Bases de Gröbner y su aplicación a la resolución de Sudokus

Bárbara Zapater Zarroca

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directores del trabajo:
José Ignacio Cogolludo Agustín y
Jorge Martín Morales

9 de febrero de 2021

Prólogo

Lógica, rapidez, paciencia y matemáticas. Teniendo en cuenta estos cuatro conceptos podemos resolver el juego del Sudoku, el cual sigue siendo un pasatiempo emocionante para millones de personas. Geométricamente hablando, un Sudoku es un tablero de tamaño 9×9 dividido en cajas 3×3, las cuales poseen números entre el 1 y el 9. Este rompecabezas obedece las siguientes reglas: no puede haber números repetidos en la misma fila, columna o caja 3×3. Pero, ¿por, para qué y cómo se aplican las matemáticas a la resolución de este pasatiempo? Es en este contexto donde se basa el presente trabajo.

La historia de los Sudokus se remonta a un juego del siglo XVIII, donde los matemáticos suizos lo llamaron "Cuadrados latinos". Sin embargo, el juego que conocemos actualmente fue inventado a finales de la década de 1970 en Nueva York. Este juego, ideado por el arquitecto Howard Garns, se conocía como "Ubicar números", pues consistía en colocar números en los espacios vacíos de una cuadrícula. Actualmente, este rompecabezas se conoce como "Sudoku". El nombre proviene de dos palabras japonesas: *Su*, que significa número y *Doku*, que significa solo. Este juego matemático fue muy conocido en Japón a partir de 1986 aunque su popularidad mundial llegaría unos años más tarde, en torno al 2005.

Hoy en día el Sudoku sigue siendo un enigma habitual en los periódicos, páginas online, revistas, concursos... Además, como se trata de un puzle numérico que estimula las capacidades mentales y la memoria, permite que no sea solo una diversión, sino que también resulte un aprendizaje.

Por otra parte, existen algunas variantes de este famoso juego. En [7] se da un modelo matemático junto con su sistema de ecuaciones algebraicas. Algunas de estas variantes son: el tablero está coloreado en gris y blanco de manera que las celdas grises contienen números pares y las celdas blancas solamente impares (Sudoku par-impar), se puede dar como pista inicial la suma de un grupo de celdas en vez del valor de cada celda individual (Sudoku killer), el tablero tiene formas distintas de un rectángulo (Sudokus geométricos), etc.

Aunque de primeras resulte cuanto menos curioso, realmente el Sudoku se basa en fundamentos matemáticos, y por ello existen métodos numéricos con los que poder resolverlos. Tratando el Sudoku como si fuera un grafo, vinculando así la geometría y el álgebra, podemos resolver este juego lógico. Un concepto clave para ello son las bases de Gröbner que, de una manera elegante y directa, nos permitirán conocer todas las soluciones de un sistema de ecuaciones. Estas bases de ideales se forman de tal manera que para todo polinomio del ideal, el término principal de este polinomio es divisible por alguno de los términos principales de los polinomios que componen dicha base. Además, para ello, en este trabajo nos familiarizaremos con una de las muchas aplicaciones de las bases de Gröbner, la coloración de grafos. Cabe mencionar la variedad de aplicaciones relacionadas con esta teoría, entre las que se encuentran calcular el polinomio mínimo en extensiones de cuerpos, dar demostraciones automáticas en Geometría Euclidiana, estudiar sistemas criptográficos y programación entera e incluso estudiar algunos resultados de Teoría de grafos.

Este trabajo está organizado del siguiente modo. En el Capítulo 1 se tratan los fundamentos algebraicos y conceptos previos que introducen la teoría de las bases de Gröbner. En el Capítulo 2 profundizaremos en dicha teoría para lo cual trabajaremos con polinomios en varias variables. Para estos dos primeros capítulos de información más teórica nos hemos basado en el libro [5], pero hay otras referencias sobre este tema como son [1] y [9]. A continuación, en el Capítulo 3 nos centraremos en estudiar el problema del coloreado en un grafo, lo cual está fundamentado en la Sección 3 de [4]. Finalizando, en el Capítulo 4 aplicaremos lo estudiado en los tres capítulos previos para conseguir nuestro objetivo, resolver Sudokus aplicando las matemáticas y la computación. Este capítulo final apoya su desarrollo y base teórica en [7]. Por último, en el Apéndice A se presentan varios códigos, utilizados para la resolución de algunos ejemplos implementados mediante el software SageMath [10], el cual usa en "background" el programa SINGULAR [6] para calcular las bases de Gröbner.

Toda esta base matemática es la que permite que la gente pueda poner a prueba su cerebro con acertijos lógicos, interesantes y desafiantes. Por lo cual, el Sudoku seguirá siendo un entretenimiento querido y popular en la vida cotidiana de millones de personas en todo el mundo.

Palabras clave: polinomios, algoritmo de la división, orden monomial, ideales monomiales, Lema de Dickson, bases de Gröbner, Teorema de las bases de Hilbert, algoritmo de Buchberger, grafo, k-coloración, Sudoku, Shidoku.

Summary

In this project it will be explained several theoretical results and practical examples related to Sudokus. More specifically, this work will be based on the study of the Gröbner bases and its application to both graph theory and Sudokus resolution.

This project is divided into four chapters. A brief description of each chapter will be given inmediately below.

- **Chapter 1: Previous concepts and fundamentals**

  To begin with, the necessary concepts for understanding the other chapters are given. These concepts include definitions such as monomial, polynomial, affine space, affine and linear varieties and ideal, among others. The existence and uniqueness of the division algorithm for polynomials in one variable will be studied.

- **Chapter 2: Gröbner Bases**

  Once the previous part is completed, the main part of this project will be studied. In this second chapter, the theory of Gröbner bases will be introduced and studied. Polinomials in $K[x_1,\dots,x_n]$ will be dealt and how to order monomials will be discussed, explaining some of the existing monomial orderings types. This concept will be important to study the division algorithm in $K[x_1,\dots,x_n]$ which will be better understood by an example. Besides, Dickson's Lemma and Hilbert's basis Theorem will be stated and proved. Then, Buchberger's algorithm will be understood. That result will be used to construct the Gröbner bases. A code of this algorithm has been implemented using SageMath, which can be found in the Appendix A. To end this chapter, four problems about polynomials and ideals will be solved thanks to the Gröbner bases:

  1. *The ideal description problem.*
  2. *The ideal membership problm.*
  3. *The problem of solving polinomial equations.*
  4. *The implicitization problem.*

- **Chapter 3: Graph coloring**

  Graph coloring with k colors is the main goal of this chapter. First of all, the kind of graphs we need will be defined and then, the explanation and resolution of this problem will be treated. To do this, a system of polynomial equations imposing some conditions will be generated. To solve this system, the Gröbner bases will be used, for which a SageMath code has been implemented. Moreover, this code is explained in the Appendix A.

- **Chapter 4: Sudokus and Gröbner bases**

  Sudokus will be solved using Gröbner bases theory and the Sudoku will be considered as if it was a graph in order to apply some results of Chapther 3. That is, to solve Sudokus a system of polynomial equations has to be obtained, in the same way that it is obtained for the graph coloring problem in the previous chapter. An ideal in the polynomial ring of several variables will

be associated to the Sudoku. This ideal will be generated by the polynomials which define the system of equations. The reduced Gröbner basis will be calculated for this ideal whose generators form a system equivalent to the original system. That is why solving this new system of equations, using mathematics and computation, the solution to the Sudoku is obtained. In the Appendix A it is explained how to write with SageMath a Sudoku with the initial clues given to be able to apply the code generated for the previous chapter and then the system will be solved. Finally, some mathematical conjectures are discussed. Moreover, a conclusion to this interesting application of the Gröbner bases is given.

Índice general

Capítulo 1

Conceptos y fundamentos previos

A lo largo de este capítulo daremos algunas definiciones y algunos resultados preliminares que serán de relevancia para comprender las bases de Gröbner, objeto principal de estudio del marco teórico.

1.1. Polinomios en espacios afines

Definición 1. Un *monomio* x^α en las variables $x_1, \ldots, x_n$ es un producto de la forma

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

donde todos los exponentes $\alpha_1, \ldots, \alpha_n$ son enteros no negativos. El *orden total* de un monomio es la suma de sus exponentes, el cual denotaremos mediante $|\alpha|$.

Definición 2. Un *polinomio* f en las variables $x_1, \ldots, x_n$ con coeficientes en un cuerpo K es una combinación lineal finita de monomios con coeficientes también en K. Escribiremos el polinomio f de la siguiente manera:

$$f = \sum_\alpha a_\alpha x^\alpha,\ a_\alpha \in K,\ \alpha = (\alpha_1, \ldots, \alpha_n).$$

Denotaremos mediante $K[x_1, \ldots, x_n]$ al conjunto de todos los polinomios en $x_1, \ldots, x_n$ con coeficientes en el cuerpo K. Este conjunto forma un *anillo de polinomios*.

Definición 3. Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio en $K[x_1, \ldots, x_n]$. Entonces:

i) El coeficiente del monomio x^α es a_α.

ii) Si $a_\alpha \neq 0$, entonces $a_\alpha x^\alpha$ será un término del polinomio f.

iii) El grado total de $f \neq 0$ es el máximo $|\alpha|$ tal que el coeficiente a_α es no nulo. Lo denotaremos mediante $grado(f)$.

Ejemplo 1.

- Sean los monomios $-15x^2$ y $3xy^4$. Entonces el orden total del primer monomio es 2 y el orden total del segundo monomio es $1+4=5$.
- Sea ahora el polinomio $f = 3xy^4 - 15x^2$ formado como combinación lineal de los dos monomios anteriores. En primer lugar, notar que f es un polinomio en $\mathbb{R}[x,y]$.
  - El coeficiente del monomio $3xy^4$ es 3 y el coeficiente de $-15x^2$ es -15.
  - f está compuesto por dos términos: $3xy^4$ y $-15x^2$.
  - $grado(f) = 5$ (ya que $1+4=5>2$).

1.2. Variedades afines

Definición 4. Sea un cuerpo K y un entero n positivo. Entonces denotaremos mediante K^n al *espacio afín* de dimensión n sobre K formado por n-tuplas cuyos elementos están en K.

Los polinomios y los espacios afines están relacionados. La ventaja de trabajar con el anillo de polinomios $K[x_1,\dots,x_n]$ es que se puede identificar, cuando K es infinito, con las funciones polinómicas del espacio afín K^n. Es decir, identificamos los polinomios con las funciones evaluadas en K^n. De este modo, los polinomios definen variedades afines y así se puede enlazar el álgebra con la geometría.

Definición 5. Sea K un cuerpo y sean $f_1,\dots,f_s$ polinomios en $K[x_1,\dots,x_n]$. Entonces la *variedad afín* definida por $f_1,\dots,f_s$ viene dada por el siguiente conjunto

$$\mathbf{V}(f_1,\dots,f_s) = \{(a_1,\dots,a_n) \in K^n \,|\, f_i(a_1,\dots,a_n) = 0,\ \forall\ 1 \le i \le s\} \subseteq K^n.$$

Es decir, $\mathbf{V}(f_1,\dots,f_s)$ es el conjunto de puntos $a_1,\dots,a_n$ que anulan a todos los polinomios $f_1,\dots,f_s$.

Definición 6. Fijemos ahora un cuerpo K y consideremos un sistema lineal de m ecuaciones con coeficientes en K

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1, \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m. \end{aligned} \tag{1.1}$$

La solución de estas ecuaciones forman una variedad afín en K^n llamada *variedad lineal*.

En el Capítulo 2 estudiaremos cómo obtener todas las soluciones del sistema de ecuaciones (1.1) y en el Capítulo 3 lo aplicaremos.

1.3. Ideales

El objetivo de esta sección es introducir el concepto de ideal. Así mismo, veremos cómo están relacionados los ideales con las variedades afines.

Definición 7. Un subconjunto $I \subseteq K[x_1,\dots,x_n]$ se dice que es un *ideal* si cumple:

i) $0 \in I$.

ii) Si $f, g \in I$, entonces $f + g \in I$.

iii) Si $f \in I$ y $h \in K[x_1,\dots,x_n]$, entonces $hf \in I$.

El primer ejemplo natural de un ideal es el ideal generado por un número finito de polinomios. Es decir, si $f_1,\dots,f_s \in K[x_1,\dots,x_n]$ entonces

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

es un ideal de $K[x_1,\dots,x_n]$. Diremos que $\langle f_1,\dots,f_s\rangle$ es el *ideal generado* por $f_1,\dots,f_s$.

Definición 8. Sea I un ideal. Se dice que I está *finitamente generado* si existe un número finito de polinomios $f_1,\dots,f_s \in K[x_1,\dots,x_n]$ tal que $I = \langle f_1,\dots,f_s\rangle$.

