SAHUARUS
Revista Electrónica de Matemáticas,
Departamento de Matemáticas, Universidad de Sonora,
Vol. 3, No. 1. Octubre, 2018, pp. 18–34.

Una introducción a las bases de Groebner

Vinicio Antonio Gómez Gutiérrez

Facultad de Ciencias, UNAM
e-mail: vgomez@ciencias.unam.mx

Resumen

En este artículo nos proponemos dar una introducción elemental a las bases de Groebner, lo suficientemente accesible para que estudiantes de las ciencias físico-matemáticas y de las ingenierías puedan utilizar esta herramienta en sus cursos de cálculo. Por poner un ejemplo, en el estudio de multiplicadores de Lagrange pueden aparecer sistemas de ecuaciones polinomiales en varias variables. A diferencia de los sistemas de ecuaciones lineales, no son tan conocidos métodos para resolver dichos problemas. Esperamos contribuir a la difusión de una parte del álgebra que simplifica tanto la teoría como la práctica de la resolución de sistemas de ecuaciones polinomiales. Cabe mencionar que las aplicaciones de las bases de Groebner van mucho más allá de resolver sistemas de ecuaciones, pero en este artículo las presentaremos desde este punto de vista. Esperamos, por añadidura, despertar la curiosidad para acercarse al álgebra, esa parte de las matemáticas cuya belleza no se ve con los ojos.

1 Introducción. El método de eliminación.

Empezaremos dando un breve repaso al método de eliminación de Gauss para resolver un sistema de ecuaciones lineales, pensando en extenderlo a sistemas de ecuaciones polinomiales. Luego repasaremos brevemente algunos conceptos y resultados que aparecen en el estudio de los polinomios de varias variables. A continuación explicaremos qué es una base de Groebner, y describiremos a grandes rasgos el algoritmo de Buchberger. Finalmente, ilustraremos en un ejemplo cómo las ideas relacionadas con la teoría de las bases de Grobner permite abordar los sistemas de ecuaciones polinomiales desde una perspectiva más amplia.

Consideremos un sistema de ecuaciones lineales

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n \end{aligned}$$

El método de eliminación de Gauss nos da un camino para transformar este sistema de ecuaciones en otro, más fácil de resolver. Con tres operaciones elementales: permutar dos ecuaciones, multiplicar una ecuación por un número distinto de cero, y sumarle a una ecuación otra ecuación, se puede ir eliminando una variable de las ecuaciones siguientes hasta llegar a un sistema de ecuaciones en el cual, de la última ecuación podamos despejar la última variable, luego podamos sustituir en la penúltima ecuación, despejar la penúltima

variable, y así sucesivamente hasta obtener el valor de la primera variable. Esto, en el caso de que el sistema de ecuaciones tenga una única solución. En general, el método de eliminación nos proporciona un sistema de ecuaciones equivalente al original, el cual está en una forma en la cual es más fácil describir el conjunto de soluciones, aún cuando sea vacío o infinito.

Presentaremos una generalización del método de eliminación de Gauss para sistemas de ecuaciones polinomiales. Las tres operaciones elementales mantienen su validez: podemos permutar dos ecuaciones, podemos sumarle una ecuación a otra, e incluso podemos multiplicar una ecuación, no sólo por un número, sino por un polinomio si es que así lo necesitamos. En el proceso de tratar de resolver así un sistema de ecuaciones polinomiales, la matemática se fue desarrollando, y un poquito de eso es de lo que hablaremos este artículo, además de lo que anunciamos en el resumen.

2 Conceptos preliminares.

2.1 Ideales de polinomios.

Sea $K[x_1, x_2, \ldots, x_n]$ el conjunto de polinomios en n variables con coeficientes en un campo K (para fines de nuestro artículo, $K = \mathbb{R}$ ó $\mathbb{C}$ según sea necesario). Estamos interesados en resolver sistemas de ecuaciones. Sin pérdida de generalidad podemos suponer que las ecuaciones están igualadas a cero:

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\cdots \\ f_s(x_1, \ldots, x_n) &= 0. \end{aligned}$$

Nos gustaría transformar el sistema de ecuaciones dado en otro más sencillo que tenga el mismo conjunto de soluciones. Consideremos dos operaciones que podemos realizar con el conjunto de ecuaciones.

- Podemos sumar dos ecuaciones
$$f_1 = 0$$
$$f_2 = 0$$
y obtener una nueva ecuación
$$f_1 + f_2 = 0.$$
- Podemos multiplicar una ecuación
$$f_1 = 0$$
por un factor $h(x_1, \ldots, x_n)$ y obtener una nueva ecuación
$$f_1 \cdot h = 0.$$
En particular, si elegimos adecuadamente el factor h puede ser que al sumar con otra ecuación eliminemos un término.

Vamos a estudiar conjuntos de polinomios que sean cerrados bajo estas operaciones.

