Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

Herramientas del álgebra conmutativa computacional para el problema de coloración de grafos

Autor: Alberto Martín Heras
Tutor: Philippe Gimenez
2023

Índice general

Introducción

Los grafos son una estructura matemática de gran utilidad en la modelización de problemas en numerosos ámbitos. En particular el problema de la coloración de un grafo, resulta ser uno de los problemas más importantes de la *teoría de grafos*. Esta cuestión se aplica a diversas áreas entre las que se encuentran la programación de horarios y la asignación de recursos. Es por esto que dar respuesta a este problema de elevada complejidad resulta de gran interés para numerosos campos de estudio. Gran cantidad de algoritmos que resuelven este problema vienen de emplear técnicas propias de la teoría de grafos. En este trabajo se busca abordar esta cuestión desde otra perspectiva, utilizando para ello resultados del álgebra conmutativa y empleando métodos propios del álgebra conmutativa computacional.

Los problemas en los cuales vamos a centrar esta memoria son los siguientes: determinar la k-coloreabilidad de un grafo y obtener el número de k-coloraciones propias de este, estudiar en qué casos un grafo es únicamente k-coloreable y establecer un criterio para saber cuándo se puede extender una precoloración de un grafo. Para tratar estas tres cuestiones asociaremos ciertas variedades afines a un grafo las cuales recogen toda la información necesaria para dar solución a cada uno de estos problemas. Emplearemos herramientas del álgebra conmutativa computacional para estudiar los ideales de polinomios asociados a estas variedades lo que nos permitirá establecer criterios de coloración y dar respuesta a estas cuestiones.

La estructura que se seguirá en el trabajo es la siguiente:

- En primer lugar, se introducirán los conceptos básicos de la teoría de grafos y se planteará el problema de coloración de un grafo y se estudiarán algunos resultados en el contexto de teoría de grafos. También se aportarán cotas inferiores y superiores para el número cromático de un grafo.

- En el segundo capítulo del trabajo se darán las nociones básicas de álgebra conmutativa relativa a la correspondencia entre variedades afines e ideales de polinomios. Se introducirán dos herramientas: las *bases de Gröbner* y los *certificados de incompatibilidad de Nullstellensatz* y se estudiarán sus propiedades en detalle.

- En el tercer capítulo, se establecerá la relación entre las k-coloraciones de un grafo con los puntos de ciertas variedades afines a través de los *ideales de coloración* del grafo y se analizarán las características de estos ideales. A partir de estas propiedades se establecerán criterios de coloración aplicando las bases de Gröbner y los certificados de Nullstellensatz.

  Además, se emplearán estas herramientas para el estudio particular de grafos únicamente coloreables así como en el estudio de las extensiones de una precoloración de un grafo.

Capítulo 1

Grafos

1.1. Primeras definiciones

En primer lugar vamos a introducir los conceptos básicos de teoría de grafos para establecer el marco en el que vamos a trabajar a lo largo de este trabajo.

Definición 1.1.1. Un grafo es una par $G = (V, A)$, donde V es un conjunto no vacío cuyos elementos se denominan vértices del grafo y A es un conjunto cuyos elementos se denominan aristas, para los cuales existe una relación que asocia a cada arista un par no ordenado de vértices. A este par de vértices los denominamos extremos de la arista.

Dado un grafo $G = (V, A)$, si los conjuntos V y A son finitos, se dice que el grafo es finito y $|V|$ se denomina orden de G. En caso contrario, se dice que el grafo G es infinito.

A menudo nos referiremos a un grafo G sin explicitar el par (V, A). En estos casos denotaremos por $V(G)$ al conjunto de vértices de G, y por $A(G)$ al conjunto de aristas de G.

Notamos que en la definición no se excluye que los dos extremos de una arista sean iguales. De igual forma, en la definición varias aristas pueden tener los mismos extremos.

Definición 1.1.2. Dado un grafo G:

1. Diremos que una arista $a \in A(G)$ es un lazo si sus extremos coinciden.
2. Diremos que G tiene aristas múltiples si existen distintas aristas con el mismo par de extremos.
3. Diremos que G es un grafo simple si no tiene lazos ni aristas múltiples.

Dado un grafo simple G y una arista $a \in A(G)$, a queda determinada por sus extremos $u, v \in V(G)$. Esto justifica las notaciones (u, v) o (v, u) que utilizaremos indistintamente para referimos a a. En esta situación diremos que a une los vértices u y v y que los vértices u y v son adyacentes.

Dado que solo se tratará con grafos simples finitos a lo largo del trabajo, utilizaremos el término grafo para referirnos a un grafo simple finito. En esta situación es usual tomar como conjunto de vértices de un grafo el conjunto $\{1, \ldots, n\}$. En este trabajo seguiremos esta convención.

Definición 1.1.3. Dado un grafo G, se dice que un grafo H es un subgrafo de G si $V(H) \subset V(G)$ y $A(H) \subset A(G)$. En este caso escribiremos $H \subset G$ y decimos que su orden es $|V(H)|$.

Sea G un grafo y un conjunto de vértices $W \subset V(G)$. Denotamos por $G[W]$ al grafo cuyo conjunto de vértices es W y sus aristas son todas las aristas de G que unen pares de vértices de W. Decimos que $G[W]$ es el subgrafo inducido por W.

Se dice que un subgrafo H de un grafo G es un subgrafo inducido si $H = G[V(H)]$; es decir, si H coincide con el subgrafo inducido por sus vértices.

Dados dos grafos G y H se define el grafo $G + H$ de la siguiente forma: $V(G + H) = V(G) \sqcup V(H)$ y $(i, j) \in A(G + H)$ si $i, j \in V(G)$ y $(i, j) \in A(G)$, o bien $i, j \in V(H)$ y $(i, j) \in A(H)$.

Sean G un grafo y $W \subsetneq V(G)$. Se define $G - W \subset G$ como el subgrafo inducido por los vértices $V(G) \setminus W$. Es decir, $G - W = G[V(G) \setminus W]$.

Definición 1.1.4. Sea G un grafo.

1. Se dice que G es un grafo completo si todo vértice de G es adyacente al resto de vértices.

2. Sea H un subgrafo inducido de orden k de G. Se dice que H es un clique de tamaño k si H es un grafo completo.

3. Diremos que $\omega(G) = \max(k \geq 1 : \text{ existe un clique de tamaño } k)$ es el número de clique de G.

El concepto de *conjunto independiente* surge de forma natural al dualizar la noción de clique.

Definición 1.1.5. Sea G un grafo.

1. Se dice que un vértice $v \in V(G)$ es aislado si no es adyacente a ningún otro vértice de G.

2. Se dice que un subconjunto de vértices $W \subset V(G)$ es un conjunto independiente si los vértices del subgrafo inducido $G[W]$ son aislados.

3. Diremos que $\alpha(G) = \max(|W| : W \subset V(G)$ es un conjunto independiente) es el número de independencia de G.

1.2. El problema de coloración de grafos

Introducimos ahora el problema de coloración de un grafo, el cual vamos a estudiar en detalle en el capítulo 3 con las herramientas del álgebra conmutativa que vamos a desarrollar en el capítulo 2.

Definición 1.2.1. Una k-coloración de un grafo G es una aplicación $\rho : V(G) \to C$ donde C es un conjunto tal que $|C| = k$. Los elementos del conjunto C se denominan colores. Dado un color $c \in C$, $\rho^{-1}(c)$ se denomina la clase del color c y se denota por $cl(c)$.

Se dice que ρ es una k-coloración propia si dos vértices adyacentes no tienen el mismo color. Es decir, si $u, v \in V(G)$ y $(u, v) \in A(G)$ entonces $\rho(u) \neq \rho(v)$.

Se dice que ρ es una k-coloración impropia, si ρ no es una coloración propia; es decir, si existe un par de vértices adyacentes $u, v \in V(G)$ y $(u, v) \in A(G)$ con el mismo color, $\rho(u) = \rho(v)$.

Se dice que un grafo G es k-coloreable si existe una k-coloración propia de G.

Observación 1. El papel del conjunto C en la definición es el de etiquetar cada vértice del grafo con un color, por lo que no es muy relevante cual escojamos. Realmente la información que determina la k-coloración es el conjunto de las clases de coloración, las cuales establecen una partición de los vértices del grafo. Explícitamente, si tenemos dos coloraciones de un grafo G, $\rho : V(G) \to C$ y $\tilde{\rho} : V(G) \to \tilde{C}$, que inducen las mismas clases de coloración en el conjunto de vértices, podemos encontrar una biyección $\sigma : C \to \tilde{C}$ tal que $\sigma \circ \rho = \tilde{\rho}$. Es decir, podemos encontrar una correspondencia biyectiva entre los conjuntos C y $\tilde{C}$ que respete las clases de coloración.

Este hecho justifica que habitualmente se tome como conjunto de colores un conjunto arbitrario que denotaremos $C = \{c_1, c_2, \ldots, c_k\}$. En el capitulo 3 veremos que se pueden considerar conjuntos de colores específicos porque estos proporcionan alguna simplificación en la notación.

Fijado un conjunto de k colores $C = \{c_1, c_2, \ldots, c_k\}$ decimos que $\{\rho : V(G) \to C\}$ es el conjunto de k-coloraciones de un grafo G. Diremos que el cardinal de este conjunto es el número de k-coloraciones (propias e impropias) de G. De igual forma, decimos que $\{\rho : V(G) \to C :$ ρ es una k-coloración propia$\}$ es el conjunto de k-coloraciones propias de G y nos referiremos al cardinal de este conjunto como el número de k-coloraciones propias de G. Atendiendo a la observación 1, podemos ver que el número de k-coloraciones y el número de k-coloraciones propias de G no depende del conjunto C escogido.

Observación 2. Es importante destacar que las clases de coloración de una k-coloración propia de un grafo G resultan ser conjuntos independientes de G.

Dado un grafo G se plantea si existe una k-coloración propia de G y en caso de haberla, calcular cuántas k-coloraciones propias distintas hay. Esta es la pregunta a la que vamos a dedicar este trabajo y a la cual daremos respuesta en el tercer capitulo. Primero vamos a estudiar esta cuestión en el ámbito de la teoría de grafos.

Observación 3. Dado un grafo G k-coloreable, se tiene que cada subgrafo $H \subset G$ es k-coloreable. Esto ocurre porque cada k-coloración propia de G se restringe a una k-coloración propia de H.

Definición 1.2.2. Sea G un grafo. Decimos que G es un grafo no conexo si existen dos subconjuntos disjuntos de vértices no vacíos $V_1, V_2 \subset V(G)$ tales que $V(G) = V_1 \cup V_2$ y para cada $i \in V_1$ y $j \in V_2$ se tiene que i y j no son adyacentes.

Se dice que un grafo G es conexo si G no es no conexo.

Sea $x \in V(G)$. Se dice que el subgrafo $H \subset G$ es la componente conexa de x si $x \in V(H)$, H es conexo y para cada subgrafo conexo $H' \subset G$ con $x \in H'$ se tiene que $H' \subset H$.

Observación 4. Dado un grafo G, notamos que el conjunto $\{H_1, \ldots, H_s\}$ de las componentes conexas de G satisface que $\{V(H_1), \ldots, V(H_s)\}$ es una partición de $V(G)$. Además, G es conexo si y solo si la única componente conexa de G es G.

Proposición 1.2.1. *Sea G un grafo y sea $\{H_1, \ldots, H_s\}$ el conjunto de las componentes conexas de G. Entonces, se tiene que G es k-coloreable si y solo si cada H_i es k-coloreable para $1 \leq i \leq s$. Además, en este caso, el número de k-coloraciones propias de G es igual al producto del número de k-coloraciones propias de cada H_i.*

Demostración. Claramente, si G es k-coloreable, entonces cada componente conexa es k-coloreable como hemos detallado en la observación 3.

Recíprocamente, supongamos que cada componente conexa de G es k-coloreable. Sea C un conjunto de k colores. Para cada i, $1 \leq i \leq s$, existen $\rho_i : V(H_i) \to C$ k-coloraciones propias de cada H_i. Definimos la k-coloración $\rho : V(G) \to C$ de la siguiente manera: dado un vértice $x \in V(G)$ existe un único i_0, $1 \leq i_0 \leq s$, para el cual $x \in V(H_{i_0})$. Entonces definimos $\rho(x) = \rho_{i_0}(x)$. La aplicación ρ está bien definida porque $\{V(H_1), \ldots, V(H_s)\}$ es una partición de $V(G)$ y además es una k-coloración propia.

Para ver que efectivamente ρ es propia, sean $x, y \in V(G)$ adyacentes. Existe un único i_0, $1 \leq i_0 \leq s$, para el cual $x \in V(H_{i_0})$. Entonces $G[\{x, y\}]$ es un grafo conexo por ser x e y adyacentes. Por definición de componente conexa de x se tiene que $G[\{x, y\}] \subset H_{i_0}$ y por lo tanto $y \in V(H_{i_0})$. Entonces $\rho(y) = \rho_{i_0}(y) \neq \rho_{i_0}(x) = \rho(x)$.

Supongamos que G es k-coloreable. Hemos visto que cada elección de las k-coloraciones propias de H_i, ρ_i, se corresponde con una k-coloración propia de G. Además, dos elecciones distintas de las k-coloraciones ρ_i de los grafos H_i se corresponden con dos k-coloraciones de G distintas. Toda k-coloración propia de G puede recuperarse a partir de las k-coloraciones que induce sobre cada H_i. Entonces, el número de k-coloraciones propias de G es igual al producto del número de k-coloraciones propias de cada H_i.

□

Esta proposición indica que podemos estudiar la k-coloreabilidad de un grafo G a través de sus componentes conexas y además obtener el número de k-coloraciones propias de G a partir del número de k-coloraciones propias de cada una de las componentes conexas de G.

Definición 1.2.3. Sea G un grafo y sea $k \geq 1$. Denotamos por $P_G(k)$ al número de k-coloraciones propias de G.

El número cromático de G, $\chi(G)$, es el mínimo valor de $k \geq 1$ tal que $P_G(k) > 0$. Es decir, $\chi(G) = \min(k \geq 1 \ : \ P_G(k) > 0)$.

Observación 5. La proposición 1.2.1 implica que dado G un grafo cuyas componentes conexas son $H_1, \ldots, H_s$, se pude obtener $\chi(G)$ y $P_G(k)$ a partir de los valores de $\chi(H_i)$ y $P_{H_i}(k)$ de la siguiente manera:

$$\chi(G) = \max(\chi(H_i) : \ 1 \leq i \leq s)$$
$$P_G(k) = \prod_{i=1}^{s} P_{H_i}(k)$$

La aplicación $P_G : \mathbb{N} \to \mathbb{Z}_{\geq 0}$ recoge toda la información asociada al número de coloraciones propias del grafo G. Esta aplicación resulta ser un polinomio de grado igual al número de vértices de G.

Proposición 1.2.2. *Sea G un grafo de n vértices. Entonces $P_G(k)$ es un polinomio mónico en k de grado n con coeficientes enteros de signo alternado. Es decir, el coeficiente t-ésimo de $P_G(k)$ tiene signo $(-1)^{n-t}$, $0 \leq t \leq n$.*

Demostración. Vamos a razonar por inducción sobre el número de aristas de G.

Si $|A(G)| = 0$ se tiene que ningún par de vértices son adyacentes por lo que cada k-coloración de G es propia. Por lo tanto, $P_G(k) = |\{\rho : V(G) \to C\}| = k^n$.

Supongamos que existe una arista, a de extremos $i, j \in V(G)$. Consideramos el grafo de n vértices $G - a$, resultado de eliminar la arista a de G, y el grafo de $n-1$ vértices G/a resultado de identificar los dos extremos de a. Notamos que una k-coloración propia de

$G - a$ se identifica o bien con una k-coloración propia de G si los vértices i y j tienen distinto color, o bien con una k-coloración propia de G/a en el caso de que se coloreen los vértices i y j del mismo color. Esta correspondencia se expresa de la siguiente forma: $P_{G-a}(k) = P_G(k) + P_{G/a}(k)$, lo que es equivalente a lo siguiente:

$$P_G(k) = P_{G-a}(k) - P_{G/a}(k)$$

El número de aristas de los grafos $G-a$ y G/a es menor que el de G por lo que podemos aplicar la hipótesis de inducción y deducir que $P_{G-a}(k)$ es un polinomio mónico en k de grado n con coeficientes enteros, y $P_{G/a}(k)$ es un polinomio mónico en k de grado $n-1$ con coeficientes enteros. Por tanto se concluye que $P_G(k)$ es es un polinomio mónico en k de grado n con coeficientes enteros. Además, el coeficiente t-esimo de $P_{G-a}(k)$ tiene signo $(-1)^{n-t}$ y el coeficiente t-ésimo de $-P_{G/a}(k)$ tiene signo $-(-1)^{n-1-t} = (-1)^{n-t}$. En consecuencia, el coeficiente t-ésimo de $P_G(k)$ tiene signo $(-1)^{n-t}$, $0 \leq t \leq n$.

□

Definición 1.2.4. Sea G un grafo de n vértices. Se denomina polinomio cromático de G al polinomio mónico de grado n, $P_G(k)$.

En general, calcular tanto el número cromático como el polinomio cromático de un grafo resulta difícil; sin embargo, para ciertos tipos de grafos es posible caracterizar su número cromático. Por ejemplo, en el caso de grafos completos claramente se puede ver que el número cromático coincide con el orden del grafo ya que todos los vértices son adyacentes entre sí. También resulta sencillo calcular el número cromático de la siguiente familia de grafos:

Para cada $n \geq 2$ se define el *grafo ciclo de orden* n, que denotaremos por C_n, de la siguiente forma: los vértices de C_n son $V(C_n) = \{1, \ldots, n\}$. Dados dos vértices $i, j \in V(C_n)$, se tiene que $(i, j) \in A(C_n)$ si y solo si i y j son consecutivos o $i = 1$ y $j = n$ (o viceversa).

Entonces se tiene que:

$$\chi(C_n) = \begin{cases} 2, & \text{si } n \text{ es par} \\ 3, & \text{si } n \text{ es impar.} \end{cases}$$

Evidentemente $\chi(C_n) \geq 2$ puesto que los vértices de C_n no son aislados. Para n par podemos encontrar un 2-coloración de C_n coloreando los vértices de forma alternada. Sin embargo, esto no ocurre si n es impar por lo que en este caso se necesitan 3 colores para colorear C_n.

La observación 3 implica que $\chi(H) \leq \chi(G)$ para cada subgrafo $H \subset G$. Este hecho nos permite dar una cota inferior del numero cromático de G: para cada clique de tamaño m, $K_m \subset G$, se tiene que $m = \chi(K_m) \leq \chi(G)$, por lo tanto $\omega(G) \leq \chi(G)$.

Notamos que esta cota no se alcanza en general como podemos ver en el ejemplo de C_n tomando n impar estrictamente mayor que 3. En esta situación se tiene que $\chi(C_n) = 3$

como hemos visto; sin embargo, no existe ningún clique de tamaño 3.

Podemos mejorar esta cota inferior haciendo uso de la información que proporciona el número de independencia de un grafo.

Proposición 1.2.3. *Sea G un grafo. Se tiene que* $\text{máx}\left(\omega(G), \dfrac{|V(G)|}{\alpha(G)}\right) \leq \chi(G)$.

Demostración. Dada una k-coloración propia de G se tiene que cada clase de coloración, $cl(c_i)$, es un conjunto independiente como hemos destacado en la observación 2. Por lo tanto se tiene que $|V(G)| = \sum_{i=1}^{k} |cl(c_i)| \leq k \cdot \alpha(G)$. Por lo tanto se tiene que $\dfrac{|V(G)|}{\alpha(G)} \leq k$ y en particular $\dfrac{|V(G)|}{\alpha(G)} \leq \chi(G)$.

□

Vamos a introducir un algoritmo de coloración que proporciona una coloración propia de un grafo. En general, el número de colores que emplea el algoritmo es mayor que el número cromático del grafo, pero permite obtener cotas superiores para este. La descripción del *algoritmo de coloración voraz* es la siguiente:

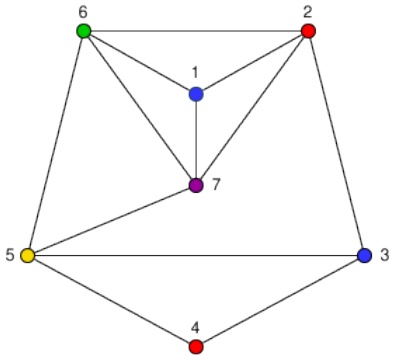
Algoritmo voraz

INPUT: G
OUTPUT: $\rho : V(G) \to C$ coloración propia de G
$\overline{C} \leftarrow \{c_1, \ldots c_n\}$
$\rho(1) \leftarrow c_1$
$C \leftarrow \{c_1\}$
for $2 \leq i \leq n$ do
  $H \leftarrow \overline{C} \setminus \{\rho(j) : \ j < i, \ (i,j) \in A(G)\}$
  $t \leftarrow min(j \geq 1 : \ c_j \in H)$
  $\rho(i) \leftarrow c_t$
  $C \leftarrow C \cup \{c_t\}$
end for

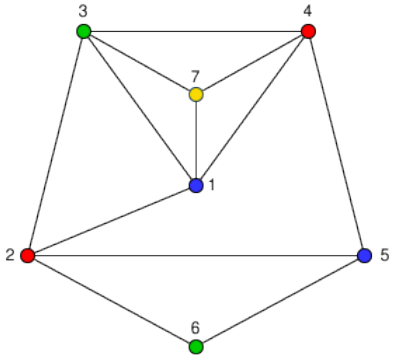
Vamos a detallar el funcionamiento del algoritmo. En primer lugar, dado que sabemos que el número máximo de colores necesarios para colorear el grafo es a lo sumo n se elige un conjunto de colores $\overline{C} = \{c_1, \ldots, c_n\}$ de n elementos. El algoritmo voraz colorea los vértices del grafo G en orden empezando por el vértice 1 y acabando en el vértice n. Para ello en el paso i-ésimo se colorea el vértice i empleando el color con el índice más bajo de entre los que no han sido empleados para colorear ninguno de los vértices adyacentes de i. De esta forma, la coloración resultante es propia.

Notamos que la forma en las que se tomen los vértices de G influye en el orden en el que se colorean cuando se emplea el algoritmo voraz. De hecho, dependiendo de esta

elección, este algoritmo puede producir coloraciones propias de G que emplean distinto número de colores. Podemos ver este hecho en el siguiente ejemplo:



(a) figura 1.1



(b) figura 1.1

Ejemplo 1. Tomamos el mismo grafo G en el que hemos nombrado los vértices de dos formas distintas. Si se nombran los vértices como en la figura 1.1a, se tiene que el algoritmo voraz devuelve ρ_1, una coloración propia de G que emplea 5 colores la cual se muestra en dicha figura:

$$\rho_1(1) = \rho_1(3) = c_1,\ \rho_1(2) = \rho_1(4) = c_2,\ \rho_1(5) = c_3,\ \rho_1(6) = c_4,\ \rho_1(7) = c_5$$

Sin embargo, si se aplica el algoritmo voraz al grafo G con los vértices nombrados como en la figura 1.1b, se obtiene, ρ_2, una 4-coloración propia de G:

$$\rho_2(1) = \rho_2(5) = c_1,\ \rho_2(2) = \rho_2(4) = c_2,\ \rho_2(3) = \rho_2(6) = c_3,\ \rho_2(7) = c_4$$

Se puede observar esta 4-coloración el la figura 1.1b.

Dado que G contiene un subgrafo completo de 4 vértices se deduce que $\chi(G) = 4$ y por lo tanto en el segundo caso hemos el algoritmo devuelve una coloración óptima en el sentido que emplea exactamente $\chi(G)$ colores.

Observación 6. En general, dado un grafo G siempre es posible encontrar un orden de sus vértices para el cual el algoritmo de coloración voraz devuelve una coloración propia que emplea $\chi(G)$ colores.

Para verlo, tomamos $\rho : V(G) \to C$ una coloración propia de G que emplee $\chi(G)$ colores. Supondremos que el conjunto de colores es de la forma $C = \{c_1, c_2, \ldots, c_{\chi(G)}\}$. Denotamos por $cl(c_i) \subset V(G)$ a la clase del color c_i. Modificamos ρ mediante el siguiente procedimiento para obtener una coloración propia $\tilde{\rho}$ que también emplea $\chi(G)$ colores:

INPUT: $\rho : V(G) \to C$ $\chi(G)$-coloración porpia
OUTPUT: $\tilde{\rho} : V(G) \to C$ $\chi(G)$-coloración propia
$\tilde{\rho}(1) \leftarrow \rho(1), \tilde{\rho}(2) \leftarrow \rho(2), \ldots, \tilde{\rho}(n) \leftarrow \rho(n)$
for $2 \leq i \leq n$ do
  for $v \in cl(c_i)$ do
    $H \leftarrow C \setminus \{\tilde{\rho}(j) : \ (v, j) \in A(G)\}$
    $t \leftarrow min(j \geq 1 : \ c_j \in H)$
    $\tilde{\rho}(v) \leftarrow c_t$
  end for
end for

Notamos que en cada paso del procedimiento anterior, la coloración $\tilde{\rho}$ sigue siendo propia y evidentemente emplea $\chi(G)$ colores. Diremos que la coloración $\tilde{\rho}$ que obtenemos tras terminar este proceso está reducida. Denotamos por $\tilde{C}_i \subset V(G)$ a la clase del color c_i de la coloración $\tilde{\rho}$. Ordenamos los vértices de los conjuntos $\tilde{C}_i$ de forma arbitraria y establecemos el siguiente orden sobre los vértices de G: primero los vértices de $\tilde{C}_1$ siguiendo el orden escogido, después los vértices de $\tilde{C}_2$ atendiendo al orden escogido en $\tilde{C}_2$. De esta forma procedemos con cada clase de color $\tilde{C}_i$ hasta terminar con $\tilde{C}_{\chi(G)}$.

Examinando el algoritmo voraz y atendiendo a la estructura de $\tilde{\rho}$, que está reducida, notamos que con este orden de $V(G)$, el algoritmo voraz devuelve precisamente la coloración $\tilde{\rho}$. Por lo tanto, el algoritmo devuelve una coloración propia de G que emplea exactamente $\chi(G)$ colores.

Hemos encontrado cotas inferiores para el número cromático de un grafo G. Ahora tratamos de acotar superiormente $\chi(G)$: claramente se tiene que $\chi(G) \leq |V(G)|$ para cada grafo G ya que podemos colorear cada vértice de G de un color distinto y obtener una $|V(G)|$-coloración propia. Notamos que se da la igualdad en el caso de grafos completos. Esta cota superior del número cromático no emplea ninguna información del grafo G salvo su orden. Por eso, tratamos de buscar acotaciones que involucren más datos de G y sean más ajustadas. Los conceptos que vamos a introducir nos van a permitir establecer cotas superiores del número cromático analizando el funcionamiento del algoritmo voraz para ciertos órdenes de los vértices de G.

Definición 1.2.5. Sea G un grafo.

1. Sea v un vértice de G. El grado de v es el número de vértices adyacentes a v y se denota por $d(v)$.

2. Denotamos por $\Delta(G)$ al máximo de los grados de los vértices de G; es decir, $\Delta(G) = \text{máx}\,(d(v) : \ v \in V(G))$.

3. Denotamos por $\delta(G)$ al mínimo de los grados de los vértices de G; es decir,

$$\delta(G) = \min(d(v) : \ v \in V(G)).$$

Examinando el algoritmo voraz podemos notamos lo siguiente: en el paso i-ésimo se colorea el vértice i para el cual se elige el color disponible con menor índice; es decir, el color que se le asigna a este vértice debe pertenecer al conjunto $\{c_1, \ldots, c_{d(i)+1}\}$ porque en el peor de los casos todos los vértices adyacentes a i son menores que i y se les ha asignado los primeros $d(i)$ colores. Por lo tanto, el algoritmo requiere de a lo sumo $d(i)+1$ colores para colorear el vértice i y en consecuencia necesita como máximo $\Delta(G)+1$ colores. De este hecho se deduce que $\chi(G) \leq \Delta(G)+1$. Esta cota se alcanza en el caso de los grafos completos y en los grafos ciclo de orden impar. De hecho, el *teorema de Brooks* asegura que estos son los únicos grafos conexos para los que se da la igualdad. Se puede encontrar la demostración del teorema en [15, Thm. 5.1.22].

Teorema 1.2.1. *Sea G un grafo. Sea $k = \max(\delta(H) : \ H = G[W],\ W \subset V(G))$. Entonces $\chi(G) \leq k+1$.*

Demostración. De la definición de k se tiene que en particular $\delta(G) \leq k$ por lo tanto es posible encontrar un vértice $x_n \in V(G)$ tal que $d(x_n) \leq k$. Consideramos el subgrafo $H_{n-1} = G - \{x_n\}$, al ser un subgrafo inducido se tiene por hipótesis que $\delta(H_{n-1}) \leq k$. Entonces es posible encontrar un vértice $x_{n-1} \in V(H_{n-1})$ tal que $d_{H_{n-1}}(x_{n-1}) \leq k$. Repitiendo el proceso con el subgrafo inducido $H_{n-2} = G - \{x_n, x_{n-1}\}$ encontramos un vértice de H_{n-2} cuyo orden en H_{n-2} es menor que k. De esta forma podemos renombrar todos los vértices de G de forma que cada uno de los vértices de G es adyacente a como máximo k vértices precedentes. Si aplicamos el algoritmo de coloración voraz a G con este nuevo orden de los vértices, notamos que en el paso i el número de colores que se necesitan para colorear el vértice x_i es a lo sumo $k+1$ y por tanto el algoritmo requiere como máximo $k+1$ colores. En consecuencia $\chi(G) \leq k+1$.

□

Es posible modificar el algoritmo voraz y mejorar su eficacia si se conoce el número cromático de un subgrafo H_0 del grafo G que se quiere colorear. En este caso, se obtiene además una cota más ajustada para el número cromático de G.

