Miscelánea Matemática **79** (2024) 11-22 SMM

DOI: https://doi.org/10.47234/mm.7903

Generalización del algoritmo de la división y bases de Gröbner

Kevin Duran
Departamento de Matemáticas
Universidad Autónoma Metropolitana, Unidad Iztapalapa
cbi2183012000@izt.uam.mx
y
Yuriko Pitones
Departamento de Matemáticas
Universidad Autónoma Metropolitana, Unidad Iztapalapa
ypitones@xanum.uam.mx

1. Introducción

La teoría de bases de Gröbner es una herramienta que permite abordar problemas de diferentes áreas de las matemáticas desde una perspectiva algorítmica y computacional y en las últimas décadas ha resultado ser de gran interés para la comunidad debido a las diversas aplicaciones que tiene. El contenido de este texto está dirigido a un público no especializado, principalmente a estudiantes con conocimientos básicos de álgebra moderna, el objetivo principal es acercar al lector desde un enfoque intuitivo a esta área de las matemáticas.

En los años 60, Bruno Buchberger [2, 4] y Heisuke Hironaka [9] introdujeron de manera independiente nuevos algoritmos para manipular sistemas de ecuaciones polinomiales que tienen como consecuencia el desarrollo de la teoría de bases de Gröbner, lo cual implica de manera directa una demostración constructiva del famoso teorema de la base de Hilbert, que coloquialmente se puede entender como que todo sistema infinito de ecuaciones polinomiales es equivalente a otro con un número finito de ecuaciones.

En este artículo para definir las bases de Gröbner analizaremos el problema de la *pertenencia*, esto es, de qué manera podemos determinar cuándo un polinomio pertenece a un ideal I del anillo de polinomios en n variables, este problema también está fuertemente relacionado con

Palabras clave: Algoritmo de la división, órdenes monomiales, bases de Gröbner.

el teorema de la base de Hilbert. El contenido es el siguiente: en la sección 1, se presentan algunos preliminares, definiciones y notación que se usará en todo el texto. En la sección 2, se introducen los órdenes monomiales y se presenta el algoritmo generalizado de la división de polinomios, que resulta ser en gran medida la base para desarrollar esta teoría, en la sección 3, se definen las bases de Gröbner y se muestran algunos resultados clásicos y en la sección 4, se mencionan de forma panorámica algunas aplicaciones de las bases de Gröbner.

2. Preliminares

Esta sección contiene un poco de notación y algunas definiciones que se usan en el contenido de este artículo. También plantearemos el problema de la *pertenencia*, lo presentamos como motivación para generalizar el algoritmo de la división de polinomios y consecuentemente introducir las bases de Gröbner.

Denotaremos por R al anillo de polinomios en n variables sobre un campo $\mathbb{K}$, esto es, $R = \mathbb{K}[x_1, \ldots, x_n]$.

Definición 2.1. Un ideal del anillo R es un subconjunto no vacío $I \subset R$ que satisface:

1. I es un subgrupo de $(R, +)$.
2. Para todo $f \in R$ y todo $g \in I$ se tiene que $fg \in I$ y $gf \in I$.

Denotaremos por $\langle f \rangle$ al ideal generado por $f \in R$.

Definición 2.2. Sea $f \in R$, la variedad definida por f, es el conjunto de todos los elementos $a \in \mathbb{K}^n$ tales que $f(a) = 0$, y se denota por $V(f) = \{a \in \mathbb{K}^n \mid f(a) = 0\}$.

En general, dados $f_1, \ldots, f_\ell \in R$, definimos $V(f_1, \ldots, f_\ell) = \{a \in \mathbb{K}^n \mid f_i(a) = 0 \text{ para } i = 1, \ldots, \ell\}$.

Si consideramos un ideal $I = \langle f_1, \ldots, f_\ell \rangle \subset R$ generado por ℓ elementos, su variedad $V(I)$, consiste de las soluciones del sistema infinito, $f = 0$ con $f \in I$. Por otro lado, podemos considerar las soluciones del sistema finito determinado por los generadores $f_1 = 0, \ldots, f_\ell = 0$, es fácil ver que una solución del sistema infinito es una solución del sistema finito, pues $f_i \in I$ para $i = 1, \ldots, \ell$, esto también es consecuencia del teorema de la base de Hilbert. Además, si $a \in \mathbb{K}^n$ es una solución del segundo sistema (finito) y f un elemento de I, entonces $f(a) = 0$ pues $f = \sum_{i=1}^{\ell} u_i f_i$ con $u_i \in R$. Por lo tanto, $V(I) = V(f_1, \ldots, f_\ell)$.