Definición 2.1 *Un subconjunto $I \subset K[x_1, x_2, \ldots, x_n]$ es un **ideal** si cumple las tres propiedades siguientes:*

i) $0 \in I$ *(el polinomio constante cero pertenece a I).*

ii) $f, g \in I \Rightarrow f + g \in I$ *(si dos polinomios pertenecen a I, la suma pertenece a I).*

iii) Si $f \in I$ *y* $h \in K[x_1, x_2, \ldots, x_n]$ *entonces* $f \cdot h \in I$ *(el producto de un polinomio del ideal por un polinomio cualquiera, es otro polinomio que pertenece al ideal).*

A continuación veamos un ejemplo. Sea $\mathbb{R}[x, y]$ el conjunto de polinomios de dos variables con coeficientes en $\mathbb{R}$ y sea

$$I = \{(x^2 + y^2 - 25) \cdot h_1(x, y) + (y - 0.75x) \cdot h_2(x, y) : h_1, h_2 \in \mathbb{R}[x, y]\}.$$

Se puede ver que I es un ideal. Lo llamaremos el ideal generado por los polinomios

$$f_1(x, y) = x^2 + y^2 - 25, \quad f_2(x, y) = y - 0.75x.$$

Lo denotaremos como sigue:

$$I = \langle f_1, f_2 \rangle.$$

Notemos que todos los polinomios $f \in I$ satisfacen que

$$f(4, 3) = f(-4, -3) = 0.$$

En particular los puntos $(4, 3)$ y $(-4, -3)$ son las soluciones del sistema de ecuaciones

$$\begin{aligned} x^2 + y^2 - 25 &= 0 \\ y - 0.75x &= 0. \end{aligned}$$

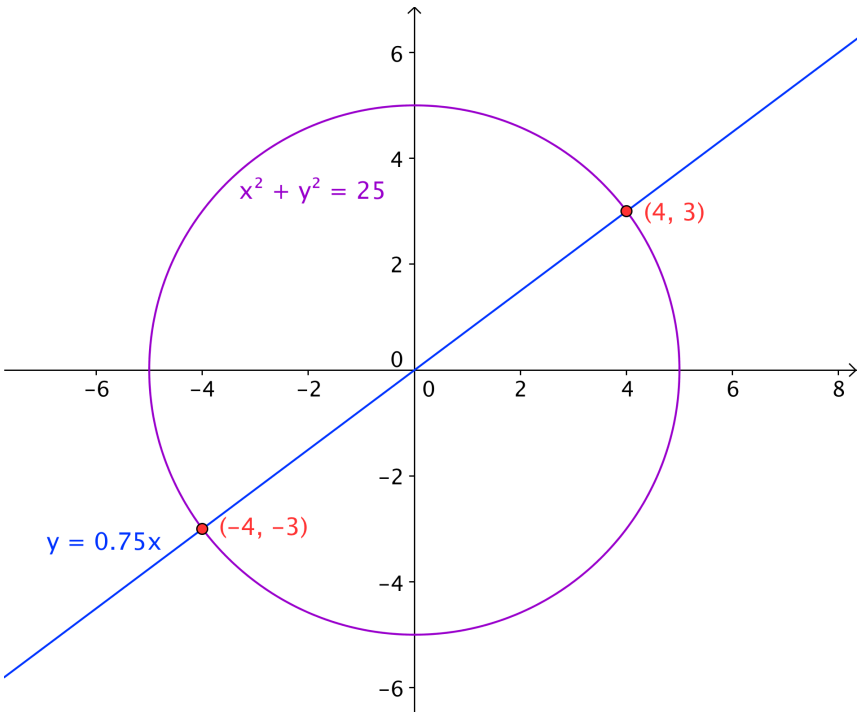

Figura 1: Un sistema de dos ecuaciones con dos incógnitas.

En otras palabras: el conjunto de soluciones del sistema de dos ecuaciones

$$f_1(x, y) = 0$$
$$f_2(x, y) = 0$$

coincide con el conjunto de soluciones del sistema de ecuaciones infinito

$$f(x, y) = 0 \quad \forall f \in \langle f_1, f_2 \rangle.$$

El problema de encontrar otro conjunto de ecuaciones

$$g_1(x, y) = 0$$
$$g_2(x, y) = 0$$

que tenga el mismo conjunto de soluciones se traduce en encontrar g_1, g_2 tales que

$$\langle g_1, g_2 \rangle = \langle f_1, f_2 \rangle.$$

En general: dado un conjunto de polinomios $\{f_1, f_2, \ldots, f_s\} \subset \mathbb{R}[x_1, \ldots, x_n]$, el conjunto

$$\langle f_1, f_2, \ldots, f_s \rangle = \{f_1 \cdot h_1 + f_2 \cdot h_2 + \ldots + f_s \cdot h_s \quad con \quad h_1, h_2, \ldots, h_s \in \mathbb{R}[x_1, x_2, \ldots, x_n]\}$$

es un ideal, el **ideal generado** por los polinomios $f_1, f_2, \ldots, f_s$.

