Las bases de Gröbner en el estudio de los polinomios simétricos

Cifuentes, V.[I]; Patiño, B.; Pérez, H.[II]

Resumen. En este artículo presentamos dos algoritmos, el primero permite escribir un polinomio simétrico f en $k[x_1, \cdots, x_n]$, con k un cuerpo, en términos de las funciones simétricas elementales; el segundo, determina si un polinomio f en $k[x_1, \cdots, x_n]$, con k un cuerpo, es simétrico, y si este es el caso, cómo escribirlo en términos de las funciones simétricas elementales. Además, probamos de manera detallada cómo se obtiene una base de Gröbner G en el caso particular cuando se considera el orden lex sobre los términos, herramienta necesaria para presentar el segundo algortimo. Adicionalmente, mostramos una pequeña aplicación de los polinomios simétricos en el cálculo del anillo de invariantes de un grupo finito de matrices dado. Ilustramos los resultados con variados ejemplos.

Palabras clave: Polinomios simétricos, polinomios simétricos elementales, bases de Gröbner, anillo de invariantes.

Abstract. In this article we present two algorithms, the first one allows to write a polynomial $f \in k[x_1, \cdots, x_n]$, with k a field, in terms of the symmetrical elementary functions, the second one determines if a polynomial $f \in k[x_1, \cdots, x_n]$, with k a field, is symmetrical, and if this one is the case, how to write it in terms of the symmetrical elementary functions. As complement, we show in a detailed way how Gröbner's base is obtained in the particular case when the order is considered to be lex, necessary tool to present the second algorithm. Finally we present a small application of the symmetrical polynomials in the calculation of the rings of invariants of a finite matrix groups. We ilustrate the results with several examples.

Keywords: Symmetric polinomials, elementary symmetric functions, Gröbner bases, rings of invariants.

I Docente escuela de matemáticas, Universidad Pedagógica y Tecnológica de Colombia, Tunja, Colombia. veciva@yahoo.com.

II Estudiantes licenciatura en matemáticas, Universidad Pedagógica y Tecnológica de Colombia, Tunja, Colombia. azulcielo22@hotmail.com, hperez042000@yahoo.com

Clasificación de materias (AMS): 53A35,58A05,53A35.

1. INTRODUCCIÓN

Durante las últimas décadas se han logrado avances significativos en el desarrollo de métodos algorítmicos en matemáticas, tanto para realizar cálculos que manualmente son bastante extensos o que a veces pueden tornarse difíciles, como para demostrar proposiciones y teoremas. En álgebra conmutativa la teoría y métodos de las bases de Gröbner, permiten realizar cálculos efectivos en $k[x_1, \cdots, x_n]$, el anillo de polinomios en n indeterminadas con coeficientes en un cuerpo k. Los paquetes computacionales como Singular, CoCoa, Maple, entre otros, cuentan con una librería que permite realizar los cálculos anteriormente mencionados usando dicha técnica.

En el estudio de los polinomios simétricos, las bases de Gröbner nos permiten determinar si un polinomio es simétrico y si este es el caso, cómo escribirlo en términos de los polinomios simétricos elementales. Este procedimiento es constructivo y por tanto podemos presentar un algoritmo, el cual es una motivación para el estudio de la teoría de invariantes desde el punto de vista computacional, es decir, de calcular de manera explícita el anillo de invariantes de un grupo finito.

2. PRELIMINARES

2.1 Orden de términos

Definición 2.1. *Un producto de potencias en $A = k[x_1, \cdots, x_n]$ es una expresión de la forma $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, donde $\alpha := (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$. El conjunto de todos los productos de potencias será denotado por*

$$\mathbb{T}^n = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_i \in \mathbb{N}, i = 1, \cdots, n\}$$

Definición 2.2. *Un polinomio $f \neq 0 \in k[x_1, \cdots, x_n]$ es una suma finita de términos de la forma $a_i x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, con $a_i \neq 0 \in k$, es decir,*

$$f = a_1 X^{\alpha_1} + \cdots + a_t X^{\alpha_t}$$

donde, $X^{\alpha_1} > X^{\alpha_2} > \cdots > X^{\alpha_t}$ y $X^{\alpha_i} \in \mathbb{T}^n$. En este caso

- *$lp(f) = X^{\alpha_1}$, es el producto de potencias principal de f.*
- *$lc(f) = a_1$, es el coeficiente principal de f.*

- $lt(f) = a_1 X^{\alpha_1}$, *es el término principal de* f.

Definición 2.3. *Un orden de términos es un orden total* $<$ *que satisface las siguientes dos condiciones:*

(i) $1 < X^\alpha$ *para todo* $X^\alpha \in \mathbb{T}^n$, $X^\alpha \neq 1$.

(ii) *Si* $X^\alpha < X^\beta$, *entonces* $X^\alpha X^\gamma < X^\beta X^\gamma$ *para todo* $X^\gamma \in \mathbb{T}^n$.

Existen diferentes ordenes, se presentan a continuación los tres más conocidos en la literatura, éstos son usados en los paquetes computacionales existentes como CoCoa, Maple, Singular.

Definición 2.4. *Sean* $X^\alpha < X^\beta$ *productos de potencias, se definen los siguientes ordenes sobre* $\mathbb{T}^n$ *con* $x_1 > x_2 > \cdots > x_n$.

