S(G_i, G_j)$ entre $\mathbb{G}$ da como resultado 0.*

Demostración. Es evidente que si $\mathbb{G}$ es una base de Gröbner entonces es un sistema de generadores de I entonces $R(S(G_i, G_j) : \mathbb{G}) = 0$.
Sea $0 \neq F \in I$ entonces $F = \sum Q_i G_i$ y tenemos

$$exp(F) \preceq \text{máx}\{exp(Q_i G_i) | i = 1, \ldots, t\}.$$

Se puede alcanzar la igualdad de la siguiente forma. Llamamos:

$$\begin{aligned} \delta &= \text{máx}\{exp(Q_i G_i) | i = 1, \ldots, t\}, \\ \delta(i) &= exp(Q_i G_i). \end{aligned}$$

Si $exp(F) < \delta$, descomponemos F en la siguiente forma:

$$\begin{aligned} F &= \sum_i Q_i G_i \\ &= \sum_{\delta(i)=\delta} Q_i G_i + \sum_{\delta(i)<\delta} Q_i G_i \\ &= \sum_{\delta(i)=\delta} lm(Q_i) G_i + \sum_{\delta(i)=\delta} (Q_i - lm(Q_i)) G_i + \sum_{\delta(i)<\delta} Q_i G_i. \end{aligned}$$

Las dos últimas sumas son "*despreciables*", ya que su exponente es menor que δ. Vamos a cambiar $\sum_{\delta(i)=\delta} lm(Q_i) G_i$ mediante otra expresión. Usando el Lema (2.2) tenemos:

$$\sum_{\delta(i)=\delta} lm(Q_i) G_i = \sum c_{jk} X^{\delta - \gamma(jk)} S(G_i, G_k),$$

con $exp(X^{\delta-\gamma(jk)} S(G_i, G_k)) < \delta$. Los restos de la división de $S(G_i, G_k)$ por $G_1, \ldots, G_t$ son cero, entonces resulta:

$$S(G_i, G_k) = \sum Q_{jki} G_i; \quad Q_{jki} \in K[X_1, \ldots, X_n]$$

y por el algoritmo de la división tenemos:

$$exp(Q_{jki} G_i) \leq exp(S(G_j, G_k)).$$

Encontramos pues una expresión del siguiente tipo:

$$F = \sum_i Q'_i G_i \text{ con } exp(Q'G_i) < \delta.$$

Repitiendo el proceso tantas veces como sea necesario, llegamos a una expresión

$$F = \sum_i Q_i G_i,$$

en donde $exp(F) = \text{máx}\{exp(Q_i G_i) | i = 1, \ldots, t\}$, y como consecuencia $exp(F) = exp(Q_i G_i)$ para algún índice i, esto es:

$$exp(F) = exp(Q_i G_i) = exp(Q_i) + exp(G_i) \in \{exp(G_1), \ldots, exp(G_t)\} + \mathbb{N}^n.$$

y $\mathbb{G}$ es una base de Gröbner.

Teorema 2.4. ***(Algoritmo de Buchberger)*** *Sea I un ideal no nulo de $K[X_1, \ldots, X_n]$ con un sistema de generadores $\{F_1, \ldots, F_t\}$. Es posible construir una base de Gröbner de I siguiendo los pasos:*

i. Se define $\mathbb{G}_0 = \{F_1, \ldots, F_t\}$;

ii. Se define $\mathbb{G}_{n+1} = \bigcup \{R(S(F, G); \mathbb{G}_n) \neq 0 | F, G \in \mathbb{G}_n\}$.

Entonces cuando $\mathbb{G}_i = \mathbb{G}_{i+1}$, tenemos que $\mathbb{G}_i$ es una base de Gröbner de I.

Demostración. Dado $\mathbb{G}_0 = \{F_1, \ldots, F_t\}$, si $R(S(F, G); \mathbb{G}_0) = 0$ para cada par $F, G \in \mathbb{G}_0$, entonces tenemos una base de Gröbner. Si no lo es, existen $F, G \in \mathbb{G}_0$ tales que $R(S(F, G); \mathbb{G}_0) \neq 0$. Llamamos $G_{t+1} = R(S(F, G); \mathbb{G})$. Tenemos que $\mathcal{N}(G_{t+1}) \subseteq \overline{\Delta}$. Entonces, si definimos:

$$\mathbb{G}_{(1)} = \{G_1, \ldots, G_t, G_{t+1}\},$$

obtenemos una partición

$$\Delta^1, \ldots, \Delta^t, \Delta^{t+1}, \overline{\Delta^1},$$

siendo $\Delta^{t+1} \cup \overline{\Delta^{(1)}} = \overline{\Delta}$. Si $R(F; \mathbb{G}_0) = 0$, para $F \in K[X_1, \ldots, X_n]$, entonces $R(F; \mathbb{G}_{(1)}) = 0$, y en el caso en que $R(S(G_i, G_j), \mathbb{G}_0) = 0$, también se tiene $R(S(G_i, G_j), G_{(1)}) = 0$ por lo tanto se puede aprovechar el trabajo hecho.

Si para todo $F, G \in \mathbb{G}_{(1)}$ se verifica $R(S(F, G); \mathbb{G}_{(1)}) = 0$, entonces tenemos una base de Gröbner. En el caso contrario tenemos un nuevo $G_{t+2} = R(S(F, G); \mathbb{G}_{(1)}) \neq 0$, y definimos $\mathbb{G}_{(2)} = \{G_1, ...G_{t+1}, G_{t+2}\}$, teniendo que $\mathcal{N}(G_{t+2}) \subseteq \overline{\Delta^{(1)}}$.

Si en algún momento encontramos una base de Gröbner, ya hemos terminado, en caso contrario tendríamos una cadena ascendente de sistemas de generadores:

$$\mathbb{G}_0 \subset \mathbb{G}_{(1)} \subset \cdots$$

Asociada tenemos una cadena ascendente de monoideales:

$$exp(\mathbb{G}_0) + \mathbb{N}^n \subset exp(\mathbb{G}_{(1)}) + \mathbb{N}^n \subset \cdots$$

Como consecuencia del Lema de Dickson esta cadena se estabiliza y por tanto existe un índice n tal que

$$exp(\mathbb{G}_{(n)}) + \mathbb{N}^n = exp(\mathbb{G}_{(n+1)}) + \mathbb{N}^n$$

tenemos entonces

$$exp(\mathbb{G}_{(t+n+1)}) \in exp(\mathbb{G}_{(n)}) + \mathbb{N}^n = \mathbb{N}^n \setminus \overline{\Delta^{(n)}},$$

pero $exp(\mathbb{G}_{(t+n+1)}) \in \overline{\Delta^{(n)}}$, lo que es una contradicción.

Calculando una Base de Gröbner

Vamos a ilustrar el cálculo de una base de Gröbner mediante el Algoritmo de Buchberger en un ejemplo sencillo

Ejemplo 2.1. *Consideremos*[1] $M = \{F_1, F_2\} \subseteq K[X, Y]$ *(K denota, como es usual, un cuerpo), donde* $F_1 = X^2Y + X + 1$, $F_2 = XY + Y^2 + 1$.

Usamos el orden lexicográfico con $X >_{lex} Y$. Ponemos, claro, $\mathbb{G}_0 = \{F_1, F_2\}$. Un primer cálculo nos dice que

$$R(S(F_1, F_2); \mathbb{G}_0) = Y^3 + Y + 1$$

De acuerdo con el Algoritmo de Buchberger, ponemos

$$\mathbb{G}_1 = \{F_1, F_2, F_3\}, \text{ donde } F_3 = Y^3 + Y + 1.$$

Observemos que no calculamos $S(F_1, F_1)$ ni $S(F_2, F_2)$, puesto que ambos son trivialmente nulos.

Sigamos aplicando el algoritmo: tenemos que calcular $R(S(F_1, F_2); \mathbb{G}_1)$, $R(S(F_1, F_3); \mathbb{G}_1)$ y $R(S(F_2, F_3); \mathbb{G}_1)$. En realidad, puesto que $F_3 = R(S(F_1, F_2); \mathbb{G}_0)$, tenemos inmediatamente que $F_1 = R(S(F_1, F_2); \mathbb{G}_1) = 0$, ya que $F_3 \in \mathbb{G}_1$. Esto es porque si $S(F_1, F_2) = Q_1F_1 + Q_2F_2 + F_3$ es una división de $S(F_1, F_2)$ entre $\mathbb{G}_0 = F_1, F_2$ (con resto F_3), entonces claramente $S(F_1, F_2) = Q_1F_1 + Q_2F_2 + 1 \cdot F_3 + 0$ es una división de (F_1, F_2) entre $\mathbb{G}_1 = \{F_1, F_2, F_3\}$ (con resto 0). Sólo tenemos, pues, que calcular $R(S(F_1, F_3); \mathbb{G}_1)$ y $R(S(F_2, F_3); \mathbb{G}_1)$. Bien, tenemos que

$$S(F_1, F_3) = Y^2F_1 - X^2F_3 = -X^2Y + XY^2 - X^2 + Y^2.$$

[1]Ejemplo tomado de José Gómez Torrecillas, *Guía de estudio*, septiembre 2003, Universidad de Granada.

$X^2Y + X + 1$	$Q_1 : -1$
$XY + Y^2 + 1$	$Q_2 : Y$
$Y^3 + Y + 1$	$Q_3 : -1$

$-X^2Y + XY^2 - X^2 + Y^2$	
$-X^2Y - X - 1$	
$H_1 : XY^2 - X^2 + X + Y^2 + 1$	
$XY^2 + Y^3 + Y$	
$H_2 : -X^2 + X + Y^2 + 1 - Y^3 - Y$	
$-X^2 + X \longrightarrow$	resto
$H_3 : -Y^3 + Y^2 - Y + 1$	$R : -X^2 + X$
$-Y^3 - Y - 1$	
$H_4 : Y^2 + 2$	$R : -X^2 + X$
$Y^2 + 2 \longrightarrow$	
$H_5 : 0$	$R : -X^2 + X + Y^2 + 2$

Escribimos $F_4 = R(S(F_1, F_3); \mathbb{G}_1) = -X^2 + X + Y^2 + 2$.

Ahora tenemos

$$S(F_2, F_3) = Y^2F_2 - XF_3 = -XY - X + Y^4 + Y^2$$

Dividimos:

$X^2Y + X + 1$	$Q_1 :$
$XY + Y^2 + 1$	$Q_2 : -1$
$Y^3 + Y + 1$	$Q_3 : Y$

$XY - X + Y^4 + Y^2$	
$-XY - Y^2 - 1$	
$H_1 : -X + Y^4 + 2Y^2 + 1$	
$-X \longrightarrow$	resto
$H_2 : Y^4 + 2Y^2 + 1$	$R = -X$
$Y^4 + Y^2 + Y$	
$H_3 : Y^2 - Y + 1$	$R : -X$
$Y^2 - Y + 1 \longrightarrow$	
$H_4 : 0$	$R : -X + Y^2 - Y + 1$

Escribimos

$$F_5 = R(S(F_2, F_3); \mathbb{G}_1) = -X + Y^2 - Y + 1$$

y

$$\mathbb{G}_2 = \{F_1, F_2, F_3, F_4, F_5\}$$

En el proceso anterior obtenemos un sistema de generadores que es una base de Gröbner, y que tiene, posiblemente, demasiados elementos. Veamos como optimizar el número de elementos de una base de Gröbner.

2.2. Bases de Gröbner minimales y reducidas

Comenzaremos viendo un procedimiento que permite, a partir de una base de Gröbner $\mathbb{G}$ de un ideal I, eliminar algunos de los polinomios de $\mathbb{G}$ para obtener una base de Gröbner de I con un número menor de polinomios. Ilustramos primero dicho procedimiento con un ejemplo.

Ejemplo 2.2. *Continuamos con el Ejemplo* (2.1).

Tenemos la base de Gröbner del ideal I, calculada tras aplicar el Algoritmo de Buchberger:

$$\mathbb{G} = \{F_1, F_2, F_3, F_4, F_5\},$$

donde

$$\begin{aligned} F_1 &= X^2Y + X + 1 \\ F_2 &= XY + Y^2 + 1 \\ F_3 &= Y^3 + Y + 1 \\ F_4 &= -X^2 + X + Y^2 + 2 \\ F_5 &= -X + Y^2 - Y + 1 \end{aligned}$$

Tenemos, pues, usando el orden lexicográfico con $X > Y$ para calcular los exponentes de $F_1, \ldots, F_5$ que

$$\text{Exp}(I)=((2,1)+\mathbb{N}^2) \cup ((1,1)+\mathbb{N}^2) \cup ((0,3)+\mathbb{N}^2) \cup ((2,0)+\mathbb{N}^2) \cup ((1,0)+\mathbb{N}^2)$$

Ahora, $(1,1) \in (1,0)+\mathbb{N}^2$, lo que implica que

$$Exp(I) = ((1,1)+\mathbb{N}^2) \cup ((0,1)+\mathbb{N}^2) \cup ((2,0)+\mathbb{N}^2) \cup ((1,0)+\mathbb{N}^2)$$

Como $(1,1) \in (1,0)+\mathbb{N}^n$, deducimos que

$$Exp(I) = ((0,3)+\mathbb{N}^2) \cup ((2,0)+\mathbb{N}^2) \cup ((1,0)+\mathbb{N}^2).$$

Una vez más, $(2,0) \in (1,0) + \mathbb{N}^2$, luego

$$Exp(I) = ((0,3) + \mathbb{N}^2) \cup ((1,0) + \mathbb{N}^2).$$

Así que tenemos $F_3, F_5 \in I$ que verifican

$$Exp(I) = (exp(F_3) + \mathbb{N}^2) \cup (exp(F_5) + \mathbb{N}^2).$$

Puesto que $exp(F_3) = (0,3)$ y $exp(F_5) = (1,0)$. Por tanto, $\{F_3, F_5\}$ es una base de Gröbner de I.