Veamos ahora que una variedad depende solamente del ideal generado por sus ecuaciones.

Proposición 1.1. *Si $\langle f_1,\dots,f_s\rangle = \langle g_1,\dots,g_t\rangle$, entonces se tiene $\mathbf{V}(f_1,\dots,f_s) = \mathbf{V}(g_1,\dots,g_t)$.*

Ejemplo 2. Consideramos la variedad $\mathbf{V}(2x^2+3y^3-11, x^2-y^2-3)$. Sea $I_1 = \langle 2x^2+3y^3-11, x^2-y^2-3\rangle = \langle F_1, F_2\rangle$ y sea $I_2 = \langle x^2-4, y^2-1\rangle = \langle f_1, f_2\rangle$. Veamos, por doble contenido, que $I_1 = I_2$:

- $F_1 = 2f_1 + 3f_2 \in I_2$, $F_2 = f_1 - f_2 \in I_2 \Rightarrow I_1 \subseteq I_2$.
- $f_1 = \frac{1}{4}(F_1 + 3F_2) \in I_1$, $f_2 = \frac{1}{5}(F_1 - 2F_2) \in I_1 \Rightarrow I_2 \subseteq I_1$.

Por lo tanto, aplicando la Proposición 1.1 obtenemos $\mathbf{V}(2x^2+3y^3-11, x^2-y^2-3) = \mathbf{V}(x^2-4, y^2-1) = \{(\pm 2, \pm 1)\}$.

Este ejemplo nos muestra que si cambiamos los polinomios que generan el ideal, podemos determinar más fácil la variedad.

1.4. Polinomios en una variable

En esta sección vamos a estudiar el algoritmo de la división para polinomios en una variable. Este algoritmo lo usaremos para determinar la estructura de los ideales en $K[x]$. Asimismo nos ayudará a entender la idea del máximo común divisor ya que se muestra un método para calcularlo, el cual es análogo al algoritmo de Euclides sobre los enteros.

Definición 9. Sea f un polinomio no nulo de modo que $f = c_0x^m + c_1x^{m-1} + \cdots + c_m \in K[x]$ con $c_i \in K$ y $c_0 \neq 0$ (es decir, $grado(f) = m$). Se dice que c_0x^m es el *término principal* de f y lo denotaremos mediante $LT(f)$.

Proposición 1.2 (El algoritmo de la división en $K[x]$)**.** *Sea K un cuerpo y sea g un polinomio no nulo en $K[x]$. Entonces todo polinomio $f \in K[x]$ se puede escribir como*

$$f = q \cdot g + r,$$

donde $q, r \in K[x]$ y el resto verifica $r = 0$ o $grado(r) < grado(g)$. Es más, q y r son únicos y existe un algoritmo para calcularlos.

Tomamos como variables de entrada g y f y como variables de salida q y r. A continuación, se muestra un algoritmo presentado en forma de pseudocódigo para hallar tales q y r.

Algoritmo 1 Algoritmo de la división en $K[x]$

Inicialización: $q := 0, r := f$
WHILE $r \neq 0$ **AND** $LT(g)$ divide a $LT(r)$ **DO**
  $q := q + LT(r)/LT(g)$
  $r := r - (LT(r)/LT(g)) \cdot g$
RETURN q, r

Dado un ideal nos gustaría ser capaces de encontrar su generador de una forma efectiva. Para ello necesitamos la siguiente definición.

Definición 10. Un *máximo común divisor* de los polinomios $f_1, \ldots, f_s \in K[x]$ es un polinomio h tal que:

i) h divide a $f_1, \ldots, f_s$.

ii) Si p es otro polinomio que divide a $f_1, \ldots, f_s$, entonces p es múltiplo de h.

Cuando h cumpla estas propiedades, lo denotaremos $h = mcd(f_1, \ldots, f_s)$.

A continuación, se muestran las principales propiedades de este máximo común divisor.

Proposición 1.3. *Sean $f_1,\dots,f_s \in K[x]$, con $s \geq 2$. Entonces:*

i) *$mcd(f_1,\dots,f_s)$ existe y es único salvo una constante multiplicativa no nula en K.*

ii) *$mcd(f_1,\dots,f_s)$ es un generador del ideal $\langle f_1,\dots,f_s\rangle$.*

iii) *Si $s \geq 3$, entonces $mcd(f_1,\dots,f_s) = mcd(f_1, mcd(f_2,\dots,f_s))$.*

iv) *Existe un algoritmo para calcular $mcd(f_1,\dots,f_s)$.*

Veamos cómo funciona tal algoritmo presentado en forma de pseudocódigo.

- Para $s = 2$. Tomamos como variables de entrada los polinomios f_1 y f_2 y obtenemos como variable de salida $h = mcd(f_1, f_2)$.

Algoritmo 2 Algoritmo de Euclides para encontrar el $mcd(f_1, f_2)$

```
Inicialización: h := f_1, s := f_2
WHILE s ≠ 0 DO
    res := resto(h, s)
    h := s
    s := res
RETURN h
```

- Para $s \geq 3$. Tomamos como variables de entrada los polinomios $f_1,\dots,f_s$ y llamamos *polin* a la lista formada por dichos polinomios. Para calcular el máximo común divisor, denotado en el pseudocódigo mediante *m*, hay que crear una función que llame al algoritmo de Euclides para dos polinomios, explicado justo antes.

Algoritmo 3 Algoritmo de Euclides para encontrar el $mcd(f_1,\dots,f_s)$

```
Inicialización: f_1, f_2, ..., f_s
polin := [f_1, f_2, ..., f_s]
i := 1
j := longitud (polin)
m = mcd (polin[j − 1], polin[j])
WHILE i < j − 1 DO
    m = mcd (m, polin[(j − 1) − i])
    i := i + 1
RETURN m
```

Problema: *Problema de pertenencia al ideal en $K[x]$.*
Dados los polinomios $f_1,\dots,f_s \in K[x]$, ¿existe un algoritmo para saber si un polinomio cualquiera $f \in K[x]$ pertenece al ideal $\langle f_1,\dots,f_s\rangle$?

Solución:
Efectivamente existe un algoritmo para resolver este problema. Consiste en:

- Usar el algoritmo de Euclides para hallar el máximo común divisor de $f_1,\dots,f_s$, denotado por h. Por la propiedad (ii) de la Proposición 1.3, h genera el ideal $\langle f_1,\dots,f_s\rangle$.
- Por tanto, $f \in \langle f_1,\dots,f_s\rangle$ equivale a decir que $f \in \langle h\rangle$. Así que tenemos que usar el algoritmo de la división para poder escribir $f = qh + r$ con $grado(r) < grado(h)$.
- Entonces f pertenecerá al ideal si y solo si $r = 0$.

Entre otras cosas, en el siguiente capítulo resolveremos este mismo problema pero para polinomios definidos en varias variables, es decir $f_1,\dots,f_s \in K[x_1,\dots,x_n]$, utilizando una extrategia similar: encontraremos una buena base del ideal, que será concretamente una base de Gröbner, y utilizaremos el algoritmo de la división para determinar si un polinomio está en el ideal.

Capítulo 2

Bases de Gröbner

En este capítulo estudiaremos una generalización del algoritmo de la división en varias variables. También estudiaremos las bases de Gröbner e importantes resultados que nos ayudarán a encontrar dichas bases, las cuales nos permitirán resolver problemas sobre ideales de polinomios y variedades. Más concretamente, nos centraremos en estudiar y resolver estas cuatro cuestiones:

1. *Problema de la descripción del ideal*:
   ¿Los ideales $I \subseteq K[x_1,\dots,x_n]$ están formados por un conjunto finito de polinomios? O en otras palabras, ¿podemos escribir $I = \langle f_1,\dots,f_s\rangle$ para $f_i \in K[x_1,\dots,x_n]$?

2. *Problema de pertenencia al ideal*:
   Dado un polinomio $f \in K[x_1,\dots,x_n]$ consiste en decidir si $f \in I = \langle f_1,\dots,f_s\rangle$.

3. *Problema de resolución de un sistema de ecuaciones*:
   Consiste en encontrar todas las soluciones en K^n del sistema de ecuaciones polinómicas $f_1(x_1,\dots,x_n) = \cdots = f_s(x_1,\dots,x_n) = 0$.

4. *Problema de implicitación en ideales*:
   Queremos encontrar un sistema de ecuaciones (en $x_1,\dots,x_n$) cuyas soluciones son los puntos de la variedad $V \subseteq K^n$ dada por las ecuaciones paramétricas $x_1 = f_1(t_1,\dots,t_m),\dots,x_n = f_n(t_1,\dots,t_m)$ donde f_i son polinomios o funciones racionales en las variables t_j.

2.1. Orden monomial en varias variables

En esta sección vamos a estudiar las propiedades necesarias para ser capaces de ordenar (ascendente, o descendentemente) los términos de un polinomio en varias variables inequívocamente. Los conceptos explicados a continuación nos serán útiles cuando expliquemos el algoritmo de la división en $K[x_1,\dots,x_n]$.

Para la siguiente definición nos será de utilidad recordar que un conjunto posee orden total si dados tres elementos a,b,c se cumple la propiedad reflexiva, transitiva, antisimétrica y la de totalidad ($b \leq a$, o $a \leq b$).

Definición 11. Un *orden monomial* sobre $K[x_1,\dots,x_n]$ es cualquier relación $>$ en $\mathbb{Z}^n_{\geq 0}$, o equivalentemente cualquier relación en el conjunto de monomios $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$ satisfaciendo:

i) $>$ es un orden total (o lineal) en $\mathbb{Z}^n_{\geq 0}$.

ii) Si $\alpha > \beta$, $\gamma \in \mathbb{Z}^n_{\geq 0}$ entonces $\alpha+\gamma > \beta+\gamma$. Esto es equivalente a decir que si $x^\alpha > x^\beta$ y x^γ es cualquier monomio entonces se cumple $x^\alpha x^\gamma > x^\beta x^\gamma$.

iii) $>$ es un buen orden en $\mathbb{Z}^n_{\geq 0}$. Esto significa que si $A \subseteq \mathbb{Z}^n_{\geq 0}$ es no vacío, entonces existe $\alpha \in A$ tal que $\beta > \alpha$ para todo $\beta \neq \alpha$ en A.

El siguiente lema nos ayudará a entender mejor qué significa la condición iii). Además, lo usaremos para justificar que algunos algoritmos deben terminar en un número finito de pasos.

Lema 2.1. *Una relación de orden $>$ en $\mathbb{Z}^n_{\geq 0}$ se dice que es un buen orden si y solo si toda secuencia estrictamente decreciente en $\mathbb{Z}^n_{\geq 0}$ termina.*

Existe una gran variedad de órdenes monomiales. Veamos cómo se definen tres de ellos aunque el que nosotros utilizaremos para todo lo explicado posteriormente será el orden lexicográfico, el cual explicamos a continuación.

Definición 12. Sean $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Diremos que α posee un *orden lexicográfico* respecto a β (lo denotaremos mediante $\alpha >_{lex} \beta$) si en la diferencia $\alpha - \beta \in \mathbb{Z}^n$ la primera componente de más a la izquierda, no nula, es positiva. Si esto se cumple, escribiremos $x^\alpha >_{lex} x^\beta$.

Con esta definición de orden lexicográfico estamos ordenando los términos de un polinomio teniendo en cuenta los monomios de mayor grado. Sin embargo, puede darse el caso de querer ordenar dichos términos utilizando el grado total de los monomios. Es por ello por lo que definimos el siguiente orden monomial.

Definición 13. Sean $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Diremos que α posee un *orden lexicográfico graduado* respecto a β (lo denotaremos mediante $\alpha >_{grlex} \beta$) si

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

Otra forma de ordenar los monomios es utilizar el orden lexicográfico graduado inverso, el cual es menos intuitivo pero es el más eficiente computacionalmente hablando.

Definición 14. Sean $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Diremos que α posee un *orden lexicográfico graduado inverso* respecto a β (lo denotaremos mediante $\alpha >_{grvlex} \beta$) si

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

y en la diferencia $\alpha - \beta \in \mathbb{Z}^n$ la primera componente de más a la derecha, no nula, es negativa.

Ejemplo 3. Sea $f(x,y,z) = 3x^3 - 3y^2 + 4x^2z^4 + z^6$. Vamos a reescribir el polinomio ordenando sus términos, dependiendo del orden monomial usado con $x > y > z$.

- Orden lexicográfico. El término mayor es aquel cuya primera componente de más a la izquierda (al restar los vectores), no nula, sea positiva. Para ello, escribimos cada término de f como un vector de tres componentes donde cada una de ellas corresponde al exponente de la variable x, y, z respectivamente:

  $$x^3 \to (3,0,0) \qquad y^2 \to (0,2,0) \qquad x^2z^4 \to (2,0,4) \qquad z^6 \to (0,0,6)$$

  Así que $f(x,y,z) = 3x^3 + 4x^2z^4 - 3y^2 + z^6$.