(i) *El orden lex (lexicográfico)*

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \text{la primera coordenada } \alpha_i \text{ y } \beta_i \text{ en } \alpha \text{ y } \beta \text{ de izquierda a} \\ \text{derecha, las cuales son diferentes satisfacen } \alpha_i < \beta_i \end{cases}$$

donde $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n), \beta = (\beta_1, \beta_2, \cdots, \beta_n) \in \mathbb{N}^n$

(ii) *El orden deglex (lexicográfico de grado)*

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ o \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \quad y\ X^\alpha < X^\beta \text{ con respecto a lex} \\ \text{con } x_1 > x_2 > \cdots > x_n. \end{cases}$$

donde $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{N}^n, \beta = (\beta_1, \beta_2, \cdots, \beta_n) \in \mathbb{N}^n$

(iii) *El orden degrevlex (lexicográfico de grado reverso)*

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ o \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ y la primera coordenada de } \alpha_i \text{ y } \beta_i \text{ en} \\ \alpha \text{ y } \beta \text{ desde la derecha, las cuales son diferentes satisfacen} \\ \alpha_i > \beta_i. \end{cases}$$

donde $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{N}^n, \beta = (\beta_1, \beta_2, \cdots, \beta_n) \in \mathbb{N}^n$

2.2 Nociones básicas de bases de Gröbner

En esta sección presentamos las nociones básicas de la teoría de las bases de Gröbner, que serán necesarias en las secciones posteriores. Un estudio detallado de esta teoría se puede hacer siguiendo el libro de Adams y Loustaunau (veáse [1]).

Definición 2.5. *Un conjunto de polinomios distinto de cero* $G = \{g_1, \cdots, g_t\}$ *contenido en un ideal* $I :=< f_1, \cdots, f_k >$*, es una base de Gröbner para* I *si, y sólo si, para todo* $f \in I, f \neq 0$*, existe* $i \in \{1, \cdots, t\}$ *tal que* $lp(g_i)$ *divide a* $lp(f)$*.*

Definición 2.6. *Sean* $0 \neq f, g \in k[x_1, \cdots, x_n]$*. Se define el mínimo común múltiplo de* f *y* g*, denotado por* $lcm(f, g)$*, al polinomio* l *tal que:*

(i) f, g *dividen a* l*.*

(ii) *Si* f, g *dividen a un polinomio* h*, entonces* l *divide a* h*.*

(iii) $lc(l) = lc(f)lc(g)$*.*

Definición 2.7. *Sean* $0 \neq f, g \in k[x_1, \cdots, x_n]$*. Sea* $L = lcm(lp(f), lp(g))$*. El polinomio*

$$S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g$$

se denomina el S*- polinomio de* f *y* g*.*

Teorema 2.8. *Sea* $G = \{g_1, \cdots, g_t\}$ *un conjunto de polinomios no nulos en* $k[x_1, \cdots, x_n]$*. Entonces* G *es una base de Gröbner para el ideal* $I =< g_1, \cdots, g_t >$ *si, y sólo si, para todo* $i \neq j$

$$S(g_i, g_j) \xrightarrow{G}_+ 0,$$

Proposición 2.9. *Sea* $G \subset k[x_1, \cdots, x_n]$ *un conjunto finito y sean* $f, g \in G$ *tales que*

$$lcm(lp(f), lp(g)) = lp(f) \cdot lp(g)$$

es decir que los monomios principales de f *y* g *son primos relativos. Entonces*

$$S(g_i, g_j) \xrightarrow{G}_+ 0,$$

3. POLINOMIOS SIMÉTRICOS

Cuando se estudian las raíces de un polinomio surgen de manera natural polinomios simétricos, los cuales reciben el nombre de funciones simétricas elementales. Éstas juegan un papel fundamental ya que cualquier polinomio simétrico en $k[x_1, \cdots, x_n]$ puede ser escrito en términos de dichas funciones. En esta sección mostraremos un algoritmo que permite hacer dicho procedimiento.

Definición 3.1. *Un polinomio $f \in k[x_1, \cdots, x_n]$ es simétrico si*

$$f(x_{i_1}, \cdots, x_{i_n}) = f(x_1, \cdots, x_n)$$

para todas las posibles permutaciones $x_{i_1}, \cdots, x_{i_n}$ de las variables $x_1, \cdots, x_n$.

Ejemplo 3.2. *Sea $A = \mathbb{Q}[x, y, z]$, entonces el polinomio $f(x, y, z) = x^3 + x^2y^2z^2 + y^3 + z^3$ es simétrico ya que*

$$f(x, y, z) = f(x, z, y) = f(y, x, z) = f(y, z, x) = f(z, x, y) = f(z, y, x).$$

Definición 3.3. *Dadas las variables $x_1, \cdots, x_n$, se define $\sigma_1, \cdots, \sigma_n \in k[x_1, \cdots, x_n]$ de la siguiente manera:*

$$\begin{aligned}
\sigma_1 &= x_1 + \cdots + x_n \\
&\vdots \\
\sigma_i &= \sum_{j_1 < j_2 < \cdots < j_i} x_{j1} x_{j2} x_{j3} \cdots x_{ji} \\
&\vdots \\
\sigma_n &= x_1 x_2 x_3 \cdots x_n
\end{aligned}$$

