

Metodos polinomiales para trabajar con grafos

Ana Isabel PÉREZ MARTÍN

Trabajo Fin de Grado
dirigido por Philippe GIMÉNEZ

Grado en Matemáticas
Universidad de Valladolid
Julio 2014



Universidad de Valladolid

Índice general

1. Introducción	1
2. El problema de la coloración de grafos	3
2.1. Definiciones	3
2.2. El algoritmo austero de coloración	5
2.3. Polinomios cromáticos y números cromáticos	6
2.4. Un problema clásico: El problema de los cuatro colores	11
2.5. La conjetura de Xu	12
3. Conceptos algebraicos	15
3.1. Ideales y variedades afines	15
3.2. Bases de Gröbner	19
3.3. Ideales 0-dimensionales	22
4. Aplicación a la colorabilidad de grafos	25
4.1. Caracterizaciones polinomiales de la k -coloración	25
4.2. Ideales de coloración	29
4.3. Grafos únicamente k -coloreables	35
4.4. Grafos parcialmente coloreados	42
5. Sudokus, grafos y bases de Gröbner	47
5.1. Definición e historia	47
5.2. La relación entre los Sudokus y los grafos	49
5.3. Un algoritmo a lapiz y papel para resolver Sudokus	50
5.4. Resolución de Sudokus por bases de Gröbner	53
6. Conclusión	59
Bibliografía	61

Capítulo 1

Introducción

La presente memoria se debe a la realización de un Trabajo de Fin de Grado en Matemáticas y consiste, como indica su título, en la descripción de determinados métodos polinomiales para trabajar en grafos, y en particularidad en su coloración.

Los resultados principales serán la identificación de grafos k -coloreables y únicamente k -coloreables, y cómo encontrar una k -coloración propia.

El primer capítulo de la memoria consistirá en una introducción a la Teoría de la Coloración de grafos, se presentarán el “Problema de los Cuatro Colores” y la “Conjetura de Xu” y se incluirá un algoritmo para colorear grafos.

En el segundo capítulo se incluirá todo el bagaje algebraico necesario para demostrar los teoremas de los capítulos siguientes, es decir, las variedades afines y las bases de Gröbner.

El tercer capítulo es el capítulo central de este proyecto. En el se dan teoremas que, utilizando las bases de Gröbner, permiten distinguir cuando un grafo es k -coloreable y únicamente k -coloreable.

En el cuarto capítulo se estudia el caso particular de la “resolución de Sudokus”, que en el fondo es un problema de coloración de grafos. Aquí se da un algoritmo, basado de nuevo en las bases de Gröbner, que permite resolverlos mediante el cálculo de ideales.

Finalmente, en el último capítulo se proporcionará una breve conclusión sobre el uso de polinomios cromáticos para resolver el problema de la coloración de grafos.

Capítulo 2

El problema de la coloración de grafos

En la asignatura de Matemática Discreta, de tercer curso del Grado en Matemáticas, se estudian los grafos (especialmente los grafos planos) y se ve una introducción a la k -colorabilidad de un grafo. Sin embargo, a lo largo de este capítulo se incluyen algunas de las definiciones que se vieron en la asignatura, principalmente con el propósito de fijar una notación.

2.1. Definiciones

2.1 Definición. Un *grafo* $G = (V, E)$, o simplemente G , es un par ordenado de conjuntos, donde los elementos de E , a su vez, son pares de elementos de V . Los elementos de V se llaman *vértices*, y los de E , *aristas*. Se dice que:

- G es *orientado* si las aristas sólo se pueden recorrer en un sentido. En caso contrario diremos que es *no orientado*.
- G es *simple* si no tiene ni aristas múltiples ni bucles.
- G es *conexo* si existe un camino que permite recorrer todos los vértices.

Nota. En este trabajo (salvo mención explícita), cuando se hable de un *grafo* G de n vértices nos referiremos a un grafo simple, no orientado y conexo, en el que $V = \{1, 2, \dots, n\}$, y los elementos de E se denotarán por $\{i, j\}$, con $i, j \in V$ e $i < j$.

2.2 Definición. Definimos el *grado* de un vértice como el número de aristas que inciden en él. Diremos que un grafo G es *regular* cuando todos los vértices de G tienen el mismo grado.

2.3 Definición. Sea G un grafo de n vértices, sea k un entero positivo, con $k < n$. Sea $C_k = \{c_1, c_2, \dots, c_k\}$ un conjunto de k elementos, donde cada $c_k \in \mathbb{Z}_+$ se denomina *color*. Una k -coloración de los vértices de G , o simplemente, una k -coloración de G , es una aplicación $\nu : V \rightarrow C_k$.

El número de k -coloraciones de un grafo G de n vértices es k^n , ya que cada vértice se puede colorear con k colores distintos.

2.4 Definición. Dada una k -coloración de G se dice que es *propia* si todo par de vértices adyacentes recibe colores distintos, es decir, si $\forall i, j \in V, \{i, j\} \in E, \nu(i) \neq \nu(j)$. En caso contrario, la k -coloración se llama *impropia*.

2.5 Definición. Dadas dos coloraciones de un grafo G , se dice que son distinguibles si no se puede obtener una como permutación de los elementos de la otra.

2.6 Definición. Se dice que G es k -coloreable si tiene al menos una k -coloración propia y que es *únicamente k -coloreable* si tiene solamente una k -coloración propia distinguible.

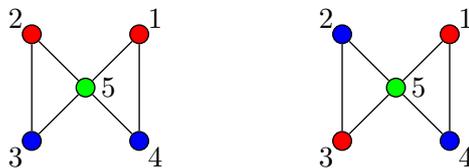
Nota. Si G es un grafo de n vértices y únicamente k coloreable, entonces tendrá $k!$ -coloraciones diferentes no distinguibles entre sí, ya que

$$\#\{Perm\{1, \dots, k\}\} = k!.$$

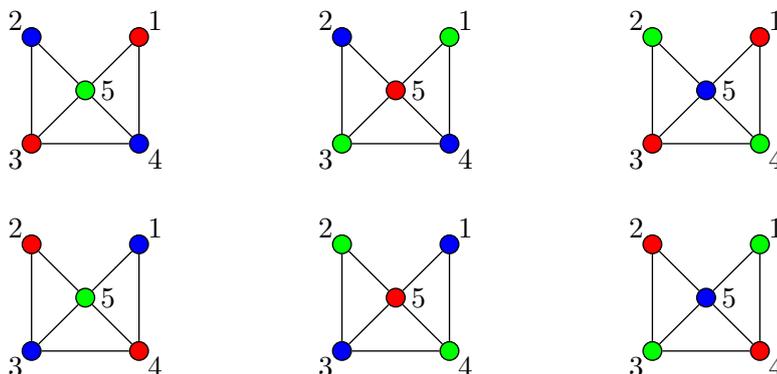
2.7 Ejemplo. Consideremos el grafo

$$G = (\{1, 2, 3, 4, 5\}, \{\{1, 5\}, \{1, 4\}, \{4, 5\}, \{2, 5\}, \{3, 5\}, \{2, 3\}\})$$

y veamos que es 3-coloreable, pero no únicamente 3-coloreable. Esto se puede hacer fácilmente calculando sus coloraciones propias:



Al añadirle la arista $\{3, 4\}$ al grafo anterior, conseguimos un grafo H que es únicamente 3-coloreable, y observamos que tiene $3! = 6$ coloraciones propias no distinguibles.



Uno de nuestros objetivos será buscar una forma de saber si un grafo tiene una coloración propia, y si la tiene cuándo es única. Una primera forma de hacerlo es buscar las coloraciones propias mediante un algoritmo de coloración.

2.2. El algoritmo austero de coloración

Vamos a dar entonces un procedimiento general que nos permita encontrar una coloración propia de un grafo G de n vértices usando el mínimo número de colores posibles.

Supongamos que tenemos un conjunto ordenado de n colores, $C = (c_1, \dots, c_n)$. Está claro que a lo sumo necesitamos n colores, uno para cada vértice. El siguiente algoritmo permite obtener una coloración para cada ordenación de los vértices.

ALGORITMO AUSTERO (*greedy algorithm*):

1. Ordenar los vértices del grafo: v_1, \dots, v_n ;
 2. A v_1 le asignamos el color c_1 ;
 3. Para i desde 2 hasta n
 - para j desde 1 hasta $i - 1$
 - si v_j es adyacente a v_i descartamos el color de v_j de C ;
 - fin si;
 - fin para;
 - asignamos a v_i el primer elemento de C no descartado;
 - fin para;
- FIN

Sin embargo este algoritmo no es tan efectivo como puede parecer a primera vista. Vamos a verlo con un ejemplo:

2.8 Ejemplo. Consideramos el grafo $G = \{1, 2, 3, 4\}, \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$, y veamos que dependiendo de cómo etiquetemos los vértices obtenemos una u otra coloración:



Por lo tanto, el problema ahora sería: “Dados los $n!$ órdenes posibles, encontrar el orden para el cual necesitemos el menor número de colores”, es decir, encontrar el orden óptimo de los vértices. Pero este orden óptimo es consecuencia de encontrar una k -coloración del grafo, con el menor k posible, y no al revés.

Esto quiere decir que para encontrar la k -coloración de un grafo G de n vértices, con el menor k posible, tendremos que aplicar el algoritmo a los $n!$ distintos órdenes de los vértices, y escoger la que menos colores utilice. Luego, esta no es una forma efectiva de encontrar la coloración de un grafo.

Nuestro objetivo a lo largo de los siguientes capítulos será buscar formas mejores de hacerlo.

2.3. Polinomios cromáticos y números cromáticos

2.9 Definición. El *número cromático* de G , denotado por $\chi(G)$ es el menor número de colores, k , necesarios para tener una k -coloración propia del grafo. Es decir, el k que hace que G sea k -coloreable pero no $(k - 1)$ -coloreable. Se dice que G es k -cromático si $\chi(G) = k$.

Vamos a acotar $\chi(G)$:

Está claro que si denotamos por $\Delta(G)$ el máximo grado de G (es decir, todos los vértices de G tienen grado menor o igual que $\Delta(G)$), entonces el algoritmo austero utiliza a lo sumo $\Delta(G) + 1$ colores. Luego $\chi(G) \leq \Delta(G) + 1$.

Pero esta cota puede mejorarse:

2.10 Proposición. Sea G un grafo con grado máximo $\Delta(G)$, y que tiene al menos un vértice w de grado estrictamente menor que $\Delta(G)$, entonces $\chi(G) \leq \Delta(G)$.

Demostración. Sea G un grafo que cumple las hipótesis de la proposición. Ordenamos los vértices de forma que w sea el último vértice de la lista, esto es $w = v_n$. Sea s el número de vértices adyacentes a w . Los etiquetamos v_{n-s}, \dots, v_{n-1} de tal forma que precedan a w , delante de estos consideramos los vértices adyacentes a v_{n-1} que no hayamos considerado hasta ahora, luego los de v_{n-2} y así sucesivamente hasta que no tengamos más vértices. Si ahora aplicamos el Algoritmo Austero,

$$\#\{\text{vecinos anteriores}\} \leq \Delta(G) - 1, \quad (2.1)$$

porque todos los vértices excepto w tienen algún vecino posterior. Como el grado de w es estrictamente menor que $\Delta(G)$, para w también se verifica 2.1. Luego para todo $v \in G$ hay a lo sumo $\Delta(G) - 1$ colores prohibidos, y por tanto bastará con $\Delta(G)$ colores para colorearlo.

□

Vamos a dar ahora algunos resultados más acerca del número cromático, para ello necesitamos la siguiente definición.

2.11 Definición. Sean G y H dos grafos, decimos que H es un subgrafo de G , y denotamos $H \subset G$, si se verifica que $V(H) \subset V(G)$ y $E(H) \subset E(G)$, donde $V(G)$, $V(H)$ denotan los vértices de G y H respectivamente y $E(G)$, $E(H)$ las aristas.

2.12 Proposición. Sea $H \subset G$, entonces $\chi(G) \geq \chi(H)$.

Demostración. Sea $\chi(G) = k$, entonces H , como subgrafo de G , admite una k -coloración propia, es decir, $\chi(H) \leq k$.

□

2.13 Proposición-Definición. Denotamos por $G+H$ el grafo resultante de la unión $G \cup H$, esto es, al añadir todas las aristas necesarias para que todos vértice de G sean adyacentes con todos los vértices de H . Entonces $\chi(G + H) = \chi(G) + \chi(H)$

Demostración. Por la proposición anterior $\chi(G + H) \geq \chi(G)$ y $\chi(G + H) \geq \chi(H)$, luego resulta inmediato que $\chi(G + H) \geq \chi(G) + \chi(H)$.

La otra desigualdad también es evidente, ya que como cada uno de los vértices de G es adyacente a cada uno de los vértices de H , no se puede usar ninguno de los colores usados en la coloración de G para la de H , y viceversa. Por lo tanto $\chi(G + H) \leq \chi(G) + \chi(H)$

□

Pero aparte de conocer el número k de colores que necesitamos para colorear un grafo G , también queremos saber el número de formas de colorearlo con k colores. Esto es precisamente lo que indica el polinomio cromático.

2.14 Proposición-Definición. *Sea G un grafo de n vértices. Llamamos polinomio cromático de G al polinomio de grado n en la variable k que cuenta el número de formas distintas (no distinguibles) en que se puede colorear G usando k colores; aunque no es necesario que se utilicen todos. Se denota por $\chi_G(k)$.*

Para demostrar que $\chi_G(k)$ es un polinomio exactamente de grado n en k necesitamos enunciar un resultado previo, y fijar una notación.

Notación. Sea G un grafo de n vértices. Sea $e \in E$. Denotamos por $G \setminus \{e\}$ el grafo que se obtiene a partir de G suprimiendo la arista e , sin quitar los vértices.

2.15 Definición. Sea G un grafo de aristas E , y sea $e \in E$. Se define la *contracción de G por e* , y se denota G/e , al grafo G' resultante de identificar los vértices de G adyacentes por e y suprimir las aristas dobles y bucles. Se dice que un grafo H es *contracción de G* si se obtiene por sucesivas contracciones por las aristas.

Nota. El conjunto formado por G y sus contracciones es un conjunto parcialmente ordenado ($A \leq B$ si A es contracción de B).

2.16 Proposición. *Con la notación anterior, se verifica que*

$$\chi_G(k) = \chi_{G \setminus \{e\}}(k) - \chi_{G/e}(k).$$

Demostración (2.16). Observemos que $\chi_{G/e}(k)$ es el número de coloraciones propias de G para las que los vértices adyacentes por e reciben el mismo color; y que las coloraciones propias de G obligatoriamente llevarán dos colores distintos en los vértices adyacentes por e , luego $\chi_G(k)$ será el número de coloraciones propias de $G \setminus \{e\}$ que asignen a los vértices adyacentes por e

dos colores distintos. Ahora bien, $\chi_{G \setminus \{e\}}$ es la suma del número de formas de colorear $G \setminus \{e\}$ dando a los vértices adyacentes por e colores distintos y del número de formas de colorear $G \setminus \{e\}$ dándolos colores iguales. Escrito de otra forma, $\chi_{G \setminus \{e\}}(k) = \chi_G(k) + \chi_{G/e}(k)$.