Lema 2.5. *Sea I un ideal no nulo de $K[X_1, \ldots, X_n]$ y $\mathbb{G} = \{G_1, \ldots, G_t\}$ una base de Gröbner de I. Sea $F \in \mathbb{G}$ un polinomio que verifica:*

$$exp(F) \in \{exp(G) | F \neq G \in \mathbb{G}\} + \mathbb{N}^n,$$

entonces $\mathbb{G} \setminus \{F\}$ es una base de Gröbner de I.

Una base de Gröbner $\mathbb{G}$ de un ideal no nulo I de $K[X_1, ...X_n]$ se llama **minimal** si verifica:

i. $lc(F) = 1$ para cada $F \in \mathbb{G}$.

ii. $exp(F) \notin \{exp(G) | F \neq G \in \mathbb{G}\} + \mathbb{N}^n$ para cada $F \in \mathbb{G}$.

Simplemente eliminando los elementos que sobran tenemos la siguiente proposición.

Proposición 2.6. *Todo ideal no nulo I de $K[X_1, \ldots, X_n]$ tiene una base de Gröbner minimal.*

Corolario 2.7. *Dado un subconjunto $\mathbb{G} = \{G_1, ...G_t\} \subseteq I$ de un ideal de $K[X_1, \ldots, X_n]$ son equivalentes:*

i. $\mathbb{G}$ es una base de Gröbner minimal.

ii. $\{exp(G_1), \ldots, exp(G_t)\}$ es un sistema mínimo de generadores de Exp(I).

Como consecuencia los términos líderes de una base de Gröbner minimal están determinados de forma única y cada dos bases de Gröbner minimales tienen el mismo numero de elementos.

Un ideal puede tener bases de Gröbner minimales distintas. Para buscar la unicidad vamos a introducir las bases de Gröbner reducidas. Una base de Gröbner $\mathbb{G}$ de un ideal no nulo de I se llama **reducida** si verifica:

i. $lc(F) = 1$ para cada $F \in \mathbb{G}$.

ii. $\mathcal{N}(F) \cap (\{exp(G) | F \neq G \in \mathbb{G}\} + \mathbb{N}^n) = \varnothing$ para cada $F \in \mathbb{G}$.

Es claro que toda base de Gröbner reducida de un ideal no nulo de I es una base de Gröbner minimal.

Teorema 2.8. *Cada ideal no nulo tiene una única base de Gröbner reducida*

Demostración. Si $\mathbb{G}$ es una base minimal, un elemento $F \in \mathbb{G}$ se llama **reducido** si

$$\mathcal{N}(F) \cap (\{exp(G)\ F \neq G \in \mathbb{G}\} + \mathbb{N}^n) = \varnothing.$$

Si $F \in \mathbb{G}$ es reducido, entonces es reducido en cualquier base de Gröbner minimal $\mathbb{G}'$ que lo contenga y que verifique:

$$\{exp(G) | G \in \mathbb{G}\} = \{exp(G) | G \in \mathbb{G}'\}.$$

Definimos para cada $F \in \mathbb{G}$ los siguientes elementos:

$$\begin{aligned} F' &= R(F, \mathbb{G} \setminus \{F\}); \\ \mathbb{G}' &= (\mathbb{G} \setminus \{F\}) \cup \{F'\}. \end{aligned}$$

$\mathbb{G}'$ es también una base de Gröbner de I si $exp(F) \neq exp(F')$, entonces de las relaciones:

$$\begin{aligned} F &= \sum Q_G G + R(F; \mathbb{G} \setminus \{F\}) = \sum Q_G G + F' \\ exp(F) &= \text{máx}\{\{exp(Q_G G) | G \in \mathbb{G} \setminus \{F\}\} \cup \{exp(F')\}\} \end{aligned}$$

Y por ser todos los exponentes distinitos, se tiene que existe $G \in \mathbb{G} \setminus \{F\}$ tal que $exp(F) = exp(Q_G G)$, lo que es una contradicción con el hecho de ser $\mathbb{G}$ una base de Gröbner minimal. Tenemos entonces que $\mathbb{G}'$ es una base de Gröbner y que F' es reducido. Aplicando este proceso a cada uno de los elementos obtenemos una base de Gröbner reducida.

Para ver la unicidad, si $\mathbb{G}$ y $\mathbb{G}'$ son dos bases de Gröbner reducidas, se verifica:

$$Exp(I) = exp(\mathbb{G}) + \mathbb{N}^n = exp(\mathbb{G}') + \mathbb{N}^n.$$

Dado $F \in \mathbb{G}$, tenemos las relaciones siguientes:

$$\begin{array}{l} exp(F) = exp(G') + \gamma, \quad G' \in \mathbb{G}', \quad \gamma \in \mathbb{N}^n \\ exp(G') = exp(G) + \gamma', \quad G \in \mathbb{G}, \quad \gamma' \in \mathbb{N}^n \end{array}$$

de donde se deduce que $exp(F) = exp(G) + \gamma + \gamma'$, y por ser $\mathbb{G}$ minimal tenemos $\gamma = 0 = \gamma'$. Entonces $exp(F) = exp(G')$ y como consecuencia tenemos la igualdad:

$$exp(\mathbb{G}) = exp(\mathbb{G}').$$

Dado ahora $F \in \mathbb{G}$ existe $G' \in \mathbb{G}'$ tal que $exp(F) = exp(G')$. Entonces $F - G'$ tiene todos sus términos menores que $exp(F)$. Como $F - G' \in I$ tenemos $R(F - G'; \mathbb{G}) = 0$. Como $\mathbb{G}$ y $\mathbb{G}'$ son reducidas y $exp(\mathbb{G}) = exp(\mathbb{G}')$, tenemos

$$\mathcal{N}(F - G') \subseteq \overline{\Delta} = \mathbb{N}^n \setminus Exp(I),$$

Para probar esta inclusión consideraremos el siguiente desarrollo:

$$\begin{array}{ll} & \mathcal{N}(F - G') \cap (exp(\mathbb{G}) + \mathbb{N}^n) = \\ = & \mathcal{N}(F - G') \cap (\cup\{exp(L) + \mathbb{N}^n | l \in \mathbb{G}\}) \\ = & \cup\{\mathcal{N}(F - G') \cap (\cup exp(L) + \mathbb{N}^n) | l \in \mathbb{G}\} \\ = & \cup\{\mathcal{N}(F - G') \cap (\cup exp(L) + \mathbb{N}^n) | F \neq l \in \mathbb{G}\} \\ = & \mathcal{N}(F - G') \cap (\cup\{exp(L) | F \neq l \in \mathbb{G}\} + \mathbb{N}^n) \\ \subseteq & (\mathcal{N}(F) \cap (\{exp(L) | F \neq l \in \mathbb{G}\} + \mathbb{N}^n)) \\ \cup & \mathcal{N}(G') \cap (\{exp(L) | G' \neq l \in \mathbb{G}'\} + \mathbb{N}^n))) = \phi \end{array}$$

Entonces $R(F - G'; \mathbb{G}) = F - G'$, de donde $F = G'$.

Actualmente hay varios programas computacionales que calculan bases de Gröbner, por ejemplo Mathematica, Maxima, Maple, de esta forma podemos obtener bases de Gröbner en menos tiempo y con mayor precisión. En el Apéndice aparecen algunas de las órdenes utilizadas para trabajar con bases de Gröbner. En el ejemplo (3.13) se puede observar como calcular una base de Gröbner reducida dada una lista de polinomios.

Capítulo 3

APLICACIONES DE LAS BASES DE GRÖBNER

Vamos a estudiar algunas aplicaciones de la teoría de bases de Gröbner hasta ahora desarrollada. Los cálculos de las bases de Gröbner en los ejemplos, se han hecho usando el Software Mathematica 8.

Problema de pertenencia

Sea I un ideal izquierda de $K[X_1, \ldots, X_n]$ con un sistema de generadores $\{F_1, \ldots, F_r\}$; dado $F \in K[X_1, \ldots, X_n]$, nos planteamos el problema de determinar si $F \in I$. Para esto se calcula una base Gröbner $\mathbb{G} = \{G_1, \ldots, G_t\}$ de I; entonces tenemos $F \in I$ si, y sólo si, $R(F; \mathbb{G}) = 0$.

Representantes canónicos

Dado un ideal I daremos un criterio y un método, para determinar un representante canónico en cada clase del cociente $K[X_1, \ldots, X_n]/I$.

En primer lugar, dado I, construimos una base de Gröbner $\mathbb{G}$ de I. Para cada

$$F \in K[X_1, \ldots, X_n]$$

consideramos el resto $R(F; \mathbb{G})$ y es claro que se verifica:

$$F + I = R(F; \mathbb{G}) + I.$$

Además, $R(F; \mathbb{G})$ es único verificando la igualdad anterior y $\mathcal{N}(R(F; \mathbb{G})) \subseteq \overline{\Delta} = \mathbb{N}^n \setminus Exp(I)$. Este elemento $R(F; \mathbb{G})$ lo llamamos la forma normal de la clase de F con respecto a $\mathbb{G}$.

Ideales cofinitos

Pasamos ahora a estudiar el caso de ideales cofinitos, esto es, ideales I de $K[X_1, \ldots, X_n]$ tales que el cociente $K[X_1, \ldots, X_n]/I$ es de dimensión finita como K–espacio vectorial. Se trata de dar un método que permita calcular una base del cociente $K[X_1, \ldots, X_n]/I$.

Para cada clase $F + I$ de $K[X_1, \ldots, X_n]/I$ considerando una base de Gröbner de I, tenemos un representante R de la clase $F + I$ tal que $\mathcal{N}(R) \subseteq \mathbb{N}^n \setminus Exp(I)$. De aquí resulta que R se puede escribir en la forma

$$R = \sum_{\alpha} c_\alpha X^\alpha,$$

con $\alpha \notin \{exp(G) : G \in \mathbb{G}\} + \mathbb{N}^n = Exp(I)$ y $c_\alpha \in K$.. Tenemos entonces que $\{X^\beta | \beta \in \mathbb{N}^n \setminus Exp(I)\}$ es un sistema de generadores linealmente independiente de $K[X_1, \ldots, X_n]/I$.

Como subproducto podemos determinar cuándo un ideal a la izquierda es cofinito; lo es si, y sólo si, el cardinal del conjunto $\mathbb{N}^n \setminus Exp(I)$ es finito.

Proposición 3.1. *Sea I un ideal a la izquierda de $K[X_1, \ldots, X_n]$ con base de Gröbner reducida $\mathbb{G}$. Son equivalentes los siguientes enunciados:*

i. I es cofinito;

ii. Para cada indeterminada X_i existen $G_j \in \mathbb{G}$ y $\nu_i \in \mathbb{N}$ tales que $lm(G_j) = X_i^{\nu_i}$

Demostración. ($\Rightarrow$) Como I es cofinito, dado X_i existe $\nu_i \in N$ tal que $X_i^{\nu_i}$ es el término líder de un polinomio en I, entonces $(0, \ldots, \nu_i, \ldots, 0) \in Exp(I) = exp(\mathbb{G}) + N^n$. Llamemos $\alpha(j) = exp(G_j)$ para cada $G_j \in \mathbb{G}$. Existen $j \in \{1, \ldots, t\}$ y $\gamma \in \mathbb{N}^n$ tales que

$$(0, \ldots, \nu_i, \ldots, 0) = \alpha(j) + \gamma,$$

entonces $\alpha_h(j) = 0 = \gamma_h$ si $h \neq i$. Luego $exp(G_j) = (0, \ldots, \mu_i, \ldots, 0)$ para algún $\mu_i \in \mathbb{N}$, esto es, $lm(G_j) = X_i^m$ para algún $m \in \mathbb{N}$.

($\Leftarrow$) Consideramos $\alpha \in \mathbb{N}^n \setminus Exp(I)$. Por hipótesis, para cada X_i existe G_j tal que $lt(G_j) = X_i^{\nu_i}$. Si $\alpha_i \geq \nu_i$, entonces tenemos una expresión del siguiente tipo:

$$\alpha = (0, \ldots, \nu_i, \ldots, 0) + (\alpha_1, \ldots, \alpha_i - \nu_i, \ldots, \alpha_n) \in exp(G_j) + \mathbb{N}^n \subseteq Exp(I),$$

lo que es una contradicción, y por tanto necesariamente $\alpha_i < \nu_i$, para cada índice i. En consecuencia existe un número finito de elementos $\alpha \in \mathbb{N}^n \setminus Exp(I)$ y por tanto I es cofinito.

Eliminación de variables

Teorema 3.2. *Sea $\mathbb{G} = \{G_1, \ldots, G_t\}$ una base de Gröbner de un ideal no nulo $I \subseteq K[X_1, \ldots, X_n]$ con respecto al orden lexicográfico con $X_1 > \cdots > X_n$. Entonces $\mathbb{G} \cap K[X_{i+1}, \ldots, X_n]$ es una base de Gröbner del i–**ésimo ideal de eliminación** $I_i = I \cap K[X_{i+1}, \ldots, X_n]$.*

Demostración. Supongamos que $\mathbb{G}_i = \{G_k, \ldots, G_t\}$. Dado $F \in I_i$ se tiene $exp(F) \in \Delta(j)$ para algún $j = k, \ldots, t$, ya que F no tiene monomios en los que aparezcan $X_1, \ldots, X_i$. Por lo tanto $exp(F) \in \{exp(G_k), \ldots, exp(G_t)\} + \mathbb{N}^n$, y se tiene $Exp(I_i) = \{exp(G_k), \ldots, exp(G_t)\} + \mathbb{N}^n$.