Teorema 1.2.2. *Sea G un grafo. Sea $H_0 \subset G$ tal que para cada subgrafo $H_0 \subsetneq H \subset G$ existe un vértice $v \in V(H) \setminus V(H_0)$ tal que $d_H(v) \leq k$. Es decir, para cada cada subgrafo $H_0 \subsetneq H \subset G$ se tiene que $\delta(H) \leq k$. Entonces $\chi(G) \leq \max(k+1, \chi(H_0))$.*

Demostración. La prueba de esta demostración es similar a la de la proposición previa: en primer lugar, podemos suponer que $H_0 \neq G$, pues en caso contrario la desigualdad se satisface de forma trivial. Se tiene que por hipótesis es posible tomar un vértice $x_n \in V(G)$ tal que $d(x_n) \leq k$. Considerando el subgrafo $H_{n-1} = G - \{x_n\}$ se tiene que o bien $H_{n-1} = H_0$, o bien existe un vértice $x_{n-1} \in V(H_{n-1})$ tal que $d_{H_{n-1}}(x_{n-1}) \leq k$. Supongamos que se da el segundo caso, podemos proceder de la misma manera hasta que finalmente se llegue al primer caso y obtengamos una reordenación de los vértices

$V(G) \setminus V(H_0)$.

Por otro lado, dado que conocemos el número cromático de H_0 podemos suponer que podemos reordenar los vértices de H_0 de forma que el algoritmo voraz los coloree de forma óptima; es decir, empleando $\chi(H_0)$ colores. Con este nuevo orden se tiene que los vértices de H_0 y G son $V(H_0) = \{x_1, \ldots, x_{|H_0|}\}$ y $V(G) = \{x_1, \ldots, x_{|H_0|}, x_{|H_0|+1}, \ldots, x_n\}$ respectivamente. Si aplicamos el algoritmo voraz a G con este orden de sus vértices, se tiene que en el paso i-ésimo se necesitan como máximo $\chi(H_0)$ colores para colorear el vértice x_i en el caso de que $x_i \in H_0$, o $k+1$ colores si $x_i \notin H_0$. De este hecho se deduce que $\chi(G) \leq \text{máx}\,(k+1, \chi(H_0))$.

□

Capítulo 2

Introducción conceptos algebraicos

2.1. Variedades afines

Sea $\mathbb{K}$ un cuerpo infinito, denotamos por $\mathbb{K}[x_1, \ldots, x_n]$ al anillo de polinomios sobre $\mathbb{K}$ en n variables. El contenido de esta sección se va a desarrollar para un cuerpo infinito cualquiera; sin embargo, lo usual es trabajar con $\mathbb{K} = \mathbb{C}$ o cualquier cuerpo algebraicamente cerrado, que como veremos proporciona grandes ventajas.

Dado un subconjunto $S \subset \mathbb{K}[x_1, \ldots, x_n]$ consideramos el siguiente subconjunto del espacio afín n-dimensional $\mathbb{A}^n_{\mathbb{K}}$:

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{K}} : \ f(a_1, \ldots, a_n) = 0 \ \ \forall f \in S\}$$

Los conjuntos $V \subset \mathbb{A}^n_{\mathbb{K}}$ para los cuales existe un conjunto $S \subset \mathbb{K}[x_1, \ldots, x_n]$ con $V = V(S)$ se denominan *variedades afines*.

Notación 2.1.1. *Dado un conjunto finito de polinomios $S = \{p_1, \ldots, p_s\} \subset \mathbb{K}[x_1, \ldots, x_n]$ denotamos por $V(p_1, \ldots, p_s)$ a la variedad afín $V(\{p_1, \ldots, p_s\})$.*

De forma dual, dada una variedad afín $V \subset \mathbb{A}^n_{\mathbb{K}}$ definimos el siguiente conjunto de polinomios:

$$I(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : \ f(a) = 0 \ \ \forall a \in V\}$$

Este conjunto resulta ser un ideal del anillo de polinomios: resulta sencillo ver que dados $f, g \in I(V)$ su suma es también un elemento de $I(V)$, puesto que $(f + g)(a) = f(a) + g(a) = 0$ para cada $a \in V$. De igual forma dado $h \in \mathbb{K}[x_1, \ldots, x_n]$ se tiene que $(hf)(a) = h(a) \cdot f(a) = h(a) \cdot 0 = 0$ por lo que $hf \in I(V)$.

El objetivo de esta sección es estudiar la relación entre estas dos operaciones que culminará con el *Nullstellensatz*. Este resultado nos asegurará que si trabajamos en un

cuerpo algebraicamente cerrado y bajo ciertas condiciones adicionales, las correspondencias anteriores resultan ser inversas de la otra. Este hecho nos permitirá estudiar las cuestiones relacionadas a una variedad afín V mediante el ideal de polinomios $I(V)$ y viceversa.

Proposición 2.1.1. *Las correspondencias $V(\cdot)$ e $I(\cdot)$ invierten las contenciones. Es decir:*

1. *Dados dos subconjuntos $S_1 \subset S_2 \subset \mathbb{K}[x_1, \ldots, x_n]$, se tiene que $V(S_2) \subset V(S_1)$*
2. *Dadas dos variedades afines $V_1 \subset V_2 \subset \mathbb{A}^n_{\mathbb{K}}$, entonces se tiene que $I(V_2) \subset I(V_1)$*

Demostración. 1. Sean $S_1 \subset S_2 \subset \mathbb{K}[x_1, \ldots, x_n]$. Sea $a \in V(S_2)$. Para cada polinomio $f \in S_2$ se tiene que $f(a) = 0$. En particular para cada polinomio $f \in S_1 \subset S_2$ se tiene que $f(a) = 0$; es decir, $a \in V(S_1)$.

2. Sean $V_1 \subset V_2 \subset \mathbb{A}^n_{\mathbb{K}}$ dos variedades afines. Sea $f \in I(V_2)$, entonces $f(a) = 0$ para cada $a \in V_2$. En particular para cada $a \in V_1 \subset V_2$ se tiene que $f(a) = 0$ y por lo tanto $f \in I(V_1)$.

□

Observación 7. Un hecho notable es que el conjunto $S \subset \mathbb{K}[x_1, \ldots, x_n]$ y el ideal generado por este, $\langle S \rangle$, determinan la misma variedad afín. Esto es decir $V(S) = V(\langle S \rangle)$. Este hecho plantea de forma natural si esta correspondencia entre ideales y variedades afines es biunívoca; es decir, si $I(\cdot)$ y $V(\cdot)$ son inversas la una de la otra.

Proposición 2.1.2. *Sean $W \subset \mathbb{A}^n_{\mathbb{K}}$ una variedad afín y $J \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal.*

1. *$J \subset I(V(J))$*
2. *$W = V(I(W))$*

Demostración. 1. Sean $f \in J$ y $a \in V(J)$. Por la definición de $V(J)$ se deduce que $f(a) = 0$. De esta forma $f(a) = 0$ para cada $a \in V(J)$ y en consecuencia $f \in I(V(J))$.

2. Dada una variedad afín $W \subset \mathbb{A}^n_{\mathbb{K}}$ existe un ideal $J \subset \mathbb{K}[x_1, \ldots, x_n]$ con $W = V(J)$. Entonces se tiene que $J \subset I(V(J)) = I(W)$ como hemos probado en el apartado previo. En virtud de la proposición 2.1.1 obtenemos la contención $V(I(W)) \subset V(J) = W$.

   La otra contención se deduce de las definiciones de $I(W)$ y de $V(I(W))$. Dados $a \in W$ y $f \in I(W)$ se tiene que $f(a) = 0$ por definición de $I(W)$. Por lo tanto, $a \in V(I(W))$.

□

Proposición 2.1.3. *Sean dos ideales $I, J \subset \mathbb{K}[x_1, \ldots, x_n]$. Entonces se satisfacen las siguientes igualdades:*

1. $V(I + J) = V(I) \cap V(J)$.
2. $V(I \cap J) = V(I) \cup V(J)$.

Demostración. 1. Se tiene que $I \subset I + J$ lo que implica que $V(I + J) \subset V(I)$ por la proposición 2.1.1. Igualmente se tiene que $J \subset I+J$ y por lo tanto $V(I+J) \subset V(I)$. En consecuencia $V(I + J) \subset V(I) \cap V(J)$.

Recíprocamente, sea $a \in V(I) \cap V(J)$. Dado $p \in I + J$ existen $f \in I$ y $g \in J$ tales que $p = f + g$. Entonces se tiene que $p(a) = f(a) + g(a) = 0$ porque tanto f como g se anulan en a.

2. Las contenciones $I \cap J \subset I$ e $I \cap J \subset J$ implican las contenciones $V(I) \subset V(I \cup J)$ y $V(J) \subset V(I \cup J)$. Es decir, se tiene que $V(I) \cup V(J) \subset V(I \cap J)$.

Recíprocamente, sea $a \in V(I \cap J)$. Supongamos que $a \notin V(I)$. Entonces existe $f \in I$ tal que $f(a) \neq 0$. Sea $g \in J$, $fg \in I \cap J$ por lo que $f(a)g(a) = 0$. Podemos deducir que $g(a) = 0$. Por lo tanto $a \in V(J)$. En consecuencia $V(I \cap J) \subset V(I) \cup V(J)$.

□

Proposición 2.1.4. *Sea $S \subset \mathbb{A}^n_{\mathbb{K}}$ un conjunto finito. Entonces S es una variedad afín. En particular, si W es una variedad finita, cada subconjunto $S \subset W$ es una variedad afín.*

Demostración. En primer lugar probamos la afirmación para un solo punto. Sea $a = (a^1, \ldots, a^n) \in \mathbb{A}^n_{\mathbb{K}}$ un punto. Se tiene que $\{a\} = V(x_1 - a^1, \ldots x_n - a^n)$: efectivamente se tiene que $b = (b^n, \ldots, b^n) \in V(x_1 - a^1, \ldots x_n - a^n)$ si y solo si $b^i - a^i = 0$ para cada i, $1 \leq i \leq n$; es decir, $b \in V(x_1 - b^1, \ldots x_n - b^n)$ si y solo si $b = a$.

Sea $S = \{a_1, \ldots, a_s\}$ un subconjunto finito de $\mathbb{A}^n_{\mathbb{K}}$ donde $a_i = (a_i^1, \ldots, a_i^n)$. Consideramos el ideal $I = \bigcap_{i=1}^s \langle x_1 - a_i^1, \ldots, x_n - a_i^n \rangle$. Por la proposición 2.1.3 tiene que $V(I) = \bigcup_{i=1}^s V(x_1 - a_i^1, \ldots x_n - a_i^n) = \bigcup_{i=1}^s \{a_i\} = S$.

□

Proposición 2.1.5. *Sean $W_1 \subset \mathbb{A}^n_{\mathbb{K}}$ y $W_2 \subset \mathbb{A}^m_{\mathbb{K}}$ dos variedades afines. Sean $I_1 = I(W_1) \subset \mathbb{K}[x_1, \ldots, x_n]$ y $I_2 = I(W_2) \subset \mathbb{K}[x_{n+1}, \ldots, x_{n+m}]$ donde $I_1 = \langle f_1, \ldots, f_s \rangle$ y $I_2 = \langle g_1, \ldots, g_t \rangle$. Entonces $W_1 \times W_2$ es una variedad afín de $\mathbb{A}^{n+m}_{\mathbb{K}}$ y se tiene que $W_1 \times W_2 = V(f_1, \ldots, f_s, g_1, \ldots, g_t)$.*

Demostración. Sea $(a, b) \in V(f_1, \ldots, f_s, g_1, \ldots, g_t)$ donde $a \in \mathbb{A}^n_{\mathbb{K}}$ y $b \in \mathbb{A}^m_{\mathbb{K}}$. Se tiene que $f_i(a) = f_i(a, b) = 0$ para cada i, $1 \leq i \leq s$; es decir, $a \in V(I_1) = W_1$. De igual manera, $g_i(b) = g_i(a, b) = 0$ para cada i, $1 \leq i \leq t$, y por lo tanto $b \in W_2$. En consecuencia

$(a, b) \in W_1 \times W_2$.

Recíprocamente, sea $(a, b) \in W_1 \times W_2$, entonces $f_i(a) = f_i(a, b) = 0$ para cada i, $1 \leq i \leq s$ porque $a \in W_1$. De igual forma, $g_i(b) = g_i(a, b) = 0$ para cada i, $1 \leq i \leq t$ ya que $b \in W_2$. Entonces $(a, b) \in V(f_1, \ldots, f_s, g_1, \ldots, g_t)$.

□

Definición 2.1.1. Sean I, J dos ideales de un anillo conmutativo R. El conjunto

$$I : J = \{r \in R : \ rg \in I \ \forall g \in J\}$$

es un ideal de R que contiene a I. Este ideal se denomina ideal cociente de I y J.

Lema 2.1.1. *Sean I, J, K tres ideales de un anillo conmutativo R. Entonces se tiene:*

$$K \subset I : J \iff J \subset I : K$$

Demostración. Supongamos que $K \subset I : J$ y sean $g \in J$ y $h \in K$. Se tiene que $gh \in I$ porque $h \in I : J$. Dado que h es arbitrario podemos deducir que $g \in I : K$. La otra implicación se demuestra invirtiendo los roles de J y K.

□

Corolario 2.1.1. *Sean I, J dos ideales de $\mathbb{K}[x_1, \ldots, x_n]$. Entonces se tiene:*

$$J \subset I \iff 1 \in I : J$$

Demostración. Tomamos el ideal $K = \mathbb{K}[x_1, \ldots, x_n]$. Por el lema 2.1.1, se tiene que $J \subset I : K \ \Leftrightarrow \ K \subset I : J$. El ideal $I : K = I : \mathbb{K}[x_1, \ldots, x_n] = I$ ya que para para cada $f \in I : K$ se debe satisfacer $f \cdot 1 \in I$. Además, $K \subset I : J$ ocurre si y solo si $1 \in I : J$. Luego se deduce la equivalencia afirmada.

□

Proposición 2.1.6. *Sean $W_1, W : 2$ dos variedades afín de $\mathbb{A}^n_{\mathbb{K}}$. Entonces se satisface la igualdad:*

$$I(W_1) : I(W_2) = I(W_1 \setminus W_2)$$

Demostración. Sea $f \in I(W_1 \setminus W_2)$ y sea $g \in I(W_2)$. Vamos a probar que el producto fg pertenece a $I(W_1)$, para ello tomamos $a \in W_1$ y comprobamos que fg se anula en a. Si $a \in W_1 \setminus W_2$, entonces $f(a) = 0$. Si por el contrario $a \in W_2 \cap W_1$, se tiene que $g(a) = 0$. En cualquier caso, $(fg)(a) = 0$ y por lo tanto $f \in I(W_1) : I(W_2)$.

Recíprocamente, sea $f \in I(W_1) : I(W_2)$ y sea $a \in W_1 \setminus W_2$. Dado que $a \notin W_2$ se tiene que existe un polinomio $g \in I(W_2)$ tal que $g(a) \neq 0$. Entonces, de la definición de

ideal cociente se tiene que $fg \in I(W_1)$ y en consecuencia $0 = (fg)(a) = f(a)g(a)$, de lo que se deduce que $f(a) = 0$. En consecuencia $f \in I(W_1 \setminus W_2)$.

□

Nos planteamos si cada ideal del anillo de polinomios es el ideal de una cierta variedad afín. La respuesta es negativa ya que los ideales de una variedad afín satisfacen una propiedad adicional, son ideales *radicales*.

Proposición 2.1.7. *Dado un ideal I de un anillo conmutativo R se define*

$$\sqrt{I} = \{r \in R : \exists\, n \geq 1 \text{ tal que } r^n \in I\}.$$

Este conjunto es un ideal que contiene a I denominado radical de I.

Demostración. Se tiene que $0 \in \sqrt{I}$ pues de forma trivial $0^1 = 0 \in I$.

$\sqrt{I}$ es cerrado para la suma: dados $a, b \in \sqrt{I}$, vamos a probar que $a + b \in \sqrt{I}$. Existen $n, m \geq 1$ tales que $a^n, b^m \in I$. Empleando la fórmula del binomio de Newton podemos notar lo siguiente:

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} = b^m \left[\sum_{k=0}^{n-1} \binom{n+m}{k} a^k b^{n-k} \right]$$

$$+a^n \left[\sum_{k=n}^{n+m} \binom{n+m}{k} a^{k-n} b^{n+m-k} \right] \in I$$

Por lo que se deduce que $a + b \in \sqrt{I}$.

$\sqrt{I}$ es cerrado para el producto por elementos de R. Dados $a \in \sqrt{I}$ y $r \in R$ se tiene que existe $n \geq 1$ tal que $a^n \in I$. Entonces se deduce que $(ra)^n = r^n a^n \in I$ y por lo tanto $ra \in \sqrt{I}$.

Evidentemente $I \subset \sqrt{I}$ pues para cada $a \in I$ tomando $n = 1$ se satisface $a^1 \in I$.

□

Definición 2.1.2. Se dice que un ideal $I \subset R$ es radical si $I = \sqrt{I}$.

Proposición 2.1.8. *Dada una variedad afín $W \subset \mathbb{A}^n_{\mathbb{K}}$, el ideal $I(W)$ es un ideal radical.*

Demostración. Dado un polinomio $f \in \sqrt{I(W)}$ existe un $n \geq 1$ tal que $f^n \in I(W)$. Luego, para cada $a \in W$ se tiene que $f(a)^n = f^n(a) = 0$ de lo que se deduce que $f(a) = 0$. Por lo tanto, $f \in I(W)$.

□

Esta proposición nos indica que debemos restringirnos a los ideales radicales de $\mathbb{K}[x_1, \ldots, x_n]$ para establecer una correspondencia con variedades afines de $\mathbb{A}^n_{\mathbb{K}}$. Sin embargo, aún en esta situación no obtenemos una correspondencia biunívoca en general.

Un ejemplo de este hecho es el ideal radical $J = \langle x^2 + 1 \rangle \subset \mathbb{R}[x]$. Podemos ver que no es el ideal de ninguna variedad de $\mathbb{A}^1_{\mathbb{R}}$. En efecto pues no existe ningún $a \in \mathbb{A}^1_{\mathbb{R}}$ para el cual $a^2 = -1$. Por lo tanto, la única variedad afín de la cual J pudiera ser su ideal seria $V = \emptyset$ pero $I(\emptyset) = \mathbb{R}[x] \supsetneq J$.

Notamos que si hubiésemos trabajado sobre $\mathbb{C}$ en el ejemplo anterior no habría surgido este problema, pues en efecto $J = \langle x^2 + 1 \rangle \subset \mathbb{C}[x]$ es el ideal de la variedad $V = \{i, -i\}$. Esto pone en manifiesto la importancia de trabajar sobre un cuerpo $\mathbb{K}$ algebraicamente cerrado como hemos adelantado al principio de capítulo.

Teorema 2.1.2 (Nullstellensatz forma débil)**.** *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal. Entonces, $V(I) = \emptyset$ si y solo si $I = \mathbb{K}[x_1, \ldots, x_n]$. En particular, $V(I) = \emptyset$ si y solo si $1 \in I$.*

Demostración. La demostración del teorema se pueden encontrar en [5, Chap. 4.1, Thm. 1].

□

Teorema 2.1.3 (Nullstellensatz)**.** *Dado un ideal de polinomios $I \subset \mathbb{K}[x_1, \ldots, x_n]$ sobre un cuerpo algebraicamente cerrado $\mathbb{K}$, se tiene que $I(V(I)) = \sqrt{I}$. En particular se tiene una correspondencia biunívoca:*

$$\begin{array}{ccc} \{\textit{variedades afines de } \mathbb{A}^n_{\mathbb{K}}\} & \longleftrightarrow & \{\textit{ideales radicales de } \mathbb{K}[x_1, \ldots, x_n]\} \\ V & \longmapsto & I(V) \\ V(I) & \longleftarrow & I \end{array}$$

Demostración. La demostración del teorema se pueden encontrar en [5, Chap. 4.1, Thm. 2].

□

Es posible dar un resultado más general que permite caracterizar cuándo una variedad afín es vacía.

Corolario 2.1.2. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Sean $p_1, \ldots, p_r, g \in \mathbb{K}[x_1, \ldots, x_n]$ tales que $V(p_1, \ldots, p_r, g) = \emptyset$. Entonces, $\langle p_1, \ldots, p_r \rangle = \mathbb{K}[x_1, \ldots, x_n]$ si y solo si $g \in \langle p_1, \ldots, p_r \rangle$.*

Demostración. Si $g \in \langle p_1, \ldots, p_r \rangle$, entonces se tiene que

$$\emptyset = V(p_1, \ldots, p_r, g) = V(\langle p_1, \ldots, p_r, g \rangle) = V(\langle p_1, \ldots, p_r \rangle).$$

Como consecuencia del teorema 2.1.2 se deduce que $\langle p_1, \ldots, p_r \rangle = \mathbb{K}[x_1, \ldots, x_n]$.

Recíprocamente, si $\langle p_1, \ldots, p_r \rangle = \mathbb{K}[x_1, \ldots, x_n]$ se deduce que $g \in \langle p_1, \ldots, p_r \rangle = \mathbb{K}[x_1, \ldots, x_n]$ trivialmente.

□

Teorema 2.1.4 (Teorema de la base de Hilbert)**.** *Sea $\mathbb{K}$ un cuerpo. Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal. Existe un número finito de polinomios $p_1, \ldots, p_s \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $I = \langle p_1, \ldots, p_s \rangle$.*

Demostración. La demostración del teorema 2.1.4 se dará en el tercer capítulo haciendo uso de las bases de Gröbner. □

El teorema 2.1.4 asegura que todo ideal de polinomios está finitamente generado. En particular, dado un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ podemos encontrar polinomios $p_1, \ldots, p_s$ que generan el ideal, $I = \langle p_1, \ldots, p_s \rangle$ y por lo tanto, atendiendo a las observaciones dadas, se puede deducir que la variedad $V(I) = V(\langle p_1, \ldots, p_s \rangle)$ queda determinada por este conjunto finito de generadores. Es decir, $V(I) = V(p_1, \ldots, p_s)$.

Otra consecuencia del teorema de la base de Hilbert es que el anillo $\mathbb{K}[x_1, \ldots, x_n]$ satisface la *condición de la cadena ascendente*. Esto también se expresa diciendo que $\mathbb{K}[x_1, \ldots, x_n]$ es un *anillo noetheriano*.

Corolario 2.1.3 (Condición de la cadena ascendente)**.** *Sea $\{I_n\}_{n \geq 1}$ una familia numerable de ideales de $\mathbb{K}[x_1, \ldots, x_n]$ tales que $I_1 \subset I_2 \subset \cdots I_n \subset \cdots$. Decimos que $\{I_n\}_{n \geq 1}$ es una cadena ascendente de ideales. Entonces existe N tal que $I_N = I_{N+k}$ para cada $k \geq 0$.*

Demostración. Sea $\{I_n\}_{n \geq 1}$ una cadena ascendente de ideales en $\mathbb{K}[x_1, \ldots, x_n]$. consideramos el conjunto $I = \cup_{n \geq 1} I_n$ que resulta ser un ideal:

- $0 \in I_1 \subset I$.
- I es cerrado para la suma: dados $f, g \in \cup_{n \geq 1} I_n$, de la condición de cadena se tiene que existe un $n_0 \geq 1$ tal que $f, g \in I_{n_0}$. Entonces $f + g \in I_{n_0} \subset I$.
- I es cerrado para la multiplicación por un polinomio arbitrio: dados $f \in \cup_{n \geq 1} I_n$ y $r \in \mathbb{K}[x_1, \ldots, x_n]$ se tiene que existe un $n_0 \geq 1$ tal que $f \in I_{n_0}$. Por lo tanto $rf \in I_{n_0} \subset I$.

Por el teorema 2.1.4 sabemos que existen $f_1, \ldots f_s \in \mathbb{K}[x_1, \ldots, x_n]$ tales que $I = \langle f_1, \ldots f_s \rangle$. En particular se tiene que $f_1, \ldots f_s \in I$, por lo tanto de la condición de cadena se deduce que existe $N \geq 1$ tal que $f_1, \ldots f_s \in I_N$. En consecuencia $I = \langle f_1, \ldots f_s \rangle \subset I_N \subset I_{N+k} \subset I$ para cada $k \geq 0$ y por tanto $I_N = I_{N+k} = I$ para cada $k \geq 0$.

□

Introducimos los *ideales cero dimensionales*, los cuales son una clase especial de ideales de polinomios que van a intervenir en el capítulo 3.

Definición 2.1.3. Se dice que un ideal de polinomios $I \subset \mathbb{K}[x_1, \ldots, x_n]$ es cero dimensional si el conjunto $V(I)$ es finito.

Mediante la correspondencia entre ideales y variedades afines que hemos detallado, notamos que esta definición concuerda con la idea intuitiva de dimensión de una variedad. Es decir, una curva es una variedad de dimensión 1, una superficie es una variedad de dimensión 2 y un conjunto finito de puntos es una variedad de dimensión 0. La definición rigurosa de dimensión de una variedad hace uso de la *dimensión de Krull* del anillo de coordenadas de la variedad. En este trabajo solo analizaremos los ideales cero dimensionales y estudiaremos algunas de sus caracterizaciones.

2.2. Bases de Gröbner

Dado un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ y un polinomio f arbitrario resulta natural plantearse si f pertenece al ideal I. En dimensión 1 conocemos una caracterización sencilla de la relación de pertenencia a un ideal. Esta viene dada por el algoritmo de división euclídea de la siguiente manera. En primer lugar ideal I será de la forma $I = \langle p \rangle$ para algún polinomio $p \in \mathbb{K}[x]$ pues todo ideal es principal en $\mathbb{K}[x]$.

El algoritmo de división euclídea permite expresar f de manera única de la siguiente forma: $f = q \cdot p + r$ donde $deg(r) < deg(p)$. Utilizamos la notación deg para denotar el grado de un polinomio $p(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{K}[x]$: $deg(p) = min\{k \geq 0 : \ a_k \neq 0\}$.

En estas condiciones $p \in I$ si y solo si $r = 0$.

La situación cambia cuando tratamos con polinomios en $\mathbb{K}[x_1, \ldots, x_n]$ para $n > 1$. Ya no es un *dominio de ideales principales* y como veremos el teorema 2.1.4, solo podemos asegurar que un ideal este generado por un número finito de polinomios. Es decir, dado un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ existen $p_1, \ldots, p_s \in \mathbb{K}[x_1, \ldots, x_n]$ tales que $I = \langle p_1, \ldots, p_s \rangle$.

Para tratar de resolver el problema de pertenencia a un ideal podemos tratar de generalizar el algoritmo de división euclídea para $n > 1$ y permitiendo dividir entre un conjunto ordenado de polinomios en vez de entre solo un polinomio. Para ello debemos definir primero la noción de *orden monomial* que nos va permitir comparar los monomios que componen un polinomio y definir el *multigrado* y el *monomio principal* del polinomio. El papel del multigrado va a ser el que tiene el grado en la división euclídea.

2.2.1. Órdenes monomiales y algoritmo de división

Definición 2.2.1. Un orden monomial $<$ sobre $\mathbb{K}[x_1, \ldots, x_n]$ es una relación sobre el conjunto de monomios $\mathcal{M}_{\mathbb{K}}(n) = \{\mathbf{x}^\alpha \ : \ \alpha \in \mathbb{Z}^n_{\geq 0}\}$ que satisface:

1. $<$ es un orden total en $\mathcal{M}_{\mathbb{K}}(n)$.

2. Si $\mathbf{x}^\alpha < \mathbf{x}^\beta$ y $\mathbf{x}^\gamma \in \mathcal{M}_{\mathbb{K}}(n)$ entonces $\mathbf{x}^{\alpha+\gamma} < \mathbf{x}^{\beta+\gamma}$.

3. El orden $<$ es un buen orden; es decir, todo subconjunto no vacío de $\mathcal{M}_{\mathbb{K}}(n)$ tiene un elemento mínimo para $<$.

Ejemplo 2. A continuación presentamos tres ejemplos para ilustrar esta definición. Estos órdenes monomiales son los más habituales en aplicaciones prácticas:

- El orden lexicográfico: Decimos que $\mathbf{x}^\alpha <_{lex} \mathbf{x}^\beta$ con $\alpha = (a_1, \ldots, a_n)$ y $\beta = (b_1, \ldots, b_n)$ si el primer dígito i_0 (empezando por la izquierda) para el cual $a_{i_0} \neq b_{i_0}$ satisface $a_{i_0} < b_{i_0}$.

  Por ejemplo, $x^2y^2z^4t <_{lex} x^2y^3z^2t$ pues con la notación anterior se tiene que $\alpha = (2, 2, 4, 1)$ y $\beta = (2, 3, 2, 1)$ y la primera coordenada empezando por la izquierda en la cual difieren α y β (la segunda) es mayor la componente de β.

- El orden lexicográfico graduado: Decimos que $\mathbf{x}^\alpha <_{glex} \mathbf{x}^\beta$ con $\alpha = (a_1, \ldots, a_n)$ y $\beta = (b_1, \ldots, b_n)$ si $deg(\mathbf{x}^\alpha) = \sum_{i=1}^n a_i < \sum_{i=1}^n b_i = deg(\mathbf{x}^\beta)$, o bien $deg(\mathbf{x}^\alpha) = deg(\mathbf{x}^\beta)$ y $\mathbf{x}^\alpha <_{lex} \mathbf{x}^\beta$.

  Por ejemplo, $x^2y^3z^2t <_{glex} x^2y^2z^4t$ pues $deg(x^2y^3z^2t) = 8 < 9 = deg(x^2y^2z^4t)$.

  $xy^3zt2 <_{glex} xy^3z^2t$ puesto que el grado de ambos monomios coincide y la primera empezando por la izquierda en la cual difieren α y β se tiene que la componente de β es mayor.

