Una introducción a las Bases de Gröbner

An introduction to Gröbner's Basis

Daniel Steven Moran[1,a]

Resumen. Las Bases de Gröbner constituyen un eje central en la teoría del Álgebra Computacional. Su versatilidad y gran número de aplicaciones han permitido que dichas bases sean usadas para la investigación de diversas ramas de las matemáticas, como por ejemplo Álgebra Conmutativa, Geometría Algebraica, Teoría de Gráficas, Teoría de Códigos, Criptografía, por mencionar solamente algunas de ellas. El presente artículo tiene finalidad introductoria hacia las bases de Gröbner, tomando como referencia algunas de sus aplicaciones.

Palabras claves: Álgebra conmutativa, Teoría de anillos, bases de Gröbner, Teoría de gráficas, Aspectos computacionales y sus aplicaciones.

Abstract. The Gröbner Basis constitute a central axis in the theory of Computational Algebra. Its versatility and large number of applications have allowed these to be used for research in various branches of mathematics, such as Commutative Algebra, Algebraic Geometry, Graph Theory, Code Theory, Cryptography, to mention only some of them. The present document has an introductory purpose towards the Gröbner basis, taking as reference some of its applications.

Keywords: Commutative algebra, ring theory, Gröbner basis, graph theory, Computational aspects and applications.

Mathematics Subject Classification: 13P10.

Recibido: octubre de 2018 Aceptado: noviembre de 2019

1. Introducción

Cuando Paul Gordan -experto en la teoría de invariantes para los *Mathematische Annalen*- recibió el revolucionario trabajo [6] de David Hilbert donde exponía uno de sus grandes resultados (que posteriormente se llamaría Teorema de la Base de Hilbert), dijo:

> "Esto es teología, ¡No Matemática!"

[1]Departamento de Matemáticas, Universidad de Pamplona, Pamplona, Colombia.
[a]daniel.moran@unipamplona.edu.co

y rechazó el artículo. Gordan argumentó que la exposición era insuficiente e incomprensiva, y le envió los siguientes comentarios a Klein:

> "El problema no es la forma... sino algo mucho mas profundo. Hilbert ha desdeñado presentar sus ideas siguiendo las reglas formales, y piensa que es suficiente con que nadie contradiga su demostración... está contento pensando que la importancia y corrección de sus proposiciones son suficientes... pero para un trabajo en *Annalen* no es suficiente."

Uno de los problemas de la demostración dada por Hilbert era que su demostración era puramente de existencia, la cual carecía de interés práctico.

Tres años más tarde, en 1893, Hilbert envía una segunda evaluación [7] a los *Annalen*, proporcionando estimaciones sobre el grado máximo del conjunto mínimo de generadores usando sistemas homogéneos de parámetros. Esta vez, su propuesta fue revisada por Klein el cual le respondió en una carta a Hilbert:

> "Sin duda este es el trabajo más importante en álgebra general que los *Annalen* ha publicado."

El teorema al cual Klein se refería, ha resistido el paso de la historia y actualmente se conoce bajo el nombre de Teorema de la Base de Hilbert: *Todo ideal en el anillo de polinomios* $\mathbb{K}[x_1, ..., x_n]$ *es finitamente generado.* Posteriormente, el mismo Gordan reconocería la importancia del trabajo de Hilbert diciendo:

> "He de admitir que incluso la teología tiene sus ventajas."

y publica en [4] una versión del teorema propuesto por Hilbert en donde utiliza por primera vez ideas similares a las de Bases de Gröbner, las cuales llamó "*le systeme irréductible N*".

Posteriormente, Macaulay (1862-1937) introduce en [8] los órdenes totales en el conjunto de los monomios de un anillo de polinomios, con los cuales caracterizó las posibles funciones de Hilbert de ideales graduados, comparándolas con ideales monomiales. Esas ideas de Macaulay, fueron retomadas 12 años después por Wolfgang Gröbner (1899-1980), el cuál publicó en [5] aplicaciones de las ideas de Macaulay para ordenar polinomios, y resolvió parcialmente el problema de encontrar explícitamente una base del $\mathbb{K}$-espacio vectorial $\frac{\mathbb{K}[x_1, ..., x_n]}{I}$, siendo I un ideal de dimensión cero. En 1964, Gröbner le propone a su estudiante de doctorado, Bruno Buchberger (1942-), la continuidad del problema del cálculo que había emprendido. Para sorpresa de ambos, consiguieron desarrollar un algoritmo que era válido para *cualquier* ideal I, el cual fue el resultado principal de su tesis doctoral [2]. En honor a su maestro, Buchberger le llamó posteriormente a estos conjuntos: **Bases de Gröbner**.

En el 2007, Buchberger recibió un premio de la Association for Computing Machinery's Paris Kanellakis Theory and Practice Award por su trabajo, reconociendo la importancia de su contribución a las matemáticas y a las ciencias computacionales.