□

Demostración (2.14). Veamos que $\chi_G(k)$ es un polinomio con coeficientes enteros. Vamos a razonar por inducción sobre el número de vértices de G : Si $n = 1$, $\chi_G(k) = k$, luego es cierto. Supongamos ahora que $\chi_G(k)$ es siempre un polinomio en k con coeficientes enteros para grafos G con $|E(G)| \leq m$. Sea H un grafo cualquiera con $m + 1$ aristas. Si e es una arista de H por 2.16,

$$\chi_H(k) = \chi_{H \setminus \{e\}}(k) - \chi_{H/e}(k),$$

donde $H \setminus \{e\}$ tiene m aristas y H/e tiene m aristas o menos. Por inducción, los dos términos a la derecha de la igualdad son polinomios en k con coeficientes enteros. Luego su resta, $\chi_H(k)$ también será un polinomio con coeficientes enteros. Veamos ahora que $\chi_G(k)$ tiene grado exactamente n . Razonamos por inducción sobre el número de vértices. Para el caso $n = 1$ es trivial. Veamos el caso general: Supongamos ahora que para todo grafo G de m vértices. Se verifica que χ_G tiene grado m . Consideramos ahora un grafo G de $m + 1$ vértices. Sea v un vértice de G , sea H el subgrafo de G que se obtiene al quitar a G el vértice v y todas las aristas, e_1, \dots, e_s , que inciden en él.

$$\begin{aligned} \chi_G(k) &= \chi_{G \setminus \{e_1\}}(k) - \chi_{G/e_1}(k) = \chi_{G \setminus \{e_1, e_2\}}(k) - \chi_{(G \setminus \{e_1\})/e_2}(k) - \chi_{G/e_1}(k) = \dots \\ &\dots = \chi_{G \setminus \{e_1, e_2, \dots, e_s\}}(k) - \chi_{(G \setminus \{e_1, \dots, e_{s-1}\})/e_s}(k) - \dots - \chi_{(G \setminus \{e_1\})/e_2}(k) - \chi_{G/e_1}. \end{aligned}$$

Observamos que $G \setminus \{e_1, e_2, \dots, e_s\}$ no es conexo: es el grafo formado por H y el vértice aislado v . Como v no es adyacente a ningún vértice de H , podemos colorearlo de k formas distintas, independientemente de la coloración de H , luego $\chi_{G \setminus \{e_1, e_2, \dots, e_s\}} = k\chi_H$, así que $\chi_{G \setminus \{e_1, e_2, \dots, e_s\}}$ tiene grado $m + 1$, ya que por hipótesis, χ_H tiene grado m (porque H tiene m vértices). Veamos ahora que el resto de polinomios tienen grado menor o igual que m . Pero esto es evidente porque los grafos G'/e tienen un vértice menos que G' , luego tendrán a lo sumo, m vértices, y por tanto darán lugar a un polinomio de grado estrictamente menor que $m + 1$, que en ningún caso podrán anular $\chi_{G \setminus \{e_1, e_2, \dots, e_s\}}$.

□

Describamos ahora brevemente la relación entre número cromático y polinomio cromático en los grafos únicamente k -coloreables.

Si G es un grafo únicamente k -coloreable, entonces, por definición, $\chi(G) = k$ y $\chi_G(\chi(G)) = k!$, ya que tenemos que considerar todas las permutaciones posibles en el conjunto de los colores. Por otra parte, como G es únicamente k -coloreable, no es r -coloreable, para $r < k$ luego $\chi_G(\chi(r)) = 0$ para todo $r < k = \chi(G)$.

Vamos a ilustrar esto con un ejemplo.

2.17 Ejemplo. Volvamos a considerar los grafos en 2.7: Sus polinomios cromáticos se pueden calcular a simple vista con ayuda de la Combinatoria:

Calculemos primero el de G .

- Empezamos por el vértice 5: Como es el primero que coloreamos tenemos k colores posibles.
- Para el vértice 4 tenemos todos los colores menos el que hemos usado en 5 porque son adyacentes, luego $k - 1$.
- Para el vértice 1 no podremos utilizar los colores empleados ni en 5 ni en 4, luego tendremos $k - 2$.
- Por último, la situación de los vértices 4 y 2, es la misma que la de 4 y 1 respectivamente.
- Multiplicando todas las posibilidades encontramos el polinomio cromático:

$$\chi_G(k) = k \cdot (k - 1)^2 \cdot (k - 2)^2.$$

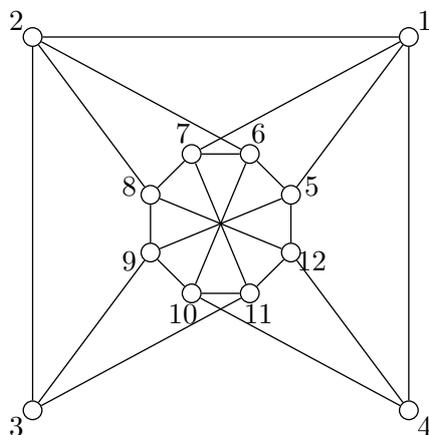
Vamos a calcular ahora el de H :

- Para 5, 4 y 1 utilizamos el mismo argumento que en G . - Con 3 (y con 2) sucede como con 1. Como es adyacente a 5 y a 4 (respectivamente a 3 y a 5) sólo lo podremos colorear con los colores que no hayamos usado en estos vértices, luego con $k - 2$.
- Multiplicando obtenemos todas las posibilidades de coloración, y por tanto, el polinomio cromático:

$$\chi_H(k) = k \cdot (k - 1) \cdot (k - 2)^3.$$

Luego G y H son 3-coloreables pero no 2-coloreables. Además, tenemos que $\chi_G(3) = 12$, $\chi_H(3) = 6 = 3!$ y $\chi_G(r) = \chi_H(r) = 0$ para $r = 1, 2$. Luego concluimos que H es únicamente 3-coloreable y que G no es únicamente k -coloreable para ningún k .

En los dos grafos del ejemplo anterior es fácil calcular el polinomio cromático, y por tanto el número de k -coloraciones de los grafos, pero ¿qué ocurre si consideramos un grafo más complicado? Consideremos el siguiente grafo:



En este caso no es fácil calcular el polinomio cromático, por lo tanto necesitaremos calcular el número de coloraciones de otra manera. Éste es, precisamente, uno de los objetivos del capítulo 4.

Además de éste nos plantearemos otro problema:

Sea G un grafo y H un subgrafo de G con una k -coloración propia. ¿Es posible extender la k -coloración propia de H a una k -coloración propia de G . Si es posible, ¿de cuántas formas distintas se puede hacer? Y si no es posible, ¿cuál es el mínimo número m que necesitamos para obtener una m -coloración propia de G que conserve la k -coloración de H ?

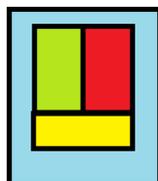
Estos problemas también se solucionarán en el capítulo 4 con un enfoque bastante innovador: las bases de Gröbner. Sin embargo, estas preguntas tienen su origen en un problema clásico muy conocido: “El Problema de los Cuatro Colores”.

2.4. Un problema clásico: El problema de los cuatro colores

El “Problema de los Cuatro Colores” es un problema topológico, propuesto por Francis Guthrie a principios de 1850 y que no se resolvió hasta finales del siglo siguiente. El problema era encontrar el mínimo número de colores necesarios para colorear un mapa, de modo que dos regiones fronterizas no compartiesen el mismo color.

La conjetura fue planteada en 1852 cuando Guthrie, después de haber coloreado un mapa de Inglaterra con cuatro colores, conjeturó que todo mapa político se podía colorear con a lo sumo cuatro colores.

Es evidente que tres colores no son suficientes, porque se puede crear fácilmente un mapa que necesite al menos cuatro, por ejemplo:



En 1879, Alfred Bray Kempe probó que cinco colores eran suficientes pero, aunque no se había encontrado todavía un mapa de que no fuese 4-coloreable, tampoco se había demostrado que todos tenían que serlo.

Tras varias demostraciones fallidas como la de Alfred Kempe en 1879 (que fue refutada por Percy Heawood en 1890) o la de Peter Guthrie Tait en 1890 (que fue refutada por Julius Petersen en 1891), finalmente en 1976 se publica una prueba (asistida por ordenador) que garantiza que todos los mapas políticos se pueden colorear con a lo sumo cuatro colores. Sin embargo, esta prueba, propuesta por Kenneth Appel y Wolfgang causó una gran controversia, precisamente porque se ayudaba de un ordenador.

En 1997, Neil Robertson, Daniel Sanders, Paul Seymour y Robin Thomas publicaron una prueba de 42 páginas, también hecha con la ayuda de un ordenador, que sí fue comúnmente aceptada, poniendo fin a un problema que había ocupado a los matemáticos durante más de un siglo, y que de hecho se había convertido en el problema más estudiado de la teoría de grafos.

Aparte de este resultado se han enunciado otros muchos en relación a la colorabilidad de un tipo de grafo. Sin embargo, nosotros en este documento no vamos a considerar los resultados que versan sobre un tipo concreto de grafos, sino que vamos a proporcionar métodos generales para estudiar la colorabilidad en todo tipo de grafos, independientemente del espacio topológico en el que se ubiquen.

2.5. La conjetura de Xu

Otro problema que también se ha estudiado mucho en teoría de grafos es la Conjetura de Xu:

En 1990, Xu demostró el siguiente teorema, que da una cota inferior del número de aristas que tiene que tener un grafo únicamente k -coloreable:

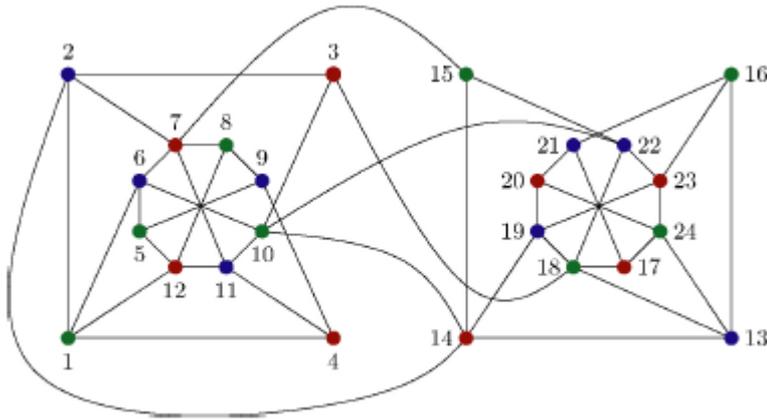
2.18 Teorema (de Xu). *Dado un grafo G simple y conexo, si G es únicamente k -coloreable, entonces*

$$|E| \geq (k-1)n - \frac{k(k-1)}{2}.$$

donde E son las aristas y n el número de vértices de G .

Además conjeturó que si G es simple, conexo y únicamente k -coloreable y se verifica $|E| \geq (k-1)n - \frac{k(k-1)}{2}$, entonces G contiene un subgrafo completo de k -vértices.

En 2001 Akbari, Mirrokni, Sadjad demostraron que la conjetura era falsa. Para ello utilizaron el siguiente grafo, con $E = 45$, $n = 24$ y $k = 3$.



La demostración de que la conjetura era falsa se basaba en un argumento combinatorio, y Akbari, sin embargo quería una prueba algorítmica.

Esto nos lleva a un nuevo problema: Encontrar un algoritmo efectivo que permita distinguir la k -colorabilidad única y generarla, y esto es precisamente nuestro objetivo en este trabajo.

Capítulo 3

Conceptos algebraicos

En este capítulo estudiaremos el álgebra del anillo de polinomios $\mathbb{K}[X_1, \dots, X_n]$ y la geometría que está asociada a él. El álgebra viene dada por los ideales y la geometría por las variedades afines. Además, en particular, estudiaremos las bases de Gröbner, que nos permiten solucionar algunos problemas de ideales polinomiales. Este capítulo está basado principalmente en [CLS].

3.1. Ideales y variedades afines

El concepto de ideal de un anillo se ha tratado repetidamente en muchas de las asignaturas del Grado en Matemáticas, por lo tanto en esta sección no se hará. Empezaremos estudiando qué son las variedades afines y, finalmente describiremos la relación que existe entre ellas y los ideales.

3.1 Definición. Sea \mathbb{K} un cuerpo y $f_1, \dots, f_r \in \mathbb{K}[X_1, \dots, X_n]$. Definimos

$$V(f_1, \dots, f_r) = \{(a_1, \dots, a_n) \in \mathbb{K}^n : f_i(a_1, \dots, a_n) = 0, \quad \forall 1 \leq i \leq r\}.$$

Llamamos $V(f_1, \dots, f_r)$ la *variedad afín* definida por f_1, \dots, f_r .

La variedad $V(f_1, \dots, f_r) \subset \mathbb{K}^n$ es, por lo tanto, el conjunto de soluciones del sistema de ecuaciones

$$f_1(X_1, \dots, X_n) = \dots = f_r(X_1, \dots, X_n) = 0,$$

es decir, los puntos comunes a las hipersuperficies asociadas a los polinomios f_1, \dots, f_r .

3.2 Lema. Si $V, W \subset \mathbb{K}^n$ son variedades afines, también lo son $V \cup W$ y $V \cap W$.

Demostración. Sean $V = V(f_1, \dots, f_r)$ y $W = V(g_1, \dots, g_s)$. Veamos que

$$V \cap W = V(f_1, \dots, f_r, g_1, \dots, g_s)$$

$$V \cup W = V(f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s).$$

La primera igualdad es evidente, ya que decir que $\mathbf{x} \in V \cap W$ es lo mismo que decir que $f_1(\mathbf{x}) = \dots = f_r(\mathbf{x}) = g_1(\mathbf{x}) = \dots = g_s(\mathbf{x}) = 0$.

Probemos ahora la segunda igualdad:

Si $\mathbf{x} \in V$, entonces para todo i , $f_i(\mathbf{x}) = 0$, lo que implica que $f_i g_j(\mathbf{x}) = 0$ para todo j . Luego $V \cup W \subset V(f_i g_j)$.

Para probar la otra inclusión tomamos $\mathbf{x} \in V(f_i g_j)$. Si $\mathbf{x} \in V$ hemos acabado. Sino, existe un $f_{i_0} \in V$ tal que $f_{i_0}(\mathbf{x}) \neq 0$. Como $f_{i_0} g_j(\mathbf{x}) = 0$ para todo j , todos los g_j se tienen que anular en \mathbf{x} , y por tanto $\mathbf{x} \in W$.

□

3.3 Proposición. Si $\{f_1, \dots, f_r\}, \{g_1, \dots, g_s\}$ son sistemas de generadores del mismo ideal en $\mathbb{K}[X_1, \dots, X_n]$, entonces $V(f_1, \dots, f_r) = V(g_1, \dots, g_s)$.

Demostración. La demostración es evidente.

□

Nota. El recíproco de la proposición anterior no es cierto en general. Basta considerar $I = \langle X^2 \rangle$ y $J = \langle X^3 \rangle$ en $\mathbb{K}[X]$. Pero veremos que sí es cierto en el caso de que I sea un ideal radical.

3.4 Proposición-Definición. Sea $V \subset \mathbb{K}[X_1, \dots, X_n]$ una variedad afín. Entonces

$$I(V) = \{f \in \mathbb{K}[X_1, \dots, X_n] : f(\mathbf{x}) = 0, \forall \mathbf{x} \in V\}$$

es un ideal, que se llama ideal de anulación de V , o simplemente, ideal de V .

Demostración. Sean $f, g \in I(V)$, $h \in \mathbb{K}[X_1, \dots, X_n]$, y $\mathbf{x} \in V$.

- 1) $0 \in I(V)$, ya que el polinomio cero se anula en todo \mathbb{K}^n .
- 2) $f(\mathbf{x}) + g(\mathbf{x}) = 0 + 0 = 0$.

$$3) h(\mathbf{x})f(\mathbf{x}) = h(\mathbf{x}) \cdot 0 = 0.$$

Luego $I(V)$ es un ideal. □

Vamos a trabajar ahora con la variedad afín de un ideal de polinomios. Como sólo hemos tratado la variedad afín definida por un conjunto finito de polinomios, tenemos que asegurar que todo ideal $I \subset \mathbb{K}[X_1, \dots, X_n]$ es de generación finita. Pero esto es precisamente el *Teorema de la Base de Hilbert* [CLS, pag.73].