Proposición 3.4. *Si $x_1, \cdots, x_n$ son las raíces de un polinomio $f(x)$, entonces $f(x)$ puede ser expresado usando las funciones $\sigma_1, \cdots, \sigma_n$ de la siguiente manera*

$$f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \cdots + (-1)^{n-1}\sigma_{n-1}x + (-1)^n\sigma_n \qquad (1)$$

Proposición 3.5. *Los polinomios $\sigma_1, \cdots, \sigma_n$ en la definición 3.3 son simétricos y se denominan las funciones simétrica elementales.*

Demostración. Usando la proposición anterior, ya que $x_1, \cdots, x_n$ son las raíces de un polinomio $f(x)$, podemos escribir f de la siguiente manera

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n) \qquad (2)$$

luego, al realizar cualquier permutación $x_{i_1}, \cdots, x_{i_n}$ de las variables $x_1, \cdots, x_n$, se obtiene el mismo polinomio salvo por el orden de los factores, así, los coeficientes en (3.1) son funciones simétricas. □

Teorema 3.6. *Teorema fundamental de polinomios simétricos. Cualquier polinomio simétrico en $k[x_1, \cdots, x_n]$ pueden ser escrito de manera única como un polinomio en las funciones simétricas elementales $\sigma_1, \cdots, \sigma_n$.*

Demostración. La prueba puede ser consultada en [2]. □

La demostración del teorema anterior nos permite presentar un algoritmo para escribir cualquier polinomio simétrico $f \in k[x_1, \cdots, x_n]$ en términos de los polinomios simétricos elementales.

Algoritmo para polinomios simétricos

ENTRADA: $f \neq 0 \in k[x_1, \cdots, x_n]$ polinomio simétrico
$\sigma_1, \cdots, \sigma_n$ las funciones simétricas elementales.
SALIDA: $a_1, a_2, \cdots, a_s, h_1, h_2, \cdots, h_s$ tal que $f = a_1h_1 + \cdots + a_sh_s$
INICIO: $a_1 := 0, a_2 := 0, \cdots, a_s := 0, h_1 := 0, h_2 := 0, \cdots, h_s := 0$
$p := f$

MIENTRAS $p \neq 0$ **HAGA**

Calcule $lt(p) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$

$h_i := h_i + \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \cdots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n}$.
$a_i := a_i + \frac{lt(p)}{lt(h_i)}$

$p := p - a_i h_i$

$f = a_1h_1 + a_2h_2 + \cdots + a_sh_s$

Ejemplo 3.7. *Considere el polinomio*

$$f = (x^2 + y^2)(x^2 + z^2)(y^2 + z^2) \in k[x, y, z]$$

escriba f como un polinomio en las funciones simétricas elementales $\sigma_1, \sigma_2, \sigma_3$, donde, $x > y > z$ y se considera el orden lex.

$$f(x,y,z) = x^4y^2 + x^4z^2 + x^2y^4 + 2x^2y^2z^2 + x^2z^4 + y^4z^2 + y^2z^4$$

Primer paso a través del mientras:
$lt(p) = x^4y^2$;

$$\begin{aligned} h_1 &= \sigma_1^2\sigma_2^2 \\ &= x^4y^2 + 2x^4yz + x^4z^2 + 2x^3y^3 + 8x^3y^2z + x^3yz^2 + 2x^3z^3 + y^2y^4 + 8x^2y^3z + 15x^2y^2z^2 \\ &\quad + 8x^2yz^3 + x^2z^4 + 2xy^4z + 8xy^3z^2 + 8xy^2z^3 + 2xyz^4 + y^4z^2 + 2y^3z^3 + y^2z^4 \end{aligned}$$

$lt(h_1) = x^4y^2; a = \frac{x^4y^2}{x^4y^2} = 1$

$$\begin{aligned} p &= f - a_1h_1 = f - \sigma_1^2\sigma_2^2 \\ &= -2x^4yz - 2x^3y^3 - 8x^3y^2z - 8x^3yz^2 - 2x^3z^3 - 8x^2y^3z - 13x^2y^2z^2 - 8x^2yz^3 \\ &\quad - 2xy^4z - 8xy^3z^2 - 8xy^2z^3 - 2xyz^4 - 2y^3z^3 \end{aligned}$$

Segundo paso a través del mientras:
$lt(p) = -2x^4yz$;

$$\begin{aligned} h_2 &= \sigma_1^3\sigma_3^1 \\ &= x^4yz + 3x^3y^2z + 3x^3yz^2 + 3x^2y^3z + 6x^2y^2z^2 + 3x^2yz^3 + xy^4z + 3xy^3z^2 + 3xy^2z^3 + xyz^4 \end{aligned}$$

$lt(h_2) = x^4yz; a_2 = \frac{-2x^4yz}{x^4yz} = -2$

$$\begin{aligned} p &= p - a_2h_2 = f - \sigma_1^2\sigma_2^2 + 2\sigma_1^3\sigma_3^1 \\ &= -2x^3y^3 - 2x^3y^2z - 2x^3yz^2 - 2x^3z^3 - 2x^2y^3z - x^2y^2z^2 - 2x^2yz^3 - 2xy^3z^2 - 2xy^2z^3 - 2y^3z^3 \end{aligned}$$