- Orden lexicográfico graduado. El término mayor es aquel cuyo grado total es mayor, y si dos términos poseen el mismo grado entonces se utilizará el orden lexicográfico para ordenarlos. Entonces:

  $$grado(x^3) = 3 \qquad grado(y^2) = 2 \qquad grado(x^2z^4) = 6 \qquad grado(z^6) = 6$$

  Además $(2,0,4) >_{lex} (0,0,6)$ (hay que mirar el orden lexicográfico de esos dos términos ya que tienen el mismo grado). Así que $f(x,y,z) = 4x^2z^4 + z^6 + 3x^3 - 3y^2$.

- Orden lexicográfico graduado inverso. El término mayor es aquel cuyo grado es mayor, y si dos términos poseen el mismo grado entonces será mayor aquel que tenga la componente de más a la derecha (al restar los vectores), no nula y negativa. Entonces:

$$grado(x^3) = 3 \qquad grado(y^2) = 2 \qquad grado(x^2z^4) = 6 \qquad grado(z^6) = 6$$

Además $(2,0,4) - (0,0,6) = (2,0,-2)$ y vemos que la componente de más a la derecha no nula es negativa (hay que hacer la diferencia de esos dos ya que tienen el mismo grado) de modo que $(2,0,4) >_{grvlex} (0,0,6)$. Así que $f(x,y,z) = 4x^2z^4 + z^6 + 3x^3 - 3y^2$.

Usaremos la siguiente terminología.

Definición 15. Sea $f = \sum_{\alpha} a_\alpha x^\alpha$ un polinomio no nulo en $K[x_1,\ldots,x_n]$ y sea $>$ un orden monomial.

i) El *multigrado* de f obedece a la siguiente fórmula: $multigrado(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} \,|\, a_\alpha \neq 0)$.

ii) El *coeficiente principal* de f es el coeficiente correspondiente al monomio $x^{multigrado(f)}$. Lo denotaremos mediante $LC(f)$.

iii) El *monomio principal* de f es el monomio que es igual a $x^{multigrado(f)}$. Lo denotaremos mediante $LM(f)$.

iv) El *término principal* de f se denota mediante $LT(f) = LC(f) \cdot LM(f)$.

Ejemplo 4. Retomando el Ejemplo 3:

- Aplicando el orden lexicográfico habíamos obtenido $f(x,y,z) = 3x^3 + 4x^2z^4 - 3y^2 + z^6$. Entonces: $multigrado(f) = (3,0,0)$ y $LT(f) = 3 \cdot x^3 = 3x^3$.
- Aplicando tanto el orden lexicográfico graduado como el orden lexicográfico graduado inverso habíamos obtenido $f(x,y,z) = 4x^2z^4 + z^6 + 3x^3 - 3y^2$. Entonces: $multigrado(f) = (2,0,4)$ y $LT(f) = 4 \cdot x^2z^4 = 4x^2z^4$.

2.2. El algoritmo de la división en varias variables

En esta sección formularemos un algoritmo de la división en $K[x_1,\ldots,x_n]$ extendiendo el algoritmo de la división en una variable, estudiado en la Proposición 1.2, pero con una pequeña diferencia ya que ahora el resto no quedará determinado de forma única.

Teorema 2.2 (El algoritmo de la división en $K[x_1,\ldots,x_n]$)**.** *Sea $>$ un orden monomial en $\mathbb{Z}^n_{\geq 0}$ y sea $f = (f_1,\ldots,f_s)$ una s-tupla ordenada de polinomios en $K[x_1,\ldots,x_n]$. Entonces todo polinomio $f \in K[x_1,\ldots,x_n]$ se puede escribir como*

$$f = q_1f_1 + \cdots + q_sf_s + r$$

donde $q_i, r \in K[x_1,\ldots,x_n]$ y el resto verifica $r = 0$ o r es una combinación lineal de monomios con coeficientes en K tal que ninguno de ellos es divisible por ningún término principal $LT(f_1),\ldots,LT(f_s)$.

Tomamos como variables de entrada $f_1,\ldots,f_s,f$ y como variables de salida $q_1,\ldots,q_s,r$. A continuación, se muestra un algoritmo presentado en forma de pseudocódigo para hallar tales $q_1,\ldots,q_s,r$.

Algoritmo 4 Algoritmo de la división en varias variables

Inicialización: $q_1 := 0, \ldots, q_s := 0, r := 0, p := f$
WHILE $p \neq 0$ **DO**
  $i := 1$
  $division := falso$
  WHILE $i \leq s$ **AND** $ocurre\_division = falso$ **DO**
    IF $LT(f_i)$ divide a $LT(p)$ **THEN**
      $q_i := q_i + LT(p)/LT(f_i)$
      $p := p - (LT(p)/LT(f_i)) \cdot f_i$
      $ocurre\_division := verdad$
    ELSE
      $i := i + 1$
  WHILE $ocurre\_division = falso$ **THEN**
    $r := r + LT(p)$
    $p := p - LT(p)$

Ejemplo 5. Veamos un ejemplo de cómo funciona este algoritmo en $\mathbb{Q}[x,y]$. Queremos dividir el polinomio $f(x,y) = x^3y + x^2 + 2xy^2 + xy + x + y$ entre $f_1(x,y) = x^2y + 1$ y $f_2(x,y) = xy$ usando el orden lexicográfico $x > y$.

- Para comenzar, consideramos $q_1 = 0, q_2 = 0, r = 0, p = f$.
- Como $LT(f_1) = x^2y$ divide a $LT(p) = x^3y$ entonces podemos actualizar los valores de q_1 y p obteniendo $q_1 = x$, y $p = x^2 + 2xy^2 + xy + y$.
- Sin embargo ahora, $LT(p) = x^2$ no es dividido por $LT(f_1) = x^2y$ ni por $LT(f_2) = xy$. Entonces el algoritmo nos indica que x^2 pasa a formar parte del resto de la división. Actualizando, obtenemos $r = x^2$, y $p = 2xy^2 + xy + y$.
- Ahora, $LT(f_2) = xy$ sí divide a $LT(p) = 2xy^2$ y obtenemos los siguientes valores actualizados: $q_2 = 2y$, y $p = xy + y$.
- Como $LT(f_2) = xy$ divide a $LT(p) = xy$ entonces actualizando tenemos $q_2 = 2y + 1$, y $p = y$.
- Para finalizar, vemos que ni $LT(f_1) = x^2y$ ni $LT(f_2) = xy$ divide a $LT(p) = y$ de modo que y es parte del resto y así $r = x^2 + y$. En este caso tenemos $p = 0$, luego hemos terminado la división y el algoritmo finaliza.
- Recopilando todo, tenemos:

$$x^3y + x^2 + 2xy^2 + xy + x + y = (x)(x^2y + 1) + (2y + 1)(xy) + (x^2 + y).$$

Llegados a este punto podemos preguntarnos si los cocientes y el resto obtenidos pueden variar dependiendo del cuerpo de polinomios en el que trabajemos. Veamos con el siguiente ejemplo que efectivamente, el cuerpo es importante.

Ejemplo 6. Tomamos los polinomios f, f_1, f_2 del Ejemplo 5 con la diferencia de que ahora todos ellos están en el cuerpo finito $\mathbb{Z}_3[x,y]$. Al aplicar el algoritmo de la división y dividir f entre f_1 y f_2 usando el orden lexicográfico $x > y$ se obtiene:

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

También podemos obtener distintos cocientes $q_1, \ldots, q_s$ y distinto resto r dependiendo de cómo están ordenados los divisores $f_1, \ldots, f_s$. De modo que el Ejemplo 5 nos ayuda a entender porqué el algoritmo de la división en $K[x_1, \ldots, x_n]$ necesita que $f = (f_1, \ldots, f_s)$ sea una s-tupla ordenada de polinomios

usando un orden monomial y también nos ilustra que el resto no está determinado de manera única: Si dividimos f entre $[f_1, f_2]$ obtenemos $q_1 = x, q_2 = 2y+1, r = x^2+y$ (ver Ejemplo 5), mientras que si dividimos f entre $[f_2, f_1]$ obtenemos $q_1 = x^2+2y+1, q_2 = 0, r = x^2+x+y$.

Recalcar también que el algoritmo de la división depende fuertemente de la elección del orden monomial, es decir, los cocientes y el resto pueden variar dependiendo del orden monomial elegido.

Vimos en el primer capítulo, al final de la Sección 1.4, que una de las caraterísticas del algoritmo de la división en $K[x]$ es resolver el problema de pertenencia al ideal, obteniendo entonces que la condición $r = 0$ era una condición suficiente y necesaria para concluir que $f \in \langle f_1, \ldots, f_s \rangle$.
Ahora nos encontramos en la siguiente situación,

Problema: *Problema de pertenencia al ideal en $K[x_1, \ldots, x_n]$.*
Como hemos visto anteriormente, dado un polinomio $f \in K[x_1, \ldots, x_n]$, consiste en decidir si
$f \in I = \langle f_1, \ldots, f_s \rangle$.
¿Se puede hacer algo parecido al caso en una variable? ¿Existe algún algoritmo para resolverlo?

Solución:
Todavía no podemos resolverlo, ya que ahora la condición $r = 0$ es una condición suficiente pero no necesaria para afirmar que $f \in \langle f_1, \ldots, f_s \rangle$. Para solucionar este problema queremos encontrar un conjunto generador del ideal, en el que el resto se determine de forma única y en el que la condición $r = 0$ sea equivalente a pertenecer al ideal. Este conjunto será el que, posteriormente, llamaremos base de Gröbner. Para llegar hasta allí, necesitamos introducir previamente los conceptos y resultados de la siguiente sección.

2.3. Ideales monomiales

Definición 16. Un ideal $I \subseteq K[x_1, \ldots, x_n]$ se dice *ideal monomial* si existe un subconjunto $A \subseteq \mathbb{Z}^n_{\geq 0}$ tal que I está formado por todos los polinomios de la forma $\sum_{\alpha \in A} h_\alpha x^\alpha$ donde $h_\alpha \in K[x_1, \ldots, x_n]$. Lo denotaremos $I = \langle x^\alpha | \alpha \in A \rangle$.

Es decir, un ideal monomial se puede generar por monomios pero esto no quiere decir que todos los elementos del ideal sean monomios. Veamos un ejemplo de ideal que es monomial, y otro que no.

Ejemplo 7. $I = \langle xy + y^2, yx - y^2 \rangle$ es un ideal monomial y sin embargo $I' = \langle xy + y^2, x - y \rangle$ no lo es. En efecto:

- Llamamos $f_1 = xy + y^2$ y $f_2 = yx - y^2$. Entonces $\frac{1}{2}(f_1 + f_2) = xy \in I$ y $\frac{1}{2}(f_1 - f_2) = y^2 \in I$.

  Luego podemos escribir $\langle xy + y^2, yx - y^2 \rangle = \langle xy, y^2 \rangle$. De modo que I es un ideal generado por monomios, así que I es un ideal monomial.

- Llamamos $f_1 = xy + y^2$ y $f_2 = x - y$. Entonces $yf_2 + f_1 = 2xy \in I$ y $yf_2 - f_1 = 2y^2 \in I$.

  Luego podemos escribir $\langle xy + y^2, x - y \rangle = \langle xy, y^2, x - y \rangle$ y ver así que I' no se puede generar por monomios. Luego I' no es un ideal monomial.

Lema 2.3. *Sea $I = \langle x^\alpha | \alpha \in A \rangle$ un ideal monomial. Entonces un monomio x^β pertenece a I si y solo si x^β es divisible por x^α para algún $\alpha \in A$.*

Lema 2.4. *Sea I un ideal monomial y sea $f \in K[x_1, \ldots, x_n]$. Entonces las siguientes afirmaciones son equivalentes:*

i) $f \in I$.

ii) Todo término de f está en I.

iii) f es una combinación lineal en el cuerpo K de monomios de I.

Colorario 2.5. *Dos ideales monomiales son iguales si y solo si contienen los mismos monomios.*

A continuación, se enuncia y demuestra el Lema de Dickson ya que tendrá gran importancia en resultados teóricos posteriores.

Teorema 2.6 (Lema de Dickson)**.** *Todo ideal monomial $I = \langle x^\alpha | \alpha \in A \rangle$ se puede escribir como $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, donde los enteros $\alpha(i) \in A$, $\forall i = 1, \ldots, s$. En particular, I tiene una base finita.*

Demostración. Procedamos por inducción sobre el número de variables, n.

- Sea $n = 1$. Entonces I está finitamente generado en $K[x_1]$ por los monomios x_1^α, donde $\alpha \in A \subseteq \mathbb{Z}_{\geq 0}$. Esto es porque tomando $\beta \leq \alpha$ como el menor elemento de A entonces x_1^β divide a todo x_1^α y así, por el Lema 2.3, $I = \langle x_1^\beta \rangle$.