La aplicación de este resultado es como sigue. Dado un sistema $F_j = 0\}_{j=1,\ldots,s}$ en el que $\mathbb{G} := \{F_j | j = 1, \ldots, s\}$ es una base de Gröbner, ordenamos los elementos de $\mathbb{G}$ de forma que $\mathbb{G}_i = \{F_{k_i}, F_{k_i+1}, \ldots, F_s\}$ con $1 \leq k_i \leq k_{i+i} \leq s$, para cada índice $i = 0, 1, \ldots, n-1$. Entonces comenzamos resolviendo el sistema $F_j = 0\}_{j=k_{n-1},\ldots,s}$. A continuación, con los valores obtenidos resolvemos el sistema $F_j = 0\}_{j=k_{n-2},\ldots,s}$, y así proseguimos hasta resolver el sistema inicial $F_j = 0\}_{j=1,\ldots,t}$.

Intersección de Ideales

Dados dos ideales A y B del anillo $K[X_1, \ldots, X_n]$, se trata de determinar la intersección $A \cap B$. Vamos a hacer uso de la técnica de eliminación de variables, para esto introducimos una nueva variable T, y consideramos la extensión de anillos

$$\omega : K[X_1, \ldots, X_n] \longrightarrow K[T, X_1, \ldots, X_n].$$

El ideal A se extiende al ideal A^e en $K[T, X_1, \ldots, X_n]$ generado por los mismos elementos, esto es, si $A = \langle F_1, \ldots, F_s \rangle$, entonces $A^e = K[T, X_1, \ldots, X_n]A = \langle F_1, \ldots, F_s \rangle$ en $K[T, X_1, \ldots, X_n]$. De forma análoga tenemos para $B = \langle G_1, \ldots, G_t \rangle$.

Teorema 3.3. *Sean $A = \langle F_1, \ldots, F_s \rangle$ y $B = \langle G_1, \ldots, G_t \rangle$, ideales de $K[X_1, \ldots, X_n]$. Se considera una nueva variable T, la extensión $\omega : K[X_1, \ldots, X_n] \longrightarrow K[T, X_1, \ldots, X_n]$ y el ideal $C := TA^e + (1-T)B^e \subseteq K[T, X_1, \ldots, X_n]$. Se verifica*

$$A \cap B = C \cap K[X_1, \ldots, X_n],$$

esto es, $A \cap B$ es el primer ideal eliminación de C con respecto al orden lexicográfico con $T > X_1 > \cdots > X_n$

Demostración. Dado $F \in A \cap B$ se tiene $F = TF + (1-T)F$, luego $A \cap B \subseteq C \cap K[X_1, \ldots, X_n]$.

Sea ahora $F \in C \cap K[X_1, \ldots, X_n]$, existen $U_i, V_j \in K[T, X_1, \ldots, X_n]$ tales que

$$F = T \sum_{i=1}^{s} U_i F_i + (1-T) \sum_{j=1}^{t} V_j G_j.$$

Al evaluar esta expresión en $T = 1$ se obtiene

$$F = \sum_{i=1}^{s} U_i(1, X_1, \ldots, X_n) F_i(X_1, \ldots, X_n) \in A,$$

Al evaluar $T = 0$ se tiene

$$F = \sum_{j=1}^{t} V_j(1, X_1, \ldots, X_n) G_j(X_1, \ldots, X_n) \in B,$$

Luego $F \in A \cap B$.

Ejemplo 3.1. *Determina la intersección de los ideales $A = (X, Y)$ y $B = (X-1, Y-1)$ en $K[X, Y]$.*

Solución. Introducimos una nueva variable T. Un sistema de generadores para $TA + (1-T)B$ es $\{TX, TY, (1-T)(X-1), (1-T)(Y-1)\}$. Una pequeña manipulación nos conduce al sistema de generadores: $\{TX, TY, T + X - 1, X - Y\}$. A partir de aquí una base de Gröbner es: $\{TX, TY, T + X - 1, X - Y, Y^2 - Y\}$, y una base de Gröbner reducida es: $\{TX, TY, T + Y - 1, X - Y, Y^2 - Y\}$.
El primer ideal de eliminación tiene como base de Gröbner $\{X - Y, Y^2 - Y\}$. Por lo tanto $A \cap B = (X - Y, Y^2 - Y)$.

En el Elemplo (3.15) de Apéndice se implementa un algoritmo para la intersección de ideales en Mathematica.

3.1. Interpolación con Bases de Gröbner

3.1.1. Método de Interpolación de Lagrange

Dado un conjunto de puntos distintos $x_1, \ldots, x_t \in K^n$ deseamos determinar un polinomio $F \in K[X_1, \ldots, X_n]$ tal que $F(x_1), \ldots, F(x_t)$ tomen unos valores determinados $v_1, \ldots, v_t \in K$. Esto es, el problema que se plantea es: dados $x_1, \ldots, x_t \in K^n$, distintos, y $v_1, \ldots, v_t \in K$, determinar todos los polinomios $F \in K[X_1, \ldots, X_n]$ tales que $F(x_i) = v_i$ para cada $i = 1, \ldots, t$.

Una forma de determinar estos polinomios F es considerar primero el problema homogéneo, esto es, el conjunto de polinomios

$$I = F \in K[X_1, \ldots, X_n] | F(p_i) = 0; i = 1, \ldots, t.$$

De esta forma tenemos un ideal I que es cofinito en $K[X_1, \ldots, X_n]$.

Observa que los polinomios F que son solución al problema de interpolación forman una clase módulo I, y que, por lo tanto, la solución al problema de interpolación es única módulo I.

Se sabe que si $\mathbb{G}$ es una base de Gröbner del ideal I, cada clase módulo I tiene un único representante de la forma $\sum_{\alpha \in \mathbb{N}^n \setminus Exp(\mathbb{G})} c_\alpha X^\alpha$

Para determinar una solución F basta considerar un elemento genérico $\sum_{\alpha \in \mathbb{N}^n \setminus Exp(\mathbb{G})} a_\alpha X^\alpha$ e imponer las condiciones iniciales, esto es:

$$\sum_{\alpha \in \mathbb{N}^n \setminus Exp(\mathbb{G})} a_\alpha x_i^\alpha = \nu_i.$$

para $i = 1, \ldots, t$. Éste es un sistema de ecuaciones lineales en las indeterminadas $\{a_\alpha | \alpha \in \mathbb{N}^n \setminus Exp(\mathbb{G})\}$, y cada solución de este sistema proporciona una solución al problema de la interpolación.

Interpolación univariante

Consideremos el caso de un polinomio en $K[X]$, determinar $F \in K[X]$ tal que $F(x_i) = y_i$, $i = 1, 2, 3$ con $x_i \neq x_j$ si $i \neq j$

Si $F(x_i) = 0$ tenemos que

$$\begin{array}{lcll} F(x_1) = 0 & \Leftrightarrow & x - x_1 | F & \Leftrightarrow \quad F \in \langle x - x_1 \rangle \\ F(x_2) = 0 & \Leftrightarrow & x - x_2 | F & \Leftrightarrow \quad F \in \langle x - x_2 \rangle \\ F(x_3) = 0 & \Leftrightarrow & x - x_3 | F & \Leftrightarrow \quad F \in \langle x - x_3 \rangle \end{array}$$

Luego $F \in I = \langle X - x_1 \rangle \cap \langle X - x_2 \rangle \cap \langle X - x_3 \rangle$. Si $\mathbb{G}$ es una base de Gröbner del ideal I, $\mathbb{G} = \{(X - x_1)(X - x_2)(X - x_3)\}$ por lo que el conjunto cociente $K[X]/I$ esta formado por lo polinomios de grado 2, como el conjunto $\mathcal{B} = \mathbb{N} \setminus Exp(\mathbb{G})$ es de dimensión finita entonces $K[X]/I$ también lo es, esto es,

$$K[X]/I = \{a_0 + a_1 X + a_2 X^2 | a_0, a_1, a_2 \in K\},$$

lo que implica que I es un ideal cofinito.

Supongamos F_1 y F_2 soluciones al problema de interpolación, entonces

$$(F_1 - F_2)(x_i) = F_1(x_i) - F_2(x_i) = y_i - y_i = 0 \Rightarrow F_1 - F_2 \in I.$$

Para determinar un polinomio solución basta con tomar $F + I = \sum_{\beta \in \mathcal{B}} a_\beta X^\beta + I$, una clase de equivalencia modulo I y resolver el sistema

$$\left.\begin{array}{rcl} a_0 + a_1 x_1 + a_2 x_1 & = & y_1 \\ a_0 + a_1 x_2 + a_2 x_2 & = & y_2 \\ a_0 + a_1 x_3 + a_2 x_3 & = & y_3 \end{array}\right\}$$

Interpolación multivariante

Ahora consideremos determinar $F \in K[X,Y]$ tal que $F(x_i, y_i) = z_i$, $i = 1,2,3$ con $(x_i, y_i) \neq (x_j, y_j)$ si $i \neq j$
Determinamos $F[X,Y]$ tal que $F(x_i, y_i) = 0$. Observemos que $F(x_i, y_i) = 0 \Rightarrow F \in \langle X - x_i, Y - y_i \rangle$ ya que si dividimos F por $Y - y_i$ implica que $F = (Y - y_i)Q + R$, $R, Q \in K[X,Y]$ y $exp(R) < 1$ entonces $R \in K[X]$ luego el que $F(x_i, y_i) = 0$ implica

$$F = (Y - y_i)Q(x_i, y_i) + R(x_i) = 0 \Rightarrow R(x_i) = 0 \Rightarrow X - x_i | R$$

de forma que

$$F = (Y - y_i)Q(x_i, y_i) + (X - x_i)R' = 0$$

por tanto $F \in \langle X - x_i, Y - y_i \rangle$ y $F \in I = \bigcap_{i=1}^{3} \langle X - x_i, Y - y_i \rangle$

Determinamos $\mathcal{B} = \mathbb{N}^2 \setminus Exp(\mathbb{G})$, siendo $\mathbb{G}$ una base de Gröbner de I y resolvemos el sistema en los a_β siguiente $\sum_{\beta \in \mathcal{B}} a_\beta x_i^\beta = v_i$, $i = 1,2,3$.

Ejemplo 3.2. *Dados los puntos $p_1 = (0,5,0)$, $p_2 = (1,5,3)$ y $p_3 = (-1,5,-1)$ determinar un polinomio $F \in \mathbb{R}[X,Y,Z]$ tal que $F(p_1) = 2, F(p_2) = 1, F(p_3) = 0$.*

Solución. Tenemos que

$$I = \langle X, Y - 5, Z \rangle \cap \langle X - 1, Y - 5, Z - 3 \rangle \cap \langle X + 1, Y - 5, Z + 1 \rangle.$$

Una base de Gröbner para I es $\mathbb{G} = \{-3Z - 2Z^2 + Z^3, -5 + Y, 6X - 5Z + Z^2\}$, luego $\mathbb{N}^3 \setminus Exp(I) = \{(0,0,0), (0,0,1), (1,0,0)\}$. Entonces el polinomio interpolador será de la forma

$$\sum_{\beta \in \mathbb{N}^3 \setminus Exp(I)} a_\beta X^\beta = a_{(0,0,0)} + a_{(0,0,1)} Z + a_{(0,0,2)} Z^2.$$

Lo que resta es determinar las incógnitas a_β planteando el siguiente sistema de ecuaciones lineales con los puntos dados $p_1 = (0,5,0)$, $p_2 = (1,5,3)$ y $p_3 = (-1,5,-1)$.

$$\begin{array}{ll} a_{(0,0,0)} + 0a_{(0,0,1)} + 0a_{(0,0,2)} = 2 & p_1 = (0,5,0) \\ a_{(0,0,0)} + 3a_{(0,0,1)} + 9a_{(0,0,2)} = 1 & p_1 = (1,5,3) \\ a_{(0,0,0)} - 1a_{(0,0,1)} + 1a_{(0,0,2)} = 0 & p_1 = (-1,5,-1) \end{array}$$

Al resolver el sistema se obtiene $a_{(0,0,0)} = 2$, $a_{(0,0,2)} = 17/12$ y $a_{(0,0,0)} = -7/12$, de manera que el polinomio interpolador es

$$F(X,Y,Z) = 2 + \frac{17}{12}Z - \frac{7}{12}Z^2.$$

Si se hubiera utilizado el orden graduado lexicográfico, el resultado sería $\mathbb{G} = \{-5 + Y, 6X - 5Z + Z^2, 3X - 2Z + XZ, 2X + X^2 - Z\}$ y $\mathbb{N}^3 \backslash Exp(I) = \{(0,0,0),(0,0,1),(0,0,2)\}$ El sistema a resolver sería:

$$\begin{array}{ll} a_{(0,0,0)} + 0a_{(0,0,1)} + 0a_{(1,0,0)} = 2 & p_1 = (0,5,0) \\ a_{(0,0,0)} + 3a_{(0,0,1)} + 1a_{(1,0,0)} = 1 & p_1 = (1,5,3) \\ a_{(0,0,0)} - 1a_{(0,0,1)} - 1a_{(1,0,0)} = 0 & p_1 = (-1,5,-1) \end{array}$$

Luego $a_{(0,0,0)} = 2$, $a_{(0,0,1)} = -3/2$ y $a_{(1,0,0)} = -7/2$, por lo que el polinomio interpolador en este caso sería

$$F(X,Y,Z) = 2 - \frac{3}{2}Z + \frac{7}{2}X.$$

En los problemas de interpolación por medio de bases de Gröbner el orden monomial utilizado es importante, pues permite obtener polinomios de interpolación con unas u otras características. Por ejemplo, un orden lexicográfico producirá polinomios en los que algunas indeterminadas tendrán grados relativamente altos y un orden graduado producirá polinomios en los que los grados de las distintas indeterminadas son semejantes. Esto se debe a que el conjunto $\alpha \in \mathbb{N}^n \setminus Exp(\mathbb{G})$ depende del orden monomial seleccionado.

A veces nos encontramos con curvas como la que aparece en la figura (3.1).