Observación 2.3. Un ideal puede tener distintos conjuntos generadores con distinta cardinalidad.

Por ejemplo, en $\mathbb{K}[x, y]$, $\langle x + y, x \rangle = \langle x, y \rangle = \langle x + xy, x^2, y^2, y + xy \rangle$.

Un caso particular es cuando en un anillo todos los ideales son generados por un solo elemento, a tales anillos se les llama dominios de ideales principales y se denotan como DIP. La definición general es la siguiente.

Definición 2.4. Un anillo R es un dominio de ideales principales si para todo $f, g \neq 0$ sucede que $fg \neq 0$ y $gf \neq 0$ y todo ideal $I \subset R$ es de la forma $I = \langle f \rangle$ con $f \in R$, esto es, I es generado por un solo elemento.

Entonces, si logramos obtener un «mejor» conjunto de generadores del ideal $I = \langle f_1, \ldots, f_\ell \rangle$ (el cual será llamado base de Gröbner para I), tendremos una «mejor» representación de la variedad $V(f_1, \ldots, f_\ell)$, y por «mejor» nos referimos a un conjunto de generadores que nos permita entender la estructura algebraica de $I = \langle f_1, \ldots, f_\ell \rangle$.

El siguiente resultado es una versión del teorema de la base de Hilbert, el cual nos garantiza que todo ideal en el anillo R es finitamente generado. Por lo tanto nos interesa describir un algoritmo que nos permita calcular un conjunto de generadores para un ideal en R.

Teorema 2.5. [6, teo. 2.1.1] *Sea I un ideal de R, entonces existen polinomios $f_1, \ldots, f_\ell \in R$ tales que $I = \langle f_1, \ldots, f_\ell \rangle$.*

Plantearemos ahora el problema de la *pertenencia*, conociendo un conjunto de generadores para un ideal I, esto es, $I = \langle f_1, \ldots, f_\ell \rangle$ podemos preguntarnos lo siguiente:

1. Sea $f \in R$, ¿bajo qué condiciones, $f \in I$?
2. Si $f \in I$, ¿de qué manera podemos encontrar $u_1, \ldots, u_\ell \in R$ tal que $f = u_1 f_1 + \cdots + u_\ell f_\ell$?

En un contexto geométrico, esto es equivalente a preguntarse si, dada una variedad algebraica $V(f_1, \ldots, f_\ell) \subset \mathbb{K}^n$, ¿podemos determinar si esta variedad está contenida o no en $V(f)$?

Estas preguntas se pueden responder fácilmente usando el algoritmo de la división cuando $R = \mathbb{K}[x]$ con $\mathbb{K}$ un campo, sin embargo, este método falla cuando consideramos polinomios en más de una variable, pues para $R = \mathbb{K}[x_1, \ldots, x_n]$ con $n \geq 2$, R no es un dominio de ideales principales.

3. Algoritmo generalizado de la división

Esta sección la comenzaremos definiendo el grado de un polinomio y el algoritmo de la división para polinomios de una sola variable e introducimos la noción de órdenes monomiales, estos últimos nos permiten generalizar dicho algoritmo.

Definición 3.1. Sea $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{K}[x]$ un polinomio en la variable x con coeficientes en $\mathbb{K}$, el grado del polinomio f es el exponente más grande de la variable x que tiene coeficiente distinto de cero para algún $0 \leq i \leq n$, y se denota como $\mathrm{gr}(f)$.

Si consideramos polinomios en $\mathbb{K}[x]$, podemos resolver los dos problemas anteriores utilizando el algoritmo de la división clásico.

Dados $f, g \in \mathbb{K}[x]$ existen únicos $q, r \in \mathbb{K}[x]$ tales que,

$$f = gq + r \ \textit{con}\ r = 0 \ \textit{o}\ \mathrm{gr}(r) < \mathrm{gr(g)}.$$

Entonces, $f \in \langle g \rangle$ siempre que el residuo de la división de f entre g es igual a cero y además q es el polinomio buscado en la pregunta (2) que hemos planteado anteriormente. Una de las razones que justifican el uso del algoritmo de la división es la siguiente proposición.