- El orden lexicográfico inverso graduado: Decimos que $\mathbf{x}^\alpha <_{grevlex} \mathbf{x}^\beta$ con $\alpha = (a_1, \ldots, a_n)$ y $\beta = (b_1, \ldots, b_n)$ si $deg(\mathbf{x}^\alpha) = \sum_{i=1}^n a_i < \sum_{i=1}^n b_i = deg(\mathbf{x}^\beta)$, o bien $deg(\mathbf{x}^\alpha) = deg(\mathbf{x}^\beta)$ y el primer dígito empezando por la derecha i_0 para el cual $a_{i_0} \neq b_{i_0}$ satisface $a_{i_0} > b_{i_0}$.

  Al igual que en el caso anterior $x^2y^3z^2t <_{grevlex} x^2y^2z^4t$ pues el grado del primer monomio es menor que el del segundo, $deg(x^2y^3z^2t) = 8 < 9 = deg(x^2y^2z^4t)$. $xy^3zt2 <_{grevlex} xy^3z^2t$ puesto que el grado de ambos monomios coincide y la primera empezando por la derecha en la cual difieren α y β se tiene que la componente de β es menor.

La prueba de que en efecto estos son órdenes monomiales se deduce del corolario 2.2.1 que desarrollaremos más adelante.

Un hecho importante que se debe destacar es que cada uno de estos tres órdenes monomiales satisface que $x_n < \cdots < x_2 < x_1$. Es posible definir los órdenes monomiales

anteriores para un orden diferente sobre las variables: por ejemplo se puede definir el orden lexicográfico de forma que se satisfaga $x_1 < x_3 < x_2$ en vez de $x_3 < x_2 < x_1$ como ocurre en la definición usual. Bajo este nuevo orden monomial $<_{lex'}$, se tiene que $\mathbf{x}^\alpha <_{lex'} \mathbf{x}^\beta$ con $\alpha = (a_1, a_2, a_3)$ y $\beta = (b_1, b_2, b_3)$ si al comparar las componentes de α y β empezando por la segunda, después la tercera componente y por último la primera, la primera vez que estas difieren, la componente de α correspondiente es menor que la de β. Por ejemplo, se tiene que $x_1^3 x_2 x_3^2 <_{lex'} x_1 x_2 x_3^3$.

Las definiciones de los órdenes lexicográfico graduado y lexicográfico inverso graduado se pueden modificar de forma similar. Si se utiliza alguno de estos órdenes se debe especificar el orden que se fija sobre las variables; en caso de no hacerlo, se entiende que $x_n < \cdots < x_2 < x_1$.

Definición 2.2.2. Sea $f = \sum_{\alpha \in \mathbb{Z}_{\geq}^n} a_\alpha \mathbf{x}^\alpha$ un polinomio no nulo de $\mathbb{K}[x_1, \ldots, x_n]$ y sea $<$ un orden monomial.

1. Se dice que multigrado(f)=máx $\big(\alpha \in \mathbb{Z}_{\geq}^n : \ a_\alpha \neq 0\big)$.

2. El coeficiente principal de f es $LC(f) = a_{multigrado(f)} \neq 0$.

3. El monomio principal de f es $LM(f) = x^{multigrado(f)}$.

4. El término principal de f es $LT(f) = a_{multigrado(f)} x^{multigrado(f)}$.

Definición 2.2.3. Sea I un ideal de $\mathbb{K}[x_1, \ldots, x_n]$ distinto de 0. Denotamos por $\langle LT(I) \rangle = \langle LT(f) \ : \ f \in I \rangle$ al ideal de los términos principales de I.

Teorema 2.2.1 (Algoritmo de División en $\mathbb{K}[x_1, \ldots, x_n]$)**.** *Sea $<$ un orden monomial en $\mathbb{K}[x_1, \ldots, x_n]$. Sea f un polinomio en $\mathbb{K}[x_1, \ldots, x_n]$ y $\{p_1, \ldots, p_s\}$ un conjunto ordenado de polinomios en $\mathbb{K}[x_1, \ldots, x_n]$. Entonces existen polinomios $q_1, \ldots, q_s, r$ tales que*

$$f = q_1 p_1 + \cdots + q_s p_s + r$$

donde o bien $r = 0$, o bien cada uno de los términos de r no es divisible entre ninguno de los términos principales de $p_1, \ldots, p_s$. Además se satisface que

$$\text{máx}\,(LM(q_i)LM(p_i) : \ 1 \leq i \leq s, \ q_i p_i \neq 0) \leq LM(f).$$

Demostración. Vamos a describir el algoritmo de división que proporciona los polinomios $q_1, \ldots, q_s, r$. La demostración de la propiedades que los caracterizan y la veracidad del algoritmo se pude encontrar en [5, Chap. 2.3, Thm. 3].

Algoritmo de división

INPUT: $p_1, \ldots, p_s, f$
OUTPUT: $q_1, \ldots, q_s, r$
$q_1 \leftarrow 0, \ldots, q_s \leftarrow 0; r \leftarrow 0$
$p \leftarrow f$
while $p \neq 0$ do
  $i \leftarrow 1$
  $division \leftarrow false$
  while $i \leq s$ AND $division = true$ **do**
    if $LT(p_i)$ divide a $LT(p)$ **then**
      $q_i \leftarrow q_i + \dfrac{LT(p)}{LT(p_i)}$
      $p \leftarrow p - \dfrac{LT(p)}{LT(p_i)} p_i$
      $division \leftarrow true$
    else
      $i \leftarrow i + 1$
    end if
    if $division = false$
      $r \leftarrow R + LT(p)$
      $p \leftarrow p - LT(p)$
    end if
  end while
end while

□

Observación 8. Dados $p_1, \ldots, p_s, f \in \mathbb{K}[x_1, \ldots, x_n]$, notamos que los polinomios $q_1, \ldots, q_s, r$ que devuelve el algoritmo tras efectuar la división de f entre $p_1, \ldots, p_s$ dependen del orden de $p_1, \ldots, p_s$.

Este algoritmo generaliza al algoritmo de división euclídea en $\mathbb{K}[x]$; sin embargo, no se comporta tan bien como esperaríamos y no resuelve completamente el problema de pertenencia a un ideal. Dado un polinomio f y un ideal I generado por los polinomios $p_1, \ldots, p_s$, es claro que si tras efectuar el algoritmo de división de f entre $\{p_1, \ldots, p_s\}$ se obtiene un resto nulo, f pertenece a I. En cambio puede darse que $f \in I$ y $r \neq 0$ como vemos en el siguiente ejemplo.

Ejemplo 3. Dado el ideal $I = \langle x^2yz + z^3, xy^2z^2 + xz \rangle \subset \mathbb{C}[x, y, z]$ y el polinomio $f = x^3yz^2 - x^2y^3z^2 - x^2z + xy^3z^2 - xy^2z^2 + xyz + xz^4 - xz - y^2z^4 + yz^4$, y nos planteamos si f pertenece a I. Empleando el orden lexicográfico dividimos f entre el par ordenado

$(x^2yz + z^3, xy^2z^2 + xz)$ que genera el ideal empleando el algoritmo de división. Este nos proporciona la siguiente expresión de f como combinación lineal de los generadores más un resto, en este caso $-x^2z + yz^4$.

$$f = (xz - y^2z) \cdot (x^2yz + z^3) + (y - 1) \cdot (xy^2z^2 + xz) + (-x^2z + yz^4) \tag{2.1}$$

Este resto, que es distinto de 0, está caracterizado de forma que cada uno de sus monomios no es divisible entre ninguno de los monomios principales de los generadores. Sin embargo, $-x^2z+yz^4 \in I$ ya que $(-x^2z+yz^4) = yz(x^2yz+z^3)-x(xy^2z^2+xz)$, por lo que $f \in I$. En este caso no se tiene la equivalencia que existe en $\mathbb{K}[x]$ entre pertenencia de un polinomio a I y que el algoritmo de división proporcione resto 0. Esto ocurre porque se tiene $\langle LT(x^2yz + z^3), LT(xy^2z^2 + xz)\rangle \subsetneq \langle LT(I)\rangle$.

La idea fundamental de las bases de Gröbner es buscar un conjunto de generadores adecuado par a I en el sentido que permitan caracterizar la pertenencia al ideal a través del resto del algoritmo de división evitando situaciones como la expuesta en el ejemplo anterior.

2.2.2. Ideales monomiales

Vamos a introducir los *ideales monomiales* los cuales juegan un papel fundamental en el estudio de las bases de Gröbner.

Definición 2.2.4. Se dice que un ideal de polinomios $I \subset \mathbb{K}[x_1, \ldots, x_n]$ es un ideal monomial si existe un conjunto $A \subset \mathbb{Z}^n_{\geq 0}$ tal que $I = \langle \mathbf{x}^\alpha : \alpha \in A\rangle$.

En la definición anterior el conjunto A puede ser infinito.

Lema 2.2.2. *Sea $I = \langle \boldsymbol{x}^\alpha : \alpha \in A\rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal monomial. Entonces se tiene que un monomio $\boldsymbol{x}^\beta \in \mathbb{K}[x_1, \ldots, x_n]$ pertenece a I si y solo si $\boldsymbol{x}^\beta$ es divisible entre $\boldsymbol{x}^{\alpha_0}$ para algún $\alpha_0 \in A$.*

Demostración. $\Leftarrow$. Es trivial.

$\Rightarrow$. Si $\mathbf{x}^\beta \in I$ existen $\alpha_1, \ldots \alpha_r \in A$ y $h_{\alpha_1}, \ldots h_{\alpha_r} \in \mathbb{K}[x_1, \ldots, x_n]$ tales que $\mathbf{x}^\beta \in I = \sum_{i=1}^r h_{\alpha_i}\mathbf{x}^{\alpha_i}$. Para cada índice $1 \leq i \leq r$ se tiene que cada término del producto $h_{\alpha_i}\mathbf{x}^{\alpha_i}$ es divisible entre $\mathbf{x}^{\alpha_i}$. $\mathbf{x}^\beta$ debe ser igual a alguno de estos términos y por lo tano debe ser divisible entre algún $\mathbf{x}^{\alpha_i}$.

□

Lema 2.2.3. *Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal monomial. Sea $f \in \mathbb{K}[x_1, \ldots, x_n]$. Entonces son equivalentes las siguientes afirmaciones:*

1. $f \in I$.

2. *Cada término de* f *pertenece a* I.

3. f *es* $\mathbb{K}$*-combinación lineal de monomios en* I.

Demostración. Claramente se tienen las implicaciones $3 \Rightarrow 2 \Rightarrow 1$ de la definición de ideal.

$1 \Rightarrow 3$. Si $f \in I$. Entonces f se escribe $f = \sum_{i=1}^{r} h_{\alpha_i} \mathbf{x}^{\alpha_i}$ para ciertos $\alpha_1, \dots \alpha_r \in A$ y $h_{\alpha_1}, \dots h_{\alpha_r} \in \mathbb{K}[x_1, \dots, x_n]$. Desarrollando los productos $h_{\alpha_i} \mathbf{x}^{\alpha_i}$ notamos que cada uno de los monomios que intervienen es múltiplo de $\mathbf{x}^{\alpha_i}$ y por lo tanto pertenece a I por el lema previo. En consecuencia f se escribe como $\mathbb{K}$-combinación lineal de monomios en I.

□

Este resultado implica que un ideal monomial está caracterizado por sus monomios; es decir, si dos ideales monomiales, I, I', contienen los mismos monomios entonces son iguales: $f \in I$ si y solo si f es $\mathbb{K}$-combinación lineal de monomios en I, por lo tanto $f \in I$ si y solo si f es $\mathbb{K}$-combinación lineal de monomios en I'. Esto es equivalente a que $f \in I'$.

Teorema 2.2.4 (Lema de Dickson)**.** *Sea* $I = \langle \boldsymbol{x}^{\alpha} : \alpha \in A \rangle \subset \mathbb{K}[x_1, \dots, x_n]$ *un ideal monomial. Entonces existen* $\alpha_1 \dots \alpha_r \in A$ *tales que* $I = \langle \boldsymbol{x}^{\alpha_1}, \dots, \boldsymbol{x}^{\alpha_r} \rangle$.

Demostración. La demostración del teorema se encuentra en [5, Chap. 2.4, Thm. 5].

□

Corolario 2.2.1. *Sea* $<$ *una relación en el conjunto de monomios* $\mathcal{M}_{\mathbb{K}}(n)$ *que satisface:*

1. $<$ *es un orden total en* $\mathcal{M}_{\mathbb{K}}(n)$.

2. *Si* $\boldsymbol{x}^{\alpha} < \boldsymbol{x}^{\beta}$ *y* $\boldsymbol{x}^{\gamma} \in \mathcal{M}_{\mathbb{K}}(n)$ *entonces* $\boldsymbol{x}^{\alpha+\gamma} < \boldsymbol{x}^{\beta+\gamma}$.

Entonces $<$ *es un buen orden si y solo si* $1 \leq \boldsymbol{x}^{\alpha}$ *para cada* $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Demostración. La demostración del corolario se puede encontrar en [5, Chap. 2.4, Cor. 6].

□

Este resultado proporciona una caracterización simple de un orden monomial. Podemos aplicarlo para comprobar que los tres ejemplos de órdenes monomiales expuestos (Ej.2) lo son efectivamente.

2.2.3. Definición de base de Gröbner

Definición 2.2.5. Sean $<$ un orden monomial sobre $\mathbb{K}[x_1, \ldots, x_n]$ y un ideal I. Se dice que con conjunto finito $\mathcal{G} = \{g_1, \ldots, g_s\} \subset I$ es una base de Gröbner de I si

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

Se dice que un conjunto $\mathcal{G} = \{g_1, \ldots, g_s\} \subset \mathbb{K}[x_1, \ldots, x_n]$ es una base de Gröbner si G es una base de Gröbner del ideal $\langle g_1, \ldots, g_s\rangle$.

Como hemos notado en el ejemplo 2.1 los polinomios $\{x^2y, xy^2 + x\}$ no forman una base de Gröbner con el orden lexicográfico para el ideal que generan.

Teorema 2.2.5 (Base de Gröbner)**.** *Fijado un orden monomial $<$ en $\mathbb{K}[x_1, \ldots, x_n]$ todo ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ no nulo posee una base de Gröbner. Además toda base de Gröbner de un ideal I genera I.*

Demostración. Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal. En primer lugar probamos la existencia de una base de Gröbner de I. Observamos que el ideal $\langle LT(I)\rangle$ coincide con el ideal $\langle LM(f) : \ f \in I\rangle$: cada uno de los generadores de $\langle LT(I)\rangle$ es de la forma $LT(h) = LC(h) \cdot LM(h)$ para un cierto $h \in I$, luego pertenece a $\langle LM(f) : \ f \in I\rangle$ lo que implica $\langle LT(I)\rangle \subset \langle LM(f) : \ f \in I\rangle$. La otra contención se deduce de forma similar notando que cada generador de $\langle LM(f) : \ f \in I\rangle$ es de la forma $LM(h) = \frac{1}{LC(h)} \cdot LT(h)$ para un cierto $h \in I \setminus \{0\}$ y por lo tanto es múltiplo de un generador de $\langle LT(I)\rangle$.

El ideal $\langle LM(f) : \ f \in I\rangle$ es monomial luego por el lema de Dickson (teorema 2.2.4) existen $g_1, \ldots, g_s \in I$ tales que $\langle LM(f) : \ f \in I\rangle = \langle LM(g_1), \ldots LM(g_s)\rangle$. Este último ideal es igual a $\langle LT(g_1), \ldots LT(g_s)\rangle$ por un razonamiento análogo al dado en la prueba de que $\langle LT(I)\rangle = \langle LM(f) : \ f \in I\rangle$. Por lo tanto, se concluye que $\langle LT(I)\rangle = \langle LT(g_1), \ldots LT(g_s)\rangle$.

Vamos a probar que si $\mathcal{G} = \{g_1, \ldots, g_s\}$ es una base de Gröbner de I, entonces $I = \langle g_1, \ldots, g_s\rangle$. Dado que $\mathcal{G} \subset I$, se tiene que $\langle g_1, \ldots, g_s\rangle \subset I$. Para probar la otra inclusión tomamos $f \in I$. Mediante el algoritmo de división en $\mathbb{K}[x_1, \ldots, x_n]$ podemos encontrar $p_1, \ldots, p_s, r \in \mathbb{K}[x_1, \ldots, x_n]$ tales que f se escribe de la siguiente forma:

$$f = p_1g_1 + \cdots + p_sg_s + r$$

donde o bien r es nulo, o bien satisface que ninguno de sus términos no es divisible entre ninguno de los términos principales de $g_1, \ldots, g_s$.

Supongamos que $r \neq 0$. Se tiene que $r = f - p_1g_1 + \cdots p_rg_s \in I$ y por lo tanto $LT(r) \in \langle LT(I)\rangle = \langle LM(g_1), \ldots LM(g_s)\rangle$ y en consecuencia $LM(r) \in \langle LM(g_1), \ldots LM(g_s)\rangle$. Por el lema 2.2.2 se deduce que existe un índice $1 \leq i \leq s$ tal que $LM(g_i)$ divide a $LM(r)$.

Para este índice se tiene que $LT(g_i)$ divide a $LT(r)$ lo cual es absurdo. Se concluye que $r = 0$ y por tanto $f \in \langle g_1, \ldots, g_s \rangle$.

□

A continuación presentamos la demostración del teorema de la base de Hilbert (teorema 2.1.4), como consecuencia del resultado precedente.

Demostración del teorema 2.1.4. Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal. Fijamos un orden monomial arbitrario en $\mathbb{K}[x_1, \ldots, x_n]$. Por el teorema 2.2.5 sabemos que existe una base de Gröbner de I, $\mathcal{G} = \{p_1, \ldots, p_s\}$ y que $I = \langle p_1, \ldots, p_s \rangle$.

□

Teorema 2.2.6. *Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal y sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ una base de Gröbner para un orden monomial $<$ fijado.*

Sea $f \in \mathbb{K}[x_1, \ldots, x_n]$. Entonces existe un único $r \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $f = p + r$ con $p \in I$ y que satisface que o bien $r = 0$, o bien ningún término de r es divisible entre ninguno de los $LT(g_1), \ldots, LT(g_s)$. Además p se escribe como una combinación lineal de la forma $p = p_1 g_1 + \cdots + p_s g_s$ donde los polinomios p_i satisfacen que

$$\text{máx}\,(LM(q_i)LM(p_i) : \ 1 \leq i \leq s, \ q_i p_i \neq 0) \leq LM(f).$$

Demostración. Sea $f \in \mathbb{K}[x_1, \ldots, x_n]$. Mediante el algoritmo de división en $\mathbb{K}[x_1, \ldots, x_n]$ podemos escribir f de la siguiente forma:

$$f = p_1 g_1 + \cdots + p_s g_s + r$$

para ciertos polinomios $p_1, \ldots p_s, r \in \mathbb{K}[x_1, \ldots, x_n]$, donde o bien $r = 0$, o bien ninguno de sus términos no es divisible entre ninguno de los términos principales de $g_1, \ldots, g_s$. Además se satisface que $\text{máx}\,(LM(q_i)LM(p_i) : \ 1 \leq i \leq s, \ q_i p_i \neq 0) \leq LM(f)$. Tomamos $p = p_1 g_1 + \cdots p_r g_s \in I$ y obtenemos la expresión buscada.

Para probar la unicidad de r razonamos por reducción al absurdo. Suponemos que existen $r, r' \in \mathbb{K}[x_1, \ldots, x_n]$ distintos que satisfacen la condición enunciada para ciertos polinomios $p, p' \in I$ respectivamente. Se tiene que $r - r' = p' - p \in I$. El polinomio $r - r'$ es no nulo por lo tanto $a\mathbf{x}^\alpha = LT(r - r') \in \langle LT(I) \rangle = \langle g_1, \ldots, g_s \rangle$. Mediante un argumento similar al dado en la prueba de 2.2.5 podemos deducir que existe un índice $1 \leq i \leq s$ tal que $LT(g_i)$ divide a $\mathbf{x}^\alpha$. El monomio $\mathbf{x}^\alpha$ aparece en alguno de los términos de r o de r' y por lo tanto este término es divisible entre $LT(g_i)$ lo que contradice la definición de r y r'.

□

Una consecuencia de este teorema es que el resto, r, proporcionado por el algoritmo de división tras efectuar la división de un polinomio f entre una base de Gröbner $\mathcal{G}$, no depende del orden escogido de los elementos de G. En este caso se habla de *forma*

normal de f y se denota $\overline{f}^{\mathcal{G}} = r$. La forma normal de un polinomio f respecto de una base de Gröbner de un ideal I da solución al problema de pertenencia al ideal.

Corolario 2.2.2. *Sea* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *un ideal y sea* $\mathcal{G} = \{g_1, \ldots, g_s\}$ *una base de Gröbner para un orden monomial* $<$ *fijado. Un polinomio* $f \in \mathbb{K}[x_1, \ldots, x_n]$ *pertenece a* I *si y solo si el resto de la división de* f *entre* $\mathcal{G}$ *es* 0*. Es decir,* $f \in I$ *si y solo si* $\overline{f}^{\mathcal{G}} = 0$*.*

Demostración. Si el resto de la división de f entre $\mathcal{G}$ entonces f se escribe como combinación lineal de $g_1, \ldots, g_s$ que son elemento de I, luego f pertenece a I.

Recíprocamente, si $f \in I$ entonces la expresión $f = f + r$ con $r = 0$ es de la forma descrita en 2.2.6 y puesto que el resto de la división de f entre G es único se deduce que el resto es 0.

□

Definición 2.2.6.

1. Sean $\mathbf{x}^\alpha, \mathbf{x}^\beta \in \mathcal{M}_{\mathbb{K}}(n)$. El mínimo común múltiplo de $\mathbf{x}^\alpha$ y $\mathbf{x}^\beta$ es $mcm(\mathbf{x}^\alpha, \mathbf{x}^\beta) = \mathbf{x}^\gamma$ donde $\gamma_i = \max(\alpha_i, \beta_i)$ para cada índice $1 \leq i \leq n$.
2. Sean $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ polinomios no nulos. Sea $L = mcm(LM(f), LM(g))$. Denominamos el S-polinomio de f y g al polinomio

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

Proposición 2.2.1 (Criterio de Buchberger)**.** *Sea* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *un ideal y sea* $\mathcal{G} = \{g_1, \ldots g_s\}$ *una base de* I*. Entonces* $\mathcal{G}$ *es una base de Gröbner de* I *si y solo si para cada par* $i \neq j$ *existe un orden de los polinomios de* $\mathcal{G}$ *para el cuales se tiene que el resto de la división de* $S(g_i, g_j)$ *entre el conjunto ordenado* $\mathcal{G}$ *es* 0*.*

Demostración. La demostración se encuentra en [5, Chap 2.6, Thm. 6].

□

Proposición 2.2.2. *Sean* $g_1, \ldots g_s \in \mathbb{K}[x_1, \ldots, x_n]$ *tales que sus monomios principales son primos entre si dos a dos; es decir,* $L = mcm(LM(g_i), LM(g_j)) = LM(g_i) \cdot LM(g_j)$ *si* $i \neq j$*. Entonces se tiene que* $\mathcal{G} = \{g_1, \ldots g_s\}$ *es una base de Gröbner.*

Demostración. La demostración se deduce de la proposición [5, Prop.2.9.4] y del teorema [5, Chap 2.9, Thm. 3].

□

En particular, si $f_1, \ldots f_s \in \mathbb{K}[x_1, \ldots, x_n]$ satisfacen que para cada par de estos polinomios sus monomios principales son primos entre sí y sus coeficientes principales son 1, entonces $\{f_1, \ldots f_s\}$ es una base de Gröbner minimal.

2.2.4. Bases de Gröbner minimales y reducidas

En esta sección supondremos fijado un orden monomial $<$ en $\mathbb{K}[x_1, \ldots, x_n]$.

Definición 2.2.7. Una base de Gröbner $G = \{g_1, \ldots, g_s\}$ se dice que es minimal si se cumple:

1. $LC(g_i) = 1$ para cada i.
2. Para cada par de índices $i \neq j$, $LT(g_i)$ no divide a $LT(g_j)$.

Lema 2.2.7. *Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ una base de Gröbner para un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Si existen $i \neq j$ tales que $LT(g_i)$ divide a $LT(g_j)$, se tiene que $\mathcal{G} \setminus \{g_j\}$ es una base de Gröbner de I.*

Demostración. Sea $f \in I$, entonces existe $1 \leq i_0 \leq n$ tal que $LT(g_{i_0})$ divide a $LT(f)$. Si $i_0 \neq j$ entonces $g_{i_0} \in G \setminus \{g_j\}$ y por tanto $LT(f) \in \langle LT(g_1), \ldots\ LT(g_{j-1}), LT(g_{j+1}), \ldots, LT(g_s)\rangle$. Si $i_0 = j$, entonces se tiene que $LT(g_i)$ divide a $LT(f)$ y por tanto también se cumple que $LT(f) \in \langle LT(g_1), \ldots\ LT(g_{j-1}), LT(g_{j+1}), \ldots, LT(g_s)\rangle$.

□

Este lema asegura la existencia de las bases de Gröbner minimales de un ideal no nulo y nos proporciona una forma de obtener una base de Gröbner minimal de un ideal a partir de una base de Gröbner $\mathcal{G}$: podemos eliminar sucesivamente cada polinomio de $\mathcal{G}$ para el cual exista otro polinomio en la base cuyo término principal divida al término principal del primero. Sabemos que en cada uno de estos pasos el conjunto obtenido tras eliminar cada uno de estos polinomios sigue siendo una base de Gröbner del ideal I. Tras realizar esta operación un número finito de veces obtenemos un conjunto $\tilde{\mathcal{G}}$ que es una base de Gröbner de I y además satisface la segunda condición de la definición 2.2.7. Por último dividiendo cada uno de los polinomios de $\tilde{\mathcal{G}}$ entre su respectivo coeficiente principal obtenemos una base de Gröbner minimal de I.

Proposición 2.2.3. *Sean $\mathcal{G} = \{g_1, \ldots, g_s\}$ y $\mathcal{F} = \{f_1, \ldots, f_t\}$ dos bases de Gröbner minimales de un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Entonces se tiene que $t = s$ y salvo reordenación de los elementos de $\mathcal{G}$ y $\mathcal{F}$ se satisface que $LT(g_i) = LT(f_i)$ para todo i, $1 \leq i \leq s$.*

Demostración. Vamos a probar de forma inductiva que se tiene que $LT(g_i) = LT(f_i)$ salvo reordenación de los polinomios de $\mathcal{F}$ para cada $1 \leq i \leq s$.

Dado que $g_1 \in I$, de la condición de base de Gröbner de $\mathcal{F}$ se deduce que existe i tal que $f_i \in \mathcal{F}$ cumple que $LT(f_i)$ divide a $LT(g_1)$. Tras reordenar los elementos de $\mathcal{F}$, podemos suponer que $i = 1$. Por otra parte, $f_1 \in I$. La condición de base de Gröbner de $\mathcal{G}$ implica que existe $g_j \in \mathcal{G}$ tal que $LT(g_j)$ divide a $LT(f_1)$. Entonces $LT(g_j)$ divide a $LT(g_1)$ y se deduce que $j = 1$ por ser $\mathcal{G}$ una base de Gröbner minimal. Dado que $LT(f_1)$ divide a $LT(g_1)$ y de igual manera $LT(g_1)$ divide $LT(f_1)$, se tiene que $LT(g_1) = LT(f_1)$.

Sea $r \leq s$ y supongamos que $LT(g_k) = LT(f_k)$ para cada $k = 1, \ldots, r-1$. Vamos a demostrar que $LT(g_r) = LT(f_r)$. Dado que $g_r \in I$ se tiene que existe i tal que $LT(f_i)$ divide a $LT(g_r)$. Podemos deducir que $i > r-1$ puesto que en caso contrario $LT(f_i) = LT(g_i)$ por hipótesis y se tendría que $LT(g_i)$ dividiría a $LT(g_r)$ en contra de la minimalidad de $\mathcal{G}$. Tras reordenar los polinomios de $\mathcal{F} \setminus \{f_1, \ldots, f_{r-1}\}$ podemos suponer que $i = r$. Entonces $f_r \in I$ lo que implica que existe $g_j \in \mathcal{G}$ tal que $LT(g_j)$ divide a $LT(f_r)$ por la condición de base de Gröbner de $\mathcal{G}$. De de la minimalidad de $\mathcal{G}$ y del hecho de que $LT(g_j)$ divide a $LT(g_r)$ se deduce que $g_j = g_r$ y que por tanto $LT(g_j) = LT(f_j)$.

Hemos probado que $s \leq t$, para demostrar que se tiene la igualdad razonamos por reducción al absurdo: supongamos que $s < t$, entonces se tiene que $f_{s+1} \in I$ y por lo tanto $LT(f_{s+1}) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$ puesto $\mathcal{G}$ es una base de Gröbner de I. Además se tiene que $LT(g_i) = LT(f_i)$ para cada $i = 1, \ldots, s$ por lo que $LT(f_{s+1}) \in \langle LT(f_1), \ldots, LT(f_s) \rangle$. Por lo tanto existe $1 \leq i \leq s$ tal que $LT(f_i)$ divide a $LT(f_{s+1})$ lo que contradice el hecho de que $\mathcal{F}$ es base de Gröbner minimal.

□

Las bases de Gröbner minimales de un ideal no son únicas. Para obtener un resultado de unicidad debemos imponer condiciones más fuertes en la base de Gröbner.

Definición 2.2.8. Se dice que una base de Gröbner $\mathcal{G}$ para un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ es una base de Gröbner reducida si se cumple que:

1. $LC(g) = 1$ para cada $g \in \mathcal{G}$.
2. Para cada $g \in \mathcal{G}$, ningún término de g pertenece a $\langle LT(\mathcal{G} \setminus \{g\}) \rangle$.

Podemos notar que toda base de Gröbner reducida es una base de Gröbner minimal.