- Supongamos que es cierto para $n-1$ (con $n > 1$) y veamos si se cumple el resultado para n. Asumimos la siguiente notación: escribiremos las variables como $x_1, \ldots, x_{n-1}, y$ de modo que los monomios en $K[x_1, \ldots, x_{n-1}, y]$ se escribirán como $x^\alpha y^m$ con $\alpha \in \mathbb{Z}_{\geq 0}^{n-1}$, $m \in \mathbb{Z}_{\geq 0}$.
  Supongamos que $I \subseteq K[x_1, \ldots, x_{n-1}, y]$ es un ideal monomial. Para encontrar los generadores de I, definimos $J \subseteq K[x_1, \ldots, x_{n-1}]$ como un ideal generado por los monomios x^α tales que $x^\alpha y^m \in I$ para algún $m \geq 0$. Es decir,

  $$J = \langle x^\alpha \in K[x_1, \ldots, x_{n-1}] \,|\, x^\alpha y^m \in I, m \geq 0 \rangle.$$

  Por ser J un ideal monomial en $K[x_1, \ldots, x_{n-1}]$, aplicando la hipótesis de inducción existirá un número finito de generadores de modo que tenemos $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, con $\alpha(i) \in A$.
  Para cada $1 \leq i \leq s$, por definición de J, se cumple $x^{\alpha(i)} y^{m_i} \in I$ para algún $m_i \geq 0$. Sea m el máximo de los m_i. Entonces para cada $0 \leq k \leq m-1$ consideramos $J_k \subseteq K[x_1, \ldots, x_{n-1}]$ como un ideal generado por los monomios x^β tales que $x^\beta y^k \in I$. Es decir,

  $$J_k = \langle x^\beta \in K[x_1, \ldots, x_{n-1}] \,|\, x^\beta y^k \in I, 0 \leq k \leq m-1 \rangle.$$

  Aplicando de nuevo la hipótesis de inducción tenemos $J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)} \rangle$, o equivalentemente, J_k está generado por un número finito de monomios.
  Veamos que I está generado por los siguientes monomios:

  $$\begin{aligned}
  &\text{procedentes de } J : x^{\alpha(1)} y^m, \ldots, x^{\alpha(s)} y^m \\
  &\text{procedentes de } J_0 : x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)} \\
  &\text{procedentes de } J_1 : x^{\alpha_1(1)} y, \ldots, x^{\alpha_1(s_1)} y \\
  &\quad \vdots \\
  &\text{procedentes de } J_{m-1} : x^{\alpha_{m-1}(1)} y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1}.
  \end{aligned}$$

  Tenemos que cada monomio de I es divisible por alguno de la lista anterior. En efecto, tomamos $x^\alpha y^p \in I$:

  - Si $p \geq m$ entonces $x^\alpha y^p$ es divisible por algún $x^{\alpha(i)} y^m$ debido a la construcción de J.
  - Si $p \leq m-1$ entonces $x^\alpha y^p$ es divisible por algún $x^{\alpha_p(j)} y^p$ debido a la construcción de J_p.

Así que por el Lema 2.3 tenemos que la lista anterior de monomios genera un ideal con los mismos monomios que I, y por el Corolario 2.5 se tiene que ambos ideales son el mismo.
Por último, veamos que el conjunto finito de generadores se puede escoger de los generadores del ideal. Denotando ahora las variables como $x_1,\dots,x_n$, entonces $I = \langle x^\alpha | \alpha \in A\rangle$ es nuestro ideal monomial. Queremos ver que I está generado por un número finito de x^α's, con $\alpha \in A$. Hemos visto que $I = \langle x^{\beta(1)},\dots,x^{\beta(s)}\rangle$ para ciertos monomios $x^{\beta(i)} \in I$, $i = 1,\dots,s$. Como $x^{\beta(i)} \in I$, por el Lema 2.3 se tiene que cada $x^{\beta(i)}$ es divisible por $x^{\alpha(i)}, \alpha(i) \in A$. Por doble contenido se ve fácilmente que $I = \langle x^{\alpha(1)},\dots,x^{\alpha(s)}\rangle$ completando así la demostración.

□

Una de las consecuencias del Lema de Dickson es que dadas las dos primeras condiciones de la Definición 11, la condición iii) tiene un equivalente. Veámoslo:

Colorario 2.7. *Sea $>$ una relación de orden en $\mathbb{Z}^n_{\geq 0}$ cumpliendo:*

i) $>$ es un orden total en $\mathbb{Z}^n_{\geq 0}$.

ii) Si $\alpha > \beta$, $\gamma \in \mathbb{Z}^n_{\geq 0}$ entonces $\alpha + \gamma > \beta + \gamma$.

Entonces $>$ es un buen orden si y solo si $\alpha \geq 0$ para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$.

2.4. El Teorema de las bases de Hilbert y bases de Gröbner

En esta sección se darán resultados teóricos los cuales servirán para dar una solución al problema de la descripción del ideal explicado al principio de este capítulo. La idea principal es que dado un orden monomial, todo polinomio no nulo tiene un único término principal. Entonces para cualquier ideal I podemos definir su *ideal de términos principales* de la siguiente manera.

Definición 17. Sea $I \subseteq K[x_1,\dots,x_n]$ un ideal distinto del nulo. Entonces, una vez fijado un orden monomial en $K[x_1,\dots,x_n]$:

i) Denotaremos mediante $LT(I)$ al conjunto de todos los términos principales de todos los elementos de I que sean no nulos. Es decir,

$$LT(I) = \{cx^\alpha \,|\, \text{existe } f \in I\setminus\{0\} \text{ tal que } LT(f) = cx^\alpha\}.$$

ii) Denotaremos mediante $\langle LT(I)\rangle$ al ideal generado por los elementos del conjunto $LT(I)$.

Proposición 2.8. *Sea $I \subseteq K[x_1,\dots,x_n]$ un ideal distinto del nulo, entonces*

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

ii) Existen $g_1,\dots,g_t \in I$ tales que se cumple la igualdad $\langle LT(I)\rangle = \langle LT(g_1),\dots,LT(g_t)\rangle$.

Para probar el siguiente resultado, haremos uso de la Proposición 2.8 y del Teorema 2.2 (algoritmo de la división), dando así una respuesta afirmativa al problema de la descripción del ideal explicado al principio de este capítulo.

Teorema 2.9 (Teorema de las bases de Hilbert)**.** *Todo ideal $I \subseteq K[x_1,\dots,x_n]$ está finitamente generado. En otras palabras, $I = \langle g_1,\dots,g_t\rangle$ con $g_1,\dots,g_t \in I$.*

Demostración.

- Si $I = \{0\}$, como $\{0\}$ es un generador de I y es un conjunto finito entonces se tiene el resultado.

- Si $I \neq \{0\}$, entonces un conjunto generador $g_1,\ldots,g_t$ de I se puede construir de la siguiente manera:
  Como I tiene un ideal de términos principales, por la Proposición 2.8 existen $g_1,\ldots,g_t \in I$ tales que $\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$. Comprobemos ahora que, efectivamente, $I = \langle g_1,\ldots,g_t\rangle$. Para ello, procedamos por doble contenido:

  - Dado que todo $g_i \in I$, es claro que $\langle g_1,\ldots,g_t\rangle \subseteq I$.
  - Sea $f \in I$ un polinomio cualquiera. Fijado un orden monomial, se aplica el algoritmo de la división en varias variables para dividir f por $[g_1,\ldots,g_t]$ y obtenemos

    $$f = q_1g_1 + \cdots + q_tg_t + r$$

    donde ningún término de r es divisible por ningún $LT(g_i), i = 1,\ldots,t$. Veamos que $r = 0$. Para ello procedamos por reducción al absurdo suponiendo $r \neq 0$. En tal caso $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$ (ya que $r = f - q_1g_1 - \cdots - q_tg_t \in I$) y por el Lema 2.3 se tiene que $LT(r)$ debe ser divisible por algún $LT(g_i), i = 1,\ldots,t$. Como esto contradice la afirmación anterior de que ningún término de r es divisible por ningún $LT(g_i)$, se tiene $r = 0$. Por lo tanto $f = q_1g_1 + \cdots + q_tg_t + 0 \in \langle g_1,\ldots,g_t\rangle$, completando así la demostración del segundo contenido $I \subseteq \langle g_1,\ldots,g_t\rangle$.

  Luego, por doble contenido, $I = \langle g_1,\ldots,g_t\rangle$.

□

Definición 18. Dado un orden monomial, un subconjunto finito $G = \{g_1,\ldots,g_t\}$ de un ideal $I \subseteq K[x_1,\ldots,x_n]$ se dirá *base de Gröbner* si

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

De una manera menos formal, un conjunto $\{g_1,\ldots,g_t\} \subseteq I$ es una base de Gröbner de I si y solo si el término principal de cada elemento de I es divisible por alguno de los $LT(g_i)$, para $i = 1,\ldots,t$.

Por convenio se tiene $\langle\emptyset\rangle = \{0\}$. Definimos entonces el conjunto vacío $\emptyset$ como la base de Gröbner del ideal nulo $\{0\}$.

Colorario 2.10. *Dado un orden monomial, todo ideal $I \subseteq K[x_1,\ldots,x_n]$ tiene una base de Gröbner. Es más, cualquier base de Gröbner de un ideal I es una base de I.*

Veamos una consecuencia geométrica del Teorema 2.9 bastante importante, ya que luego nos permitirá resolver sistemas de ecuaciones en varias variables de una forma sencilla.

Definición 19. Sea $I \subseteq K[x_1,\ldots,x_n]$ un ideal. Denotaremos mediante $\mathbf{V}(I)$ al conjunto

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

Proposición 2.11. *El conjunto $\boldsymbol{V}(I)$ es una variedad afín. En particular, si $I = \langle f_1,\ldots,f_s\rangle$, entonces $\boldsymbol{V}(I) = \boldsymbol{V}(f_1,\ldots,f_s)$.*

A continuación, veamos que, al aplicar el algoritmo de la división en varias variables, el resto de la división es único cuando los divisores forman una base de Gröbner.

Proposición 2.12. *Fijado un orden monomial, sea $G = \{g_1,\ldots,g_t\}$ una base de Gröbner del ideal $I \subseteq K[x_1,\ldots,x_n]$ y sea $f \in K[x_1,\ldots,x_n]$. Entonces existe un resto único $r \in K[x_1,\ldots,x_n]$ que cumple las dos siguientes propiedades:*

i) Ningún término de r es divisible por $LT(g_i)$, para $i = 1,\ldots,t$.

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

En particular, r es el resto de la división de f entre G sin importar el orden de los elementos de G.

Colorario 2.13. *Sea $G = \{g_1,\ldots,g_t\}$ una base de Gröbner del ideal $I \subseteq K[x_1,\ldots,x_n]$ y sea $f \in K[x_1,\ldots,x_n]$. Entonces $f \in I$ si y solo si el resto de la división de f entre G es cero.*

2.5. Criterio y algoritmo de Buchberger

A partir de ahora escribiremos $\bar{f}^F$ para denotar el resto de la división del polinomio f entre la s-tupla ordenada $F = (f_1, \ldots, f_s)$. Si F es una base de Gröbner para el ideal $\langle f_1, \ldots, f_s \rangle$ entonces la s-tupla F no es necesario que esté ordenada.

Ejemplo 8. Dividiendo $f = x^4y^2$ por $F = (xy-1, y^2-1) \subseteq K[x,y]$, utilizando el orden lexicográfico $(x > y)$, obtenemos

$$\overline{x^4y^2}^F = x^2$$

ya que mediante el algoritmo de la división se tiene

$$x^4y^2 = (x^3y + x^2) \cdot (xy-1) + (0) \cdot (y^2-1) + x^2.$$

A continuación, veremos el criterio de Buchberger, el cual nos ayudará a saber si el generador de un ideal dado es una base Gröbner o no. Para ello necesitamos introducir previamente dos definiciones.

Definición 20. Sean $f, g \in K[x_1, \ldots, x_n]$ polinomios no nulos. Si $multigrado(f) = \alpha$ y $multigrado(g) = \beta$, sea $\gamma = (\gamma_1, \ldots, \gamma_n)$ donde $\gamma_i = \max(\alpha_i, \beta_i)$ para cada $i = 1, \ldots, n$. Llamaremos x^γ al *mínimo común múltiplo* de $LM(f)$ y $LM(g)$, es decir, $x^\gamma = mcm(LM(f), LM(g))$.

Definición 21. Sean $f, g \in K[x_1, \ldots, x_n]$ polinomios no nulos. Definimos el *S-polinomio* de f y g como

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

Ahora ya sí podemos enunciar el siguiente resultado, el cual como ya hemos explicado, sirve para saber cuándo una base de un ideal es una base de Gröbner.