Tercer paso a través del mientras:
$lt(p) = -2x^3y^3$;

$$\begin{aligned} h_3 &= \sigma_2^3 \\ &= x^3y^3 + 3x^3y^2z + 3x^3yz^2 + x^3z^3 + 3x^2y^3z + 6x^2y^2z^2 + 3x^2yz^3 + 3xy^3z^2 \quad + 3xy^2z^3 + y^3z^3 \end{aligned}$$

$lt(h_3) = x^3y^3; a_3 = \frac{-2x^3y^3}{x^3y^3} = -2$

$$\begin{aligned} p &= p - a_3h_3 = f - \sigma_1^2\sigma_2^2 + 2\sigma_1^3\sigma_3^1 + 2\sigma_2^3 \\ &= 4x^3y^2z + 4x^3yz^2 + 4x^2y^3z + 11x^2y^2z^2 + 4x^2yz^3 + 4xy^3z^2 + 4xy^2z^3 \end{aligned}$$

Cuarto paso a través del mientras:
$lt(p) = 4x^3y^2z$;

$$\begin{aligned} h_4 &= \sigma_1\sigma_2\sigma_3 \\ &= x^3y^2z + x^3yz^2 + x^2y^3z + 3x^2y^2z^2 + x^2yz^3 + xy^3z^2 + xy^2z^3 \end{aligned}$$

$lt(h_4) = x^3y^2z, a_4 = \frac{4x^3y^2z}{x^3y^2z} = 4$

$p = p - a_4h_4 = f - \sigma_1^2\sigma_2^2 + 2\sigma_1^3\sigma_3^1 + 2\sigma_2^3 - 4\sigma_1\sigma_2\sigma_3 = x^2y^2z^2$

Quinto paso a través del mientras:
$lt(p) = x^2y^2z^2$

$$h_5 = \sigma_3^2 = x^2y^2z^2$$

$lt(h_5) = x^2y^2z^2, a_5 = \frac{x^2y^2z^2}{x^2y^2z^2} = 1$

$p = f - a_5h_5 = f - \sigma_1^2\sigma_2^2 + 2\sigma_1^3\sigma_3^1 + 2\sigma_2^3 - 4\sigma_1\sigma_2\sigma_3 - \sigma_3^2 = 0$
Ya que $p = 0$ *el ciclo mientras termina y se obtiene,*

$$f = \sigma_1^2\sigma_2^2 - 2\sigma_1^3\sigma_3^1 - 2\sigma_2^3 + 4\sigma_1\sigma_2\sigma_3 + \sigma_3^2$$

4. BASES DE GRÖBNER Y POLINOMIOS SIMÉTRICOS

Las bases de Gröbner son una herramienta útil en el estudio de los polinomios simétricos, ya que permiten determinar si un polinomio en $k[x_1, \cdots, x_n]$ es simétrico, y en caso afirmativo expresar f en términos de los polinomios simétricos elementales.

Proposición 4.1. *En el anillo* $k[x_1, \cdots, x_n, y_1, \cdots, y_n]$ *se fija un orden en los monomios de tal manera que un monomio que contenga una de las variables* $x_1, \cdots, x_n$ *es mayor que cualquier monomio en* $k[y_1, \cdots, y_n]$. *Sea* G *una base de Gröbner del ideal* $\langle \sigma_1 - y_1, \cdots, \sigma_n - y_n \rangle \subset k[x_1, \cdots, x_n, y_1, \cdots, y_n]$. *Dado* $f \in k[x_1, \cdots, x_n]$ *y* $g = \bar{f}^G$ *el residuo de* f *al dividirlo por* G. *Entonces:*

(i) f *es simétrico si, y sólo si,* $g \in k[y_1, \cdots, y_n]$

(ii) *Si* f *es simétrico, entonces* $f = g(\sigma_1, \cdots, \sigma_n)$ *es la única expresión de* f *como un polinomio en las funciones simétricas elementales* $\sigma_1, \cdots, \sigma_n$

La proposición anterior muestra la necesidad de conocer métodos para calcular una base de Gröbner para $\langle \sigma_1 - y_1, \cdots, \sigma_n - y_n \rangle$. Una manera de hacerlo es usando el algoritmo de Buchberger.[1] Sin embargo, cuando se usa el orden lex, hay un método bastante sencillo para calcular una base para dicho ideal, el cual mostramos en detalle a continuación.

Proposición 4.2. *Fijado el orden lex sobre* $k[x_1, \cdots, x_n, y_1, \cdots, y_n]$ *con* $x_1 > \cdots > x_n > y_1 > \cdots > y_n$. *Entonces los polinomios*

