Universidad de El Salvador

Facultad de Ciencias Naturales y Matemática
Escuela de Matemática

TEORÍA DE INVARIANTES EN ANILLOS DE POLINOMIOS

T E S I S

PARA OBTENER EL TÍTULO DE:

Licenciado(a) en Matemática

PRESENTAN:

Brenda Guadalupe Mendoza Funes, MF11010
José Mauricio Calles Ramírez, CR11070

DIRECTOR DEL TRABAJO:
Lic. Mario Alexis Ruíz

Ciudad universitaria
6 de junio de 2017

UNIVERSIDAD DE EL SALVADOR

RECTOR:

MSc. Roger Armando Arias

VICE-RECTOR ADMINISTRATIVO INTERINO:

ING. Nelson Bernabé Granados

SECRETARIO GENERAL:

MSc. Cristobal Ríos

FISCAL GENERAL:

Licda. Beatriz Mélendez

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

DECANO:

Lic. Mauricio Hernán Lovo Córdova

VICE-DECANO:

Lic. Carlos Antonio Quintanilla Aparicio

SECRETARIA:

Licda. Damaris Melany Herrera Turcios

ESCUELA DE MATEMÁTICA

DIRECTOR DE ESCUELA:

Dr. José Nerys Funes Torres

ASESOR:

Lic. Mario Alexis Ruíz

Dedicatoria

La presente Tesis está dedicada principalmente a Dios
ya que sin Él no hubiésemos podido concluir con nuestra carrera.
A nuestros padres Guadalupe, Vilma y Santos, por su amor, apoyo y comprensión.

También es dedicado a la memoria de nuestro amigo
Jorge Luis Osorio Martínez (1993-2016),
por su apoyo en nuestro trabajo de graduación, aunque hoy ya no esté físicamente con nosotros sabemos que desde el cielo nos anima a seguir adelante y se alegra de nuestro triunfo.

Agradecimientos

Principalmente a Dios por protegernos durante todo nuestro trayecto, y por llenarnos de sabiduría y fortaleza para superar todos los obstáculos y dificultades en nuestros estudios y así culminar con nuestra carrera.
A nuestros padres y familiares; por sus consejos, palabras de aliento y por su apoyo incondicional para lograr llegar hasta esta instancia de nuestros estudios.
A nuestro docente director del trabajo de graduación, Lic. Mario Alexis Ruíz; por su dedicación, apoyo, esfuerzo y disponibilidad de tiempo y trabajo en cada aspecto de nuestra investigación. Gracias por dirigirnos en este último paso de nuestra carrera.
A nuestro jurado calificador Lic. Ernesto Américo Hidalgo, Lic. Yoceman Adony Sifontes; por su dedicación, revisiones y correcciones en nuestro trabajo. A nuestros amigos: Jorge (q.d.e.p), Erick, Karlita, Rafa, Estely, Francisco, Rauda, Wilner, Glenda, Marleny, Vane, Eu, Karla, Saúl, Orlando, Mike, Margarita, Cidia; por su amistad sincera, palabras de aliento, su colaboración que en algún momento nos brindaron en equipo. Así como también a los docentes Licda. Mirna, MSc. Palacios, MSc. Gámez, MSc. Gabriel por su colaboración y apoyo en nuestro trabajo de graduación.

Índice general

Resumen

La teoría invariante es una rama del álgebra abstracta que trata de acciones de grupos sobre variedades algebraicas, tales como espacios vectoriales, desde el punto de vista de su efecto sobre las funciones. Clásicamente, la teoría se ocupó de la cuestión de la descripción explícita de funciones polinomiales que no cambian, o que son invariantes, bajo las transformaciones de un grupo lineal dado. Por ejemplo, si consideramos la acción del Grupo Especial Lineal $SL(n, \mathbb{C})$ en el espacio de matrices de tamaño $n \times n$ y actúa por multiplicación a la izquierda, entonces el determinante es invariante de esta acción porque el determinante de AX es igual al determinante de X, cuando A está en $SL(n, \mathbb{C})$.

En el desarrollo del trabajo presentaremos algunas aplicaciones de la teoría de invariantes en diversos temas, como lo es en geometría proyectiva y en el cálculo del grupo de Galois.

Introducción

El presente trabajo esta estructurado por tres capítulos. En Capítulo I se encuentra la teoría básica necesaria sobre polinomios simétricos, la acción de un grupo sobre el conjunto de polinomios en varias variables y se dan a conocer la teoría de bases de Groebner con el objetivo de reducir polinomios con un orden monomial. Luego en el Capítulo II, se desarrollan los contenidos propios de la teoría de invariantes en anillos de polinomios con coeficientes complejos y se dan a conocer algunos de los resultados más importantes, así como también los algoritmos necesarios que servirán para encontrar un conjunto de invariantes algebraicamente independientes que generen el anillo total de invariantes de un subgrupo finito de matrices del Grupo General Lineal con entradas complejas, utilizando bases de Groebner, además al final de este capítulo se dan a conocer dos ejemplos concretos en los cuales se haga uso de los resultados y algoritmos expuestos para encontrar un conjunto algebraicamente independiente de polinomios invariantes que generen el anillo invariantes.

En el Capítulo III se muestran algunas de las aplicaciones de la teoría de invariantes. En primer lugar usamos la teoría de invariantes para calcular el Grupo de Galois dado un polinomio mónico irreducible sobre algún campo y sus raíces mediante algoritmos computacionales. En segundo lugar se utiliza la teoría de invariantes junto con un anillo de polinomios muy peculiar como lo es el anillos de soporte, donde cada polinomio en este anillo corresponde a una propiedad geométrica en el espacio proyectivo, además se demuestra el Primer Teorema Fundamental de la Teoría de Invariantes.

Metodología

Para cumplir satisfactoriamente con los objetivos propuestos en esta investigación se seguirán las siguientes etapas:

I. **Revisión bibliográfica:** Se indagará en diferentes libros, artículos y revistas de divulgación matemática, con la finalidad de conocer y relacionar los enfoques de cada autor, no se espera tener un libro o documento como base, sin embargo es importante aclarar que se tendrá un banco de documentos que facilite el acceso a la información para superar dudas que se presenten durante la investigación.

II. **Demostración de los principales teoremas:** Se demostrarán con la mayor cantidad de detalles posible cada uno de los resultados enunciados, especialmente aquellos que fundamentan los resultados principales que se desean establecer.

III. **Forma de Trabajo.** Se realizarán reuniones periódicas con el Docente Director del trabajo, para discutir todos los aspectos de la investigación sobre el trabajo escrito y las presentaciones que se realizarán.

IV. **Exposiciones**. Se realizarán dos exposiciones:

- Primera exposición: presentación del perfil del trabajo de investigación.
- Segunfa exposición: presentación final del trabajo de investigación.

Capítulo 1

El Anillo Invariante de Polinomios Simétricos

1.1. Polinomios Simétricos

Se dice que un polinomio $f \in \mathbb{C}[\boldsymbol{x}] := \mathbb{C}[x_1, x_2, \ldots, x_n]$, (donde $\boldsymbol{x} := \{x_1, x_2, \ldots, x_n\}$), es *simétrico* si es invariante bajo cualquier permutación de las variables $x_1, x_2, \ldots, x_n$. Por ejemplo el polinomio $f(x_1, x_2, x_3) = x_1x_2 + x_1x_3$ no es simétrico ya que $f(x_1, x_2, x_3) \neq f(x_2, x_1, x_3) = x_1x_2 + x_2x_3$.
Por otra parte el polinomio $f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ si es simétrico.

Sea z una nueva variable y consideremos el polinomio

$$\begin{aligned} g(z) &= (z - x_1)(z - x_2)\cdots(z - x_n) \\ &= z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \ldots + (-1)^n \sigma_n \end{aligned}$$

Observemos que los coeficientes del polinomio g en la nueva variable z son,

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \ldots + x_n \\ \sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_2x_3 + x_2x_4 + \ldots + x_{n-1}x_n \\ \sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n \\ &\vdots \\ \sigma_n &= x_1x_2x_3\cdots x_{n-2}x_{n-1}x_n \end{aligned}$$

los cuales son simétricos respecto a las variables $x_1, x_2, \ldots, x_n$. Los polinomios $\sigma_1, \sigma_2, \ldots, \sigma_n \in \mathbb{C}[\boldsymbol{x}]$ son llamados *polinomios simétricos elementales.*

Ya que la propiedad de un polinomio de ser simétrico es preservada bajo suma y multiplicación de polinomios, los polinomios simétricos forman un subanillo de $\mathbb{C}[\boldsymbol{x}]$. Esto implica que cualquier expresión en forma de polinomio $p(\sigma_1, \sigma_2, \ldots, \sigma_n)$ en los polinomios simétricos elementales es un polinomio simétrico en $\mathbb{C}[\boldsymbol{x}]$. Por ejemplo, el monomio $c\sigma_1^{\mu_1}\sigma_2^{\mu_2}\ldots\sigma_n^{\mu_n}$ en términos de los polinomios simétricos elementales es simétrico y además es un polinomio homogéneo de grado $\mu_1 + 2\mu_2 + 3\mu_3 + \cdots + n\mu_n$ en las variables originales $x_1, x_2, \ldots, x_n$.

Definición 1.1
Orden Lexicográfico.

Dado $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ y $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Decimos que $\alpha >_{lex} \beta$, si en la diferencia de los vectores $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$, la primera entrada de la izquierda diferente de cero es positiva. En lo que sigue escribiremos $\boldsymbol{x}^\alpha \succ_{lex} \boldsymbol{x}^\beta$ si $\alpha >_{lex} \beta$.

El orden lexicográfico sobre $\mathbb{Z}^n_{\geq 0}$ es un orden monomial.

Definición 1.2
Sea $f := \sum_a \alpha_a x^a \in \mathbb{C}[x_1, \ldots, x_n]$ no nulo, y sea $\prec$ un orden monomial.

a. *El multigrado de f es $mgrad(f) := \max\{a \in \mathbb{Z}^n_{\geq 0} | \quad \alpha_a \neq 0\}$*

b. *El monomio inicial de f es $lm(f) := x^{mgrad(f)}$*

c. *El coeficiente inicial de f es $lc(f) := \alpha_{mgrad(f)}$*

d. *El término inicial de f es $lt(f) := lc(f) \cdot lm(f)$*

Teorema 1.1
(Teorema principal de polinomios simétricos). *[4, pág. 2 y cap. 1] Todo polinomio simétrico $f \in \mathbb{C}[\boldsymbol{x}]$ puede ser escrito de forma única como un polinomio*

$$f(x_1, x_2, \ldots, x_n) = p\left(\sigma_1(x_1, x_2, \ldots, x_n), \sigma_2(x_1, x_2, \ldots, x_n), \ldots, \sigma_n(x_1, x_2, \ldots, x_n)\right)$$

en los polinomios simétricos elementales.

Demostración. Sea $f \in \mathbb{C}[\boldsymbol{x}]$ un polinomio simétrico, entonces el siguiente algoritmo reescribe a f de forma única como un polinomio en $\sigma_1, \sigma_2, \ldots, \sigma_n$.
Para cualquier monomio $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ de f se cumple que todas las imágenes $x_{\pi_1}^{\alpha_1} x_{\pi_2}^{\alpha_2} \cdots x_{\pi_n}^{\alpha_n}$ bajo cualquier permutación π de variables están en f.
Esto implica que el término inicial $lt(f) = cx_1^{\gamma_1} x_2^{\gamma_2} \cdots x_n^{\gamma_n}$ de f satisface que $\gamma_1 > \gamma_2 > \ldots > \gamma_n$. En el algoritmo, reemplazamos f por un nuevo polinomio simétrico $\overset{\smile}{f} = f - c\sigma_1^{\gamma_1-\gamma_2}\sigma_2^{\gamma_2-\gamma_3} \cdots \sigma_{n-1}^{\gamma_{n-1}-\gamma_n}\sigma^{\gamma_n}$, y si $\overset{\smile}{f}$ no es cero, entonces se busca el monomio lexicográficamente más grande de $\overset{\smile}{f}$ y así se vuelve a reescribir $\overset{\smile}{f}$ como se hizo en un principio para f.