En este caso para x_0 tenemos dos valores de y, y si además agregamos información sobre las derivadas en los puntos, los métodos de interpolación no son eficientes para estas curvas. Por esto es conveniente considerar una parametrización de la curva, dada por funciones $x = x(t)$ y $y = y(t)$ y determinar cada una de ellas independientemente por los métodos de interpolación clásicos.
Este mismo problema se plantea en el caso multivariado al considerar superficies u otros conjuntos algebraicos.
Una vez determinados los polinomios de interpolación para cada una de las funciones coordenadas utilizamos la teoría de eliminación de variables con bases de Gröbner para eliminar los parámetros utilizados y obtener funciones implícitas para los conjuntos algebraicos.

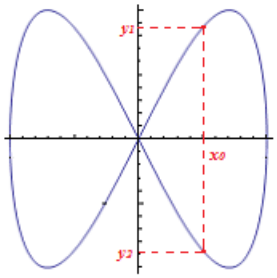


Figura 3.1: Curva $(sin(t), sin(2t)),\ \ 0 \leq t \leq 2\pi$

Es importante observar que si tenemos un conjunto finito de puntos en $\mathbb{R}^2$ o en $\mathbb{R}^3$ con coordenadas $p_i = (x_i, y_i) \in \mathbb{R}^2$ o $q_i = (x_i, y_i, z_i) \in \mathbb{R}^3$, $i = 1, \ldots, s$ y queremos determinar un polinomio F tal que $F(p_i) = z_i$ para todo i, en el primer caso, o un polinomio G tal que $G(q_i) = 0$, podemos hacerlo de dos maneras:

i. Calculando una base de Gröbner del ideal generado por los puntos q_i tal y como se describió en esta sección, ó

ii. Calculando un polinomio interpolación en dos variables; para este caso es aconsejable abordar el problema mediante el uso de una parametrización para poder abordar el problema con total generalidad.

Esta última aproximación limita el tipo de polinomios interpolación, pero es más efectiva, mientras que la primera requiere el uso de más indeterminadas, lo cual es un problema si consideramos valores superiores a 2 y 3.

Veamos una aplicación estándar.

Ejemplo 3.3. *Considere la esfera de radio uno en* $\mathbb{R}^3$ *y una parametrización de la esfera, con* $0 \leq \alpha \leq 2\pi$ *y* $0 \leq \beta \leq 2\pi$. *Véase la figura* (3.2)*:*

Es claro que nosotros trabajamos con polinomios, por esta razón habría que reescribir esta parametrización
Sea $A = sen\alpha$, $B = cos\alpha$, $C = sen\beta$, $D = cos\beta$ entonces tenemos

$$\begin{aligned} x &= BD \\ y &= AD \\ z &= C \\ 1 &= A^2 + B^2 \\ 1 &= C^2 + D^2 \end{aligned}$$

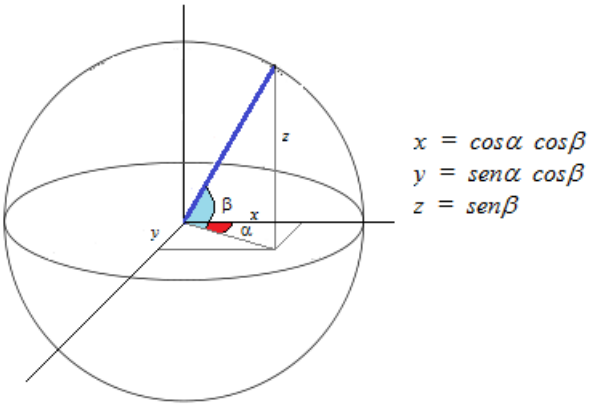


Figura 3.2: Esfera de radio 1

Aplicando teoría de eliminación determinamos una base de Gröbner de esta paramerización elimando las variables A, B, C y D, para obtener la forma implícita de la esfera.

Obtenemos una base de Grobner de $I = \langle X-BD, Y-AD, Z-C, A^2+B^2-1, C^2+D^2-1\rangle$ eliminado las variables y $\mathbb{G} = \{-1 + X^2 + Y^2 + Z^2\}$, que es la forma implícita de la esfera de radio uno en $\mathbb{R}^3$

Al obtener la base de Gröbner eliminando variables encontramos la mínima curva o superficie que contiene la parametrización dada. Veamos un ejemplo.

Ejemplo 3.4. *Dados los puntos* $p_1 = (1, 2)$, $p_2 = (0, 1)$, $p_3 = (0, 4)$ *y* $p_4 = (-1, 3)$ *determinar un polinomio* $F(X, Y)$ *tal que para cada punto* p_i *se tiene* $F(p_i) = 0$.

Por como está definido el problema, vemos que para resolverlo podemos hacerlo usando los casos antes mencionados.
Si calculamos una base de Gröbner para el ideal generado por los puntos obtenemos

$$G = \{2Y^3 - 15Y^2 + 33Y - 2X - 20, Y^4 - 10Y^3 + 35Y^2 - 50Y + 24\}$$

Calculando una combinación lineal de los dos generadores obtenemos un polinomio que interpole los puntos,

$$F(X, Y) = Y^4 - 8Y^3 + 20Y^2 + (-17)Y + (-2)X + 4$$

Por otro lado si parametrizamos los puntos de tal forma que cada punto p_i sea representado por $p_i = (x(t), y(t))$; $t \in [a, b]$; obtenemos

$$x(t) = \frac{-8}{3}t^3 + 6t^2 - \frac{13}{3}t + 1.$$
$$y(t) = \frac{-32}{3}t^3 + 24t^2 - \frac{34}{3}t + 2.$$

Con $0 \leq t \leq 3/2$. Para determinar el polinomio F tal que $F(x_i, y_i) = 0$ necesitamos una base de Gröbner de

$$I = (X + \frac{8}{3}t^3 - 6t^2 + \frac{13}{3}t - 1, Y + \frac{32}{3}t^3 - 24t^2 + \frac{34}{3}t - 2)$$

eliminando la variable t y obtenemos la base de Gröbner

$$\mathbb{G} = \{20 - 30X + 240X^2 + 128X^3 - 33Y - 120XY - 96X^2Y + 15Y^2 + 24XY^2 - 2Y^3\}.$$

De forma que $F(X, Y) = 20 - 30X + 240X^2 + 128X^3 - 33Y - 120XY - 96X^2Y + 15Y^2 + 24XY^2 - 2Y^3$. Este polinomio es la mínima curva que contiene a los puntos dados. Ver figura (3.3).

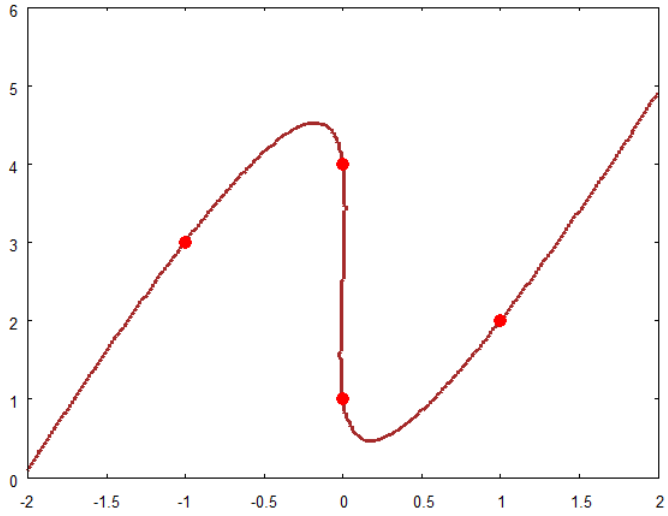


Figura 3.3: Gráfica de F(X,Y)

Veamos ahora un ejemplo de superficie.

Ejemplo 3.5. *Dados los puntos* $p_1 = (0, 1, 1)$, $p_2 = (2, -1, 0)$, $p_3 = (2, 3, 2)$ *y* $p_4 = (2, -1, 4)$, *determinar un polinomio* $F(X, Y, Z)$ *tal que para cada punto* p_i *se tiene* $F(p_i) = 0$.

Si calculamos una base de Gröbner para el ideal generado por lo puntos obtenemos

$$G = \{Z^3 - 3Z^2 - 4Z + 3Y + 3, Z^4 - 7Z^3 + 14Z^2 - 8Z, -2Z^3 + 12Z^2 - 16Z - 3X + 6\}$$

y un polinomio que interpole los puntos puede ser. Véase figura 3.4.

$$F(X, Y, Z) = Z^4 - 8Z^3 + 23Z^2 - 28Z + 3Y - 3X + 9$$

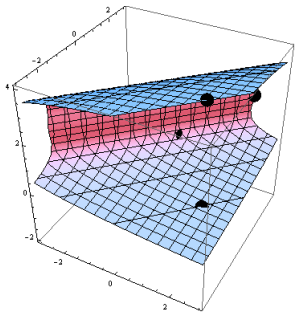


Figura 3.4: Gráfica de F(X,Y)

Si determinamos una parametrización en dos variables t y s, con $0 \leq t \leq 3/2$ y $0 \leq s \leq 1$ usando un orden graduado lexicográfico obtenemos lo siguiente:

$$\begin{aligned} x(t,s) &= 36s - 16s^2 - 12t. \\ y(t,s) &= 1 - 140s + 48s^2 + 60t. \\ z(t,s) &= 1 - 54s + 24s^2 + 22t. \end{aligned}$$

Determinamos una base de Gröbner para

$$\{X - 36s + 16s^2 + 12t, Y - 1 + 140s - 48s^2 - 60t, Z - 1 + 54s - 24s^2 - 22t\},$$

y eliminando las variables t y s obtenemos

$$F(X,Y,Z) = 193 - 140X + 36X^2 + 82Y - 12XY + Y^2 - 300Z + 72XZ - 12YZ + 36Z^2.$$

Véase figura 3.5.

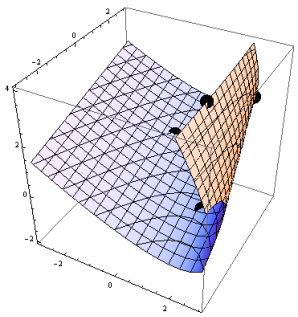


Figura 3.5: Gráfica de F(X,Y)

3.1.2. Interpolación de Hermite

Si complementamos el método de interpolación de Lagrange mediante el uso de valores para las derivadas, se tiene el método de interpolación de Hermite. Se trata en este caso de determinar un polinomio $F \in K[X_1, \ldots, X_n]$ tal que en un conjunto finito de puntos $x_1, \ldots, x_t$ (distintos) tomen valores dados v_i, y para vectores unitarios w_{i,j_i} se tenga $D^{(h)}_{w_{i,j_i}} F(x_i) = v_{i,j_i,h}$ para $i = 1, \ldots, t$, $j_i = 1, \ldots, s(i)$, $h = 1, \ldots, s(i, j_i)$. En este caso $D^{(h)}_{w_{i,j_i}} F(x_i) = v_{i,j_i,h}$ es el valor de la derivada h–ésima de F según la dirección indicada por w_{i,j_i}.

Con la notación anterior el conjunto

$$I = \{F \in K[X_1, \ldots, X_n] | F(x_i) = 0 \text{ y } D^{(h)}_{w_{i,j_i}} F(x_i) = 0, \forall i, j_i, h\}$$

es un ideal cofinito.
De forma análoga al método de interpolación de Lagrange, dada una base de Groebner $\mathbb{G}$ de I, el cociente $K[X_1, \ldots, X_n]/I$ es un espacio vectorial de dimensión finita, y cada solución al problema de interpolación de Hermite está unívocamente determinada módulo I.

Dada una base de Groebner $\mathbb{G}$ de I, cada clase módulo I tiene un único representante de la forma $\sum_{\alpha \in \mathbb{N}^n \setminus Exp(\mathbb{G})} a_\alpha X^\alpha$. Para determinar una solución basta considerar el sistema de ecuaciones lineales

$$\begin{array}{c} \sum_{\alpha \in \mathbb{N}^n \setminus Exp(\mathbb{G})} a_\alpha X^\alpha = v_i \\ D^{(h)}_{w_{i,j_i}} \sum_{\alpha \in \mathbb{N}^n \setminus Exp(\mathbb{G})} a_\alpha X^\alpha = v_{i,j_i,h} \end{array}$$

para todos i, j_i, h.

La solución al problema de interpolación de Hermite es única módulo I.