3.5 Lema. Sea I un ideal de $\mathbb{K}[X_1, \dots, X_n]$, entonces $I \subset I(V(I))$. La igualdad no tiene porqué ocurrir.

Demostración. Sea $f \in I$, es decir, f se puede escribir como suma finita de polinomios de I . Como estos polinomios se anulan en $V(I)$, también lo hará f . Luego $f \in I(V(I))$.

Tomando $I = \langle X_1^2, X_2^2 \rangle \in \mathbb{K}[X_1, X_2]$ demostramos que la igualdad no siempre se verifica. □

Nota. Si \mathbb{K} es algebraicamente cerrado, el *Teorema de los Ceros de Hilbert* asegura que $I(V(I)) = \sqrt{I}$. La versión débil del Teorema de los Ceros de Hilbert asegura que si \mathbb{K} es algebraicamente cerrado, entonces $V(I) = \emptyset$ si y solo si $1 \in I$. (las demostraciones de ambos teoremas se encuentran en [Ful]).

Ideales cociente

Ahora vamos a definir qué son los ideales cocientes, y cuál es la variedad afín de un ideal cociente.

3.6 Proposición-Definición. Sean I, J ideales de $\mathbb{K}[X_1, \dots, X_n]$. Definimos el ideal cociente de I por J

$$I : J = \{f \in \mathbb{K}[X_1, \dots, X_n] : fg \in I, \forall g \in J\}.$$

Además $I \subset I : J$.

Demostración. Para probar que $I \subset I : J$ es suficiente con la definición de ideal, ya que para todo $g \in \mathbb{K}[X_1, \dots, X_n]$, y por tanto para todo $g \in J$, $fg \in I$. Para probar que $I : J$ es un ideal, hay que verificar que se cumplen las tres propiedades, lo cual es inmediato.

□

Ahora vamos a definir los cerrados de Zariski, ya que los utilizaremos para demostrar el siguiente teorema.

3.7 Definición. La *clausura de Zariski* de un subespacio de un espacio afín es la variedad afín más pequeña que contiene el conjunto. Si, $S \in \mathbb{K}^n$, la clausura de Zariski se denota por \bar{S} y es igual a $V(I(S))$.

3.8 Lema. Sean I y J ideales de $\mathbb{K}[X_1, \dots, X_n]$. Entonces

$$V(I : J) \supset \overline{V(I) \setminus V(J)}$$

y además si \mathbb{K} es algebraicamente cerrado y I es radical, se tiene la igualdad.

Demostración. Veamos primero que $I : J \subset I(V(I) \setminus V(J))$.

Sea $f \in I : J$ y $\mathbf{x} \in V(I) \setminus V(J)$. Por la definición de ideal cociente $fg \in I$ para todo $g \in J$. Como $\mathbf{x} \in V(I)$, $f(\mathbf{x})g(\mathbf{x}) = 0$, para cualquier $g \in J$. Como \mathbf{x} no pertenece a $V(J)$, entonces, para algún $g \in J$, $g(\mathbf{x}) \neq 0$. Luego, obligatoriamente $f(\mathbf{x}) = 0$ para todo $\mathbf{x} \in V(I) \setminus V(J)$, y por tanto $I : J \subset I(V(I) \setminus V(J))$. Calculando la variedad afín de los ideales a ambos lados de la igualdad concluimos la primera parte de la demostración ya que

$$V(I : J) \supset V(I(V(I) \setminus V(J))) = \overline{V(I) \setminus V(J)},$$

donde la contención se debe a que la variedad invierte la inclusión y la igualdad a la definición de la clausura de Zariski.

Supongamos ahora que \mathbb{K} es algebraicamente cerrado y que I es radical. Sea $\mathbf{x} \in V(I : J)$, es decir, si $hg \in I$ para todo $g \in J$, entonces $h(\mathbf{x}) = 0$. Ahora tomamos $h \in I(V(I) \setminus V(J))$, luego h se anula en $V(I) \setminus V(J)$. Si $g \in J$, g se anula en $V(J)$, luego hg se anula en $V(I)$, luego por el teorema de Nullstellensatz $hg \in \sqrt{I} = I$, para todo $g \in J$. Como antes habíamos visto $h(\mathbf{x}) = 0$, $\mathbf{x} \in V(I(V(I) \setminus V(J)))$, y concluimos.

□

3.9 Corolario. Sean V y W variedades en \mathbb{K}^n . Entonces

$$I(V) : I(W) = I(V \setminus W).$$

Demostración. En la demostración de la proposición anterior vimos que $I : J \subset I(V(I) \setminus V(J))$. Basta considerar $I = I(V)$ y $J = I(W)$: $I(V) : I(W) \subset I(V(I(V)) \setminus V(I(W))) = I(V \setminus W)$.

La otra inclusión se deduce de la definición de ideal cociente.

□

3.2. Bases de Gröbner

Aunque el concepto de bases de Gröbner corresponde al tema 2 de la asignatura optativa *Álgebra conmutativa y computacional*, [DN], y algunos de los conceptos enunciados se estudian en ella, aparecen en esta sección porque son la base del capítulo siguiente.

En esta sección consideraremos que estamos trabajando en el anillo de polinomios $\mathbb{K}[X_1, \dots, X_n]$, que denotaremos por R . Empezaremos definiendo qué es un orden monomial, ya que es indispensable fijar uno cuando trabajamos con bases de Gröbner, pues los resultados computacionales dependen del orden fijado.

3.10 Definición. Un *orden monomial* en R es una relación \prec en $\mathbb{Z}_{\geq 0}^n$, esto es, una relación en el conjunto de monomios X^α , $\alpha \in \mathbb{Z}_{\geq 0}^n$, que satisfaga:

1. \prec es una relación de orden total en $\mathbb{Z}_{\geq 0}^n$.
2. Si $\alpha < \beta$ y $\gamma \in \mathbb{Z}_{\geq 0}^n$, entonces $\alpha + \gamma < \beta + \gamma$.
3. \prec es un *buen orden* en $\mathbb{Z}_{\geq 0}^n$, es decir, todo conjunto no vacío de $\mathbb{Z}_{\geq 0}^n$ tiene elemento minimal para \prec .

A continuación vamos a presentar los órdenes monomiales más importantes:

3.11 Definición. Sea $\alpha = (\alpha_1, \dots, \alpha_n)$ y $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$.

(i) *Orden lexicográfico (lex):*

Decimos que $\alpha >_{lex} \beta$ si, en el vector $\alpha - \beta \in \mathbb{Z}^n$, la primera entrada por la izquierda distinta de cero es positiva. Escribiremos también $X^\alpha >_{lex} X^\beta$ si $\alpha >_{lex} \beta$.

(ii) *Orden lexicográfico graduado (grlex):*

Decimos que $\alpha >_{grlex} \beta$ si

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

(iii) *Orden lexicográfico graduado inverso (grevlex)*:

Decimos que $\alpha >_{grevlex} \beta$ si

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

y, en el vector $\alpha - \beta \in \mathbb{Z}^n$ la primera entrada por la derecha distinta de cero es negativa .

3.12 Definición-Notación. Sea

$$f = \sum_{\text{finita}} a_\alpha X^\alpha$$

un polinomio distinto de 0 en $\mathbb{K}[X_1, \dots, X_n]$. Fijamos sobre $\mathbb{K}[X_1, \dots, X_n]$ un orden monomial.

1. Cada uno de los a_α se llama *coeficiente del monomio* X^α .
2. Si $a_\alpha \neq 0$ entonces $a_\alpha X^\alpha$ es un *término de* f .
3. El *multigrado total de* f , denotado $\text{multideg}(f)$ es el mayor α tal que $a_\alpha \neq 0$.
4. Llamamos *monomio dominante de* f , y denotamos por $\text{LM}(f)$, a $X^{\text{multideg}(f)}$.
5. Llamamos *coeficiente dominante de* f , y denotamos por $\text{LC}(f)$, al coeficiente $a_{\text{multideg}(f)}$.
6. Llamamos *término dominante de* f , y denotamos por $\text{LT}(f)$, al producto $\text{LC}(f) \cdot \text{LM}(f)$.

3.13 Definición. Sea G un subconjunto de $\mathbb{K}[X_1, \dots, X_n]$ el *ideal inicial* de G se define

$$\text{LT}(G) := \langle \text{LM}(g) : g \in G \setminus \{0\} \rangle.$$

En particular estamos interesados en el caso de que G sea un ideal, ya que nos permite definir las bases de Gröbner.

3.14 Definición. Fijado un orden monomial, se define una base de Gröbner, $\mathcal{G} = \{g_1, \dots, g_s\}$, de un ideal I de R como un subconjunto finito de elementos de I , cuyos monomios iniciales generan $\text{LT}(I)$, es decir, se verifica

$$\langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle = \langle \text{LT}(I) \rangle.$$

Por el Teorema de la Base de Hilbert ([CLS, 73]) todo ideal no nulo I de R admite una base de Gröbner.

3.15 Proposición. *Toda base de Gröbner de un ideal I es sistema de generadores de I .*

Demostración. $\mathcal{G} = \{g_1, \dots, g_s\}$ es una base de Gröbner de I .

Es evidente que el ideal generado por los elementos de \mathcal{G} está contenido en I , $(\mathcal{G}) \subset I$. Veamos ahora que también se verifica la otra inclusión. Sea $f \in I$, utilizando el algoritmo de división de polinomios, escribimos $f = f_1g_1 + \dots + f_sg_s + r$, donde $q_1, \dots, q_s, r \in R$ y tales que para todo monomio $\mathbb{X}^\alpha \in \text{supp}(r)$, $\mathbb{X}^\alpha \notin (LT(g_1), \dots, LT(g_s))$. Pero por otra parte $(LT(g_1), \dots, LT(g_s)) = LT(I)$ porque \mathcal{G} es base de Gröbner de I . Luego si $r \neq 0$, $LT(r) \notin LT(I)$, y tenemos una contradicción porque $r = f - (f_1g_1 + \dots + f_sg_s) \in I$. Luego concluimos que $r = 0$, y por tanto $f \in (\mathcal{G})$. □

3.16 Proposición. *Sea $\mathcal{G} = \{g_1, \dots, g_s\}$ una base de Gröbner de un ideal I de R con respecto a un orden monomial fijado sobre R . Para todo elemento f de R existen dos polinomios $q, r \in R$ únicos, que verifican:*

- $f = q + r$,
- $q \in I$,
- $\forall \mathbb{X}^\alpha \in \text{supp}(r)$, $\mathbb{X}^\alpha \notin (LT(g_1), \dots, LT(g_s))$.

Demostración. Primero veamos que existen q y r cumpliendo las condiciones de la proposición. Si dividimos f entre todos los elementos de \mathcal{G} , obtenemos $f = f_1g_1 + \dots + f_sg_s + r$, donde f_1, \dots, f_s, r son elementos de R . Poniendo $q = f_1g_1 + \dots + f_sg_s$ y concluimos. Veamos ahora que q y r son únicos. Sean $q, q', r, r' \in R$, $q, q' \in I$ y r, r' que verifican $f = q + r = q' + r'$. Razonamos por reducción al absurdo: Suponemos que $r \neq r'$. Entonces tenemos que $0 \neq r - r' = q' - q \in I$ y por lo tanto $(r - r') \in (LT(g_1), \dots, LT(g_s))$ porque \mathcal{G} es base de Gröbner. Como $LT(r - r') \in \text{supp}(r) \cup \text{supp}(r')$, hemos llegado a una contradicción. Luego $r = r'$. □

3.17 Corolario. *Fijamos un orden monomial en R . Sea $\mathcal{G} = \{g_1, \dots, g_s\}$ una base de Gröbner de un ideal I de R y f un polinomio de R . Las siguientes condiciones son equivalentes:*

1. $f \in I$.

2. El resto de la división de f entre los elementos de \mathcal{G} es 0.

Demostración. (2) \Rightarrow (1): Basta aplicar el teorema 3.15. (1) \Rightarrow (2): Como $f \in I$ basta considerar $q = f$ y $r = 0$, y escribir $f = q + r$, donde $q \in (\mathcal{G})$. Aplicamos la proposición 3.16 y concluimos que r es único, y por tanto tiene que ser 0.

□

3.18 Definición. Sea $I \in \mathbb{K}[X_1, \dots, X_n]$ un ideal, llamamos *monomios estándar* de I , y denotamos por $\mathfrak{B}_{\prec}(I)$ a los monomios que no son dominantes de ningún polinomio en I .

3.19 Definición. Sea $\mathcal{G} = \{g_1, \dots, g_s\}$ una base de Gröbner. Se dice que es una *base de Gröbner reducida* si verifica, para todo $i \in \{1, \dots, s\}$:

1. $LC(g_i) = 1$.
2. $LM(g_i)$ no es divisible por $LM(g_j)$ para $i \neq j$.
3. $\text{supp}(g_i - LM(g_i)) \subset \mathfrak{B}_{\prec}(I)$.

3.3. Ideales 0-dimensionales

3.20 Definición. Se dice que un ideal tiene *dimension de Krull 0* o que es *0-dimensional* si $V(I)$ es finito.

3.21 Proposición. Sea \mathbb{K} algebraicamente cerrado. Sea $R = \mathbb{K}[X_1, \dots, X_n]$ dotado de un orden monomial. Son equivalentes:

1. I es 0-dimensional.
2. R/I es un \mathbb{K} espacio vectorial de dimensión finita.

Demostración. (1) \Rightarrow (2): Si I es 0-dimensional, podemos tener dos casos, que $V(I)$ sea vacío o que tenga un número finito de elementos:

Si $V(I) = \emptyset$, entonces el polinomio constante 1 está en el ideal (por 3.1), y $R/I = 0$.

Sino, sea $X_i \in R/I$, y consideramos $[X_i^j]$, $j = 1, 2, \dots$. Como R/I es de dimensión finita, existe $m \in \mathbb{N}$, y existen $c_i \in R$, $1 \leq i \leq n$ tales que

$$[0] = \sum_{j=0}^m c_j [X_i^j] = \left[\sum_{j=0}^m c_j X_i^j \right]$$

luego

$$\sum_{j=0}^m c_j X_i^j \in I,$$

y como \mathbb{K} es algebraicamente cerrado, la ecuación

$$\sum_{j=0}^m c_j X_i^j = 0$$

tiene a lo sumo m soluciones. Esto es, si $\mathbf{x} = (x_1, \dots, x_n) \in V(I)$ solo hay m_i posibles valores para la componente i -ésima.

(2) \Rightarrow (1): Sea $V(I) = \{\mathbf{v}^1, \dots, \mathbf{v}^r\} \in \mathbb{K}^n$, con $\mathbf{v}^i = (v_1^i, \dots, v_n^i)$, $1 \leq i \leq r$. Definimos

$$f_j(X_j) = \prod_{i=1}^p (X_j - v_j^i)$$

que, por construcción, es un elemento de $I(V(I)) = \sqrt{I}$. Es decir, existe $m_j \in \mathbb{N}$ tal que $f_j^{m_j}(X_j) \in I$.

Haciendo lo mismo con cada indeterminada conseguimos

$$f_1^{m_1}(X_1), \dots, f_n^{m_n}(X_n) \in I,$$

es decir,

$$\langle f_1^{m_1}(X_1), \dots, f_n^{m_n}(X_n) \rangle \subset I.$$

Por lo tanto

$$R/I \subset R/\langle f_1^{m_1}(X_1), \dots, f_n^{m_n}(X_n) \rangle.$$

□

3.22 Lema. Sea $R = \mathbb{K}[X_1, \dots, X_n]$ dotado de un orden monomial e I un ideal 0-dimensional de R . Entonces $\dim_{\mathbb{K}} R/I \geq |V(I)|$.