Teorema 2.2.8. *Dado un ideal $I \neq 0$ existe una única base de Gröbner reducida para cada orden monomial.*

Demostración. Fijamos un orden monomial $<$. Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal distinto de 0. Vamos a dar un método para construir una base de Gröbner reducida de I a partir de una base de Gröbner minimal de I, $\mathcal{G} = \{g_1, \ldots g_s\}$:

- Tomamos g_1 y aplicamos el algoritmos de división entre $H_1 = \{g_2, \ldots, g_s\}$, obteniendo como resto h_1 que es no nulo. Notamos que $LT(h_1) = LT(g_1)$ por lo que $H_1 \cup \{h_1\}$ sigue siendo una base de Gröbner minimal de I. Por la caracterización del resto del algoritmo división se tiene que ningún término de h_1 es divisible entre ninguno de los términos principales de los polinomios de H_1; es decir, ningún término de h_1 pertenece a $\langle LT(\mathcal{G} \setminus \{g_1\}) \rangle$.

- Realizamos ahora un procedimiento similar con el polinomio g_2. Dividimos g_2 entre $H_2 = \{h_1, g_3, \ldots, g_s\}$ aplicando el algoritmos de división y obtenemos como resto el polinomio h_2. Se satisface que h_2 es distinto de 0 y $LT(h_2) = LT(g_2)$ lo que implica que $H_2 \cup \{h_2\}$ es unas base de Gröbner minimal de I. Además, h_2 cumple que ninguno de sus términos pertenece a $\langle LT(H_2)\rangle = \langle LT(\mathcal{G} \setminus \{g_2\})\rangle$.

- Procedemos de esta forma reduciendo cada uno de los polinomios de $g_i \in \mathcal{G}$. En el m-esimo paso dividimos g_m entre $H_n = \{h_1, h_2, \ldots, h_{m-1}, g_{m+1}, \ldots, g_s\}$ aplicando el algoritmo de división y obteniendo el resto no nulo h_m. Este polinomio satisface que $LT(h_m) = LT(g_m)$ y además ninguno de sus términos pertenece a $\langle LT(H_m)\rangle = \langle LT(\mathcal{G} \setminus \{g_m\})\rangle$.

Tras llevar a cabo este procedimiento se obtiene un conjunto $H = \{h_1, \ldots, h_s\}$ de polinomios tales que $LT(h_i) = LT(g_i)$ para cada $i = 1, \ldots, s$. Por lo tanto, H es una base de Gröbner minimal de I, dado que $\langle LT(h_1), \ldots LT(h_s)\rangle = \langle LT(g_1), \ldots LT(g_s)\rangle = \langle LT(I)\rangle$, $LC(h_i) = LC(g_i) = 1$ y además $LT(h_i) = LT(g_i) \notin \langle LT(G \setminus \{g_i\})\rangle = \langle LT(H \setminus \{h_i\})\rangle$ para cada $i = 1, \ldots, s$.

Para ver que H es una base de Gröbner reducida, basta notar que dado $h_i \in H$ cada uno de sus términos no es divisible entre ninguno de los términos principales de los polinomios de $H_i = \{h_1, \ldots, h_{i-1}, g_{i+1}, \ldots, g_s\}$. El hecho de que los términos principales de los polinomios g_j y h_j coincidan para todo j implica que ninguno de los términos de h_i pertenece a $\langle LT(\mathcal{G} \setminus \{g_i\})\rangle$.

Vamos a probar ahora la unicidad de las bases de Gröbner reducidas. Sean $\mathcal{G} = \{g_1, \ldots, g_s\}$ y $\mathcal{H} = \{h_1, \ldots, h_s\}$ dos bases de Gröbner reducidas de un ideal no nulo I. Por la proposición 2.2.3 sabemos que ambas deben tener el mismo número de elementos y que $LT(g_i) = LT(h_i)$ para cada i puesto que $\mathcal{G}$ y $\mathcal{H}$ son bases de Gröbner minimales. Sea $1 \leq i \leq s$. Si $g_i \neq h_i$ se tiene que $g_i - h_i \in I$ y por la condición de base de Gröbner de $\mathcal{H}$ deducimos que existe $h_j \in H$ tal que $LT(h_j)$ divide a $LT(g_i - h_i)$. Dado que $LT(g_i) = LT(h_i)$ se tiene que $LM(g_i - h_i) < LM(h_i)$ y por lo tanto se tiene que $j \neq i$. Notamos que $LM(g_i - h_i)$ es uno de los monomios que aparecen en g_i o en h_i. Por lo tanto, $LT(h_j)$ divide a uno de los términos de h_i o $LT(g_j)$ divide a uno de los términos de g_i, lo que en ambos casos contradice el hecho de que $\mathcal{G}$ y $\mathcal{H}$ son bases de Gröbner reducidas.

□

Una consecuencia directa de este teorema, es que podemos caracterizar la igualdad de ideales a través de las bases de Gröbner reducidas: dos ideales $I, J \subset \mathbb{K}[x_1, \ldots, x_n]$ son iguales si y solo si sus bases de Gröbner reducidas son iguales. Es claro, que si las bases de Gröbner reducidas de I y J, $\mathcal{G}_I$ y $\mathcal{G}_J$ respectivamente, coinciden, entonces se da la igualdad de ideales. Esto ocurre porque en particular $\mathcal{G}_I$ y $\mathcal{G}_J$ generan los ideales i y J respectivamente. Recíprocamente, si se tiene que $I = J$, entonces se deduce que ambos tienen la misma base de Gröbner reducida que es única como se ha probado en el teorema 2.2.8.

Lema 2.2.9. *La base de Gröbner reducida de* $\mathbb{K}[x_1, \ldots, x_n]$ *para cualquier orden monomial es* $\mathcal{G} = \{1\}$.

Demostración. Se tiene que $\mathcal{G} = \{1\}$ es una base de Gröbner de $\mathbb{K}[x_1, \ldots, x_n]$ para cualquier orden monomial porque

$$\langle LT(\mathbb{K}[x_1, \ldots, x_n])\rangle = \langle \mathcal{M}_{\mathbb{K}}(n)\rangle = \mathbb{K}[x_1, \ldots, x_n] = \langle 1\rangle.$$

El resto de condiciones necesarias para se la base de Gröbner reducida de $\mathbb{K}[x_1, \ldots, x_n]$ se satisfacen de forma trivial.

□

El *Algoritmo de Buchberger* proporciona un método para calcular una base de Gröbner de un ideal no nulo a partir de un conjunto de generadores, de la cual se puede extraer una base de Gröbner minimal y a partir de ella se puede obtener la base de Gröbner reducida del ideal. Este algoritmo está implementado en numerosos programas de computación y se ha desarrollado avances que mejoran su rendimiento.

2.2.5. Bases de Gröbner universales

Evidentemente una base de Gröbner de un ideal I para un orden monomial $<$ no tiene por que ser una base de Gröbner para otro orden monomial $<'$. Cada orden monomial puede presentar ciertas ventajas para resolver algún problema particular o por motivos computacionales. Es un hecho que desde un punto de vista de complejidad computacional el orden lexicográfico inverso graduado es la mejor alternativa para calcular una base de Gröbner de un ideal. Por el contrario, obtener una base de Gröbner de un ideal para el orden lexicográfico resulta muy costoso computacionalmente, produce polinomios con órdenes muy elevados y coeficientes muy grandes en general.

Sin embargo, hay ciertas bases de Gröbner que lo son para cada orden monomial en $\mathbb{K}[x_1, \ldots, x_n]$. Este tipo de base se denomina *base de Gröbner universal*. A continuación se prueban una serie de resultados con el fin de demostrar que todo ideal no nulo admite una base de Gröbner universal. Además se prueba que el número de bases de Gröbner reducidas de un ideal no nulo es finito.

Definición 2.2.9. Sea I un ideal de $\mathbb{K}[x_1, \ldots, x_n]$ no nulo. Se definen los siguientes conjuntos:

1. El conjunto de todos los órdenes monomiales en $\mathcal{M}^n_{\mathbb{K}}$,
   $\mathcal{T} = \{<: <$ es un orden monomial$\}$.

2. El conjunto de base de Gröbner reducidas de I,
   $\mathcal{R} = \{\mathcal{G}_< \ : \ \mathcal{G}_<$ es base de Gröbner reducida para un orden monomial $< \in \mathcal{T}\}$.

3. El conjunto de ideales de términos principales de I,
   $\mathcal{L} = \{\langle LT_< (I)\rangle : <$ es orden monomial$\}$.

Lema 2.2.10. *Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ una base de Gröbner para un orden monomial $<_1$ en $\mathcal{M}_{\mathbb{K}}(n)$. Sea $<_2$ otro orden monomial tal que $LT_{<_1}(g_i) = LT_{<_2}(g_i)$. Entonces $\mathcal{G}$ es una base de Gröbner para el orden $<_2$.*

Demostración. Sea $I = \langle g_1, \ldots, g_s \rangle$. Hay que probar que

$$\langle LT_{<_2}(I) \rangle \subset \langle LT_{<_2}(g_1), \ldots, LT_{<_2}(g_s) \rangle.$$

Sea $f \in I$. Supongamos que $LT_{<_2}(f)$ no pertenece al ideal $\langle LT_{<_2}(g_1), \ldots, LT_{<_2}(g_s) \rangle$. Aplicamos el algoritmo de división para dividir f entre $\mathcal{G}$ empleando el orden monomial $<_2$. Obtenemos la expresión:

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

Entonces, $LT_{<_2}(f)$ es uno de los términos de r que entonces es un polinomio no nulo. Por la caracterización del resto del algoritmo de división, se tiene que ninguno de los términos de r es divisible entre ninguno de los términos principales de los polinomios de $\mathcal{G}$. Pero $r = f - q_1 g_1 - \cdots q_s g_s \in I$ y por lo tanto $LT_{<_1}(r)$ es divisible entre algún $LT_{<_1}(g_i)$. Por hipótesis se tiene que $LT_{<_1}(g_i) = LT_{<_2}(g_i)$ y por tanto $LT_{<_2}(g_i)$ divide a $LT_{<_1}(r)$ lo cual es absurdo. En conclusión, $LT_{<_2}(f) \in \langle LT_{<_2}(g_1), \ldots, LT_{<_2}(g_s) \rangle$ y por lo tanto, $\mathcal{G}$ es una base de Gröbner de I para el orden $<_2$.

□

Proposición 2.2.4. *Existe una biyección entre $\mathcal{R}$ y $\mathcal{L}$.*

Demostración. Sea $\mathcal{G} \in \mathcal{R}$. Existe un orden monomial $<_0 \in \mathcal{T}$ tal que $\langle LT_{<_0}(\mathcal{G}) \rangle = \langle LT_{<_0}(I) \rangle$. Asociamos a $\mathcal{G}$ el ideal de términos principales $\langle LT_{<_0}(I) \rangle$.

Recíprocamente, sea $\langle LT_{<_0}(I) \rangle$ un ideal de términos principales de I para un cierto orden monomial $<_0$. Existe una única base de Gröbner reducida, $\mathcal{G}_{<_0}$ para I para este orden monomial. Debemos probar que si $<$ es otro orden monomial tal que $\langle LT_{<}(I) \rangle = \langle LT_{<_0}(I) \rangle$ entonces $\mathcal{G}_{<_0}$ es la base de Gröbner reducida de I para $<$.

Sea $\mathcal{G}_{<_0} = \{g_1, \ldots, g_s\}$ la única base de Gröbner de I asociada para el orden monomial $<_0$, vamos a ver que $LT_{<}(g_i) = LT_{<_0}(g_i)$ para cada $i = 1, \ldots, s$. Sea i fijado, $1 \leq i \leq s$. En primer lugar, notamos que $LT_{<}(g_i)$ es un término de g_i y por lo tanto de la condición de base de Gröbner reducida de $\mathcal{G}_{<_0}$ deducimos que $LT_{<}(g_i)$ no es divisible entre $LT_{<_0}(g_j)$ para ningún $i \neq j$. Supongamos que no se cumple que $LT_{<}(g_i) = LT_{<_0}(g_i)$. En este caso se tendría que $LM_{<}(g_i) <_0 LM_{<_0}(g_i)$. Supongamos que $LT_{<_0}(g_i)$ divide a $LT_{<}(g_i)$, entonces existe $\mathbf{x}^\gamma$ tal que $\mathbf{x}^\gamma LM_{<_0}(g_i) = LM_{<}(g_i)$ y en consecuencia se tiene:

$$LM_{<}(g_i) \leq \mathbf{x}^\gamma LM_{<}(g_i) < \mathbf{x}^\gamma LM_{<_0}(g_i) = LM_{<}(g_i)$$

lo cual es absurdo. Por lo tanto $LT_{<_0}(g_i)$ no divide a $LT_{<}(g_i)$. Sin embargo, se tiene que $LT_{<}(g_i) \in \langle LT_{<}(I) \rangle = \langle LT_{<_0}(I) \rangle$ lo que implica que existe algún $1 \leq j \leq s$

tal que $LT_{<_0}(g_j)$ divide a $LT_<(g_i)$ lo cual no ocurre. Por lo tanto, concluimos que $LT_<(g_i) = LT_{<_0}(g_i)$.

Este hecho implica que

$$\langle LT_<(g_1), \ldots, LT_<(g_s)\rangle = \langle LT_{<_0}(g_1), \ldots, LT_{<_0}(g_s)\rangle = \langle LT_{<_0}(I)\rangle = \langle LT_<(I)\rangle.$$

Es decir, $\mathcal{G}_{<_0}$ es una base Gröbner de I para el orden monomial $<$. Además se tiene que $LC_<(g_i) = LC_{<_0}(g_i) = 1$ y $LT_<(g_i) = LT_{<_0}(g_i) \notin \langle LT_{<_0}(G_{<_0} \setminus \{g_i\})\rangle = \langle LT_<(\mathcal{G}_{<_0} \setminus \{g_i\})\rangle$. Esto implica que $G_{<_0}$ es una base de Gröbner minimal de I para $<$. Para ver que además $\mathcal{G}_{<_0}$ es la base de Gröbner reducida de I para este orden monomial tomamos un término de g_i para un i fijado, $1 \leq i \leq s$ y comprobamos que no es divisible entre ninguno de los términos principales de los polinomios $\mathcal{G}_{<_0} \setminus \{g_i\}$ para el orden $<$. Efectivamente esto es consecuencia de la igualdad de los términos principales de los polinomios de la base para los dos órdenes monomiales y del hecho que $\mathcal{G}_{<_0}$ es una base de Gröbner reducida para el orden $<_0$.

□

Proposición 2.2.5. *El conjunto $\mathcal{L}$ es finito.*

Demostración. Razonamos por redución al absurdo y asumimos que $\mathcal{L}$ es infinito. Para cda ideal de términos principales de $\mathcal{L}$ escogemos un orden monomial de $\mathcal{T}$ y denotamos por $\mathcal{T}_0 \subset \mathcal{T}$ al conjunto de estos órdenes. Notamos que por hipótesis $\mathcal{T}_0$ es un conjunto infinito.

El teorema de la base de Hilbert asegura que $I = \langle f_1, \ldots, f_s\rangle$ para ciertos polinomios $f_1, \ldots, f_s \in I$. Dado que el número de términos que aparecen en los polinomios $f_1, \ldots, f_s$ es finito podemos encontrar un subconjunto infinito $\mathcal{T}_1 \subset \mathcal{T}_0$ y un conjunto de términos $m_1, \ldots, m_s$ tales que para cada $<\in \mathcal{T}_1$ se tiene que $LT_<(f_i) = m_i$ para cada $i = 1, \ldots s$.

- Caso 1: Si $\langle LT_{<_0}(m_1), \ldots, LT_{<_0}(m_s)\rangle = \langle LT_{<_0}(I)\rangle$ para algún $<_0\in \mathcal{T}_1$ entonces se deduce que $\{f_1, \ldots, f_s\}$ es una base de Gröbner de I para $<_0$ y en consecuencia es una base de Gröbner de I para cada orden monomial de $\mathcal{T}_1$ por el lema 2.2.10. Esto implica que el ideal de términos principales de I, $\langle LT_{<_0}(I)\rangle$ es el mismo para todo orden monomial $<\in \mathcal{T}_1$ en contra de lo que habíamos supuesto.

- Caso 2: Si por el contrario $\langle LT_<(m_1), \ldots, LT_<(m_s)\rangle \subsetneq \langle LT_<(I)\rangle$ para cada $<\in \mathcal{T}_1$, podemos encontrar $f \in I$ tal que $LT_{<_0}(f) \notin \langle LT_{<_1}(m_1), \ldots, LT_{<_0}(m_s)\rangle$ para un orden monomial $<_0\in \mathcal{T}_1$. Dividimos f entre $\{f_1, \ldots, f_s\}$ mediante el algoritmo de división para el orden $<_0$ y obtenemos como resto el polinomio $f_{s+1} \in I$. Dado que $LT_{<_0}(f)$ no es divisible entre ninguno de los m_i se tiene que es uno de los términos de f_{s+1} y de hecho $LT_{<_0}(f_{s+1}) = LT_{<_0}(f)$. Al tenerse que $f_{s+1} \neq 0$, de la caracterización del resto del algoritmo de división se deduce que ningún término de f_{s+1} es divisible entre ninguno de los m_i. El número de términos de f_{s+1} es finito, por ello podemos encontrar un subconjunto infinito $\mathcal{T}_2 \subset \mathcal{T}_1$ y un término de f_{s+1}, m_{s+1}, tales que para cada $<\in \mathcal{T}_2$ se tiene que $LT_<(f_i) = m_i$ para cada

$i = 1, \ldots, s, s+1$. Además $m_{s+1} \notin \langle m_1, \ldots, m_s \rangle$.

En esta situación se pueden dar dos casos:

1. Se da la igualdad $\langle m_1, \ldots, m_s, m_{s+1} \rangle = \langle LT_< (I) \rangle$ para algún orden monomial $<\in \mathcal{T}_2$ y se podría aplicar un razonamiento similar al del caso 1 donde se llegaría a una contradicción.
2. Para cada orden monomial $<\in \mathcal{T}_2$ se tiene que $\langle m_1, \ldots, m_s, m_{s+1} \rangle \neq \langle LT_< (I) \rangle$ y se podría volver a argumentar como en el caso 2. Se podría tomar $f_{s+2} \in I$ cuyos términos no fuesen múltiplos de ningún m_i, $1 \leq i \leq s+1$ y repetir el procedimiento de forma inductiva.

Entonces, o bien se tiene que se llega al caso 1 en algún paso y se obtiene una contradicción; o bien se construye una sucesión de términos $\{m_{s+i}\}_{i \geq 0}$ tales que $m_{s+i} \notin \langle m_1, \ldots, m_s, m_{s+1}, \ldots, m_{s+i-1} \rangle$ par cada $i \geq 1$. Por el corolario 2.1.3, existe un $n_0 \geq 0$ tal que la cadena de ideales $\langle m_1, \ldots, m_{s+i} \rangle$ se estabiliza; es decir, $\langle m_1, \ldots, m_s, \ldots, m_{s+n_0} \rangle = \langle m_1, \ldots, m_s, \ldots, m_{s+n_0+1} \rangle$ lo que implica que $m_{s+n_0+1} \in \langle m_1, \ldots, m_s, \ldots, m_{s+n_0} \rangle$ llegando a una contradicción.

□

Corolario 2.2.3. *El conjunto de bases de Gröbner reducidas de un ideal I, $\mathcal{R}$, es finito.*

Corolario 2.2.4. *Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal distinto de 0. La unión de todas las bases de Gröbner reducidas de I para cada orden monomial, $\mathcal{G}_u$ es una base de Gröbner universal. Por lo tanto, todo ideal no nulo tiene una base de Gröbner universal.*

Demostración. En primer lugar, notamos que el conjunto $\mathcal{G}_u$ es finito pues el número de base de Gröbner reducidas de un ideal I es finito. Fijado un orden monomial $<\in \mathcal{T}$, veamos que $\mathcal{G}_u$ es una base de Gröbner de I para $<$: se tiene que la base de Gröbner reducida de I para este orden monomial, $\mathcal{G}_<$, está contenida en $\mathcal{G}_u$. Por lo tanto se satisface $\langle LT_< (\mathcal{G}_u) \rangle \supset \langle LT_< (\mathcal{G}_<) \rangle = \langle LT_< (I) \rangle$ y se da la igualdad $\langle LT_< (\mathcal{G}_u) \rangle = \langle LT_< (I) \rangle$.
□

2.2.6. Caracterización ideales cero dimensionales

Las bases de Gröbner además de resolver el problema de pertenencia a un ideal, son útiles para caracterizar los ideales cero dimensionales. El siguiente resultado proporciona condiciones equivalentes a que un ideal de polinomios sea cero dimensional.

Teorema 2.2.11. *Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal de polinomios sobre un cuerpo algebraicamente cerrado $\mathbb{K}$. Son equivalentes los siguientes:*

1. *I es un ideal cero dimensional; es decir, $V(I)$ es finito.*

2. *Para cada* i, $1 \leq i \leq n$ *existe un exponente* $m_i \geq 0$ *tal que* $x_i^{m_i} \in \langle LT(I) \rangle$.

3. *Dada* $\mathcal{G}$ *una base de Gröbner de* I, *para cada* i, $1 \leq i \leq n$, *existe un exponente* $m_i \geq 0$ *y un elemento* $g_i \in \mathcal{G}$ *tal que* $x_i^{m_i} = LM(g_i)$.

4. *El* $\mathbb{K}$*-espacio vectorial* $\mathbb{K}\langle\{\boldsymbol{x}^\alpha : \boldsymbol{x}^\alpha \notin LT(I)\}\rangle$ *generado por el conjunto de monomios que no pertenecen a* $\langle LT(I) \rangle$ *es de dimensión finita.*

5. *El* $\mathbb{K}$*-espacio vectorial* $\mathbb{K}[x_1, \ldots, x_n]/I$ *es de dimensión finita.*

Demostración. $1 \Rightarrow 2$. Supongamos que la variedad $V(I)$ es finita.

Si $V(I) = \emptyset$ entonces por el Nullstellensatz se deduce que $I = \mathbb{K}[x_1, \ldots, x_n]$ luego se satisface trivialmente que $1 = x_i^0 \in I$ para cada $1 \leq i \leq n$.

Supongamos que $V(I) \neq \emptyset$. Fijamos un índice $1 \leq i \leq n$. Para este índice el conjunto de coordenadas i-ésimas de los puntos de la variedad $V(I)$ $\{a_1, \ldots, a_s\}$ es finito. Consideramos el siguiente polinomio

$$f = \prod_{j=1}^{s} (x_i - a_j)$$

f se anula en todos los puntos de la variedad por lo tanto $f \in I(V(I)) = \sqrt{I}$. por lo tanto existe $m \geq 1$ tal que $f^m \in I$. El término principal de f^m es precisamente $x^{ms} \in \langle LT(I) \rangle$.

$2 \Rightarrow 3$. Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ una base de Gröbner de I. Fijado un índice $1 \leq i \leq n$ existe $m \geq 0$ tal que $x_i^m \in \langle LT(I) \rangle$. Por la caracterización de las bases de Gröbner sabemos que existe un $g_i \in \mathcal{G}$ tal que $LT(g_i)$ divide a x_i^m. Esto solo ocurre si $LM(g_i) = x_i^{m_i}$ para un $m_i \geq 0$.

$3 \Rightarrow 4$. Para cada i tomamos el mínimo $m_i \geq 0$ para el cual existe $g_i \in \mathcal{G}$ tal que $LM(g_i) = x_i^{m_i}$. Si alguno de estos m_i es 0, entonces uno de los polinomios que forman $\mathcal{G}$ es una constante y en consecuencia $I = \mathbb{K}[x_1, \ldots, x_n]$. En esta situación $\{\mathbf{x}^\alpha : \mathbf{x}^\alpha \notin LT(I)\} = \emptyset$ y $\mathbb{K}\langle\{\mathbf{x}^\alpha : \mathbf{x}^\alpha \notin LT(I)\}\rangle = 0$ que es un espacio vectorial de dimensión finita.

Supongamos que $m_i \geq 1$ para cada i. Dado un monomio $\mathbf{x}^\alpha$ con $\alpha = (a_1, \ldots, a_n)$ tal que $m_i \leq a_i$ se tiene que $x_i^{m_i}$ divide a $\mathbf{x}^\alpha$ y como consecuencia $\mathbf{x}^\alpha \in \langle LT(I) \rangle$.

Recíprocamente, si $\mathbf{x}^\alpha$ no pertenece a $\langle LT(I) \rangle$, entonces no puede ser divisible entre ninguno de los términos principales de de los polinomios de $\mathcal{G}$ por ser una base de Gröbner de I. En particular, para cada i, $1 \leq i \leq n$, se tiene que $\mathbf{x}^\alpha$ no es divisible entre $x_i^{m_i}$. Entonces no puede darse $m_i \leq a_i$ para ningún i.

Los monomios $\mathbf{x}^\alpha \in \mathbb{K}\langle\{\mathbf{x}^\alpha : \ \mathbf{x}^\alpha \notin LT(I)\}\rangle$ son precisamente los que satisfacen que $0 \leq a_i \leq m_i - 1$ para cada i. Luego el número de estos monomios es el producto $m_1 \cdots m_n$. Por definición se deduce que el conjunto de monomios que pertenecen a $\mathbb{K}\langle\{\mathbf{x}^\alpha : \ \mathbf{x}^\alpha \notin LT(I)\}\rangle$ son una base de este espacio vectorial y por lo tanto su dimensión es $m_1 \cdots m_n$.

$4 \Rightarrow 5$. En primer lugar supongamos que $\mathbb{K}\langle\{\mathbf{x}^\alpha : \ \mathbf{x}^\alpha \notin LT(I)\}\rangle = 0$. Entonces $1 \in \langle LT(I)\rangle$ y por lo tanto $I = \mathbb{K}[x_1, \ldots, x_n]$. En consecuencia, $\mathbb{K}[x_1, \ldots, x_n]/I = 0$ es un espacio vectorial de dimensión finita.

Supongamos que $\mathbb{K}\langle\{\mathbf{x}^\alpha : \ \mathbf{x}^\alpha \notin LT(I)\}\rangle \neq 0$. Sea $B = \{p_1, \ldots, p_r\}$ una base de $\mathbb{K}\langle\{x^\alpha : \ x^\alpha \notin LT(I)\}\rangle$. Consideramos el conjunto $\overline{B} = \{[p_1], \ldots, [p_r]\}$. Vamos a ver que $\overline{B}$ genera $\mathbb{K}[x_1, \ldots, x_n]/I$.

Sea $[f] \in \mathbb{K}[x_1, \ldots, x_n]/I$ donde $f \in \mathbb{K}[x_1, \ldots, x_n]$. Por 2.2.6, existen polinomios $g \in I$ y r tales que $f = g + r$ donde ningún término de r es divisible entre ningún coeficiente principal de un polinomio de I. Por lo tanto $r \in \mathbb{K}\langle\{x^\alpha : \ x^\alpha \notin LT(I)\}\rangle$.

De la condición de base de B se deduce que existen constantes $c_1, \ldots, c_r \in \mathbb{K}$ tales que $\sum_{j=0}^{r} c_j p_j = r$. Tomando clases de equivalencia módulo I en la expresión deducimos que $\sum_{j=0}^{r} c_j [p_j] = [r] = [f - g] = [f]$ puesto que $g \in I$.

De hecho, podemos ver que $\overline{B}$ es un conjunto linealmente independiente y por lo tanto es una base de $\mathbb{K}[x_1, \ldots, x_n]/I$: si $[0] = \sum_{j=0}^{r} c_j [p_j]$ para unas constantes $c_1, \ldots, c_r \in \mathbb{K}$, se deduce que $f = \sum_{j=0}^{r} c_j p_j \in I$. Si f es distinto de 0, entonces $LT(f) \in \langle LT(I)\rangle$ y por lo tanto $LM(f) \in \langle LT(I)\rangle$. El monomio $LM(f)$ debe ser uno de los que aparecen en la expresión de algún p_j. Sin embargo, cada uno de los monomios que aparecen en la expresión de p_j no pertenecen al ideal de términos principales de I por definición. Esta contradicción implica que f debe ser 0. La condición de base de B implica que las constantes $c_1, \ldots, c_r$ son nulas y por lo tanto $\overline{B}$ es una base de $\mathbb{K}[x_1, \ldots, x_n]/I$.

$5 \Rightarrow 1$. Vamos a probar que el número de coordenadas i-ésimas de los puntos de $V(I)$ es finito lo que implica que $V(I)$ es también finito. Fijado un índice $1 \leq i \leq n$ se tiene que $\{[x_i^k] : \ k \geq 0\}$ es linealmente dependiente pues la dimensión de $\mathbb{K}[x_1, \ldots, x_n]/I$ es finita.

Por lo tanto existen $k_0 \geq 0$ y constantes $c_0, \ldots, c_{k_0}$ tales que

$$[0] = \sum_{j=0}^{k_0} c_j [x_i^j] = \left[\sum_{j=0}^{k_0} c_j x_i^j \right].$$

Es decir, $\sum_{j=0}^{k_0} c_j x_i^j \in I$. Luego cada punto de la variedad $V(I)$ se anula en este polinomio que tiene un número finito de raíces. Cada coordenada i-ésima de cada punto de $V(I)$ debe ser una de las raíces del polinomio, por lo tanto solo hay número finito de ellas y en consecuencia $V(I)$ es finito.