Dado un ideal $I \subset K[x_1, \ldots, x_n]$ con K un campo (para fines de este trabajo será $\mathbb{R}$ ó $\mathbb{C}$) podemos definir una relación de equivalencia en el conjunto de los polinomios de n variables como sigue:

$$f \sim g \Leftrightarrow f - g \in I.$$

Nótese que $f \sim g$ si y sólo si existe $q \in I$ tal que $f = g+q$, o lo que es lo mismo, $g = f-q$. Pensando en el contexto de sistemas de ecuaciones, si q pertenece al ideal generado por los polinomios que definen nuestro sistema de ecuaciones, podemos obtener g restándole q a f y sustituir f por g. Nos proponemos determinar g de manera que el sistema de ecuaciones modificado tenga el mismo conjunto de soluciones que el sistema original, pero que sea más fácil de resolver. Si realizamos los intercambios de manera que el sistema de ecuaciones final esté inducido por una base de Groebner del ideal generado por los polinomios del sistema de ecuaciones original, lograremos este objetivo.

Estaremos de acuerdo en que un polinomio es más simple que otro si es de menor grado. Dado un polinomio de una variable, el grado lo determina el monomio de mayor grado, y dicho monomio es único. En el caso de polinomios de varias variables, para no perder la unicidad de dicho monomio, necesitamos un criterio que tome en cuenta todos los exponentes a los cuales pueden estar elevadas cada una de las variables. Es lo que vamos a discutir a continuación.

2.2 El orden lexicográfico

A cada monomio de un polinomio f en las variables $x_1, x_2, \ldots, x_n$ le podemos asociar un vector de n números enteros no negativos, a saber, el vector de los exponentes a los cuales están elevadas las variables:

$$x^{\boldsymbol{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \leftrightarrow (a_1, a_2, \ldots, a_n) = \boldsymbol{a}.$$

Definición 2.2 *Sean $x^{\boldsymbol{a}}$ y $x^{\boldsymbol{b}}$ dos monomios en $K[x_1, \ldots, x_n]$. Decimos que $x^{\boldsymbol{a}}$ es mayor que $x^{\boldsymbol{b}}$ (y lo denotamos por $x^{\boldsymbol{a}} \succ x^{\boldsymbol{b}}$) si la primera entrada distinta de cero del vector $\boldsymbol{a} - \boldsymbol{b}$ de izquierda a derecha, es positiva. Este orden es llamado el orden lexicográfico.*

Veamos un ejemplo. En $\mathbb{R}[x, y, z]$ con el orden lexicográfico, resulta que $x \succ y \succ z$. Para convencerse de ello, consideremos la correspondencia

$$\begin{aligned} x &\leftrightarrow (1, 0, 0), \\ y &\leftrightarrow (0, 1, 0), \\ z &\leftrightarrow (0, 0, 1). \end{aligned}$$

Observando el vector $(1, 0, 0) - (0, 1, 0) = (1, -1, 0)$ comprobamos que $x \succ y$. Análogamente podemos decir que $y \succ z$ porque $(0, 1, 0) - (0, 0, 1) = (0, 1, -1)$.

Nótese que el orden lexicográfico permite ordenar monomios que tienen grados iguales, por ejemplo $x^3y^3z^3 \succ x^2y^3z^4$, sin embargo, con este orden tenemos que $x^2 \succ y^{30}$. Hay otras maneras de ordenar los monomios que se pueden formar con varias variables, pero para hacer más simple la exposición, nos limitaremos a trabajar con ésta manera de ordenar los polinomios.

Definición 2.3 *Sea $f \in K[x_1, x_2, \ldots, x_n]$ un polinomio de varias variables.*

1. *El* ***monomio principal*** *de un polinomio f es el mayor monomio de f con respecto al orden lexicográfico $\succ$. Lo denotaremos por* $\mathrm{MP}(f)$. *Siguiendo a Cox [1], asumiremos que el monomio principal siempre es mónico (tiene coeficiente* 1*).*

2. *El* ***multigrado*** *de un polinomio f es el vector de exponentes del monomio principal de f.*

3. *El* ***coeficiente principal*** *de un polinomio f es el coeficiente del monomio principal de f. Lo denotaremos por* $\mathrm{CP}(f)$.

4. *El* ***término principal*** *de un polinomio f es el producto del coeficiente principal de f por el monomio principal de f. Lo denotaremos por* $\mathrm{TP}(f)$.