Teorema 2.14 (Criterio de Buchberger)**.** *Sea I un ideal de polinomios. Entonces una base $G = \{g_1, \ldots, g_t\}$ de I es una base de Gröbner de $I \Leftrightarrow \overline{S(g_i, g_j)}^G = 0$, $\forall i, j$ tales que $i \neq j$.*

Demostración. Ver [5, Capítulo 2, Sección 6]. □

Ejemplo 9. Sea $I = \langle x^2 - y^2 + z, z - 1 \rangle$. Veamos que $G = \{x^2 - y^2 + z, z - 1\}$ es una base de Gröbner para I utilizando el orden lexicográfico habitual $(x > y > z)$.
Denotamos $g_1 = x^2 - y^2 + z$ y también $g_2 = z - 1$. Entonces $LT(g_1) = x^2$, $LT(g_2) = z$ y $x^\gamma = x^2 z$ (ya que $multigrado(g_1) = (2,0,0)$ y $multigrado(g_2) = (0,0,1)$). De este modo

$$S(g_1, g_2) = \frac{x^2 z}{x^2} \cdot g_1 - \frac{x^2 z}{z} \cdot g_2 = x^2 - y^2 z + z^2.$$

Ahora, aplicando el algoritmo de la división obtenemos

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

Por lo tanto

$$\overline{S(g_1, g_2)}^G = 0.$$

Así que por el criterio de Buchberger se tiene que G es una base de Gröbner para I.

Ya hemos visto en el Corolario 2.10 que todo ideal tiene una base de Gröbner. Además, gracias al Teorema 2.14 (criterio de Buchberger) ya sabemos ver si una base dada es una base de Gröbner o no. Pero dado un ideal $I \subseteq K[x_1, \ldots, x_n]$, ¿podemos construir nosotros una base de Gröbner para I? La respuesta a esto es que sí. Para ello utilizaremos el siguiente algoritmo.

Teorema 2.15 (Algoritmo de Buchberger)**.** *Sea $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ un ideal de polinomios. Entonces podemos construir una base de Gröbner $G = \{g_1, \ldots, g_t\}$ de I en un número finito de pasos utilizando el siguiente algoritmo:*

Algoritmo 5 Algoritmo de Buchberger

Inicialización: $F = (f_1, \ldots, f_s)$
$G := F$
REPEAT
  $G' := G$
  FOR cada par $\{p, q\}, p \neq q$ en G' **DO**
    $r := \overline{S(p,q)}^{G'}$
    IF $r \neq 0$ **THEN** $G := G \cup \{r\}$
UNTIL $G = G'$
RETURN G

Por lo tanto, usando el criterio de Buchberger y el algoritmo de Buchberger hemos conseguido un método para obtener bases de Gröbner. Pero estas bases, habitualmente tienen más elementos de los necesarios. Veamos que podemos eliminar alguno utilizando el siguiente lema.

Lema 2.16. *Sea G una base de Gröbner de $I \subseteq K[x_1, \ldots, x_n]$ y sea $p \in G$ un polinomio tal que $LT(p) \in \langle LT(G \setminus \{p\})\rangle$. Entonces $G \setminus \{p\}$ es también una base de Gröbner de I.*

Ejemplo 10. Consideramos el anillo de polinomios $\mathbb{Q}[x,y,z]$ con el orden lexicográfico habitual ($x > y > z$) y sea $I = \langle f_1, f_2\rangle = \langle x^2 + y, x^3 + z\rangle$.
Lo primero es ver que $F = \{f_1, f_2\}$ no es una base de Gröbner:
Como $LT(S(f_1, f_2)) = xy \notin \langle LT(f_1), LT(f_2)\rangle = \langle x^2, x^3\rangle$, entonces el criterio de Buchberger nos garantiza que F no es una base de Gröbner de I.
Vamos a construir una base de Gröbner, a partir de F, utilizando el algoritmo de Buchberger.
Iniciamos el algoritmo y así $G' = F$. Ahora, dividiendo $S(f_1, f_2) = xy - z$ por F obtenemos como resto $f_3 = xy - z$, el cual es no nulo. Por lo tanto debemos actualizar nuestra base $G' = \{f_1, f_2, f_3\}$. Entonces,

$$\overline{S(f_1, f_2)}^{G'} = \overline{S(f_2, f_3)}^{G'} = 0,$$

$$\overline{S(f_1, f_3)}^{G'} = xz + y^2 \neq 0.$$

Por lo tanto, añadiendo $f_4 = xz + y^2$, $G' = \{f_1, f_2, f_3, f_4\}$. Ahora,

$$\overline{S(f_1, f_2)}^{G'} = \overline{S(f_1, f_3)}^{G'} = \overline{S(f_1, f_4)}^{G'} = \overline{S(f_2, f_3)}^{G'} = 0,$$

$$\overline{S(f_3, f_4)}^{G'} = -y^3 - z^2 \neq 0.$$

Así que tenemos una nueva $G' = \{f_1, f_2, f_3, f_4, f_5\}$, siendo $f_5 = -y^3 - z^2$, para la cual se cumple

$$\overline{S(f_i, f_j)}^{G'} = 0, \ \forall\, 1 \leq i < j \leq 5.$$

Así, por el criterio de Buchberger tenemos que $G = \{f_1, f_2, f_3, f_4, f_5\}$ es una base de Gröbner de I con respecto al orden lexicográfico.
Notar ahora que $LT(f_2) = x \cdot LT(f_1)$. Así que por el Lema 2.16 podemos prescindir de f_2 en nuestra nueva base de Gröbner. Como no hay más casos en los que el término principal de un generador divida al término principal de otro generador, entonces la mínima base de Gröbner que podemos obtener es:

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

Definición 22. Una *base de Gröbner minimal* de un ideal de polinomios $I \subseteq K[x_1, \ldots, x_n]$ es una base de Gröbner G de I la cual cumple:

i) $\forall p \in G, LC(p) = 1$.

ii) $\forall p \in G, LT(p) \notin \langle LT(G \setminus \{p\})\rangle$.

Desafortunadamente el ideal I inicial puede tener varias bases de Gröbner minimales, ya que por ejemplo tomando $\tilde{f}_1 = x^2 + y + az$ con $a \in \mathbb{Q}$ también sería $G = \{\tilde{f}_1, f_3, f_4, f_5\}$ una base de Gröbner minimal. Pero afortunadamente hay una base minimal que es mejor que el resto. Su definición es la siguiente.

Definición 23. Una *base de Gröbner reducida* de un ideal de polinomios $I \subseteq K[x_1, \ldots, x_n]$ es una base de Gröbner G de I la cual cumple:

i) $\forall p \in G, LC(p) = 1$.

ii) $\forall p \in G$, ningún monomio de p está en $\langle LT(G \setminus \{p\})\rangle$.

Teorema 2.17. *Sea I un ideal de polinomios no nulo. Entonces, para un orden monomial dado, I tiene una única base de Gröbner reducida.*

Demostración. Introduzcamos la siguiente definición: Diremos que $g \in G$, G base de Gröbner minimal de I, es un elemento reducido respecto de G si ningún monomio de g pertenece a $\langle LT(G)\setminus\{p\}\rangle$ con $p \in G$. Notar que si g es un elemento reducido respecto de G entonces g también es reducido respecto cualquier otra base de Gröbner minimal de I que contenga a g y que tenga los mismos términos principales.

El objetivo para ver la existencia de una base de Gröbner reducida es partir de una base de Gröbner minimal G y modificarla hasta que todos sus elementos sean elementos reducidos.

Dado $g \in G$ un elemento reducido respecto de G, tomamos $g' = \overline{g}^{G\setminus\{g\}}$ y $G' = (G\setminus\{g\}) \cup \{g'\}$. Veamos que G' es una base de Gröbner minimal de I. Para ello notar que $LT(g') = LT(g)$ ya que al dividir g entre $G\setminus\{g\}$, necesariamente $LT(g)$ pasa a formar parte del resto porque no es divisible por ningún elemento de $LT(G\setminus\{g\})$. Así tenemos que $\langle LT(g')\rangle = \langle LT(g)\rangle$. Como claramente $G' \subseteq I$ tenemos que G' es una base de Gröbner minimal de I. Además, g' es un elemento reducido de G' por construcción. Ahora tomamos los elementos de G y aplicamos el procedimiento anterior hasta que todo elemento sea reducido, obteniendo así una base de Gröbner reducida.

Queda por probar la unicidad de esta base de Gröbner reducida, la cual acabamos de ver que existe. Sean G y $\tilde{G}$ dos bases de Gröbner reducidas de I. En particular G y $\tilde{G}$ son también bases de Gröbner minimales de I, luego $LT(G) = LT(\tilde{G})$. Entonces dado $g \in G$, existirá un $\tilde{g} \in \tilde{G}$ tal que $LT(g) = LT(\tilde{g})$. Así que si probamos $g = \tilde{g}$ entonces $G = \tilde{G}$ y la unicidad estará probada. Para ver que $g = \tilde{g}$, consideremos el polinomio $g - \tilde{g}$, el cual está en I. Como G es una base de Gröbner se sigue que $\overline{g-\tilde{g}}^{G} = 0$. También, como $LT(g) = LT(\tilde{g})$ entonces ambos se cancelan al efectuar la resta $g - \tilde{g}$ y el resto de términos no son divisibles por ninguno de los $LT(g) = LT(\tilde{g})$ ya que G y $\tilde{G}$ son bases de Gröbner reducidas. Se sigue que $\overline{g-\tilde{g}}^{G} = g - \tilde{g}$ y por lo anterior $g - \tilde{g} = 0$, luego $g = \tilde{g}$ completando así la demostración. □

El siguiente resultado, a pesar de estar categorizado como corolario tendrá gran relevancia en los dos capítulos posteriores. Tener en cuenta que un cuerpo K se dice *algebraicamente cerrado* si cada polinomio de grado al menos 1, con coeficientes en K, tiene un cero en K.

Colorario 2.18. *Sea K un cuerpo algebraicamente cerrado. Dado un ideal $I \subseteq K[x_1, \ldots, x_n]$ y dada G una base de Gröbner reducida de I entonces $\mathbf{V}(I) = \emptyset$ si y solo si $G = \{1\}$.*

2.6. Aplicaciones de las bases de Gröbner

En esta sección vamos a resolver, utilizando las bases de Gröbner, los problemas sobre ideales y variedades enumerados y brevemente explicados al principio de este segundo capítulo.

1. *Problema de la descripción del ideal.*
   Ya se explicó que este problema consiste en saber si los ideales $I \subseteq K[x_1,\dots,x_n]$ están formados por un conjunto finito. Lo resolvimos utilizando el Teorema 2.9, ya que este resultado afirma que todo ideal está finitamente generado.

2. *Problema de pertenencia al ideal.*
   Dado un ideal $I = \langle f_1,\dots,f_s\rangle \subseteq K[x_1,\dots,x_n]$ podemos saber si un polinomo f pertenece a I de la siguiente manera:

   - Encontrar una base de Gröbner $G = \{g_1,\dots,g_t\}$ de I utilizando el Teorema 2.15 (algoritmo de Buchberger).
   - Por el Corolario 2.13 podemos afirmar que $f \in I \Leftrightarrow \overline{f}^G = 0$.

3. *Problema de resolución de un sistema de ecuaciones.*
   Veamos cómo podemos aplicar las bases de Gröbner para resolver sistemas de ecuaciones en varias variables:

   - Si encontramos una base de Gröbner de un ideal, con respecto al orden lexicográfico, la forma de las ecuaciones se simplifica bastante, ya que las variables se van eliminando sucesivamente. Un sistema de ecuaciones de esta forma es mucho más fácil de resolver.
   - Por la Proposición 2.11, la cual dice que las variedades afines están determinadas por ideales, se tiene que las soluciones obtenidas con el procedimiento anterior, son todas las que existen.

4. *Problema de implicitación en ideales.*
   El problema de encontrar un sistema de ecuaciones cuyas soluciones sean los puntos de una variedad puede resolverse utilizando nuevamente las bases de Gröbner. Veamos cómo:

   - Consideramos las ecuaciones paraméticas

   $$\begin{aligned} x_1 &= f_1(t_1,\dots,t_m),\\ &\vdots\\ x_n &= f_n(t_1,\dots,t_m), \end{aligned}$$

   las cuales definen un subconjunto de una variedad $\mathbf{V} \subseteq K^n$. Nos centramos en el caso de que f_i sean realmente polinomios. Consideramos la siguiente variedad afín en K^{m+n}

   $$\begin{aligned} x_1 - f_1(t_1,\dots,t_m) &= 0,\\ &\vdots\\ x_n - f_n(t_1,\dots,t_m) &= 0. \end{aligned}$$

   La idea es eliminar las variables $t_1,\dots,t_m$ de esas ecuaciones. Para ello tenemos que obtener una base de Gröbner.