Proposición 3.2. [6, cor. 4] $\mathbb{K}[x]$ *es un dominio de ideales principales.*

Ahora veremos cómo calcular un generador para ideales en $\mathbb{K}[x]$.

Definición 3.3. Sea $\mathbb{K}[x]$ el anillo de polinomios en la variable x, y sean $f, g \in \mathbb{K}[x]$. Un elemento $u \in \mathbb{K}[x]$ es el máximo común divisor de f y g y se denota como $\mathrm{mcd}(f, g)$ si se satisface lo siguiente:

1. u divide a f y a g, usualmente lo denotamos como: $u|f$ y $u|g$.
2. Siempre que $h|f$ y $h|g$ se tiene que $h|u$.

Proposición 3.4. [1, prop. 1.3.5] *Sean* $f_1, f_2 \in \mathbb{K}[x]$ *distintos de cero, entonces* $\langle f_1, f_2 \rangle = \langle \mathrm{mcd}(f_1, f_2) \rangle$.

Ejemplo 3.5. Sean $f_1 = x^3 - 3x + 2$ y $f_2 = x^2 - 1$ polinomios en $\mathbb{Q}[x]$, utilizando el algoritmo de la división determinamos el $\mathrm{mcd}(f_1, f_2)$ para encontrar $g \in \mathbb{Q}[x]$ tal que $\langle f_1, f_2 \rangle = \langle g \rangle$.

Observa que,

$$f_1 = x^3 - 3x + 2 = (x-1)^2 (x+2),$$
$$f_2 = x^2 - 1 = (x-1)(x+1).$$

Entonces el $\mathrm{mcd}(f_1, f_2) = x - 1$, y por lo tanto $\langle x^3 - 3x + 2, x^2 - 1 \rangle = \langle x - 1 \rangle$.

Consecuentemente, tenemos la siguiente proposición.

Proposición 3.6. [1, prop. 1.3.8] *Sean* $f_1, \ldots, f_\ell$ *polinomios en* $\mathbb{K}[x]$ *entonces:*

1. $\langle f_1, \ldots, f_\ell \rangle = \langle \mathrm{mcd}(f_1, \ldots, f_\ell) \rangle$.
2. *Si* $\ell \geq 3$ *entonces* $\mathrm{mcd}(f_1, \ldots, f_\ell) = \mathrm{mcd}(f_1, \mathrm{mcd}(f_2, \ldots, f_\ell))$.

Entonces, para ideales en $\mathbb{K}[x]$ es relativamente «fácil» encontrar un «mejor» conjunto generador del ideal, basta usar el algoritmo de la

división para encontrar el mcd de un conjunto de polinomios en $\mathbb{K}[x]$, y consecuentemente resolvemos el problema de la *pertenencia*.

Para generalizar estas ideas a polinomios que dependen de un número finito de variables en la siguiente sección introducimos los órdenes monomiales.

3.1 Órdenes monomiales

En el algoritmo de la división para el caso de una variable, implícitamente ordenamos los términos de los polinomios de forma creciente o decreciente respecto al grado, pues al realizar una división, nuestra intención es siempre eliminar el término de mayor grado. Sin embargo, la idea de orden en el anillo R ya no es clara.

Por ejemplo, consideremos el polinomio $f = x_1^3x_4^2 + x_1^4x_4$ ¿cómo podemos ordenar los términos de f? Intentar ordenarlos por su grado no es una opción viable.

Para presentar una generalización del algoritmo de la división en R, lo primero será ordenar los monomios de cualquier polinomio $f \in R$.

El conjunto de monomios lo denotaremos como $\mathbb{T}^n$, es decir $\mathbb{T}^n = \{x_1^{\beta_1} \cdot\cdot\cdot\cdot x_n^{\beta_n} | \beta_i \in \mathbb{N}, i = 1, \ldots, n\}$. Para denotar un monomio en $\mathbb{T}^n$ usaremos la siguiente notación: $x^\beta := x_1^{\beta_1} \cdot\cdot\cdot\cdot x_n^{\beta_n}$, donde $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ es llamado vector de exponentes.