¿Qué son y para qué sirven dichas bases de Gröbner? El presente artículo tiene una finalidad introductoria hacia las bases de Gröbner, para lo cual daremos algunas nociones básicas en álgebra conmutativa.

2. Nociones Básicas

Sea $\mathbb{K}[x_1, ..., x_n]$, el anillo de polinomios en varias indeterminadas con coeficientes en un campo $\mathbb{K}$. Definimos lo que es un ideal en $\mathbb{K}[x_1, \ldots, x_n]$:

Definición 2.1. Un subconjunto $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ es un **ideal** si satisface:

1. $0 \in I$
2. Si $f, g \in I$, entonces $f + g \in I$
3. Si $f \in I$ y $h \in \mathbb{K}[x_1, \ldots, x_n]$, entonces $hf \in I$

Se puede verificar bajo esta definición que el conjunto:

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

es un ideal, donde $f_1, \ldots, f_s, h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$. Este ideal es llamado *ideal generado por* $f_1, \ldots, f_s$.

Como $\mathbb{K}[x_1, \ldots, x_n]$ no es un dominio de ideales principales, no es un anillo Euclidiano. Consecuencia de ello, es que $\mathbb{K}[x_1, \ldots, x_n]$ no posee algoritmo de la división como lo posee $\mathbb{Z}$ y $\mathbb{K}[x]$, los cuales son anillos euclidianos. Poseer un algoritmo de la división es una gran herramienta.

Teorema 2.2 (Algoritmo de la división)**.** *Dados* $f, g \in \mathbb{K}[x]$*, existen únicos* $q, r \in \mathbb{K}[x]$ *tales que*

$$f = qg + r \tag{1}$$

donde $r = 0$ *o* $gr(r) < gr(g)$*.*

Si el residuo llega a ser 0, la expresión que tenemos es

$$f = qg, \tag{2}$$

la cual, en términos de ideales de polinomios, significa que $f \in \langle g \rangle$. Por tanto, el algoritmo de la división constituye una prueba algorítmica para determinar si un polinomio pertenece o no a un ideal dado en $\mathbb{K}[x]$.

Ejemplo 2.3. El polinomio $f = x^2 - 3x + 2$ pertenece al ideal $I = \langle x - 2\rangle$, porque $f = (x-1)(x-2)$. En cambio, el polinomio $g = x^5 - 4x + 1$ no pertenece al ideal $J = \langle x^3 - x^2 + x\rangle$ porque al hacer la división de $g = x^5 - 4x + 1$ entre $x^3 - x^2 + x$, el residuo no es cero. Así, no es posible escribir a f de la forma $f = qg$, luego no pertenece al ideal generado por $x^3 - x^2 + x$.

Notemos que cuando dividimos estamos tratando de eliminar siempre el término de mayor grado. Para hacer esto, implícitamente se está usando una noción de orden en $\mathbb{K}[x]$. Este orden es el dado por el grado. Ordenar un polinomio en $\mathbb{K}[x]$ no genera mayor dificultad, porque lo que hacemos es poner primero el de grado mayor (si el orden es descendente), luego el de un grado menor, y así sucesivamente:

$$x^n \succ x^{n-1} \succ \cdots \succ x^2 \succ x \succ 1.$$

Pero la noción de orden en el anillo $\mathbb{K}[x, y]$ ya no es tan clara. Por ejemplo, si tenemos el polinomio $f = x^2y - y^3 - xy^2 + x^3 \in \mathbb{Q}[x, y]$, ¿Cómo ordenamos los términos de f? Observemos que ordenarlo por su grado absoluto es un intento fallido, puesto que f es polinomio homogéneo.

Así pues, para tener un algoritmo de la división en $\mathbb{K}[x_1, \ldots, x_n]$ es necesario esclarecer cómo ordenamos a los polinomios en este anillo. Nótese que todo monomio en $\mathbb{K}[x_1, \ldots, x_n]$, es posible relacionarlo biyectivamente con un elemento en $\mathbb{N}^n$:

$$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \longleftrightarrow (a_1, a_2, ..., a_n).$$

Por tanto, todo orden que se establezca en el conjunto $\mathbb{N}^n$ inducirá un orden en $\mathbb{K}[x_1, \ldots, x_n]$.

2.1. Órdenes Monomiales

Definición 2.4 (Orden Monomial)**.** Un orden monomial $\succ$ sobre $\mathbb{K}[x_1, \ldots, x_n]$ es una relación $\succ$ sobre $\mathbb{N}^n$ (o equivalentemente, es una relación sobre el conjunto de monomios $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n} = x^\alpha$, donde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$), que satisface:

(i) $\succ$ es un buen orden sobre $\mathbb{N}^n$

(ii) Si $\alpha \succ \beta$ y $\gamma \in \mathbb{N}^n$, entonces $\alpha + \gamma \succ \beta + \gamma$

(iii) $\succ$ es un buen orden sobre $\mathbb{N}^n$, esto significa que todo subconjunto no vacío de $\mathbb{N}^n$ tiene un elemento minimal bajo $\succ$. En otras palabras, si $A \subseteq \mathbb{N}^n$ es no vacío, entonces existe $\alpha \in A$ tal que $\beta \succ \alpha$ para todo $\beta \neq \alpha$ en A.