2.3 El algoritmo de la división para polinomios de varias variables.

Sea $f \in \mathbb{R}[x_1, \ldots, x_n]$. Consideremos un vector de polinomios $(f_1, f_2, \ldots, f_s)$. Dividir f entre $(f_1, f_2, \ldots, f_s)$ nos dará como resultado un vector de cocientes $(q_1, q_2, \ldots, q_s)$ y un residuo r tales que

$$f = q_1 f_1 + q_2 f_2 + \cdots + q_s f_s + r.$$

Para aplicar el algoritmo de la división es necesario haber elegido previamente el orden que se utilizará para comparar los monomios. Para que todo funcione bien, dicho orden debe cumplir ciertas propiedades, como ser compatible con la suma, y cumplir el principio del buen orden. Por simplicidad, de aquí en adelante daremos por hecho que estamos utilizando el orden lexicográfico, el cual cumple las propiedades requeridas. Para dividir el polinomio f entre el vector de polinomios $(f_1, \ldots, f_s)$ procedemos como sigue:

Algorithm 1 División de un polinomio f entre un vector de polinomios $(f_1, \ldots, f_s)$.

$q_1 := 0, \ldots, q_s := 0$, $r := 0$ ▷ Al principio los cocientes y el residuo valen cero
$p := f$
while $p \neq 0$ **do**
  $i := 1$
  $divfin := false$
  while $i \leq s$ y $divfin = false$ **do**
    if $TP(f_i)$ divide a $TP(p)$ **then**
      $q_i := q_i + \frac{TP(p)}{TP(f_i)}$
      $p := p - \frac{TP(p)}{TP(f_i)} f_i$
      $divfin := true$
    else
      $i := i + 1$
    end if
  end while
  if $divfin = true$ **then**
    $r := r + TP(p)$
    $p := p - TP(p)$
  end if
end while

El residuo final r, si no fue cero, tiene que ser una combinación lineal de un conjunto de monomios tales que ninguno debe ser divisible por ninguno de los términos principales de los polinomios f_i.

Veamos un ejemplo. Se trata de dividir el polinomio

$$f = x^2y + xy^2 + y^2$$

entre el vector de polinomios

$$(f_1, f_2) = (xy - 1, y^2 - 1).$$

Primero dividimos f entre f_1. La primera etapa del proceso es dividir f entre f_1. Nos preguntamos si el término principal de f_1 divide al término principal de f. En caso de que sí, realizaremos la división como en el caso de polinomios de una variable, en caso de que no, excluiremos al término principal de f de dicha división.

El término principal de f_1 es xy. El término principal de f es x^2y. Procedemos a dividir como en el caso de polinomios de una variable. Concretamente, multiplicamos f_1 por x y el producto se lo restamos a f. Obtenemos el polinomio $p = xy^2 + x + y^2$. Ahora multiplicamos f_1 por y y el producto se lo restamos a p. El resultado es $r_1 = x + y^2 + y$.

La segunda etapa del proceso es dividir r_1 entre f_2. Nos preguntamos si el término principal de f_2 divide al término principal de r_1. En caso de que sí, realizaremos la división como en el caso de polinomios de una variable, en caso de que no, excluiremos al término

principal de r_1 de dicha división. El término principal de f_2 es y^2. El término principal de r_1 es x. Como $TP(f_2)$ no divide a $TP(r_1)$, consideraremos al término principal de r_1 como parte del residuo final de la división, y trataremos de dividir $y^2 + y$ entre f_2. Ahora nos preguntamos si el término principal de $f_2 = y^2 - 1$ divide al término principal de $y^2 + y$. Como la respuesta es afirmativa, procedemos a dividir $y^2 + y$ entre $y^2 - 1$. Obtenemos un cociente igual a 1 y un residuo $y + 1$, pero el residuo final de la división de f entre (f_1, f_2) será $r_2 = x + y + 1$.

En resumen

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

El residuo final es $x + y + 1$.

Ahora dividamos al polinomio

$$f = x^2y + xy^2 + y^2$$

entre el vector de polinomios que se obtiene al invertir el orden de los polinomios del ejemplo anterior

$$(h_1, h_2) = (f_2, f_1) = (y^2 - 1, xy - 1).$$

La primera etapa del proceso es dividir f entre h_1.

Nos preguntamos si el término principal de $h_1 = y^2 - 1$ divide al término principal de $f = x^2y + xy^2 + y^2$. No es el caso. Procedemos a incluir el término principal de f al residuo final de la división. Ahora trataremos de dividir el polinomio $xy^2 + y^2$ entre $y^2 - 1$. Nos preguntamos si y^2 divide a xy^2. Como la respuesta es afirmativa, procedemos a dividir $xy^2 + y^2$ entre $y^2 - 1$. Resulta que:

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

De aquí se sigue que:

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

El primer residuo de la división es $r_1 = x^2y + x + 1$.

La segunda etapa del proceso es dividir r_1 entre h_2.

Nos preguntamos si el término principal de $xy-1$ divide al término principal de x^2y+x+1. La respuesta es que sí. Procedemos a dividir r_1 entre h_2. El resultado es:

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

El segundo cociente es x, y el segundo residuo es $r_2 = 2x + 1$.

Incorporando esta información:

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

En este caso, el residuo final es $2x + 1$. Esto nos muestra que el orden en que se realizan las divisiones puede conducir a resultados distintos.