En el conjunto anterior definiremos un orden, el cual será un orden total, esto es, dados $x^\alpha, x^\beta \in \mathbb{T}^n$ se cumple exactamente una de las siguientes relaciones, $x^\alpha < x^\beta, x^\alpha = x^\beta$ o $x^\alpha > x^\beta$, es decir, cualquier par de elementos en $\mathbb{T}^n$, deben ser comparables.

Definición 3.7. Un orden monomial en $\mathbb{T}^n$ es un orden total $<$ que satisface las siguientes dos condiciones:

1. $1 < x^\beta$, para todo $x^\beta \in \mathbb{T}^n$ con $x^\beta \neq 1$.
2. Si $x^\alpha < x^\beta$, entonces $x^\alpha x^\gamma < x^\beta x^\gamma$ para todo $x^\gamma \in \mathbb{T}^n$.

Un ejemplo clásico de orden monomial es el siguiente.

Ejemplo 3.8. Definimos el orden lexicográfico en $\mathbb{T}^n$ (con $x_1 > \ldots > x_n$) como sigue:

$$x^\alpha < x^\beta \iff \begin{cases} \text{la primera coordenada no cero de izquierda a} \\ \text{derecha en } \beta - \alpha \text{ es positiva.} \end{cases}$$

El siguiente teorema considera que usando un orden monomial en el conjunto $\mathbb{T}^n$, siempre se pueden comparar todos sus elementos entre sí.

Teorema 3.9. [1, teo. 1.4.6] *El conjunto $\mathbb{T}^n$, junto con un orden monomial es un conjunto bien ordenado.*

Si consideramos $f \in R$ expresado en la forma $f = a_1x^{\alpha_1} + \cdots + a_nx^{\alpha_n}$, donde cada $x^{\alpha_i} \in \mathbb{T}^n$ y $a_i \in \mathbb{K}$ y un orden monomial en $\mathbb{T}^n$, podemos comparar y reordenar sus monomios de tal forma que, el monomio líder de f, denotado como $\mathrm{lm}(f)$, es el monomio más grande respecto a ese orden, es decir, podemos escribir $\mathrm{lm}(f) = x^{\alpha_1}$ y el término líder, el cual denotaremos como $\mathrm{lt}(f)$ es $\mathrm{lt}(f) = a_1x^{\alpha_1}$.

Ejemplo 3.10. Sea $R = [x, y, z]$ y consideremos el polinomio $f = 3x^2z - 2x^3y^4 + 7x^2y^2z^3 - 9xy^3z^3$, determinemos el monomio líder respecto al orden lexicográfico con $x > y > z$.

Podemos escribir los vectores exponentes de cada monomio de f:

$$\alpha = (2, 0, 1), \beta = (3, 4, 0), \gamma = (2, 2, 3) \text{ y } \delta = (1, 3, 3).$$

Notemos que, $\beta - \alpha = (1, 4, -1)$, esto implica que, $x^2z < x^3y^4$, por otro lado, $\beta - \gamma = (1, 2, -3)$, así , $x^2y^2z^3 < x^3y^4$ y $\beta - \delta = (2, 1, -3)$, por lo tanto, $xy^3z^3 < x^3y^4$, y consecuentemente $\mathrm{lm}(f) = x^3y^4$.

El lector puede encontrar más información y ejemplos sobre órdenes monomiales en las siguientes referencias [1, 7, 6, 11, 12].

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

Ahora que sabemos ordenar los términos de cualquier polinomio en R, podemos dar una solución parcial a los problemas mencionados en la sección 2, extendiendo el algoritmo de la división para polinomios en n variables.

La idea básica de este algoritmo es la misma que para el caso de polinomios en una sola variable, ahora queremos dividir un polinomio f entre polinomios $f_1, \ldots, f_\ell$ cancelando términos de f y usaremos los términos líderes de cada f_i.

Definición 3.11. Dados un orden monomial y $f, g, h \in R$ con $g \neq 0$, decimos que f se reduce a h módulo g en un paso, y se denota como $f \xrightarrow{g} h$, si y solo si $\mathrm{lt}(g)$ divide a un monomio X de f y

$$h = f - \frac{X}{\mathrm{lt}(g)}g.$$

Ejemplo 3.12. Sea $f = 6x^2y - x + 4y^3 - 1$ y $g = 2xy + y^3$ polinomios en $\mathbb{Q}[x, y]$ con el orden lexicográfico, $f \xrightarrow{g} h$ con $h = -3xy^3 - x + 4y^3 - 1$, pues en este caso $6x^2y$ es el término que eliminamos usando $\mathrm{lt}(g) = 2xy$, de hecho, $\mathrm{lt}(f) = 6x^2y$.