Algunos ejemplos de órdenes monomiales son:

2.1.1. Orden Lexicográfico (Lex)

Sean $\alpha = (\alpha_1, \ldots, \alpha_n)$ y $\beta = (\beta_1, \ldots, \beta_n)$ en $\mathbb{N}^n$. Definimos $\alpha \succ_{lex} \beta$ si la primera entrada de izquierda a derecha diferente de cero de la n-ada $\alpha - \beta \in \mathbb{N}^n$ es positiva. Escribimos $x^\alpha \succ_{lex} x^\beta$, si $\alpha \succ_{lex} \beta$

Ejemplo 2.5. Al comparar $(1, 2, 0)$ y $(0, 3, 4)$, usando el orden lexicográfico, tendríamos que $(1, 2, 0) \succ_{lex} (0, 3, 4)$, porque $\alpha - \beta = (1, -1, -4)$.

Ejemplo 2.6. Si comparamos $(3, 2, 4)$ con $(3, 2, 1)$ tendríamos que $(3, 2, 4) \succ_{lex} (3, 2, 1)$ porque $\alpha - \beta = (0, 0, 3)$.

2.1.2. Orden Lexicográfico Graduado (Grlex)

Sean $\alpha, \beta \in \mathbb{N}^n$. Definimos $\alpha \succ_{grlex} \beta$ si $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, o $|\alpha| = |\beta|$ y $\alpha \succ_{lex} \beta$.

Ejemplo 2.7. Si comparamos $(1, 2, 3)$ con $(3, 2, 0)$ tendríamos que $(1, 2, 3) \succ_{grlex} (3, 2, 0)$ porque $|(1, 2, 3)| > |(3, 2, 0)|$.

Ejemplo 2.8. Si comparamos $(1, 2, 4)$ con $(1, 1, 5)$ tendríamos que $(1, 2, 4) \succ_{grlex} (1, 1, 5)$ porque $|(1, 2, 4)| = |(1, 1, 5)|$ y $(1, 2, 4) \succ_{lex} (1, 1, 5)$

2.1.3. Orden Lexicográfico Graduado Reverso (Grevlex)

Sean $\alpha, \beta \in \mathbb{N}^n$. Definimos $\alpha \succ_{grevlex} \beta$ si $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, o $|\alpha| = |\beta|$ y la primera entrada de derecha a izquierda distinta de la n-ada diferencia $\alpha - \beta \in \mathbb{N}^n$ es negativa.

Ejemplo 2.9. Si comparamos $(4, 7, 1)$ con $(4, 2, 3)$ tendríamos que $(4, 7, 1) \succ_{grevlex} (4, 2, 3)$ porque $|(4, 7, 1)| = 12 > |(4, 2, 3)| = 9$

Ejemplo 2.10. Si comparamos $(1, 5, 2)$ con $(4, 1, 3)$ tendríamos que $(1, 5, 2) \succ_{grevlex} (4, 1, 3)$ porque $|(1, 5, 2)| = 8 = |(4, 1, 3)|$ y $(1, 5, 2) - (4, 1, 3) = (-3, 4, -1)$

Observación 1. A pesar de que el *grlex* y el *grevlex* usan ambos el orden total, lo que los diferencia es el peso que les da a las variables. El *grlex* les da más peso a las de la izquierda y el *grevlex* a los de la derecha; aunque puede pasar que

$$x^5yz \succ_{grlex} x^4yz^2$$

y

$$x^5yz \succ_{grevlex} x^4yz^2$$

Para hablar de un orden en los polinomios, es necesario fijarse en el orden de cada uno de los monomios. Esto motiva la siguiente definición:

Definición 2.11. Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio no cero en $\mathbb{K}[x_1, ..., x_n]$ y sea $\succ$ un orden monomial.

i) El **multigrado** de f es:

$$multigr(f) = \text{máx}\{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0\}$$

(el máximo es tomado con respecto al orden monomial $\succ$)

ii) El **coeficiente líder** de f es

$$LC(f) = a_{multigr(f)} \in k$$

iii) El **monomio líder** de f es

$$LM(f) = x^{multigr(f)}$$

con coeficiente 1.

iv) El **término líder** de f es

$$LT(f) = LC(f) \cdot LM(f)$$

Ejemplo 2.12. Sea $f = 2xy^2z - z^2 - 5x^3 + 8x^2z^2 \in \mathbb{R}[x, y, z]$. De esta forma, la representación de xy^2z en $\mathbb{N}^3$ es $(1, 2, 1)$, la de z^2 es $(0, 0, 2)$, la de x^3 es $(3, 0, 0)$ y la de x^2z^2 es $(2, 0, 2)$. Al usar $\succ_{lex}$, tendríamos:

$$multigr(f) = (3, 0, 0)$$
$$LC(f) = -5$$
$$LM(f) = x^3$$
$$LT(f) = -5x^3$$

De ahora en adelante (a menos de que algo distinto se especifique), se supondrá algún orden monomial fijo.