Ahora sólo queda ver que la representación de un polinomio simétrico en términos de polinomios simétricos elementales es única. En otras palabras, debemos mostrar que los polinomios simétricos elementales $\sigma_1, \sigma_2, \ldots, \sigma_n$ son algebraicamente independientes sobre $\mathbb{C}$. Supongamos lo contrario, es decir, que existe un polinomio distinto de cero $p(y_1, y_2, \ldots, y_n)$ tal que $p(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$ en $\mathbb{C}[\boldsymbol{x}]$.
Dado cualquier monomio $cy_1^{\alpha_1} y_2^{\alpha_2} \cdots y_n^{\alpha_n}$ de p, se puede encontrar el monomio $x_{\sigma_1}^{\alpha_1+\alpha_2+\ldots+\alpha_n} x_{\sigma_2}^{\alpha_2+\alpha_3+\ldots+\alpha_n} \cdots x_{\sigma_n}^{\alpha_n}$ que es el monomio inicial de $\sigma_1^{\alpha_1}\sigma_2^{\alpha_2} \cdots \sigma_n^{\alpha_n}$.
Ya que la aplicación lineal

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto (\alpha_1 + \alpha_2 + \ldots + \alpha_n, \alpha_2 + \alpha_3 + \ldots + \alpha_n, \ldots, \alpha_n)$$

es inyectiva, todos los otros monomios $\sigma_1^{\beta_1}\sigma_2^{\beta_2} \cdots \sigma_n^{\beta_n}$ en la expansión del polinomio $p(\sigma_1, \sigma_2, \ldots, \sigma_n)$ tienen diferentes monomios iniciales. El monomio más grande $x_1^{\alpha_1+\alpha_2+\ldots+\alpha_n} x_2^{\alpha_2+\ldots+\alpha_n} \cdots x_n^{\alpha_n}$ no es anulado por ningún otro monomio y por lo tanto $p(\sigma_1, \sigma_2, \ldots, \sigma_n) \neq 0$ y esto es una contradicción, lo que completa la prueba. □

Ejemplo 1.1
Se ilustrará el algoritmo anterior escribiendo el polinomio simétrico $f(x_1, x_2) = x_1^3 + x_2^3$ *como un polinomio en los polinomios simétricos elementales. El monomio líder de* f *es* x_1^3*, ahora encontramos* $\overset{\smile}{f} = f - \sigma_1^{3-0}\sigma_2^0 = f - \sigma_1^3 =$

$x_1^3 + x_2^3 - (x_1 + x_2)^3 = -3x_1^2x_2 - 3x_1x_2^2 \neq 0$ *de donde se obtiene que* $f = \widehat{f} + \sigma_1^3$ *, sea* $g = \widehat{f}$ *entonces como* $g \neq 0$ *se vuelve necesario buscar el término líder de* g *que es* $-3x_1^2x_2$ *y calcular* $\widehat{g} = g - (-3\sigma_1^{2-1}\sigma_2) = -3x_1^2x_2 - 3x_1x_2^2 + 3(x_1 + x_2)(x_1x_2) = 0$ *por lo que el algoritmo termina y* $g = -3\sigma_1\sigma_2$ *así* $f = \sigma_1^3 + g$.
$\therefore f = \sigma_1^3 - 3\sigma_1\sigma_2$, *el cual queda escrito en términos de los polinomios simétricos elementales.*

El subanillo $\mathbb{C}[\boldsymbol{x}]^{S_n}$ de polinomios simétricos en $\mathbb{C}[\boldsymbol{x}]$ es el prototipo de un anillo de invariantes. Los polinomios simétricos elementales $\sigma_1, \sigma_2, \ldots, \sigma_n$ forman un *sistema fundamental de invariantes.*

Definición 1.3
El polinomio $P_k(x) := x_1^k + x_2^k + \ldots + x_n^k$ *es llamado la k-ésima suma de potencias.*

Proposición 1.1
El subanillo de polinomios simétricos es generado por las primeras n-ésimas sumas de potencias es decir

$$\mathbb{C}[\boldsymbol{x}]^{S_n} = \mathbb{C}[\sigma_1, \sigma_2, \ldots, \sigma_n] = \mathbb{C}[p_1, p_2, \ldots, p_n]$$

.

Demostración. Una partición de un entero d es un vector de coordenadas enteras $\lambda := (\lambda_1, \lambda_2, \ldots, \lambda_n)$ tal que $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq 0$ y además $\lambda_1 + \lambda_2 + \ldots + \lambda_n = d$. Asignando el monomio $x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}$ de grado d a la partición $\lambda(i_1, i_2, \ldots, i_n)$ la cual es una cadena decreciente ordenada de exponentes. Esto da lugar al siguiente orden monomial en el conjunto de monomios de grado d en $\mathbb{C}[\boldsymbol{x}]$. De manera que $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} \prec x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}$ si la partición $\lambda(i_1, i_2, \ldots, i_n)$ es lexicográficamente más grande que $\lambda(j_1, j_2, \ldots, j_n)$ o si son iguales y $(i_1, i_2, \ldots, i_n)$ es lexicográficamente más pequeño que $(j_1, j_2, \ldots, j_n)$.

Observemos que este orden no es un orden monomial en el conjunto de monomios de $\mathbb{C}[\boldsymbol{x}]$ en el sentido de la teoría de Bases de Groebner. Como un

ejemplo para $n = 3$ y para $d = 4$ se tiene el siguiente orden en los monomios $x_1^4 \prec x_2^4 \prec x_3^4 \prec x_2x_3^3 \prec x_2^3x_3 \prec x_1^2x_3^2 \prec x_1^2x_2^2 \prec x_1x_2x_3^2 \prec x_1x_2^2x_3 \prec x_1^2x_2x_3$. Observemos que el término inicial de un producto de sumas de potencia es igual a $lt(p_{i_1}p_{i_2}\dots p_{i_n}) = c_{i_1i_2\dots i_n} \cdot x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$, siempre y cuando $i_1 \geq i_2 \geq \dots \geq i_n$, donde $c_{i_1i_2\dots i_n}$ es un entero positivo. Ahora estamos preparado para describir un algoritmo que demuestra la **Proposición 1.1**. Reescribiremos un polinomio simétrico dado $f \in \mathbb{C}[\boldsymbol{x}]$ como una función polinómica en $p_1, p_2, \dots, p_n$. Por el **Teorema 1.1**, se puede suponer que f es uno de los polinomios simétricos elementales. En particular, el grado d de f es inferior o igual a n. Su termino inicial viene dado por $lt(f) = cx_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ en donde $n \geq i_1 \geq i_2 \geq \dots \geq i_n$. Reemplazaremos a f por $\overset{\smile}{f} = f - \frac{c}{c_{i_1i_2\dots in}}p_{i_1}p_{i_2}\cdots p_{i_n}$. Por la observación anterior los términos iniciales en esta diferencia se anulan, y se tiene $lt(\overset{\smile}{f}) \prec lt(f)$. Ya que tanto f y $\overset{\smile}{f}$ tienen el mismo grado d, este proceso termina con el resultado esperado.

□

Ejemplo 1.2

Mostraremos con este ejemplo el proceso de reescribir el polinomio $f = x_1x_2x_3$ en función de p_1, p_2 y p_3 siguiendo el algoritmo de la prueba del teorema anterior.

Usando el método anterior se tiene

$$\begin{aligned} x_1x_2x_3 &\to \frac{1}{6}p_1^3 - \frac{1}{2}\sum_{i\neq j}x_ix_j - \frac{1}{6}\sum_k x_k^3 \\ &\to \frac{1}{6}p_1^3 - \frac{1}{2}\left(p_1p_2 - \sum_k x_k^3\right) - \frac{1}{6}\sum_k x_k^3 \\ &\to \frac{1}{6}p_1^3 - \frac{1}{2}p_1p_2 + \frac{1}{3}p_3 \end{aligned}$$

El **Teorema 1.1** y la **Proposición 1.1** nos muestran que los monomios de los polinomios simétricos elementales y los monomios en la series de potencias son ambas bases para el $\mathbb{C}$-espacio vectorial del anillo de polinomios simétricos $\mathbb{C}[\boldsymbol{x}]^{S_n}$.

1.2. Bases de Groebner

En esta sección daremos la teoría necesaria para calcular una base Groebner para un ideal $I \subset \mathbb{C}[\boldsymbol{x}]$. Para esto es necesario establecer un orden entre los términos de un polinomio $f \in \mathbb{C}[\boldsymbol{x}]$.

En el estudio de los polinomios simétricos, las bases de Groebner permiten determinar si un polinomio es simétrico, y de ser así dar un algoritmo el cual reescriba un polinomio simétrico dado en función de los polinomios simétricos elementales definidos anteriormente.
Daremos una breve introducción a la teoría de bases de Groebner cuyo propósito general es encontrar generadores de polinomios en varias variables. Estos conceptos fueron introducidos por Bruno Buchberger en 1965 en donde las bases de Groebner son una versión del algoritmo de Euclides el cual funciona también para más de una variable.
Sea $g \in \mathbb{C}[\boldsymbol{x}]$, se denota $lt(g)$ al *término líder* del polinomio g, esto es el producto de potencias más grande con coeficiente diferente de cero en el polinomio g con respecto a "$\prec$". El *ideal inicial* denotado por $init(I)$ asociado con un ideal $I \subset \mathbb{C}[\boldsymbol{x}]$ es el ideal monomial generado por $\{lt(f) : f \in I\}$. Con ello se da paso a definir lo que es una base Groebner.

Definición 1.4
Un conjunto $G = \{g_1, g_2, \ldots, g_k\}$ de generadores para I se dice que es una base de Groebner para I con respecto al orden "$\prec$" si el ideal inicial $init(I)$ está generado por:

$$\{lt(g_1), lt(g_2), \ldots, lt(g_k)\}.$$

En la definición anterior una base de Groebner se dice reducida si ningún $lt(g_i)$ divide a los monomios de g_j para todo $i, j \in \{1, 2, \ldots, k\}$ distintos.
Los monomios $m \notin init(I)$ son llamados *estándar* y los monomios $m \in init(I)$ son llamados *no estándar*.

Proposición 1.2
Sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner para un ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$ y sea $f \in \mathbb{C}[x_1, \ldots, x_n]$. Entonces existe un único $r \in \mathbb{C}[x_1, \ldots, x_n]$ con las siguientes dos propiedades:

(I) Ningún término de r es divisible por cualquiera de los términos líderes: $lt(g_1), \ldots, lt(g_t)$

(II) Existe algún $g \in I$ tal que $f = g + r$

En particular, r es el residuo de f en G sin importar cuántos elementos de G son listados al utilizar el algoritmo de la división.

Demostración. Por el algoritmo de la división [1, pág. 64, cap. 2], tenemos que $f = a_1 g_1 + \ldots + a_t g_t + r$, donde r satisface la condición (I). Incluso podemos ver que satisface la condición (II), tomando $g = a_1 g_1 + \cdots + a_t g_t \in I$, Esto prueba la existencia de r.
Para probar la unicidad, supóngase que $f = g + r = g' + r'$ satisfaciendo (I) y (II). $\Rightarrow r - r' = g' - g \in I$, así que si $r \neq r'$, entonces $lt(r - r') \in \langle lt(I) \rangle = \langle lt(g_1), \ldots, lt(g_t) \rangle$. Entonces se tiene que, $lt(r - r')$ es divisible por algún $lt(g_i)$. Esto último es imposible, ya que ningún término de r, r' es divisible por uno de los términos lideres $lt(g_1), \ldots, lt(g_t)$. Así $r - r'$ debe ser cero, y la unicidad está probada. □

Corolario 1.1
(Pertenencia a un ideal). *Sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner para un ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$ y sea $f \in \mathbb{C}[x_1, \ldots, x_n]$. Entonces $f \in I$ si y sólo si el residuo de f en G es cero.*

Demostración. Si el residuo es cero, entonces ya hemos observado que $f \in I$. Recíprocamente, dado $f \in I$, entonces $f = f + 0$ satisface las dos condiciones de la **Proposición 1.2**. Se sigue que 0 es el residuo de f en la división por G. □

Ejemplo 1.3
Con ayuda del algoritmo de Buchberger [1, pág. 90, cap. 2] se encontrará

una base de Groebner para el ideal $I = \langle y - x^2, z - x^3 \rangle \subset \mathbb{R}^3$. *Tenemos que* $G = \{y - x^2, z - x^3\}$ *es una base de Groebner con el orden lexicográfico* $y > z > x$. *Para probar esto, consideremos el S-polinomio*

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = yx^3 - zx^2$$

Usando el algoritmo de la división, encontramos que

$$yx^3 - zx^2 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0$$

Así que $\overline{S(y - x^2, z - x^3)}^G = 0$ *y por el* ***Corolario 1.1****,* G *es una base de Groebner para* I.