En este sentido, podemos pensar en h como el residuo de dividir f entre g.

Definición 3.13. Sean f, h y $f_1, \ldots, \ldots, f_\ell$ polinomios en R con $f_i \neq 0$ para $i = 1, \ldots, \ell$ y $F = \{f_1, \ldots, f_\ell\}$, decimos que f se reduce a h módulo F, y se denota como $f \xrightarrow{F} h$, si y solo si existe un conjunto de índices $i_1, \ldots, i_t \in \{1, \ldots, \ell\}$ y una secuencia de polinomios $h_1, \ldots, h_{t-1} \in R$ tal que

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Ejemplo 3.14. Sea $f = x^2y, f_1 = xy - x, f_2 = x^2 - y$ polinomios en $\mathbb{Q}[x, y]$ con el orden lexicográfico y $F = \{f_1, f_2\}$, entonces

$$f \xrightarrow{F} y$$

pues,

$$f \xrightarrow{f_1} x^2 \xrightarrow{f_2} y.$$

Definición 3.15. Sea $f \in R$ y $F = \{f_1, \ldots, f_\ell\}$ un conjunto de polinomios en R distintos de cero.

Si $f \xrightarrow{F} r$ y r no puede ser reducido módulo F, entonces llamamos a r un residuo de f respecto a F.

Este proceso de reducción nos brinda una idea general e intuitiva de cómo se puede generalizar el algoritmo de la división y destacamos que uno de los elementos importantes es la necesidad de establecer un orden monomial.

En general, el objetivo es dividir $f \in R$ entre $f_1, \ldots f_\ell \in R$, esto significa poder expresar f en la forma

$$f = u_1 f_1 + \cdots + u_\ell f_\ell + r,$$

donde los cocientes $u_1, \ldots, u_\ell$ y el residuo r son elementos de R.

Ejemplo 3.16. Dividiremos $f = xy^2 + 1$ entre $f_1 = xy + 1$ y $f_2 = y+1$ respecto al orden lexicográfico. Usaremos el esquema de la división para polinomios en una variable. La diferencia es que ahora hay varios divisores y cocientes, listando los divisores f_1, f_2 y los cocientes u_1, u_2 horizontalmente, tenemos;

$$\begin{array}{r} \quad u_1 = \quad u_2 = \\ xy+1, y+1 \overline{)\quad x\,y^2 \quad +1} \end{array}$$

Los términos líderes $\mathrm{lt}(f_1) = xy$ y $\mathrm{lt}(f_2) = y$ dividen a $\mathrm{lt}(f) = xy^2$, realizamos la división de f respecto a f_1, esto es, dividimos xy^2 entre xy, obteniendo y y luego restamos yf_1 de f, obteniendo:

$$\begin{array}{r|l} & u_1 = y \quad u_2 = \\ \hline xy^2 & +1 \\ xy^2 + & y \\ \hline & -y+1 \end{array} \qquad xy+1, y+1$$

Repetiremos el proceso para $-y+1$, pero utilizaremos $\mathrm{lt}(f_2)$, pues $\mathrm{lt}(f_1)$ no divide a $\mathrm{lt}(-y+1) = y$

$$\begin{array}{r|l} & u_1 = y \quad u_2 = -1 \\ \hline xy^2 & +1 \\ xy^2 + & y \\ \hline & -y+1 \\ & -y-1 \\ \hline & 2 \end{array} \qquad xy+1, y+1$$

Como $\mathrm{lt}(f_1)$ y $\mathrm{lt}(f_2)$ no dividen a 2, tenemos que $r = 2$ y hemos acabado. Así, podemos expresar $f = xy^2 + 1$ de la forma:

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

El ejemplo anterior es una ilustración de cómo funciona el algoritmo de división en varias variables. También nos muestra qué propiedad queremos que tenga el residuo, ninguno de sus términos debe ser divisible por el monomio líder de cualquier polinomio por los que estamos dividiendo, aquí podemos hacer referencia al procedimiento de reducción, esto significa que el residuo no puede ser reducido módulo el conjunto de polinomios que intervienen en la división, con esta motivación enunciamos la forma general del algoritmo de división.