2.2. Algoritmo de la división en $\mathbb{K}[x_1, \ldots, x_n]$

La idea básica del algoritmo de la división en $\mathbb{K}[x_1, \ldots, x_n]$ es la misma que en caso de $\mathbb{K}[x]$: queremos cancelar el término principal de f (con respecto a un orden monomial fijo) por multiplicación de algún f_i apropiado y restar. Entonces este monomio (que es el cociente) llega a ser un término en el correspondiente q_i.

Teorema 2.13 (Algoritmo de la división en $\mathbb{K}[x_1, \ldots, x_n]$)**.** *Sea $\succ$ un orden monomial sobre $\mathbb{N}^n$, y sea $F = (f_1, \ldots, f_s)$ una s-ada ordenada de polinomios en $\mathbb{K}[x_1, \ldots, x_n]$. Entonces dado $f \in \mathbb{K}[x_1, \ldots, x_n]$ existen $q_i, r \in \mathbb{K}[x_1, \ldots, x_n]$, tales que*

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

y $r = 0$ o r es combinación lineal, con coeficientes en $\mathbb{K}$, de monomios, ninguno de los cuales es divisible por algún $LT(f_1), \ldots, LT(f_s)$. Llamamos a r el residuo de f bajo la división por F. Más aún, si $q_if_i \neq 0$, entonces

$$multigr(f) \geq multigr(q_if_i)$$

Demostración. Ver [3]. □

Ejemplo 2.14. Al dividir el polinomio $f = x^2y + xy^2 + y^2$ entre $f_1 = xy - 1$ y $f_2 = y^2 - 1$, usando $\succ_{lex}$, se obtiene:

$$
\begin{array}{rl}
 & q_1 : x + y \\
 & q_2 : \\
f_1 = xy - 1 & \overline{} \\
f_2 = y^2 - 1 & \left) \begin{array}{l} x^2y + xy^2 + y^2 \\ x^2y - x \end{array} \right. \\
 & \overline{} \\
 & \begin{array}{l} xy^2 + x + y^2 \\ xy^2 - y \end{array} \\
 & \overline{} \\
 & x + y^2 + y
\end{array}
$$

y ya no es posible continuar con la división, puesto que $LT(x + y^2 + y) = x$ no es divisible por ninguno de los términos líderes $LT(f_1) = xy$ y $LT(f_2) = y^2$. Pero $x + y^2 + y$ no es el residuo, porque y^2 es divisible por $LT(f_2)$.

Para resolver el problema, se crea una "columna de residuos" donde se saca al término que no es divisible por ninguno de los $LT(f_i)$ y se continua la división hasta que el residuo cumple con la condición de no ser divisible por $LT(f)$.

$$
\begin{array}{rlll}
 & q_1 : x + y & & \\
 & q_2 : & & \underline{r} \\
xy - 1 & \overline{} & & \\
y^2 - 1 & \left) \begin{array}{l} x^2y + xy^2 + y^2 \\ x^2y - x \end{array} \right. & & \\
 & \overline{} & & \\
 & \begin{array}{l} xy^2 + x + y^2 \\ xy^2 - y \end{array} & & \\
 & \overline{} & & \\
 & x + y^2 + y & & \\
 & \overline{} & & \\
 & y^2 + y & \longrightarrow & x
\end{array}
$$

De esta manera, ya es posible continuar con la división, porque el $LT(y^2 + y) = y^2$ es divisible por $LT(f_2) = y^2$:

$$
\begin{array}{rl|l}
 & q_1 : x+y & \\
 & q_2 : 1 & r \\
\hline
xy-1 & x^2y+xy^2+y^2 & \\
y^2-1 & x^2y-x & \\
\hline
 & xy^2+x+y^2 & \\
 & xy^2-y & \\
\hline
 & x+y^2+y & \\
\hline
 & y^2+y & \longrightarrow \quad x \\
 & y^2-1 & \\
\hline
 & y+1 & \\
\hline
 & 1 & \longrightarrow \quad x+y \\
\hline
 & 0 & \longrightarrow \quad x+y+1
\end{array}
$$

Por tanto,

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

Observación 2. El algoritmo en una sola indeterminada proporciona un único residuo. Caso contrario es el de varias indeterminadas donde el orden en cómo se toman los f_i importa, por lo cual pueden obtenerse distintos residuos.