En la práctica, el cálculo de los cocientes y los residuos se simplifica si utilizamos las computadoras. Para ser más precisos, podemos utilizar SageMath el cual es software libre [4], tiene documentación específica para bases de Groebner [5] y [6]. Otra opción es utilizar el sistema de álgebra computacional Maxima [2], el cual tiene un paquete especial para trabajar con bases de Groebner [3].

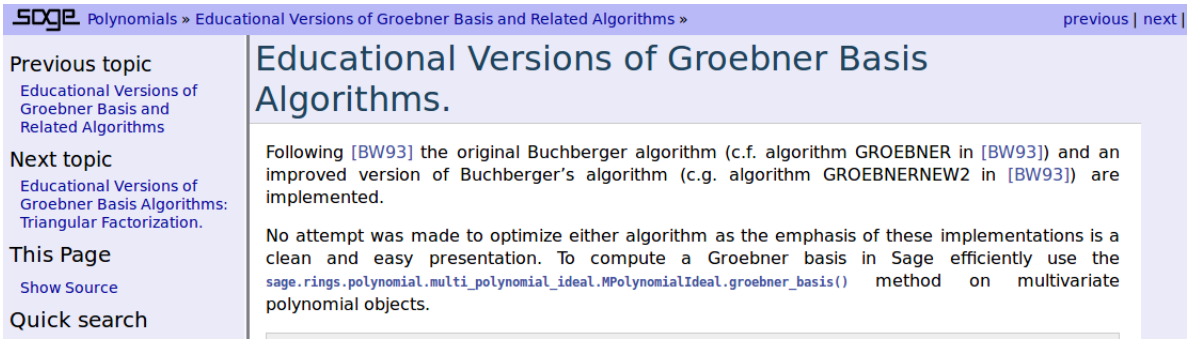

Figura 2: Bases de Groebner con Sage

2.4 El S-polinomio de dos polinomios p y q.

En el estudio del algoritmo de la división, tanto en el conjunto de los números enteros, como en el conjunto de los polinomios de una variable, resulta de gran utilidad el algoritmo de Euclides, pues facilita el cálculo del máximo común divisor de dos enteros (respectivamente de dos polinomios) y permite expresarlo como combinación lineal mínima de dichos dos enteros (respectivamente de dos polinomios). Tendrímos que poder decir, de todas las combinaciones lineales posibles de dos polinomios en varias variables, decir cuál es la mínima. Podemos intuír que si el orden depende de cuál es el término de mayor grado, entonces una combinación lineal en la cual se cancele dicho término, sería la mínima.

Definición 2.4 *Sean $p, q \in \mathbb{R}[x_1, \ldots, x_n]$ dos polinomios distintos del polinomio cero.*

Si $\boldsymbol{a} = (a_1, \ldots, a_n)$ y $\boldsymbol{b} = (b_1, \ldots, b_n)$ son los multigrados de p y q, respectivamente, y si $\boldsymbol{c} = (c_1, \ldots, c_n)$ es el vector de coordenadas enteras $c_i = max\{a_i, b_i\}$, entonces $x^{\boldsymbol{c}}$ es el mínimo común múltiplo de $x^{\boldsymbol{a}}$ y de $x^{\boldsymbol{b}}$, los monomios principales de p y q.

*El **S-polinomio** de p y q es el polinomio*

$$S(p,q) = \frac{x^{\boldsymbol{c}}}{TP(p)}p - \frac{x^{\boldsymbol{c}}}{TP(q)}q.$$

Observaciones:

1. Decimos que monomio $x^{\boldsymbol{c}}$ es el mínimo común múltiplo de los monomios $x^{\boldsymbol{a}}$ y $x^{\boldsymbol{b}}$ porque tiene la propiedad de que es un múltiplo de $x^{\boldsymbol{a}}$ y de $x^{\boldsymbol{b}}$ (pues $x^{\boldsymbol{c}} = x^{\boldsymbol{c}-\boldsymbol{a}} \cdot x^{\boldsymbol{a}}$, y $x^{\boldsymbol{c}} = x^{\boldsymbol{c}-\boldsymbol{b}} \cdot x^{\boldsymbol{b}}$). Además es el monomio de menor grado con esta propiedad.

2. Nótese que al calcular el S-polinomio de p y q se cancelan los términos principales de $\frac{x^{\mathbf{c}}}{\mathrm{TP}(p)}p$ y de $\frac{x^{\mathbf{c}}}{\mathrm{TP}(q)}q$. En ese sentido es una combinación lineal mínima de p y q.

Ejemplo. El S-polinomio de $p = xy - 1$ y de $q = y^2 - 1$ es el polinomio

$$(*) \quad S(p,q) = y(xy-1) - x(y^2-1) = xy^2 - y - xy^2 + x = x - y.$$

3 Bases de Groebner.

3.1 Bases de Groebner.

Sea $\prec$ el orden lexicográfico en el conjunto de los monomios que se pueden formar usando n variables. Sea $I \subset \mathbb{R}[x_1, \ldots, x_n]$ un ideal de polinomios.