Lema 1.1
(Hilbert 1890, Gordan 1900). *Cada ideal monomial* M *es finitamente generado por monomios.*

Demostración. Si procedemos por inducción sobre n, el número de variables del anillo de polinomios. Si $n = 1$, entonces estamos en el caso de $\mathbb{C}[x_1]$ y en este anillo por definición un ideal monomial M es de la forma $\left\{x^j : j \in J\right\}$ donde J es algún conjunto de enteros no negativos.

Sabemos que el conjunto J tiene un elemento minimal, supóngase que es j_0, entonces el ideal monomial es generado por el único monomio $\left\{x^{j_0}\right\}$, por tanto es finitamente generado y así se cumple para $n = 1$.

Ahora suponiendo que el **Lema 1.1** es cierto para $n - 1$ variables. Para cada $j \in \mathbb{N}$, consideremos el ideal monomial M_j en $n - 1$ variables generado por todos los monomios $m \in \mathbb{C}[x_1, x_2, \ldots, x_{n-1}]$ tal que $m \cdot x_n^j \in M$. Luego por hipótesis inductiva el ideal monomial M_j es finitamente generado, es decir M_j es generado por un conjunto finito S_j de monomios. Observemos la siguiente inclusión $M_0 \subseteq M_1 \subseteq, \ldots, \subseteq M_j \subseteq M_{j+1} \subseteq \ldots$, por la hipótesis de inducción, además el ideal monomial $\bigcup_{j=0}^{\infty} M_j$ es finitamente generado. Esto implica la existencia de un entero r tal que $M_r = M_{r+1} = M_{r+2} = \ldots$, por lo que se deduce que un monomio $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n}$ pertenece a M si y sólo si $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_{n-1}^{\alpha_{n-1}}$ pertenece a M_t, donde $t = min\{r, \alpha_n\}$.

De aquí que el conjunto finito de monomios $\bigcup_{j=0}^{r} S_j \cdot x_n^j$ genera a M. □

Corolario 1.2
Sea "$\prec$" cualquier orden monomial en $\mathbb{C}[\boldsymbol{x}]$. Entonces no hay una cadena descendente infinita de monomios $m_1 \succ m_2 \succ m_3 \succ \ldots$

Demostración. Consideremos cualquier conjunto infinito $\{m_1, m_2, m_3, \ldots\}$ de monomios en $\mathbb{C}[\boldsymbol{x}]$. Ahora por el lema anterior este ideal es finitamente generado. Por lo tanto existe un entero j tal que $m_j \in \langle m_1, m_2, m_3, \ldots, m_{j-1}\rangle$ esto significa que m_i divide a m_j para todo $i < j$. Ya que "$\prec$" es un orden monomial esto implica que $m_i < m_j$ para $i < j$. □

Teorema 1.2 I. *Cada ideal $I \subset \mathbb{C}[\boldsymbol{x}]$ tiene una base de Groebner G para cualquier orden monomial "$\prec$".*

II. *Cada base de Groebner G genera su propio ideal I.*

Demostración. El literal I) lo podemos deducir directamente del **Lema 1.1** y la definición de bases de Groebner. Probaremos el literal II) por reducción al absurdo.

Supongamos que las bases de Groebner G no generan sus ideales, es decir, el conjunto $I/\langle G\rangle$ no es vacío.
Por el **Corolario 1.2** el conjunto de términos iniciales $\{lt(f) : f \in I/\langle G\rangle\}$ tiene un elemento minimal $lt(f_0)$ con respecto a "$\prec$". El término $lt(f_0)$ pertenece al ideal $init(I) = \langle init(G)\rangle$.
Sea $g \in G$ tal que $lt(g)$ divide a l $lt(f_0)$ es decir $lt(f_0) = m \cdot lt(g)$.
Ahora consideremos el polinomio $f_1 := f_0 - m \cdot g$, por construcción el polinomio $f_1 \in I/\langle G\rangle$. Pero además tenemos que $lt(f_1) \prec lt(f_0)$.
Esto contradice la minimalidad en la elección de f_0, por lo tanto las bases de Groebner G generan su ideal I. □

A partir de este obtenemos como consecuencia directa el siguiente resultado.

Teorema 1.3
(Teorema de la base de Hilbert). *Cada ideal en el anillo de polinomios* $\mathbb{C}[\boldsymbol{x}]$ *es finitamente generado.*

Demostración. Si $I = \{0\}$, entonces el conjunto finito $\{0\}$ es un conjunto de generadores. Si I contiene algún polinomio distinto de cero, entonces, existen $g_1, \ldots, g_s \in I$ tales que $init(I) = \langle lt(g_1), \ldots, lt(g_s)\rangle$. Afirmamos que $I = \langle g_1, \ldots, g_s\rangle$.
Es claro que $\langle g_1, \ldots, g_s\rangle \subset I$, puesto que cada $g_i \in I$. Ahora sea $f \in I$ cualquier polinomio. Si aplicamos el algoritmo de la división para dividir f entre $g_1, \ldots, g_s$, obtenemos una expresión de la forma

$$f = a_1 g_1 + \ldots + a_t g_t + r$$

donde cada término de r no es divisible por ninguno de los $lt(g_1), \ldots, lt(g_t)$. Si escribimos

$$r = f - a_1 g_1 - \ldots - a_t g_t \in I$$

y suponemos que $r \neq 0$, entonces $lt(r) \in init(I) = \langle lt(g_1), \ldots, lt(g_s)\rangle$, por lo que $lt(r)$ debe ser divisible por algún $lt(g_i)$, lo cual contradice el hecho de ser un residuo distinto de cero, y por lo tanto, r debe ser cero.
Con esto tenemos

$$f = a_1 g_1 + \ldots + a_t g_t + 0 \in \langle g_1, \ldots, g_s\rangle,$$

lo que muestra que $I \subset \langle g_1, \ldots, g_s\rangle$. Esto termina la prueba. □

Teorema 1.4
Sea I un ideal y sea $\prec$ cualquier orden monomial en $\mathbb{C}[\boldsymbol{x}]$, entonces se cumple que el conjunto de monomios estándar es una $\mathbb{C}$-base para el anillo $\mathbb{C}[\boldsymbol{x}]/I$ de residuos módulo I.

Demostración. Sea G una base de Groebner para I, y consideremos el siguiente algoritmo que calcula las clases de residuo módulo I.
Entrada: $p \in \mathbb{C}[\boldsymbol{x}]$.

1. Comprobar si todos los monomios en p son estándar. Si es así, hemos terminado: p está en forma normal y módulo equivalente I del polinomio de entrada.

2. De lo contrario sea $hnst(p)$ el más grande monomio que no es estándar en p. Encontrar $g \in G$ talque el $lt(g)$ divide a $hnst(p)$ es decir $m \cdot lt(g) = hnst(p)$.

3. Reemplazar p por $\widetilde{p} = p - m \cdot p$ y luego regresar al paso 1.

Ahora se tiene que $lt(\widetilde{p}) \prec lt(p)$ en el paso 3 y por lo tanto por el **Corolario 1.2** implica que el algoritmo termina con una representación para $p \in \mathbb{C}[\boldsymbol{x}]$ como una combinación $\mathbb{C}$-lineal de monomios estándar módulo I. Se concluye la demostración del **Teorema 1.4** observando que tal representación es necesariamente única, ya que, por definición, cada polinomio en I contiene al menos un monomio no estándar. Esto significa que el polinomio cero no se puede escribir como combinación lineal no trivial de monomios estándar en $\mathbb{C}[\boldsymbol{x}]/I$. □

Sea I el ideal de $\mathbb{C}[\boldsymbol{x}, \boldsymbol{y}] = \mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_n]$, el cual es generado por todos los polinomios de la forma $\sigma_i(x_1, x_2, \ldots, x_n) - y_i$ donde $i = 1, 2, \ldots, n$ y cada σ_i es el polinomio simétrico elemental. En otras palabras, I es el ideal de todas las relaciones algebraicas entre las raíces y los coeficientes de un polinomio genérico en una variable.

Definición 1.5
El i-ésimo polinomio simétrico completo h_i es definido por la suma de todos los monomios de grado i dado un conjunto de variables. En particular

$$h_i(x_k, x_{k+1}, \ldots, x_n) = \sum_{\nu_k + \nu_{k+1} + \ldots + \nu_n = i} x_k^{\nu_k} x_{k+1}^{\nu_{k+1}} \cdots x_n^{\nu_n}.$$

Teorema 1.5
La única base de Groebner reducida de I, con respecto al orden monomial lexicográfico inducido de $x_1 \succ x_2 \succ \ldots \succ x_n \succ y_1 \succ y_2 \ldots \succ y_n$ es igual a

$$G = \left\{ h_k(x_k, \ldots, x_n) + \sum_{i=1}^{k} (-1)^i h_{k-i}(x_k, \ldots, x_n) y_i : k = 1, 2, \ldots, n \right\}.$$

Demostración. En la prueba utilizaremos algunos resultados sobre polinomios simétricos y desarrollo de Hilbert de álgebras graduadas. Observemos en primer lugar la siguiente identidad del polinomios simétricos

$$h_k(x_k,\ldots,x_n)+\sum_{i=1}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)\sigma_i(x_1,\ldots,x_{k-1},x_k,\ldots,x_n)=0.$$

Esta identidad muestra que G es un subconjunto del ideal I. Introduciendo el grado en $\mathbb{C}[\boldsymbol{x},\boldsymbol{y}]$ asiendo $grad(x_i)=1$ y $grad(y_j)=j$. El ideal I es homogéneo con respecto a este grado. El anillo cociente $\mathbb{C}[\boldsymbol{x},\boldsymbol{y}]/I$ es isomorfo como una álgebra graduada a $\mathbb{C}[x_1,\ldots,x_n]$ y por lo tanto la serie de Hilbert de $R=\bigoplus_{d=0}^{\infty}R_d$ es igual a

$$H(R,z)=\sum_{d=0}^{\infty}\dim_{\mathbb{C}}(R_d)\,z^d=(1-z)^{-n}.$$

Ahora por el **Teorema 1.4** tenemos que el cociente $\mathbb{C}[\boldsymbol{x},\boldsymbol{y}]/init_{\prec}(I)$ módulo el ideal inicial tiene la misma serie de Hilbert $(1-z)^{-n}$. Consideremos el ideal monomial $J=\langle x_1,x_2^2,x_3^3,\ldots,x_n^n\rangle$, generado por los monomios iniciales de los elementos de G, observemos que $J\subset init_{\prec}(I)$, y que la otra inclusión también se cumple. Para la prueba de esta afirmación se verifica que la serie de Hilbert de $R':=\mathbb{C}[\boldsymbol{x},\boldsymbol{y}]/J$ es igual a la serie de Hilbert de R.
Una base para el espacio vectorial R' es dado por el conjunto de todos los monomios $x_1^{i_1}\ldots x_n^{i_n}y_1^{j_1}\ldots y_n^{j_n}$ cuyos exponentes satisfacen las restricciones $i_1<1,\ i_2<2,\ldots,i_n<n$. Esto muestra que la serie de Hilbert de R' es igual a

$$H(R',z)=\left(\sum z^{i_1+i_2+\ldots+i_n}\right)\left(\sum z^{j_1+2j_2+\ldots+nj_n}\right).$$

El segundo sumando es sobre todos los $(j_1,j_2,\ldots,j_n)\in\mathbf{N}^n$ y esto es igual a $\left[(1-z)(1-z^2)\cdots(1-z^n)\right]^{-1}$. El primer sumando es sobre todos los vectores de la forma $(i_1,i_2,\ldots,i_n)\in\mathbf{N}^n$ con $i_\mu<\mu$ y por lo tanto, es igual al polinomio $(1+z)(1+z+z^2)\cdots(1+z+z^2+\ldots+z^{n-1})$. Encontramos el producto de los polinomios anteriores como se sigue:

$$\begin{aligned} H(R', z) &= \left(\frac{1}{1-z}\right)\left(\frac{1+z}{1-z^2}\right)\left(\frac{1+z+z^2}{1-z^3}\right)\cdots\left(\frac{1+z+z^2+\ldots+z^{n-1}}{1-z^n}\right) \\ &= \left(\frac{1}{1-z}\right)\left(\frac{1}{1-z}\right)\left(\frac{1}{1-z}\right)\cdots\left(\frac{1}{1-z}\right) \\ &= H(R, z) \end{aligned}$$

y esto completa la prueba. □

Lema 1.2
Sea G una base de Groebner para el ideal polinomial I. Sea $p \in G$ un polinomio tal que $lt(p) \in init(G - \{p\})$. Entonces $G - \{p\}$ es también una base de Groebner para I.