Ejemplo 2.15. Al dividir $f = xy^2 - x$ entre $f_1 = xy - 1$ y $f_2 = y^2 - 1 \in \mathbb{K}[x, y]$ con el orden lexicográfico, podemos hacerlo de dos formas: $F = (f_1, f_2)$ o $F = (f_2, f_1)$. Si tomamos el primer caso, esto da como resultado

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

Sin embargo, con $F = (f_2, f_1)$ se tiene como resultado

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

El primer cálculo mostraría que $f \notin \langle f_1, f_2 \rangle$, pero el segundo cálculo muestra que $f \in \langle f_1, f_2 \rangle$.

Se puede decir entonces que en el caso de una indeterminada, la forma de decidir si un polinomio pertenece o no pertenence a un ideal es sencilla, puesto que se sigue inmediatamente del algoritmo de la división. En el caso de varias indeterminadas lo que se tendría es una condición *suficiente* (que $r = 0$) para determinar que el polinomio esté en el ideal, mas no *necesaria* para estar en el ideal: El residuo puede no dar cero, y aún así, estar en el ideal.

2.3. Bases de Gröbner

El ejemplo anterior mostró que el algoritmo de la división en $\mathbb{K}[x_1, \ldots, x_n]$ está lejos de ser perfecto, y consecuencia de ello, el problema de la pertenencia de un ideal está parcialmente sin resolver. De hecho, el algoritmo recibe su máxima potencialidad cuando se acopla con las bases de Gröbner. Sean $I \subseteq R$ un ideal no cero y $G = \{g_1, \ldots, g_t\} \subseteq I$. Denotaremos por $LT(I)$ al conjunto de términos líderes no cero de I, es decir:

$$LT(I) = \{cx^\alpha \text{ para algún } f \in I - \{0\} \text{ con } LT(f) = cx^\alpha\}$$

De esta manera, denotaremos por $\langle LT(I)\rangle$ el ideal generado por los elementos de $LT(I)$.

Definición 2.16 (Base de Gröbner)**.** Un subconjunto finito $G = \{g_1, \ldots g_t\}$ de un ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ diferente de $\{0\}$ es llamado Base de Gröbner, si:

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

El siguiente teorema muestra que las Bases de Gröbner no tienen los mismos problemas que se han venido evidenciando del algoritmo de la división en $\mathbb{K}[x_1, \ldots, x_n]$.

Teorema 2.17. *Sea $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ un ideal y sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I. Entonces, dado $f \in \mathbb{K}[x_1, \ldots, x_n]$, existe un único residuo $r \in \mathbb{K}[x_1, \ldots, x_n]$ con las siguientes dos propiedades:*

i) Ningún término de r es divisible por $LT(g_1), \ldots,$ o $LT(g_t)$.

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

En particular, r es el residuo de la división de f por G no importando cómo los elementos de G se listen cuando se use el algoritmo de la división.

Demostración. El algoritmo de la división da cuenta de la existencia de tal r. Tenemos que $f = q_1g_1 + \cdots + q_tg_t + r$, donde r satisface (i). También satisface (ii) porque $g = q_1g_1 + \cdots + q_tg_t \in I$. Para la unicidad, sean $r, r' \in \mathbb{K}[x_1, \ldots, x_n]$ tales que $f = g + r = g' + r'$, que satisfacen (i) y (ii). Entonces $r - r' = g' - g \in I$. Así que si $r \neq r'$, entonces $LT(r - r') \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Como consecuencia del algoritmo de la división (2.13), no es difícil ver que un monomio pertenece a un ideal si es divisible por alguno de sus generadores, por tanto se sigue que $LT(r - r')$ es divisible por uno de los $LT(g_1), \ldots, LT(g_t)$. Así que $r - r' = 0$, porque ninguno de los términos, r y r' son divisibles por algún $LT(f_i)$, por definición. Luego $r = r'$. □

2.4. ¿Cómo se construye una base de Gröbner?

Sean $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ polinomios no nulos. Sean $\alpha = multigr(f)$, $\beta = multigr(g)$ y $\gamma = (\gamma_1, \ldots, \gamma_n)$ donde $\gamma_i = \max(\alpha_i, \beta_i)$ para cada i. Definimos:

Definición 2.18 (Mínimo Común Múltiplo y S-Polinomios). i) x^γ como el **mínimo común múltiplo** de $LM(f)$ y $LM(g)$, y escribimos $x^\gamma = mcm\,(LM(f), LM(g))$.

ii) El **S-Polinomio** de f y g es la combinación

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

2.4.1. Criterio y Algoritmo de Buchberger

Existen diversos algoritmos para construir una base de Gröbner. Aquí expondremos el algoritmo clásico que fue el que planteó Buchberger en su tesis. Para entender cómo trabaja el algoritmo, se enuncia un importante lema llamado Criterio de Buchberger:

Lema 2.19 (Criterio de Buchberger). *Sea I un ideal polinomial. Entonces una base $G = \{g_1, ..., g_t\}$ de I es base de Gröbner de I si y sólo si para todos los pares $i \neq j$, el residuo de la división de $S(g_i, g_j)$ por G (listados en cualquier orden) es cero.*

Demostración. Ver [3]. □

A continuación, se expone el algoritmo para obtener una base de Gröbner:

Teorema 2.20 (Algoritmo de Buchberger para construir Bases de Gröbner). *Sea $I = \langle f_1, ..., f_s\rangle \neq \langle 0\rangle$ un ideal polinomial. Entonces una base de Gröbner para I puede ser construida en un número finito de pasos a través del siguiente algoritmo, donde denotamos por $\overline{f}^F$ al resto de la división de f por F.:*

Input: $F = (f_1, ..., f_s)$
Output: a Groebner basis $G = (g_1, ...g_t)$ for I, with $F \subseteq G$
$G := F$
REPEAT
  $G' := G$
  FOR each pair $\{p, q\}$, $p \neq q$ *in* G' *DO*
    $S := \overline{S(p,q)}^{G'}$
    IF $S \neq 0$ *THEN* $G' = G \cup \{S\}$
UNTIL $G = G'$

Demostración. Pasaremos a explicar en qué consiste el algoritmo. Una prueba de este puede encontrarse en [3]. En términos generales, el criterio de Buchberger constituye la piedra angular de este algoritmo: primero, se supone que el conjunto inicial G es Base de Gröbner: si esto es cierto, el algoritmo de Buchberger garantiza que $\overline{S(g_i, g_j)}^G = 0$ para todo $i \neq j$. En caso que estos residuos no sean cero, se procede a agregar estos residuos a lo que supusimos ser base de Gröbner. Precisamente es lo importante del algoritmo: al estar estos elementos en el conjunto, el cálculo de los residuos ya serán cero. Se sigue este

procedimiento, hasta que todos los residuos de los S-Polinomios entre la base de Gröbner den cero. Por último, la base resultante será la base de Gröbner de para I. □

Ejemplo 2.21. Sea $I = \langle x^2 - 1, y^2 - 1, x^2 - y\rangle \subseteq \mathbb{C}[x, y]$ con $\succ_{lex}$.

Sea $G' = \{x^2 - 1, y^2 - 1, x^2 - y\}$. Calculamos:

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

$$\overline{S(x^2 - 1, y^2 - 1)}^{G'} = 0$$
$$\overline{S(x^2 - 1, x^2 - y)}^{G'} = y - 1$$
$$\overline{S(y^2 - 1, x^2 - y)}^{G'} = y - 1$$

Como algunos S-Polinomios nos dieron distintos de 0, debemos agregarlos a G'. Así:

$$G'' = \{\underbrace{x^2 - 1, y^2 - 1, x^2 - y}, y - 1\}$$

De nuevo calculamos los S-Polinomios:

$$\overline{S(x^2 - 1, y^2 - 1)}^{G'} = 0$$
$$\overline{S(x^2 - 1, x^2 - y)}^{G'} = 0$$
$$\overline{S(y^2 - 1, x^2 - y)}^{G'} = 0$$
$$\overline{S(x^2 - 1, y - 1)}^{G'} = 0$$
$$\overline{S(y^2 - 1, y - 1)}^{G'} = 0$$
$$\overline{S(x^2 - y, y - 1)}^{G'} = 0$$

Como los residuos dan cero, podemos decir que

$$\{x^2 - 1, y^2 - 1, x^2 - y, y - 1\}$$

es base de Gröbner para I.

3. Algunas aplicaciones de las Bases de Gröbner

Después de saber lo que son las Bases de Gröbner y algunos resultados básicos, veamos algunas aplicaciones de estas:

3.1. Pertenencia de un polinomio a un ideal

Habíamos dicho que el problema de la pertenencia de un polinomio a un ideal, estaba parcialmente resuelto porque sólo teníamos un algoritmo que lo permitía para $\mathbb{K}[x]$. Con las bases de Gröbner, se puede generalizar el resultado a varias indeterminadas.

Corolario 3.1 (Pertenencia de un polinomio en un ideal)**.** *Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner de un ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ y $f \in \mathbb{K}[x_1, \ldots, x_n]$. Entonces, $f \in I$ si y sólo si el residuo de la división de f entre G es cero.*