Definición 3.1 *El ideal generado por los términos principales de todos los polinomios $f \in I$, es el* ***ideal inicial*** *de I. Lo denotaremos por $Id_{in}(I)$.*

Definición 3.2 *Un subconjunto finito de polinomios $G = \{g_1, g_2, \ldots, g_s\} \subset I$ es una* ***base de Groebner*** *para el ideal I con respecto al orden $\prec$, si*

$$\langle \mathrm{TP}(g_1), \ldots, \mathrm{TP}(g_s) \rangle = Id_{in}(I),$$

en otras palabras, si el ideal generado por los términos principales de los polinomios que pertenecen a G, coincide con el ideal inicial de I.

Nótese que siempre se da la contención

$$\langle \mathrm{TP}(g_1), \ldots, \mathrm{TP}(g_s) \rangle \quad \subset \quad Id_{in}(I),$$

la otra contención puede no darse. Veamos un ejemplo.

Sea $F = \{f_1, f_2\}$ con

$$f_1 = xy - 1, \quad f_2 = y^2 - 1.$$

Sea I el ideal generado por F. Con respecto al orden lexicográfico $x \succ y$, los términos principales de los elementos de F son

$$\mathrm{TP}(f_1) = xy, \quad \mathrm{TP}(f_2) = y^2.$$

Con estos monomios generamos a los polinomios de la forma

$$f = xyh_1 + y^2 h_2.$$

En cambio el ideal inicial de I está generado por los términos principales de todos los polinomios que pertenecen a I. Sus elementos son sumas finitas de la forma

$$\mathrm{TP}(g_1)h_1 + \mathrm{TP}(g_2)h_2 + \cdots + \mathrm{TP}(g_r)h_r,$$

con $g_1, g_2, \ldots, g_r \in I$.

Notemos que en I está el S-polinomio de f_1 y f_2. Este polinomio lo calculamos después de la definición de S-polinomio (lo marcamos con un asterisco $(*)$ para identificarlo fácilmente).

$$S(f_1, f_2) = x - y.$$

El monomio $x = \mathrm{TP}(S(f_1, f_2)) \in Id_{in}(I)$, pero no pertenece al ideal generado por $\mathrm{TP}(f_1)$ y $\mathrm{TP}(f_2)$. Por lo tanto, F no es una base de Groebner para el ideal I.

Ahora veamos otro ejemplo, en el cual se cumple la igualdad

$$\langle \mathrm{TP}(g_1), \ldots, \mathrm{TP}(g_s) \rangle = Id_{in}(I).$$

Sea $G = \{g_1, g_2\} = \{x - z, y - z\}$. Con el orden lexicográfico $x \succ y \succ z$, el término principal de g_1 es x, mientras que el término principal de g_2 es y. Sea $J = \langle x, y \rangle$, el ideal generado por los términos principales de g_1 y g_2. Se puede ver que $f \in J$ si y sólo si es de la forma $f = x \cdot h$ ó $f = y \cdot h$ para algún polinomio $h \in \mathbb{R}[x, y, z]$.

Sea I el ideal generado por G. Para ver que el ideal inicial $Id_{in}(I)$ está coincide con J basta ver que el término principal de todo polinomio $f \in I$ es divisible por x o por y. Dado que estamos trabajando con el orden lexicográfico $x \succ y \succ z$, los únicos polinomios cuyo término principal no pertenece a J son los polinomios que sólo dependen de z y son distintos del polinomio cero.

Sea $f \in I$. f es de la forma $f(x, y, z) = (x - z) \cdot h_1(x, y, z) + (y - z) \cdot h_2(x, y, z)$. Dado que los polinomios $g_1(x, y, z) = x - z$ y $g_2(x, y, z) = y - z$ se anulan en la recta formada por todos los puntos de la forma (t, t, t), también f se anula en dichos puntos.

Si $TP(f)$ no perteneciera a J, entonces f sería de la forma $f(x, y, z) = f(z)$. Pero por el hecho de que f se anula en todos los puntos de la forma $(x, y, z) = (t, t, t)$, entonces f necesariamente tendría que ser el polinomio cero. De lo anterior se sigue que los ideales J y $Id_{in}(I)$ son iguales, y que G es una base de Groebner para el ideal I.

Las bases de Groebner tienen muchas propiedades interesantes, entre ellas mencionaremos las siguientes:

- Si $G = \{g_1, \ldots, g_s\}$ es una base de Groebner, y f es un polinomio cualquiera, entonces no importa el orden en que enlistemos los elementos de G para formar un vector $(g_1, \ldots, g_s)$, la división de f entre dicho vector $(g_1, \ldots, g_s)$ siempre dará el mismo residuo. Véase [1], Capítulo 2, Sección 6, Proposición 1.