□

Observación 9. Podemos notar que en la demostración del teorema se ha probado que si $I \subset \mathbb{K}[x_1, \ldots, x_n]$ es un ideal cero dimensional, entonces los $\mathbb{K}$-espacios vectoriales $\mathbb{K}\langle\{x^\alpha \ : \ x^\alpha \notin LT(I)\}\rangle$ y $\mathbb{K}[x_1, \ldots, x_n]/I$ son de dimensión finita e isomorfos pues tienen la misma dimensión. Dada $\mathcal{G}$ una base de Gröbner de I, esta dimensión coincide con el producto $m_1 \cdots m_n$, donde cada m_i es el mínimo valor de $m \geq 0$ para el cual x_i^m es el monomio principal de un polinomio de $\mathcal{G}$. Si además G es una base de Gröbner minimal de I, entonces para cada i, $1 \leq i \leq n$, existe un único polinomio en $\mathcal{G}$ cuyo monomio principal es de la forma x_i^m para $m \geq 0$ y en este caso $m = m_i$.

Además de presentar una caracterización muy útil de los ideales cero dimensionales, el teorema 2.2.11 proporciona una cota para el número de punto de la variedad afín asociada a uno de estos ideales. Como se ve en la demostración de teorema si $x_i^{m_i} \in \langle LT(I)\rangle$ para $1 \leq i \leq n$ entonces podemos asegurar que $|V(I)| \leq \prod_{i=1}^n m_i$. Sin embargo, esta cota puede mejorarse y en el caso de ideales radicales podemos conocer el número de puntos de $V(I)$ a partir de la dimension de $\mathbb{K}[x_1, \ldots, x_n]/I$.

Proposición 2.2.6. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal cero dimensional.*

1. $|V(I)| \leq dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I)$.

2. *Si I es un ideal radical entonces se obtiene la igualdad, es decir,*

$$|V(I)| = dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I).$$

Demostración. 1. Si $V(I) = \emptyset$ tenemos por el Nullstellensatz que $I = \mathbb{K}[x_1, \ldots, x_n]$ por lo tanto $\mathbb{K}[x_1, \ldots, x_n]/I = 0$ que tiene dimensión 0 por lo que se satisface la desigualdad del enunciado.

Supongamos que $V(I) = \{p_1, \ldots, p_s\} \neq \emptyset$. Vamos a construir un conjunto de polinomios $\{f_1, \ldots, f_s\}$ tal que $\{[f_1], \ldots, [f_s]\}$ es un conjunto linealmente independiente de $|V(I)|$ elementos.

Para $1 \leq i \leq s$ vamos a tomar $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $f_i(p_i) = 1$ y $f_i(p_j) = 0$ para $j \neq i$. En esta situación dada una combinación lineal de $[f_1], \ldots, [f_s]$ como la siguiente

$$[0] = \sum_{i=0}^{s} c_i[f_i] = \left[\sum_{i=0}^{s} c_i f_i\right]$$

se deduce que $f = \sum_{i=0}^s c_i f_i$ pertenece a I. Por lo tanto de la definición de $V(I)$ se tiene que para cada $1 \leq j \leq s$ se concluye que $0 = f(p_j) = \sum_{i=0}^s c_i f_i(p_j) = c_j$

lo que implica la independencia lineal de $\{[f_1], \ldots, [f_s]\}$.

Basta probar que existen los polinomios f_i. Fijamos $1 \leq i \leq s$. Sean $p_j \neq p_i$, existe una coordenada $1 \leq k \leq n$ para la cual $p_i^n \neq p_j^k$. Definimos el polinomio $g_j = \dfrac{x_k - p_j^k}{p_i^n - p_j^k}$ que satisface que $g_j(p_i) = 1$ y $g_j(p_j) = 0$. Tomamos $f_i = \prod_{j \neq i} g_j$ que satisface lo requerido.

2. Supongamos que I es un ideal radical; es decir que $\sqrt{I} = I$. Vamos a probar que el conjunto $[f_1], \ldots, [f_s]$ genera el espacio vectorial $\mathbb{K}[x_1, \ldots, x_n]/I$.

   Sea $[h] \in \mathbb{K}[x_1, \ldots, x_n]/I$ donde $h \in \mathbb{K}[x_1, \ldots, x_n]$. Consideramos el polinomio $g = \sum_{i=0}^{s} h(p_i) f_i$ y vamos a probar que $[h] = [g]$; es decir, que $h - g = h - \sum_{i=0}^{s} h(p_i) f_i \in I$.

   Notamos que el polinomio $h - g$ se anula en cada punto de la variedad afín $V(I)$:

$$(h - g)(p_j) = h(p_j) - \sum_{i=0}^{s} h(p_i) f_i(p_j) = h(p_j) - h(p_j) = 0$$

   Por lo tanto por el Nullstellensatz se deduce que $h - g \in I(V(I)) = \sqrt{I} = I$ lo que implica que efectivamente $\{[f_1], \ldots, [f_s]\}$ es una base de $\mathbb{K}[x_1, \ldots, x_n]/I$.

□

A continuación vamos a proporcionar una caracterización muy útil de los ideales cero dimensionales radicales.

Proposición 2.2.7. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal cero dimensional. Entonces las siguientes afirmaciones son equivalentes:*

1. *I es un ideal radical.*
2. *$|V(I)| = dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I)$.*
3. *Para cada i, $1 \leq i \leq n$, existe un polinomio $g_i \in I$ en la variable i-ésima libre de cuadrados.*

Demostración. $1 \Rightarrow 2$. Lo hemos probado en la proposición 2.2.6.

$2 \Rightarrow 1$. Si $|V(I)| = dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I)$, entonces el conjunto definido en la demostración de la proposición 2.2.6 $\{[f_1], \ldots, [f_s]\}$ es una base de $\mathbb{K}[x_1, \ldots, x_n]/I$.

Sea $h \in \sqrt{I}$. Se tiene que $[h] = \sum_{i=1}^{s} a_i[f_i]$ para ciertos $a_1, \ldots, a_s \in \mathbb{K}$. Equivalentemente se tiene que $h - \sum_{i=1}^{s} a_i f_i \in I$. Sea $p_j \in V(I)$ para $1 \leq j \leq s$, $0 = (h - \sum_{i=1}^{s} a_i f_i)(p_j) = h(p_j) - a_j$; es decir, $a_j = h(p_j)$. Por el Nullstellensatz sabemos que $\sqrt{I} = I(V(I))$ lo que implica que el polinomio h se anula en todos los puntos de $V(I)$. En consecuencia $a_j = 0$ para cada j, lo que implica $[h] = 0$ o equivalentemente $h \in I$.

$1 \Rightarrow 3$. Supongamos que existe un índice $1 \leq i_0 \leq n$ para el cual se cumple que si $g \in \mathbb{K}[x_{i_0}]$ es un polinomio libre de cuadrados entonces $g \notin I$. Vamos a probar que $I \subsetneq \sqrt{I}$. La variedad afín $V(I) = \{p_1, \ldots, p_s\}$ es finita por ser I un ideal cero dimensional. Sea $\{a_1, \ldots, a_k\}$ el conjunto de todas las coordenadas i_0-ésimas de los puntos de $V(I)$. Definimos el polinomio $g_{i_0}(x_{i_0}) = (x_{i_0} - a_1) \cdots (x_{i_0} - a_k)$ que claramente pertenece a $\mathbb{K}[x_{i_0}]$ y es libre de cuadrados puesto que las valores $a_1, \ldots, a_k$ no se repiten. Entonces por hipótesis se tiene que $g_{i_0} \notin I$. Sin embargo, $g_{i_0}(p_j) = 0$ para cada $p_j \in V(I)$ lo que implica que $g_{i_0} \in \sqrt{I}$ por el Nullstellensatz.

$3 \Rightarrow 1$. Supongamos que para cada i, $1 \leq i \leq n$, existe un polinomio $g_i \in I$ en la variable i-ésima libre de cuadrados. Fijamos i, $1 \leq i \leq n$. El conjunto $I \cap \mathbb{K}[x_i]$ es un ideal de $\mathbb{K}[x_i]$ y por lo tanto esta generado por un polinomio p_i que debe pertenecer a I. Dado que el polinomio g_i pertenece al ideal $I \cap \mathbb{K}[x_i]$ debe ser múltiplo de p_i. En particular, el polinomio p_i es libre de cuadrados y entonces p_i coincide con su parte libre de cuadrados. La proposición [6, Prop.2.7] implica que $\sqrt{I} = I + \langle p_1, \ldots, p_n \rangle$ ya que I es cero dimensional por hipótesis. Entonces $\sqrt{I} = I$ ya que $p_i \in I$ para cada i. Notamos que el resultado [6, Prop.2.7] se da para el caso $\mathbb{K} = \mathbb{C}$; sin embargo, la prueba de esta proposición sigue siendo cierta para un cuerpo infinito algebraicamente cerrado arbitrario.

□

Las bases de Gröbner permiten abordar cuestiones como la resolución de sistemas de ecuaciones de polinomios en $\mathbb{K}[x_1, \ldots, x_n]$; lo que es lo mismo, permiten obtener los puntos de una determinada variedad afín $V(I)$ para un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$.

Proposición 2.2.8. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Dado un ideal radical cero dimensional $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Para casi cualquier cambio de variables lineal se tiene que la base de Gröbner reducida de I para el orden lexicográfico $(z_n < \cdots < z_2 < z_1)$ es de la siguiente forma:*

$$\{z_1 - h_1(z_n), \ldots, z_{n-1} - h_{n-1}(z_n), h_n(z_n)\} \tag{2.2}$$

para las nuevas variables $z_1, \ldots, z_n$, donde cada $h_i(z_n) \in \mathbb{K}[z_n]$.

Demostración. La prueba de esta proposición se deduce de los resultados [11, Prop. 3.7.22] y [11, Thm. 3.7.25] y del hecho que todo cuerpo algebraicamente cerrado es un cuerpo perfecto.

□

Es decir, para calcular los puntos de una determinada variedad afín finita $V \subset \mathbb{A}^n_{\mathbb{K}}$ asociada al ideal radical cero dimensional $I = I(V) = \langle p_1, \ldots, p_r \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ podemos construir la base de Gröbner reducida de I para el orden lexicográfico. Si obtenemos que la base es de la forma 2.2, podemos obtener las coordenadas n-ésimas de los puntos de la variedad obteniendo las raíces de h_n y a partir de estas recuperar los valores del resto de coordenadas evaluando en los polinomios h_i. Si por el contrario la base de Gröbner reducida no es de la forma descrita, podemos aplicar una transformación lineal a las variables y obtener de nuevo la base de Gröbner para el orden lexicográfico en las nuevas variables $z_1, \ldots, z_n$ y repetir el procedimiento descrito anteriormente. La proposición nos asegura que tras un número finito de intentos obtendremos que la base de Gröbner reducida de I será de la forma 2.2 y por lo tanto obtendremos todos los puntos de V.

El uso del orden lexicográfico, a pesar de ser menos aconsejable que otros órdenes monomiales, permite aplicar el procedimiento descrito anteriormente para resolver sistemas de ecuaciones polinómicas de forma computacional.

A menudo resulta más importante saber si una variedad afín definida por un ideal es no vacía más que conocer específicamente sus puntos. Dicho de otra forma, dado un conjunto de polinomios a veces estaremos interesados en mostrar la existencia de alguna raíz común a todos los polinomios aún cuando no conozcamos el valor de esta. Podemos aplicar la teoría de las bases de Gröbner para afrontar este problema cuando se trabaja sobre un cuerpo algebraicamente cerrado.

Proposición 2.2.9. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado y sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Entonces, $V(I) = \emptyset$ si y solo si la base reducida de I para cualquier orden monomial es $\{1\}$.*

Demostración. En virtud del teorema 2.1.2, podemos afirmar que $V(I) = \emptyset$ si y solo si $I = \mathbb{K}[x_1, \ldots, x_n]$. Denotamos por $\mathcal{G}$ a la base de Gröbner de I para un orden monomial $<$ arbitrario fijado. Entonces, por el lema 2.2.9 se tiene que $V(I) = \emptyset$ si y solo si $\mathcal{G} = \{1\}$. □

2.3. Certificado de incompatibilidad de Nullstellensatz

Como hemos observado al final de la subsección anterior, la teoría de las bases de Gröbner nos proporcionan un criterio para determinar si un sistema de ecuaciones polinómicas carece de soluciones en un cuerpo algebraicamente cerrado. En esta sección vamos a desarrollar otra herramienta que nos va a permitir dar solución a la misma cuestión. La idea subyacente es la siguiente: dado un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, se puede traducir la igualdad $I = \mathbb{K}[x_1, \ldots, x_n]$ a la existencia de soluciones de un sistema de ecuaciones lineales el cual podemos resolver de forma computacional.

Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Sea $I = \langle p_1, \ldots, p_r \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal tal que la variedad afín asociada $V(I)$ es vacía. Por el teorema 2.1.2 sabemos que este hecho es equivalente a que $I = \mathbb{K}[x_1, \ldots, x_n]$ y en particular $V(I) = \emptyset$ si y solo si $1 \in I$. Por lo tanto existirán polinomios $\beta_1, \ldots, \beta_r \in \mathbb{K}[x_1, \ldots, x_n]$ tales que:

$$1 = \sum_{i=1}^{r} \beta_i p_i$$

Definición 2.3.1. En las condiciones anteriores diremos que $1 = \sum_{i=1}^{r} \beta_i p_i$ es un certificado de incompatibilidad de Nullstellensatz (o simplemente certificado de Nullstellensatz) de I.

Dados $p_1, \ldots, p_r \in \mathbb{K}[x_1, \ldots, x_n]$ diremos que $1 = \sum_{i=1}^{r} \beta i p_i$ es un certificado de incompatibilidad de Nullstellensatz para este conjunto de polinomios.

Llamamos grado de un certificado de Nullstellensatz $1 = \sum_{i=1}^{r} \beta_i p_i$ al máximo de los grados de los polinomios $\beta_1, \ldots, \beta_r$.

Dado un ideal de polinomios $I = \langle p_1, \ldots, p_r \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ sobre un cuerpo algebraicamente cerrado $\mathbb{K}$, podemos tratar de probar que la variedad afín $V(I)$ es vacía buscando un certificado de incompatibilidad de Nullstellensatz. Para ello podemos suponer que los polinomios $\beta_1, \ldots, \beta_r$ de este certificado sean de grado menor que k, para $k \geq 0$ fijado. Imponiendo esta condición conseguimos transformar el problema en la resolución de un sistema de ecuaciones lineales de la siguiente forma:

Sea m el máximo de los grados de los polinomios $p_1, \ldots, p_r$. Podemos escribir los polinomios β_i y p_i de la siguiente manera:

$$\beta_i = \sum_{|\delta| \leq k} \beta_{\delta,i} x^{\delta} \ , \quad p_i = \sum_{|\gamma| \leq m} p_{\gamma,i} x^{\gamma}$$

donde $\beta_{\delta,i}, p_{\gamma,i} \in \mathbb{K}$. Con esta notación obtenemos que para cada i, $1 \leq i \leq r$, el producto $\beta_i p_i$ se escribe:

$$\beta_i p_i = \sum_{|\delta| \leq k \ , \ |\gamma| \leq m} (\beta_{\delta,i} p_{\gamma,i}) x^{\delta+\gamma}$$

Si imponemos que se satisfaga la condición de que $\{\beta_1, \ldots, \beta_r\}$ sea un certificado de Nullstellensatz para I obtenemos la siguiente expresión:

$$1 = \sum_{i=1}^{r} \beta_i p_i = \sum_{i=1}^{r} \left[\sum_{|\delta| \leq k \ , \ |\gamma| \leq m} (\beta_{\delta,i} p_{\gamma,i}) x^{\delta+\gamma} \right] = \sum_{|\delta| \leq k \ , \ |\gamma| \leq m} \left[\sum_{i=1}^{r} \beta_{\delta,i} p_{\gamma,i} \right] x^{\delta+\gamma}$$

Para cada par de índices (δ, γ) con $|\delta| > 0$ o $|\gamma| > 0$ se tiene que el coeficiente del monomio $x^{\delta+\gamma}$ del polinomio constante 1 es nulo. El término constante de la combinación lineal $\sum_{i=1}^{r} \beta_i p_i$ debe ser 1. Estas dos condiciones se corresponden con el siguiente sistema de ecuaciones lineales:

$$\begin{cases} \sum_{i=1}^{r} \beta_{\mathbf{0},i} p_{\mathbf{0},i} = 1, \\ \\ \sum_{\delta+\gamma=\alpha} \left[\sum_{i=1}^{r} \beta_{\delta,i} p_{\gamma,i}\right] = 0 \qquad \text{si } |\alpha| > 0. \end{cases} \tag{2.3}$$

Se trata de un sistema de ecuaciones lineales con una incógnita por cada par (δ, i) para δ con $|\delta| \leq k$ y $1 \leq i \leq r$ y con una ecuación por cada α con $|\alpha| \leq k + m$. Una solución de este sistema se corresponde con un certificado de Nullstellensatz de I de grado menor que k. Podemos deducir que existe un certificado de incompatibilidad de Nullstellensatz para I de grado menor que k si y solo si el sistema 2.3 es compatible.

Se conocen cotas superiores para el grado máximo de un certificado de Nullstellensatz de un conjunto de polinomios $p_1, \ldots, p_r$ en relación al tamaño de estos polinomios. Estas cotas son doblemente exponenciales respecto al máximo grado de los polinomios y no se pueden mejorar pues existen casos en los que estas cotas se alcanzan.

Esta observación permite establecer un método para determinar si existe alguna solución de un sistema de ecuaciones polinómicas o equivalentemente si la variedad afín asociada al ideal generado por estos polinomios es vacía. Se considera un sistema de ecuaciones como el siguiente:

$$\begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ p_r(x_1, \ldots, x_n) = 0 \end{cases} \tag{2.4}$$

donde $p_1, \ldots, p_r \in \mathbb{K}[x_1, \ldots, x_n]$. Para determinar la existencia de soluciones de 2.4 se trata de buscar un certificado Nullstellensatz de estos polinomios. En primer lugar, se fija un grado $k \geq 0$ que va ser el grado máximo de los polinomios β_i que intervienen en el certificado Nullstellensatz. Se comprueba si el sistema de ecuaciones descrito en 2.3 es compatible. En caso de ser compatible, se obtiene un certificado Nullstellensatz que nos permite afirmar que no existe ninguna solución del sistema de ecuaciones polinómicas. Si por le contrario, el sistema de ecuaciones es incompatible aumentamos el grado máximo de los polinomios β_i y repetimos el procedimiento con $k+1$. Si el sistema de ecuaciones polinómicas no tiene ninguna solución, existirá un $k_0 \geq 0$ para el que el sistema de ecuaciones lineales sea compatible. Además podemos asegurar que k_0 debe ser menor que una cierta cota M que depende de los grados de $p_1, \ldots, p_r$. En el caso de que se obtengan sistemas lineales incompatibles para cada $k \leq M$ se pude asegurar que existe alguna solución del sistema de ecuaciones polinómicas.

Podemos observar que el tamaño de los sistemas lineales crecen rápidamente si se

aumenta el grado máximo k de los polinomios β_i. Esto sumado al hecho de que las cotas superiores para el grado del certificado son elevadas, indica que el uso de los certificados de Nullstellensatz para probar la existencia de soluciones de ecuaciones polinómicas no es adecuado en general por su elevado coste computacional. Sin embargo, para determinados sistemas de ecuaciones con una estructura característica resultan ser competitivos y pueden ser empleados. Esto es precisamente lo que sucede en el problema de coloración de grafos como veremos en el siguiente capítulo.

2.3.1. Ideas para mejorar el rendimiento

En esta sección se presentan tres ideas que permiten optimizar la eficacia del uso de certificados de incompatibilidad de Nullstellensatz para probar la ausencia de soluciones de un sistema de ecuaciones polinómicas:

- Bajo ciertas condiciones es posible prescindir de la condición de que el cuerpo $\mathbb{K}$ sobre el que se trabaja sea algebraicamente cerrado. Esto permite implementar los cálculos de forma más rápida y eficiente sobre algunos cuerpos específicos como se verá en el capítulo 3.

  Proposición 2.3.1. *Sea $\mathbb{K}$ un cuerpo no necesariamente algebraicamente cerrado. Sea $\overline{\mathbb{K}}$ las clausura algebraica de $\mathbb{K}$. Sean $p_1, \ldots, p_r \in \mathbb{K}[x_1, \ldots, x_K]$, entonces existe un certificado de Nullstellensatz $1 = \sum_{i=1}^{r} \beta_i p_i$ para $p_1, \ldots, p_r$ donde $\beta_i \in \overline{\mathbb{K}}[x_1, \ldots, x_n]$ si y solo si existe un certificado Nullstellensatz $1 = \sum_{i=1}^{r} \beta_i' p_i$ para $p_1, \ldots, p_r$ donde $\beta_i' \in \mathbb{K}[x_1, \ldots, x_n]$.*

  Demostración. Evidentemente si $1 = \sum_{i=1}^{r} \beta_i' p_i$ es un certificado de Nullstellensatz para $p_1, \ldots, p_r$ donde $\beta_i' \in \mathbb{K}[x_1, \ldots, x_n] \subset \overline{\mathbb{K}}[x_1, \ldots, x_n]$ tomando $\beta_i = \beta_i'$ se concluye.

  Suponemos ahora que existe un certificado de Nullstellensatz $1 = \sum_{i=1}^{r} \beta_i p_i$ para $p_1, \ldots, p_r$ donde $\beta_i \in \overline{\mathbb{K}}[x_1, \ldots, x_n]$. Entonces podemos encontrar tal certificado como solución del sistema de ecuaciones 2.3 que será compatible para cierto $k \geq 0$. Dado que los coeficientes de los polinomios p_i están en $\mathbb{K}$, los coeficientes de este sistema de ecuaciones también están en $\mathbb{K}$. Para resolver este sistema se llevan a cabo operaciones en $\mathbb{K}$ sobre los coeficientes lo que permite obtener una solución con coeficientes en $\mathbb{K}$. Esta solución se corresponde con un certificado Nullstellensatz $1 = \sum_{i=1}^{r} \beta_i' p_i$ donde cada polinomio $\beta_i' \in \mathbb{K}[x_1, \ldots, x_n]$.

  □

- Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Decimos que $g \in \mathbb{K}[x_1, \ldots, x_n]$ es *redundante* para un ideal $I = \langle p_1, \ldots, p_r \rangle$ de $\mathbb{K}[x_1, \ldots, x_n]$ si se anula en la variedad $V(I)$. En este caso también decimos que g es un polinomio redundante para los polinomios $p_1, \ldots, p_r$. En virtud del Nullstellensatz se tiene que g es redundante

para $p_1, \ldots, p_r$ si satisface que $g \in I(V(I)) = \sqrt{I}$.

La igualdad $I = \mathbb{K}[x_1, \ldots, x_n]$ es equivalente a que $I + \langle g \rangle = \mathbb{K}[x_1, \ldots, x_n]$: evidentemente si $I = \mathbb{K}[x_1, \ldots, x_n]$ entonces $I + \langle g \rangle = \mathbb{K}[x_1, \ldots, x_n]$. Recíprocamente, si $I + \langle g \rangle = \mathbb{K}[x_1, \ldots, x_n]$ entonces $\sqrt{I} = \mathbb{K}[x_1, \ldots, x_n]$ y por lo tanto $I = \mathbb{K}[x_1, \ldots, x_n]$. De este hecho se deduce que existe un certificado de incompatibilidad de Nullstellensatz de I si y solo si existe un certificado de Nullstellensatz para los polinomios $p_1, \ldots, p_r, g$.

Observación 10. Podemos aprovechar este hecho para optimizar el uso de certificados de incompatibilidad de Nullstellensatz para probar que la variedad $V(I)$ es vacía: tomando polinomios redundantes $g_1, \ldots g_s$ para los polinomios $p_1, \ldots, p_r$, es posible que el orden mínimo de un certificado de Nullstellensatz de los polinomios $p_1, \ldots, p_r, g_1, \ldots, g_s$ sea menor que el orden mínimo de certificado de Nullstellensatz para los polinomios $p_1, \ldots, p_r$. En esta situación se deben resolver menos sistemas lineales para obtener tal certificado; sin embargo, el tamaño de estos sistemas será mayor.

- Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Sean $I = \langle p_1, \ldots, p_r \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ y g un polinomio tal que $V(I + \langle g \rangle) = \emptyset$. Es posible utilizar el corolario 2.1.2 para determinar si I es igual a $\mathbb{K}[x_1, \ldots, x_n]$ probando si $g \in I$. De esta forma, se puede modificar la definición 2.3.1 para explotar este hecho.

  Definición 2.3.2. En las condiciones anteriores decimos que

  $$g = \sum_{i=1}^{r} \beta_i p_i$$

  es un certificado de incompatibilidad de Nullstellensatz alternativo (o simplemente certificado de Nullstellensatz alternativo) de I .

  Llamamos grado de un certificado de Nullstellensatz alternativo $g = \sum_{i=1}^{r} \beta_i p_i$ al máximo de los grados de los polinomios $\beta_1, \ldots, \beta_r$.

  Observación 11. Es posible utilizar emplear los certificado de Nullstellensatz alternativos de un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ para probar que la variedad afín $V(I)$ es vacía. Basta adaptar el procedimiento que hemos desarrollado para la búsqueda de un certificado de Nullstellensatz de I: se trata de buscar una expresión $g = \sum_{i=1}^{r} \beta_i p_i$ para ciertos polinomios β_i de grado $k \geq 0$ fijado. Esta condición se traduce en un sistema de ecuaciones lineales similar a 2.3. De hecho, este sistema solo difiere de 2.3 en el término independiente que depende del polinomio g.

  Emplear los certificados de Nullstellensatz alternativos en vez de los los certificados de Nullstellensatz usuales para probar que la variedad $V(I)$ es vacía puede ser

ventajoso. Puede darse el caso de que el orden mínimo del certificado de Nullstellensatz alternativo necesario sea menor que el orden mínimo del certificado de Nullstellensatz estándar.

Capítulo 3

Ideales de coloración

Durante este capítulo denotaremos por G a un grafo simple y finito y trabajaremos sobre un cuerpo $\mathbb{K}$ algebraicamente cerrado cuya característica no divida a $k \geq 1$ que fijamos.

3.1. Criterios de k-coloreabilidad

En esta sección vamos a abordar la forma de asociar coloraciones de un grafo a puntos de una variedad afín, y detallaremos la forma de emplear las herramientas introducidas en el capitulo anterior para discutir la coloreabilidad de un grafo.

Definición 3.1.1. Sea G un grafo. Se define el siguiente polinomio de $\mathbb{K}[x_1, \ldots, x_n]$:

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

Se dice que f_G es el polinomio del grafo G.

Observación 12. Dado un grafo G se tiene que el polinomio f_G es libre de cuadrados por ser G un grafo simple y por lo tanto el ideal $\langle f_G \rangle$ es radical (véase [5, Chap. 4.2, Def. 10]).

Para estudiar las k-coloraciones de un grafo G de n vértices podemos estudiar las k-coloraciones de la forma $\rho : V(G) \to C$ donde $C \subset \mathbb{K}$ es un conjunto de k elementos. Entonces la k-coloración queda determinada de forma unívoca por el punto $a = (\rho(1), \ldots, \rho(n)) \in C^n \subset \mathbb{A}^n_{\mathbb{K}}$.

Notación 3.1.1. *En esta situación denotaremos por ρ_a a la k-coloración asociada al punto $a = (a_1, \ldots, a_n) \in C^n$. Es decir $\rho_a(i) = a_i$.*

Proposición 3.1.1. *Sea G un grafo y sea f_G el polinomio de G. Sea $C \subset \mathbb{K}$ un conjunto de k elementos y $\rho_a : V(G) \to C$ una k-coloración de G asociada al punto $a \in \mathbb{A}^n_{\mathbb{K}}$. Entonces ρ_a es una k-coloración propia de G si y solo si $a \notin V(f_G)$.*

Demostración. Si $a \in V(f_G)$ se tiene que $f_G(a) = \prod_{i<j,\ (i,j)\in A(G)} (a_i - a_j) = 0$. Existe un par de vértices $i, j \in V(G)$ tales que $(i, j) \in A(G)$ y $a_i = a_j$, por lo tanto la ρ_a es una coloración impropia.

Recíprocamente, si ρ_a es una coloración impropia, entonces existe un par de vértices adyacentes i, j tales que $a_i = \rho_a(i) = \rho_a(j) = a_j$. Por lo tanto,

$$f_G(a) = \prod_{i<j,\ (i,j)\in A(G)} (a_i - a_j) = 0$$

y en consecuencia $a \in V(f_G)$.

□

Definición 3.1.2. Sea $1 \leq k$. Denotamos por $\mathcal{H}_{n,k}$ al conjunto de todos los grafos de vértices $\{1, \ldots, n\}$ con un subgrafo completo de $k + 1$ vértices y el resto de los vértices aislados.

Podemos observar que ninguno de los grafos pertenecientes a $\mathcal{H}_{n,k}$ es k-coloreable, puesto que en caso de existir una k-coloración ρ de $H \in \mathcal{H}_{n,k}$ se tendría una k-coloración inducida en el subgrafo completo de $k + 1$ vértices $\tilde{H}$. Tal coloración de $\tilde{H}$ no puede existir pues todos sus vértices son adyacentes y hay $k + 1$ de ellos.

Definición 3.1.3. Sea G un grafo de n vértices y sea $k \geq 1$. Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado cuya característica no divida a k. Se definen los siguientes ideales de polinomios, llamados ideales de coloración de G:

1. $I_{n,k} = \langle x_i^k - 1 : \ i \in V(G) \rangle$
2. $I_{G,k} = \langle x_i^k - 1 : \ i \in V(G) \rangle + \langle \sum_{l=0}^{k-1} x_i^{k-l-1} x_j^l : \ (i, j) \in A(G) \rangle$
3. $J_{n,k} = \langle f_H : \ H \in \mathcal{H}_{n,k} \rangle$

Notamos que en el caso de que $k \geq n$ se tiene que $\mathcal{H}_{n,k} = \emptyset$. En esta situación se toma $J_{n,k} = 0$.