   - Supongamos que hemos obtenido una base de Gröbner para el ideal $I = \langle x_1 - f_1,\dots,x_n - f_n\rangle$ con respecto al orden lexicográfico ($t_1 > \cdots > t_m > x_1 > \cdots > x_n$). Entonces los polinomios de la base de Gröbner que solo involucran las variables $x_1,\dots,x_n$ son las soluciones del sistema de ecuaciones.

Capítulo 3

Coloreado de grafos

En este capítulo vamos a definir el concepto de grafo simple, al cual llamaremos grafo, y veremos cómo aplicar las bases de Gröbner a la Teoría de grafos, en particular daremos una solución al problema del k-coloreado en un grafo.

Definición 24. Un *grafo* $\mathcal{G}$ es un par $\mathcal{G} = (V, E)$, donde V es un conjunto finito de puntos, llamados *vértices*, y E es un conjunto de pares no ordenados de vértices, llamadas *aristas* del grafo. Además diremos que dos vértices son *adyacentes* si ambos son extremos de la misma arista.

Definición 25. Un *camino* entre dos vértices u_1 y u_t es una sucesión de aristas de la forma $\{u_1, u_2\}, \{u_2, u_3\}, \ldots, \{u_{t-1}, u_t\}$ que une los vértices u_1 y u_t.

Definición 26. Sea $\mathcal{G} = (V, E)$ un grafo. Se dice que $\mathcal{G}$ es un *grafo conexo* si para todo par $u, v \in V$ siempre existe un camino que une u y v.

Definición 27. Sea $\mathcal{G}$ un grafo conexo con vértices $V = \{1, \ldots, n\}$ y aristas $E = \{1, \ldots, m\}$. Sea C un conjunto finito cuyos elementos llamaremos colores. Una *coloración* de $\mathcal{G}$ es una correspondencia tal que a cada uno de los vértices de $\mathcal{G}$ se le asigna un color de C de manera que dos vértices adyacentes no pueden recibir el mismo color. Formalmente, una coloración de $\mathcal{G}$ es una aplicación $\gamma : V \longrightarrow C$ tal que $\gamma(u) \neq \gamma(v)$ si existe una arista de $\mathcal{G}$ que une u y v. El valor de $\gamma(u)$ es el color que recibe el vértice u en la coloración γ.

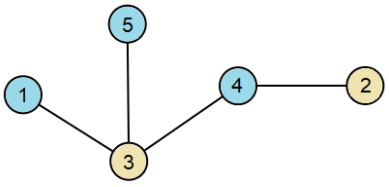
Definición 28. Una coloración de un grafo $\mathcal{G}$ con k colores ($k \geq 1$) se llama *k-coloración* de $\mathcal{G}$.

Definición 29. Diremos que un grafo $\mathcal{G}$ es *k-coloreable* si existe una k-coloración asignada.

Observar que si $\mathcal{G}$ es k-coloreable inmediatamente se tiene que $\mathcal{G}$ es también $(k+1)$-coloreable. Notar también que si n es el número de vértices entonces $\mathcal{G}$ es n-coloreable.

Definición 30. El *número cromático* de un grafo $\mathcal{G}$ se define como el mínimo valor $k \in \mathbb{N}$ tal que $\mathcal{G}$ es k-coloreable y se denota por $\chi(\mathcal{G})$. Si $k = \chi(\mathcal{G})$ se dice que el grafo es *k-cromático*.

Ejemplo 11. Sea $\mathcal{G}$ un grafo conexo formado por 5 vértices, luego $V = \{1, 2, 3, 4, 5\}$, y por 4 aristas, luego $E = \{\{1, 3\}, \{2, 4\}, \{3, 4\}, \{3, 5\}\}$. Este grafo es claramente 5-coloreable ya que tiene 5 vértices. Sin embargo, $\chi(\mathcal{G}) = 2$ y así $\mathcal{G}$ es 2-coloreable.



Ahora que tenemos claras las definiciones anteriores, vamos a explicar en qué consiste el problema que queremos resolver usando bases de Gröbner.

1. *Problema del k-coloreado en un grafo*:
   Sea $\mathcal{G} = (V,E)$ un grafo. Entonces el problema del k-coloreado en un grafo busca que el grafo sea k-coloreable, es decir, ver que existe una aplicación $\gamma : V \longrightarrow C_k = \{c_1,\ldots,c_k\}$ tal que si $\{u,v\} \in E$ entonces $\gamma(u) \neq \gamma(v)$.

3.1. Resolución del problema del k-coloreado

Para resolver el problema del k-coloreado en un grafo utilizaremos un sistema de ecuaciones polinómicas. A continuación se explica cómo obtener las ecuaciones del sistema y veremos un ejemplo práctico. Si el lector tiene interés en conocer los detalles, ver [2].

Consideramos un grafo con n vértices. Sea x_i la variable asignada al vértice $i \in V$ y sea c_t el elemento asignado a cada color. Consideremos el conjunto $\{c_t : 1 \leq t \leq k\} \subseteq K$, con K cuerpo y con $k \leq i$. Como este ha de ser algebraicamente cerrado, para poder aplicar luego la Proposición 2.18, tendría que ser $K = \mathbb{C}$. Sin embargo, como los polinomios con los que vamos a trabajar tienen coeficientes en $\mathbb{Q}$, podemos en realidad considerar el cuerpo de los racionales $K = \mathbb{Q}$.

Definimos las dos siguientes funciones:

$$f(x) = \prod_{t=1}^{k}(x - c_t),\ g(x,y) = \frac{f(x) - f(y)}{x - y}.$$

Vamos a ver qué condiciones necesitamos y cómo escribirlas matemáticamente para obtener así nuestro sistema de ecuaciones polinómicas.

- Queremos que todos nuestros vértices estén coloreados. Por la definición de f, si $f(x_i) = 0$ se tiene entonces $x_i = c_t$, o lo que es lo mismo, a cada vértice se le asigna un color. De modo que:

  $$f(x_i) = 0,\ \forall i \in \{1,\ldots,n\}.$$

  La función $f(x_i)$ es un producto de polinomios ya que es de la forma $f(x_i) = (x_i - c_1)\cdots(x_i - c_k)$, y el producto de polinomios es un polinomio. Luego, $f(x_i)$ es un polinomio en la variable x_i. Como $K[x_i] \subseteq K[x_1,\ldots,x_n]$ entonces $f(x_i)$ es un polinomio en las variables $x_1,\ldots,x_n$.

- Además queremos que no haya dos vértices conectados por la misma arista y que tengan el mismo color, es decir, que todo par de vértices conectados por una arista tengan colores diferentes. Por las definiciones de f y g, si $g(x_i,x_j) = 0$ se tiene entonces $f(x_i) - f(x_j) = 0$ (luego cada vértice tiene un color asignado) y $x_i - x_j \neq 0$ (luego son colores distintos). De modo que:

  $$g(x_i,x_j) = 0,\ \text{si}\{i,j\} \in E.$$

  Sabemos que $g(x_i,x_j)$ es un polinomio en el anillo de polinomios $K[x_1,\ldots,x_n]$ porque como $f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$, podemos escribir

  $$g(x_i,x_j) = \frac{x_i^k - x_j^k}{x_i - x_j} + \frac{a_{k-1}x_i^{k-1} - a_{k-1}x_j^{k-1}}{x_i - x_j} + \cdots + \frac{a_1x_i - a_1x_j}{x_i - x_j} + \frac{a_0 - a_0}{x_i - x_j}.$$

  Entonces para cualquier fracción $\dfrac{a_m(x_i^m - x_j^m)}{x_i - x_j}$ sabemos que $(x_i^m - x_j^m) = (x_i - x_j)(x_i^{m-1} + x_i^{m-2}x_j + \cdots + x_j^{m-1})$. Por lo tanto $\dfrac{a_m(x_i^m - x_j^m)}{x_i - x_j} = a_m(x_i^{m-1} + x_i^{m-2}x_j + \cdots + x_j^{m-1})$.

De modo que nuestro sistema de ecuaciones polinómicas, para resolver el problema del k-coloreado, es el siguiente

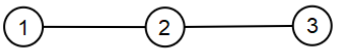
$$\begin{cases} f(x_i) = 0, \ \forall i \in \{1, \dots, n\} \\ g(x_i, x_j) = 0, \ \text{si} \ \{i, j\} \in E. \end{cases} \tag{3.1}$$

Por el Corolario 2.18, tenemos que el sistema tiene solución si y solo si $G \neq \{1\}$, o equivalentemente, el sistema no tiene solución si y solo si $G = \{1\}$, siendo G base de Gröbner reducida. Si efectivamente posee solución, podemos afirmar que el grafo es k-coloreable.

Para hallar los valores de las ecuaciones del sistema, utilizaremos el software SageMath [10]. Se ha creado un código llamado "Resolución del problema del coloreado", el cual podemos encontrar en el Apéndice A. Bastará introducir nuestro grafo e indicar el número de colores que queremos usar.

Para resolver este sistema podemos utilizar las bases de Gröbner tal y como se explicó en el tercer problema de la Sección 2.6. Para entender esto mejor, estudiemos el siguiente ejemplo.

Ejemplo 12. Consideramos el grafo no dirigido $\mathcal{G} = (V, E)$ con $V = \{1, 2, 3\}$ y $E = \{\{1, 2\}, \{2, 3\}\}$.



Nuestro sistema de ecuaciones polinómicas es:

$$\begin{cases} 2x_1^2 - x_1 = 0 \\ 2x_2^2 - x_2 = 0 \\ 2x_3^2 - x_3 = 0 \\ 2x_1 + 2x_2 - 1 = 0 \\ 2x_2 + 2x_3 - 1 = 0 \end{cases}$$

Vamos a aplicar lo estudiado en el capítulo anterior sobre cómo resolver un sistema de ecuaciones utilizando bases de Gröbner, ya que hemos obtenido un sistema de ecuaciones en varias variables.

- Hallamos una base de Gröbner, con respecto al orden lexicográfico, del ideal I, el cual está generado por las ecuaciones del sistema anterior. Esta base es:

  $$G = \{f_1, f_2, f_3\} = \{x_1 - x_3, x_2 + x_3 - 1, x_3^2 - x_3\}.$$

  Por el Corolario 2.18 se tiene que el grafo es 2-coloreable si y solo si $1 \notin G$. Por lo tanto, como existe solución (ya que la base no es trivial), se tiene que este grafo es 2-coloreable. Veamos en el siguiente paso cuál es su solución.

- Resolviendo el sistema formado por $f_1 = 0, f_2 = 0$ y $f_3 = 0$, obtenemos que sus soluciones son:

  $$x_1 = x_3 = 0 \text{ y } x_2 = 1 \qquad \text{o} \qquad x_1 = x_3 = 1 \text{ y } x_2 = 0.$$

  Por la Proposición 2.11, se tiene que estas soluciones halladas son todas las que existen.

  De este modo, identificando el valor 0 al color azul y el valor 1 al color marrón, tenemos que el grafo se puede pintar de estas dos maneras:

Observar que este procedimiento es válido para cualquier grafo, incluso si consideramos grafos más complejos, como puede ocurrir en el caso de los Sudokus, tal y como se estudia en el siguiente capítulo.

Capítulo 4

Sudokus y bases de Gröbner

Los Sudokus están formados por un tablero en el que hay una cuadrícula 9×9 dividida en 9 cajas de tamaño 3×3 en las cuales aparecen números del 1 al 9 cumpliendo ciertas condiciones. Estas condiciones son: en cada caja de 3×3 no puede haber números repetidos, al igual que cada fila y cada columna han de estar completas sin repeticiones. Cada juego empieza con el tablero parcialmente relleno por ciertos dígitos, a los cuales llamaremos *pistas*, y el objetivo para resolverlo es encontrar qué número corresponde a cada celda en blanco.

A lo largo de este capítulo será importante tener claro que un *puzle Sudoku* es un subconjunto de un Sudoku que determina de forma única el resto del tablero.

La finalidad de este capítulo es resolver dicho juego matemático usando las bases de Gröbner. Para ello, interpretaremos el Sudoku como un grafo y la resolución del Sudoku como un problema del k-coloreado, de modo que:

- El grafo tiene 81 vértices, uno para cada celda.
- Asignando a cada número un color, tenemos $k = 9$ colores.
- Las aristas están definidas por las relaciones de adyacencia: donde queremos diferentes números (misma fila, columna y caja 3×3) necesitamos diferentes colores.

Definición 31. Dado un Sudoku, cada fila, cada columna o cada caja 3×3 formará una *región*.

Definición 32. Diremos que dos vértices están *ligados* si pertenecen a la misma región.