Demostración. Sea $f \in I$. Entonces, si $I = \langle G \rangle = \langle g_1, \ldots, g_t \rangle$, entonces existen $q_1, \ldots, q_t \in \mathbb{K}[x_1, \ldots, x_n]$ tal que:

$$f = q_1 g_1 + \cdots + q_t g_t$$

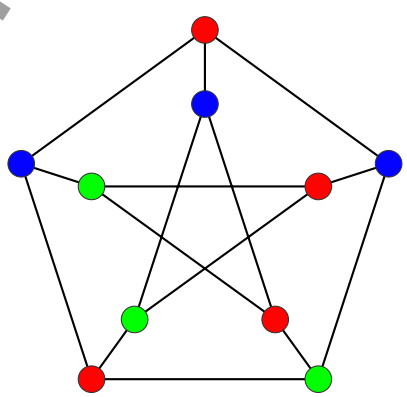
Por otro lado, el algoritmo de la división en $\mathbb{K}[x_1, \ldots, x_n]$ dice que $f = q_1 g_1 + \cdots + q_t g_t + r$, luego $r = 0$. El otro lado de la implicación es trivial: si f entre G es cero, entonces $f = q_1 g_1 + \cdots + q_t g_t$. Luego, $f \in \langle g_1, \ldots, g_t \rangle$. □

De esta manera, una forma para determinar si un polinomio f pertenece o no a un ideal I es calcular una Base de Gröbner G para I (con respecto a cualquier orden monomial $\succ$), y dividir el polinomio entre G usando el Algoritmo de la División. Si el residuo es cero, entonces $f \in I$.

3.2. Coloración de gráficas

Una gráfica Γ es un par (V, E) que consiste de un conjunto V de **vértices** y un conjunto E (disjunto de V), de **aristas**, junto con una función de incidencia ψ_Γ que asocia a cada arista de Γ un par no ordenado (no necesariamente distintos) de vértices de Γ. Una parte importante de la teoría de gráficas se refiere a la coloración de vértices de gráficas. El problema de coloración consiste en lo siguiente: Dada una gráfica $\Gamma = (V, E)$ asignar un conjunto de colores tal que no existan dos vértices adyacentes que tengan el mismo color.

Ejemplo 3.2. La siguiente gráfica corresponde a la Gráfica de Petersen:



Esta es una gráfica con 10 vértices y 15 aristas. Aquí, la gráfica de Petersen está coloreada con 3 colores. Este es el mínimo número de colores con el cual pueden colorearse sus vértices.

Si bien, la gráfica del ejemplo anterior puede colorearse de varias maneras - con 10 colores, inclusive- interesa el número mínimo de colores con el cual esta gráfica puede colorearse. Esto motiva la siguiente definición:

Definición 3.3. Una gráfica Γ es k-coloreable si existe una asignación de k colores distintos a cada uno de los vértices de manera que no haya dos vértices adyacentes que tengan el mismo color. El mínimo número de colores con tal propiedad es llamado **número cromático**, y es denotado por $\chi = \chi(\Gamma)$.

Ejemplo 3.4. Si Γ es la gráfica de Petersen, entonces $\chi(\Gamma) = 3$.

Lo que se mostrará a continuación son algunas observaciones basadas en [1]. En este trabajo se relacionan algunos resultados de ideales en anillos de polinomios al problema de coloración. Para mostrar particularmente lo que concierne al problema de coloración, se define un polinomio asociado a la gráfica a partir de sus vértices.

Definición 3.5 (Polinomio e Ideal asociados a la gráfica)**.** Sea $\Gamma = (V, E)$ una gráfica, y sean $u, v \in V$ cualesquiera vértices de la gráfica. Entonces, el **polinomio de la gráfica**, denotado por f_Γ, es un elemento del anillo $\mathbb{C}[V]$ dado por:

$$f_\Gamma := \prod_{\{u,v\}\in E} (u - v)$$

Y el **ideal asociado a la gráfica**, denotado por I_Γ es el ideal dado por:

$$I_\Gamma := \langle v^k - 1 \rangle \text{ para todo } \ v \in V.$$

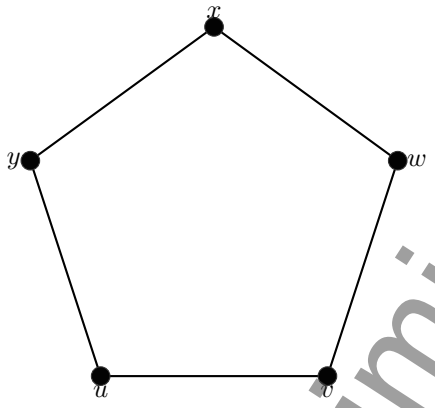
donde $k \in \mathbb{Z}^+$.

El problema de coloración se reduce a un problema de pertenencia de un polinomio a un ideal:

Teorema 3.6 (Criterio para k-coloración)**.** *Sean f_Γ como en la definición anterior y $k \in \mathbb{Z}^+$ fijo. Entonces, el grafo Γ es k-coloreable si y sólo si $f_\Gamma \notin I$.*

Demostración. Ver [1]. □

Ejemplo 3.7. El siguiente ejemplo es puramente ilustrativo, puesto que el número cromático de las gráficas ciclo es bien conocido. Sea $\Gamma = C_5$.