- Para saber si un polinomio f pertenece al ideal generado por una base de Groebner, basta dividir el polinomio f entre un vector de polinomios cuyas entradas son los elementos de G. El polinomio f pertenecerá al ideal si y sólo si el residuo de esta división es cero. Véase [1], Capítulo 2, Sección 6, Corolario 2.

- El S-polinomio $S(g_i, g_j)$ de dos polinomios cualesquiera de una base de Groebner, siempre deja residuo cero al dividir entre $(g_1, \ldots, g_s)$. Véase [1], Capítulo 2, Sección 6, Teorema 6.

- Consideremos un sistema de ecuaciones

$$f_1 = 0$$
$$f_2 = 0$$
$$\ldots$$
$$f_m = 0,$$

si $G = \{g_1, \ldots, g_s\}$ es una base de Groebner del ideal generado por $F = \{f_1, \ldots, f_m\}$, entonces el sistema de ecuaciones

$$g_1 = 0$$
$$g_2 = 0$$
$$\ldots$$
$$g_s = 0,$$

tiene el mismo conjunto de soluciones que el original, pero con la ventaja de que, en general, es más fácil de resolver. Véase [1], Capítulo 3, Secciones 1 y 2.

Nótese que, en particular, el sistema de ecuaciones

$$x - z = 0$$
$$y - z = 0,$$

asociado a la base de Groebner G del ejemplo anterior, ciertamente es fácil de resolver.

3.2 El algoritmo de Buchberger.

Consideremos el problema de encontrar una base de Groebner $G = (g_1, \ldots, g_s)$ de un ideal I generado por un conjunto de polinomios conocido $F = (f_1, \ldots, f_r)$.

Veamos un ejemplo. Sea I el ideal generado por los polinomios

$$f_1 = x + y - 2z$$
$$f_2 = 3x - 2y - z.$$

Vamos a calcular una base de Groebner para I usando el algoritmo de Buchberger, con $G = \{f_1, f_2\}$ como punto de partida.

Calculemos los S-polinomios de parejas de G. En este caso solamente es uno, el siguiente:

Algorithm 2 El algoritmo de Buchberger

```
G ← F                                   ▷ El punto de partida es el vector de polinomios F
repeat
    G' ← G
    for cada pareja {p, q} ⊂ G' do calcular el residuo R de dividir S(p, q) entre G'
        if R ≠ 0 then
            G = G ∪ {R}                 ▷ Agregamos R al conjunto de generadores G
        end if
    end for
until G = G'   ▷ Hasta que todos los S-polinomios de elementos de G dejen residuo cero
```

$$S(f_1, f_2) = y - z.$$

Dividimos $S(f_1, f_2)$ entre $\{f_1, f_2\}$. Se puede ver que el residuo es $y - z$. Como no es cero, lo incluímos en el conjunto G. Ahora

$$G = \{f_1, f_2, f_3\},$$

con $f_3 = y - z$.

Calculamos los tres S polinomios de parejas de G:

$$S(f_1, f_2) = y - z$$
$$S(f_1, f_3) = xz + y^2 - 2yz$$
$$S(f_2, f_3) = xz - \frac{2}{3}y^2 - \frac{1}{3}yz.$$

Se puede ver que al dividir cada uno de estos polinomios entre G obtenemos residuo cero. Terminamos la ejecución del algoritmo. Comprobemos que el resultado es una base de Groebner.

Por una parte, el ideal generado por los términos principales de los tres polinomios de G. Es el ideal

$$\langle x, 3x, y\rangle = \langle x, y\rangle.$$

Los polinomios que pertenecen a este ideal son los polinomios $f(x, y, z)$ que son múltiplos de x ó múltiplos de y.

Por otra parte, observemos $Id_{in}(I)$, el ideal generado por los términos principales de todos los polinomios de $I = \langle f_1.f_2, f_3\rangle$. Claramente $\langle x, y\rangle \subset Id_{in}(I)$. La única manera en que ambos ideales podrían ser diferentes sería que la contención fuera propia. Un polinomio $f \in Id_{in}(I)$ que no fuera múltiplo de x ni múltiplo de y tendría que ser un polinomio que dependiera exclusivamente de z. Sin embargo, también tendría que anularse en todos los

puntos de la forma (t,t,t) pues los tres polinomios de G se anulan en dicho conjunto. f tendría que ser el polinomio constante cero, luego entonces la contención no es propia. En conclusión, G es una base de Groebner para I.

La similitud con el ejemplo de la subsección anterior no es mera coincidencia, pues

$$G_1 = \{x - z, y - z\} \quad y \quad G_2 = \{x + y - 2z, 3x - 2y - z, y - z\}$$

son dos bases de Groebner para el mismo ideal I.

3.3 Una aplicación

Para finalizar este trabajo, mostraremos cómo las ideas relacionadas con las bases de Groebner pueden ayudarnos a abordar de una manera más sencilla problemas de cálculo.