Demostración. Sabemos que $init(G) = init(I)$. Si $lt(p) \in init(G-p)$, entonces $lt(G - \{p\}) = lt(G)$. De la definición, se sigue que $G - \{p\}$ es también una base de Groebner para I. □

Capítulo 2

Teoría de Invariantes bajo la Acción de Grupos Finitos

2.1. Cantidad de Invariantes

En el presente capítulo estudiaremos los anillos de polinomios invariantes bajo la acción de grupos finitos y daremos respuesta al problema de cuántos invariantes existen dado un grupo finito de matrices dado y de qué grado.

Estamos interesados en estudiar polinomios en el anillo $\mathbb{C}[\boldsymbol{x}]$ que quedan invariantes bajo la acción de ciertos grupos finitos de matrices $\Gamma \subset GL(\mathbb{C}^n)$.

El resultado principal de este capítulo es una colección de algoritmos para encontrar un conjunto finito $\{I_1, I_2, \ldots, I_m\}$ de invariantes fundamentales, los cuales generen el subanillo invariante $\mathbb{C}[\boldsymbol{x}]^\Gamma$.

Proposición 2.1
Para cada grupo finito de matrices $\Gamma \subset GL(\mathbb{C}^n)$, el anillo $\mathbb{C}[\boldsymbol{x}]^\Gamma$ tiene exactamente n invariantes algebraicamente independientes, es decir el anillo $\mathbb{C}[\boldsymbol{x}]^\Gamma$ tiene transcendencia de grado n sobre $\mathbb{C}$.

Demostración. Para cada $i \in \{1, 2, \ldots, n\}$ definimos:

$P_i := \prod_{\pi \in \Gamma} (x_i \circ \pi - t) \in \mathbb{C}[\boldsymbol{x}][t]$. Luego Considérese a $P_i = P_i(t)$ un polinomio mónico visto como un polinomio en la variable t, en el cual sus coeficientes

están en $\mathbb{C}[\boldsymbol{x}]$. Entonces P_i es un polinomio invariante bajo la acción de Γ en la *x-variables* estos coeficientes son invariantes. En otras palabras este polinomio está en $\mathbb{C}[\boldsymbol{x}]^\Gamma[t]$.
Notamos que $t = x_i$ es una raíz del polinomio $P_i(t)$ porque una de las matrices $\pi \in \Gamma$ en la definición de P es igual a la identidad. Esto significa que todas las variables $x_1, \ldots, x_n$ son algebraicamente dependientes salvo ciertos invariantes. Así el subanillo de invariantes $\mathbb{C}[\boldsymbol{x}]^\Gamma$ y el anillo completo de polinomios $\mathbb{C}[\boldsymbol{x}]$ tienen la misma trascendencia de grado n sobre el campo $\mathbb{C}$. □

Definición 2.1
El operador de Reynold "" esta definido por*

$$\begin{aligned} * : \mathbb{C}[\boldsymbol{x}] &\to \mathbb{C}[\boldsymbol{x}]^\Gamma \\ f &\longmapsto f^* := \frac{1}{\mid \Gamma \mid} \sum_{\pi \in \Gamma} f \circ \pi. \end{aligned}$$

De la definición anterior podemos deducir las siguientes propiedades del operador de Reynold.

Proposición 2.2
El operador de Reynold tiene las siguientes propiedades:

1) "" es una aplicación $\mathbb{C}$-lineal, es decir $(\lambda f + \nu g)^* = \lambda f^* + \nu g^*$ para todo $f, g \in \mathbb{C}[\boldsymbol{x}]$ y para todo $\lambda, \nu \in \mathbb{C}$.*

2) "" restringido a $\mathbb{C}[\boldsymbol{x}]^\Gamma$ es la aplicación identidad, es decir $I = I^*$ para todo invariante $I \in \mathbb{C}[\boldsymbol{x}]^\Gamma$.*

3) "" es un homomorfismo de $\mathbb{C}[\boldsymbol{x}]^\Gamma$-módulo, es decir $(fI)^* = f^*I$ para todo $f \in \mathbb{C}[\boldsymbol{x}]$ y para todo invariante $I \in \mathbb{C}[\boldsymbol{x}]^\Gamma$.*

Demostración. 1. Sean $\lambda, \nu \in \mathbb{C}$ y sean $f, g \in \mathbb{C}[\boldsymbol{x}]$ y como Γ es un grupo

que actúa linealmente en el anillo $\mathbb{C}[\boldsymbol{x}]$ entonces

$$\begin{aligned}(\lambda f+\nu g)^* &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}(\lambda f+\nu g)\circ\pi\\ &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}[(\lambda f)\circ\pi+(\nu g)\circ\pi]\\ &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}[\lambda(f\circ\pi)+\nu(g\circ\pi)]\\ &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}\lambda(f\circ\pi)+\frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}\nu(g\circ\pi)\\ &= \lambda\frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}f\circ\pi+\nu\frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}g\circ\pi\\ &= \lambda f^*+\nu g^*\end{aligned}$$

Así, "$*$" es una aplicación lineal sobre $\mathbb{C}$.

2. Sea $I\in\mathbb{C}[\boldsymbol{x}]^\Gamma\subset\mathbb{C}[\boldsymbol{x}]$ entonces

$$\begin{aligned}I^* &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}I\circ\pi=\frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}I\\ &= \frac{1}{\mid\Gamma\mid}(\mid\Gamma\mid\cdot I)=I\end{aligned}$$

3. Ahora para probar que "$*$" es un homomorfismo de $\mathbb{C}[\boldsymbol{x}]^\Gamma$-módulos, tomemos $f,g\in\mathbb{C}[\boldsymbol{x}]$, $I\in\mathbb{C}[\boldsymbol{x}]^\Gamma$, tenemos:

$$\begin{aligned}(f+g)^* &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}(f+g)\circ\pi\\ &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}(f\circ\pi)+\frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}(g\circ\pi)\\ &= f^*+g^*\end{aligned}$$

$$\begin{aligned}(If)^* &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}(If)\circ\pi\\ &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}(I\circ\pi)(f\circ\pi)\\ &= \frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}I(f\circ\pi)\\ &= I\frac{1}{\mid\Gamma\mid}\sum_{\pi\in\Gamma}(f\circ\pi)\\ &= If^*\end{aligned}$$

Lo que completa la prueba.

□

Teorema 2.1
(Teorema de finitud de Hilbert). *El anillo invariante* $\mathbb{C}[\boldsymbol{x}]^\Gamma$ *de un grupo finito de matrices* $\Gamma \subset GL(\mathbb{C}^n)$ *es finitamente generado.*

Demostración. Sea $\mathcal{I}_\Gamma = \langle \mathbb{C}[\boldsymbol{x}]^\Gamma_+ \rangle$ el ideal en $\mathbb{C}[\boldsymbol{x}]$, el cual está generado por todos los invariantes homogéneos de grado positivo. Por la **Proposición 2.2**, cada invariante I es una combinación $\mathbb{C}$-lineal de monomios simétricos $(x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n})^*$. Estos invariantes homogéneos son la imagen de monomios bajo el operador de Reynold. Esto implica que el ideal $\mathcal{I}_\Gamma$ está generado por los polinomios $(x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n})^*$, donde $e = (e_1, e_2, \ldots, e_n)$ se extiende sobre todos los vectores no nulos con entradas enteras no negativas. Por el teorema de la base de Hilbert (**Teorema 1.3**), cada ideal en el anillo de polinomio $\mathbb{C}[\boldsymbol{x}]$ es finitamente generado. Así existe un número finito de invariantes homogéneos $I_1, I_2, \ldots, I_m$ tal que $\mathcal{I}_\Gamma = \langle I_1, I_2, \ldots, I_m \rangle$. Probaremos que todo invariante homogéneo $I \in \mathbb{C}[\boldsymbol{x}]^\Gamma$ puede ser escrito como funciones polinomiales en $I_1, I_2, \ldots, I_m$.
Supongamos lo contrario, y sea I un elemento homogéneo de grado mínimo en
$\dfrac{\mathbb{C}[\boldsymbol{x}]^\Gamma}{\mathbb{C}[I_1, I_2, \ldots I_m]}$. Ya que $I \in \mathcal{I}_\Gamma$, se tiene $I = \displaystyle\sum_{j=1}^{s} f_j I_j$ para algunos polinomios homogéneos $f_j \in \mathbb{C}[x]$ de grado menor que $deg(I)$.
Aplicando el operador de Reynold en ambos lados de esta ecuación tenemos:

$$I = I^* = \left(\sum_{j=1}^{s} f_j I_j\right)^* = \sum_{j=1}^{s} f_j^* I_j$$

De la **Proposición 2.2**, los nuevos coeficientes f_j^* son invariantes homogéneos cuyo grado es menor que $deg(I)$. De la suposición de minimalidad en I, tomamos $f_j^* \in \mathbb{C}[I_1, \ldots, I_m]$ y por tanto $I \in \mathbb{C}[I_1, \ldots, I_m]$, lo cual es una contradicción a la suposición que se ha hecho. □

Teorema 2.2
(La cota del grado de Noether) *El anillo invariante* $\mathbb{C}[\boldsymbol{x}]^\Gamma$ *de un grupo finito de matrices* Γ *tiene una base algebraica consistiendo a lo más de* $\binom{n+|\Gamma|}{n}$

invariantes cuyo grado está acotado superiormente por el orden del grupo, $|\Gamma|$.

Demostración. Para cada vector $\boldsymbol{e} = (e_1, e_2, \ldots, e_n)$ de enteros no negativos, asociamos el invariante homogéneo $\boldsymbol{J}_e(x) = (x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n})^*$ el cual es obtenido aplicando el operador de Reynold al monomio con exponente el vector $\boldsymbol{e}$. Sea $e = |\boldsymbol{e}| = e_1 + e_2 + \ldots + e_n$ y $u_1, u_2, \ldots, u_n$ un nuevo conjunto de variables, consideremos el siguiente polinomio:

$$\begin{aligned} S_e(\boldsymbol{u}, \boldsymbol{x}) &= \{(x_1 u_1 + \ldots + x_n u_n)^e\}^* \\ &= \frac{1}{|\Gamma|} \sum_{\pi \in \Gamma} [u_1(x_1 \circ \pi) + \ldots + u_n(x_n \circ \pi)]^e \end{aligned}$$

en las nuevas variables cuyos coeficientes son polinomios en las variables $x_1, \ldots, x_n$. El operador de Reynold "$*$", actúa sobre dichos polinomios considerando a u_i como constantes. Por la expansión completa de la expresión anterior, encontramos que el coeficiente de $u_1^{e_1} \cdots u_n^{e_n}$ en S_e es el invariante $\boldsymbol{J}_e$.
Los polinomios S_e son las sumas de potencia de los $|\Gamma|$ polinomios

$u_1(x_1 \circ \pi) + \ldots + u_n(x_n \circ \pi)$ donde π varía sobre todo Γ. Ahora por la **Proposición 1.1** se puede expresar cada suma de potencias S_e en términos de las primeras $|\Gamma|$ sumas de potencias de $S_1, S_2, \ldots, S_{|\Gamma|}$. Tal representación de S_e muestra que los u-coeficientes son funciones polinomiales en los u-coeficientes de $S_1, S_2, \ldots, S_{|\Gamma|}$.
Este argumento prueba que el polinomio invariante $\boldsymbol{J}_e$ con $|\boldsymbol{e}| > |\Gamma|$ está contenido en el subanillo $\mathbb{C}[\{\boldsymbol{J}_e : |\boldsymbol{e}| < |\Gamma|\}]$.
Hemos observado que cada invariante es una combinación $\mathbb{C}$-lineal de los invariantes especiales $\boldsymbol{J}_e$. Esto implica que

$$\mathbb{C}[\boldsymbol{x}]^\Gamma = \mathbb{C}[\{\boldsymbol{J}_e :| \boldsymbol{e} |<| \Gamma |\}].$$

El conjunto de vectores $\boldsymbol{e} \in \mathbb{N}^n$ talque $|\boldsymbol{e}| < |\Gamma|$ tiene cardinalidad $\binom{n+|\Gamma|}{n}$. □

Proposición 2.3
Para cualesquiera dos enteros $n, p \geq 2$*, existen p-elementos del grupo*

$\Gamma \subset GL(\mathbb{C}^n)$ *tal que cada base algebraica para* $\mathbb{C}[\boldsymbol{x}]^\Gamma$ *contiene a lo más* $\binom{n+p-1}{n-1}$ *invariantes de grado* d.