Ejemplo 3.6. *Determine un polinomio $F(T, S)$ tal que cumpla con las siguientes condiciones:*

$$\begin{array}{ll} F(0,0) = 1 & D_{(1,0)} F(0,0) = 2 \\ F(0,1) = -1 & D_{(0,1)} F(0,0) = -2 \\ F(1,0) = 10 & D^2_{(1,0)} F(0,0) = 6 \\ F(1,1) = 7 & D_{(1,0)} F(0,1) = -1 \\ & D_{(0,1)} F(0,1) = -3 \end{array}$$

Solución. Tenemos que

$$\begin{array}{rl} F \in I & = \langle T, S \rangle \cap \langle T, S-1 \rangle \cap \langle T-1, S \rangle \cap \langle T-1, S-1 \rangle \\ & \cap \langle T^2, S \rangle \cap \langle T, S^2 \rangle \cap \langle T^3, S \rangle \cap \langle T^2, S-1 \rangle \cap \langle T, (S-1)^2 \rangle. \end{array}$$

Una base de Gröbner para I es $\{ST - S^2T, S^4 - 2S^3 + S^2, T^4 - T^3, ST^3 - ST^2\}$.
Luego $\mathbb{N}^2 \setminus Exp(I) = \{(0,0), (1,0), (2,0), (3,0), (0,1), (0,2), (0,3), (1,1), (2,1)\}$

Por lo que $F = a_{(0,0)} + a_{(1,0)}T + a_{(2,0)}T^2 + a_{(3,0)}T^3 + a_{(0,1)}S + a_{(0,2)}S^2 + a_{(0,3)}S^3 + a_{(1,1)}ST + a_{(2,1)}T^2S$. Planteamos el sistema de ecuaciones correspondientes conforme los valores de la función y sus derivadas en cada punto. De manera que se obtiene el polinomio

$$F(T,S) = 4T^3 + 3T^2 + 2S^2T - 3ST + 2T - 3S^3 + 3S^2 - 2S + 1.$$

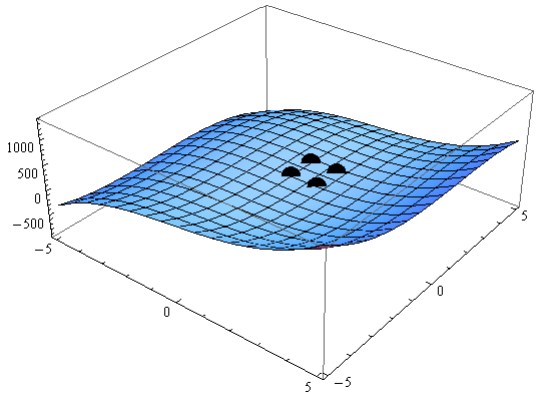


Figura 3.6: Gráfica de F(T,S)

Ahora vamos a retomar el caso mostrado en la figura 3.1, donde puntos como (x_0, y_1) y (x_0, y_2) pertenecen a la misma y además se proporciona valores de la derivada en ellos. Para esto es preciso recordar algunas cuestiones de derivación paramétrica. Algunas curvas pueden ser dadas en forma paramétrica como

$$\begin{aligned} x &= x(t), \\ y &= y(t), \end{aligned}$$

y se quiere determinar

$$\frac{dy}{dx}.$$

Suponga que $x = x(t)$ y $y = y(t)$ son funciones continuamente diferenciables, y que $x'(t) \neq 0$ para cualquier t de cierto intervalo. Entonces las ecuaciones paramétricas definen a y como una función diferenciable de x y su derivada es:

$$\frac{dy}{dx} = \frac{dy}{dt}\frac{dt}{dx} = \frac{\frac{dy}{dt}}{\frac{dx}{dt}}.$$

Veamos el ejemplo

Ejemplo 3.7. *Dados los puntos* $p_1 = (1, 0)$, $p_2 = (0, 1)$, $p_3 = (-1, 0)$ *y* $p_4 = (0, -1)$, *la derivada en los puntos* p_2 *y* p_4 *es cero en las direcciones* $(-1, 0)$ *y* $(1, 0)$ *respectivamente. Determinar un polinomio* $F(X, Y)$ *tal que para cada punto* p_i *se tiene* $F(p_i) = 0$ *y cumpla con los valores de su primera derivada en cada punto. Note que la curva que se pide no es una función, ya que hay dos puntos diferentes con la misma preimagen. Para esto determinamos una parametrización que contenga los puntos dados incluyendo la información de la derivada.*

$$x(t) = -t - \frac{11t^2}{18} + \frac{2t^3}{9} + \frac{11t^4}{18} - \frac{2t^5}{9}$$
$$y(t) = 1 - \frac{23t^2}{18} + \frac{t^3}{18} + \frac{5t^4}{18} - \frac{t^5}{18}$$

Obtenemos una base de Gröbner del ideal $I = \langle X + t + \frac{11t^2}{18} - \frac{2t^3}{9} - \frac{11t^4}{18} + 2t^5 9, Y - 1 + \frac{23t^2}{18} - \frac{t^3}{18} - \frac{5t^4}{18} + \frac{t^5}{18} \rangle$. *Para encontrar el polinomio que contiene la parametrización eliminamos la varible* t.

$F(X,Y) = 3122 + 26X - 3196X^2 - 28X^3 + 74X^4 + 2X^5 + 1660Y - 6220XY - 8196X^2Y + 508X^3Y - 40X^4Y - 3283Y^2 - 2586XY^2 - 4371X^2Y^2 + 320X^3Y^2 + 388Y^3 + 6220XY^3 - 1280X^2Y^3 + 161Y^4 + 2560XY^4 - 2048Y^5$

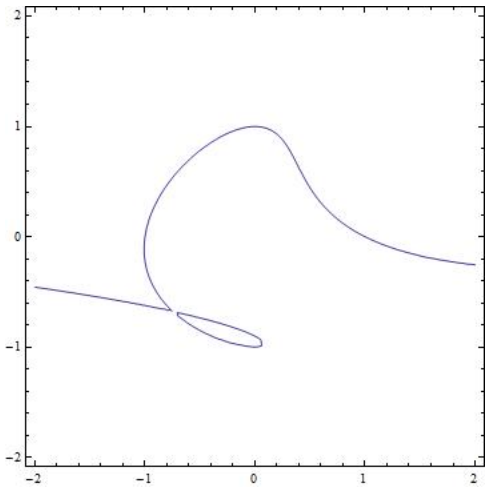


Figura 3.7: Gráfica de F(X,Y)

3.2. Bases de Gröbner y coloreado de grafos

Definición 3.4. *Un **grafo** es un par $G = (V, E)$ formados por dos conjuntos: V el conjunto de **vértices**, y E el conjunto de **lados**. Cada lado $x \in E$ determina un conjunto de vértices $\{v_1, v_2\}$; si el lado no es orientado, el orden de estos vértices es indiferente, y si el lado es orientado, este orden importa, por esto en este caso designaremos los vértices como un par (v_1, v_2), y llamamos a v_1 el origen del lado y a v_2 el fin. Cuando $v_1 = v_2$ decimos que el lado es un lazo.*

Un grafo simple será un grafo con un conjunto finito de vértices, con lados no orientados y sin lazos, y entre cada dos vértices hay a lo más un lado. Así cada lado se puede identificar con el $\{v_1, v_2\}$ de sus vértices; si $x = \{v_1, v_2\}$ es un lado, diremos que x conecta v_1 y v_2, y que v_1, v_1 son adyacentes.

Llamaremos grafo orientado a un grafo con un conjunto finito de vértices en el que todos los lados son orientados y para cada par ordenado (v_1, v_2) existe a lo más un lado con origen v_1 y fin v_1; también en este caso excluiremos a los lazos. En este caso cada lado se puede identificar con el par ordenado (v_1, v_2); si $x = (v_1, v_2)$, diremos que x conecta v_1 con v_2, y llamamos $ori(x) = v_1$ y $fin(x) = v_2$.

Un **camino** en un grafo orientado es una sucesión finita de lados $x_1 \cdots x_t$ en la que $fin(x_i) = ori(x_{i+1})$ para $i = 1, \ldots, t-1$. El extremo inicial del camino es $ori(x_1)$ y el extremo final es $fin(x_t)$. La longitud de un camino es el numero de lados que contiene. Un camino es cerrado si el extremo final coincide con el extremo inicial. Un camino es simple si en la sucesión de vértices $ori(x_1), fin(x_1), ori(x_2), \ldots, fin(x_t)$ no hay ninguno repetido, y un camino cerrado es simple, también llamado un **ciclo**, si los únicos vértices repetidos son $fin(x_t)$ y $ori(x_1)$. Un camino cerrado es un circuito si no repite aristas.

Dado un grafo no orientado un camino es una sucesión de lados $x_1 \cdots x_t$ a los que podemos dar orientación de forma que sean un camino (orientado); los diferentes tipos de caminos se definen en estos grafos de la forma obvia.

El orden n de un grafo $G = (V, E)$ es el número de vértices o el cardinal de V. Asimismo se define el tamaño E de un grafo $G = (V, E)$, como el cardinal de E o el número de aristas de G.

De aquí en adelante nos referiremos a grafos simples a menos que se especifique lo contrario.

3.2.1. Coloreado de Grafos

Dado un grafo $G = (V, E)$, una coloración de G consiste en asignar un color a cada vértice de forma que dos vértices, entre los que existe un lado, tienen colores distintos.

Observa que una coloración es una aplicación $c : V \to C$ del conjunto de vértices V al conjunto de colores C, que verifica ciertas condiciones; si $v = \{v_1, v_2\}$ es un lado, entonces $c(v_i) \neq c(v_j)$.

Existe una amplia teoría sobre coloraciones de grafos. Vamos a estudiar un aspecto de la teoría en el que podremos hacer uso de los anillos de polinomios y de las bases de Gröbner.

Supongamos que queremos dar a un grafo G una coloración con d colores, esto es, una d–coloración. Como el conjunto C con d elementos puede ser cualquiera, tomamos $C = \{\xi^i | i = 0, \ldots, d-1\}$, las raíces d–ésimas de la unidad, siendo ξ una raíz d–ésima primitiva. Una coloración será una aplicación $c : V \to C$ verificando la condición anterior.

Supongamos que el conjunto de vértices es $V = \{v_1, \ldots, v_t\}$, y llamamos X_i al valor asignado al vértice v_i; se tiene $X_i^d - 1 = 0$.

Por otro lado para dos vértices v_i, v_j se tiene

$$X_i^d - 1 = X_j^d - 1,$$

esto es: $X_i^d - X_j^d = 0$. desarrollando esta expresión tenemos:

$$0 = X_i^d - X_j^d = (X_i - X_j)(X_i^{d-1} + X_i^{d-2}X_j + \cdots + X_iX_j^{d-2} + X_i^{d-1}).$$

Si $\{v_i, v_j\}$ es un lado del grafo, se tiene $X_i - X_j \neq 0$, y por tanto necesariamente $X_i^{d-1} + X_i^{d-2}X_j + \cdots + X_iX_j^{d-2} + X_i^{d-1} = 0$.

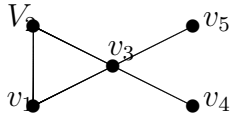
Como consecuencia, si existe una d–coloración c, el siguiente sistema de ecuaciones polinómicas tiene una solución:

$$\begin{cases} X_i^d - 1 = 0, & v_i \in V, \\ X_i^{d-1} + X_i^{d-2}X_j + \cdots + X_iX_j^{d-2} + X_i^{d-1} = 0 & \{v_i, v_j\} \in E. \end{cases}$$

Cada solución de este sistema es una coloración del grafo.

Para futuras aplicaciones, llamamos $I(G, d)$ al ideal generado por los polinomios anteriores, y lo llamaremos el ideal de d–coloración del grafo G. Cada elemento de $V(I(G, d))$ corresponde a una d-coloración.

Ejemplo 3.8. *Veamos el siguiente ejemplo.*



Vamos a colorear con 2 y 3 colores.

caso de dos colores.
Para dos colores tenemos que resolver el sistema:

$$\begin{aligned}
X_1^2 - 1 &= 0\\
X_2^2 - 1 &= 0\\
X_3^2 - 1 &= 0\\
X_4^2 - 1 &= 0\\
X_5^2 - 1 &= 0\\
X_1 + X_2 &= 0\\
X_1 + X_3 &= 0\\
X_2 + X_3 &= 0\\
X_3 + X_4 &= 0\\
X_3 + X_5 &= 0
\end{aligned}$$

Usando Mathematica

```
GröbnerBasis[
{X1^2-1,X2^2-1,X3^2-1,X4^2-1,X5^2-1,X1+X2,X1+X3,X2+X3,X3+X4,X3+X5},
   {X1,X2,X3,X4,X5}]
```

Vemos que la base de Gröbner del ideal generado por estos polinomios es trivial: $\{1\}$. En consecuencia no existe una coloración de este grafo con dos colores. Lo cual, por otro lado es evidente por la existencia del subgrafo completo $\{v_1, v_2, v_3\}$.

caso de dos colores.
Para tres colores tenemos que resolver el sistema:

$$\begin{aligned}
X_1^3 - 1 &= 0\\
X_2^3 - 1 &= 0\\
X_3^3 - 1 &= 0\\
X_4^3 - 1 &= 0\\
X_5^3 - 1 &= 0\\
X_1^2 + X_1X_2 + X_2^2 &= 0\\
X_1^2 + X_1X_3 + X_3^2 &= 0\\
X_2^2 + X_2X_3 + X_3^2 &= 0\\
X_3^2 + X_3X_4 + X_4^2 &= 0\\
X_3^2 + X_3X_5 + X_5^2 &= 0
\end{aligned}$$

```
GröbnerBasis[
{X1^3-1,X2^3-1,X3^3-1,X4^3-1,X5^3-1,X1^2+X1X2+X2^2,
 X1^2+X1 X3+X3^2,X2^2+X2 X3+X3^2,X3^2+X3 X4+X4^2,
 X3^2+X3 X5+X5^2},{X1,X2,X3,X4,X5}]
```

La base de Gröbner del ideal generado por estos polinomios es:

$$\{X_1 + X_2 + X_3, X_2^2 + X_2X_3 - X_3X_5 - X_5^2, X_3^2 + X_3X_5 + X_5^2, \\ X_3X_4 + X_4^2 - X_3X_5 - X_5^2, -1 + X_4^3, -1 + X_5^3\}.$$

Para averiguar cuántas coloraciones distintas existen, tenemos que calcular la co–dimensión de este ideal, esto es, el número de soluciones distintas. En Mathematica usamos la orden:

```
L=Solve[{
-1+X5^3==0,-1+X4^3==0,X3 X4+X4^2-X3 X5-X5^2==0,
    X3^2+X3 X5+X5^2==0,X2^2+X2 X3-X3 X5-X5^2==0,
 X1+X2+X3==0},{X1,X2,X3,X4,X5}]

Length[L]
```

El número de soluciones (3-coloraciones) distintas es 24.

Cuerpos finitos

Anteriormente trabajando en el cuerpo $\mathbb{C}$ hemos utilizamos las raíces de la unidad para colorear un grafo, pero ¿Será posible estudiar la coloración de un grafo en un cuerpo con menos elementos? En efecto, sí. Supongamos que queremos 5–colorear un grafo; vamos a trabajar en el cuerpo $\mathbb{F}_5$.