Teorema 3.17. [6, teo. 3] *Sea $<$ un orden monomial en $\mathbb{T}^n$ y $F = \{f_1, \dots f_\ell\}$ un conjunto de polinomios en R, entonces todo $f \in R$ puede expresarse de la forma:*

$$f = u_1 f_1 + \ldots + u_\ell f_\ell + r,$$

donde $u_i, r \in R$ para $i = 1, \dots, \ell$, además, $r = 0$ o r es una combinación lineal de monomios con coeficientes en $\mathbb{K}$, ninguno de los cuales es divisible por $\mathrm{lt}(f_i)$ para $i = 1, \dots, \ell$.

Observación 3.18. Notemos que en el algoritmo de la división en R no se habla de la unicidad de los cocientes $u_1, \dots, u_\ell$ ni de la unicidad del residuo r, en realidad no la hay, observemos el ejemplo 3.16, si hubiésemos comenzado dividiendo $\mathrm{lt}(f)$ entre $\mathrm{lt}(f_2)$ obtendríamos que $u_2 = xy$ y $u_1 = -1$.

Por tanto, la no unicidad del residuo del teorema 3.17 impide usar el algoritmo directamente para resolver el problema de la pertenencia

de un polinomio a un ideal $I \subset R$. Si resulta que el residuo de dividir f entre $F \subset R$ es nulo, podremos concluir que $f \in I$, pero si $r \neq 0$ no podremos concluir nada. En la siguiente sección veremos que las bases de Gröbner nos ayudarán a solucionar este problema.

4. Bases de Gröbner

En esta sección introducimos la definición de bases de Gröbner y enunciamos algunos resultados que responderán a las preguntas planteadas en la sección 2.

Definición 4.1. Sea $I \in \mathbb{K}[x_1, \ldots, x_n]$ un ideal distinto de cero y $<$ un orden monomial fijo en $\mathbb{K}[x_1, \ldots, x_n]$. Entonces, el ideal inicial denotado por $\mathrm{LT}(I)$ es el conjunto de los términos líderes de elementos no cero de I, es decir:

$$\mathrm{LT}(I) = \{cx^\alpha | \text{ existe } f \in I \setminus \{0\} \text{ con } \mathrm{lt}(f) = cx^\alpha\}.$$

Denotamos por $\langle \mathrm{LT}(I) \rangle$ al ideal generado por los elementos de $\mathrm{LT}(I)$.

Ya hemos visto que los términos principales juegan un papel importante en el algoritmo de la división y como consecuencia tenemos lo siguiente; si tenemos un conjunto finito de generadores para I, digamos $I = \langle f_1, \ldots, f_\ell \rangle$, entonces en general $\langle f_1, \ldots, f_\ell \rangle$ y $\langle \mathrm{LT}(I) \rangle$ son ideales distintos. Por definición tenemos que $\mathrm{lt}(f_i) \in \mathrm{LT}(I) \subset \langle \mathrm{LT}(I) \rangle$, esto implica que $\langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_\ell) \rangle \subset \langle \mathrm{LT}(I) \rangle$, sin embargo, $\langle \mathrm{LT}(I) \rangle$ puede ser estrictamente mas grande.

Proposición 4.2. [6, prop. 3] *Sea $I \subset R$ un ideal distinto de cero, entonces:*

1. $\langle \mathrm{LT}(I) \rangle$ *es un ideal monomial.*
2. *Existen $g_1, \ldots, g_\ell \in I$, tales que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_\ell) \rangle$.*

La parte 2 de la proposición anterior nos lleva a la siguiente definición.

Definición 4.3. Dado un orden monomial en R, un subconjunto finito $G = \{g_1, \ldots, g_\ell\}$ de un ideal $I \subset R$ diferente de cero, se dice que G es una base de Gröbner si

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_\ell) \rangle.$$

Notemos que en la definición 4.3 no pedimos que G sea un conjunto generador de I, pues de la propia definición tendremos que I está generado por G.

Proposición 4.4. [8, teo. 16] *Toda base de Gröbner de I es un sistema de generadores de I. Es decir, si $G = \{g_1, \ldots, g_\ell\}$ es una base de Gröbner para I, entonces*

$$I = \langle g_1, \ldots, g_\ell \rangle.$$

Veamos ahora que la no unicidad del residuo en la division de $f \in R$ entre $G \subset R$ desaparece cuando G es una base de Gröbner.