Nuestro objetivo es dar colores (dígitos del 1 al 9) a cada vértice de modo que si dos vértices están ligados tienen que tener colores distintos. Es decir, queremos resolver el problema del 9-coloreado en un grafo, el cual viene representado mediante un Sudoku, para lo cual utilizaremos el procedimiento descrito en el Capítulo 3. Por lo tanto, buscamos una manera de colorear el grafo con exactamente 9 colores.

Notar que no podríamos completar el Sudoku con menos de 9 números diferentes ya que entonces dejaríamos alguna celda vacía. Por ello, el número cromático [1] de nuestro grafo es 9.

4.1. Sudokus

En un Sudoku cada vértice tiene otros 20 vértices con los que estar ligado. Como tenemos 81 celdas, entonces el número de aristas de nuestro grafo es igual a $\dfrac{81 \cdot 20}{2} = 810$.

[1] Si H es un grafo, para calcular su número cromático con SageMath, utilizamos la función $chromatic\_number(H)$.

Para resolver el problema del 9-coloreado utilizaremos un sistema de ecuaciones polinómicas tal y como se presenta en el Capítulo 3. Veamos qué datos tenemos y cómo, a partir de ellos, construimos las ecuaciones.

Consideramos un Sudoku, el cual tiene 81 celdas y las numeramos de izquierda a derecha y de arriba abajo. Identificando celdas con vértices, tenemos que la celda i corresponde a la variable x_i asignada a cada vértice, con $i = \{0,\dots,80\}$. Escribimos el conjunto de colores como $\{c_k : 1 \leq k \leq 9\} \subseteq \mathbb{Q}[x_0,\dots,x_{80}]$.

Sea $I \subseteq \mathbb{Q}[x_0,\dots,x_{80}]$. Entonces, para que el grafo sea 9-coloreable necesitamos un sistema de ecuaciones polinómicas obtenido de forma análoga a como construimos el sistema (3.1).

- Queremos que todos nuestros vértices estén coloreados (es decir, que todas las celdas estén rellenas por un número). Entonces consideramos el polinomio

$$f(x_i) = \prod_{k=1}^{9}(x_i - c_k) = 0,\ \forall\, 0 \leq i \leq 80.$$

- Queremos que no haya dos vértices conectados por la misma arista y que tengan el mismo color, es decir, que se cumplan las relaciones de adyacencia definidas anteriormente. De modo que tenemos

$$g(x_i,x_j) = \frac{f(x_i) - f(x_j)}{x_i - x_j} = 0,\ \forall\, 0 \leq i < j \leq 80.$$

Además de considerar f y g, para poder resolver el Sudoku, toda la información inicial debe ser incluida en forma de polinomios. ¿Qué forma tendrán estos nuevos? Si en la celda x_i tenemos la información de que está el valor c_k, con $i = 0,\dots,80$, $k = 1,\dots,9$, entonces el polinomio será $x_i - c_k$.

Entonces el ideal I para el cual tendremos que hallar una base de Gröbner (como en el problema del k-coloreado) es $I = J + L = \langle f(x_i), g(x_i,x_j)\rangle + \langle x_i - c_k\rangle$, siendo L el ideal generado por los polinomios de las incógnitas que ya tienen valor.

Ejemplo 13. Consideramos el puzle Sudoku de la Figura 4.1.

3		4						
		8	4	9			6	
		7			1			
7					8		5	
		2	6		4	3		
	8		9					1
			3			2		
	2			8	6	4		
						8		6

Figura 4.1

Como acabamos de explicar, una de las cosas que tenemos que hacer para resolverlo, es añadir los siguientes polinomios al ideal I:

$$x_0 - 3, x_2 - 4, x_{11} - 8, x_{12} - 4, x_{13} - 9, x_{16} - 6, x_{20} - 7, x_{23} - 1, x_{27} - 7, x_{32} - 8,$$
$$x_{34} - 5, x_{38} - 2, x_{39} - 6, x_{41} - 4, x_{42} - 3, x_{46} - 8, x_{48} - 9, x_{53} - 1, x_{57} - 3,$$
$$x_{60} - 2, x_{64} - 2, x_{67} - 8, x_{68} - 6, x_{69} - 4, x_{78} - 8, x_{80} - 6.$$

Observación 1. Una vez que hemos añadido toda la información inicial del Sudoku, se obtiene que alguno de los polinomios $f(x_i)$ no es realmente necesario, ya que al considerar $f(x_i)$ estamos consiguiendo que todos los vértices estén coloreados, pero hay algunos que ya están coloreados desde el principio. Sin embargo, podemos dejar estos valores duplicados ya que, matemáticamente, no es contradictorio.

Toda la información sobre las soluciones de un Sudoku está contenida en la variedad afín

$$\mathbf{V}(I) = \{(c_0,\dots,c_{80}) \in \mathbb{Q}^{81} \,|\, H(c_0,\dots,c_{80}) = 0, H \in I\}.$$

De modo que, como $I = J + L$ entonces tenemos que considerar la siguiente variedad afín para hallar las soluciones de nuestro problema:

$$\mathbf{V}(J+L) = \mathbf{V}(\langle f(x_i), g(x_i,x_j), x_i - c_k\rangle).$$

Una vez que tenemos claro qué forma tiene el ideal I, tenemos que hallar una base de Gröbner reducida de I, con respecto al orden lexicográfico.

Proposición 4.1. *Las siguientes afirmaciones son equivalentes:*

i) *La única solución del Sudoku es* $c = (c_0,\dots,c_{80})$.

ii) $I = J + L = \langle \{x_0 - c_0,\dots,x_{80} - c_{80}\}\rangle$.

iii) $G = \{x_i - c_k \,|\, i = 0,\dots,80\}$, *donde* c_k *son números del 1 al 9, es una base de Gröbner reducida de* I.

Demostración. Ver [8, Proposición 25]. □

Es decir, la base de Gröbner reducida de I, G, contendrá polinomios de la forma $x_i - c_k$. Resolviendo el sistema formado por los polinomios de G igualados a 0 se obtiene $x_i = c_k$ de modo que la celda x_i tendrá el valor c_k. Por la Proposición 2.11 estas soluciones son todas las que existen.

Para entender todo esto es interesante ver cómo se aplica la teoría explicada anteriomente a un ejemplo práctico de resolución de un Sudoku. Sin embargo, antes de empezar, es conveniente trabajar primero con una versión más simple de los Sudokus, llamada Shidokus.

4.1.1. Caso particular: Shidokus

Los Shidokus son un caso particular de los Sudokus ya que las reglas de estos rompezabezas son las mismas: todas sus regiones contienen exactamente solo una vez cada número. La única diferencia es que los Shidokus están formados por una cuadrícula 4×4 dividida en 4 cajas de tamaño 2×2, de modo que los dígitos ahora se moverán del 1 al 4.

En un Shidoku cada vértice tiene otros 7 vértices con los que estar ligado. Como tenemos 16 celdas, entonces el número de aristas de nuestro grafo es igual a $\dfrac{16 \cdot 7}{2} = 56$.

Observar que ahora, nuestro objetivo es resolver el problema del 4-coloreado en un grafo aplicando el método explicado en este capítulo. Para entender mejor cómo, veamos el siguiente ejemplo.

Ejemplo 14. Sea el puzle Shidoku, correspondiente a la imagen de la izquierda, de la Figura 4.2.

1		2	3
	2		
4			2
		1	

1	4	2	3
3	2	4	1
4	1	3	2
2	3	1	4

Figura 4.2

Para resolverlo, tenemos que calcular la base de Gröbner reducida del ideal I. Este ideal estará formado por:

- Polinomios de la forma $f(x_i) = \prod_{k=1}^{4} (x_i - c_k)$, $\forall\, 0 \leq i \leq 15$.

- Polinomios de la forma $g(x_i, x_j) = \dfrac{f(x_i) - f(x_j)}{x_i - x_j} = 0$, $\forall\, 0 \leq i < j \leq 15$.

- Los siguientes polinomios, que equivalen a las condiciones iniciales:

$$x_0 - 1, x_2 - 2, x_3 - 3, x_5 - 2, x_8 - 4, x_{11} - 2, x_{14} - 1.$$

Considerando I el ideal formado por todos esos polinomios, podemos calcular la base de Gröbner, con respecto al orden lexicográfico, de I. La base obtenida es:

$$G = \{x_0 - 1, x_1 - 4, x_2 - 2, x_3 - 3, x_4 - 3, x_5 - 2, x_6 - 4, x_7 - 1, x_8 - 4,$$
$$x_9 - 1, x_{10} - 3, x_{11} - 2, x_{12} - 2, x_{13} - 3, x_{14} - 1, x_{15} - 4\}.$$

Esta base es la que nos proporciona la solución del Shidoku. Esto se traduce en que la imagen de la derecha de la Figura 4.2 es la solución de nuestro puzle Shidoku inicial.

A continuación, se explican los pasos que se han realizado con SageMath para la resolución del ejemplo anterior.

- Se ha introducido el tablero vacío de un Shidoku mediante el código explicado en el Apéndice A.
- Se han calculado los polinomios $f(x_i)$, $g(x_i, x_j)$ aplicando el código creado para la resolución del problema del coloreado (ver Apéndice A). Se ha definido J como el ideal generado por estos polinomios.
- Se han introducido los polinomios referentes a las condiciones iniciales y se ha definido L como el ideal generado por estos polinomios.
- Se ha calculado la base de Gröbner del ideal $I = J + L$. Para este ejemplo se ha utilizado la función, ya integrada en SageMath, $I.groebner\_basis()$. Es conveniente usar esta función en vez de aplicar el algoritmo de Buchberger (el cual está implementado en el Apéndice A) ya que el algoritmo no proporciona una base de Gröbner reducida.

Sin embargo, a pesar de obtener la base de Gröbner reducida, es posible que nuestro Shidoku inicial no posea solución única. Esto se puede observar con el siguiente ejemplo.

Ejemplo 15. Veamos qué ocurre con el Shidoku de la Figura 4.3.

1			
2			
	1		
			3

Figura 4.3

Repitiendo los mismos pasos que en el ejemplo anterior, obtenemos una base de Gröbner G aunque ahora no todos los polinomios de la base son de la forma $x_i - c_k$.

Entonces, para encontrar la solución del Shidoku (la cual existe ya que $G \neq \{1\}$), tenemos que resolver el sistema de ecuaciones formado por los polinomios de G igualados a 0. Una vez resuelto, lo esperado es obtener soluciones de la forma $x_i = c_k$ las cuales nos proporcionen la solución del sistema. Sin embargo, la solución del sistema no es única, lo que implica que existe una variedad de soluciones para nuestro Shidoku. Estas soluciones son las que podemos observar en la Figura 4.4.

1	4	3	2
2	3	4	1
3	1	2	4
4	2	1	3

1	3	4	2
2	4	3	1
3	1	2	4
4	2	1	3

1	3	2	4
2	4	3	1
3	1	4	2
4	2	1	3

Figura 4.4

4.1.2. Resolución Sudokus

Ahora que hemos entendido cómo resolver los Shidokus, podemos aumentar el tamaño de n y seguir los mismos pasos para conseguir el objetivo de este capítulo: resolver los Sudokus utilizando el problema del 9-coloreado y las bases de Gröbner.

Continuamos con el puzle Sudoku del Ejemplo 13, el cual queremos resolver. Recordar que ya habíamos hallado los polinomios correspondientes a las condiciones iniciales (los cuales generan L) de modo que solo falta construir el ideal $I = J + L$ y obtener su base de Gröbner G. De este modo, siguiendo los mismos pasos que para los Shidokus y utilizando SageMath, se tiene que la solución es:

3	9	4	7	6	5	1	2	8
2	1	8	4	9	3	5	6	7
5	6	7	8	2	1	9	3	4
7	4	9	1	3	8	6	5	2
1	5	2	6	7	4	3	8	9
6	8	3	9	5	2	7	4	1
8	7	6	3	4	9	2	1	5
9	2	1	5	8	6	4	7	3
4	3	5	2	1	7	8	9	6

Figura 4.5

Desafortunadamente, los sistemas de ecuaciones polinómicas que resuelven los Sudokus no son muy "amigables" ya que el número de ecuaciones es bastante elevado. A pesar de que existen funciones, ya incluidas en los paquetes de la mayoría de los lenguajes de programación, para resolver dichos sistemas, producir el sistema de ecuaciones y aplicar las bases de Gröbner no es un buen método en general. Sin embargo, este enfoque tiene algunas ventajas como por ejemplo obtener todas las posibles soluciones tal y como se ha visto en el Ejemplo 15.

4.1.3. Generalización $n \times n$

Al principio de este capítulo hemos definido que un Sudoku está formado por una cuadrícula 9×9 y también hemos visto que se puede reducir n dando así lugar a los Shidokus. Entonces, tiene su lógica preguntarnos ¿n puede ser cualquier número natural, exceptuando el 0? Y efectivamente la respuesta a esto es afirmativa, podemos elegir n.