Sea $G = (V, E)$ un grafo simple, con vértices v_i y lados $\{v_i, v_j\}$ con $i \neq j$. Supongamos que tenemos una 5–coloración de G dada por la aplicación $c : V \to \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. Veamos las condiciones que verifican los elementos $c(v_i) = x_i \in \mathbb{F}_5$. La primera es que $x_i^5 = x_i$, ya que $\mathbb{F}_5 \setminus \{0\}$ es un grupo abeliano de orden 4; para incluir al elemento 0 añadimos un factor X a la relación $X^4 = 1$. Si $e = \{v_1, v_2\}$ es un lado, entonces $c(v_i) \neq c(v_j)$, esto es, $x_i \neq x_j$. Como se tiene $x_i^5 - x_i = 0 = x_j^5 - x_j$, obtenemos

$$x_i^5 - x_j^5 = x_i - x_j.$$

El primer miembro factoriza como $(x_i - x_j)(x_i^4 + x_i^3x_j + x_i^2x_j^2 + x_ix_j^3 - x_j^4)$, como $x_i - x_j \neq 0$, se tiene la relación

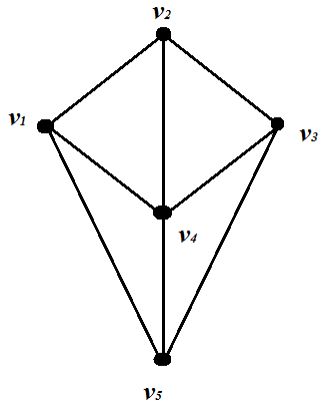
$$x_i^4 + x_i^3x_j + x_i^2x_j^2 + x_ix_j^3 - x_j^4 = 1$$

En resumen, se tienen las relaciones:

$$\begin{array}{ll} x_i^5 - x_i = 0 & v_i \in V \\ x_i^4 + x_i^3x_j + x_i^2x_j^2 + x_ix_j^3 - x_j^4 - 1 = 0 & \{v_i, v_j\} \in E. \end{array}$$

¿Cuál es la ventaja de esta aproximación al estudio de la coloración? La simplicidad de los cálculos a realizar, ya que en este caso trabajamos con los enteros módulo 5 en vez de trabajar con los números complejos.

Ejemplo 3.9. *Considere el siguiente grafo:*



El sistema de ecuaciones para este grafo será:

$$\left.\begin{array}{l} x_1^5 - x_1 = 0 \\ x_2^5 - x_2 = 0 \\ x_3^5 - x_3 = 0 \\ x_4^5 - x_4 = 0 \\ x_5^5 - x_5 = 0 \\ x_1^4 + x_1^3x_2 + x_1^2x_2^2 + x_1x_2^3 - x_2^4 - 1 = 0 \\ x_1^4 + x_1^3x_4 + x_1^2x_4^2 + x_1x_4^3 - x_4^4 - 1 = 0 \\ x_1^5 + x_1^3x_5 + x_1^2x_5^2 + x_1x_5^3 - x_5^4 - 1 = 0 \\ x_2^4 + x_2^3x_3 + x_2^2x_3^2 + x_2x_3^3 - x_3^4 - 1 = 0 \\ x_2^4 + x_2^3x_4 + x_2^2x_4^2 + x_2x_4^3 - x_4^4 - 1 = 0 \\ x_3^4 + x_3^3x_4 + x_3^2x_4^2 + x_3x_4^3 - x_4^4 - 1 = 0 \\ x_3^4 + x_3^3x_5 + x_3^2x_5^2 + x_3x_5^3 - x_5^4 - 1 = 0 \\ x_4^4 + x_4^3x_5 + x_4^2x_5^2 + x_4x_5^3 - x_5^4 - 1 = 0 \end{array}\right\}$$

Calculamos una base de Gröbner módulo 5 para este sistema de ecuaciones y determinamos las soluciones en módulo 5 de forma que el conjunto de colores estará determinado por los valores $\{0, 1, 2, 3, 4\}$.

Utilizando Mathematica hacemos lo siguiente:

```
E1 = Table[X[i]^5 - X[i], {i, 1, 5}];
```

```
Var = Table[X[i], {i, 1, 5}];
                              5-k    k-1
E2[{i_, j_}] := Sum[X[i]   X[j]   , {k, 1, 5}] - 1
Lista = {{1, 2}, {1, 4}, {1, 5}, {2, 3}, {2, 4}, {3, 4}, {3, 5},
        {4,5}};
E20 = Map[E2, Lista];
E22 = Union[E1, E20]
ecuaciones[L_] := Table[L[[i]] == 0, {i, 1, Length[L]}]
E33 = GroebnerBasis[E22, Var, Modulus -> 5]
E34 = ecuaciones[E33]
Solve[E34, {X[1], X[2], X[3], X[4], X[5]}, Modulus -> 5]
```

Si fijáramos un valor para x_2 y x_4 vemos que reduciríamos más los cálculos, por ejemplo tomemos $x_2 = 1$, $x_4 = 0$

```
Solve[E34 /. {X[2] -> 1, X[4] -> 0}, {X[1], X[2], X[3], X[4], X[5]},
 Modulus -> 5]
```

```
{{X[1] -> 2, X[3] -> 2, X[5] -> 1}, {X[1] -> 2, X[3] -> 2, X[5] -> 3},
 {X[1] -> 2, X[3] -> 2, X[5] -> 4}, {X[1] -> 2, X[3] -> 3, X[5] -> 1},
 {X[1] -> 2, X[3] -> 3, X[5] -> 4}, {X[1] -> 2, X[3] -> 4, X[5] -> 1},
 {X[1] -> 2, X[3] -> 4, X[5] -> 3}, {X[1] -> 3, X[3] -> 2, X[5] -> 1},
 {X[1] -> 3, X[3] -> 2, X[5] -> 4}, {X[1] -> 3, X[3] -> 3, X[5] -> 1},
 {X[1] -> 3, X[3] -> 3, X[5] -> 2}, {X[1] -> 3, X[3] -> 3, X[5] -> 4},
 {X[1] -> 3, X[3] -> 4, X[5] -> 1}, {X[1] -> 3, X[3] -> 4, X[5] -> 2},
 {X[1] -> 4, X[3] -> 2, X[5] -> 1}, {X[1] -> 4, X[3] -> 2, X[5] -> 3},
 {X[1] -> 4, X[3] -> 3, X[5] -> 1}, {X[1] -> 4, X[3] -> 3, X[5] -> 2},
 {X[1] -> 4, X[3] -> 4, X[5] -> 1}, {X[1] -> 4, X[3] -> 4, X[5] -> 2},
 {X[1] -> 4, X[3] -> 4, X[5] -> 3}}
```

Vimos anteriormente como colorear un grafo trabajando en un cuerpo con 5 elementos. Sin embargo trabajar la coloración en cuerpos con un número de elementos no primo, implica un poco más de trabajo pero sigue el mismo procedimiento, por ejemplo podríamos considerar $\mathbb{F}_4[X]$ y $\mathbb{F}_9[X]$.

Tenemos un cuerpo $\mathbb{F}_q$ con $q = p^n$ elementos, siendo p un número primo, sabemos que $\mathbb{F}_q = \frac{\mathbb{F}_p[X]}{(F)}$ para un cierto polinomio irreducible $F \in \mathbb{F}_p[X]$ de grado n y que $\mathbb{F}_q[Y]$ es isomorfo a $\mathbb{F}_p[X,Y]/(F)$ para cada indetereminada Y.

Sea $G = (V, E)$ un grafo simple, con vértices $V = \{v_1, \ldots, v_s\}$ y lados E, y $c : V \to \mathbb{F}_q$ una q–coloración de G. Si $e = \{v_1, v_2\}$ es un lado, entonces $c(v_i) \neq c(v_j)$.

Planteamos el siguiente sistema, que debemos resolver en $\mathbb{F}_q$.

$$\begin{array}{ll} x_i^q - x_i = 0 & v_i \in V \\ x_i^{q-1} + x_i^{q-2}x_j + ... + x_i x_j^{q-2} - x_j^{q-1} - 1 = 0 & \{v_i, v_j\} \in E \end{array} \tag{3.1}$$

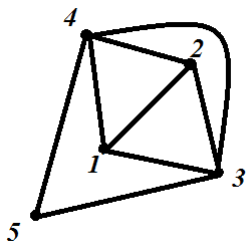
Para ello, calculamos el ideal $I(G,q)$ generado por los polinomios que conforman el sistema en $\mathbb{F}_q[X_1, ..., X_s]$. Trabajar en $\mathbb{F}_q$ es ciertamente complicado, ya que no conocemos con detalle su aritmética. Consideramos entonces la relación

$$\mathbb{F}_p[X_1, \ldots, X_s] \cong \frac{\mathbb{F}_p[X]}{(F)}[X_1, \ldots, X_s] \cong \frac{\mathbb{F}_p[X, X_1, \ldots, X_s]}{(F)},$$

y estudiamos el ideal $I(G,q)$ mediante el ideal correspondiente en $\mathbb{F}_p[X, X_1, \ldots, X_s]$.

En nuestro caso éste ideal de $\mathbb{F}_p[X, X_1, \ldots, X_s]$ es el ideal generado por los polinomio del sistema (3.1) junto con el polinomio F que define $\mathbb{F}_q$.

Ejemplo 3.10. *Considere el grafo de la figura* (3.10)



El estudio de la coloración realizado mediante el programa Mathematica es el siguiente:

```
E1 = Table[X[i]^4 - X[i], {i, 1, 5}]
E2[{i_, j_}] := X[i]^3 + X[i]^2 X[j] + X[i] X[j]^2 + X[j]^3 - 1
Lista = {{1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4}, {3, 4}, {3, 5}, {4,
   5}}
E20 = Map[E2, Lista];
E22 = Union[E1, E20];
Var = Union[Table[X[i], {i, 1, 5}], {X}];
E220 = Union[E22, {X^2 + X + 1}];
E330 = GroebnerBasis[E220, Var];
ecuaciones[L_] := Table[L[[i]] == 0, {i, 1, Length[L]}]
GroebnerBasis[E330 /. {X[5] -> 0}, {X, X[1], X[2], X[3], X[4]},
Modulus -> 2]
```

```
 {1 + X[4]^3, X[3]^2 + X[3] X[4] + X[4]^2,
 X[2]^2 + X[2] X[3] + X[2] X[4], X[1] + X[2] + X[3] + X[4],
 1 + X + X^2}

GroebnerBasis[E330 /. {X[4] -> 1, X[5] -> 0}, {X, X[1], X[2], X[3]},
Modulus -> 2]

 {1 + X[3] + X[3]^2, X[2] + X[2]^2 + X[2] X[3], 1 + X[1] + X[2] + X[3],
  1 + X + X^2}

RR[F_] := PolynomialRemainder[F, x^2 + x + 1, x]
Map[RR, E330 /. {X[3] -> x, X[4] -> 1, X[5] -> 0}]

  {0, 0, 0, X[2] + x X[2] + X[2]^2, 1 + x + X[1] + X[2], 1 + X + X^2}

GroebnerBasis[%, {X, X[1], X[2]}, Modulus -> 2]

  {X[2] + x X[2] + X[2]^2, 1 + x + X[1] + X[2], 1 + X + X^2}

Map[RR, E330 /. {X[2] -> 0, X[3] -> x, X[4] -> 1, X[5] -> 0}]

  {0, 0, 0, 0, 1 + x + X[1], 1 + X + X^2}

GroebnerBasis[%, {X, X[1]}, Modulus -> 2]

  {1 + x + X[1], 1 + X + X^2}

Map[RR, E330 /. {X[1] -> x + 1, X[2] -> 0, X[3] -> x, X[4] -> 1,
X[5] -> 0}]
GroebnerBasis[%, {X}, Modulus -> 2]

  {0, 0, 0, 0, 2 + 2 x, 1 + X + X^2}
  {1 + X + X^2}
```

En el ejemplo anterior el objetivo es ver que sí se puede encontrar las soluciones en $\mathbb{F}_4[X]$ trabajando en $\mathbb{F}_2[X]$, vamos dando valores fijos a las variables y observando que el residuo de dividir por F se va haciendo cero para los elementos de la base, el proceso podría sistematizarse, ya que en cada caso el número de elementos a considerar es finito (exactamente q).

3.2.2. Sudoku

El problema de resolver un **sudoku** se puede plantear en términos de colorear un grafo. Imaginemos que tenemos un sudoku 9×9. Cada casilla será un vértice del grafo, y habrá un lado entre cada dos vértices que estén en la misma fila, en misma columna, o en el mismo cuadrado 3×3. Tenemos $9 \times 9 = 81$ vértices y de cada vértice salen $8 + 8 + 4 = 20$ lados.