[1] Para más detalles veáse [1]

$$g_k = h_k(x_k, \cdots, x_n) + \sum_{i=1}^{k}(-1)^i h_{k-i}(x_k, \cdots, x_n)y_i,\ k = 1, \cdots, n,$$

forman una base de Gröbner para el ideal $\langle \sigma_1 - y_1, \cdots, \sigma_n - y_n \rangle$*, donde*

$$h_i(x_1, \cdots, x_s) = \sum_{|\alpha|=i}(X^\alpha)$$

es la suma de todos los monomios de grado total i *en* $x_1, \cdots, x_s$*.*

Demostración. En primer lugar se debe probar que el conjunto de los $g_k, k = 1 \cdots, n$ son un subconjunto del ideal $\langle \sigma_1 - y_1, \cdots, \sigma_n - y_n \rangle$.
Paso 1. Probar que

$$0 = h_k(x_k, \cdots, x_n) + \sum_{i=1}^{k} h_{k-i}(x_k, \cdots, x_n)\sigma_i$$

Paso 1.1 Probar que $0 = \sum_{i=0}^{k}(-1)^i h_{k-i}(x_1, \cdots, x_n)\sigma_i(x_1, \cdots, x_n)$
En la demostración denotaremos $x := x_1, \cdots, x_n$. Si $X^\alpha = x_{j_1}^{\alpha_1} x_{j_2}^{\alpha_2} \cdots x_{j_a}^{\alpha_a}$ es un monomio que aparece en $h_{k-i}(x)\sigma_i(x)$, donde a denota el número de variables que aparecen en X^α entonces se debe tener que $i \leq a$, en efecto, ya que σ_i es la suma de todos los monomios que son productos de i distintas variables, entonces cada término que aparece en el producto $h_{k-i}(x)\sigma_i(x)$ deben involucrar como mínimo las i variables que aparecen en $\sigma_i(x)$. Así, el número de variables que aparecen en X^α es mayor o igual a i, es decir, $a \geq i$.
Ahora, ya que $i \leq a$ entonces determinar todos los monomios que involucren i variables de las a variables dadas en X^α , se reduce a resolver un problema de combinatoria ya que al usar cualquier orden de términos hay solamente una forma de escribir cada monomio. Por cada combinación $C_{a,i}$ se obtienen $i!$ permutaciones, luego $C_{a,i} \times r! = P_{a,i} = \frac{a!}{(a-i)!}$, donde $P_{a,i}$ denota el número de permutaciones, es decir $C_{a,i} = \frac{a!}{(a-i)i!} = \binom{a}{i}$, las cuales según la definición de σ_i, son monomios que aparecen allí, por tanto, hay $\binom{a}{i}$ términos de $\sigma_i(x)$ que aparecen en X^α. Ya que $h_{k-i}(x)$ es la suma de todos los monomios de grado total $k - i$ en $x_1, \cdots, x_n$, los cuales tiene coeficiente 1, y existen $\binom{a}{i}$ términos de σ_i que involucran variables de X^α, entonces X^α aparecerá $\binom{a}{i}$ veces en $h_{k-i}(x)\sigma_i(x)$, así, el coeficiente de X^α en $\sum_{i=0}^{k}(-1)^i h_{k-i}(x)\sigma_i(x)$ es $\sum_{i=0}^{a}(-1)^i\binom{a}{i}$. Aplicando el teorema del binomio se obtiene

$$0 = (-1+1)^a = \sum_{i=0}^{a}\binom{a}{i}(-1)^i(1)^{a-i} = \sum_{i=0}^{a}\binom{a}{i}(-1)^i$$

es decir, el coeficiente con que aparece X^α en $h_{k-i}(x)\sigma_i(x)$ es cero, por tanto,

$$0 = \sum_{i=0}^{k} (-1)^i h_{k-i}(x_1, \cdots, x_n)\sigma_i(x_1, \cdots, x_n)$$

Paso 1.2 Probar que

$$0 = h_k(x_k, \cdots, x_n) + \sum_{i=1}^{k} (-1)^i h_{k-i}(x_k, \cdots, x_n)\sigma_i(x_1, \cdots, x_n), \tag{3}$$

lo cual es equivalente a probar que

$$0 = \sum_{i=0}^{k} (-1)^i h_{k-i}(x_1, \cdots, x_n)\sigma_i(x_1, \cdots, x_n).$$

Para usar la identidad probada en el paso 1.1, se deben separar las variables $x_1, \cdots, x_{k-1}$, para esto, sea $A = \{1, 2, \cdots, k-1\}$, el conjunto formado por los subíndices de las variables $x_i, i = 1, \cdots, k-1$, $S \subset A$, X^S el producto de las correspondientes variables según los subíndices involucrados en S, $|S|$ el número de elementos en S y sea

$$H = \{S/S \subset A\} \qquad = \{\emptyset, \{1\}, \{2\}, \cdots, \{k-1\}, \{1,2\}, \{1,3\}, \cdots, \{1,2,\cdots,k-2\}\}$$

Mostraremos que $\sum_{S \in H} X^s \sigma_{i-|S|}(x_k, \cdots, x_n) = \sigma_i(x_1, \cdots, x_n)$