Nota. $\dim_{\mathbb{K}} R/I$ es la dimensión de R/I como espacio vectorial sobre \mathbb{K} .

Demostración. Sea $V(I) = \{\mathbf{v}^1, \dots, \mathbf{v}^r\} \subset \mathbb{K}^n$. Definimos los polinomios f_i , $1 \leq i \leq r$

$$f_i(\mathbf{X}) = \frac{\prod_{j=1, j \neq i}^r (\mathbf{X} - \mathbf{v}^j)}{\prod_{j=1, j \neq i}^r (\mathbf{v}^i - \mathbf{v}^j)}.$$

Por construcción, f_1, \dots, f_r no pertenecen a I (ya que $f_i(v_j)$ vale 1 si $i = j$ y 0 sino).

Si probamos que $[f_1], \dots, [f_r] \subset R/I$ son linealmente independientes, entonces $r \leq \dim_{\mathbb{K}} R/I$ y habremos terminado la demostración.

Vamos a probarlo razonando por reducción al absurdo: si no fueran linealmente independientes, existirían $c_i \in R$ $1 \leq i \leq r$ tales que

$$[0] = \sum_{i=1}^r c_i [f_i] = [\sum_{i=1}^r c_i f_i].$$

Sea $g = \sum_{i=1}^r c_i f_i \in I$, luego g se anula en todo $V(I) = \{\mathbf{v}^1, \dots, \mathbf{v}^r\} \subset \mathbb{K}^n$. Luego para $1 \leq i \leq r$ tenemos

$$0 = g(\mathbf{v}^i) = \sum_{i=1}^r (c_i f_i)(\mathbf{v}^i) = 0 + (c_i f_i)(\mathbf{v}^i) = c_j$$

Luego, $[f_1], \dots, [f_r]$ son linealmente independientes.

□

3.23 Lema. *Sea I un ideal 0-dimensional. Los siguientes enunciados son equivalentes:*

1. I es un ideal radical
2. I contiene un polinomio libre de cuadrados en cada indeterminada
3. $|\mathfrak{B}_{\prec}(I)| = |V(I)|$.

Demostración. Tenemos la equivalencia (1) \Leftrightarrow (3) por [CLS, Teorema 10] y por [CLS, Proposición 4]. Además, por [CLS, Proposición 2.7] si I es radical, $p_{i,red} \in I$, $\forall i$ y por tanto (1) \Rightarrow (2). Respectivamente, si (2) es cierto, entonces $p_{i,red} = p_i$ y por tanto I es radical.

□

En resumen, si I es 0-dimensional y radical, entonces se verifica

$$|V(I)| = \dim_{\mathbb{K}} \mathbb{K}[X_1, \dots, X_n]/I = |\mathfrak{B}_{\prec}(I)|.$$

Capítulo 4

Aplicación a la colorabilidad de grafos

En el capítulo anterior apuntamos que las bases de Gröbner servían para resolver algunos problemas de ideales de polinomios. En este capítulo nos centramos en el problema de coloración de grafos simples no orientados, y en particular en reconocer cuándo uno de estos grafos es únicamente k -coloreable. Trabajaremos principalmente con los resultados en [HW] y [LHM].

Además, en este capítulo consideraremos:

- \mathbb{K} es un cuerpo algebraicamente cerrado.
- G , al igual que en el capítulo 2, G será un grafo simple, no orientado, de vértices V , y aristas E .
- $R = \mathbb{K}[X_1, \dots, X_n]$ un anillo sobre \mathbb{K} en las indeterminadas X_1, \dots, X_n .
- C_k el conjunto de las raíces k -ésimas de la unidad, y la coloración de un grafo G de n vértices se representará por el vector (v_1, v_2, \dots, v_n) , $v_i \in C_k, \forall i$.

4.1. Caracterizaciones polinomiales de la k -coloración

4.1 Definición. El *polinomio asociado al grafo* G viene dado por

$$f_G = \prod_{\{i,j\} \in E, i < j} (x_i - x_j)$$

4.2 Definición-Notación. Sea $k < n$ un entero positivo y suponemos que la característica de \mathbb{K} no es divisible por k . Sea \mathcal{H} el conjunto de grafos con n vértices, formados por el grafo completo de $k + 1$ vértices (K_{k+1}), y el resto de vértices, aislados.

Nos interesan los siguientes ideales de R :

$$\begin{aligned} J_{n,k} &= \langle f_H : H \in \mathcal{H} \rangle \\ I_{n,k} &= \langle X_i^k - 1 : i \in V \rangle \\ I_{G,k} &= I_{n,k} + \langle \frac{X_i^k - X_j^k}{X_i - X_j} : \{i, j\} \in E \rangle \end{aligned} \tag{4.1}$$

Nota. Para simplificar, dado que el cuerpo va a ser irrelevante, podemos suponer que $\mathbb{K} = \mathbb{C}$.

Veamos que estos ideales nos permiten dar una formulación algebraica de la k -colorabilidad.

4.3 Lema. Los ideales $I_{n,k}$, $I_{G,k}$ e $I_{n,k} + \langle f_G \rangle$ son 0-dimensionales.

Demostración. Como $I_{n,k} \subset I_{G,k}$ e $I_{n,k} \subset I_{n,k} + \langle f_G \rangle$ bastará probar que $V(I_{n,k})$ es finito. Pero $V(I_{n,k}) = \{\mathbf{v} = (v_1, \dots, v_n) : v_i \text{ raíz } k\text{-ésima de } 1\}$, luego $|V(I_{n,k})| = k^n < \infty$. □

4.4 Proposición. Las variedades $V(I_{n,k})$, $V(I_{G,k})$ y $V(I_{n,k} + \langle f_G \rangle)$ están en biyección con todas las k -coloraciones, las k -coloraciones propias y las k -coloraciones impropias de G , respectivamente.

Demostración. En la demostración del lema anterior describimos $V(I_{n,k})$, como las n -uplas de raíces k -ésimas de la unidad, luego corresponden a todas las k -coloraciones posibles de G por definición. Veamos ahora que las coloraciones impropias están en biyección con $V(I_{n,k} + \langle f_G \rangle)$. Sea $\mathbf{v} = (v_1, \dots, v_n) \in V(I_{n,k})$ una coloración de G . $\mathbf{v} \in V(I_{n,k} + \langle f_G \rangle) \Leftrightarrow \mathbf{v} \in V(f_G) \Leftrightarrow f_G(\mathbf{v}) = 0 \Leftrightarrow v_i = v_j$ para algún $\{i, j\} \in E \Leftrightarrow \mathbf{v}$ es una k -coloración impropia. Por último veamos que las coloraciones propias están en biyección con $V(I_{G,k})$. Sea $\mathbf{v} = (v_1, \dots, v_n) \in V(I_{n,k})$, $\mathbf{v} \in V(I_{G,k}) \Leftrightarrow \mathbf{v} \in V(\frac{X_i^k - X_j^k}{X_i - X_j}, \forall \{i, j\} \in E) \Leftrightarrow \frac{v_i^k - v_j^k}{v_i - v_j} = 0, \forall \{i, j\} \in E \Leftrightarrow v_i \neq v_j \forall \{i, j\} \in E$, porque si $v_i = v_j$, para algún $\{i, j\} \in E$, entonces $\frac{v_i^k - v_j^k}{v_i - v_j} = kv_i^{k-1} \neq 0$. □

Ahora veamos algunos resultados sobre los ideales definidos en (4.1) que más adelante nos permitirán traducir los conceptos algebraicos al lenguaje geométrico y viceversa.

4.5 Lema. *Los ideales $I_{n,k}$, $I_{G,k}$ y $I_{n,k} + \langle f_G \rangle$ son radicales.*

Demostración. La demostración es trivial porque como por 4.3, los ideales son 0-dimensionales, podemos aplicar el lema 3.23, y como los polinomios que generan $I_{n,k}$ son libres de cuadrado en cada indeterminada, los tres ideales son radicales. □

4.6 Lema. *Se verifica la siguiente relación:*

$$I_{n,k} : I_{G,k} = I_{n,k} + \langle f_G \rangle.$$

Demostración.

$$I_{n,k} : I_{G,k} = I(V(I_{n,k})) : I(V(I_{G,k})) = I(V(I_{n,k}) \setminus V(I_{G,k})) = I(V(I_{n,k} + \langle f_G \rangle)).$$

Donde la primera igualdad se debe a que los ideales son radicales (lema 4.5 y teorema de los Ceros de Hilbert [CLS, pag.73]), la segunda al corolario 3.9 y la tercera al lema 4.4. □

4.7 Lema. *Sea χ_G el polinomio cromático de G . Se verifica:*

$$\chi_G(k) = \dim_{\mathbb{K}} R/I_{G,k},$$

$$k^n - \chi_G(k) = \dim_{\mathbb{K}} R/(I_{n,k} + \{f_G\}).$$

Demostración. En el capítulo 2 definimos el polinomio cromático $\chi_G(k)$ como el número de coloraciones de un grafo G (de n vértices) con k colores. Además, como el número de k -coloraciones de G es k^n , el número de coloraciones impropias será $k^n - \chi_G(k)$. Luego $\chi_G(k) = |V(I_{G,k})|$ y $k^n - \chi_G(k) = |V(I_{G,k} + \{f_G\})|$. Aplicando el lema 3.23 quedan probadas las igualdades. □

Volvamos ahora al ejemplo 2.7 y calculemos de esta forma los polinomios cromáticos de los grafos G y H . Para ello vamos a usar el programa “Singular” [Sin]: Fijamos el anillo y el orden monomial. Trabajamos en \mathbb{Q} porque aunque para la teoría necesitamos un cuerpo algebraicamente cerrado y de característica no divisible por k , en la práctica, para los cálculos a continuación, nos da lo mismo, así que tomamos el cuerpo de característica 0 por defecto.

```
> ring R= 0, x(1..5),dp;
```

Vamos a calcular el número cromático de G :

```
> ideal IG= x(1)^3-1, x(2)^3-1, x(3)^3-1, x(4)^3-1, x(5)^3-1,
x(1)^2+x(1)*x(4)+x(4)^2, x(1)^2+x(1)*x(5)+x(5)^2,
x(4)^2+x(4)*x(5)+x(5)^2, x(2)^2+x(2)*x(3)+x(3)^2,
x(3)^2+x(3)*x(5)+x(5)^2, x(2)^2+x(2)*x(5)+x(5)^2;
> vdim(groebner(IG));
==>12
```

Ahora calculamos el número cromático de H :

```
> ideal IH= IG, x(3)^2+x(3)*x(4)+x(4)^2;
> vdim(groebner(IH))
==>6
```

Evidentemente hemos obtenido los mismos resultado que en 2.7, pero esta vez el cálculo ha sido inmediato.

Ahora que ya tenemos los conceptos necesarios vamos a dar una caracterización para la no k -colorabilidad de un grafo, y para ello nos vamos a apoyar en el teorema de Kleitman-Lovász.

4.8 Teorema (Kleitman-Lovász). *Sea $K_{n,k}$ el ideal de todos los polinomios $f \in R$ tales que $f(v_1, \dots, v_n) = 0$ para todos los $(v_1, \dots, v_n) \in \mathbb{K}^n$ con a lo sumo k componentes distintas. Entonces*

$$K_{n,k} = J_{n,k}.$$

La prueba del teorema se encuentra en [Lov], y no se incluye en este trabajo. Este resultado es fundamental para demostrar el siguiente teorema.

4.9 Teorema. *Los siguientes enunciados son equivalentes:*

1. G no es k -coloreable.

2. $\dim_{\mathbb{K}} R/I_{G,k} = 0$.
3. El polinomio constante 1 pertenece al ideal $I_{G,k}$.
4. El polinomio f_G pertenece al ideal $I_{n,k}$.
5. El polinomio f_G pertenece al ideal $J_{n,k}$.

Demostración. (1) \Rightarrow (2): Supongamos que G no es k -coloreable. Entonces por el lema 4.7 obtenemos (2). (2) \Rightarrow (3): Como ya hemos visto antes $\dim_{\mathbb{K}} R/I_{G,k} = |\mathcal{B} \prec (I_{G,k})|$, luego $1 \in I_{G,k}$. (3) \Rightarrow (4): Si $I_{G,k} = \langle 1 \rangle$, podemos escribir $I_{n,k} = I_{n,k} : I_{G,k} = I_{n,k} + \langle f_G \rangle$, por el lema 4.6. Luego $f_G \in I_{n,k}$. (4) \Rightarrow (1): Supongamos que $f_G \in I_{n,k}$, es decir, $I_{n,k} + \langle f_G \rangle = I_{n,k}$, como ya hemos visto, y por el lema 2.14, $k^n - \chi_G(k) = k^n$; luego $\chi_G(k) = 0$, con lo que hemos demostrado (1). (1) \Rightarrow (5): Si G no es k -coloreable, entonces para todo $\mathbf{v} = (v_1, \dots, v_n)$ con a lo sumo k componentes distintas se verifica $f_G(\mathbf{v}) = 0$, luego $f_G \in K_{n,k} = J_{n,k}$ (donde la igualdad se verifica por el teorema 4.8). (5) \Rightarrow (1): Supongamos $f_G \in J_{n,k} = K_{n,k}$ (donde la igualdad ocurre por el teorema 4.8), es decir, para todo $\mathbf{v} \in \mathbb{K}^n$ con a lo sumo k entradas distintas, $f_G(\mathbf{v}) = 0$. Esto implica que en G hay al menos dos vértices adyacentes tienen el mismo color para toda k -coloración, luego G no es k -coloreable. □

4.2. Ideales de coloración

Esta sección se compone de toda la mecánica necesaria para probar los teoremas de la sección siguiente.

Puesto que vamos a trabajar con bases de Gröbner y con el Algoritmo de División de polinomios en varias variables ([CLS, pag.61-69]) necesitamos fijar un orden monomial en R . Así, a lo largo de esta sección vamos a suponer que tenemos un orden monomial \prec fijado.

4.10 Definición-Notación. Sea ν una k -coloración propia del grafo G , y sea $l \leq k$ el número de colores que empleamos en la coloración.

- La *clase de color* de un vértice $i \in V$, denotada $cl(i)$, es el conjunto de vértices con el mismo color que i .
- El *máximo* de la clase $cl(i)$ es el mayor vértice contenido en la clase. De este modo ponemos $m_1 < m_2 < \dots < m_l = n$ los máximos de las l clases de color.

Notación. Sea U un subconjunto de los vértices de un grafo. Denotaremos h_U^d el polinomio de grado d obtenido como la suma de todos los monomios de grado d en las indeterminadas $\{X_i; i \in U\}$. Además, definimos $h_U^0 = 1$.

Ahora vamos a definir los conceptos de ν -base y ν -base reducida.

4.11 Definición. Sea ν una k -coloración propia de G . Para cada vértice $i \in V$ definimos de la siguiente manera los polinomios g_i :

$$g_i = \begin{cases} X_i^k - 1 & \text{si } i = m_l = n, \\ h_{\{m_j, \dots, m_l\}}^{k-l+j} & \text{si } i = m_j \text{ para algún } j \neq l, \\ X_i - X_{\max_{cl(i)}} & \text{si no.} \end{cases} \quad (4.2)$$

El conjunto $\{g_1, \dots, g_n\}$ se llama ν -base del grafo G respecto de la coloración ν .

Nota. La aplicación $\nu \mapsto \{g_1, \dots, g_n\}$ depende solamente de cómo son las particiones de los vértices en las clases de color. En particular, si el grafo es únicamente k -coloreable, el conjunto $\{g_1, \dots, g_n\}$ es único.

4.12 Definición. Sea ν una k -coloración propia de G . El k -ideal de coloración, o simplemente *ideal de coloración* (si k está claro por el contexto) asociado a ν es el ideal

$$A_\nu = \langle g_1, \dots, g_n \rangle,$$

donde los g_i se definen como en (4.2).