Resolver un sudoku consiste en colorear el correspondiente grafo con nueve colores, y por tanto es un problema que ya hemos resuelto. Sin embargo en la práctica la resolución consume mucho tiempo. Veamos el caso de un sudoku 4×4. En este caso tenemos $4 \times 4 = 16$ vértices, que podemos representar por $v_{i,j}$, en donde i y j varían entre 1 y 4. Además de cada vértice salen $3 + 3 + 1 = 7$ lados. Tenemos por tanto $16 + \frac{7 \times 16}{2} = 72$ ecuaciones:

Resolviendo el Sudoko en Mathematica tenemos lo siguiente
Escribimos los vértices:

```
Var = Flatten[Table[Vij, {i, 1, 4}, {j, 1, 4}]]
```

Las ecuaciones de los vértices:

```
EcuVert = Table[Var[[i]]^4 - 1, {i, 1, Length[Var]}];
```

Los lados:

```
Lado1[i_, j_] :=  Join[Table[{Vij, Vik}, {k, j + 1, 4}],
Table[{Vij,Vkj}, {k, i + 1, 4}]]
Lados2 = Flatten[Join[Table[Lado1[i, j], {i, 1, 4}, {j, i, 4}],
         Table[Lado1[i, j], {i, 1, 4}, {j, 1, i - 1}]], 2];
Lados3 = {{V11],V22]}, {V12, V21}, {V13,V24},{V14, V23}, {V31, V42},
{V32, V41},{V33, V44}, {V34, V43}};
Lados = Sort[Join[Lados2, Lados3]];
```

Las ecuaciones de los lados son:

```
Ecuacion[x_, y_] := x^3 + x^2 y + x y^2 + y^3
Ecuacion2[L_] := Ecuacion[L[[1]], L[[2]]]
EcuLados = Map[Ecuacion2, Lados];
```

Ecuaciones del sudoko 4×4

```
EcuSudoku = Join[EcuVert, EcuLados];
```

Vamos a estudiar el caso en el que $v_{1,1} = 1$, $v_{1,4} = -1$, $v_{2,1} = -1$, $v_{2,2} = I$, $v_{3,3} = 1$, $v_{4,4} = I$

```
CondInicial = {V11 - 1, V14 + 1, V21 + 1, V22 - I, V33 - 1, V44 - I};
EcuSudokuEjemplo = Join[EcuSudoku, CondInicial];
GB = GroebnerBasis[EcuSudokuEjemplo, Var]
Sistema = Table[GB[[i]] == 0, {i, 1, Length[GB]}];
SO = Solve[Sistema, Var];
Length[SO]
Table[Sort[SO[[i]], #1[[1, 2]] < #2[[1, 2]] &], {i, 1, Length[SO]}];
MatrixForm[%]
```

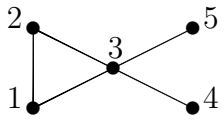
$v_{1,1} \to 1, v_{1,2} \to -i, v_{1,3} \to i, v_{1,4} \to -1, v_{2,1} \to -1, v_{2,2} \to i, v_{2,3} \to -i, v_{2,4} \to 1, v_{3,1} \to i, v_{3,2} \to -1, v_{3,3} \to 1, v_{3,4} \to -i, v_{4,1} \to -i, v_{4,2} \to 1, v_{4,3} \to -1, v_{4,4} \to i$

Observa que en este caso se tiene una solución única.

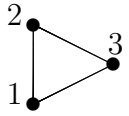
3.2.3. Grafos unívocamente coloreables

Dado grafo G que es d–coloreable, esto es, admite una d–coloración, decimos que G es unívocamente d–coloreable si para cada dos d–coloraciones distintas c_1 y c_2 existe una biyección $\theta : C \to C$ del conjunto de colores tal que $c_2 = \theta \circ c_1$. Observa que si G es unívocamente d–coloreable, entonces el conjunto $V(I(G, d))$ tiene exactamente $d!$ elementos, esto es, uno por cada permutación del conjunto de colores.

Observa que el grafo



no es unívocamente 3–coloreable; en cambio sí lo es el grafo



Observa que todo grafo d–completo es unívocamente d–coloreable.

El problema planteado es cómo determinar cuando un grafo d–coloreable es unívocamente d–coloreable.

Hacemos el siguiente desarrollo. Dada una coloración c, podemos suponer que los vértices $\{v_1, \ldots, v_s\}$ están coloreados de forma que los d últimos vértices están coloreados con los d colores. Asignamos los vértices $v_1, \ldots, v_s$ las indeterminadas $X_1 > \cdots < X_{s-d} > Y_1 > \ldots > Y_d$, y los polinomios:

$$\begin{array}{l} U_d(Y_d) := Y_d^d - 1 \\ U_i(Y_i, \ldots, Y_d) := \sum_{\alpha_i + \cdots + \alpha_d = i} Y_i^{\alpha_i} \cdots Y_d^{\alpha_d}, \qquad \text{si } i = 1, \ldots, d-1 \\ V_{i,j_i}(X_{j_i}, Y_i) := X_{j_i} - Y_i, \qquad \text{si } c(X_{j_i}) = c(Y_i), \text{para } i = 2, \ldots, d \\ V_{1,j_1}(X_{j_1} + Y_2 + \cdots + Y_d, \qquad \text{si } c_(X_{j_1}) = c(Y_1) \end{array}$$

Los grafos unívocamente d–coloreables se pueden caracterizar mediante el siguiente teorema

Teorema 3.5 (Hillar-Wibdfeldt (2006).)**.** *Sea G un grafo con una d–coloración c. Con la notación anterior son equivalentes:*

1. *G es unívocamente d –coloreable.*
2. *$\{U_d\} \cup \{U_i \mid \ i = 1 \ldots, d-1\} \cup \{V_{i,j_i} \mid \ j_i \ i = 2, \ldots, d\} \cup \{V_{1,j_1} \mid \ j_1\} \subseteq I(G, d)$.*
3. *$\{U_d\} \cup \{U_i \mid \ i = 1 \ldots, d-1\} \cup \{V_{i,j_i} \mid \ j_i; \ i = 2, \ldots, d\} \cup \{V_{1,j_1} \mid \ j_1\}$ es una base de Gröbner reducida de $I(G, d)$.*

El objetivo de este Teorema es hacer que $Exp(I(G,d))$ sea igual a $(Y_d^d, Y_{d-1}^{d-1}, \ldots, Y_2^2, Y_1, X_{s-d}, \ldots, X_1)$, y por tanto en este caso tendremos: $\mathbb{N}^s \setminus Exp(I(G,d))$ tiene cardinal $d1$

3.3. Caminos en grafos

3.3.1. Ciclos en grafos

Dado un grafo $G = (V, E)$ con vértices $\{v_1, \ldots, v_s\}$ y un entero positivo $d \leq s$, estamos interesados en estudiar si G contiene ciclos de longitud d. Para esto consideramos indeterminadas $X_1, \ldots, X_s$ e $Y_1, \ldots, Y_s$.

Si el grafo contiene un ciclo de longitud d y v_i es un vértice es de este ciclo, consideramos $y_i = 1$, en caso contrario escribimos $y_i = 0$. Como consecuencia se tiene $y_1 + \cdots + y_s = d$. Observemos también que $y_1x_1 + \cdots + y_sx_s = \sum_{i=1}^{d} i = \frac{d(d+1)}{2}$ y que $y_1x_1^2 + \cdots + y_sx_s^2 = \sum_{i=1}^{d} i^2 = \frac{d(d+1)(2d+1)}{6}$

$$\begin{array}{l} Y_1 + \cdots + Y_s - d = 0, \\ Y_1X_1 + \cdots + Y_sX_s - \frac{d(d+1)}{2} = 0 \\ Y_1X_1^2 + \cdots + Y_sX_s^2 - \frac{d(d+1)(2d+1)}{6} = 0 \\ \left.\begin{array}{l} Y_1(Y_1 - 1) = 0 \\ \vdots \\ Y_s(Y_s - 1) = 0 \end{array}\right\} \end{array}$$

Dado un vértice v_i con $y_i = 1$, consideramos $x_i = k$, si v_i ocupa el lugar k en el ciclo. Como consecuencia se tiene $(x_i - 1) \cdots (x_i - d) = 0$.

$$\begin{array}{l} (X_1 - 1) \cdots (X_1 - d) \\ \vdots \\ (X_s - 1) \cdots (X_s - d) \end{array}$$

Supongamos que v_i ocupa el lugar k en el ciclo, otro vértice v_j ocupará el lugar siguiente, $k + 1$ ó 1, según el caso, y en cualquier caso se tiene $y_j = 1$. Tenemos:

1. Si $k < d$, entonces $x_j = k + 1$, y se tiene $x_i - x_j + 1 = 0$.
2. Si $k = d$, entonces $x_j = 1$, y se tiene $x_i - x_j - (d - 1) = 0$.

Para $y_i = 1$ e $y_j = 1$, se tiene:

1. Si $x_i < d$ y la dirección en el ciclo es de v_i a v_j, entonces $x_j = k + 1$, y como antes tenemos $x_i - x_j + 1 = 0$.
2. Si $x_i > 2$ y la dirección en el ciclo es de v_j a v_i, entonces se obtiene el caso anterior intercambiando i y j.
3. Si $x_i = d$ y la dirección en el ciclo es de v_i a v_j, entonces $x_j = 1$, y como antes tenemos $x_i - x_j - (d - 1) = 0$.
4. Si $x_i = 1$ y la dirección en el ciclo es de v_j a v_i, entonces se obtiene el caso anterior intercambiando i y j.

Tenemos pues la relación $(x_i - x_j + 1)(x_i - x_j - (d-1)) = 0$ para cada j tal que $\{i,j\} \in E$ y la dirección en el ciclo es de v_i a v_j. Podemos escribir esta relación $y_i(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0$

Si $\{i,j\} \in E$ y se tiene $Y_i = 1$, $y_j = 0$, entonces no nos interesan las relaciones de x_i y x_j. Por tanto, siguiendo con la notación anterior tendremos $y_i(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0$, que es $x_i x_i = 0$, de donde $x_i = 0$, pero esto no es posible.

Si $\{i,j\} \in E$ y se tiene $y_i = 0$, las relaciones de x_i y x_j no nos interesan. Por tanto, siguiendo con la notación anterior tendremos $y_i(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0$.

Juntando ahora todas estas relaciones tenemos $y_i \prod_{\{i,j\}\in E}(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0$. De esta forma, como el producto tiene al menos dos factores y algún y_j no nulo, los factores con $y_j = 0$ que dan un factor x_i^2 podemos simplificarlos ya que los x_i son no nulos.

Esto nos da las relaciones:

$$Y_i \prod_{\{i,j\}\in E}(X_i - Y_j X_j + Y_j)(Y_i - Y_j X_j - Y_j(d-1)) \ \}_{i=1,\ldots,s}$$

Como consecuencia si el grafo G tiene un ciclo de longitud d, entonces el siguiente sistema tiene una solución.

$$\begin{array}{l} Y_1 + \cdots + Y_s - d = 0, \\ Y_1 X_1 + \cdots + Y_s X_s - \frac{d(d+1)}{2} = 0, \\ Y_1 X_1^2 + \cdots + Y_s X_s^2 - \frac{d(d+1)(2d+1)}{6} = 0, \\ \ Y_i(Y_i - 1) = 0 \ \}_{i=1,\ldots,s} \\ \ (X_i - 1)\cdots(X_i - d) = 0 \ \}_{i=1,\ldots,s} \\ \ Y_i \prod_{\{i,j\}\in E}(X_i - Y_j X_j + Y_j)(Y_i - Y_j X_j - Y_j(d-1)) = 0 \ \}_{i=1,\ldots,s} \end{array}$$

Teorema 3.6. *Dado un grafo $G = (V,E)$ con vértices $V = \{v_1, \ldots, v_s\}$ y $d < s$ un entero positivo, son equivalentes:*

1. *G contiene un ciclo de longitud d.*
2. *El sistema de ecuaciones*

$$\begin{array}{l} Y_1 + \cdots + Y_s - d = 0, \\ Y_1 X_1 + \cdots + Y_s X_s - \frac{d(d+1)}{2} = 0, \\ Y_1 X_1^2 + \cdots + Y_s X_s^2 - \frac{d(d+1)(2d+1)}{6} = 0, \\ \ Y_i(Y_i - 1) = 0 \ \}_{i=1,\ldots,s} \\ \ (X_i - 1)\cdots(X_i - d) = 0 \ \}_{i=1,\ldots,s} \\ \ Y_i \prod_{\{i,j\}\in E}(X_i - Y_j X_j + Y_j)(Y_i - Y_j X_j - Y_j(d-1)) = 0 \ \}_{i=1,\ldots,s} \end{array}$$

tiene una solución.

Según lo anterior, cada solución dará un ciclo de longitud d de G.

Observación: Tenemos que limitar las posibles permutaciones cíclicas de los vértices que conforman el ciclo.

Demostración. Sólo es necesario probar que si si $x_1, \ldots, x_s, y_1, \ldots, y_s$ es una solución del sistema, entonces existe un ciclo de longitud d en el grafo.

Consideramos los índices i tales que $y_i \neq 0$; estos son los vértices del ciclo. Vamos a ver que estos vértices forman un ciclo. Para $y_i \neq 0$ tenemos que existe un índice j tal que $y_j \neq 0$ y $x_i - x_j + 1 = 0$ ó $x_i - x_j - (d-1) = 0$. En el primer caso $x_j = x_i + 1$, y en el segundo $x_i + 1 = x_j + d$; como $x_i, x_j \in \{1, \ldots, d\}$, se tiene $x_i = d$ y $x_j = 1$. Ahora un simple razonamiento sobre el principio prueba que los x_i para los que $y_i \neq 0$ recorren el conjunto $\{1, \ldots, d\}$, y tenemos un ciclo.

Desarrollamos un algoritmo en Mathematica para determinar si un grafo tiene ciclos de d vértices.