Para mayor facilidad tomaremos $y = x_k, \cdots, x_n$ y $x = x_1, \cdots, x_{k-1}$

$$\begin{aligned}
\sum_{S \in H} X^s \sigma_{i-|S|}(y) = \sigma_i(y) + x_1\sigma_{i-1}(y) + x_2\sigma_{i-1}(y) + \cdots + x_{k-1}\sigma_{i-1}(y) + \\
x_1x_2\sigma_{i-2}(y) + \cdots + x_1x_{k-1}\sigma_{i-2}(y) + \cdots + x_{k-2}x_{k-1} \\
\sigma_{i-2}(y) + \cdots + x_1x_2\cdots x_{k-1}\sigma_{i-\{k-1\}}(y) \\
= \sigma_i(y) + \sigma_{i-1}(y)(x_1 + x_2 + \cdots + x_{k-1}) + \sigma_{i-2}(y)(x_1x_2 \\
+ \cdots \quad + x_{k-2}x_{k-1}) + \cdots + \sigma_{i-k+1}(y)(x_1x_2\cdots x_{k-1}) \\
= \sigma_i(y) + \sigma_{i-1}(y)\sigma_1(x) + \sigma_{i-2}(y)\sigma_2(x) + \sigma_{i-3}(y)\sigma_3(x)\cdots \\
+ \sigma_{i-(k-2)}(y)\sigma_{k-2}(x)
\end{aligned}$$

Ya que cada producto $\sigma_{i-j}(y)\sigma_j(x), j = 0, \cdots, k-2$, es la suma de todos los monomios de i variables distintas de las variables involucradas en cada uno de ellos, se obtiene la identidad deseada.

$$\begin{aligned}
\sum_{i=0}^{k} (-1)^i h_{k-i}(y)\sigma_i(x) &= \sum_{i=0}^{k} (-1)^i h_{k-i}(y) \sum_{S} \in HX^S\sigma_{i-|S|}(y) \\
&= h_k(y) \sum_{S \in H} X^S\sigma_{0-|S|}(y) - h_{k-1}(y) \sum_{S \in H} X^S\sigma_{1-|S|}(y) + h_{k-2}(y) \\
&\quad \sum_{S \in H} X^S\sigma_{2-|S|}(y) + \cdots + (-1)^k h_0(y) \sum_{S \in H} X^S\sigma_{k-|S|}(y) \\
&= \sum_{S \in H} X^S[h_k(y)\sigma_{0-|S|}(y) - h_{k-1}(y)\sigma_{1-|S|}(y) + h_{k-2}(y)\sigma_{2-|S|}(y) \\
&\quad + \cdots + (-1)^k h_0(y)\sigma_{k-|S|}(y)]
\end{aligned}$$

$$= \sum_{S\in H} X^S[\sum_{i=|S|}^{k}(-1)^i h_{k-i}(y)\sigma_{k-|S|}(y)]$$

donde la suma $\sum_{i=|S|}^{k}(-1)^i h_{k-i}(y))\sigma_{k-|S|}(y) = 0$, para cada $S \in H$. En efecto, haciendo la sustitución $j = i - |s|$, se obtiene,

$$\sum_{i=|S|}^{k}(-1)^i h_{k-i}(y))\sigma_{k-|S|}(y) = (-1)^{|s|}\sum_{j=0}^{k-|s|}(-1)^j h_{(k-|s|)-j}(y)\sigma_j(y) = 0$$

usando la identidad del paso 1.1. Así,

$$\sum_{i=0}^{k}(-1)^i h_{k-i}(y)\sigma_i(x) = \sum_{S\in H} X^S(\sum_{i=|S|}^{k}(-1)^i h_{k-i}(y)\sigma_{k-|S|}(y)) = \sum_{S\in H} X^S(0) = 0$$

Al sustraer 4.1 de la definición dada de g_k, obtenemos,

$$g_k = \sum_{i=1}^{k}(-1)^i h_{k-i}(x_k, \cdots, x_n)(y_i - \sigma_i) \tag{4}$$

lo cual prueba que $< g_1, \cdots, g_n > \subset < \sigma_1 - y_1, \cdots, \sigma_n - y_n >$.
Para mostrar la otra inclusión hay que notar que, ya que $h_0 = 1$, se puede escribir 4.2 como

$$g_k = (-1)^k(y_k - \sigma_k) + \sum_{i=1}^{k-1}(-1)^i h_{k-i}(x_k, \cdots, x_n)(y_i - \sigma_i) \tag{5}$$

Para mostrar $\langle \sigma_1 - y_1, \cdots, \sigma_n - y_n \rangle \subset \langle g_1, \cdots, g_n \rangle$ basta observar que de (4.3) se tiene que

$$\sigma_k - y_k = (-1)^{1-k} g_k + (-1)^{2-k}\textstyle\sum_{i=1}^{k-1}(-1)^i h_{k-i}(x_k, \cdots, x_n)(y_i - \sigma_i)$$

y por inducción sobre k se muestra que
si $k = 1$, $\quad \sigma_1 - y_1 = g_1$
si $k = 2$, $\quad \sigma_2 - y_2 = -g_2 + h_1(x_2, \cdots, x_n)g_1$
supongamos que para $k = s$,

$$\sigma_s - y_s = g_s - h'_{s-1}(x_s, \cdots, x_n)g_{s-1} + \cdots + h'_1((x_s, \cdots, x_n)g_1.$$