4.13 Lema. *El conjunto de polinomios $\{g_1, \dots, g_n\}$ es una base de Gröbner minimal para el ideal $A_\nu = \langle g_1, \dots, g_n \rangle$ que genera para cualquier orden monomial con $X_1 \succ \dots \succ X_n$.*

Demostración. Es una base de Gröbner del ideal que generan porque para cada i , $LT(g_i)$ es una potencia de X_i . En efecto, el conjunto $\{LT(g_i), 1 \leq i \leq n\}$ es

$$\{X_{m_1}^{k-l+1}, X_{m_2}^{k-l+2}, \dots, X_{m_l}^k\} \cup \{X_i : i \neq m_j \forall j\},$$

cuyos elementos son primos entre si y por [CLS, Prop. 4 p. 101] es una base de Grobner y además es minimal.

□

4.14 Definición. Sea ν una k -coloración propia de G . Para cada vértice $i \in V$ definimos de la siguiente manera los polinomios \tilde{g}_i :

$$\tilde{g}_i = \begin{cases} X_i^k - 1 & \text{si } i = m_l, \\ h_{\{m_j, \dots, m_l\}}^j & \text{si } i = m_j \text{ para algun } j \neq l, \\ h_{i, m_2, \dots, m_l}^1 & \text{si } i \in cl(m_1) \\ X_i - X_{\max cl(i)} & \text{si no.} \end{cases} \quad (4.3)$$

El conjunto $\{\tilde{g}_1, \dots, \tilde{g}_n\}$ se llama ν -base reducida del grafo G respecto de la coloración ν .

Nota. También podemos usar la definición anterior para calcular la coloración propia de un grafo haciendo el procedimiento inverso, más adelante veremos un ejemplo.

4.15 Corolario. Si $k = l$, los ideales polinomiales generados por (4.2) y por (4.3) coinciden.

Demostración. Sea $l = k$. Si $i \in cl(m_1) \setminus \{m_1\}$, entonces $g_i = X_i - X_{m_1} = \tilde{g}_i - \tilde{g}_{m_1}$. Luego ya hemos acabado porque si $i \notin cl(m_1) \setminus \{m_1\}$, $g_i = \tilde{g}_i$.

□

4.16 Lema. El conjunto de polinomios $\{\tilde{g}_1, \dots, \tilde{g}_n\}$ es la base de Gröbner reducida para el ideal $\langle \tilde{g}_1, \dots, \tilde{g}_n \rangle$ que genera, para cualquier orden monomial $X_1 \succ \dots \succ X_n$.

Demostración. Es una base de Gröbner del ideal que generan porque para cada i , $LT(\tilde{g}_i)$ es una potencia de X_i . Por lo tanto, los $LT(\tilde{g}_i)$ son primos dos a dos, luego $\{\tilde{g}_1, \dots, \tilde{g}_n\}$ es base de Gröebner. Además es reducida porque el coeficiente de cada monomio dominante es 1 y para todo i , $1 \leq i \leq n$, $LM(\tilde{g}_i) \nmid LM(\tilde{g}_j)$, si $j \neq i$; y tampoco divide a los demás monomios del soporte de \tilde{g}_i .

□

4.17 Lema. Sea $U \subset \{1, \dots, n\}$, e $\{i, j\} \subset U$, entonces para todo entero d no negativo se verifica

$$(X_i - X_j)h_U^d = h_{U \setminus \{j\}}^{d+1} - h_{U \setminus \{i\}}^{d+1}.$$

Demostración. Como $h_U^{d+1} - h_{U \setminus \{i\}}^{d+1} = X_i h_U^d$, y h_U^{d+1} es simétrico en las indeterminadas $\{X_l : l \in U\}$, el polinomio $X_i h_U^d + h_{U \setminus \{i\}}^{d+1}$ también lo es. Tomamos la permutación $\sigma = (i, j)$ y obtenemos:

$$X_i h_U^d + h_{U \setminus \{i\}}^{d+1} = \sigma(X_i h_U^d + h_{U \setminus \{i\}}^{d+1}) = X_j h_U^d + h_{U \setminus \{j\}}^{d+1}.$$

□

4.18 Lema. *Para cada $i = 1, \dots, l$ se verifica*

$$X_{m_i}^k - 1 = X_n^k - 1 + \sum_{t=i}^{l-1} \left[\prod_{j=t+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_t, \dots, m_l\}}^{k-l+t}.$$

Demostración. Para probar este lema, veamos primero que:

$$\begin{aligned} & \sum_{t=i}^{l-1} \left[\prod_{j=t+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_t, \dots, m_l\}}^{k-l+t} = \\ &= \left[\prod_{j=s+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_i, m_{s+i}, \dots, m_l\}}^{k-l+s+i-1} + \sum_{t=s+i}^{l-1} \left[\prod_{j=t+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_t, \dots, m_l\}}^{k-l+t}. \end{aligned}$$

Usaremos el Principio de Inducción:

Para $s = 1$ es cierto.

Supongamos que es cierto para $s \leq l - i$ y veamos que también lo es para el natural siguiente:

$$\begin{aligned} & \sum_{i=1}^{l-1} \left[\prod_{j=t+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_t, \dots, m_l\}}^{k-l+t} = \\ &= \left[\prod_{j=s+i}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_i, m_{s+i}, \dots, m_l\}}^{k-l+s+i-1} + \sum_{t=s+i}^{l-1} \left[\prod_{j=t+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_t, \dots, m_l\}}^{k-l+t} \\ &= \prod_{j=s+i+1}^l (X_{m_i} - X_{m_j}) (X_{m_i} - X_{m_{s+i}}) h_{\{m_i, m_{s+i}, \dots, m_l\}}^{k-l+s+i-1} + \sum_{t=s+i+1}^{l-1} \left[\prod_{j=t+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_t, \dots, m_l\}}^{k-l+t} + \\ & \quad + \left[\prod_{j=s+i+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_{s+i}, \dots, m_l\}}^{k-l+s+i} \end{aligned}$$

Por el lema anterior:

$$\begin{aligned}
&= \left[\prod_{j=s+i+1}^l (X_{m_i} - X_{m_j}) \right] (h_{\{m_i, m_{s+i+1}, \dots, m_l\}}^{k-l+s+i} - h_{\{m_{s+i}, \dots, m_l\}}^{k-l+s+i}) \\
&+ \sum_{t=s+i+1}^{l-1} \left[\prod_{j=t+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_t, \dots, m_l\}}^{k-l+t} + \left[\prod_{j=s+i+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_{s+i}, \dots, m_l\}}^{k-l+s+i} \\
&= \left[\prod_{j=s+i+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_i, m_{s+i+1}, \dots, m_l\}}^{k-l+s+i} + \sum_{t=s+i+1}^{l-1} \left[\prod_{j=t+1}^l (X_{m_i} - X_{m_j}) \right] h_{\{m_t, \dots, m_l\}}^{k-l+t}
\end{aligned}$$

Luego, la igualdad es cierta para $s \leq l - i$.

Tomando ahora $s = l - i$:

$$\begin{aligned}
&X_n^k - 1 + \prod_{j=l}^l (X_{m_i} - X_{m_j}) h_{\{m_i, m_l\}}^{k-1} \\
&= X_n^k - 1 + (X_{m_i} - X_{m_l}) h_{\{m_i, m_l\}}^{k-1}
\end{aligned}$$

Y otra vez por el lema anterior:

$$\begin{aligned}
&= X_n^k - 1 + h_{m_i}^k - h_{m_l}^k = X_n^k - 1 + X_{m_i}^k - X_{m_l}^k \\
&= X_n^k - 1 + X_{m_i}^k - X_n^k = X_{m_i}^k - 1.
\end{aligned}$$

□

Veamos ahora un teorema que nos permita saber si un grafo tiene coloraciones propias.

4.19 Lema. Sean g_1, \dots, g_n definidos como en (4.2). Entonces $I_{G,k} \subset A_\nu$.

Demostración. Veamos que todos los generadores de $I_{n,k}$ se pueden escribir en función de los generadores de A_ν .

Veamos primero que $\{X_i^k - 1\} \in A_\nu$ para todo $i \in \{1, \dots, n\}$:

a) $i \in m_1, \dots, m_l$, es cierto por el lema 4.18 $X_i^k - 1 \in A_\nu$.

b) Sino, sea $f_i = X_i - X_{\max_{cl(i)}}$. Entonces existe un polinomio $h \in R$ que verifica:

$$X_{\max_{cl(i)}}^k - 1 = (f_i - X_i)^k - 1 = X_i - 1 + f_i h \in A_\nu.$$

Luego $X_i^k - 1 \in A_\nu$ para toda $i \in \{1, \dots, n\}$.

Veamos ahora que los elementos de la forma $\left\{ \frac{(X_i - X_j)^k}{X_i + X_j} : \{i, j\} \in E \right\}$ se pueden escribir en función de los generadores de A_ν . Para ello vamos a probar un enunciado más fuerte:

$$\text{Si } U \subset \{m_1, \dots, m_l\} \text{ con } |U| \geq 2 \text{ entonces } h_U^{k+1-|U|} \in A_\nu. \quad (4.4)$$

Vamos a probarlo por inducción sobre $s = |U|$:

Si $s = l$, $g_{m_1} = h_{\{m_1, \dots, m_l\}}^k - l + 1 \in A_\nu$ definido en 4.2. Luego es cierto.

Supongamos que es cierto para $s+1$ ($s+1 = |U \cup \{v\}|$ para algún $v \in \{m_1, \dots, m_l\} \setminus U$) y veamos que si $h_U^{k+1-|U|} \in A_\nu$, entonces para todo $W \subset \{m_1, \dots, m_l\}$, con $|W| = |U|$, se tiene que $h_W^{k+1-|W|} \in A_\nu$:

Sea $v \in \{m_1, \dots, m_l\} \setminus U$, usando el lema anterior tenemos que:

$$(X_u - X_v)h_{\{v\} \cup U}^{k-s} = h_U^{k-s+1} - h_{\{v\} \cup U \setminus \{u\}}^{k-s+1}.$$

Como el polinomio a la izquierda de la ecuación, y h_U^{k-s+1} están en A_ν , también lo estará $h_{\{v\} \cup U \setminus \{u\}}^{k-s+1}$, luego se verifica para cualquier conjunto $W \subset \{m_1, \dots, m_l\}$, con $|W| = s$.

En particular, si $\{i, j\} \in E$, es decir $cl(i) \neq cl(j)$, tenemos que

$$\frac{(X_i - X_j)^k}{X_i + X_j} \in A_\nu.$$

Como hemos probado que todos los generadores de $I_{n,k}$ se pueden escribir en función de los generadores de A_ν , se verifica: $I_{n,k} \subset A_\nu$.

□

Una vez que hemos visto que un grafo G tiene coloraciones propias, la siguiente pregunta que nos hacemos es cuántas y cuáles. Para responder a esto utilizamos el teorema 4.21, que nos da el número de coloraciones distinguibles. Luego para obtener el número de coloraciones totales habrá que multiplicar por $k!$ (para obtener todas las permutaciones de los colores).

4.20 Lema. Sean g_1, \dots, g_n definidos como en (4.2). Se verifican las siguientes propiedades:

1. A_ν es radical.
2. $|V(A_\nu)| = \prod_{j=1}^l (k - l + j)$.

Demostración. (1) Por el lema anterior $I_{G,k} \subset A_\nu$. A_ν es radical porque contiene un ideal radical (si $I_{G,k}$ contiene un polinomio libre de cuadrado en cada indeterminada, también lo contiene A_ν y aplicamos el lema 3.23).

(2) Por el lema 4.13, $\{g_1, \dots, g_n\}$ es una base de Gröbner minimal de A_ν . Luego

$$\mathfrak{B}_{\prec}(A_\nu) = \prod_{\text{finitos}} X_{m_i}^{k-l+i}$$

donde $1 \leq i \leq l$. Por lo tanto,

$$|\mathfrak{B}_{\prec}(A_\nu)| = \prod_{i=1}^l (k - l + i).$$

□

4.21 Teorema. *Se verifica*

$$I_{G,k} = \bigcap_{\nu} A_\nu,$$

donde ν recorre todas las k -coloraciones propias de G .

Demostración. Como $I_{G,k} \subset A_\nu$ (lema 4.19) y además $V(I_{G,k})$ está en biyección con todas las coloraciones propias (lema 4.4), se verifica que

$$V(I_{G,k}) = \bigcup_{\nu} A_\nu$$

donde ν recorre las coloraciones propias de G .

Los lemas 4.5 y 4.20 aseguran que $V(I_{G,k})$ y A_ν son radicales, y obtenemos

$$I_{G,k} = I(V(I_{G,k})) = I\bigcup_{\nu} V(A_\nu) = \bigcap_{\nu} I(V(A_\nu)) = \bigcap_{\nu} A_\nu.$$

□

4.3. Grafos únicamente k -coloreables

En esta sección daremos los teoremas necesarios para identificar los grafos únicamente k -coloreables. Todos los teoremas se apoyan en el contenido de la sección anterior, por lo que aquí también supondremos un orden monomial \prec fijado sobre R .

4.22 Teorema. *Sea ν una k -coloración de G que usa todos los colores, y sean g_1, \dots, g_n definidos como en (4.2). Los siguientes enunciados son equivalentes:*

1. G es únicamente k -colorable.
2. Los polinomios g_1, \dots, g_n generan el ideal $I_{G,k}$.
3. Los polinomios g_1, \dots, g_n pertenecen al ideal $I_{G,k}$.
4. El polinomio f_G asociado a G pertenece al ideal $I_{n,k} : \langle g_1, \dots, g_n \rangle$.
5. $\dim_{\mathbb{K}} R/I_{G,k} = k!$.

Demostración. (1) \Rightarrow (2): Sea G únicamente k -coloreable, construimos los $\{g_i, 1 \leq i \leq n\}$ para esta coloración propia ν . Como ν es única, aplicando el lema 4.21 $I_{G,k} = A_\nu = \langle g_1, \dots, g_n \rangle$. (2) \Rightarrow (3): Trivial (los generadores de un ideal son elementos de él). (3) \Rightarrow (4): Si $g_1, \dots, g_n \in I_{G,k}$, también se verifica $A_\nu = \langle g_1, \dots, g_n \rangle \subset I_{G,k}$. Como por el lema 3.8 $I_{n,k} : I_{G,k} = I_{n,k} + \langle f_G \rangle$, se verifica:

$$I_{n,k} + \langle f_G \rangle = I_{n,k} : I_{G,k} \subset I_{n,k} : \langle g_1, \dots, g_n \rangle.$$

Luego $\langle f_G \rangle = I_{n,k} : \langle g_1, \dots, g_n \rangle$, y en particular $f_G \in I_{n,k} : \langle g_1, \dots, g_n \rangle$. (4) \Rightarrow (5): Sea $A_\nu := \langle g_1, \dots, g_n \rangle$. Como $f_G \in I_{n,k} : A_\nu$, $I_{n,k} + \langle f_G \rangle \subset I_{n,k} : A_\nu$. Aplicando otra vez 3.8 tenemos:

$$I_{n,k} : I_{G,k} = I_{n,k} + \langle f_G \rangle \subset I_{n,k} : A_\nu$$

Ahora, como $V(A_\nu) \subset V(I_{n,k})$ y como $V(I_{n,k}) \subset V(I_{G,k})$ (por 4.4 y por 4.19), podemos escribir:

$$|V(I_{n,k})| - |V(I_{G,k})| = |V(I_{n,k} : I_{G,k})| \geq |V(I_{n,k} : A_\nu)| = |V(I_{n,k})| - |V(A_\nu)|.$$

Y como $|V(I_{n,k})| = k^n$ y $|V(A_\nu)| = k!$, deducimos que $|V(I_{G,k})| = k!$, y por tanto $\dim_{\mathbb{K}} R/I_{G,k} = k!$. (5) \Rightarrow (1): Si $k! = \dim_{\mathbb{K}} R/I_{G,k} = |V(I_{G,k})|$, entonces G tiene $k!$ coloraciones no distinguibles, por lo tanto una única distinguible. □

4.23 Teorema. *Sea G un grafo con n vértices. Son equivalentes:*

1. G es únicamente k -coloreable,
2. La base de Gröbner reducida para $I_{G,k}$ respecto de cualquier orden monomial tal que $X_1 \succ \dots \succ X_n$ es de la forma $\{\tilde{g}_1, \dots, \tilde{g}_n\}$ para los polinomios descritos en (4.3).