Algoritmo La variable t es el número de vértices en el ciclo, y la s es el número de variables o vértices en este caso.

```
Var[M_, s_] := Table[M[i], {i, 1, s}]
VarXY = Union[Var[X, 5], Var[Y, 5]]
Var[X, 5]
Var[Y, 5]
Ecuaciones[L_] := Table[L[[i]] == 0, {i, 1, Length[L]}]
Primera[s_] := Table[Y[j]*(Y[j] - 1), {j, 1, s}]
Suma[t_, s_] :={ Sum[Y[j] , {j, 1, s}] - t}
Segunda[t_, s_] := Table[Product[(X[j]-k),{k,1,t}],{j,1,s}]
Tercera[t_, L_List] := Complement[Table[Y[j]Product[
             (X[j] - Y[L[[j, i]]]*X[L[[j, i]]] + Y[L[[j, i]]])
             (X[j] - Y[L[[j, i]]]*X[L[[j, i]]] - Y[L[[j, i]]](t - 1)),
             {k,1,Length[L[[j]]]}],{j, 1, Length[L]}],
             Var[Y, 5]]

SumaCuadrados[t_] := (t (t + 1) (2 t + 1))/6
SumaC[t_, s_] := {Sum[Y[j]*X[j]^2, {j, 1, s}] - Sumacuadrados[t]}
Ecu[t_, s_, L_] :=  Union[Suma[t, s], Primera[s], Segunda[t, s],
                    Tercera[t, L],  SumaC[t, s]]
```

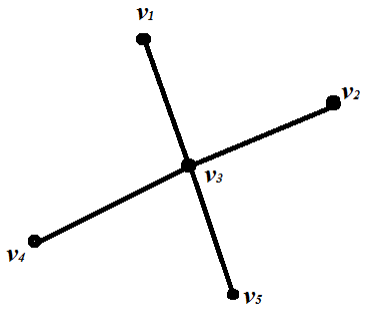


Figura 3.8: Grafo

Ejemplo 3.11. *Considere el grafo de la figura (3.8) y determine si tiene ciclos de longitud 3.*

A simple vista vemos que no tiene ciclos de longitud 3, implementaremos un algoritmo en Mathematica para ver que funcionan las relaciones planteadas.
Primero elaboramos la lista que contiene la información de los vértices en este caso el vértice v_1 solo tiene relación con le vértice v_3 de forma que el primer elemento de la L será $\{3\}$, de igual manera el vértice v_3 tiene relación con los vértices v_1, v_2, v_4, v_5, así el elemento 3 de la lista será $\{1, 2, 4, 5\}$.

```
L = {{3}, {3}, {1, 2, 4, 5}, {3}, {3}}
Ecu[3, 5, L];
MatrixForm[%];
EcuGB = GroebnerBasis[Ecu[3, 5, L], Union[Var[X, 5], Var[Y, 5]]]
{1}
```

No hay ciclos de longitud 3 en este grafo

Ver ejemplos (3.16) y (3.17) en el Apéndice.

3.3.2. Caminos en un grafo

Dado un grafo orientado $D = (V, E)$ con vértices $\{v_1, \ldots, v_s\}$ y un entero positivo $d \leq s$, estamos interesados en estudiar si D tiene caminos de longitud $d-1$ sin considera los que tienen ciclos. Para esto consideramos indeterminadas $X_1, \ldots, X_s$ e $Y_1, \ldots, Y_s$.

Si el grafo contiene un camino de longitud $d-1$ y v_i es un vértice de este camino, consideramos $y_i = 1$, en caso contrario escribimos $y_i = 0$. Como consecuencia se tiene

$y_1 + \cdots + y_s = d$. Observemos también que $y_1x_1 + \cdots + y_sx_s = \sum_{i=1}^{d} i = \frac{d(d+1)}{2}$ y que $y_1x_1^2 + \cdots + y_sx_s^2 = \sum_{i=1}^{d} i^2 = \frac{d(d+1)(2d+1)}{6}$.

$$\begin{array}{l} Y_1 + \cdots + Y_s - d = 0, \\ Y_1X_1 + \cdots + Y_sX_s - \frac{d(d+1)}{2} = 0 \\ Y_1X_1^2 + \cdots + Y_sX_s^2 - \frac{d(d+1)(2d+1)}{6} = 0 \\ \left.\begin{array}{l} Y_1(Y_1-1) = 0 \\ \vdots \\ Y_s(Y_s-1) = 0 \end{array}\right\} \end{array}$$

Dado un vértice v_i con $y_i = 1$, consideramos $x_i = d - k$, si v_i ocupa el lugar k en el camino. Como consecuencia se tiene $x_i(x_i-1)\cdots(x_i-(d-1)) = 0$.

$$\begin{array}{l} X_1(X_1-1)\cdots(X_1-(d-1)) = 0 \\ \vdots \\ X_s(X_s-1)\cdots(X_s-(d-1)) = 0 \end{array}$$

Supongamos que v_i ocupa el lugar k es decir $x_i = d - k$ en el camino , otro vértice v_j ocupará el lugar siguiente, $k+1$ o $x_j = d - (k+1)$ y en cualquier caso se tiene $y_j = 1$. Tenemos que $x_i - x_j - 1 = 0$, si $\{v_i, v_j\} \in E$ de igual manera se cumple que $y_j(x_i - y_jx_j - y_j) = 0$ Juntando ahora todas estas relaciones tenemos $y_i \prod_{\{i,j\}\in E}(x_i - y_jx_j - y_j) = 0$.

Tenemos

$$Y_i \prod_{\{i,j\}\in E}(X_i - Y_jX_j - Y_j) = 0 \ \}_{i=1,\ldots,s}$$

Como consecuencia si el grafo D tiene un camino de longitud $d-1$, entonces el siguiente sistema tiene una solución.

$$\begin{array}{l} Y_1 + \cdots + Y_s - d = 0, \\ Y_1X_1 + \cdots + Y_sX_s - \frac{d(d+1)}{2} = 0, \\ Y_1X_1^2 + \cdots + Y_sX_s^2 - \frac{d(d+1)(2d+1)}{6} = 0, \\ Y_i(Y_i-1) = 0 \ \}_{i=1,\ldots,s} \\ X_i(X_i-1)\cdots(X_i-(d-1)) = 0 \ \}_{i=1,\ldots,s} \\ Y_i \prod_{\{i,j\}\in E}(X_i - Y_jX_j + Y_j) = 0 \ \}_{i=1,\ldots,s} \end{array}$$

Desarrollamos el siguiente algoritmo en Mathemática para grafos orientados

Algoritmo

La variable t es el número de vértices en el ciclo, y la s es el número de variables o vértices en este caso. El formato de la lista que contiene la información d los vértices es L=vértices de los lados que parten de v_1,vértices de los lados que parten de v_2,. . . ,

```
Var[M_, s_] := Table[M[i], {i, 1, s}]
VarXY = Union[Var[X, 5], Var[Y, 5]]
Var[X, 5]
Var[Y, 5]
Ecuaciones[L_] := Table[L[[i]] == 0, {i, 1, Length[L]}]
Primera[s_] := Table[Y[j]*(Y[j] - 1), {j, 1, s}]
Suma[t_, s_] :={ Sum[Y[j] , {j, 1, s}] - t}
Segunda[t_, s_] := Table[Product[(X[j]-k),{k,1,t}],{j,1,s}]
Tercera[t_, L_List] := Table[Y[j]Product[
            (X[j] - Y[L[[j, i]]]*X[L[[j, i]]] + Y[L[[j, i]]]),
            {k,1,Length[L[[j]]]}],{j, 1, Length[L]}]

SumaCuadrados[t_] := (t (t + 1) (2 t + 1))/6
Cuarta[t_, s_] := {Sum[Y[j]*X[j]^2, {j, 1, s}] - Sumacuadrados[t-1]}
Ecu[t_, s_, L_] :=  Union[Suma[t, s], Primera[s], Segunda[t, s],
                    Tercera[t, L],  Cuarta[t, s]]
```

Ejemplo 3.12. *Considere el grafo de la figura* (3.9) *y determine si tiene caminos de longitud 4.*

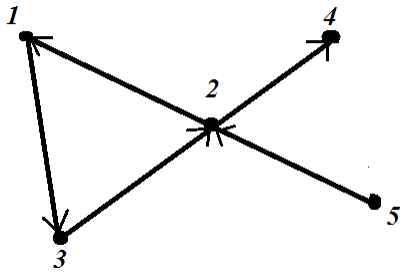


Figura 3.9: Grafo

```
lados = {{3}, {1, 4}, {2}, {}, {2}};
Ecu[4, 5, lados];
EcuGB = GroebnerBasis[Ecu[4, 5, lados], VarXY]

{1}
```

Según el algoritmo implementado este grafo no tiene caminos de longitud 4, ya que consideramos caminos que no pasan dos veces por un mismo vértice.

APÉNDICE

Bases de Gröbner con Mathematica

Para calcular bases de Gröbner utilizamos el comando
Dada la lista de polinomios y la lista de variables

```
GroebnerBasis[{poly 1, poly 2,...},{x1,x2,...}]
```

Se da la lista de polinomios, las variables y las que se quieren eliminar

```
GroebnerBasis[{poly 1, poly 2,...},{x1,x2,...},{y1,y2,...}]
```

Ejemplo 3.13.

```
GroebnerBasis[{x^2 - 2 y^2, x y - 3}, {x, y}]
{-9 + 2 y^4, 3 x - 2 y^3}
```

Mathematica por defecto trabaja con un orden Lexicográfico pero puede cambiarse el orden según se desee por ejemplo

Ejemplo 3.14.

```
GroebnerBasis[{x^2 - 2 y^2, x y - 3}, {x, y},
               MonomialOrder->DegreeReverseLexicographic]
{-3 + x y, x^2 - 2 y^2, -3 x + 2 y^3}
```

Para calcular una base de Gröbner de la intersección entre dos ideales, dada las listas de generadores de cada ideal y el número de variables a considerar podemos definir una función que determine dicha intersección.

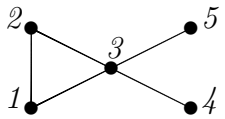
```
Interseccion[lista1_,lista2_,n_]:=Module[{lista1T,lista2T,T,i},
lista1T=Table[lista1[[i]]*T,{i,Length[lista1]}];
lista2T=Table[lista2[[i]]*(1-T),{i,Length[lista2]}];
GroebnerBasis[Union[lista1T,lista2T],Union[{T},Table[X[i],{i,1,n}]],{T}]
]
```

Ejemplo 3.15.

```
Interseccion[{X[1] - 4, X[2] - 2}, {X[1] + 2, X[2] - 3}, 2]
{6 - 5 X[2] + X[2]^2, -16 + X[1] + 6 X[2]}
```

Ciclos en grafos

Ejemplo 3.16. *Considere el grafo de la figura y determine si tiene ciclos de longitud 3.*



Escribimos la lista que contiene la información de los vértices

```
L = {{2, 3}, {1, 3}, {1, 2, 4, 5}, {3}, {3}}
```

Luego aplicamos el algoritmo descrito en la sección (3.3.1)

```
Ecu[3, 5, L];
MatrixForm[%]
EcuGB = GroebnerBasis[Ecu[3, 5, L], Union[Var[X, 5], Var[Y, 5]]];
MatrixForm[%];
EcuGBY = GroebnerBasis[Ecu[3, 5, L], Union[Var[X, 5], Var[Y, 5]],
Var[X, 5]]

  {Y[5],Y[4],-1+Y[3],-1+Y[2],-1+Y[1]}

EcuGBY2 = Ecuaciones[EcuGBY];
Solve[EcuGBY2, Var[Y, 5]]

  {{Y[5]->0,Y[4]->0,Y[3]->1,Y[2]->1,Y[1]->1}}
```

Observe que la base de Gröbner se calculó de manera que eliminara las variables X[i] así vemos que vértices pertenecen o no pertenecen al ciclo y precisamente solo tenemos un ciclo de longitud 3 para este grafo.

Ejemplo 3.17. *Considere el grafo de la figura y evalúe si tiene ciclos de longitud 3.*

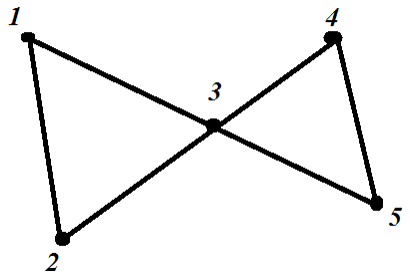


Figura 3.10: Grafo

```
L = {{2, 3}, {1, 3}, {1, 2, 4, 5}, {3, 5}, {4, 3}}
Ecu[3, 5, L];
MatrixForm[%]
EcuGB = GroebnerBasis[Ecu[3, 5, L], Union[Var[X, 5], Var[Y, 5]]];
EcuGBY = GroebnerBasis[Ecu[3, 5, L], Union[Var[X, 5], Var[Y, 5]],
Var[X, 5]]

  {-Y[5]+Y[5]^2,Y[4]-Y[5],-1+Y[3],-1+Y[2]+Y[5],-1+Y[1]+Y[5]}

EcuGBY2 = Ecuaciones[EcuGBY];
Solve[EcuGBY2, Var[Y, 5]]

  {{Y[1]->0},Y[2]->0,Y[3]->1,Y[4]->1,{Y[5]->1},
   {Y[1]->1},Y[2]->1,Y[3]->1,Y[4]->0,{Y[5]->0}}
```

Son las dos soluciones que se pueden observar en el diagrama.

Bibliografía

[1] W. W. Adams, P. Loustaunau. An Introduction to Gröbner Bases. American Mathematical Society. 1996.

[2] E. Arnold, S. Lucas, L. Taalman. Grobner basis representations of sudoku. (2009)

[3] C. Y. Chao, Z. Chen. On uniquely 3-colorable graphs, Discrete Mathematics 112 (1993), 21?27.

[4] D.O. David Cox, John Little. Ideals,Varieties, and Algorithms. Springer. 2007.

[5] J. A. de Loera. Gröbner bases and graph colorings, Beiträge zur Algebra un Geometrie 36 (1995), 89?96.

[6] J. A. de Loera, J. Lee, S. Margulies, S. Onn. Expressing combinatorial optimization problems by systems of polynomial equations and the Nullstellensatz. arXiv:0706.0578

[7] J. A. de Loera, C. J. Hillar, P. N. Malkin, M. Omar. Recognizing graph theoretic properties with polynomial ideals. The Electronic Journal of Combinatorics, 17 (2010), #R114.

[8] A. Griffith, A. Parker. A Groebner basis approach to number puzzles (2010)

[9] C. Hillar, T. Windfeldt. Algebraic characterization of uniquely vertex colorable graphs. J. Comb. Th. appear.

[10] P. Jara. Notas de trabajo. 6. Álgebra Conmutativa. Granada, 2010.

[11] F. Sagols, J. Muñoz, C. J. Colbourn. Ideals, varieties, stability, coloring and combinatorial designs. (2008).

[12] Y. Sato, S. Inoue, A. Suzuki, K. Nabeshima. Boolen Grobner bases and sudoku. (2010).

[13] B. Sturmfels. "What is . . . a Gröbner Basis??. Notices AMS 52, Number 10. 2005.

Índice alfabético