Luego,

$$\begin{aligned}\sigma_{s+1} - y_{s+1} &= (-1)^{-s} g_{s+1} + (-1)^{1-s} \sum_{i=1}^{s} (-1)^i h_{s+1-i}(x_{s+1}, \cdots, x_n)(y_i - \sigma_i) \\ &= (-1)^{-s} g_{s+1} + (-1)^{1-s}[(-1) h_{s+1}(x_{s+1}, \cdots, x_n)(y_1 - \sigma_1) + \cdots + \\ &\quad (-1)^s h_1(x_{s+1}, \cdots, x_n)(y_s - \sigma_s)] \\ &= (-1)^{-s} g_{s+1} + (-1)^{1-s}[(-1) h_{s+1}(x_{s+1}, \cdots, x_n) g_1 + \cdots + \\ &\quad (-1)^s h_1(x_{s+1}, \cdots, x_n) g_s - h_{s-1}^{'}(x_s, \cdots, x_n) g_{s-1} + \cdots + \\ &\quad h_1^{'}(x_s, \cdots, x_n) g_1].\end{aligned}$$

Por tanto, si $f \in \langle \sigma_1 - y_1, \cdots, \sigma_n - y_n \rangle$ entonces $f \in \langle g_1, \cdots, g_n \rangle$.
Por último, veamos que $lt(g_k) = x_k^k$. En efecto

$$\begin{aligned}lt(g_k) &= lt[h_k(x_k, \cdots, x_n) + \sum_{i=1}^{k} (-1)^i h_{k-i}(x_k, \cdots, x_n) y_i], k = 1, \cdots, n \\ &= \text{máx}[lt(h_k(x_k, \cdots, x_n), lt[\sum_{i=1}^{k} (-1)^i h_{k-i}(x_k, \cdots, x_n) y_i]], k = 1, \cdots, n) \\ &= \text{máx}[lt(h_k(x_k, \cdots, x_n), \text{máx}[lt(-h_{k-1}(x_k, \cdots, x_n) y_1), lt(h_{k-2}(x_k, \cdots, x_n) y_2), \cdots, \\ &\quad lt((-1)^k h_0(x_k, \cdots, x_n)) y_k]] \\ &= \text{máx}[lt(h_k(x_k, \cdots, x_n)), \text{máx}[lt(\sum_{|\alpha|=k} x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}} \cdots x_n^{\alpha_n}), lt(\sum_{|\alpha|=k-1} x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}} \cdots x_n^{\alpha_n} y_1), \\ &\quad lt(\sum_{|\alpha|=k-2} x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}} \cdots x_n^{\alpha_n} y_2), \cdots, lt((-1)^k y_k)]] \quad \textit{donde} \quad \alpha = \alpha_k + \alpha_{k+1} + \cdots + \alpha_n \\ &= \text{máx}(x_k^k, \text{máx}(x_k^{k-1}, x_k^{k-2}, \cdots, 1)) \\ &= x_k^k\end{aligned}$$

Así, los términos principales de $g_1, \cdots, g_n$ son primos relativos. Por la proposición 2.9 se obtiene $S(g_i, g_j) \xrightarrow{G}_+ 0$ y usando el teorema 2.8 concluimos que $\{g_1, \cdots, g_n\}$ forman una base de Gröbner para $\langle \sigma_1 - y_1, \cdots, \sigma_n - y_n \rangle$ □

Algoritmo para verificar si polinomio es simetrico

ENTRADA: $f \neq 0 \in k[x_1, \cdots, x_n]$
$\sigma_1, \cdots, \sigma_n$ las funciones simétricas elementales.
SALIDA: VERDADERO, si el polinomio es simétrico, y en este caso,
$f = g(\sigma_1, \cdots, \sigma_n)$
FALSO en otro caso.
INICIO: Calcule una base de Gröbner G para $\langle \sigma_1 - y_1, \cdots, \sigma_n - y_n \rangle$
Calcule el residuo g de la división de f por la base de Gröbner.

SI $g \in k[y_1, \cdots, y_n]$ **ENTONCES**

resultado:= VERDADERO

$f = g(\sigma_1, \cdots, \sigma_n)$

EN CASO CONTRARIO
resultado:= FALSO

RETORNE resultado

Ejemplo 4.3. *Considere el polinomio*

$$f = x^3 + y^3 + z^3 \in \mathbb{Q}[x, y, z]$$

Verifique si f es simétrico, si es así, escríbalo en términos de los polinomios simétricos elementales $\sigma_1, \sigma_2, \sigma_3$, usando el orden lex en $\mathbb{Q}[x, y, z, y_1, y_2, y_3]$ con $x > y > z > y_1 > y_2 > y_3$.

Paso 1. Calcular una base de Gröbner para $< \sigma_1 - y_1, \sigma_2 - y_2, \sigma_3 - y_3 >$.

Para esto usamos la proposición 4.2 y obtenemos que

$$\begin{aligned} g_1 &= h_1(x,y,z) + \sum_{i=1}^{1}(-1)^i h_{1-i}(x,y,z)y_i = \sum_{|\alpha|=1} \mathbf{x}^\alpha + (-1)h_0(x,y,z)y_1 \\ &= x + y + z - y_1 \\ g_2 &= h_2(y,z) + \sum_{i=1}^{2}(-1)^i h_{2-i}(y,z)y_i = \sum_{|\alpha|=2} \mathbf{x}^\alpha + (-1)h_1(y,z)y_1 + h_0(y,z)y_2 \\ &= y^2 + yz - yy_1 + z^2 - zy_1 + y_2 \\ g_3 &= z^3 - z^2y_1 + zy_2 - y_3 \end{aligned}$$

forman una base de Gröbner para el ideal $\langle \sigma_1 - y_1, \sigma_2 - y_2, \sigma_3 - y_3 \rangle \subset \mathbb{Q}[x,y,z,y_1,y_2,y_3]$. Así,

$$G = \{x + y + z - y_1, y^2 + yz - yy_1 + z^2 - zy_1 + y_2, z^3 - z^2y_1 + zy_2 - y_3\}$$

Paso 2. Aplicar el algoritmo de la división para hallar el residuo g obtenido al dividir f entre G. Este residuo fue calculado en [6] usando el algoritmo de la división dado en [1]. Usando el programa CoCoa.