Proposición 4.5. [8, prop. 17] *Supongamos que $G = \{g_1, \ldots, g_\ell\}$ es una base de Gröbner de un ideal $I \subset R$ respecto a un orden monomial fijo sobre R. Entonces, para todo polinomio $f \in R$ existen dos polinomios q y $r \in R$ únicos tales que*

1. $f = q + r$,
2. $q \in I$ *y*
3. *para todo monomio x^α de r, $x^\alpha \notin \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_\ell)\rangle$.*

Teorema 4.6. [1, teo. 1.6.2] *Sea $I \subset R$ un ideal distinto de cero. Las siguientes condiciones son equivalentes para un conjunto $G = \{g_1, \ldots, g_\ell\} \subset I$.*

1. *G es una base de Gröbner para I.*
2. *$f \in I$ si y solo si $f \xrightarrow{G} 0$.*

Observa que con los dos resultados anteriores tenemos resuelto el problema de la *pertenencia* que planteamos en la sección 2. Sin embargo, aún queda mucho qué decir sobre las bases de Göbner, por ejemplo cómo determinar si un conjunto de generadores de un ideal es o no una base de Gröbner, y en caso de que no lo sea, cómo construir una a partir de un sistema de generadores dado. La forma en que se construye la teoría de bases de Gröbner, permite desarrollar implementaciones computacionales eficientes para calcularlas y como consecuencia se pueden aplicar para abordar diferentes problemas. Esperamos que al lector le parezca interesante esta breve introducción, algunas buenas referencias donde se puede encontrar más información al respecto son [1, 7, 6, 8, 11, 12].

5. Aplicaciones y comentarios finales

En esta última sección comentaremos algunas aplicaciones que tienen las bases de Gröbner, mostraremos una aplicación algebraica y comentaremos de forma panorámica cómo se usan para abordar problemas clásicos en diferentes áreas de las matemáticas.

Eliminación de variables. El problema de eliminación de variables consiste en lo siguiente: dados un ideal I de $R = \mathbb{K}[x_1, \ldots, x_n]$ y un entero ℓ, $1 \leq \ell \leq n$, ¿cómo determinar un sistema de generadores del ideal $I \cap \mathbb{K}[x_{\ell+1}, \ldots, x_n]$ a partir de un sistema de generadores de I? Necesitamos definir un tipo de órdenes monomiales que permitirán contestar a esta pregunta usando bases de Gröbner.

Definición 5.1. Un orden monomial $<$ sobre R es un orden de eliminación para las primeras ℓ variables si, para todo par de monomios x^α, x^β de R,

$$x^\alpha \notin \langle x_1, \ldots, x_\ell \rangle \text{ y } x^\beta \in \langle x_1, \ldots, x_\ell \rangle \Longrightarrow x^\beta > x^\alpha.$$

Como consecuencia directa de la definición tenemos que si $<$ es un orden de eliminación para las primeras ℓ variables, para todo polinomio $f \in R$, tenemos que

$$\mathrm{lm}(f) \in \mathbb{K}[x_{\ell+1}, \ldots, x_n] \Longrightarrow f \in \mathbb{K}[x_{\ell+1}, \ldots, x_n].$$

El orden *lex* es un ejemplo de orden de eliminación para las primeras ℓ variables para todo ℓ, $1 \leq \ell \leq n$.

El resultado principal de esta aplicación es el siguiente:

Teorema 5.2. [8, teo. 34] *Sea I un ideal de R y $>$ un orden de eliminación sobre R para las primeras ℓ variables con $1 \leq \ell \leq n$. Si G es una base de Gröbner de I para el orden $>$, entonces $G \cap \mathbb{K}[x_{\ell+1}, \ldots, x_n]$ es una base de Gröbner de $I \cap \mathbb{K}[x_{\ell+1}, \ldots, x_n]$ para el orden inducido por $>$ sobre $\mathbb{K}[x_{\ell+1}, \ldots, x_n]$.*

Este resultado responde al problema de eliminación de variables ya que el conjunto G es finito y por lo tanto es fácil determinar $G \cap \mathbb{K}[x_{\ell+1}, \ldots, x_n]$ que por lo que se discutió en las secciones anteriores resulta ser un sistema de generadores del ideal $I \cap \mathbb{K}[x_{\ell+1}, \ldots, x_n]$.