Notación 3.1.2. *Sea $k \geq 1$. Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado cuya característica no divida a k. Denotaremos por R_k al conjunto de las raíces k-ésimas de la unidad en $\mathbb{K}$. Notamos que el hecho de que $\mathbb{K}$ un cuerpo algebraicamente cerrado y su característica no divida a k implica que existen k raíces de la unidad, $R_k = \{\omega_1, \ldots, \omega_k\}$.*

Proposición 3.1.2. *Sea G un grafo de n vértices y sea $k \geq 1$. Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado cuya característica no divida a k. Entonces los ideales $I_{G,k}$, $I_{n,k}$ e $I_{n,k} + \langle f_G \rangle$ son cero dimensionales y radicales.*

Demostración. Veamos en primer lugar que estos ideales son cero dimensionales. Notamos que $I_{n,k} \subset I_{G,k}$ y $I_{n,k} \subset I_{n,k} + \langle f_G \rangle$. Por la proposición 2.1.1 se tiene que $V(I_{G,k}) \subset V(I_{n,k})$ y $V(I_{n,k} + \langle f_G \rangle) \subset V(I_{n,k})$, por lo tanto solo es necesario probar que $V(I_{n,k})$ es finito. Se tiene $a \in V(I_{n,k})$ si y solo si cada componente de a es una raíz k-ésima de la unidad. Luego $V(I_{n,k}) = (R_k)^n$ es un conjunto de k^n elementos.

Dado que $I_{G,k}$, $I_{n,k}$ e $I_{n,k} + \langle f_G \rangle$ son ideales cero dimensionales, podemos aplicar la proposición 2.2.7. Para $1 \leq i \leq n$ el polinomio $x_i^k - 1$ pertenece a cada uno de los ideales y dado que este polinomio es libre de cuadrados en la variable i se deduce que $I_{G,k}$, $I_{n,k}$ e $I_{n,k} + \langle f_G \rangle$ son radicales.

□

Podemos dar una interpretación de estos ideales, en relación a las variedades afines asociadas. Para ello vamos a hacer uso del siguiente lema.

Lema 3.1.1. *Sea $k \geq 1$ y sea $\mathbb{K}$ un cuerpo cuya característica no divida a k. Sean $x, y \in \mathbb{K}$ no nulos. Entonces se tiene que $\sum_{l=0}^{k-1} x^{k-l-1}y^l = 0$ si y solo si $x \neq y$ y además $x^k = y^k$.*

Demostración. Supongamos que $x \neq y$ y $x^k = y^k$. Se tiene la siguiente igualdad: $(x^k - y^k) = (\sum_{l=0}^{k-1} x^{k-l-1}y^l)(x - y)$. Dado que $x^k = y^k$, el término de la izquierda de la igualdad es nulo. Del hecho que $x - y \neq 0$ se deduce que $\sum_{l=0}^{k-1} x^{k-l-1}y^l = 0$.

Recíprocamente, supongamos que $x = y$, entonces se obtiene la siguiente expresión $\sum_{l=0}^{k-1} x^{k-l-1}y^l = \sum_{l=0}^{k-1} x^{k-1} = kx^{k-1} \neq 0$ puesto que $x \neq 0$.

Supongamos ahora que $x^k \neq y^k$. Si se tuviese que $\sum_{l=0}^{k-1} x^{k-l-1}y^l = 0$ se obtendría una contradicción ya que $0 = 0 \cdot (x - y) = (\sum_{l=0}^{k-1} x^{k-l-1}y^l)(x - y) = x^k - y^k \neq 0$.

□

Proposición 3.1.3. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado cuya característica no divida a k. Entonces:*

1. *Los puntos de la variedad afín $V(I_{n,k}) \subset \mathbb{A}^n_{\mathbb{K}}$ están en correspondencia biyectiva con las k-coloraciones del grafo G.*
2. *Los puntos de la variedad afín $V(I_{G,k}) \subset \mathbb{A}^n_{\mathbb{K}}$ están en correspondencia biyectiva con las k-coloraciones propias del grafo G.*
3. *Los puntos de la variedad afín $V(I_{n,k} + \langle f_G \rangle) \subset \mathbb{A}^n_{\mathbb{K}}$ están en correspondencia biyectiva con las k-coloraciones impropias del grafo G.*

Demostración. 1. Sea $a = (a_1, \ldots, a_n)$ un punto de la variedad afín $V(I_{n,k}) \subset \mathbb{A}^n_{\mathbb{K}}$. Se tiene que para cada i, $1 \leq i \leq n$, $a_i^k - 1 = 0$, es decir cada a_i es una raíz de la unidad, de las cuales hay exactamente k. Por lo tanto la aplicación $\rho_a : V(G) \to R_k$ dada por $\rho_a(i) = a_i$ es una k-coloración de G.

Dada una k-coloración de G. Se puede ver como una aplicación $\rho : V(G) \to R_k$. Entonces podemos asociar de forma unívoca esta coloración el punto $a = (\rho(1), \ldots, \rho(n))$ que pertenece a $V(I_{n,k})$.

2. En primer lugar, podemos observar que $I_{n,k} \subset I_{G,k}$, lo que implica que $V(I_{G,k}) \subset V(I_{n,k})$ por 2.1.1. De esta forma cada punto $a = (a_1, \ldots, a_n)$ de la variedad afín $V(I_{G,k})$ corresponde a una k-coloración de G, $\rho_a : V(G) \to R_k$. Veamos que esta coloración es propia. Sean $i, j \in V(g)$ tales que $(i, j) \in A(G)$. El polinomio $\sum_{l=0}^{k-1} x_i^{k-l-1} x_j^l$ pertenece al ideal $I_{G,k}$ por lo tanto este polinomio se anula en a; es decir, $\sum_{l=0}^{k-1} a_i^{k-l-1} a_j^l = 0$. Por el lema 3.1.1 deducimos que $\rho_a(i) = a_i \neq a_j = \rho_a(j)$.

Si tomamos una k-coloración propia $\rho : V(G) \to R_k$ de G, le podemos asociar unívocamente un punto $a = (a_1, \ldots, a_n) \in V(I_{n,k})$. Falta probar que $a \in V(I_{G,k})$; es decir, que $\sum_{l=0}^{k-1} a_i^{k-l-1} a_j^l = 0$ para cada $(i, j) \in A(G)$. Por el lema el lema 3.1.1, esta afirmación es equivalente a que $a_i \neq a_j$ si $(i, j) \in A(G)$, que se satisface porque ρ es propia.

3. Se tiene que $V(I_{n,k} + \langle f_G \rangle) = V(I_{n,k}) \cap V(f_G)$ por la proposición 2.1.3. Sea $a \in V(I_{n,k} + \langle f_G \rangle)$. Notamos que a se corresponde con una k-coloración ρ_a puesto que $a \in V(I_{n,k})$. Se tiene que ρ_a es impropia puesto que $a \in V(f_G)$.

Sea $\rho : V(G) \to R_k$ una k-coloración impropia de G asociada al punto $a \in V(I_{n,k})$. Por ser impropia se tiene que $a \in V(f_G)$ y por lo tanto $a \in V(I_{n,k}) \cap V(f_G) = V(I_{n,k} + \langle f_G \rangle)$.

□

Corolario 3.1.1. *Sea G un grafo de orden n y sea $f_G \in \mathbb{K}[x_1, \ldots, x_n]$ el polinomio de G. Entonces $I_{n,k} : \langle f_G \rangle = I_{G,k}$.*

Demostración. Se consideran las siguientes variedades: $W_1 = V(I_{n,k})$ y $W_2 = V(\langle f_G \rangle)$. Por la proposición 3.1.3, sabemos que los puntos de la variedad W_1 están en correspondencia con las k-coloraciones no necesariamente propias de G. Por otro lado, se tiene que si $a \in W_2$ entonces la k-coloracion de G, ρ_a, es impropia por la proposición 3.1.1. En consecuencia $W_1 \setminus W_2 = V(I_{G,k})$. Aplicando la proposición 2.1.6 y notando que $I_{G,k}$, $I_{n,k}$ y $\langle f_G \rangle$ son radicales se tiene que:

$$I_{n,k} : \langle f_G \rangle = I(W_1) : I(W_2) = I(W_1 \setminus W_2) = I(V(I_{G,k})) = I_{G,k}$$

en virtud del Nullstellensatz.

□

Observación 13. Sea G un grafo de orden n. El hecho de que el ideal $I_{G,k}$ es cero dimensional radical como se ha demostrado en la proposición3.1.2, implica que

$$\dim_{\mathbb{K}}(\mathbb{K}[x_1,\ldots,x_n]/I_{G,k}) = |V(I_{G,k})|.$$

Entonces una consecuencia de la proposición 3.1.3 es que el número de k-coloraciones propias del grafo G coincide con $\dim_{\mathbb{K}}(\mathbb{K}[x_1,\ldots,x_n]/I_{G,k})$. Podemos emplear este resultado para obtener el número de k-coloraciones propias de un grafo dado.

La proposición 3.1.3 también permite obtener todas las k-coloraciones propias de G: en virtud de la proposición 2.2.8, se tiene que podemos obtener los puntos de $V(I_{G,k})$ calculando para ello $\mathcal{G}$ la base de Gröbner reducida para el orden lexicográfico del ideal $I_{G,k}$, que será de la forma 2.2 para casi cualquier cambio de variables lineal. A partir de $\mathcal{G}$, se calculan los puntos de la variedad $V(I_{G,k})$ que corresponden biunívocamente a cada una de las k-coloraciones propias de G.

Teorema 3.1.2. *Dado un grafo G de n vértices, se tiene que $f_G \in J_{n,K}$ si y solo si G no es k-coloreable.*

Demostración. Definimos el ideal de polinomios

$$\tilde{J}_{n,k} = \langle f \in \mathbb{K}[x_1,\ldots,x_n] :\ f(\rho(1),\ldots,\rho(n)) = 0\ \ \forall \rho : \{1,\ldots,n\} \to C \subset \mathbb{K}\ ,\ |C| = k\rangle.$$

Sea G un grafo de n vértices. Entonces G no es k-coloreable si y solo si $f_G \in \tilde{J}_{n,k}$. Supongamos que $f_G \in \tilde{J}_{n,k}$ y sea $\rho : \{1,\ldots,n\} \to C$ es una k-coloración de G. Se tiene que $f_G(\rho(1),\ldots,\rho(n)) = 0$ por definición de $\tilde{J}_{n,k}$ lo que implica que ρ es impropia. Supongamos que G no es k-coloreable, entonces dada un k-coloración $\rho : \{1,\ldots,n\} \to C \subset \mathbb{K}$ se tiene que ρ es impropia y por lo tanto $f(\rho(1),\ldots,\rho(n)) = 0$ por la proposición 3.1.1.

Vamos a ver que $J_{n,k} = \tilde{J}_{n,k}$. Sea $H \in \mathcal{H}_{n,k}$. Claramente podemos ver que H no es k-coloreable por lo que $f_H \in \tilde{J}_{n,k}$. Dado que los polinomios de la forma f_H con $H \in \mathcal{H}_{n,k}$ generan el ideal $J_{n,k}$ se deduce que $J_{n,k} \subset \tilde{J}_{n,k}$.

Para probar la otra contención vamos a razonar por inducción sobre el número de variables n. Evidentemente para $n = 1$ se da la igualdad de estos ideales pues ambos son 0. Sea $f \in \tilde{J}_{n,k}$ con $n > 1$. Dado un conjunto $S \subset \{1,\ldots,n-1\}$ se define el polinomio f_S el cual es el resultado de sustituir cada variable x_i con $i \in S$ por la variable x_n. Tomando $S = \emptyset$ obtenemos $f_S = f$. Podemos observar que $f_S \in \tilde{J}_{n,k}$ para cada conjunto S. En particular, dado que f_S es un polinomio en $n - |S|$ variables se tiene que si S es no vacío $f_S \in \tilde{J}_{n-|S|,k} = J_{n-|S|,k}$ por hipótesis de inducción. Además $J_{m,k} \subset J_{n,k}$ si $m < n$, por lo que en este caso se tiene que $f_S \in J_{n,k}$.

Definimos el siguiente polinomio:

$$g = \sum_S (-1)^{|S|} f_S$$

Este polinomio es combinación lineal de polinomios de $\tilde{J}_{n,k}$ por lo que $g \in \tilde{J}_{n,k}$.

Dado un índice $1 \leq i \leq n-1$ se tiene que si se sustituye en el polinomio g la variable x_i por la variable x_n se obtiene el polinomio nulo; es decir, g es múltiplo de $(x_i - x_n)$. Podemos ver este hecho desarrollando la expresión de g:

$$g(x_1, \ldots, x_{i-1}, x_n, x_{i+1}, \ldots, x_n) = \sum_S (-1)^{|S|} f_S(x_1, \ldots, x_{i-1}, x_n, x_{i+1}, \ldots, x_n) =$$

$$= \sum_{i \in S} (-1)^{|S|} f_S(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) + \sum_{i \notin S} (-1)^{|S|} f_S(x_1, \ldots, x_{i-1}, x_n, x_{i+1}, \ldots, x_n) =$$

$$= \sum_{i \in S} (-1)^{|S|} f_S(x_1, \ldots, x_n) + \sum_{i \notin S} (-1)^{|S|} f_{S \cup \{i\}}(x_1, \ldots, x_n)$$

Cuando S recorre el conjunto de subconjuntos que no contienen a i, $S' = S \cup \{i\}$ recorre el conjunto de subconjuntos que contienen a i. Esto justifica la siguiente igualdad que prueba justamente lo que se había afirmado:

$$\sum_{i \in S} (-1)^{|S|} f_S(x_1, \ldots, x_n) + \sum_{i \notin S} (-1)^{|S|} f_{S \cup \{i\}}(x_1, \ldots, x_n) =$$

$$= \sum_{i \in S} (-1)^{|S|} f_S(x_1, \ldots, x_n) - \sum_{i \in S'} (-1)^{|S'|} f_{S'}(x_1, \ldots, x_n) = 0$$

Atendiendo a este hecho, g puede ser escrito de la siguiente forma:

$$g = (x_1 - x_n) \cdots (x_1 - x_n) \cdot h$$

donde $h \in \mathbb{K}[x_1, \ldots, x_n]$. Sea $C \subset \mathbb{K}$ un conjunto de k elementos y sea una aplicación $\rho : \{1, \ldots, n\} \to C$ tal que la imagen del subconjunto $\{1, \ldots, n-1\}$ tenga cardinal $k-1$ y $\rho(i) \neq \rho(n)$ para cada $i < n$. Entonces se tiene que $h(\rho(1), \ldots, \rho(n-1), \rho(n)) = 0$ puesto que $g(\rho(1), \ldots, \rho(n-1), \rho(n)) = 0$ y ninguno de los factores $(\rho(i) - \rho(n))$ es 0. Este hecho implica que dados un conjunto $C \subset \mathbb{K}$ de $k-1$ elementos, $a \in \mathbb{K} \setminus C$ y una aplicación $\rho : \{1, \ldots, n-1\} \to C$ se tiene que $h(\rho(1), \ldots, \rho(n-1), a) = 0$. En particular desarrollando el polinomio h en potencias de x_n se tiene que cada coeficiente de x_n^i pertenece a $\tilde{J}_{n-1,k-1}$; es decir, $h \in \tilde{J}_{n-1,k-1}[x_n]$. Por hipótesis de inducción se tiene que $\tilde{J}_{n-1,k-1} = J_{n-1,k-1}$ y por tanto $h \in J_{n-1,k-1}[x_n]$.

De este hecho se deduce que para cada coeficiente de x_n^i en h, $h_i \in \mathbb{K}[x_1, \ldots, x_{n-1}]$, existen grafos de $n-1$ vértices $H_1^i, \ldots, H_{n_i}^i \in H_{n-1,k-1}$ y $f_1, \ldots, f_{n_i} \in \mathbb{K}[x_1, \ldots, x_{n-1}]$

tales que $h_i = \sum_{l=1}^{n_i} f_l p_{H_l^i}$. Entonces cada polinomio $(x_1 - x_n) \cdots (x_{n-1} - x_n) \cdot p_{H_l^i}$ es múltiplo del polinomio de un cierto grafo de $\mathcal{H}_{n,k}$ y por tanto pertenece a $J_{n,k}$. Se puede observar este hecho notando que si $\tilde{H}_l^i$ es el subgrafo de H_l^i completo de $k-1$ vértices, el grafo de n vértices $\mathbf{H}_l^i$ en el cual el vértice n-ésimo es adyacente a todos los vértices de $\tilde{H}_l^i$ satisface lo siguiente: $\mathbf{H}_l^i$ tiene n vértices, los cuales son todos aislados salvo los vértices correspondientes a $\tilde{H}_l^i$ y el vértice n-ésimo. Estos últimos son adyacentes entre si por lo que se deduce que $\mathbf{H}_l^i \in \mathcal{H}_{n,k}$. Por construcción se tiene que el polinomio del grafo $\mathbf{H}_l^i$ divide al producto $(x_1 - x_n) \cdots (x_{n-1} - x_n) \cdot p_{H_l^i}$.

Se deduce que $g \in J_{n,k}$ por ser combinación lineal de polinomios en $J_{n,k}$ y por lo tanto $f = f_\emptyset = g - \sum_{S \neq \emptyset} (-1)^{|S|} f_S \in J_{n,k}$ por ser combinación lineal de elementos de $J_{n,k}$.

□

Teorema 3.1.3. *Sea G un grafo. Sea $k \geq 1$ y sea $\mathbb{K}$ un cuerpo algebraicamente cerrado cuya característica no divida a k. Entonces las siguientes afirmaciones son equivalentes:*

1. *G no es k-coloreable.*
2. *$1 \in I_{G,k}$.*
3. *$dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I_{G,k}) = 0$.*
4. *$f_G \in I_{n,k}$.*
5. *$f_G \in J_{n,k}$.*

Demostración. $1 \Leftrightarrow 2$. En la proposición 3.1.3 hemos probado que el conjunto de coloraciones propias de G se corresponde biunívocamente con los puntos de la variedad $V(I_{G,k})$. Por lo tanto, si G no es k-coloreable si y solo si tiene que $V(I_{G,k})$ es vacía. Por el Nullstellensatz esto ocurre si y solo si $I_{G,k} = \mathbb{K}[x_1, \ldots, x_n]$; es decir, si $1 \in I_{G,k}$.

$2 \Leftrightarrow 3$. $1 \in I_{G,k}$ si y solo si $I_{G,k} = \mathbb{K}[x_1, \ldots, x_n]$ lo que es equivalente a que

$$\mathbb{K}[x_1, \ldots, x_n]/I_{G,k} = 0.$$

$1 \Leftrightarrow 4$. El grafo G no es k-coloreable si y solo si todas las k-coloraciones de G son impropias. Es decir, G no es coloreable si y solo si $V(I_{n,k}) = V(I_{n,k} + \langle f_G \rangle)$. Dado que tanto $I_{n,k}$ como $I_{n,k} + \langle f_G \rangle$ son ideales radicales por la proposición 2.2.7, se tiene que $V(I_{n,k}) = V(I_{n,k} + \langle f_G \rangle)$ es equivalente a que $I_{n,k} = I_{n,k} + \langle f_G \rangle$; es decir, es equivalente a que $f_G \in I_{n,k}$.

$1 \Leftrightarrow 5$. Lo hemos probado en el teorema 3.1.2.

□

Proposición 3.1.4. *El conjunto $\{x_i^k - 1 \ : \ 1 \leq i \leq n\}$ es una base de Gröbner universal del ideal $I_{n,k}$.*

Demostración. Aplicamos el criterio dado en la proposición 2.2.2. Para ello calculamos el mínimo común múltiplo de los monomios $LM(x_i^k - 1)$ y $LM(x_j^k - 1)$ para cada par de índices $i \neq j$: Fijamos un orden monomial $<$ arbitrario. Para este orden se debe cumplir $LT(x_i^k - 1) = x_i^k$ y $LT(x_i^k - 1) = x_j^k$ en virtud de la proposición 2.2.1. Por lo tanto se tiene que $L = mcm(LM(x_i^k - 1), LM(x_j^k - 1)) = x_i^k x_j^k = LM(x_i^k - 1) \cdot LM(x_j^k - 1)$. De esta forma se concluye que $\{x_i^k - 1 \ : \ 1 \leq i \leq n\}$ es una base de Gröbner del ideal $I_{n,k}$ para $<$.

□

Teorema 3.1.4. *El conjunto* $\{f_H \ : \ H \in \mathcal{H}_{n,k}\}$ *es una base de Gröbner universal del ideal* $J_{n,k}$.

Demostración. La demostración de este teorema se encuentra en [12, Thm. 1.1].

□

De esta forma obtenemos 4 criterios para probar si un grafo G de orden n es k-coloreable a partir del teorema 3.1.3:

- Empleando la segunda condición del teorema 3.1.3 equivalente a lo no k-coloreabilidad de G. Se tiene que $1 \in I_{G,k}$ si y solo si $I_{G,k} = \mathbb{K}[x_1, \ldots, x_n]$ lo que equivale a que $V(I_{G,k}) = \emptyset$. Entonces por la proposición 2.2.9, esto es equivalente a que la base de Gröbner reducida de $I_{G,k}$ sea $\{1\}$ para cualquier orden monomial.

  Alternativamente, se puede buscar un certificado de incompatibilidad de Nullstellensatz para el ideal $I_{G,k}$. En el caso de que exista tal certificado se tiene que G no es k-coloreable. Si por el contrario, no existe ningún certificado de Nullstellensatz para $I_{G,k}$ se deduce que G es k-coloreable.

- Se puede calcular la dimensión del espacio vectorial $\mathbb{K}[x_1, \ldots, x_n]/I_{G,k}$ y comprobar si esta es 0. En caso de que $dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I_{G,k}) = d > 0$, se deduce que G es k-coloreable y el número de k-colaciones propias de G es d.

- La cuarta afirmación equivalente a la no k-coloreabilidad de G, se puede comprobar de la siguiente manera: se fija un orden monomial cualquiera y se aplica el algoritmo de división para dividir f_G entre el conjunto $\{x_i^k - 1 \ : \ 1 \leq i \leq n\}$. La proposición 3.1.4 asegura que este conjunto en una base de Gröbner del ideal $I_{n,k}$ para el orden monomial fijado y por lo tanto $f_G \in I_{n,k}$ si y solo si el resto de la división es 0 en virtud del corolario 2.2.2.

- De igual manera, fijado un orden monomial, se puede comprobar si el polinomio f_G pertenece al ideal $J_{n,k}$ aplicando algoritmo de división para dividir f_G entre el conjunto $\{f_H \ : \ H \in \mathcal{H}_{n,k}\}$. Este conjunto es una base de Gröbner para el orden monomial fijado por el teorema 3.1.4 y por lo tanto $f_G \in J_{n,k}$ si y solo si el resto de la división es 0 en virtud del corolario 2.2.2.

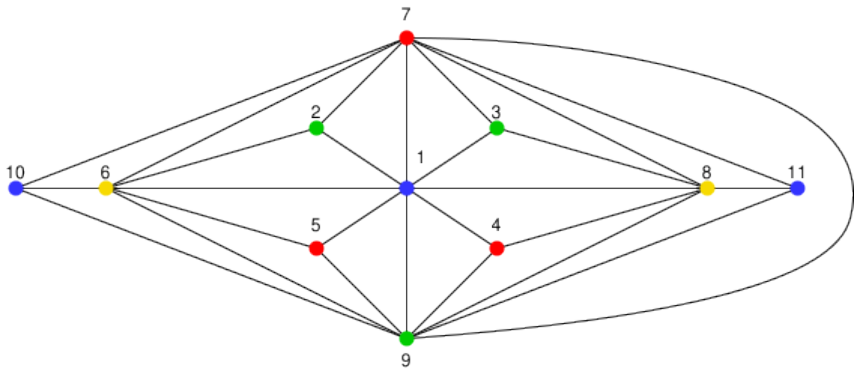


Figura 3.1: grafo de Goldner-Harary

Ejemplo 4. Vamos a emplear el primer criterio expuesto para probar que el número cromático del grafo de Goldner-Harary es 4. Este grafo, que denotaremos por G, es el que aparece en la figura 3.1. Se trata de un grafo de orden 11 que tiene 27 aristas. Podemos observar que existen cliques de tamaño 4 por lo tanto deducimos que $\chi(G) \geq 4$ como hemos probado. Vamos a probar que la base de Gröbner reducida del ideal $I_{G,4}$ para el orden lexicográfico inverso graduado es distinta de $\{1\}$ lo que nos permitirá afirmar que G es 4-coloreable y en consecuencia $\chi(G) = 4$. Para ello, utilizamos el sistema de álgebra computacional SINGULAR el cual nos permite realizar estos cálculos trabajando en el anillo $\mathbb{C}[x_1, \ldots, x_{11}]$ con este orden monomial especificado con *dp*. El comando *std* calcula la base de Gröbner reducida que necesitamos:

```
> ring r=complex,(x(1..11)),dp;
> poly f1,f2,f3,f4,f5,f6,f7,f8,f9,f10,f11;
> f1=x(1)^4-1; f2=x(2)^4-1; f1=x(3)^4-1; f4=x(4)^4-1; f5=x(5)^4-1; f6=x(6)^4-1; f7=x(7)^4-1; f8=x(8)^4-
1; f9=x(9)^4-1; f10=x(10)^4-1; f11=x(11)^4-1;

> poly f1,f2,f3,f4,f5,f6,f7,f8,f9,f10,f11,h12,h13,h14,h15,h16,h17,h18,h19,h26,h27,h37,h38,h48,h49,h56,h59,
h67,h69,h610,h78,h79,h710,h711,h89,h811,h910,h911;
> h12=x(1)^3+x(1)^2*x(2)+x(1)*x(2)^2+x(2)^3; h13=x(1)^3+x(1)^2*x(3)+x(1)*x(3)^2+x(3)^3;
h14=x(1)^3+x(1)^2*x(4)+x(1)*x(4)^2+x(4)^3; h15=x(1)^3+x(1)^2*x(5)+x(1)*x(5)^2+x(5)^3;
h16=x(1)^3+x(1)^2*x(6)+x(1)*x(6)^2+x(6)^3; h17=x(1)^3+x(1)^2*x(7)+x(1)*x(7)^2+x(7)^3;
h18=x(1)^3+x(1)^2*x(8)+x(1)*x(8)^2+x(8)^3; h19=x(1)^3+x(1)^2*x(9)+x(1)*x(9)^2+x(9)^3;
h26=x(2)^3+x(2)^2*x(6)+x(2)*x(6)^2+x(6)^v3; h27=x(2)^3+x(2)^2*x(7)+x(2)*x(7)^2+x(7)^3;
h37=x(3)^3+x(3)^2*x(7)+x(3)*x(7)^2+x(7)^3; h38=x(3)^3+x(3)^2*x(8)+x(3)*x(8)^2+x(8)^3;
h48=x(4)^3+x(4)^2*x(8)+x(4)*x(8)^2+x(8)^3; h49=x(4)^3+x(4)^2*x(9)+x(4)*x(9)^2+x(9)^3;
h59=x(5)^3+x(5)^2*x(9)+x(5)*x(9)^2+x(9)^3; h56=x(5)^3+x(5)^2*x(6)+x(5)*x(6)^2+x(6)^3;
h67=x(6)^3+x(6)^2*x(7)+x(6)*x(7)^2+x(7)^3; h69=x(6)^3+x(6)^2*x(9)+x(6)*x(9)^2+x(9)^3;
h610=x(6)^3+x(6)^2*x(10)+x(6)*x(10)^2+x(10)^3; h78=x(7)^3+x(7)^2*x(8)+x(7)*x(8)^2+x(8)^3;
h79=x(7)^3+x(7)^2*x(9)+x(7)*x(9)^2+x(9)^3; h710=x(7)^3+x(7)^2*x(10)+x(7)*x(10)^2+x(10)^3;
h711=x(7)^3+x(7)^2*x(11)+x(7)*x(11)^2+x(11)^3; h89=x(8)^3+x(8)^2*x(9)+x(8)*x(9)^2+x(9)^3;
h811=x(8)^3+x(8)^2*x(11)+x(8)*x(11)^2+x(11)^3; h910=x(9)^3+x(9)^2*x(10)+x(9)*x(10)^2+x(10)^3;
h911=x(9)^3+x(9)^2*x(11)+x(9)*x(11)^2+x(11)^3;

> ideal I=f1,f2,f3,f4,f5,f6,f7,f8,f9,f10,f11,h12,h13,h14,h15,h16,h17,h18,h19,h26,h27,h37,h38,h48,h49,
h56,h59,h67,h69,h610,h78,h79,h710,h711,h89,h811,h910,h911;
```

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

Claramente la base de Gröbner reducida de $I_{G,4}$ es distinta de $\{1\}$ y por lo tanto

$$\chi(G) = 4.$$

Además podemos calcular el número de 4-coloraciones propia de G ya que coincide con $dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I_{G,k})$. El comando *vdim* nos proporciona esta dimensión:

```
> vdim(groebner(I));
24
```

En la figura 3.1 se muestra una de estas 4-coloraciones del grafo de Goldner-Harary.

3.1.1. 3-coloreabilidad

En esta sección vamos a detallar el caso particular de la 3-coloreabilidad de un grafo G de orden n. Hemos planteado varios métodos para dar solución a esta cuestión empleando para ello la técnica de las bases de Gröbner y los certificados de incompatibilidad de Nullstellensatz. Como hemos demostrado en 3.1.3, esto es equivalente a determinar si el ideal $I_{G,3}$ es igual a $\mathbb{K}[x_1, \ldots, x_n]$ o no. Emplear las bases de Gröbner para ello resulta ser computacionalmente costoso cuando el grafo G tiene un número elevado de vértices. De hecho, si G es un grafo muy grande calcular la base de Gröbner reducida del ideal $I_{G,3}$ puede llegar a ser inviable.