Consideremos un problema clásico de multiplicadores de Lagrange.

Encontrar el volumen de la caja rectangular de volumen máximo que se puede inscribir en el elipsoide

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1.$$

El método de multiplicadores de Lagrange nos plantea el sistema de ecuaciones

$$\bigtriangledown f = \lambda \bigtriangledown g$$
$$g = 1,$$

donde

$$f(x,y,z) = xyz$$
$$g(x,y,z) = \frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2}.$$

Calculemos los gradientes de f y de g.

$$\bigtriangledown f = (yz, xz, xy)$$
$$\bigtriangledown g = \left(\frac{2x}{a^2}, \frac{2y}{b^2}, \frac{2z}{c^2}\right).$$

Simplificando el sistema de ecuaciones podemos llevarlo a la forma:

$$f_1 = 2\lambda x - a^2 yz = 0$$
$$f_2 = 2\lambda y - b^2 xz = 0$$

$$f_3 = 2\lambda z - c^2 xy = 0$$
$$f_4 = \frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} - 1 = 0.$$

Es un sistema de ecuaciones con cuatro incógnitas. Considerando el orden lexicográfico $\lambda \succ x \succ y \succ z$, vamos a calcular el S-polinomio de f_1 y f_2:

$$S(f_1, f_2) = y(2\lambda x - a^2 yz) - x(2\lambda y - b^2 xz).$$

Simplificando queda (suponiendo que buscamos una solución $z \neq 0$):

$$-a^2 y^2 + b^2 x^2 = 0.$$

Es una ecuación en la cual eliminamos a λ. Podemos reescribirla en la forma

$$\frac{x^2}{a^2} = \frac{y^2}{b^2}.$$

Análogamente podemos calcular el S-polinomio de f_1 y f_3. Y llegaremos a una ecuación análoga

$$\frac{x^2}{a^2} = \frac{z^2}{c^2}.$$

Sustituyendo en la ecuación del elipsoide

$$\frac{3x^2}{a^2} = 1$$
$$x = \frac{a}{\sqrt{3}}.$$

Análogamente

$$y = \frac{b}{\sqrt{3}}$$
$$z = \frac{c}{\sqrt{3}}.$$

Claramente

$$xyz = \frac{abc}{3\sqrt{3}}.$$

El volumen de la caja que buscamos es $\frac{8abc}{3\sqrt{3}}$.

En este caso no fue indispensable calcular una base de Groebner. Bastó utilizar el concepto del S-polinomio para obtener un sistema de ecuaciones más sencillo. Sin embargo, veamos a dónde podemos llegar usando sistemas de álgebra computacional. Para ilustrar el procedimiento utilizaremos los valores particulares

$$a = 3, \quad b = 2, \quad c = 1.$$

Obtenemos los polinomios siguientes:

$$g_1 = z - 4z^3 + 3z^5$$

$$g_2 = -yz + 3yz^3$$

$$g_3 = -2z + y^2z + 2z^3$$

$$g_4 = -4y + y^3 + 8yz^2$$

$$g_5 = -xz + 3xz^3$$

$$g_6 = -xy + 3xyz^2$$

$$g_7 = xy^2 - 4xz^2$$

$$g_8 = -36 + 4x^2 + 9y^2 + 36z^2$$

$$g_9 = 2\lambda - 3xyz.$$

El polinomio g_1 de la base de Groebner depende solamente de la variable z. Calculemos sus raíces:

$$3z^5 - 4z^3 + z = 0.$$

Descartando la solución $z = 0$, y simplificando, el polinomio queda

$$3z^4 - 4z^2 + 1 = 0.$$

Introduciendo una variable $u = z^2$ este polinomio toma la forma

$$3u^2 - 4u + 1 = 0.$$

De donde $u = 1$ ó $u = \frac{1}{3}$, en consecuencia $z = \pm 1$ ó $z = \pm\frac{1}{\sqrt{3}}$.

Después podemos sustituír para encontrar las otras soluciones, aunque descartamos algunas en las cuales los valores negativos no corresponderían a la solución buscada.

Referencias

[1] Cox, Little, O'Shea. *Ideals, Varieties and Algorithms.* Springer-Verlag. 536 páginas. New York, 1997.

[2] `http://maxima.sourceforge.net/es/index.html`

[3] `http://maxima.sourceforge.net/docs/manual/es/maxima_56.html#SEC288`. Fecha de consulta: 9 de agosto de 2018.

[4] `http://www.sagemath.org/`

[5] http://doc.sagemath.org/html/es/tutorial/tour_polynomial.html. Fecha de consulta: 9 de agosto de 2018.

[6] http://doc.sagemath.org/html/en/reference/polynomial_rings/sage/rings/polynomial/toy_buchberger.html. Fecha de consulta: 10 de agosto de 2018.

[7] Sturmfels. *WHAT IS ... a Grobner basis?* Notices of the American Mathematical Society, Vol. 52, no. 10, p. 1199 (2005).