$UseR ::= \mathbb{Q}[x,y,z,y_1,y_2,y_3]$;
$F := x^3 + y^3 + z^3$;
$L := [x + y + z - y_1, y^2 + yz - yy_1 + z^2 - zy_1 + y_2, z^3 - z^2y_1 + zy_2 - y_3]$;
$DivAlg(F, [x + y + z - y_1, L])$;
$Record[Quotients = [x^2 - xy + y^2 - xz + 2yz + z^2 + xy_1 - 2yy_1 -$
$2zy_1 + y_1^2, -3z + 3y_1, 3], Remainder = y_1^3 - 3y_1y_2 + 3y_3]$

luego,

$$g = y_1^3 - 3y_1y_2 + 3y_3$$

Paso 3. $g(y_1,y_2,y_3) = y_1^3 - 3y_1y_2 + 3y_3 \in \mathbb{Q}[y_1,y_2,y_3]$, y por tanto f es simétrico. Así,

$$f = g(\sigma_1,\sigma_2,\sigma_3) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$$

5. APLICACIÓN DE POLINOMIOS SIMÉTRICOS EN LA TEORÍA DE INVARIANTES

El ejemplo más básico de invariantes de un grupo finito de matrices está dado por los polinomios simétricos, al considerar el grupo finito de las matrices de permutación, como ilustraremos a continuación.

Definición 5.1. *El grupo S_n de todas las matrices cuadradas de tamaño n cuyas entradas son 0 ó 1, pero de tal manera que hay un único 1 en cada fila y en cada columna se llama el grupo de matrices de permutación.*

Ejemplo 5.2. *Sea $S_3 \subset GL(3,k)$ el grupo de matrices de permutación.*

$$S_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

Sea $f \in k[x,y,z]^{S_3}$ entonces $f(x) = f(A \cdot x), \forall A \in S_3$; ya que,

$$f\left[\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = f(x,y,z) \qquad f\left[\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = f(y,z,x)$$

$$f\left[\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = f(x,z,y) \qquad f\left[\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = f(z,x,y)$$

$$f\left[\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = f(y,x,z) \qquad f\left[\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = f(z,y,x)$$

se obtiene que, $f(x,y,z) = f(x,z,y) = f(y,x,z) = f(y,z,x) = f(z,x,y) = f(z,y,x)$. Los polinomios que cumplen esta condición son los polinomios simétricos, por tanto, los polinomios invariantes son los polinomios simétricos en $k[x,y,z]$.

Ejemplo 5.3. *En general si se considera el grupo $S_n \subset GL(n,k)$ de matrices de permutación, entonces*

$$k[x_1, \cdots, x_n]^{S_n} = \{\textit{cualquier polinomio simétrico en} \quad k[x_1, \cdots, x_n]\} \tag{6}$$

Por teorema (3.6), se conoce que los polinomios simétricos son polinomios en las funciones simétricas elementales con coeficientes en k, por tanto, se puede escribir (5.1) como,

$$k[x_1, \cdots, x_n]^{S_n} = k[\sigma_1, \cdots, \sigma_n]$$

Así, cualquier invariante puede ser escrito como un polinomio en las funciones simétricas elementales $\sigma_1, \cdots, \sigma_n$, además la representación en términos de las funciones simétricas elementales es única, por lo tanto, se obtiene un conocimiento explícito de los invariantes de S_n.

BIBLIOGRAFÍA

[1] Adams W. and Loustaunau P. (1994). *An Introduction to Gröbner Bases*. (Graduate Studies in Mathematics, Vol 3). Providence, R.I: American Mathematical Society.

[2] Cox D. and Little J. and O'Shea D. (1997). *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. New York: Springer.

[3] Hungerford T.W. (1974). *Algebra*. New York: Springer-Verlag.

[4] Kreuzer M. and Robbiano L. (2000). *Computational Commutative Algebra 1*. Berlin: Springer-Verlag.

[5] Kreuzer M. and Robbiano L. (2000). *Computational Commutative Algebra 2*. Berlin: Springer-Verlag.

[6] Patiño B. y Pérez H. (2009). *Uso de las bases de Gröbner en el cálculo de invariantes de grupos finitos*. Trabajo de grado. Tunja: Universidad Pedagógica y Tecnológica de Colombia.

[7] Sturmfels B. (2008). *Algorithms in Invariant Theory*. Berlin: Springer-Verlag. Second edition.

Referencia	Fecha de recepción	Fecha de aprobación
Cifuentes, V., Patiño, B., Pérez, H. Las bases de Gröbner en el estudio de los polinomios simétricos. Revista *Tumbaga* (2010), 5, 195-210.	Día/mes/año 05/10/2009	Día/mes/año