Para más información sobre eliminación de variables se le suguiere al lector la siguiente bibliografía [7, 6] y las referencias que incluyen.

Códigos y geometría algebraica. Una aplicación de las bases de Gröbner está presente en la teoría algebraica de códigos, se pueden utilizar para construir códigos de corrección de errores, que se utilizan para transmitir información de forma fiable a través de canales con ruido, estos códigos tienen propiedades deseables, como la capacidad de corregir una gran cantidad de errores [3, 10] .

Las bases de Gröbner también se utilizan en geometría algebraica computacional. Se pueden utilizar para estudiar la geometría de variedades algebraicas y para calcular invariantes geométricos, como la dimensión, el grado y las singularidades de la variedad [9]. Las bases de Gröbner también se usan para estudiar la topología de variedades algebraicas y para calcular números de intersección. Una excelente referencia donde se dan más detalles sobre la aplicación a la geometría algebraica es [5].

Álgebra computacional. Por otro lado, las bases de Gröbner tienen aplicaciones en sistemas de álgebra computacional, por ejemplo Maple y Mathematica, utilizan las bases de Gröbner como una herramienta fundamental para resolver sistemas polinomiales y realizar otros cálculos algebraicos [6, 11, 12]. Las bases de Gröbner se pueden utilizar para

calcular ideales, eliminar variables, resolver ecuaciones diferenciales y realizar otras operaciones en el cálculo simbólico. Consecuencia de esto, esta teoría se usa en el modelado de sistemas en el control automático, mediante el uso de bases de Gröbner, podemos construir modelos polinomiales precisos de sistemas no lineales y reducir su complejidad, haciéndolos más fáciles de analizar y controlar [13].

Agradecimientos

Agradecemos a los árbitros por una lectura cuidadosa del artículo y por los comentarios y mejoras sugeridas.

Bibliografía

[1] W. W. Adams y P. Loustanau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, Amer. Math. Soc., 1994.

[2] B. B., «Ein algorithmisches kriterium für die lösbarkeit eines algebraischen gleichungssystems», *Aequationes Math.*, 1970, 374–383, https://doi.org/10.1007/BF01844169.

[3] M. Boer y R. Pellikann, *Gröbner bases for error-correcting codes and their decoding*, Some Tapas of Computer Algebra, 1999.

[4] B. Buchberger, «An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal», *J. Symbolic Comput.*, vol. 41, 2006, 475–511, https://doi.org/10.1016/j.jsc.2005.09.007.

[5] V. Castellanos, «La unidad de las Matemáticas Contemporáneas», *Carta Informativa de la SMM*, núm. 41, 2004, 7–12.

[6] D. Cox, J. Little y D. O'Shea, *Ideals, varieties, and algorithms. an introduction to computational algebraic geometry and commutative algebra*, 2.ª ed., Undergraduate Texts in Mathematics, Springer, 1997, https://doi.org/10.1007/978-3-319-16721-3.

[7] V. Ene y J. Herzog, *Gröbner bases in commutative algebra*, Graduate Studies in Mathematics 130, Amer. Math. Soc., 2012.

[8] P. Gimenez, «Una introducción a las bases de Gröbner y algunas de sus aplicaciones», 2014, VI Escuela Doctoral Intercontinental de Matemáticas, https://doi.org/10.18800/9786123170561.004.

[9] H. Hironaka, «Resolution of singularities of an algebraic variety over a field of characteristic zero», *Ann. of Math.*, núm. 79, 1964, 109–326, https://doi.org/10.2307/1970486.

[10] J. Martínez-Bernal, Y. Pitones y R. H. Villarreal, «Minimum distance functions of complete intersection», *J. Algebra Appl.*, vol. 17, núm. 11, 2018, 1850204, https://doi.org/10.1142/S0219498818502043.

[11] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series 8, Amer. Math. Soc., 1996.

[12] W. V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, Algorithms and Computation in Mathematics, 2, Springer, 1998.

[13] U. Walther, T. T. Georgiou y A. Tannenbaum, «On the computation of switching surfaces in optimal control: a Gröbner basis approach», *IEEE Transactions on Automatic Control*, vol. 46, núm. 4, 2001, 534–540, https://doi.org/10.1109/9.917655.