En [13] se ha estudiado la eficacia del uso de certificados de Nullstellensatz del ideal $I_{G,3}$ para deducir que G no es 3-coloreable. Además, se estudia la aplicación de las ideas detalladas en las sección 2.3.1 para este problema en particular y se observa que su uso optimiza el rendimiento de esta herramienta. Se va describir cómo implementar estas técnicas para probar la no 3-coloreabilidad de un grafo G:

- Dado que 2 no divide a $k = 3$ podemos trabajar sobre el cuerpo finito $\mathbb{K} = \mathbb{F}_2$ y buscar un certificado de Nullstellensatz de $I_{G,3}$ en al anillo de polinomios $\mathbb{F}_2[x_1, \ldots, x_n]$. Esto se puede llevar a cabo porque los polinomios que generan el ideal $I_{G,3}$ pertenecen a $\mathbb{F}_2[x_1, \ldots, x_n]$. Por lo tanto, en virtud de la proposición 2.3.1 se puede asegurar que en caso de no existir ninguna 3-coloración de G, debe existir un certificado de Nullstellensatz de $I_{G,3}$ en $\mathbb{F}_2[x_1, \ldots, x_n]$. Trabajar en el cuerpo finito $\mathbb{F}_2$ proporciona grandes ventajas a nivel computacional e incluso puede llegar a reducir el orden del certificado de Nullstellensatz resultante en comparación con el uso de otros cuerpos como $\mathbb{Q}$.

- Podemos adaptar la idea desarrollada en la observación 10 al caso particular del ideal $I_{G,3}$. Un polinomio g redundante de $I_{G,3}$ debe pertenecer a $I_{G,3}$ porque este es un ideal radical. Supongamos que existen tres vértices de G, $i, j, l \in V(G)$, tales que forman un triángulo en el grafo G; es decir, i, j, l son adyacentes entre sí. Entonces el polinomio $g = x_i^2 + x_j^2 + x_l^2$ es redundante para $I_{G,3}$. Para ver esto, tomamos $a \in V(I_{G,3})$ y probamos que g se anula en a: los polinomios $(x_i - x_j), (x_j - x_l), (x_i - x_l)$ no se anulan en a y además se satisface $(x_i - x_j)(x_j - x_l)(x_i - x_l)g = 0$, de lo que se deduce que $g(a) = 0$.

  Hay evidencia de que para algunos grafos los cálculos necesarios para obtener un certificado de Nullstellensatz son mucho más rápidos cuando se añaden polinomios redundantes de este tipo. El problema es que no se puede asegurar que el orden mínimo de certificado de Nullstellensatz para $I_{G,3}$ decrezca siempre que se añadan estos polinomios. Por lo tanto, se debe introducir un número no muy elevado de polinomios redundantes de forma que se obtenga un balance entre el orden mínimo de certificado de Nullstellensatz para $I_{G,3}$ y el tamaño del sistema de ecuaciones lineales que se debe resolver.

- Se puede poner en práctica la tercera idea desarrollada en la sección 2.3.1 para probar la no 3-coloreabilidad de G de la siguiente manera: se toma un polinomio g que sea un monomio. De esta forma si un punto a se anula en g alguna de sus componentes debe ser nula lo que indica que esta componente no puede ser una raíz de la unidad y por lo tanto $a \notin V(I_{G,3})$. Entonces $V(I_{G,3} + \langle g \rangle) = \emptyset$ lo que indica que podemos llevar a cabo el procedimiento descrito en la observación 11 usando el polinomio g dado.

Sabemos que el uso de certificados de Nullstellensatz no es aconsejable en general por su elevado coste computacional. Sin embargo, a pesar de que la cota para el orden de un certificado de Nullstellensatz es doble exponencial en el número de variables, se tiene que en la mayoría de casos prácticos que surgen de problemas combinatorios como el de la k-coloración de grafos la cota es mucho más baja. En particular, en [13] se ha demostrado que el uso de los certificados de Nullstellensatz para probar la no 3-coloreabilidad de un grafo resulta ser eficaz en comparación con otros métodos entre los que se incluye calcular la base de Gröbner reducida de $I_{G,3}$. También se ha probado que el empleo de certificados de Nullstellensatz para el probar la no 3-coloreabilidad de un grafo sigue dando buenos resultados cuando se aplica a grafos de orden elevado. Además, en el caso particular del estudio de la no 3-coloreabilidad de un grafo, se tiene que el orden mínimo del certificado de Nullstellensatz obtenido es normalmente 1.

3.2. Grafos únicamente coloreables

En el capítulo 1 hemos notado que dos k-coloraciones distintas $\rho, \tilde{\rho} : V(G) \to R_k$ de un grafo G pueden dar lugar a las mismas clases de coloración. En esta situación

las k-coloraciones ρ y $\tilde{\rho}$ aportan la misma información y diremos que son *esencialmente idénticas*, por lo tanto consideraremos que dos k-coloraciones de G son distintas si esto no ocurre. La cuestión a la que vamos a dar solución en esta sección es determinar cuándo un grafo G tiene una única k-coloración en el sentido que hemos especificado.

La proposición 3.1.3 permite trabajar con k-coloraciones de un grafo G empleando para ello como conjunto de colores R_k. Como hemos visto, este conjunto de colores nos permite trasladar las nociones de k-coloración de G propia e impropia al ámbito del álgebra conmutativa. Este hecho justifica que consideremos este conjunto de colores para hablar de una k-coloración de G y nos permite emplear la siguiente notación.

Notación 3.2.1. *Nos referiremos a una k-coloración de G no necesariamente propia como un punto $a \in V(I_{n,k}) = (R_k)^n$. Es decir, dado $a \in V(I_{n,k})$, la k-coloración a de G designará la que habíamos denotado por ρ_a. De igual forma hablaremos de los puntos de $V(I_{G,k})$ para referirnos a las k-coloraciones propias de G.*

Definición 3.2.1. Sea G un grafo y sea ρ una k-coloración propia de G. Una k-coloración propia de G, $\tilde{\rho}$, se dice que es esencialmente idéntica a ρ si las clases de coloración de ambas coinciden; es decir, si $\tilde{\rho}$ se obtiene de ρ permutando los colores. En esta situación se dice que $\tilde{\rho}$ y ρ son esencialmente idénticas.

Diremos que un grafo G es únicamente k-coloreable si dadas dos k-coloraciones de G estas son esencialmente idénticas.

Observación 14. Notamos que si ρ una k-coloración propia de G, entonces cualquier k-coloración esencialmente idéntica a ρ debe ser propia. De igual forma, si ρ una k-coloración impropia, se tiene que cualquier k-coloración esencialmente idéntica a ρ debe ser impropia.

Definición 3.2.2. Sea G un grafo y $\gamma \in V(I_{G,k})$ una k-coloración propia de G:

1. Denotamos por $\Gamma_{G,\gamma}$ al subconjunto de $V(I_{G,k})$ de las k-coloraciones esencialmente idénticas a γ.
2. El ideal $I_{G,\gamma} = I(\Gamma_{G,\gamma})$ se denomina ideal de coloración de γ.

Se puede observar que $\Gamma_{G,\gamma}$ es una variedad afín contenida en $V(I_{n,k})$ en virtud de la proposición 2.1.4. Notamos que $I_{G,\gamma}$ es un ideal radical y además, dado que $\Gamma_{G,\gamma}$ es una variedad afín, $V(I_{G,\gamma}) = \Gamma_{G,\gamma}$ por 2.1.2. Entonces $I_{G,\gamma}$ es un ideal cero dimensional porque $\Gamma_{G,\gamma}$ es una variedad finita. En efecto el número de elementos de $\Gamma_{G,\gamma}$ es menor que el número de permutaciones de las k colores. De manera precisa, si γ emplea $l \leq k$ colores, el número de elementos de de $\Gamma_{G,\gamma}$ es

$$\binom{k}{l} \cdot l! = k \cdot (k-1) \cdots (k-l+1). \tag{3.1}$$

Esto es fácil de ver notando que cada una de los puntos de $\Gamma_{G,\gamma}$ corresponde a una asociación de los l colores a cada clase una de las l clases de coloración de γ. Hay $\binom{k}{l}$ formas distintas de seleccionar los l colores de entre los k posibles, de lo que se concluye que el número de elementos de de $\Gamma_{G,\gamma}$ es 3.1.

Además, de la definición del ideal $I_{G,\gamma}$ se deduce que $I_{G,k} \subset I_{G,\gamma}$: se tiene que $I_{G,\gamma} = I(\Gamma_{G,\gamma})$ y $I_{G,k} = I(V(I_{G,k}))$ en virtud del Nullstellensatz por ser $I_{G,k}$ radical. También se tiene que $\Gamma_{G,\gamma} \subset V(I_{G,k})$ por definición, luego basta aplicar la proposición 2.1.1 para concluir que $I_{G,k} \subset I_{G,\gamma}$.

Proposición 3.2.1. $\bigcap_{\gamma \in V(I_{G,k})} I_{G,\gamma} = I_{G,k}$.

Demostración. De la definición de $\Gamma_{G,\gamma}$ se deduce que $\bigcup_{\gamma \in V(I_{G,k})} \Gamma_{G,\gamma} = V(I_{G,k})$. Por lo tanto, dado que el ideal $I_{G,k}$ es radical por 3.1.2, se deduce por 2.1.3 que

$$\bigcap_{\gamma \in V(I_{G,k})} I_{G,\gamma} = \bigcap_{\gamma \in V(I_{G,k})} I(\Gamma_{G,\gamma}) = I\left(\bigcup_{\gamma \in V(I_{G,k})} \Gamma_{G,\gamma} \right) = I(V(I_{G,k})) = I_{G,k}$$

en virtud del Nullstellensatz.

□

Definición 3.2.3. Sea G un grafo. Sea $U \subset V(G)$ un subconjunto de vértices y $d \geq 0$. Se define el polinomio h_U^d como la suma de todos los monomios de grado d en las variables $\{x_i : i \in U\}$. Consideraremos $h_U^0 = 1$ y $h_\emptyset^d = 0$.

Observación 15. Tomando $d = k - 1$ y $U = \{i, j\}$ para dos pares de vértices adyacentes $i, j \in V(G)$ se obtiene el polinomio $h_{\{i,j\}}^{k-1} = \sum_{l=0}^{k-1} x_i^{k-l-1} x_j^l$, que es uno de los generadores de $I_{G,k}$.

Lema 3.2.1. *Sea U un subconjunto de vértices de un grafo G y sea $d \geq 0$. Sean $i, j \in U$. Entonces $(x_i - x_j)h_U^d = h_{U\setminus\{j\}}^{d+1} - h_{U\setminus\{i\}}^{d+1}$.*

Demostración. Dado un monomio m de grado $d+1$ en las variables $\{x_k : k \in U\}$ pueden darse dos casos:

- Caso 1: la variable x_i interviene en el monomomio m. En este caso, existe un monomio $\tilde{m}$ de grado d en las variables $\{x_k : k \in U\}$ tal que $m = x_i\tilde{m}$. Por lo tanto m aparece en la expresión de $x_i h_U^d$.
- Caso 2: la variable x_i no interviene en el monomomio m y por lo tanto m es uno de los términos de $h_{U\setminus\{i\}}^{d+1}$.

De esta forma se tiene que el polinomio h_U^{d+1} es igual a la suma $x_i h_U^d + h_{U\setminus\{i\}}^{d+1}$. De forma análoga se tiene que $h_U^{d+1} = x_j h_U^d + h_{U\setminus\{j\}}^{d+1}$, de lo que se deduce que $x_i h_U^d + h_{U\setminus\{i\}}^{d+1} = x_j h_U^d + h_{U\setminus\{j\}}^{d+1}$ y por lo tanto se concluye $(x_i - x_j)h_U^d = h_{U\setminus\{j\}}^{d+1} - h_{U\setminus\{i\}}^{d+1}$.

□

Notación 3.2.2. *Sea G un grafo y $\gamma \in V(I_{G,k})$ una k-coloración propia de G que emplea $l \leq k$ colores distintos. Llamaremos clase de color del vértice $I \in V(G)$ al conjunto de vértices de G que tienen el mismo color que i; es decir, el conjunto de vértices de G cuya imagen por ρ_γ es igual que $\rho_\gamma(i)$. Denotaremos a la clase de color del vértice i por $cl(i)$.*

En esta situación, sean $\{v_1, \ldots, v_l\} \subset V(G)$ un conjunto de representantes de cada una de las clases de color, de forma que para cada vértice j de G existe un único i_0, $1 \leq i_0 \leq l$, para el cual j pertenezca a la misma clase de color de v_{i_0}. Escribiremos $v(j) = v_{i_0}$ para referirnos al representante de la clase de color del vértice j.

Proposición 3.2.2. *Sea γ una k-coloración propia de un grafo G de orden n que emplea $l \leq k$ colores distintos. Para cada i, $1 \leq i \leq n$, se define el polinomio g_i de la siguiente manera:*

$$g_i = \begin{cases} x_{v_l}^k - 1, & si\ i = v_l \\ h_{\{v_j,\ldots,v_l\}}^{k-l+j}, & si\ i = v_j\ para\ j \neq l \\ x_i - x_{v(i)}, & en\ otro\ caso \end{cases} \tag{3.2}$$

En esta situación, los polinomios g_i generan el ideal de coloración $I_{G,\gamma}$. Además, $\mathcal{G} = \{g_1, \ldots, g_n\}$ es una base de Gröbner minimal del ideal $I_{G,\gamma}$ para cualquier orden monomial $<$ que satisfaga $x_{v_l} < \cdots < x_{v_2} < x_{v_1}$ y $x_{v(i)} < x_i$ para cada vértice $i \in V(G) \setminus \{v_1, \ldots, v_l\}$.

Demostración. Denotamos por I al ideal generado por los polinomios $g_1, \ldots g_n$. En primer lugar, vamos a demostrar que $I \subset I_{G,\gamma}$. Para ello, vamos a probar que cada polinomio de I se anula en cada k-coloración esencialmente idéntica a γ. Una vez demostrado esto, el hecho de que $I_{G,\gamma} = I(\Gamma_{G,\gamma})$ implica la inclusión $I \subset I_{G,\gamma}$.

Sea $\delta = (\delta_1, \ldots, \delta_n) \in \Gamma_{G,\gamma}$ una k-coloración esencialmente idéntica a γ. En primer lugar se tiene que $g_{v_l}(\delta) = \delta_{v_l}^k - 1 = 0$ puesto que $\delta \in V(I_{n,k})$.

Vamos a probar que para cada conjunto $U \subset \{v_1, \ldots, v_l\}$ con $|U| \geq 2$ el polinomio $h_U^{k+1-|U|}$ se anula en δ. En particular, este resultado implica que los polinomios $g_{v_1}, \ldots, g_{v_{l-1}}$ se anulan en δ. Razonamos por inducción sobre $|U|$:

Si $|U| = 2$, se tiene que $U = \{u_1, u_2\}$ para ciertos vértices $u_1, u_2 \in \{v_1, \ldots, v_l\}$. Entonces se tiene que

$$(\delta_{u_1} - \delta_{u_2})h_U^{k-1}(\delta) = h_{u_2}^k(\delta) - h_{u_1}^k(\delta) = \delta_{u_2}^k - \delta_{u_1}^k = 1 - 1 = 0$$

por el lema 3.2.1 y notando que $\delta \in V(I_{n,k})$. Dado que u_1 y u_2 son dos representantes de dos clases de coloración distintas de la coloración propia δ, se tiene que $\delta_{u_1} \neq \delta_{u_2}$ y por lo tanto se deduce que $h_U^{k-1}(\delta) = 0$.

Sea $U \subset \{v_1, \ldots, v_l\}$ con $|U| > 2$ y sean u_1, u_2 dos vértices distintos de U. Aplicando el lema 3.2.1 se tiene que

$$(\delta_{u_1} - \delta_{u_2}) h_U^{k+1-|U|}(\delta) = h_{U\setminus\{u_2\}}^{k+1-|U\setminus\{u_2\}|}(\delta) - h_{U\setminus\{u_1\}}^{k+1-|U\setminus\{u_2\}|}(\delta) = 0 - 0 = 0$$

donde $h_{U\setminus\{u_2\}}^{k+1-|U\setminus\{u_2\}|}(\delta) = h_{U\setminus\{u_1\}}^{k+1-|U\setminus\{u_2\}|} = 0$ por hipótesis de inducción. De nuevo, el hecho de que u_1 y u_2 son dos representantes de dos clases de coloración distintas, implica que $(\delta_{u_1} - \delta_{u_2}) \neq 0$ y por lo tanto $h_U^{k+1-|U|}(\delta) = 0$.

Resta probar que el resto de generadores de I se anulan en δ. Estos polinomios son de la forma $x_i - x_{v(i)}$ para un vértice $i \notin \{v_1, \ldots, v_l\}$. El vértice $v(i)$ es un representante de la clase de coloración de i y al ser δ esencialmente idéntica a γ se tiene que los colores de los vértices i y $v(i)$ en la coloración δ coinciden; es decir, $\delta_i = \delta_{v(i)}$ lo que implica que el polinomio $x_i - x_{v(i)}$ se anula en δ.

Sea $<$ un orden monomial que satisfaga $x_{v_l} < \cdots < x_{v_2} < x_{v_1}$ y $x_{v(i)} < x_i$ para cada vértice $i \in V(G) \setminus \{v_1, \ldots, v_l\}$. Los términos principales de los polinomios g_i son los siguientes:

- Si $i = v_l$, $LT(g_{v_l}) = LT(x_{v_l}^k - 1) = x_{v_l}^k$ por el corolario 2.2.1.
- En el caso $i = v_j$ para $j \neq l$, se tiene que $g_{v_j} = h_{\{v_j,\ldots,v_l\}}^{k-l+j}$ es unas suma de monomios en los cuales intervienen variables x_{v_t} con t mayor que j salvo en el monomio $x_{v_j}^{k-l+j}$. Se tiene que $x_{v_t} < x_{v_j}$ por hipótesis. En cada uno de lo monomios distintos de $x_{v_j}^{k-l+j}$ que aparecen en la expresión de g_{v_j} el exponente de la variable x_{v_j} es estrictamente menor que $k - l + j$ lo que permite deducir que $LT(g_{v_j}) = x_{v_j}^{k-l+j}$.
- Si $i \notin \{v_1, \ldots, v_l\}$, $g_i = x_i - x_{v(i)}$ y dado que $x_v(i) < x_i$ se tiene que $LT(g_i) = x_i$.

Podemos notar que los términos principales de los polinomios de $G = \{g_1, \ldots, g_n\}$ son primos entre sí dos a dos. Por la proposición 2.2.2 deducimos que $\mathcal{G}$ es una base de Gröbner. Además los coeficientes principales de los polinomios de $\mathcal{G}$ son todos 1 y ninguno de los términos principales de un polinomio de la base es divisible entre otro término principal de otro polinomio de $\mathcal{G}$. En consecuencia, $\mathcal{G}$ es una base de Gröbner minimal.

Para cada i, $1 \leq i \leq n$, se tiene que $LT(g_i)$ es un monomio en la variable x_i, por lo tanto en virtud del 2.2.11 se tiene que I es un ideal cero dimensional; es decir, $V(I)$ es finito.

Este hecho nos permite asegurar que el $\mathbb{K}$-espacio vectorial $\mathbb{K}\langle \mathbf{x}^\alpha : \mathbf{x}^\alpha \notin \langle LT(I)\rangle\rangle$ es isomorfo a $\mathbb{K}[x_1, \ldots, x_n]/I$ como hemos notado en la observación 9. Atendiendo a esta

observación, deducimos que la dimensión de $\mathbb{K}\langle \mathbf{x}^\alpha : \mathbf{x}^\alpha \notin \langle LT(I)\rangle\rangle$ es igual al producto $k \cdot (k-1) \cdots (k-l+1)$ dado G es una base de Gröbner minimal de I.

Entonces se tiene la siguiente cadena de desigualdades:

$$\begin{aligned} k \cdot (k-1) \cdots (k-l+1) &= |\Gamma_{G,\gamma}| \\ &= |V(I_{G,\gamma})| \\ &\leq |V(I)| \\ &\leq dim_{\mathbb{K}} \left(\mathbb{K}[x_1, \ldots, x_n]/I\right) \\ &= dim_{\mathbb{K}} \left(\mathbb{K}\langle \mathbf{x}^\alpha : \mathbf{x}^\alpha \notin \langle LT(I)\rangle\rangle\right) \\ &= k \cdot (k-1) \cdots (k-l+1) \end{aligned}$$

Por lo tanto, las desigualdades son igualdades de lo que se deduce que $V(I_{G,\gamma}) = V(I)$. Se tienen que $|V(I)| = k \cdot (k-1) \cdots (k-l+1) = dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I)$ por lo que el ideal I es radical por la proposición 2.2.7. Entonces se da la igualdad

$$I = I(V(I)) = I(V(I_{G,\gamma})) = I_{G,\gamma}$$

tras aplicar el Nullstellensatz notando que tanto I como $I_{G,\gamma}$ son ideales radicales.

□

Lema 3.2.2. *Sea G un grafo de orden n k-coloreable con $k \leq n$. Entonces existe una k-coloración de G que emplea k colores distintos.*

Demostración. Sea $\gamma \in V(I_{G,k})$ una k-coloración propia de G que usa $l \leq k$ colores. Si $l = k$, γ es la coloración buscada. En el caso de que $l < k$ se tiene que $l < n$ y por lo tanto deben existir dos vértices distintos que tienen el mismo color. Podemos colorear uno de los vértices con un color que no haya sido utilizado y obteniendo como resultado una k-coloración propia de G que emplea $l+1$ colores. Podemos repetir este procedimiento hasta obtener una k-coloración propia de G que utilice los k colores.

□

Teorema 3.2.3 (Caracterización de grafos únicamente coloreables)**.** *Sea G un grafo de orden n y sea $\gamma \in V(I_{G,k})$ una k-coloración propia de G. Sean $g_1, \ldots g_n$ definidos como en 3.2 para ciertos representantes, $v_1, \ldots, v_l$, de las clases de coloración de γ. Entonces son equivalentes las siguientes afirmaciones:*

1. *G es únicamente k-coloreable.*
2. *$dim_{\mathbb{K}} \left(\mathbb{K}[x_1, \ldots, x_n]/I_{G,k}\right) = k!$.*
3. *Los polinomios $g_1, \ldots g_n$ pertenecen a $I_{G,k}$.*
4. *Los polinomios $g_1, \ldots g_n$ generan $I_{G,k}$.*

5. $f_G \in I_{n,k} : \langle g_1, \dots g_n \rangle$.

Demostración. $1 \Rightarrow 2$. Supongamos que G es únicamente k-coloreable. Entonces por el lema 3.2.2 se tiene que existe una k-coloración propia de G, $\nu \in V(I_{G,k})$, que usa todos los k colores. Por ser G únicamente k-coloreable se deduce que toda k-coloración propia de G debe ser esencialmente idéntica a ν. Es decir, $V(I_{G,k}) = \Gamma_{G,\nu}$ que tiene $k!$ elementos. Entonces, $dim_{\mathbb{K}}(\mathbb{K}[x_1, \dots, x_n]/I_{G,k}) = V(I_{G,k}) = k!$ puesto que $I_{G,k}$ es un ideal radical cero dimensional como se ha probado en 3.1.2.

$1 \Leftarrow 2$. Recíprocamente, si $dim_{\mathbb{K}}(\mathbb{K}[x_1, \dots, x_n]/I_{G,k}) = k!$ se tiene que existe al menos una k-coloración propia en virtud del teorema 3.1.3. Por el lema 3.2.2 podemos asegurar que existe una k-coloración propia $\nu \in V(I_{G,k})$ que usa los k colores. Entonces $\Gamma_{G,\nu}$ tiene $k!$ elementos al igual que $V(I_{G,k})$. Por lo tanto se tiene la igualdad $V(I_{G,k}) = \Gamma_{G,\nu}$; esto es, toda k-coloración propia de G es esencialmente idéntica a ν. En consecuencia G es únicamente k-coloreable.

$1 \Rightarrow 3$. Supongamos que G es únicamente k-coloreable, entonces podemos deducir que toda k-coloración propia es esencialmente idéntica a γ. Además podemos asegurar que γ emplea k colores por el lema 3.2.2. Por la proposición 3.2.2 se deduce que los polinomios $g_1, \dots g_n$ generan el ideal $I_{G,\gamma}$. Sea ν otra k-coloración propia de G, se tiene que ν es esencialmente idéntica a γ y por lo tanto el $\Gamma_{G,\nu} = \Gamma_{G,\gamma}$ y entonces el ideal $I_{G,\nu}$ es igual a $I_{G,\gamma}$. Este hecho implica que $I_{G,k} = \bigcap_{\nu \in V(I_{G,k})} I_{G,\nu} = I_{G,\gamma}$ por la proposición 3.2.1. Por lo tanto, se deduce que $g_1, \dots, g_n \in I_{G,k}$.

$3 \Leftarrow 1$. Recíprocamente, si los polinomios $g_1, \dots, g_n$ pertenecen a $I_{G,k}$, se deduce que $I_{G,\gamma} \subset I_{G,k}$. Dado que siempre se satisface la inclusión $I_{G,k} \subset I_{G,\gamma}$, deducimos que ambos ideales son iguales. Entonces, $V(I_{G,k}) = V(I_{G,\gamma}) = \Gamma_{G,\gamma}$. Esto quiere decir que cada k-coloración propia de G es esencialmente idéntica a γ y en consecuencia G es únicamente k-coloreable.

$3 \Leftrightarrow 4$. La inclusión $I_{G,k} \subset \langle g_1, \dots g_n \rangle$ se satisface siempre. Por lo tanto, la igualdad $\langle g_1, \dots g_n \rangle = I_{G,k}$ es equivalente a que $\langle g_1, \dots g_n \rangle \subset I_{G,k}$, lo cual ocurre si y solo si los polinomios $g_1, \dots g_n$ pertenecen a $I_{G,k}$.

$3 \Leftrightarrow 5$. Es conocido que $I_{n,k} : \langle f_G \rangle = I_{G,k}$ por el corolario 3.1.1. Entonces aplicando el lema 2.1.1 tomando $I = I_{n,k}$, $J = \langle f_G \rangle$ y $K = \langle g_1, \dots, g_n \rangle$ se deduce que:

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

Es decir, se tiene la equivalencia $\{g_1, \dots, g_n\} \subset I_{G,k} \Leftrightarrow f_G \in I_{n,k} : \langle g_1, \dots, g_n \rangle$.

□

Este resultado proporciona varios criterios para determinar si un grafo G es únicamente k-coloreable:

- Calcular la dimensión del espacio vectorial $\mathbb{K}[x_1, \dots, x_n]/I_{G,k}$ y comprobar si coincide con $k!$.

- Si conocemos una k-coloración propia de G, podemos construir el ideal $I_{G,k} : \langle g_1, \ldots, g_n \rangle$ para los polinomios $g_1, \ldots, g_n$ como los descritos en 3.2.2. Entonces G es únicamente coloreable si y solo si $\langle g_1, \ldots, g_n \rangle \subset I_{G,k}$, lo que es equivalente por el corolario 2.1.1 a que $I_{G,k} : \langle g_1, \ldots, g_n \rangle = \mathbb{K}[x_1, \ldots, x_n]$. Podemos comprobar este hecho calculando la base de Gröbner reducida de este ideal, que denotaremos por $\mathcal{G}$, y verificando si $\mathcal{G} = \{1\}$.

  Alternativamente, podemos verificar la igualdad $I_{G,k} : \langle g_1, \ldots, g_n \rangle = \mathbb{K}[x_1, \ldots, x_n]$ calculando un certificado de incompatibilidad de Nullstellensatz si se conoce una base del ideal $I_{G,k} : \langle g_1, \ldots, g_n \rangle$.

- Si conocemos una k-coloración propia de G podemos obtener los polinomios $g_1, \ldots, g_n$ como los descritos en 3.2.2. En esta situación, podemos aplicar la cuarta equivalencia del teorema 3.2.3 y comprobar si el polinomio de grafo pertenece al ideal $I_{n,k} : \langle g, \ldots, g_n \rangle$ calculando una base de Gröbner de este ideal para ello y aplicando el algoritmo de división.

Notamos que en dos de los criterios que hemos mencionado para determinar si un grafo G es únicamente k-coloreable es necesario conocer de antemano una k-coloración propia. Esta situación no es la ideal pues en general no se conoce una k-coloración del grafo, por ello buscamos dar un resultado en el que no intervenga ninguna k-coloración de G.

Proposición 3.2.3. *Sea $\gamma \in V(I_{G,k})$ una k-coloración propia de G que usa k colores. Sean $\{v_1, \ldots, v_k\} \subset V(G)$ un conjunto de representantes de cada una de las clases de color de γ. Para cada i, $1 \leq i \leq n$, se definen los polinomios $\tilde{g}_i$ como sigue:*

$$\tilde{g}_i = \begin{cases} x_{v_l}^k - 1, & si\ i = v_l \\ h^j_{\{v_j, \ldots, v_k\}}, & si\ i = v_j\ para\ j \neq l \\ h^1_{\{i, v_2, \ldots, v_k\}} & si\ i \in cl(v_1) \\ x_i - x_{v(i)}, & en\ otro\ caso \end{cases} \tag{3.3}$$

En esta situación, los polinomios $\tilde{g}_i$ generan el ideal de coloración $I_{G,\gamma}$. Además, $\tilde{\mathcal{G}} = \{\tilde{g}_1, \ldots, \tilde{g}_n\}$ es la base de Gröbner reducida del ideal $I_{G,\gamma}$ para cualquier orden monomial $<$ que satisfaga $x_{v_k} < \cdots < x_{v_2} < x_{v_1}$ y $x_{v(i)} < x_i$ para cada vértice $i \in V(G) \setminus \{v_1, \ldots, v_k\}$.