Demostración. Considerando la acción del grupo cíclico de p-elementos en $\mathbb{C}^n$ dado

$$\Gamma := \left\{ diag\left(e^{\frac{2\pi ki}{p}}, e^{\frac{2\pi ki}{p}}, \ldots, e^{\frac{2\pi ki}{p}}\right) : k = 0, 1, \ldots, p-1 \right\}.$$

Ahora se puede determinar fácilmente la acción del operador de Reynold en todos los monomios:

$$(x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n})^* = \begin{cases} x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} & p/e = e_1 + \ldots + e_n \\ 0 & \text{otro caso} \end{cases}$$

Esto muestra que el anillo invariante $\mathbb{C}[\boldsymbol{x}]^\Gamma$ es la *subálgebra veronese* de $\mathbb{C}[\boldsymbol{x}]$, la cual es generada por todos los monomios de grado p. Cualquier base algebraica graduada de este anillo debe contener una base para el $\mathbb{C}$-espacio vectorial de dimensión $\binom{n+p-1}{n-1}$ de polinomios en n variables de grado p. □

Sea $\mathbb{C}[\boldsymbol{x}]_d^\Gamma$ el conjunto de todos los invariantes homogéneos de grado d.

Definición 2.2
Se define la serie de Hilbert del anillo invariante $\mathbb{C}[\boldsymbol{x}]^\Gamma$ *como la siguiente función:*

$$\Phi_\Gamma(z) = \sum_{d=0}^{\infty} \dim(\mathbb{C}[\boldsymbol{x}]_d^\Gamma) z^d$$

El siguiente teorema nos da una forma explícita para calcular la serie de Hilbert del anillo invariante $\mathbb{C}[\boldsymbol{x}]^\Gamma$ en términos de las matrices π de Γ.

Teorema 2.3
(Molien 1987). *La serie de Hilbert del anillo invariante* $\mathbb{C}[\boldsymbol{x}]^\Gamma$ *es igual a*

$$\Phi_\Gamma(z) = \frac{1}{|\Gamma|} \sum_{\pi \in \Gamma} \frac{1}{\det(id - z\pi)}.$$

Lema 2.1
Sea $\Gamma \subset GL(\mathbb{C}^n)$ *un grupo finito de matrices. Entonces la dimensión del*

subespacio invariante $V^\Gamma = \{v \in \mathbb{C}^n : \pi v = v, \forall \pi \in \Gamma\}$ *es igual a*

$$\frac{1}{|\Gamma|}\sum_{\pi\in\Gamma} traza(\pi).$$

Demostración. Sea $P_\Gamma = \frac{1}{|\Gamma|}\sum_{\pi\in\Gamma}\pi$ la matriz promedio. Esta aplicación lineal es una proyección en el subespacio invariante V^Γ. Ya que la matriz P_Γ define una proyección, se tiene $P_\Gamma = P_\Gamma^2$, lo cual significa que P_Γ tiene solamente los autovalores 0 y 1; por lo que el rango de la matriz P_Γ es igual a la multiplicidad del autovalor 1, y así se puede encontrar que

$$dim(V^\Gamma) = rango(P_\Gamma) = traza(P_\Gamma) = \frac{1}{\mid \Gamma \mid}\sum_{\pi\epsilon\Gamma} traza(\pi).$$

□

El **Teorema 2.3** afirma en otras palabras, que la serie de Hilbert del anillo invariante es el promedio de los polinomios característicos invertidos de todos los elementos de grupo.

Demostración. **(Teorema 2.3)** Denotaremos por $\mathbb{C}[x]_d$ al espacio vectorial de dimensión $\binom{n+d-1}{d}$ de los polinomios de grado d en $\mathbb{C}[x]$. Para toda transformación lineal $\pi \in \Gamma$ existe una transformación lineal inducida $\pi^{(d)}$ en el espacio vectorial $\mathbb{C}[x]_d$ con respecto al grupo inducido $\left\{\pi^{(d)} : \pi \in \Gamma\right\}$ de las matrices de dimensión $\binom{n+d-1}{d} \times \binom{n+d-1}{d}$. Para calcular la traza de la transformación inducida $\pi^{(d)}$ vamos a identificar al espacio vectorial $\mathbb{C}^n$ como el espacio lineal $\mathbb{C}[x]_1$. Sea $l_{\pi,1}, l_{\pi,2}, l_{\pi,3}, \ldots, l_{\pi,n} \in \mathbb{C}[x]_1$ los autovectores de $\pi = \pi^1$ y sean $p_{\pi,1}, p_{\pi,2}, p_{\pi,3}, \ldots, p_{\pi,n} \in \mathbb{C}$ los autovalores correspondientes.

Notemos que cada matriz $\pi \in \Gamma$ es diagonalizable sobre $\mathbb{C}$ ya que es de orden finito. Los autovalores de $\pi^{(d)}$ son precisamente las $\binom{n+d-1}{d}$ formas $l_{\pi,1}, l_{\pi,2}, l_{\pi,3}, \ldots, l_{\pi,n} \in \mathbb{C}[x]_1$ donde $d_1 + d_2 + \ldots + d_n = d$. Ya que la traza de las transformaciones lineales es igual a la suma de sus autovalores, por lo que tenemos la siguiente ecuación

$$traza(\pi^{(d)}) = \sum_{d_1+d_2+\ldots+d_n=d} p_{\pi,1}^{d_1}, p_{\pi,2}^{d_2}, p_{\pi,3}^{d_3}, \ldots, p_{\pi,n}^{d_n}.$$

Por el lema anterior la dimensión del subespacio invariante $\mathbb{C}[x]_d^\Gamma$ es igual al promedio de las trazas de todos los elementos del grupo. Reescribiendo esta dimensión en términos de las series de Hilbert para anillos de invariantes, tenemos

$$\begin{aligned}
\Phi_d(z) &= \sum_{d=0}^{\infty} \frac{1}{\mid \Gamma \mid} \left(\sum_{\pi \in \Gamma} p_{\pi,1}^{d_1}, p_{\pi,2}^{d_2}, p_{\pi,3}^{d_3}, \ldots, p_{\pi,n}^{d_n} \right) z^d \\
&= \frac{1}{\mid \Gamma \mid} \sum_{\pi \in \Gamma} \sum_{(d_1,d_2,\ldots,d_n) \in \mathbb{N}^n} p_{\pi,1}^{d_1}, p_{\pi,2}^{d_2}, p_{\pi,3}^{d_3}, \ldots, p_{\pi,n}^{d_n} z^{d_1+d_2+\ldots+d_n} \\
&= \frac{1}{\mid \Gamma \mid} \sum_{\pi \in \Gamma} \frac{1}{(1 - zp_{\pi 1}) \cdots (1 - zp_{\pi,n})} \\
&= \frac{1}{\mid \Gamma \mid} \sum_{\pi \in \Gamma} \frac{1}{det(id - z\pi)}.
\end{aligned}$$

□

Lema 2.2

Sean $p_1, p_2, \ldots, p_m$ elementos algebraicamente independientes de $\mathbb{C}$ los cuales son homogéneos de grado $d_1, d_2, \ldots, d_m$ respectivamente. Entonces la serie de Hilbert del subanillo graduado $R := \mathbb{C}[p_1, p_2, \ldots, p_m]$ es la siguiente:

$$H(R, z) := \sum_{n=0}^{\infty} (\dim_{\mathbb{C}} R_d) z^d = \frac{1}{(1 - z^{d_1})(1 - z^{d_2}) \cdots (1 - z^{d_m})}$$

Demostración. Dado que los p_i son algebraicamente independientes, el conjunto: $\left\{ p_1^{i_1} p_2^{i_2}, \ldots, p_m^{i_m} : i_1, i_2, \ldots, i_m \in \mathbf{N}, i_1 d_1 + i_2 d_2 + \ldots + i_m d_m = d \right\}$ es una base algebraica para R_d el conjunto de los polinomios de grado d en R. Por tanto la dimensión de R_d es igual a la cardinalidad del conjunto

$$A_d := \left\{ (i_1, i_2, \ldots, i_m) \in \mathbf{N}^m : i_1 d_1 + i_2 d_2 + \ldots + i_m d_m = d \right\}.$$

Desarrollando la expansión

$$\begin{aligned}\frac{1}{(1-z^{d_1})(1-z^{d_2})\cdots(1-z^{d_m})} &= \frac{1}{(1-z^{d_1})}\cdot\frac{1}{(1-z^{d_1})}\cdots\frac{1}{(1-z^{d_m})}\\ &= \left(\sum_{i_1=0}^{\infty} z^{i_1 d_1}\right)\left(\sum_{i_2=0}^{\infty} z^{i_2 d_2}\right)\cdots\left(\sum_{i_m=0}^{\infty} z^{i_m d_m}\right)\\ &= \sum_{d=0}^{\infty}\sum_{(i_1,i_2,\ldots,i_m)\in A_d} z^d\\ &= \sum_{d=0}^{\infty}|A_d|z^d = \sum_{d=0}^{\infty}(\dim_{\mathbb{C}} R_d)z^d\end{aligned}$$

lo que demuestra la afirmación del Lema. □

Ejemplo 2.1

El anillo invariante $\mathbb{C}[x_1,x_2]^{Z_4}$ *del grupo* $\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right\}$ *es generado por los invariantes* $I_1 := x_1^2+x_2^2$, $I_2 := x_1^2x_2^2$ *y* $I_3 = x_1x_2^3 - x_1^3x_2$.

Solución. El álgebra graduada $\mathbb{C}[I_1,I_2,I_3]$ está contenida en el subanillo invariante $\mathbb{C}[x_1,x_2]^{Z_4}$. Con el fin de establecer que estas dos álgebras son iguales, basta que, para cada $d\in\mathbf{N}$ sus componentes graduadas $\mathbb{C}[I_1,I_2,I_3]_d$ y $\mathbb{C}[x_1,x_2]_d^{Z_4}$ tengan las mismas dimensiones como $\mathbb{C}$-espacios vectoriales. En otras palabras basta mostrar que la serie de Hilbert del álgebra graduada $\mathbb{C}[I_1,I_2,I_3]$ es igual a la serie de Molien del anillo invariante $\mathbb{C}[x_1,x_2]^{Z_4}$.
La serie de Hilbert $\Phi_{Z_4}(z)$ de $\mathbb{C}[x_1,x_2]^{Z_4}$ puede ser calculada usando el teorema de Molien

$$\begin{aligned}\Phi_{Z_4}(z) &= \frac{1}{4}\left[\frac{1}{\begin{vmatrix}1-z&0\\0&1-z\end{vmatrix}}+\frac{1}{\begin{vmatrix}1+z&0\\0&1+z\end{vmatrix}}+\frac{1}{\begin{vmatrix}1&z\\-z&1\end{vmatrix}}+\frac{1}{\begin{vmatrix}1&-z\\z&1\end{vmatrix}}\right]\\ &= \frac{1+z^4}{(1-z^2)(1-z^4)}\\ &= 1+z^2+3z^4+3z^6+5z^8+5z^{10}+7z^{12}+7z^{14}+\mathcal{O}(z^{16})\end{aligned}$$

Para calcular la serie de Hilbert del álgebra graduada $\mathbb{C}[I_1,I_2,I_3]$ se usan

las bases de Groebner y se obtiene que la relación algebraica $I_3^2 - I_2 I_1^2 + 4I_2^2$ genera al ideal de sicigias de I_j. Esto implica que cada $p \in \mathbb{C}[I_1, I_2, I_3]$ puede ser escrito únicamente como $p(I_1, I_2, I_3) = q(I_1, I_2) + I_3 \cdot r(I_1, I_2)$ donde q y r son polinomios en dos variables. En otras palabras el álgebra graduada se puede escribir como suma directa de los $\mathbb{C}$-espacios vectoriales:

$$\mathbb{C}[I_1, I_2, I_3] = \mathbb{C}[I_1, I_2] \oplus I_3 \cdot \mathbb{C}[I_1, I_2].$$

La primera componente es un subanillo generado por dos polinomios invariantes homogéneos algebraicamente independientes. Usando el **Lema 2.2** encontramos que la serie de Hilbert para este anillo es $\dfrac{1}{(1-z^2)(1-z^4)}$. Entonces los elementos de grado d en $\mathbb{C}[I_1, I_2]$ están en correspondencia uno a uno con los $d+4$ elementos de $I_3 \cdot \mathbb{C}[I_1, I_2]$, la serie de Hilbert de la segunda componente es igual a $\dfrac{z^4}{(1-z^2)(1-z^4)}$. La suma de estas dos series es igual a la serie $\Phi_{Z_4}(z)$ ya que la descomposición en espacios vectoriales es una suma directa. □

2.2. Algoritmos para calcular Invariantes

En esta sección se presentan algunos algoritmos para calcular un conjunto fundamental de invariantes para cualquier grupo finito de matrices Γ.