El polinomio asociado a la gráfica f_G pertenece al anillo $\mathbb{C}[u, v, w, x, y]$. Este es:

$$f_{C_5} = (u - v)(v - w)(w - x)(x - y)(y - u)$$

Claramente, esta gráfica no es ni 1-colorable.

Tampoco es 2-coloreable, porque:

$$\begin{aligned} f_{C_5} &= (u - v)(v - w)(w - x)(x - y)(y - u) \\ &= (u^2 - 1)(-vwx + vwy + vx^2 - vxy + w^2x - w^2y - wx^2 + wxy) + \\ &\quad (v^2 - 1)(uwx - uwy - ux^2 + uxy - wxy + wy^2 + x^2y - xy^2) + \\ &\quad (w^2 - 1)(-uvx + uvy - uxy + uy^2 + vxy - vy^2 + x - y) + \\ &\quad (x^2 - 1)(uvw - uvy + uwy - vwy - u + v - w + y) + \\ &\quad (y^2 - 1)(-uvw + uvx - uwx + vwx + u - v + w - x) \end{aligned}$$

lo que significa que $f_{C_5} \in \langle u^2 - 1, v^2 - 1, w^2 - 1, x^2 - 1, y^2 - 1\rangle$. Así $\Gamma = C_5$ no es 2-coloreable.

Es conocido que $\chi(C_5) = 3$, y vamos a corroborarlo usando el teorema anterior. Para $k = 3$, el ideal asociado a la gráfica es:

$$I_{C_5} = \langle u^3 - 1, v^3 - 1, w^3 - 1, x^3 - 1, y^3 - 1\rangle$$

No es difícil ver, que bajo el orden lexicográfico, IC_5 es Base de Gröbner. Por tanto, queda por ver si f_{C_5} está o no está en I_{C_5}. Al expandir f_{C_5} en términos,

tenemos que:

$$\begin{aligned} f_{C_5} = & -u^2vwx + u^2vwy + u^2vx^2 - u^2vxy + u^2w^2x - u^2w^2y - \\ & u^2wx^2 + u^2wxy + uv^2wx - uv^2wy - uv^2x^2 + uv^2xy - \\ & uvw^2x + uvw^2y + uvwx^2 - uvwy^2 - uvx^2y + uvxy^2 - \\ & uw^2xy + uw^2y^2 + uwx^2y - uwxy^2 - v^2wxy + v^2wy^2 + \\ & v^2x^2y - v^2xy^2 + vw^2xy - vw^2y^2 - vwx^2y + vwxy^2 - \\ & uwxy^2 - v^2wxy + v^2wy^2 + v^2x^2y - v^2xy^2 + vw^2xy - \\ & vw^2y^2 - vwx^2y + vwxy^2 \end{aligned}$$

De esta manera, puede verse que ningún término de f_G tiene potencia cúbica. Lo que implica que no hay manera de que f_{C_5} pertenezca al ideal I_{C_5}. Como,

$$f_{C_5} \notin I_{C_5} = \langle u^3 - 1, v^3 - 1, w^3 - 1, x^3 - 1, y^3 - 1 \rangle$$

el grafo $\Gamma = C_5$ es 3-coloreable.

Agradecimientos
Mi más sinceros agradecimientos al Dr. Jesús Romero Valencia de la Universidad Autónoma de Guerrero por su gran contribución en la elaboración de este documento, e iniciar mi interés en el estudio de las Bases de Gröbner. Al CONACYT por permitir una estancia de investigación en el CINVESTAV-IPN con el Dr. Carlos E. Valencia Oleta, al cual también le debo su gran apoyo.

Referencias

[1] A. Alon and M. Tarsi, *Colorings and orientations of graphs*, Combinatorica **12** (1992), 125.

[2] B. Buchberger, *An algorithm for finding a basis for the residue class ring of a zero-dimensional ideal*, Ph. D. Thesis, Univ. of Innsbruck, Math. Inst., 1965.

[3] D. Cox, J. Little, and O'Shea, *Ideals, varieties and algorithms*, Fourth Edition. Ungraduated Text in Mathematics. Springer-Verlag, New York, 2015.

[4] P. Gordan, *Newer beweis des hilbertschen satzes über homogene funktionen*, Nachrichten König. Ges. Der. Wiss. Zu Gött, 1899, 240-242.

[5] W. Gröbner, *über die algebraischen Eigenschaften der Integrale von linearen Differentialgleichungen mit konstanten Koeffizienten*, Monatsh. der Math. **47** (1393), 247–284.

[6] D. Hilbert, *über die theorie del algebraischen formen*, Math. Ann. **36** (1890), 473–534, Reprinted in Gesammelte Abhandlungen, Volume II, Chelsea, New York (1965).

[7] ———, *über die vollen invariantensysteme*, Math. Ann. **42** (1893), 313–373, Reprinted in: *Theory of Algebraic Invariants*, Cambridge University Press, Cambridge (1993).

[8] F. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. **26** (1927), 531–555.