La resolución de estos Sudokus tamaño $n \times n$ es simplemente una generalización de lo estudiado con anterioridad. Es decir, para resolverlo tenemos que calcular la base de Gröbner reducida del ideal $I = J + L$ formado por:

- El ideal J formado por los polinomios f y g definidos como $f(x_i) = \prod_{k=1}^{n} (x_i - c_k)$, $g(x_i, x_j) = \dfrac{f(x_i) - f(x_j)}{x_i - x_j} = 0$, siendo $0 \leq i < j \leq n^2 - 1$.
- El ideal $L = \langle x_i - c_k \rangle$, siendo $0 \leq i \leq n^2 - 1$, $1 \leq k \leq n$.

De este modo, una vez que tenemos la base de Gröbner reducida G, por la Proposición 4.1 tendremos la solución para cualquier Sudoku de tamaño $n \times n$.

4.2. Conjeturas matemáticas

A continuación, vamos a dar algunas conjeturas matemáticas, es decir, algunas afirmaciones aparentemente verdaderas, ya que se han hecho pruebas confirmando su veracidad, pero no hay demostración matemática de ellas.

- Uno de los temas que podemos cuestionarnos es ¿cuántos posibles Shidokus y Sudokus distintos hay, ignorándose las relaciones de simetría entre soluciones similares? Tal y como se explica en [11], existen 288 tableros de Shidokus. Sin embargo, al intentar contar cuántos Sudokus existen, el número de posibilidades es mayor y el coste computacional aumenta. En [11] se explica el camino que se ha seguido para obtener una buena aproximación al número total de tableros de Sudokus válidos, siendo este número $6,6571 \cdot 10^{21}$.

- Uno de los problemas relacionados con el Sudoku que más ha interesado a los matemáticos, por haber estado mucho tiempo sin respuesta, es el del número mínimo de pistas que puede tener un Sudoku para resolverlo de manera única. Se ha conseguido encontrar multitud de puzles de 17 pistas con solución única pero ninguno con solo 16 [11]. Este problema, denominado "Problema del Sudoku mínimo" fue resuelto en 2012 con la ayuda de un ordenador evaluando todos, salvo equivalencias, los cuadrados de Sudokus en busca de algún puzle de 16 pistas. Los artífices de esta demostración son Gary McGuire, Bastian Tugemann y Gilles Civario. En el caso de los Shidokus, este número mínimo es 4, como se menciona en [11].

- Sin embargo, ni todos los Sudokus con 17 pistas, ni todos los Shidokus con 4 pistas (véase el Ejemplo 15), tienen solución única. Esto nos lleva a preguntarnos, ¿cuál es el número máximo de pistas que puede haber en una cuadrícula y aún no tener solución única? En la página 26 de [11] se observa un puzle Sudoku con 77 pistas y sin solución única. De modo que 77 es el máximo número de pistas para el cual un Sudoku no tiene solución única. Además se conjetura que para cualquier otra variante de los Sudokus, de tamaño $n \times n$, este número máximo es $n^2 - 4$.

- La dificultad en los Sudokus se cree que depende del número de pistas iniciales. Pero, sorprendentemente, esta dificultad se basa en la posición de las pistas. Esta es la razón por la que la distribución de las pistas distingue un Sudoku fácil de otro difícil. En la página 122 de [3] se muestra un Sudoku con 20 pistas de mínima dificultad y otro con 28 pistas de dificultad máxima.

- Una medida más refinada de la dificultad se hace a partir del estudio de las técnicas de resolución de Sudokus, como se muestra en [3]. Algunos métodos son más simples que otros, por lo que se puede conjeturar que si un Sudoku requiere un razonamiento más complejo para resolverlo, se le asocia una dificultad mayor. Sin embargo, estimar la dificultad de un Sudoku no es, ni mucho menos, una ciencia exacta, debido a la enorme carga de subjetividad que ello conlleva.

4.3. Conclusión

A modo de conclusión, señalar la importancia que alberga esta aplicación de las bases de Gröbner, ya que hemos conseguido unir conceptos geométricos y algebraicos. Para una modelización geométrica de los Sudokus hemos estudiado un problema fundamental de la Teoría de grafos el cual trata de colorear un grafo con k colores. De este modo, hemos sido capaces de configurar matemáticamente un Sudoku como si fuese un grafo con tantos vértices como celdas. Además, hemos resuelto sistemas de ecuaciones no lineales utilizando así la parte teórica estudiada en el Capítulo 2, la cual hace referencia a un estudio en el marco algebraico. Por lo tanto, a pesar de que aparentemente el Sudoku es un juego sencillo de pura lógica, el estudio realizado en este capítulo muestra un trasfondo claramente matemático, tanto en su planteamiento como en su resolución.

Apéndice A

Códigos SageMath

Esta parte final está destinada a mostrar todos los códigos escritos en SageMath que se han utilizado para la resolución de varios ejemplos a lo largo del presente trabajo.

- Algoritmo de la división en varias variables.

  - Las variables de entrada son (f,G,A) donde f es un polinomio, G es una lista de polinomios y A es un anillo de polinomios.
  - Las variables de salida son $(Q,A(r))$ donde Q es una lista de polinomios, que se corresponden con los cocientes, y $A(r)$ es el resto de la división.

```
def div (f,G,A):
    s = len(G)
    p = A(f)
    Q = s*[0]
    r = 0
    while p != 0:
        i = 0
        division = false
        while i < s and division == False:
            if G[i].lt().divides(p.lt()):
                Q[i] = Q[i] + p.lt()//G[i].lt()
                p = p - (p.lt()//G[i].lt())*G[i]
                division = True
            else:
                i = i + 1
        if division == False:
            r = r + p.lt()
            p = p - p.lt()
    return Q, A(r)
```

- S-polinomio.

  - Las variables de entrada son (f,g,A) donde f y g son dos polinomios y A es un anillo de polinomios.
  - La variable de salida es s, correspondiente al S-polinomio buscado.

```
def S_polinomio(f,g,A):
    a = A(f).lm()
    b = A(g).lm()
```

```
    c = lcm(a,b)
    s = A((c/a)*f-(c/b)*g)
    return s
```

- Algoritmo de Buchberger.
  - Las variables de entrada son (F,A) donde F es una lista de polinomios y A es un anillo de polinomios.
  - La variable de salida es G, la cual es una lista de polinomios (estos polinomios son los que forman la base de Gröbner).

```
def Buch(F,A):
    n=len(F)
    G=F
    for i in [0..n-2]:
        for j in [i+1..n-1]:
            s=S_polinomio(G[i],G[j],A)
            d=div(s,G,A)[1]
            if d!=0:
                return Buch(F+[d],A)
    return G
```

- Resolución del problema del coloreado.
  - Las variables de entrada son (G,k) donde G es un grafo y k es el número de colores.
  - Las variables de salida son $(f+g,A)$ donde $f+q$ son las ecuaciones de nuestro sistema y A es el anillo de polinomios.

```
def sistema (G,k):
    n = G.num_verts()
    xs = list(var('x_%d' %i) for i in range(n))
    F = QQ
    A = PolynomialRing(F,xs,order='lex')
    colores = range(k)
    f = []
    for j in xs:
        f = f + [A(prod([(j-i) for i in colores]))]
    g = []
    aristas = [[_[0],_[1]] for _ in G.edges()]
    for j in aristas:
        f1 = [A(prod([(xs[j[0]]-i) for i in colores])),
              A(prod([(xs[j[1]]-i) for i in colores]))]
        g = g + [A((f1[0]-f1[1])/(xs[j[0]]-xs[j[1]]))]
    return f + g, A
```

Observación 2. Para definir el anillo de polinomios en el que queremos trabajar, se puede especificar cualquiera de los órdenes monomiales explicados en el Capítulo 2, simplemente escribiendo lo siguiente:

- Orden lexicográfico: order = 'lex'
- Orden lexicográfico graduado: order = 'deglex'
- Orden lexicográfico graduado inverso: order = 'degrevlex'

- Creación de un tablero Sudoku, de tamaño $n \times n$, sin pistas.

  Para ello, se han tenido que crear dos funciones. Previamente es conveniente explicar que tratamos el Sudoku como si fuera una matriz, de modo que la celda x_k corresponde al elemento (i, j) con $i, j = 0, \ldots, n^2 - 1$. Por ejemplo, en un Sudoku 9×9 la celda x_{13} corresponde al elemento $(1,4)$.

  1. A través de esta función cada celda del Sudoku se convierte en un elemento matricial de la forma (i, j).
     - Las variables de entrada son (i, j, n) donde i corresponde al primer elemento del par (i, j), j corresponde al segundo elemento del par (i, j) y n hace referencia al tamaño.
     - La variable de salida es el subíndice de la celda x_k.

  ```
  #Para un Sudoku 9x9, se toma n=3
  def convertir(i,j,n):
      return ZZ(i*n+j)
  ```

  2. Mediante esta función imponemos las relaciones de adyacencia, de modo que no se repitan los dígitos en ninguna de las regiones.
     - La variable de entrada es n que hace referencia tanto al número de filas como al número de columnas.
     - La variable de salida es la lista de todas las aristas E cumpliendo las relaciones impuestas.

  ```
  #Para un Sudoku 9x9, se toma n=9
  def eqs_sudoku(n):
      R = Integers(3)
      E = []
      #Pares (i,j) (i,k) tales que x_(i,j) y x_(i,k) pertenecen
      a la misma fila
      #Pares (j,i) (k,i) tales que x_(j,i) y x_(k,i) pertenecen
      a la misma fila
      for i in range(n^2):
          for j in range(n^2):
              for k in [j+1..n^2-1]:
                  a=convertir(i,j,n^2)
                  b=convertir(i,k,n^2)
                  if (not [a,b] in E) and (not [b,a] in E):
                      E=[[a,b]]+E
                  a=convertir(j,i,n^2)
                  b=convertir(k,i,n^2)
                  if (not [a,b] in E) and (not [b,a] in E):
                      E=[[a,b]]+E
      #Pares (i1*i2,j1*j2) (i1*i3,j1*j3) tales que
      x_(i1*i2,j1*j2) y x_(i1*i3,j1*j3) pertenecen
      al mismo bloque n x n
      for i1 in range(n):
          for j1 in range(n):
              for i2 in range(n):
                  for j2 in range(n):
                      for i3 in range(n):
                          for j3 in range(n):
                              a=convertir(i1*n+i2,j1*n+j2,n^2)
  ```

```
                                        b=convertir(i1*n+i3,j1*n+j3,n^2)
                                        if a<b and (not [a,b] in E) and
                                        (not [b,a] in E):
                                            E=E+[[a,b]]
        return E
```

Observación 3. Si quisiéramos resolver un Sudoku de tamaño 9×9 con pistas iniciales dadas tendríamos que seguir los siguientes pasos:

- Primero, aplicar el código creado para la resolución del problema del coloreado pero cambiando alguno de los datos.

  ```
  def sistema (G,k) -----> def sistema (E,k)
  n = G.num_verts() -----> n = 81
  aristas = [[_[0],_[1]] for _ in G.edges()] ----->
          aristas = [[_[0],_[1]] for _ in E]
  ```

  Siendo E la lista de todas las aristas obtenida anteriormente.

- Una vez hayado el sistema, consideramos el ideal generado por las soluciones del sistema.
- Consideramos también el ideal generado por los polinomios resultantes de las pistas dadas.
- Por último sumamos ambos ideales y obtenemos su base de Gröbner correspondiente utilizando la función *I.groebner_basis*().

Bibliografía

[1] W. W. Adams and P. Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1994.

[2] D. A. Bayer. *The division algorithm and the Hilbert scheme*. ProQuest LLC, Ann Arbor, MI, 1982. Thesis (Ph.D.)–Harvard University.

[3] A. Becerra Tomé, J. Núñez Valdés, and J. M. Perea González. ¿Cuánta Matemática hay en los sudokus? *Pensamiento Matemático*, 6(1):113–136, 2016.

[4] S. Bennett. Applications of Gröbner bases. 2008.

[5] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[6] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. SINGULAR 4-2-0 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2020.

[7] J. Gago-Vargas, I. Hartillo-Hermoso, J. Martín-Morales, and J. M. Ucha-Enríquez. Sudokus and Gröbner bases: not only a divertimento. In *Computer algebra in scientific computing*, volume 4194 of *Lecture Notes in Comput. Sci.*, pages 155–165. Springer, Berlin, 2006.

[8] M.R. Gonzalez-Dorrego. Resolution of sudokus using Groebner basis. *Computer tools in education*, (3):5–21, 2018.

[9] G.-M. Greuel and G. Pfister. *A* **Singular** *introduction to commutative algebra*. Springer, Berlin, extended edition, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh and UNIX).

[10] Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2.0)*. `https://www.sagemath.org`.

[11] J. Suárez Quero. Las matemáticas en el sudoku. Universidad de Almería, Septiembre 2017.