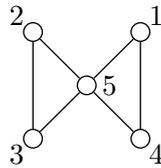
Demostración. (1) \Rightarrow (2): Inmediata por el lema 4.16 y la equivalencia (1) \Leftrightarrow (2) del teorema anterior. (2) \Rightarrow (1): Supongamos que la base de Gröbner reducida de $I_{G,k}$ es de la forma $\{\tilde{g}_1, \dots, \tilde{g}_n\}$ descrita en (4.3). Sea $\{g_1, \dots, g_n\}$ la ν -base correspondiente a la k -coloración ν descrita en (4.2) que se obtiene a partir de $\{\tilde{g}_1, \dots, \tilde{g}_n\}$ como en el corolario. Usando de nuevo la equivalencia (1) \Leftrightarrow (2) del teorema anterior, concluimos que G es únicamente k -coloreable.

Ejemplos

En esta sección vamos a analizar con detalle los tres grafos propuestos en los ejemplos del capítulo 2, aplicando los teoremas que acabamos de ver. Evidentemente llegaremos a las mismas conclusiones que en este capítulo, pero utilizando otro procedimiento. Para ello utilizaremos los teoremas 4.9 y 4.22 y nos ayudaremos del software de libre distribución “Singular” para la computación.

Ejemplo 1

Consideramos el grafo G_1 siguiente:



Primero veamos que no es 2-coloreable, pero sí es 3-coloreable. Para ello vamos a usar, por ejemplo, la equivalencia (1) \Leftrightarrow (4) del teorema 4.9. Definimos el anillo R donde estamos trabajando y el polinomio fG asociado al grafo G_1 :

```
> ring R=0,x(1..5),dp;
> poly fG(1)=(x(1)-x(4))*(x(1)-x(5))*(x(4)-x(5))*(x(2)-x(5))*
(x(3)-x(5))*(x(2)-x(3));
```

Ahora tomamos $k = 2$ y definimos el ideal $I(1) = I_{5,2}$:

```
> ideal I(1)=x(1)^2-1, x(2)^2-1, x(3)^2-1, x(4)^2-1,x(5)^2-1;
> I(1)=groebner(I(1));
> reduce(fG(1),I(1));
==>0
```

Como el resultado de la última operación es 0, $f \in I$, luego por 4.9 G no es 2-coloreable. Ahora definimos $J(1) := I_{5,3}$:

```

> ideal J(1)=x(1)^3-1, x(2)^3-1, x(3)^3-1, x(4)^3-1,x(5)^3-1;
> J(1)=groebner(J(1));
> reduce(fG(1),J(1));
==>x(1)^2*x(2)*x(3)*x(4)-x(1)*x(2)*x(3)*x(4)^2-x(1)^2*x(2)*x(3)*x(5)
-x(1)^2*x(2)*x(4)*x(5)-x(1)^2*x(3)*x(4)*x(5)+x(1)*x(2)*x(4)^2*x(5)
+x(1)*x(3)*x(4)^2*x(5)+x(2)*x(3)*x(4)^2*x(5)+x(1)^2*x(2)*x(5)^2
+x(1)^2*x(3)*x(5)^2+x(1)*x(2)*x(3)*x(5)^2+x(1)^2*x(4)*x(5)^2
-x(2)*x(3)*x(4)*x(5)^2-x(1)*x(4)^2*x(5)^2-x(2)*x(4)^2*x(5)^2
-x(3)*x(4)^2*x(5)^2-x(1)^2-x(1)*x(2)-x(1)*x(3)+x(2)*x(4)+x(3)*x(4)
+x(4)^2+x(1)*x(5)-x(4)*x(5)

```

Es decir, $f \notin J(1)$, luego G es 3-coloreable. Veamos ahora que no es únicamente 3-coloreable. Llamamos $K(1) := I_{G_1,3}$:

```

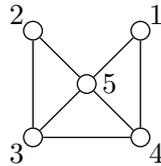
> ideal K(1)= J(1), (x(1)^2+x(1)*x(4)+x(4)^2), (x(1)^2+x(1)*x(5)+x(5)^2),
(x(4)^2+x(4)*x(5)+x(5)^2), (x(2)^2+x(2)*x(5)+x(5)^2),
(x(2)^2+x(2)*x(3)+x(3)^2), (x(3)^2+x(3)*x(5)+x(5)^2);
> vdim(groebner(K(1)));
12

```

Y como $12 \neq 3!$, concluimos por la equivalencia (1) \Leftrightarrow (5) del teorema 4.22 que G_1 no es únicamente 3-coloreable, y por el lema 4.4, que tiene doce 3-coloraciones distintas, luego tiene dos 3-coloraciones distinguibles distintas, como ya habíamos visto antes.

Ejemplo 2

Consideramos el grafo $G_2 = (V(G_1), E(E(G_1)) \cup \{3, 4\})$:



Veamos que como habíamos dicho el en capítulo 2 el grafo G_2 es únicamente 3-coloreable. Para ello haremos como en el ejemplo anterior, primero veremos que no es 2-coloreable, luego veremos que es 3-coloreable, y por último veremos que es únicamente 3-coloreable. Utilizaremos el mismo anillo, y el ideal I también es el mismo. Así que sólo tenemos que definir el polinomio fG asociado a G_2 y los ideales J y K , pero lo haremos a partir de los de G_1

Veamos que G_2 no es 2-coloreable.

```

> ideal I(2)= I(1);

> poly fG(2)=fG(1)*(x(3)-x(4));

> reduce(fG(2), I(2));
==>0

```

Luego G_2 no se puede colorear sólo con dos colores. Veamos qué sucede para $k = 3$.

```

> ideal J(2)=J(1);

> reduce(fG(2), J(2));
==>x(1)^2*x(2)*x(3)^2*x(4)-x(1)^2*x(2)*x(3)*x(4)^2
-x(1)*x(2)*x(3)^2*x(4)^2-x(1)^2*x(2)*x(3)^2*x(5)
-x(1)^2*x(3)^2*x(4)*x(5)+x(1)^2*x(2)*x(4)^2*x(5)
+x(1)^2*x(3)*x(4)^2*x(5)+x(1)*x(2)*x(3)*x(4)^2*x(5)
+x(1)*x(3)^2*x(4)^2*x(5)+x(2)*x(3)^2*x(4)^2*x(5)
+x(1)^2*x(2)*x(3)*x(5)^2+x(1)^2*x(3)^2*x(5)^2
+x(1)*x(2)*x(3)^2*x(5)^2-x(1)^2*x(2)*x(4)*x(5)^2
-x(1)*x(2)*x(3)*x(4)*x(5)^2-x(2)*x(3)^2*x(4)*x(5)^2
-x(1)^2*x(4)^2*x(5)^2-x(1)*x(3)*x(4)^2*x(5)^2
-x(3)^2*x(4)^2*x(5)^2-x(1)^2*x(3)-x(1)*x(3)^2+x(1)^2*x(4)
+x(1)*x(2)*x(4)+x(1)*x(3)*x(4)+x(2)*x(3)*x(4)+x(3)^2*x(4)
-x(2)*x(4)^2-x(1)*x(2)*x(5)-x(2)*x(3)*x(5)-x(1)*x(4)*x(5)
-x(3)*x(4)*x(5)+x(4)^2*x(5)+x(1)*x(5)^2+x(2)*x(5)^2
+x(3)*x(5)^2-1

```

Ahora que hemos visto que es 3-coloreable, sólo nos queda ver que es únicamente 3-coloreable:

```

> ideal K(2)=K(1), x(3)^2+x(3)*x(4)+x(4)^2;

> vdim(groebner(K(2)));
==>6

```

Luego por el teorema 4.22 concluimos que G_2 es únicamente k -coloreable. Como es únicamente 3-coloreable, vamos a hallar su única 3-coloración propia, para ello haremos el procedimiento descrito en 4.3 en sentido contrario. Para empezar calculamos la base de Gröbner reducida de $I_{G,3}$

```

> option(redSB); \\forzamos el cálculo de la base reducida
> groebner(K(2));

```

```

==>_[1]=x(5)^3-1
==>_[2]=x(4)^2+x(4)*x(5)+x(5)^2
==>_[3]=x(3)+x(4)+x(5)
==>_[4]=x(2)-x(4)
==>_[5]=x(1)+x(4)+x(5)

```

Ahora vamos a estudiar el resultado: Está claro que $(m_3, m_2, m_1) = (5, 4, 3)$ por cómo están definidos los g_i en 4.3. Por otra parte, tenemos un generador que es $x_2 - x_4$, luego $cl(2) = cl(4)$. Y ya sólo nos queda ver el color de 1, pero también es evidente que $cl(1) = cl(m_1)$, luego ya tenemos la coloración:

Color 1: vértices 1 y 3.

Color 2: vértices 2 y 4.

Color 3: vértice 5.

Esta coloración evidentemente coincide con la propuesta en 2.7.

Ejemplo 3

Por último vamos a trabajar con el último grafo propuesto en 2.

Siguiendo los mismos pasos que en el ejemplo anterior, podemos demostrar por medio de las bases de Gröbner, usando “Singular” que el grafo no es 2-coloreable, pero sí únicamente 3-coloreable, además podemos obtener la coloración propia. Vamos a verlo: Primero veamos que no es 2-coloreable.

```

> ring R= 0, x(1..12), lp;

> poly f=(x(1)-x(2))*(x(2)-x(3))*(x(3)-x(4))*(x(5)-x(6))
*(x(6)-x(7))*(x(7)-x(8))*(x(8)-x(9))*(x(9)-x(10))*(x(10)-x(11))
*(x(11)-x(12))*(x(12)-x(5))*(x(5)-x(9))*(x(6)-x(10))*(x(7)-x(11))
*(x(8)-x(12))*(x(1)-x(5))*(x(1)-x(7))*(x(2)-x(6))*(x(2)-x(8))
*(x(3)-x(11))*(x(3)-x(9))*(x(4)-x(10))*(x(4)-x(12));

> ideal J= x(1)^2-1, x(2)^2-1, x(3)^2-1, x(4)^2-1, x(5)^2-1,
x(6)^2-1, x(7)^2-1, x(8)^2-1, x(9)^2-1, x(10)^2-1, x(11)^2-1,
x(12)^2-1;

> J=groebner(J);

> reduce(f,J);
==>0

```

Veamos ahora que sí es 3-coloreable, para ello calculamos $I_{12,3}$. Lo denotamos $I(1)$.

```
>ideal I(1)= x(1)^3-1, x(2)^3-1, x(3)^3-1, x(4)^3-1, x(5)^3-1,
x(6)^3-1, x(7)^3-1, x(8)^3-1, x(9)^3-1, x(10)^3-1, x(11)^3-1,
x(12)^3-1;
```

```
> I(1)=groebner(I(1));
```

```
>reduce(f,I(1));
```

Como el resultado es distinto de 0, f_{G_3} no pertenece al ideal, y por tanto G_3 es 3-coloreable.

Ahora vamos a calcular el ideal $I_{G_3,3}$, que denotaremos por I , y que será el ideal generado por los siguientes. A continuación calcularemos la dimensión de $R/I_{G_3,3}$ como \mathbb{K} espacio vectorial y veremos que es 6, luego que el grafo es únicamente 3-coloreable.

```
\\Monomios de I_{n,k}
>I(1);
```

```
\\Aristas que forman el octógono
```

```
> ideal I(2)= x(5)^2+x(5)*x(6)+x(6)^2, x(6)^2+x(6)*x(7)+x(7)^2,
x(7)^2+x(7)*x(8)+x(8)^2, x(8)^2+x(8)*x(9)+x(9)^2,
x(9)^2+x(9)*x(10)+x(10)^2, x(10)^2+x(10)*x(11)+x(11)^2,
x(11)^2+x(11)*x(12)+x(12)^2, x(12)^2+x(12)*x(5)+x(5)^2;
```

```
\\Picos entre los vértices del "cuadrado" exterior y los
\\del octogono:
```

```
> ideal I(3)= x(1)^2+x(1)*x(5)+x(5)^2, x(1)^2+x(1)*x(7)+x(7)^2,
x(2)^2+x(2)*x(6)+x(6)^2, x(2)^2+x(2)*x(8)+x(8)^2,
x(3)^2+x(3)*x(9)+x(9)^2, x(3)^2+x(3)*x(11)+x(11)^2,
x(4)^2+x(4)*x(10)+x(10)^2, x(4)^2+x(4)*x(12)+x(12)^2;
```

```
\\Aristas que unen un vértice con el opuesto en el octógono:
```

```
> ideal I(4)= x(5)^2+x(5)*x(9)+x(9)^2, x(6)^2+x(6)*x(10)+x(10)^2,
x(7)^2+x(7)*x(11)+x(11)^2, x(8)^2+x(8)*x(12)+x(12)^2;
```

```
\\Aristas del "cuadrado" exterior:
```

```
> ideal I(5)= x(1)^2+x(1)*x(2)+x(2)^2, x(2)^2+x(2)*x(3)+x(3)^2,
x(1)^2+x(1)*x(4)+x(4)^2;
```

```
\\El ideal I_{G,k} es el ideal formado por los cinco anteriores:
```

```
> ideal I= I(1), I(2), I(3), I(4), I(5);
```

```
>I=groebner(I);
```

```
>vdim(I);
```

```
==>6
```

Como es únicamente 3-coloreable, calculamos la 3-coloración propia.

```
> option(redSB);
```

```
> groebner(I);
```

```
==>_[1]=x(12)^3-1  
_[2]=x(11)^2+x(11)*x(12)+x(12)^2  
_[3]=x(10)-x(12)  
_[4]=x(9)-x(11)  
_[5]=x(8)+x(11)+x(12)  
_[6]=x(7)-x(12)  
_[7]=x(6)-x(11)  
_[8]=x(5)+x(11)+x(12)  
_[9]=x(4)+x(11)+x(12)  
_[10]=x(3)+x(11)+x(12)  
_[11]=x(2)-x(12)  
_[12]=x(1)-x(11)
```

Ahora analicemos el resultado:

Por [1], al vértice 12 le corresponde la clase de color m_3 .

Los vértices 2, 7, 10, 12 tienen la misma clase de color (por [11], [6],y [3]).

Entonces, $cl(2) = cl(7) = cl(10) = cl(12) = m_3$.

Por [2], la clase de color de los vértices 11 y 12 es distinta. Luego el vértice 11 tiene clase de color m_2 .

Los vértices 1, 6, 9, 11 tienen la misma clase de color (por [12], [7],y [4]).

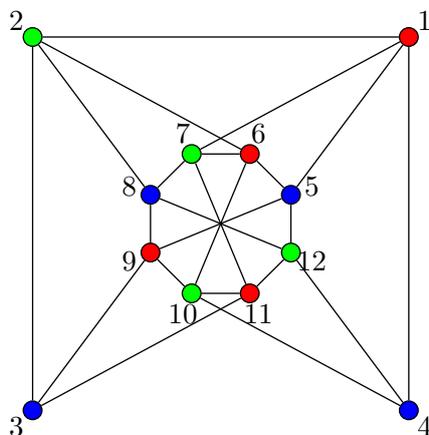
Así que $cl(1) = cl(6) = cl(9) = cl(11) = m_2$.