Subrutina 2.1
Contención Radical
Entrada: $f_1, f_2, \ldots, f_m, g \in \mathbb{C}[\boldsymbol{x}]$.
Pregunta: Sea $I = \langle f_1, f_2, \ldots, f_m \rangle$ *entonces ¿*$g \in Rad(I)$*?*
Solución: Sea G *una base de Groebner para el ideal* $\langle f_1, f_2, \ldots, f_m, gz - 1 \rangle$ *donde* z *es una nueva variable. Entonces* $g \in Rad(I)$ *si y solo si* $1 \in G$.

Subrutina 2.2
Resolución de ecuaciones homogéneas
Entrada: polinomios homogéneos $f_1, f_2, \ldots, f_m \in \mathbb{C}[\boldsymbol{x}]$

Pregunta: ¿Existe un vector distinto de cero $a \in \mathbb{C}^n$ *tal que*

$$f_1(a) = f_2(a) = \ldots = f_m(a) = 0?$$

Solución: Calcular una base de Groebner G *del ideal* $I = \langle f_1, f_2, \ldots, f_m \rangle$. *Entonces el* $Rad(I) = \langle x_1, \ldots, x_n \rangle$ *si y sólo si, un monomio de la forma* $x_i^{j_i}$ *está en el ideal monomial de* G *para cada* $i \in \{1, 2, \ldots, n\}$.

Subrutina 2.3
Dependencia algebraica.
Entrada: Un conjunto $F := \{f_1, f_2, \ldots, f_m\} \in \mathbb{C}[\boldsymbol{x}]$, *considerado como un subconjunto del campo de funciones racionales* $\mathbb{C}(\boldsymbol{x})$.
Pregunta: ¿Es F *algebraicamente independiente sobre* $\mathbb{C}$? *Si es el caso, encontrar un polinomio de m-variables* P *tal que* $P(f_1, \ldots, f_m) = 0$ *en* $\mathbb{C}(\boldsymbol{x})$.
Solución: Se introducen m *variables auxiliares* $y := (y_1, \ldots, y_m)$, *y se calcula una base de Groebner* G *para* $\{f_1 - y_1, f_2 - y_2, \ldots, f_m - y_m\}$ *con respecto al orden lexicográfico inducido* $x_1 > \ldots > x_n > y_1 > \ldots > y_m$. *Sea* $G' := G \cap \mathbb{C}[y]$. *Entonces* F *es algebraicamente independiente si y sólo sí* $G' = \emptyset$. *Por otro lado si* $P(y) \in G'$, *entonces* $P(f_1, \ldots, f_m) = 0$ *en* $\mathbb{C}[\boldsymbol{x}]$.

Subrutina 2.4
Inclusión de un subanillo
Entrada:$f_1, f_2, \ldots, f_m, g \in \mathbb{C}[\boldsymbol{x}]$.
Pregunta: ¿ $g \in \mathbb{C}[f_1, f_2, \ldots, f_m]$ *de* $\mathbb{C}[\boldsymbol{x}]$*? Si lo es, encontrar un polinomio en* m *variables* Q *tal que* $g = Q(f_1, f_2, \ldots, f_m)$ *en* $\mathbb{C}[\boldsymbol{x}]$.
Solución: Calcular una base de Groebner G *como en la* **Subrutina 2.3** *y sea* $Q \in \mathbb{C}[\boldsymbol{x}, \boldsymbol{y}]$ *la única forma normal de* g *con respecto a* G. *Entonces* $g \in \mathbb{C}[f_1, f_2, \ldots, f_m]$ *si y solo si* Q *está en* $\mathbb{C}[\boldsymbol{y}]$.
En este caso $g = Q(f_1, f_2, \ldots, f_m)$ *en* $\mathbb{C}[\boldsymbol{x}]$.

Algoritmo 2.1
Completando invariantes fundamentales.
Supongamos que se tiene un conjunto de invariantes $\{I_1, \ldots, I_m\} \subset \mathbb{C}[\boldsymbol{y}]^\Gamma$. *Se desea saber si este conjunto es completo, es decir si el anillo invariante* $\mathbb{C}[\boldsymbol{x}]^\Gamma$ *es igual a la subálgebra* $R = \mathbb{C}[I_1, \ldots, I_m]$. *Este es el caso sí y sólo sí*

la serie de Hilbert $H(R,z)$ coincide con la serie de Molien $\Phi_\Gamma(z)$. Por otro lado, se puede restar $H(R,z)$ de la serie de Molien, y se tiene:

$$\Phi_\Gamma(z) - H(R,z) = c_d z^d + \mathcal{O}(z^{d+1})$$

Donde c_d es algún entero positivo. De esto concluimos que existen c_d invariantes linealmente independientes de grado "d", los cuales no pueden ser expresados como polinomios en $I_1, \ldots, I_m$. Ahora, podemos calcular estos invariantes extras (usando el operador de Reynold) y proceder agregándolos al conjunto inicial $\{I_1, \ldots, I_m\}$.

Por tanto el problema se reduce a calcular la serie de Hilbert del álgebra graduada $\mathbb{C}[I_1, I_2, \ldots, I_m] \subset \mathbb{C}[\boldsymbol{x}]^\Gamma$, la cual es presentada en términos de generadores homogéneos. Sea $d_j := grad(I_j)$. Usando la **Subrutina 2.3**, se puede calcular cualquier base de Groebner $G = \{g_1, \ldots, g_r\}$ para el núcleo I de la aplicación en los anillos de polinomios $\mathbb{C}[y_1, \ldots, y_m] \to \mathbb{C}[x_1, \ldots, x_n]$ definida por $y_i \to I_i$. Entonces R es isomorfo como $\mathbb{C}$-álgebra a $\dfrac{\mathbb{C}[y_1, \ldots, y_m]}{I}$, donde el grado de cada variable y_i es definida por d_j. Por el **Teorema 1.4**, se tiene que como $\mathbb{C}$-espacio vectorial graduado, se cumple:

$$R \cong \frac{\mathbb{C}[y_1, \ldots, y_m]}{\langle lt(g_1), \ldots, lt(g_r)\rangle}.$$

Por tanto el d-ésimo coeficiente $\dim_{\mathbb{C}}(R_d)$ de la serie de Hilbert deseada $H(R,z)$ es igual al número de monomios $y_1^{i_1} y_2^{i_2} \cdots y_m^{i_m}$, en donde $i_1 d_1 + i_2 d_2 + \ldots + i_m d_m = d$, los cuales no son múltiplos de cualquier

$$lt(g_1), \ldots, lt(g_r).$$

Ejemplo 2.2
Consideramos el anillo de polinomios $\mathbb{C}[x,y]$ sobre el cual actúa el grupo S_2 y encontremos generadores para el anillo $\mathbb{C}[x,y]^{S_2}$.

Solución. Utilicemos la representación bidimensional de S_2, (ver [5]):
$\Gamma = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ de donde $|\Gamma| = 2$.

Para esto encontraremos la serie de Molien

$$\Phi_{S_2}(z) = \frac{1}{2}\left[\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix} - z\begin{pmatrix}1&0\\0&1\end{pmatrix}\right|} + \frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix} - z\begin{pmatrix}0&1\\1&0\end{pmatrix}\right|}\right]$$

$$= \frac{1}{(1-z)(1-z^2)}$$
$$= 1 + z + 2z^2 + 2z^3 + 3z^4 + \mathcal{O}(z^5)$$

De acuerdo con la **Proposición 2.1** existen dos invariantes algebraicamente independientes. La serie de Molien sugiere buscar invariantes de grado uno. Para esto consideramos los monomios de grado uno con el orden $x < y$, utilizando el operador de Reynold para $f(x, y) = x$, obtenemos que

$$\begin{aligned} f^* &= \frac{1}{2}\sum_{\sigma\in\Gamma}\sigma(f) \\ &= \frac{1}{2}\left[f\left(\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\right) + f\left(\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\right)\right] \\ &= \frac{1}{2}\left[f(x,y) + f(y,x)\right] \\ &= \frac{1}{2}(x+y) \end{aligned}$$

De la misma forma, si tomamos el monomio $g(x, y) = y$, obtenemos que $g^* = \frac{1}{2}(y + x)$, de donde $f^* = g^*$.

Luego el polinomio homogéneo de grado 1, $p := 2(f)^* = 2(g)^* = x + y$ es invariante y algebraicamente independiente sobre $\mathbb{C}$, esto se comprueba con la **Subrutina 2.3**.
Por el **Lema 2.2**, la serie de Hilbert del anillo $R = \mathbb{C}[p]$ es

$$H(R, z) = \frac{1}{1-z} = 1 + z + z^2 + z^3 + z^4 + \mathcal{O}(z^5)$$

Como $\Phi_{S_2}(z) - H(R, z) = z^2 + z^3 + 2z^4 + \mathcal{O}(z^5) \neq 0$, deducimos que R es un subanillo propio de $\mathbb{C}[x, y]^{S_2}$ y según el **Algoritmo 2.1** es necesario encontrar un invariante de grado dos. Considerando ahora los monomios de grado

dos: $x^2 < xy < y^2$ y utilizamos el operador de Reynold para los polinomios $f(x,y) = x^2$, $g(x,y) = xy$ y $h(x,y) = y^2$. Calculando f^*:

$$\begin{aligned} f^* &= \frac{1}{2}\left[f\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) + f\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right)\right] \\ &= \frac{1}{2}\left[f(x,y) + f(y,x)\right] \\ &= \frac{1}{2}(x^2 + y^2) \end{aligned}$$

También $h^* = \frac{1}{2}(y^2+x^2)$, por lo que $f^* = h^*$. Para g se obtiene que $g^* = xy$ ya que $g^* = \frac{1}{2}[g(x,y)+g(y,x)] = \frac{1}{2}(xy+yx) = \frac{1}{2}(2xy) = xy$. De aquí obtenemos dos polinomios $q := 2(f^*) = 2(h^*) = x^2 + y^2$ y $r := g^* = xy$ que son también invariantes homogéneos junto con $p(x,y)$. Ahora utilizamos la **Subrutina 2.3** para saber si los polinomios que se han encontrado p, q, r son algebraicamente independientes o algebraicamente dependientes. En primer lugar se calcula una base de Groebner $\mathcal{G}$ para $\{p(x,y) - u, q(x,y) - v, r(x,y) - w\}$ con las nuevas variables auxiliares u, v, w y con el orden en las variables
$u < v < w < x < y$.
Para ello se utilizará el algoritmo de Buchberger [1, pág. 90, cap. 2] para $F = \{f_1, f_2, f_3\}$ en donde $f_1 = x + y - u$, $f_2 = x^2 + y^2 - v$ y $f_3 = xy - w$.
Inicializando:
$F := G$
$G' := G$

$$\begin{aligned} S(f_1, f_3) &= \frac{xy}{y} \cdot (x + y - u) - \frac{xy}{xy} \cdot (xy - w) \\ &= x^2 - ux + w \\ S(f_1, f_3) &\longrightarrow \overline{S(f_1, f_3)}^{G'} = x^2 - ux + w =: f_4 \end{aligned}$$