Demostración. Notamos que los polinomios $\tilde{g}_i$ coinciden con los polinomios g_i definidos en la proposición 3.2.2 para esta elección de representantes, salvo para los vértices i de la clase de color del primer color. El polinomio g_{v_1} también es igual a $\tilde{g}_{v_1}$. Esto es, se satisface $\tilde{g}_i = g_i$ si y solo si $i \notin cl(v_1) \setminus \{v_1\}$. En consecuencia, basta ver que para cada $i \in cl(v_1) \setminus \{v_1\}$ se satisface que $\tilde{g}_i \in \langle g_1, \ldots, g_n \rangle$ y $g_i \in \langle \tilde{g}_1, \ldots, \tilde{g}_n \rangle$. Observamos que se tiene

$$\tilde{g}_i = g_{v_1} + (x_1 - x_{v_1}) = g_{v_1} + g_i \in \langle g_1, \ldots, g_n \rangle$$
$$g_i = \tilde{g}_i - g_{v_1} = \tilde{g}_i - \tilde{g}_{v_1} \in \langle \tilde{g}_1, \ldots, \tilde{g}_n \rangle$$

para cada $i \in cl(v_1) \setminus \{v_1\}$, lo que implica que $\langle \tilde{g}_1, \ldots, \tilde{g}_n \rangle = \langle g_1, \ldots, g_n \rangle = I_{G,\gamma}$.

Para probar que $\tilde{\mathcal{G}}$ es la base de Gröbner reducida de I para el orden monomial $<$, observamos que el término principal del polinomio $\tilde{g}_i$ es:

$$LT(\tilde{g}_i) = \begin{cases} x_{v_j}^j, & \text{si } i = v_j \\ x_i, & \text{en otro caso} \end{cases}$$

Esto puede verse razonando como se ha hecho en la prueba de la proposición 3.2.2 para obtener los términos principales de los polinomios g_i.

Entonces, notamos que estos términos principales son primos entre sí dos a dos. La proposición 2.2.2 implica que $\tilde{\mathcal{G}}$ es una base de Gröbner. Además, cada uno de los coeficientes principales es 1 y ningún término principal divide al término principal de otro $\tilde{g}_i$, por lo tanto $\tilde{\mathcal{G}}$ es una base de Gröbner minimal de $I_{G,\gamma}$.

Fijamos ahora un vértice i. Sea m_i un término de $\tilde{g}_i$ distinto de $LT(\tilde{g}_i)$ y $l \neq i$. Entonces se tienen los siguientes casos:

- Si $i = v_j$, $1 \leq j \leq k$, se tiene que $\tilde{g}_i = h^j_{\{v_j,\ldots,v_k\}}$ y entonces el término m_i es un monomio de grado j en las variables $x_{v_j}, \ldots, x_{v_k}$ distinto de $x_{v_j}^j$. Supongamos que $l = v_s$ para algún $j < s$, entonces se tiene que la variable x_{v_s} aparece en m_i con exponente menor o igual que j y por lo tanto m_i no es divisible entre $LT(\tilde{g}_l) = x_{v_s}^s$. Supongamos que no se da la situación anterior, entonces la única variable que aparece en $LT(\tilde{g}_l)$ no interviene en el término m_i y por lo tanto $LT(\tilde{g}_l)$ no divide a m_i.

- Si $i \in cl(v_1)\setminus\{v_1\}$, entonces $m_i = x_{v_j}$ para algún j distinto de 1. El único polinomio en el cual la variable x_{v_j} interviene en su término principal es $\tilde{g}_{v_j}$. Sin embargo, $LT(\tilde{g}_{v_j}) = x_{v_j}^j$ que no divide a x_{v_j}.

- Si no se da ninguno de los dos casos anteriores, $\tilde{g}_i = x_i - x_{v(i)}$ donde $v(i) \neq v_1$. De esta forma m_i debe ser $-x_{v(i)}$ que no es divisible entre ninguno de los términos principales de los polinomios de $\tilde{\mathcal{G}} \setminus \{\tilde{g}_i\}$.

En consecuencia, $\tilde{\mathcal{G}}$ es la base de Gröbner reducida de $I_{G,\gamma}$.

□

Notación 3.2.3. *Sea G un grafo de orden n. Sea $<$ un orden monomial en $\mathbb{K}(n)$ que satisfaga $x_n < \cdots < x_2 < x_1$. Sea $\gamma \in V(I_{G,k})$ una k-coloración propia de G que usa $l \leq k$*

colores. Denotamos por $C_1, \dots C_l$ *las clases de coloración de* γ *que supondremos que están ordenadas en el siguiente sentido:* $\max(C_{j+1}) < \max(C_j)$ *para cada* j, $1 \leq j \leq l-1$. *En esta situación, tomamos los siguientes representantes de las clases de coloración:*

$$v_j = \max(i : \ i \in C_j)$$

Estos representantes satisfacen que $x_{v_l} < \cdots < x_{v_2} < x_{v_1}$ *y* $x_{v(i)} < x_i$ *para cada vértice* $i \in V(G) \setminus \{v_1, \dots, v_l\}$ *siempre que se emplee un orden monomial en* $\mathcal{M}_{\mathbb{K}}(n)$ *que satisfaga* $x_n < \cdots < x_2 < x_1$. *En esta situación, elegiremos estos representantes* v_i *de las clases de coloración de una k-coloración propia de* G.

Teorema 3.2.4. *Sea* G *un grafo de orden* n. *Sea* $<$ *un orden monomial que satisfaga* $x_n < \cdots < x_2 < x_1$. *Entonces* G *es únicamente k-coloreable si y solo si la base de Gröbner reducida de* $I_{G,k}$ *es de la forma 3.3 para una k-coloración propia* γ *que use los* k *colores, y donde los representantes de las clases de coloración de* γ *escogidos son los descritos en 3.2.3.*

Demostración. Supongamos que la base de Gröbner reducida de $I_{G,k}$ es de la forma 3.3 para una k-coloración propia γ para la elección de representantes dada en 3.2.3. Entonces se deduce que $\langle \tilde{g}_1, \dots, \tilde{g}_n \rangle = I_{G,\gamma} = \langle g_1, \dots, g_n \rangle$ donde los polinomios $g_1, \dots, g_n$ están definidos como en 3.2 para esta elección de representantes. Por lo tanto $\langle g_1, \dots, g_n \rangle = I_{G,k}$ lo que por el teorema 3.2.3 implica que G es únicamente coloreable.

Recíprocamente, si G es únicamente coloreable, por el teorema 3.2.3 se tiene que $I_{G,\gamma} = \langle g_1, \dots, g_n \rangle = I_{G,k}$ donde γ una k-coloración propia de G que usa k colores y los polinomios $g_1, \dots, g_n$ son los descritos en 3.2. Entonces, la base de Gröbner reducida de $I_{G,\gamma}$, la cual denotamos por $\tilde{\mathcal{G}}$, es de la forma 3.3 en virtud de la proposición 3.2.3 y trivialmente se verifica que $\tilde{\mathcal{G}}$ es la base de Gröbner reducida de $I_{G,k}$.

□

Este teorema aporta otro criterio para comprobar si un grafo G de orden n es únicamente k-coloreable: se fija un orden monomial $<$ que satisfaga $x_n < \cdots < x_2 < x_1$ y se computa $\mathcal{G}$, la base de Gröbner reducida del ideal $I_{G,k}$. Si $\mathcal{G}$ es de la forma descrita en 3.3 para la elección de representantes dada en 3.2.3, se deduce que G es únicamente k-coloreable. Notamos que los tres órdenes monomiales definidos en 2 satisfacen la condición $x_n < \cdots < x_2 < x_1$ y por lo tanto pueden ser empleados para determinar si un grafo es únicamente k-coloreable.

Ejemplo 5. Podemos aplicar este resultado para probar que el grafo de Goldner-Harary (fig.3.1), G, es únicamente 4-coloreable. En el ejemplo 4 hemos calculado la base de Gröbner reducida del ideal $I_{G,4}$ para el orden lexicográfico inverso graduado. Si analizamos estos polinomio vemos que son de la forma descrita en 3.3 para las clases de coloración

$$C_1 = \{4, 5, 7\},\ C_2 = \{6, 8\},\ C_3 = \{2, 3, 9\}\ y\ C_4 = \{1, 10, 11\}.$$

Por lo tanto, G es únicamente 4-coloreable y toda 4-coloración de G debe ser esencialmente idéntica a la mostrada en la figura 3.1. También podríamos haber notado que $dim_{\mathbb{K}}(\mathbb{K}[x_1,\ldots,x_n]/I_{G,k}) = 24 = 4!$ para deducir este hecho.

3.3. Extensión de una precoloración

En esta sección se va a abordar el problema de extender una k-precoloración de un grafo G. Para ello se adaptan las ideas que hemos desarrollado en las secciones anteriores de forma que esta cuestión se traduzca a un problema que se puede tratar con las herramientas del álgebra conmutativa computacional que ya hemos estudiado.

Definición 3.3.1. Sea G un grafo de orden n y sea W un subconjunto de vértices m de G, con $0 < m < n$. Sea $C = \{c_1,\ldots,c_k\}$ un conjunto de k colores:

1. Se dice que una aplicación $\tilde{\rho} : W \to C$ es una k-precoloración de G si $\tilde{\rho}$ es una k-coloración propia del subgrafo inducido $G[W]$. Es decir, si se verifica que si i y j son dos vértices de W adyacentes entonces $\tilde{\rho}(i) \neq \tilde{\rho}(j)$.

2. Sea $\tilde{\rho} : W \to C$ es una precoloración de G. Se dice que $\tilde{\rho}$ se puede extender a una k-coloración propia de G si existe una k-coloración propia $\rho : V(G) \to C$ tal que $\rho\restriction_W = \tilde{\rho}$. En esta situación se dice que ρ es una extensión de $\tilde{\rho}$.

Podemos entender una k-precoloración de G como una k-coloración propia del grafo $W_G = G[W] + \Theta(V \setminus W)$, donde $\Theta(V \setminus W)$ es el grafo de vértices $V \setminus W$ los cuales son todos aislados. Es fácil probar este hecho observando que cada k-coloración propia ν de W_G se restringe a una k-coloración propia de $G[W]$; es decir, se restringe a una única k-precoloración de G, que denotamos por $\tilde{\nu}$. Recíprocamente, dada $\tilde{\nu}$ una k-precoloración de G, se puede extender a una k-coloración de W_G de forma trivial asignando a los vértices $V \setminus W$ el color c_1. Esta asignación da lugar a una k-coloración propia de W_G, ya que los vértices $V \setminus W$ son aislados por definición. Por lo general esta asignación no es biyectiva ya pueden existir varias k-coloraciones propias de W_G que se restrinjan a la misma k-precoloración de G. Esta forma de ver las precoloraciones de un grafo G permiten estudiarlas como puntos de la variedad afín $V(I_{W_G,k}) \subset \mathbb{A}^n_{\mathbb{K}}$ si se emplea como conjunto de colores $V(I_{n,k})$. Debe tenerse en cuenta que varios puntos de la variedad pueden representar la misma k-precoloración tal como se ha observado.

Observación 16. Sean $n \geq 1$, $0 < m < n$ y $k \geq 1$. Notamos que $V(I_{n,k}) = V(I_{m,k}) \times V(I_{n-m,k})$. Consideramos la proyección sobre las primeras m componentes:

$$\pi : \mathbb{A}^n_{\mathbb{K}} \longrightarrow \mathbb{A}^m_{\mathbb{K}}, \;\; \pi(a_1,\ldots,a_m,a_{m+1},\ldots,a_n) = (a_1,\ldots,a_m)$$

Se satisface que $\pi(V(I_{n,k})) = V(I_{m,k})$. Entonces dado un grafo G de orden n y $W = \{1,\ldots,m\} \subset V(G)$, se tiene que $\pi(V(I_{G,k})) \subset V(I_{G[W],k})$. En efecto, ya que dada

$\gamma \in V(I_{G,k})$ una k-coloración propia de G, su restricción a $G[W]$ es precisamente la k-coloración propia $\pi(\gamma)$.

Notación 3.3.1. *Sea G un grafo de orden n y sea W un subconjunto de m vértices de G con $0 < m < n$. Para facilitar la notación supondremos que $W = \{1, \ldots, m\}$. Dada $\nu \in V(I_{W_G,k})$ una k-coloración de W_G, denotaremos por $\tilde{\nu}$ a la precoloración obtenida de la restricción de ν a W, es decir, $\tilde{\nu} = \pi(\nu)$. Se puede ver $\tilde{\nu}$ como un punto de la variedad afín $V(I_{G[W],k}) \subset \mathbb{A}^m_{\mathbb{K}}$.*

El objetivo de la sección es caracterizar cuándo se puede afirmar que una precoloración $\tilde{\nu} \in V(I_{G[W],k})$ se puede extender a una k-coloración propia de G, lo que equivale a que $\tilde{\nu}$ pertenezca a $\pi(V(I_{G,k}))$.

Definición 3.3.2. Sea G un grafo de orden n y sea $W = \{1, \ldots, m\} \subset V(G)$ con $0 < m < n$. Sea $\tilde{\nu} \in V(I_{G[W],k})$ una precoloración de G. Denotamos por $\Gamma_{W,\tilde{\nu}} \subset V(I_{W_G,k})$ al conjunto de k-coloraciones de W_G cuyas restricciones a W son esencialmente idénticas a $\tilde{\nu}$, es decir, $\Gamma_{W,\tilde{\nu}} = \{\gamma \in V(I_{W_G,k}) : \ \tilde{\gamma} \in \Gamma_{G[W],\tilde{\nu}}\}$.

El conjunto $\Gamma_{W,\tilde{\nu}}$ es una variedad afín finita de $\mathbb{A}^n_{\mathbb{K}}$ contenida en $V(I_{W_G,k})$: esto se deduce de la proposición 2.1.4 y del hecho que la variedad $V(I_{W_G,k})$ es finita.

Lema 3.3.1. *Sea G un grafo de orden n y sea $W = \{1, \ldots, m\} \subset V(G)$ con $0 < m < n$. Sea $\tilde{\nu} \in V(I_{W_G,k})$ una k-precoloración de G. El conjunto de puntos de la variedad $\Gamma_{W,\tilde{\nu}} \cap V(I_{G,k})$ está en correspondencia con las extensiones de $\tilde{\nu}$, salvo permutación de colores. En particular, $\tilde{\nu}$ se puede extender a una k-coloración propia de G si y solo si $\Gamma_{W,\tilde{\nu}} \cap V(I_{G,k})$ es no vacía.*

Demostración. Cada punto de la variedad afín $\gamma \in \Gamma_{W,\tilde{\nu}} \cap V(I_{G,k})$ se corresponde con una k-coloración propia de G que satisface que su restricción a W es una k-precoloración esencialmente idéntica a $\tilde{\nu}$. Se pueden permutar los colores de γ de forma que la k-coloración resultante sea esencialmente idéntica a γ y además extienda a $\tilde{\nu}$. Recíprocamente, es sencillo observar que todo extensión de $\tilde{\nu}$ debe pertenecer a la variedad $\gamma \in \Gamma_{W,\tilde{\nu}} \cap V(I_{G,k})$. □

Definición 3.3.3. Sea G un grafo de orden n y sea W un subconjunto de vértices m de G, con $0 < m < n$. Sea $\tilde{\nu} \in V(I_{W_G,k})$ una precoloración de G. Se define el ideal cero dimensional $I_{W,\tilde{\nu}} = I(\Gamma_{W,\tilde{\nu}})$.

Proposición 3.3.1. *Sea G un grafo de orden n y sea $W = \{1, \ldots, m\} \subset V(G)$ con $0 < m < n$. Sea $\tilde{\nu} \in V(I_{W_G,k})$ una precoloración de G que usa $l \leq k$ colores. Sea $<$ un orden monomial en $\mathcal{M}_{\mathbb{K}}(n)$. Para cada $i \in W$ sean $g_i \in \mathbb{K}[x_1, \ldots, x_m]$ los polinomios definidos en 3.2.2 para la k-coloración $\tilde{\nu}$ del grafo $G[W]$. Entonces,*

$$I_{W,\tilde{\nu}} = \langle g_i : \ i \in W \rangle + \langle x_i^k - 1 : \ i \notin W \rangle.$$

Demostración. Sea $I = \langle g_i : \ i \in W\rangle + \langle x_i^k - 1 : \ i \notin W\rangle$. Sea $\gamma \in \Gamma_{W,\tilde{\nu}}$, vamos a probar que cada uno de los polinomios que generan I se anula en γ. Evidentemente los polinomios del tipo $x_i^k - 1$ se anulan en γ ya que $\Gamma_{W,\tilde{\nu}} \subset V(I_{n,k})$. Falta demostrar que $g_i(\gamma) = 0$ para cada $i \in W$. La restricción de γ a W, $\tilde{\gamma}$, es esencialmente idéntica a $\tilde{\nu}$, por lo tanto $\tilde{\gamma} \in \Gamma_{G[W],\tilde{\nu}}$. El ideal $I_{G[W],\tilde{\nu}} = I(\Gamma_{G[W],\tilde{\nu}}) \subset \mathbb{K}[x_1, \ldots, x_m]$ está generado por los polinomios g_i en virtud de la proposición 3.2.2. En consecuencia $g_i(\gamma) = g_i(\tilde{\gamma}) = 0$ y por lo tanto $I \subset I_{W,\tilde{\nu}}$.

Para probar la otra inclusión tomamos $\gamma \in V(I)$. Por la proposición 2.1.2 se tiene que $V(I) = V(g_i : \ i \in W) \cap V(x_i^k - 1 : \ i \notin W)$. Vamos probar que $\gamma \in \Gamma_{W,\tilde{\nu}}$; es decir, vamos a demostrar que γ es una k-coloración propia de W_G tal que $\tilde{\gamma}$ es esencialmente idéntica a $\tilde{\nu}$. De esta forma, probamos que $I_{W,\tilde{\nu}} = I(V(I_{W,\tilde{\nu}})) \subset I(V(I)) = \sqrt{I}$ en virtud del Nullstellensatz. Atendiendo a los generadores de los ideales $I_{G[W],\tilde{\nu}} \subset \mathbb{K}[x_1, \ldots, x_m]$ y $I_{n-m,k} \subset \mathbb{K}[x_{m+1}, \ldots, x_n]$ se deduce que:

$$V(I) = \Gamma_{G[W],\tilde{\nu}} \times V(I_{n-m,k}) \subset V(I_{G[W],k}) \times V(I_{n-m,k}) = V(I_{W_G,k})$$

por la proposición 2.1.5. Entonces γ es una k-coloración propia de W_G. Además $\tilde{\gamma} \in \Gamma_{G[W],\tilde{\nu}}$ lo que implica que $\tilde{\gamma}$ es esencialmente idéntica a $\tilde{\nu}$.

Veamos que $\mathcal{G} = \{g_i : \ i \in W\} \cup \{x_i^k - 1 : \ i \notin W\}$ es una base de Gröbner minimal para el orden $<$. Los términos principales de los polinomios g_i para $i \in W$ son lo que describimos en la demostración de la proposición 3.2.2 que eran de monomios en la variable x_i con coeficiente 1:

$$LT(g_i) = \begin{cases} x_{v_j}^{k-l+j}, & \text{si } i = v_j \text{ para algún } 1 \leq j \leq l \\ x_i, & \text{en otro caso.} \end{cases}$$

Para $i \notin W$, en virtud del corolario 2.2.1 se deduce que $LT(x_i^k - 1) = x_i^k$ que también es de la misma forma, por lo tanto todos los términos principales de los polinomio de $\mathcal{G}$ son primos entre sí. Por la proposición 2,2,2 deducimos que $\mathcal{G}$ es una base de Gröbner minimal de I.

Definimos m_i como el mínimo exponente m mayor o igual que 1 para el cual x_i^m es un término principal de un polinomio de $\mathcal{G}$:

$$m_i = \begin{cases} k - l + j, & \text{si } i \in W \text{ y } i = v_j \text{ para algún } 1 \leq j \leq l \\ 1, & \text{si } i \in W \text{ y } i \neq v_j \text{ para todo } 1 \leq j \leq l \\ k, & \text{si } i \notin W \ . \end{cases}$$

Entonces por la observación 9 se deduce que

$$dim_{\mathbb{K}}(\mathbb{K}[x_1,\ldots,x_n]/I) = \prod_{i=1}^{n} m_i = k^{n-m} \cdot \prod_{j=1}^{l} k-l+j = d.$$

Para demostrar la inclusión $I_{W,\tilde{\nu}} \subset I$ probamos que I es radical. Para ello basta ver que $|V(I)| \geq d$.

Se tiene que $\Gamma_{W,\tilde{\nu}} = V(I_{W,\tilde{\nu}}) \subset V(I)$, luego $|\Gamma_{W,\tilde{\nu}}| \leq |V(I)|$. El número de elementos de $\Gamma_{W,\tilde{\nu}}$ es el número de k-coloraciones de W_G cuya restricción a W es esencialmente idéntica a $\tilde{\nu}$. Sabemos que el número de k-coloraciones de $G[W]$ esencialmente idénticas a $\tilde{\nu}$ es $\prod_{j=1}^{l}(k-l+j)$ como hemos probado en 3.1. Además, cada k-coloración de $G[W]$ esencialmente idéntica a $\tilde{\nu}$ se puede extender a una k-coloración propia de W_G de k^{n-m} maneras distintas, cada una de ellas se corresponde con una k-coloración de los $n-m$ vértices aislados restantes. Entonces $|\Gamma_{W,\tilde{\nu}}| = d$ lo que implica que I es radical.

□

Teorema 3.3.2. *Sea G un grafo de orden n y sea $W = \{1,\ldots,m\} \subset V(G)$ con $0 < m < n$. Sea $\tilde{\nu} \in V(I_{W_G,k})$ una precoloración de G que usa $l \leq k$ colores. Sea $<$ un orden monomial en $\mathcal{M}_{\mathbb{K}}(n)$. Para cada $i \in W$ sean $g_i \in \mathbb{K}[x_1,\ldots,x_m]$ los polinomios definidos en 3.2.2 para la k-coloración $\tilde{\nu}$ del grafo $G[W]$. Entonces $\tilde{\nu}$ se puede extender si y solo si:*

$$1 \notin \langle g_i :\ i \in W\rangle + \langle x_i^k - 1 : i \notin W\rangle + \langle h_{\{i,j\}}^{k-1} :\ (i,j) \in A(G) \setminus A(G[W])\rangle. \tag{3.4}$$

Demostración. El lema 3.3.1 asegura que $\tilde{\nu}$ se puede extender si y solo si $\Gamma_{W,\tilde{\nu}} \cap V(I_{G,k}) \neq \emptyset$, lo que por la proposición 2.1.2 y el teorema 2.1.2 es equivalente a que

$$I(\Gamma_{W,\tilde{\nu}} \cap V(I_{G,k})) = \langle g_i :\ i \in W\rangle + \langle x_i^k - 1 :\ i \notin W\rangle + I(G,k) \subsetneq \mathbb{K}[x_1,\ldots,x_n].$$

Basta probar que el ideal $I(\Gamma_{W,\tilde{\nu}} \cap V(I_{G,k}))$ se puede escribir como el ideal de la expresión 3.4. Se satisface que

$$\{h_{\{i,j\}}^{k-1} :\ (i,j) \in A(G[W])\} \subset \langle g_i :\ i \in W\rangle.$$

Esto ocurre porque si $(i,j) \in A(G[W])$, entonces:

$$h_{\{v(i),v(j)\}}^{k-1} \in I_{G[W],\tilde{\nu}} \subset \mathbb{K}[x_1,\ldots,x_m]$$

como se ha probado en la demostración de la proposición 3.2.2. Aplicando el lema 3.2.1 se deduce que:

$$h_{\{i,v(j)\}}^{k-1} = h_{\{v(i),v(j)\}}^{k-1} + (x_i - x_{v(i)})h_{\{i,v(i),v(j)\}}^{k-2} \in I_{G[W],\tilde{\nu}}$$

$$h_{\{i,j\}}^{k-1} = h_{\{i,v(j)\}}^{k-1} + (x_j - x_{v(j)})h_{\{i,j,v(j)\}}^{k-2} \in I_{G[W],\tilde{\nu}}$$

y por lo tanto $h_{\{i,j\}}^{k-1} \in \langle g_i : \ i \in W\rangle \subset \mathbb{K}[x_1, \ldots, x_n]$. Además dado que $\Gamma_{G[W],\tilde{\nu}} \subset V(I_{m,k})$ y que el ideal $I_{m,k}$ es radical, se tiene que $I_{m,k} = I(V(I_{m,k})) \subset I(\Gamma_{G[W],\tilde{\nu}}) = I_{G[W],\tilde{\nu}}$. Por lo tanto, $x_i^k - 1 \in I_{G[W],\tilde{\nu}}$ para cada $i \in W$.

En consecuencia,

$$\langle g_i : \ i \in W\rangle + \langle x_i^k - 1 : \ i \notin W\rangle + I_{G,k} =$$
$$= \langle g_i : \ i \in W\rangle + \langle x_i^k - 1 : \ i \notin W\rangle + \langle h_{\{i,j\}}^{k-1} : \ (i,j) \in A(G) \setminus A(G[W])\rangle.$$

De este hecho se deduce la afirmación enunciada.

□

Este teorema aporta un criterio para el cual podemos hacer uso de las herramientas que hemos introducido en el segundo capítulo para saber si una k-precoloración de un grafo puede ser extendida a una k-coloración propia. Se puede calcular la base de Gröbner reducida del ideal $\langle g_i : \ i \in W\rangle + \langle x_i^k - 1 : i \notin W\rangle + \langle h_{\{i,j\}}^{k-1} : \ (i,j) \in A(G) \setminus A(G[W])\rangle$ y comprobar si esta base es $\{1\}$, en cuyo caso no existe tal extensión. En caso contrario se puede afirmar que tal extensión existe. En esta situación se pueden calcular los puntos de la variedad $\Gamma_{W,\tilde{\nu}} \cap V(I_{G,k})$ aplicando los métodos desarrollados en 2.2.8. Cada uno de estos puntos se corresponde con una extensión de $\tilde{\nu}$ salvo permutación de colores como se ha probado en el lema 3.3.1.

También es posible aplicar la técnica de los certificados de incompatibilidad de Nullstellensatz del ideal 3.4 para probar la inexistencia de extensiones de $\tilde{\nu}$.

Ejemplo 6. Supongamos que se tiene la siguiente 4-precolroación del grafo de Goldner-Harary, G (fig.3.1): tomamos $W = \{2, 3, 4, 5\}$. Los vértices 2 y 5 están coloreados con el mismo color c_1 y los vértices 3 y 4 están coloreados con el mismo color c_2 el cual es distinto a c_1. Sabemos que no existe ninguna 4-coloración de G que se restrinja a esta precoloración pues en tal caso debería darse los vértices 2 y 3 deberían tener el mismo color. Vamos a emplear el criterio desarrollado en esta sección para confirmar este hecho. Para ello calculamos la base de Gröbner reducida del ideal 3.4 utilizando SINGULAR:

```
> poly g2,g3,g4;
> g2=x(2)-x(5);
> g3=x(3)-x(4);
> g4=x(4)^3+x(4)^2*x(5)+x(4)*x(5)^2+x(5)^3;
> ideal J=g2,g3,g4,f5,f1,f6,f7,f8,f9,f10,f11,h12,h13,h14,h15,h16,h17,h18,h19,h26,h27,h37,h38,h48,h49,h56,
h59,h67,h69,h610,h78,h79,h710,h711,h89,h811,h910,h911;

> std(J);
_[1]=1
```

La base de Gröbner reducida del ideal 3.4 es $\{1\}$ lo que confirma que no existe ninugna extensión de esta precoloración.

Bibliografía

[1] W. W. Adams, P. Loustaunau (1994), *An Introduction to Gröbner Bases*. Graduate Studies in Mathematics, vol. 3. American Mathematical Society.

[2] M. F. Atiyah, I. G. Macdonald (1969), *Introduction to Conmutative Algebra*. Addison-Wesley Publishing Company, Inc., Massachusetts.

[3] T. Becker, V. Weispfenning (1993), *Gröbner Bases: a computational aproach to commutative algebra*. Undergraduate Texts in Mathematics, vol. 141. Springer Science+Business Media.

[4] B. Bollobás (1998), *Modern Graph Theory*. Graduate Texts in Mathematics, vol. 184. Springer.

[5] D. A. Cox, J. Little, D. O'Shea (2015), *Ideals, Varieties and Algoritmos* (4a. ed.). Undergraduate Texts in Mathematics. Springer.

[6] D. A. Cox, J. Little, D. O'Shea (2005), *Using Algebraic Geometry* (2a. ed.). Graduate Texts in Mathematics, vol. 185. Springer.

[7] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann: SINGULAR 4-3-0 — A computer algebra system for polynomial computations. https://www.singular.uni-kl.de (2022).

[8] J. M. Harris, J. L. Hirst, M. J. Mossinghoff (2008), *Combinatorics and Graph Theory* (2a. ed.). Undergraduate Texts in Mathematics. Springer.

[9] C. J. Hillar, T. Windfeldt (2008), *Algebraic characterization of uniquely vertex colorable graphs*, Journal of Combinatorial Theory, 98, 400-414.

[10] H. Kobayashi, S. Moritsugu, R. W. Hogan (1989), *On Radical Zero-Dimensional Ideals*, J. Symbolic Computation, 8, 545-552.

[11] M. Kreuzer, L. Robbiano (2000), *Computational Commutative Algebra 1*. Springer.

[12] J. A. De Loera (1995), *Gröbner Bases and Graph Colorings*, Beiträge zur Algebra und Geometrie, 36, 89-96.

[13] J. A. De Loera, J. Lee, P. N. Malkin, S. Margulies (2008), *Hilbert's Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility*, Proceedings of the 21st International Symposium on Symbolic and Algebraic Computation (ISSAC 2008), 197–206.

[14] L. Lovász (1994), *Stable sets and Polynomials*, Discrete Msthematics, 124, 137-153.

[15] D. B. West (2001), *Introduction to Graph Theory* (2a. ed.). Prentice-Hall.

[16] T. Windfeldt (2009), *Computational Aspects of Graph Coloring and the Quillen Suslin Theorem*, Department of Mathematical Sciences University of Copenhagen.