Por [5], [8], [9],y [10], los vértices $cl(8) = cl(5) = cl(4) = cl(3) = m_1$.

Luego obtenemos la siguiente única 3-coloración:

4.4. Grafos parcialmente coloreados

Como ya mencionamos en el capítulo 2 el otro problema relativo a los grafos que vamos a tratar aquí es, dada una coloración parcial propia de G ,



encontrar, si existe, la coloración propia del grafo G que respete la coloración parcial dada.

Vamos a definir lo que es una coloración parcial:

4.24 Definición. Sea G un grafo de n vértices, una k -coloración parcial de G es una coloración de ν vértices de G , donde $\nu \leq n$. Es decir, una k -coloración parcial de G es la k -coloración de un subgrafo $H \subset G$, donde $|V(H)| = \nu$. Se dice que la k -coloración parcial es *propia* si cada par de vértices adyacentes recibe colores distintos.

4.25 Teorema. Sea G un grafo de n vértices. Sea C una k_0 -coloración parcial propia de t vértices de G usando k_0 colores. Sea $p_{G,C}(k)$ el número de formas de completar una coloración propia de G usando k colores. Entonces $p_{G,C}(k)$ es un polinomio mónico (en k) de grado $n - t$ para $k \geq k_0$.

A continuación vamos a enunciar y demostrar el Teorema de la Inversión de Möbius, que utilizaremos para demostrar el teorema anterior. Pero antes de enunciarlo, vamos a dar algunas definiciones.

4.26 Definición. Sea (P, \leq) un conjunto parcialmente ordenado, se define el *álgebra de incidencia* asociada a P

$$\mathbb{A}(P) = \{\alpha \in \mathbb{C}^{P \times P} : \alpha(x, y) = 0 \text{ si } x > y\}.$$

4.27 Definición. Definimos la *función de Möbius* $\mu : \mathbb{A}(P) \rightarrow \{0, 1\}$

$$\mu(x, y) = \begin{cases} 0 & \text{si } x \not\leq y \\ 1 & \text{si } x = y \end{cases} \quad (4.5)$$

y el resto de valores se definen de manera inductiva por

$$\mu(x, y) = - \sum_{x \leq z < y} \mu(x, z)$$

Resulta inmediato de la definición anterior que

$$\sum_{x \leq z \leq y} \mu(x, z) = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{sino} \end{cases}$$

4.28 Teorema (de la Inversión de Möbius). *Sea (P, \leq) un conjunto parcialmente ordenado, μ la función de Möbius definida en 4.5, $f, g : P \rightarrow \mathbb{C}$, donde*

$$g(x) = \sum_{y \leq x} f(y)$$

entonces

$$f(x) = \sum_{y \leq x} \mu(x, y)g(y)$$

Demostración (de 4.28).

$$\begin{aligned} \sum_{y \leq x} \mu(x, y)g(y) &= \sum_{y \leq x} \mu(y, x) \left(\sum_{z \leq y} f(z) \right) \\ &= \sum_{z \leq y \leq x} \mu(y, x)f(z) = \sum_{z \leq y \leq x} f(z) \sum_{z \leq y \leq x} \mu(y, x) = f(x) \end{aligned}$$

□

Demostración (de 4.25). Sea G' una contracción de G con n' vértices. Sea $q_{G,C}(k)$ el número de coloraciones de G (coloraciones propias e impropias). Sea $k \geq k_0$,

$$q_{G',C}(k) = k^{n-t} = \sum_{C \leq G'} p_{G,C}(k)$$

donde la última igualdad ocurre porque las coloraciones de las contracciones de G son precisamente las coloraciones impropias. Aplicando ahora 4.28 obtenemos

$$p_{G',C}(k) = \sum_{C \leq G'} \mu(C, G')q_{G,C}(k) = \sum_{C \leq G'} \mu(C, G')k^{n'-t}$$

y con esto concluimos porque la parte de la derecha de la igualdad es un polinomio mónico de grado $n - t$.

□

Para finalizar el capítulo, vamos a dar un criterio necesario para que, dada una k -coloración parcial de un grafo G , éste pueda ser k -colorable.

4.29 Teorema. *Sea G un grafo y k su número cromático. Sea C una k -coloración parcial de G que usa $k - 2$ colores. Entonces, si se puede extender la $(k - 2)$ -coloración parcial a una k -coloración de todo G , hay al menos dos formas de hacerlo.*

Demostración. Supongamos que hay una forma de completar la coloración de G respetando la coloración parcial C . Como en la $(k - 2)$ -coloración parcial hay dos colores sin usar, c_i, c_j , una vez que hemos completado la k -coloración propia de G , podemos intercambiar c_i y c_j sin que la coloración parcial varíe. Luego hay al menos dos formas de completar la coloración de G .

□

Capítulo 5

Sudokus, grafos y bases de Gröbner

En este capítulo estudiaremos la relación entre la solución de un Sudoku y la coloración de un grafo. Además daremos algunas condiciones necesarias para que exista solución y sea única. Por último, daremos dos algoritmos para resolverlos. Este capítulo se basa principalmente en [Cro], [FJ], [Fis] y [DP]

5.1. Definición e historia

Aunque comúnmente denominamos Sudoku a un juego de lógica que se desarrolla en un tablero de 9×9 casillas divididas en filas, columnas y bloques, éste es sólo un caso particular del juego.

5.1 Definición. Un Sudoku es un juego que se realiza sobre un tablero cuadrado de dimensiones $n^2 \times n^2$, con $n \in \mathbb{N}$. A cada una de las $n^2 \times n^2$ posiciones se le llama *celda*, y se denota por $c(i, j)$, donde i es el número de la fila que ocupa y j el de la columna.

Estas celdas se dividen en n^2 filas, denotadas $F(i)$; n^2 columnas, denotadas $C(j)$; y n^2 bloques, denotados $B(k)$; $0 \leq i, k, j \leq n^2 - 1$. Las filas empiezan a numerarse de izquierda a derecha, las columnas de arriba a abajo y los bloques de izquierda a derecha y de arriba a abajo.

El juego del Sudoku consiste el tablero definido arriba con un conjunto de casillas con las entradas ya colocadas. La solución consiste en colocar, mediante procedimientos lógicos, un número, de 1 a n^2 en cada casilla del tablero con los números, sin que haya ninguno repetido en una misma fila, columna o bloque.

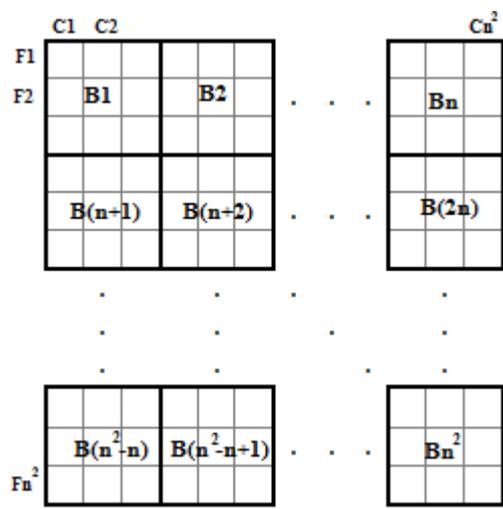


Figura 5.1: Notación

Ahora veamos un poco de la historia del Sudoku:
 Los primeros juegos numéricos similares a los Sudokus aparecieron en el siglo XIX en Francia, como resultado de eliminar dígitos de un cuadrado mágico:

El 19 de noviembre de 1892 un periódico francés, “Le Siècle” publicó un cuadrado mágico de dimensión 9×9 parcialmente completado (no era un Sudoku porque Estos puzzles no eran Sudokus porque contenían números repetidos y requerían de aritmética para resolverlos, sin embargo compartían las características básicas: no se podía repetir ningún número en la misma fila, columna o bloque.

Tres años después, el 6 de julio de 1895, otro periódico francés, “La France”, publicó otro juego más refinado mucho más parecido al Sudoku: era un tablero de 9×9 parcialmente completado que había que rellenar totalmente con números del 1 al 9, sin repetirlos en una misma fila, columna o *diagonal rota*. Estos juegos fueron bastante populares en periódicos franceses como “L’Echo de Paris” hasta la Primera Guerra Mundial.

Es decir, a partir de la historia del Sudoku podemos decir que proviene de los cuadrados mágicos, de hecho es un caso particular de estos donde el número de casillas de cada fila y cada columna es un cuadrado perfecto, y donde además hay una división extra: los bloques.

Pero, ¿por qué los cuadrados mágicos y los Sudokus son un objeto de estudio que ha tenido tanto éxito entre los matemáticos desde hace varios

siglos? La siguiente cita de en relación con los cuadrados mágicos puede explicarlo en parte:

<< *Lo que al principio era una práctica de magos y hacedores de talismanes, se ha convertido desde hace mucho tiempo en un importante objeto de estudio para los matemáticos. No porque imaginen que esto les va aportar una ventaja sólida, sino porque la teoría presenta dificultad y se considera que se pueden descubrir nuevas propiedades de los números, que pueden ser de utilidad para los matemáticos. En realidad éste ha sido el caso, ya que desde un cierto punto de vista el problema ha resultado ser más algebraico que aritmético y está íntimamente relacionado con ramas de la ciencia como el “cálculo infinitesimal”, el “cálculo de operaciones” y la “teoría de grupos”.* >>

“Magic Squares and Other Problems on a Chessboard” por Major P.A. MacMahon, R.A., D.Sc., F.R.S., publicada en *Proceedings of the Royal Institution of Great Britain, Vol XVII, No 96, pag 50-61, Feb.4 1892.*

5.2. La relación entre los Sudokus y los grafos

Tengo que cambiar la notación para que me case con la que empleo luego Consideremos un grafo G_n de $n^2 \times n^2$ vértices, que denotaremos por $c(i, j)$ donde $0 \leq i, j \leq n^2 - 1$. Supongamos que este grafo es regular y que dos vértices $c(i, j), c(i', j')$ son adyacentes si se cumple alguna de las tres condiciones siguientes:

- $i = i'$,
- $j = j'$,
- $\lfloor i/n \rfloor = \lfloor i'/n \rfloor$ y $\lfloor j/n \rfloor = \lfloor j'/n \rfloor$; donde $\lfloor \cdot \rfloor$ es la parte entera por abajo.

Nota. Es fácil comprobar que el grafo G_n corresponde a un Sudoku.

Es decir, podemos representar los Sudokus de tamaño $n^2 \times n^2$ como el grafo G_n , luego la solución parcial de un Sudoku se corresponderá con una (única) coloración parcial G_n , y encontrar la solución del Sudoku equivale a encontrar una n^2 -coloración propia de G_n .

Ahora que ya hemos identificado los Sudokus con los grafos, vamos a interpretar el teorema 4.29 del capítulo anterior en términos de Sudokus y a enunciar otro teorema relativo a la solución de los Sudokus.

“Para que la solución de un Sudoku de dimension $n^2 \times n^2$ sea única, entre los números propuestos tiene que haber al menos $n^2 - 1$ distintos.”

5.2 Teorema. *Para todo $n \in \mathbb{N}$ hay una solución para cada Sudoku de dimensión $n^2 \times n^2$ usando n^2 números. El número cromático del grafo G_n que representa al Sudoku es n^2 .*

Demostración. Primero veamos que como mínimo necesitamos n^2 números: El grafo completo de n vértices, K_{n^2} , es el grafo asociado a uno de los bloques del Sudoku S_n , por lo tanto $\chi_{G_n} \geq \chi_{K_{n^2}} = n^2$, ya que todos los vértices de K_{n^2} son adyacentes.

Veamos ahora que existe una coloración propia de S_n con n^2 colores. Denotamos los vértices como (i, j) con $0 \leq i, j \leq n^2 - 1$ y consideramos las clases residuales módulo n^2 . Para $0 \leq i \leq n^2 - 1$ escribimos $i = t_i n + d_i$, con $0 \leq d_i \leq n - 1$ y $0 \leq t_i \leq n - 1$ y hacemos lo mismo con $0 \leq j \leq n^2 - 1$. Ahora asignamos el número $c(i, j) = d_i n + t_i + n t_j + d_j$, reducido módulo n^2 a la casilla (i, j) -ésima de la cuadrícula. Para ver que lo que tenemos es una coloración propia tenemos que mostrar que dos casillas en la misma fila, columna o bloque no tienen el mismo número. Veamos que si $i = i'$, o bien $c(i, j) \neq c(i', j)$ o bien $j = j'$: si $c(i, j) = c(i', j)$, tenemos que $n t_j + d_j = n t_{j'} + d_{j'}$, y por tanto, $j = j'$. Para demostrar que dos números en la misma columna son distintos procedemos de la misma manera. Sólo nos queda mostrar que dos números en el mismo bloque tienen que ser distintos: Si $[i/n] = [i'/n]$ y $[j/n] = [j'/n]$, entonces $d_i = d_{i'}$ y $d_j = d_{j'}$; si $t_i + n t_j = t_{i'} + n t_{j'}$, y reduciendo módulo n obtenemos $t_i = t_{i'}$, así que $t_j = t_{j'}$, y de nuevo $c(i, j) = c(i', j)$.

□

Aunque según nuestra definición de Sudoku, este puede tener cualquier dimensión $n^2 \times n^2$, de ahora en adelante consideramos los Sudokus estándar, es decir, los de tamaño 9×9 .

5.3. Un algoritmo a lápiz y papel para resolver Sudokus

En esta sección, basada en su totalidad en el artículo [Cro] proporciona un algoritmo para resolver Sudokus basado simplemente en la incompatibilidad de soluciones, y sin necesidad de usar la lógica, ya que se puede implementar en un ordenador.

5.3 Definición. Dada una solución parcial del Sudoku, definimos el *marcaje* de una celda $c(i, j)$ como el conjunto de todas las entradas posibles en la celda. Esto es, los números $\{r \in \{1, \dots, n^2\}$ tales que r no está en ninguna celda de la misma fila, columna o bloque que $c(i, j)$.

5.4 Definición-Notación. Un *conjunto preferente* se compone de números $\{1, \dots, n^2\}$ y de tamaño m , con $2 \leq m \leq n^2$, cuyos números son exclusivamente ocupantes potenciales de m celdas, donde exclusivamente significa que ningún otro número en $\{1, \dots, n\}$ aparte de los del conjunto preferente puede ocupar dichas celdas.

Denotaremos un conjunto preferente por

$$\{\{s_1, \dots, s_m\}, \{c(i_1, j_1), \dots, c(i_m, j_m)\}\},$$

donde $\{s_1, \dots, s_m\}$, $1 \leq s_k \leq n^2$ para $i = 1, \dots, m$, denota el conjunto de números que forman el conjunto preferente, y $\{c(i_1, j_1), \dots, c(i_m, j_m)\}$ las celdas donde se alojan esos números.

Notación. En el caso en que el conjunto preferente sólo tenga un número, éste se denomina *solitario*.

5.5 Definición. El *rango de un conjunto preferente* es la fila, columna o caja que alberga todas las celdas del conjunto.

5.6 Teorema. (Teorema de ocupación) Sea X un conjunto preferente en el marcaje de un Sudoku. Entonces ningún número en X que aparezca en el marcaje de las celdas fuera de X , en el rango de X , puede ser parte de la solución del puzle.

Demostración. Supongamos X es un conjunto preferente con m números. Si tomamos un número de X como entrada de una celda que no pertenece a X , sólo quedarán $m - 1$ números para distribuir entre m celdas. Como no puede haber ningún número repetido en el conjunto preferente, entonces tendremos una celda vacía, lo que contradice la definición de solución de un Sudoku. Luego los números en X sólo pueden ser entradas de las celdas en X .

□

Nota. Siempre existe un conjunto preferente al que se puede recurrir para resolver un “conjunto escondido”, que posteriormente transforma el “conjunto escondido” en un conjunto preferente, excepto en el caso de un solitario.

5.7 Definición. Cuando ningún conjunto preferente del Sudoku se puede romper en subconjuntos preferentes más pequeños, necesitamos hacer una *elección aleatoria*. Esto es, buscar el conjunto preferente con menos celdas y elegir una entrada en una de ellas y continuar resolviendo el Sudoku como si esa entrada formase parte de la solución parcial.

5.8 Definición. Se dice que se ha producido una *violación* en un Sudoku cuando un número aparece repetido en una fila, columna o bloque.

Nota. Es una buena idea que cada vez que hagamos una elección aleatoria lo hagamos con un color diferente, de esta forma cuando se produzca una violación del Sudoku, simplemente borraremos el camino de ese color y eliminaremos la primera entrada de ese color del marcaje de la celda.

A continuación vamos a dar un algoritmo para resolver Sudokus, que no requiere de lógica y que se puede implementar en un ordenador:

Un Algoritmo para resolver Sudokus:

1. Marcaje de las celdas:

- (i) “Marcar provisionalmente” las celdas vacías con el conjunto $\{1, \dots, n^2\}$.
- (ii) Para cada celda $c(i, j)$ suprimir del “marcaje provisional” anterior todos los números que estén en la misma fila, columna o caja que dicha celda.
- (iii) Si una celda está marcada con un conjunto de un elemento, esa celda forma parte de la solución del Sudoku.
- (iv) Repetir lo anterior hasta que no se puedan eliminar números del “marcaje provisional”. Cuando esto suceda, habremos conseguido el marcaje del Sudoku.

2. Buscar conjuntos preferentes:

- (i) Para m desde 2 hasta n^2 , para cada celda con cardinal m , buscar conjuntos preferentes, esto es, un subconjunto de m celdas en las que solo se puedan alojar m números (iguales en todas las celdas).
- (ii) Repetir 1 hasta en el rango de cada conjunto preferente.
- (iii) Repetir hasta que no encontremos más conjuntos preferentes.

3. Encontrar la solución:

Después de 2 tenemos dos posibilidades:

- a) Se ha encontrado una solución.
- b) No se ha encontrado una solución.

Si a) entonces FIN.

Si b), elección aleatoria y repetir desde 2 hasta que:

- c) Se encuentre una solución.
- d) Se viole el Sudoku.

Si c) entonces FIN.

Si d) entonces repetir desde 2 con otra elección aleatoria.

FIN.

5.4. Resolución de Sudokus por bases de Gröbner

En esta sección vamos a resolver Sudokus bien planteados utilizando álgebra computacional y geometría algebraica. Sin embargo no utilizaremos las fórmulas dadas en el capítulo 4 porque no son una buena forma para resolver Sudokus, ya que aunque D. Leonard la ha conseguido implementar para el Sudoku de 9×9 , sólo lo ha hecho trabajando sobre el cuerpo finito \mathbb{F}_{11} y con muchas restricciones. En lugar de eso, se plantea un método mucho más eficaz.

Notación. En esta sección vamos a cambiar de nuevo la notación:

Representaremos las 81 celdas del Sudoku por 81 variables X_1, \dots, X_{81} ordenadas de izquierda a derecha y de arriba a abajo.

La solución del Sudoku se representará con un vector (a_1, \dots, a_{81}) donde el número a_i es el número que ocupa la casilla asociada a la variable x_i en la solución.

Nota. La entrada a_i en la entrada i -ésima satisface que $a_i \in \{1, \dots, 9\}$ si y solo si a_i es raíz del polinomio F_i en una sola variable y definido por

$$F_i(x_i) = \prod_{k=1}^9 (x_i - k).$$

Como el polinomio $F_i(x_i) - F_j(x_j)$ se anula en $V(x_i - x_j)$, $x_i - x_j$ es factor de $F_i(x_i) - F_j(x_j)$ para $i \neq j$, lo que da lugar a la siguiente definición:

5.9 Definición-Notación. $G_{i,j}(x_i, x_j) := \frac{F_i - F_j}{x_i - x_j} \in \mathbb{Q}[x_i, x_j]$, donde $i \neq j$.

Ahora tenemos que modelizar la solución del Sudoku de forma que no haya números repetidos en celdas que ocupen la misma fila, columna o bloque.

5.10 Definición-Notación. Definimos $E = \{(i, j) : 1 \leq i < j \leq 81 \text{ verificando } (*)\}$ donde $(*)$ equivale a la condición de que las celdas i -ésima y j -ésima no estén en la misma fila, columna o bloque 3×3 .

Sea I el ideal generado por los polinomios F_i , donde $i = 1, \dots, 81$, y por los $G_{i,j}$, con $(i, j) \in E$. Consideramos su ideal de anulación $V(I)$ y $\mathbf{a} = (a_1, \dots, a_{81})$ un punto de $V(I)$.

5.11 Teorema. *Son equivalentes:*

1. $\mathbf{a} \in V(I)$.
2. $a_i \in \{1, \dots, 9\}$ para $i = 1, \dots, 81$ y $a_i \neq a_j$ para $(i, j) \in E$.

Demostración. La implicación (2) \Rightarrow (1) es evidente ya que si se verifican las condiciones de (2), $F_i F_j$ y $G_{i,j}$ se anulan en a_i, a_j y (a_i, a_j) para todos a_i, a_j en las condiciones de (2). Luego $\mathbf{a} \in V(I)$. Demostremos ahora la otra implicación: Sea $\mathbf{a} \in V(I)$, entonces $F_i(a_i) = 0$ para todo i , luego $a_i \in \{1, \dots, 9\}$ para todo i . Para ver que $a_i \neq a_j$ para $(i, j) \in E$ razonemos por reducción al absurdo y supongamos que $a_i = a_j = b$ para algún $(i, j) \in E$. Como $F_i(x_i) = F_j(x_j) + (x_i - x_j)G_{i,j}(x_i, x_j)$, y sustituyendo se obtiene $F_i(x_i) = (x_i - b)G_{i,j}(x_i, b)$. Asumiendo que $G_{i,j}(b, b) = 0$ se tiene que b es un cero de orden mayor o igual que 2 de F_i , lo que es imposible.

□

Ahora vamos a buscar una forma de encontrar la solución (única) del Sudoku utilizando bases de Gröbner.

Sea S un Sudoku dado explícitamente y bien planteado con números preasignados $\{a_i\}$ para algún subconjunto $L \subset \{1, \dots, 81\}$. Estos números dados forman lo que en la sección anterior hemos llamado “solución parcial” del Sudoku.

5.12 Teorema. *Sea $I_S = I + \langle \{x_i - a_i\}_{i \in L} \rangle$ el ideal asociado al Sudoku S . Entonces, fijado un orden monomial cualquiera, la base de Gröbner reducida de I_S tiene la forma $\{x_1 - a_1, \dots, x_{81} - a_{81}\}$ en la solución única del Sudoku.*

Demostración. Por la proposición anterior y por el teorema de Nullstellensatz, el hecho de que el Sudoku tenga solución única implica que $\sqrt{I_S}$ es el ideal maximal $\langle x_1, \dots, x_{81} \rangle$. En particular, $(x_i - a_i)^{m_i} \in I_S$ para todo i . Pero por otra parte, I_S contiene los polinomios F_i , que son libres de cuadrado, luego concluimos que $I_S \cap \mathbb{K}[x_i]$ está generado por $x_i - a_i$, y por consiguiente $I_S = \langle x_1 - a_1, \dots, x_{81} - a_{81} \rangle$, luego la base de Gröbner es de la forma descrita en el teorema.

□

Ahora vamos a implementar un algoritmo que nos permita resolver Sudokus, basados en estos resultados. El algoritmo está descrito en [DP].

Vamos a ver cómo funciona este algoritmo para resolver el Sudoku siguiente:

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

Para ello completamos el tablero con 0, e introducimos la entrada de la celda $c(i, j)$ en la posición (i, j) de la matriz.

Notación. Esta sección no es sólo válida para los Sudokus sino que se puede extender a todo tipo de grafos. Es suficiente con considerar un conjunto de variables con cardinal el número de vértices del grafo y definir las aristas correctamente. El algoritmo que hemos usado para solucionar Sudokus también se puede implementar en el resto de grafos, pero no es general, ya que requiere una descripción del conjunto de aristas E de cada grafo particular. Esta es precisamente la razón por la cual el algoritmo está incluido en esta sección y no en la precedente.

Algoritmo para resolver Sudokus([DP, pag.107-109])

1. Describe las aristas:

```

>proc createE()
{
int i,j,k,l,a,b;
list E;
for(j = 1; j <= 9; j++)
{
for(k = 1; k <= 9; k++)
{
i = (j-1)*9+k;
a = j mod 3; if(a == 0) { a = 3; }
b = k mod 3; if(b == 0) { b = 3; }
for(l = k+1; l <= 9; l++)
{
E[size(E)+1] = list(i,i+1-k);
}
for(l = j+4-a; l <= 9; l++)

```

```

{
E[size(E)+1] = list(i, (l-1)*9+k);
}
if(a != 3)
{
E[size(E)+1] = list(i, j*9+k-b+1);
E[size(E)+1] = list(i, j*9+k-b+2);
E[size(E)+1] = list(i, j*9+k-b+3);
}
}
if(a == 1)
{
E[size(E)+1] = list(i, (j+1)*9+k-b+1);
E[size(E)+1] = list(i, (j+1)*9+k-b+2);
E[size(E)+1] = list(i, (j+1)*9+k-b+3);
}
}
}
return(E);
}

```

2. Crea los polinomios F, que hemos visto en esta sección:

```

>proc createG(ideal F, list E)
{
int i;
ideal G = F;
for(i = 1; i <= size(E); i++)
{
G[size(G)+1] = (F[E[i][1]] - F[E[i][2]])/
(var(E[i][1]) - var(E[i][2]));
}
}
return(G);
}

```

3. Introducir la solución parcial del Sudoku:

```

>proc addPreass(ideal G, intmat M)
{
int i, j, k;
for(i = 1; i <= 9; i++)
{

```

```

for(j = 1; j <= 9; j++)
{
  if(M[i,j] != 0)
  {
    k = (i-1)*9+j;
    G[size(G)+1] = var(k)-M[i,j];
  }
}
return(G);
}

```

```

4. >proc prepareRes(ideal G)
{
  intmat M[9][9];
  int i,j,k;
  for(i = 1; i <= size(G); i++)
  {
    j = ((i-1) div 9) + 1;
    k = i mod 9;
    if(k == 0) { k = 9; }
    M[j,k] = int(leadcoef(-G[size(G)-i+1][2]));
  }
  return(M);
}

```

En este algoritmo tenemos que introducir la solución parcial en forma de matriz, de modo que para $1 \leq i, j \leq 9$ si la celda $c(i, j)$ tiene una entrada que forma parte de la solución parcial, esta entrada se colocará en la posición (i, j) de la matriz. El resto de posiciones las completamos con 0.

Ahora sí, vamos a resolver el Sudoku que propuesto en la sección anterior.

```

> intmat M1[9][9] = 0,2,1,0,0,5,0,8,0,
                   8,0,4,0,2,0,0,6,1,
                   0,0,9,1,8,0,0,0,0,
                   6,0,0,0,0,0,2,3,0,
                   0,0,0,0,0,0,0,0,0,
                   0,8,7,0,0,0,0,0,6,
                   0,0,0,0,4,6,3,0,0,
                   1,9,0,0,3,0,6,0,0,
                   0,3,0,8,0,0,7,9,0;

```

```
> print(Sudoku(M1));  
==>7,2,1,6,9,5,4,8,3,  
    8,5,4,7,2,3,9,6,1,  
    3,6,9,1,8,4,5,7,2,  
    6,1,5,4,7,8,2,3,9,  
    9,4,3,2,6,1,8,5,7,  
    2,8,7,3,5,9,1,4,6,  
    5,7,2,9,4,6,3,1,8,  
    1,9,8,5,3,7,6,2,4,  
    4,3,6,8,1,2,7,9,5;
```

Capítulo 6

Conclusión

Los métodos para estudiar la coloración de grafos expuestos en este trabajo permiten dar un enfoque algebraico a un problema claramente combinatorio. Aunque estos métodos no son computacionalmente eficientes en todos los grafos (especialmente son poco eficientes en el caso de la resolución de Sudokus), lo importante es que hacen que el puente entre el Álgebra Conmutativa y la Combinatoria se pueda recorrer en ambas direcciones, ya que normalmente son los problemas algebraicos los se intentan resolver por Combinatoria y no al revés.

Bibliografía

- [Ahm] S. AHMED; *Applications of Graph Coloring in Modern Computer Science*, International Journal of Computer and Information Technology (IJCIT), Vol: 03, Issue: 02, 2012
- [Cam] A. CAMPILLO LÓPEZ; *Apuntes de la asignatura "Matemática Discreta"*, Grado en Matemáticas, UVa, 2012-2013.
- [Cox] D. COX; *Gröbner Bases. Quick Updates and Extended Snapshots*, <http://www.cs.amherst.edu/~dac/lectures/EACA.pdf> EACA 2012, Alcalá.
- [CLS] D. COX, J. LITTLE, D. O'SHEA, *Ideals, Varieties, and Algorithms*, Second Edition, Undergraduate Texts in Mathematics, Springer, 2007.
- [CLS] D. COX, J. LITTLE, D. O'SHEA, *Using Algebraic Geometry*, Second Edition, Graduate Texts in Mathematics, Springer, 2004.
- [Cro] J.F. CROOK, *A Pencil-and-Paper Algorithm for Solving Sudoku Puzzles*, Notices Amer. Math. Soc. 56, Number 4, 2009.
- [Sin] W. DECKER, G.M GREUEL, G. PFISTER, H. SCHÖNEMANN; SINGULAR 3-1-6 — *A computer algebra system for polynomial computations*, <http://www.singular.uni-kl.de> 2012.
- [DP] W. DECKER, G. PFISTER; *A First Course in Computational Algebraic Geometry*, Cambridge University Press, AIMS Library Series, 2013.
- [DN] J. M. DOMÍNGUEZ GÓMEZ, C.A. NÚÑEZ JIMÉNEZ; *Clases y guión de la asignatura de "Álgebra conmutativa y computacional"* Grado en Matemáticas, UVa, 2012-2013.
- [FJ] B. FELGENHAUER, F. JARVIS; *Mathematics of Sudoku I and II*, Mathematical Spectrum, 2006.

- [FF] P. FERNÁNDEZ-GALLARDO, J.L. FERNÁNDEZ-PÉREZ; Notas de Matemática Discreta, disponibles en http://www.uam.es/personal_pdi/ciencias/gallardo/, Universidad Autónoma de Madrid.
- [Fis] T. FISCHER; *A Necessary Solution Condition for Sudoku*, arXiv: 1210.6343v1 [math.CO] 23 Oct 2012.
- [Ful] W. FULTON; *Curvas algebraicas*, Ed. Reverté, 2005.
- [Gim] P. GIMENEZ; *Introducción a las bases de Gröbner y algunas de sus aplicaciones* Notas de la VI Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2013, Francisco Ugarte Guerra Ed., 2014.
- [GY] J. GROSS, J. YELLEN; *Graph Theory and Its Applications*, CRC, 1999.
- [HM] A.M. HEZBERG, M.R. MURTY; *Sudoku Squares and Chromatic Polynomials*, Notices Amer. Math. Soc. 54, Number 6, 2007.
- [HW] C.J. HILLAR, T. WINDFELDT; *Algebraic Characterization of Uniquely Vertex Colorable Graphs*, Elsevier Inc., 2007.
- [LHM] 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.
- [Lov] L. LOVÁSZ; *Stable sets and polynomials* Discrete Math. 124 (1994) 137-153.