$G := \{f_1, f_2, f_3, f_4\}$

$G' := G$

$$\begin{aligned} S(f_1, f_2) &= \frac{y^2}{y} \cdot (x + y - u) - \frac{y^2}{y^2} \cdot (x^2 + y^2 - v) \\ &= xy - uy - x^2 + v \\ &= (x - u) \cdot f_1 - 2f_4 + 2w + v - u^2 \\ S(f_1, f_2) &\longrightarrow \overline{S(f_1, f_2)}^{G'} = 2w + v - u^2 =: f_5 \end{aligned}$$

$G := \{f_1, f_2, f_3, f_4, f_5\}$

$G' := G$

$$\begin{aligned} S(f_2, f_3) &= \frac{xy^2}{y^2} \cdot (x^2 + y^2 - v) - \frac{xy^2}{xy} \cdot (xy - w) \\ &= x^3 + wy - vx \\ &= w \cdot f_1 + (x + u) \cdot f_4 - x f_5 + 0 \\ S(f_2, f_3) &\longrightarrow \overline{S(f_2, f_3)}^{G'} = 0 =: f_6 \end{aligned}$$

$G = \{f_1, f_2, f_3, f_4, f_5\}$

$$\begin{aligned} S(f_1, f_4) &= \frac{x^2 y}{y} \cdot (x + y - u) - \frac{x^2 y}{x^2} \cdot (x^2 - ux + w) \\ &= x^3 - ux^2 + uxy - wy \\ &= (ux - w) \cdot f_1 + (x - u) \cdot f_4 + 0 \\ S(f_1, f_4) &\longrightarrow \overline{S(f_1, f_4)}^{G'} = 0 =: f_7 \end{aligned}$$

$G = \{f_1, f_2, f_3, f_4, f_5\}$

$$\begin{aligned} S(f_1, f_5) &= \frac{yw}{y} \cdot (x + y - u) - \frac{yw}{2w} \cdot (2w + v - u^2) \\ &= 2wx - 2wu - yw + yu^2 \\ &= (u^2 - v) \cdot f_1 + (x - u) \cdot f_5 + 0 \\ S(f_1, f_5) &\longrightarrow \overline{S(f_1, f_5)}^{G'} = 0 =: f_8 \end{aligned}$$

$G = \{f_1, f_2, f_3, f_4, f_5\}$

$$\begin{aligned} S(f_2, f_4) &\longrightarrow \overline{S(f_2, f_4)}^{G'} = 0 =: f_9 \\ S(f_2, f_5) &\longrightarrow \overline{S(f_2, f_5)}^{G'} = 0 =: f_{10} \\ S(f_3, f_4) &\longrightarrow \overline{S(f_3, f_4)}^{G'} = 0 =: f_{11} \\ S(f_3, f_5) &\longrightarrow \overline{S(f_3, f_5)}^{G'} = 0 =: f_{12} \\ S(f_4, f_5) &\longrightarrow \overline{S(f_4, f_5)}^{G'} = 0 =: f_{13} \end{aligned}$$

Por lo que una base de Groebner para el ideal generado por el conjunto $\{x + y - u, x^2 + y^2 - v, xy - w\}$ es

$$G = \{x + y - u, x^2 + y^2 - v, xy - w, x^2 - ux + w, 2w + v - u^2\}.$$

Ahora para encontrar una base reducida se observa que:
$x^2 - ux + w = f_2 - uf_1 + f_5 - (y^2 - uy + w)$, por lo que f_4 es reemplazado por $y^2 - uy + w$, además el término líder de f_2 es múltiplo del término líder de f_1 ya que $LT(f_2) = y \cdot LT(f_1)$, así se elimina a f_2, también se observa que $LT(f_3) = xy = x \cdot LT(f_1)$, entonces también se deja de considerar a f_3. De modo que una base de Groebner reducida es

$$\mathcal{G} = \{x + y - u, y^2 - uy + w, 2w + v - u^2\}$$

Ahora como $G' = \mathcal{G} \cap \mathbb{C}[u, v, w] = \{2w + v - u^2\} \neq \emptyset$, tenemos que p, q y r son algebraicamente dependientes según la **Subrutina 2.3**, y satisfacen una única relación polinomial de grado dos, por lo que eliminaremos a $x^2 + y^2$ ya que $x^2 + y^2 = (x+y)^2 - 2xy$. Así la serie de Hilbert para el anillo $R' = \mathbb{C}[p, r]$ es:

$$H(R', z) = \frac{1}{(1-z)(1-z^2)} = 1 + z + 2z^2 + 2z^3 + 3z^4 + \mathcal{O}(z^5)$$

Observemos que $\Phi_{S_2}(z) - H(R', z) = 0$, así $\{x+y, xy\}$ es un conjunto completo de invariantes.

$$\therefore \ \mathbb{C}[x, y]^{S_2} = \langle x + y, xy \rangle.$$

□

Ejemplo 2.3
Encontrar generadores para el anillo invariante $\mathbb{C}[\boldsymbol{x}]^{Q_8}$.

Solución. Una representación de Q_8 es $\{\pm I, \pm J, \pm U, \pm V\}$, en donde:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, V = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Comenzamos calculando la serie de Hilbert de $\mathbb{C}[x, y]^{Q_8}$ utilizando el teorema de Molien:

$$
\begin{aligned}
\Phi_{Q_8}(z) &= \frac{1}{8}\sum_{\pi\in Q_8}\frac{1}{\det(id-z\pi)} \\
&= \frac{1}{8}\left[\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix}-\begin{pmatrix}z&0\\0&z\end{pmatrix}\right|}+\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix}-\begin{pmatrix}zi&0\\0&-zi\end{pmatrix}\right|}\right. \\
&+\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix}-\begin{pmatrix}0&z\\-z&0\end{pmatrix}\right|}+\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix}-\begin{pmatrix}0&zi\\zi&0\end{pmatrix}\right|} \\
&+\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix}-\begin{pmatrix}-z&0\\0&-z\end{pmatrix}\right|}+\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix}-\begin{pmatrix}-zi&0\\0&zi\end{pmatrix}\right|} \\
&\left.+\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix}-\begin{pmatrix}0&-z\\z&0\end{pmatrix}\right|}+\frac{1}{\left|\begin{pmatrix}1&0\\0&1\end{pmatrix}-\begin{pmatrix}0&-zi\\-zi&0\end{pmatrix}\right|}\right] \\
&= \frac{1}{8}\left[\frac{1}{(1-z)^2}+\frac{6}{1+z^2}+\frac{1}{(1+z)^2}\right] \\
&= \frac{1-z^2+z^4}{(1-z^2)^2(1+z^2)} \\
&= 1+2z^4+z^6+3z^8+2z^{10}+\mathcal{O}(z^{12}). \qquad (2.2.1)
\end{aligned}
$$

La serie de Molien sugiere buscar 2 invariantes de grado 4. Consideremos el orden en las variables $x < y$ y el orden lexicográfico en los monomios. Los monomios de grado 4 son $x^4 < x^3y < x^2y^2 < xy^3 < y^4$. Utilizando el operador de Reynold para $f(x,y) = x^4$ obtenemos

$$
\begin{aligned}
(x^4)^* =& \frac{1}{8}[f(x,y)+f(xi,-yi)+f(-y,x)+f(yi,xi)+f(-x,-y) \\
&+f(-xi,yi)+f(y,-x)+f(-yi,-xi)] \\
=& \frac{1}{2}[x^4+y^4].
\end{aligned}
$$

Entonces $p := 2(x^4)^* = 2(y^4)^* = x^4+y^4$ es un polinomio homogéneo inva-

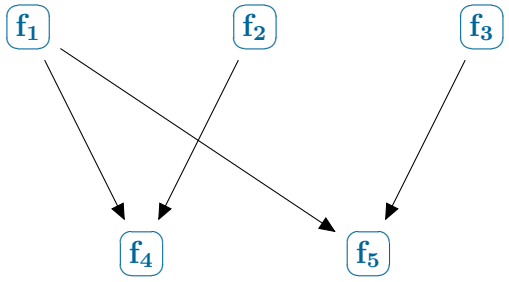
riante de grado 4.
Ahora aplicando el operador de Reynold a $f(x,y) = x^3y$:
$(x^3y)^* = \frac{1}{8}[x^3y - x^3y - x^3y + x^3y + x^3y + x^3y - x^3y - x^3y] = 0.$
Finalmente resta encontrar el polinomio que queda invariante de x^2y^2
$(x^2y^2)^* = \frac{1}{8}[x^2y^2 + x^2y^2 + x^2y^2 + x^2y^2 + x^2y^2 + x^2y^2 + x^2y^2 + x^2y^2] = x^2y^2.$
Así $q := (x^2y^2)^* = x^2y^2$ es invariante homogéneo de grado 4.
Utilizando el **Lema 2.2**, procedemos a calcular la serie de Hilbert del álgebra graduada $R := \mathbb{C}[x^4 + y^4, x^2y^2]$.

$$\begin{aligned} H(R,z) =& \frac{1}{(1-z^4)(1-z^4)} \\ =& \frac{1}{(1-z^4)^2} \\ =& 1 + 2z^4 + 3z^8 + 4z^{12} + \dots \end{aligned}$$

y al restar la serie de Molien con la serie de Hilbert observamos que

$$\Phi_{Q_8}(z) - H(R,z) = z^6 + \mathcal{O}(z^{12}).$$

Por lo tanto debemos encontrar un invariante de grado 6. Los monomios de grado 6 son $x^6 < x^5y < x^4y^2 < x^3y^3 < x^2y^4 < xy^5 < y^6$ siempre con el orden entre las variables $x < y$.
Utilizando el operador de Reynold tenemos:
$(x^6)^* = (x^4y^2)^* = (x^3y^3)^* = (y^4x^2)^* = (y^6)^* = 0$, $(x^5y)^* = \frac{1}{2}[x^5y - y^5x]$, $(y^5x)^* = -(x^5y)^*$.
Así obtenemos el invariante de grado 6, $r := 2(y^5x)^* = y^5x - x^5y$. Falta comprobar si el conjunto $\{x^4 + y^4, x^2y^2, y^5x - x^5y\}$ es un conjunto algebraicamente independiente. Sean u, v, w variables auxiliares y precederemos a utilizar la **Subrutina 2.3**. A continuación calcularemos una base de Groebner para el ideal generado por $G = \{x^4 + y^4 - u, x^2y^2 - v, y^5x - x^5y - w\}$.
Sean $\boxed{f_1} := x^4 + y^4 - u$, $\boxed{f_2} := x^2y^2 - v$, $\boxed{f_3} := y^5x - x^5y - w$.
Para calcular la base de Groebner utilizaremos el algoritmo de Buchberger [1, pág. 90, cap. 2]. Empezamos calculando los residuos de $S(f_1, f_2)$, $S(f_1, f_3)$, $S(f_2, f_3)$ y de esto obtenemos el siguiente diagrama:



$$\overline{S(f_1, f_2)}^G = y^2v + x^6 - x^2u := f_4$$

$$\overline{S(f_1, f_3)}^G = 2x^5y - yxu + w := f_5$$

$$\overline{S(f_2, f_3)}^G = 0$$

Figura 2.1: Primera iteración

Siguiendo con un proceso análogo, encontramos en la segunda iteración del algoritmo los siguientes residuos:

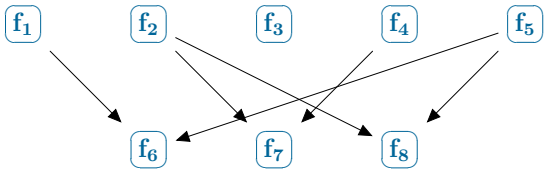


Figura 2.2: Segunda iteración

$$f_6 := -y^3w + 2x^9 - 3x^5u + xu^2.$$

$$f_7 := -x^8 + x^4u - v^2.$$

$$f_8 := y^2xu - yw - 2x^3v.$$

Luego, en la tercera iteración obtuvimos los siguientes residuos:

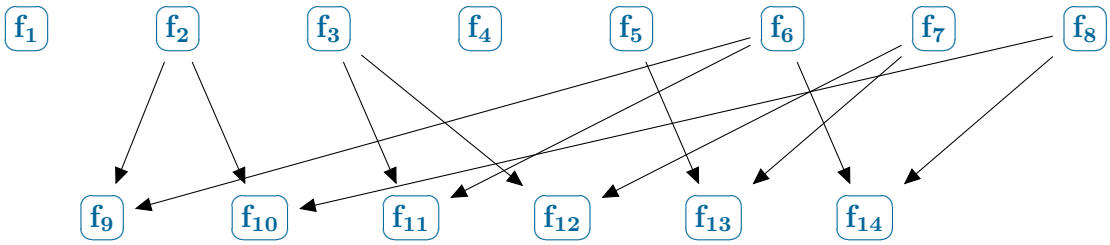


Figura 2.3: Tercera iteración

$f_9 := yvw + 3x^7u - 2x^{11} - x^3u^2.$
$f_{10} := yxw + 2x^4v - uv.$
$f_{11} := -uv + 4v^3 + w^2.$
$f_{12} := -2yx^4v^2 - x^3uw + x^7w + yuv^2.$
$f_{13} := -yx^4u - x^3w + 2yv^2.$
$f_{14} := -y^2w^2 - 2yx^3vw + 2x^{10}u - 3x^6u^2 + x^2u^3.$

En la última iteración obtuvimos los siguientes dos polinomios
$f_{15} := yxu^2 - uw + 2x^4w - 4yxv^2$.
$f_{16} := yw^3 + u^3x^7 - 4uv^2x^7 - 6vw^2x^3 + 16v^4x^3 - u^4x^3$
como residuos de los S-polinomios $S(f_5, f_{13})$ y $S(f_8, f_{14})$ respectivamente.
Por lo que una base de Groebner para el ideal generado por G es:

$\mathcal{G} := \{x^4 + y^4 - u, x^2y^2 - v, y^5x - x^5y - w, y^2v + x^6 - x^2u, 2x^5y - yxu + w,$
$-y^3w + 2x^9 - 3x^5u + xu^2, -x^8 + x^4u - v^2, y^2xu - yw - 2x^3v,$
$yvw + 3x^7u - 2x^{11} - x^3u^2, yxw + 2x^4v - uv, -uv + 4v^3 + w^2,$
$-2yx^4v^2 - x^3uw + x^7w + yuv^2, -yx^4u - x^3w + 2yv^2,$
$-y^2w^2 - 2yx^3vw + 2x^{10}u - 3x^6u^2 + x^2u^3, yxu^2 - uw + 2x^4w - 4yxv^2,$
$yw^3 + u^3x^7 - 4uv^2x^7 - 6vw^2x^3 + 16v^4x^3 - u^4x^3\}$

Ahora como $\mathcal{G}' = \mathcal{G} \cap \mathbb{C}[u, v, w] = \{-uv + 4v^3 + w^2\} \neq \emptyset$, se tiene que f_1, f_2 y f_3 son algebraicamente dependientes según la **Subrutina 2.3**, y satisfacen una única relación polinomial de grado tres: $-f_1f_2 + 4f_2^3 + f_3^2 = 0$. De esto obtenemos que la serie de Hilbert del anillo $R' = \mathbb{C}[f_1, f_2, f_3]$ es:

$$H(R', z) = \frac{1}{(1 - z^4)^2 \cdot (1 - z^6)} = 1 + 2z^4 + z^6 + 3z^8 + 2z^{10} + \mathcal{O}(z^{12}) \quad (2.2.2)$$

Observemos que al restar la ecuación (2.2.2) de (2.2.1), resulta:
$\Phi_{Q_8}(z) - H(R', z) = 0$, así $\{x^4 + y^4, x^2y^2, y^5x - yx^5\}$ es un conjunto completo de invariantes, por lo que

$$\mathbb{C}[\boldsymbol{x}]^{Q_8} = \langle x^4 + y^4, x^2y^2, y^5x - yx^5 \rangle.$$

□

Capítulo 3

Aplicaciones de la teoría de invariantes

3.1. Cálculo del grupo de Galois

Si $f \in K[\boldsymbol{x}]$ es un polinomio separable sobre un campo K, entonces el Grupo de Galois $Gal(N/K)$ del campo de escisión N de f sobre K actúa en los ceros $\alpha_1, \ldots, \alpha_n \in N$ de f, (ver [3]). Esto produce con seguridad una representación de permutación $Gal(N/K) \to S_n$, cuya imagen está denotada por $Gal(f)$, el Grupo de Galois de f. Es claro que $Gal(f)$ está determinado solamente por conjugación en S_n. En esta sección veremos métodos para el cálculo del grupo de Galois.

Supongamos que $Gal(f) \leq G$ para un subgrupo $G \leq S_n$ (esto siempre es cierto para $G = S_n$). Dado un subgrupo $H \leq G$ (usualmente un subgrupo maximal de G), nos gustaría comprobar que $Gal(f) \leq H$. La idea básica es el uso de un polinomio $F \in K[x_1, \ldots, x_n]^H$ tal que $\sigma \cdot F \neq F$ para todo $\sigma \in G - H$. Dicho polinomio es llamado un G-relativo H-invariante. En otras palabras, estamos buscando un polinomio $F \in K[x_1, \ldots, x_n]$ con $Stab_G(F) = H$, [2, pág. 210, cap. 5].

Proposición 3.1
Sea F un G-relativo H-invariante y

$$F(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \neq F(\alpha_1, \ldots, \alpha_n), \qquad \forall \sigma \in G - H$$

donde $\alpha_1, \ldots, \alpha_n$ son las raíces de f, y $Gal(f) \leq G$, entonces

$$Gal(f) \leq H \Leftrightarrow F(\alpha_1, \ldots, \alpha_n) \in K$$

Demostración. Sea $\gamma := F(\alpha_1, \ldots, \alpha_n)$, si $Gal(f) \leq H$, entonces para cada $\sigma \in Gal(f)$ tenemos que $\sigma \cdot F(\alpha_1, \ldots, \alpha_n) = F$ y por lo tanto $\sigma\gamma = \gamma$ para cada $\sigma \in Gal(N/K)$ ya que la acción de Galois en las α_i es igual que la acción por permutación en las variables x_i. Así $\gamma \in N^{Gal(N/K)} = K$. Por otro lado, si $Gal(f) \nleq H$, entonces existe $\sigma \in Gal(N/K)$ cuya acción en las α_i está en $G - H$, pero por hipótesis tenemos que $\sigma\gamma \neq \gamma$ y así $\gamma \notin K$. □

Lema 3.1
Suponga que K es un campo infinito. Entonces en la situación de la proposición anterior, existen $c_0, c_1, \ldots, c_{n-1} \in K$ tal que para cada $\beta_i := \sum_{j=0}^{n-1} c_j \alpha_i^j$, tenemos

$$F(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)}) \neq F(\beta_1, \ldots, \beta_n), \qquad \forall \sigma \in G - H$$

y $\beta_i \neq \beta_j$ para $i \neq j$. Es decir si $S \subset K$ es cualquier subconjunto tal que $|S| > deg(F) \cdot \binom{[G:H]}{2} + \binom{n}{2}$, los c_i pueden ser escogidos de S.

Demostración. Sean $C_0, C_1, \ldots, C_{n-1}$ indeterminadas en N. Entonces $B_i := \sum_{j=0}^{n-1} C_j \alpha_i^j$ son algebraicamente independientes sobre N ya que son el determinante de Vandermonde el cual es distinto de cero. Sea

$$D(C_0, C_1, \ldots, C_{n-1}) =$$

$$\prod_{1 \leq i < j \leq n} (B_i - B_j) \prod_{1 \leq i < j \leq m} \Big(F(B_{\sigma_i(1)}, B_{\sigma_i(2)}, \ldots, B_{\sigma_i(m)}) - F(B_{\sigma_j(1)}, B_{\sigma_j(2)}, \ldots, B_{\sigma_j(m)}) \Big)$$

donde $\sigma_1, \sigma_2, \ldots, \sigma_m$ es el conjunto de las clases laterales izquierdas de H en G. Ya que $\sigma \cdot F \neq \tau F$ para $\sigma \cdot H \neq \tau H$, se deduce que $D(C_0, C_1, \ldots, C_{n-1}) \neq 0$. Ya que $|S| > deg(D)$, existe $c_0 \in S$ tal que $D(c_0, C_1, \ldots, C_{n-1}) \neq 0$. Continuando de esta forma podemos encontrar $c_0, c_1, \ldots, c_{n-1} \in K$ cumpliendo $D(c_0, c_1, \ldots, c_{n-1}) \neq 0$. Pero esto significa que
$F(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)}) \neq F(\beta_1, \ldots, \beta_n), \quad \forall \sigma \in G - H$ y $\beta_i \neq \beta_j$ para $i \neq j$. □

Algoritmo 1 Cálculo de un polinomio G-relativo H-invariante.

Input: Un grupo de permutaciones $G \leq S_n$ para $n \geq 4$ y un subgrupo H maximal en G.

Out: Un polinomio $F(x_1, x_2, \ldots, x_n)$ mínimo de grado $d \leq \dfrac{n(n-1)}{2}$ con $Stab(F) = H$.

1: Encuentre la serie de Hilbert $H(R^H, z)$ y $H(R^G, z)$, luego encuentre el índice más pequeño d tal que los correspondientes coeficientes de las series son distintos.
2: Encontrar todos los invariantes homogéneos de H con grado total d.
3: Regresar un invariante con el menor número posible de monomios.

Algoritmo 3.1

Algoritmo de Stauduhar.
Sea $Gal(f) \leq G$, con respecto al orden escogido en las raíces del polinomio f (Inicialmente $G = S_n$). Primero encontrar los subgrupos de S_n y para cada par $H \leq G$ de subgrupos con H maximal en G, encontrar un G- relativo H-invariante. Iniciar con $G = S_n$ y usar la **Proposición 3.1** *hasta encontrar un $G \leq S_n$ tal que $Gal(f) \leq G$ pero $Gal(f) \nleq H$ para cada subgrupo maximal $H \leq G$. Entonces $Gal(f) = G$.*

Ejemplo 3.1

Calculo del grupo de Galois del polinomio $f(x) = 1-10x^2+x^4$ con $f(x) \in \mathbb{Q}[x]$ cuyas raíces son:
$\left\{-\sqrt{5-2\sqrt{6}}, \sqrt{5-2\sqrt{6}}, -\sqrt{5+2\sqrt{6}}, \sqrt{5+2\sqrt{6}}\right\}$ *por lo que todas son reales.*

Demostración. Es primer lugar es importante destacar que $f(x) = 1-10x^2+ x^4$ es irreducible sobre $\mathbb{Q}$, ya que para utilizar los algoritmos previos, se necesita la irreducibilidad.

Nombraremos las raíces del polinomio, haciendo un cambio de variable mediante lo siguiente:

$$\alpha := 5 - 2\sqrt{6}$$
$$\beta := 5 + 2\sqrt{6}$$

Primero observemos que: $(\sqrt{2} \pm \sqrt{3})^2 = 5 \pm 2\sqrt{6}$, es decir:

$$\pm\sqrt{5 \pm 2\sqrt{6}} = (\sqrt{2} \pm \sqrt{3}) \Rightarrow \sqrt{5 \pm 2\sqrt{6}} \in \mathbb{Q}(\sqrt{2} \pm \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

Así que el cuerpo de escisión de f es $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Sabemos que $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ tiene una representación respectiva en el grupo de permutaciones, mediante la siguiente aplicación:

$$\phi : Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \longrightarrow S_n$$

Donde $Im(\phi) = Gal(f)$, el grupo de Galois de f. Haciendo uso del algoritmo de Stauduhar (**Algoritmo 3.1**), logramos comprobar que para $G = S_4$ y sus subgrupos maximales A_4, D_8, S_3 no se logra establecer el grupo de Galois.
Supongamos a $G = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \leq S_4$.
Cuyos subgrupos maximales los podemos observar en la Figura 3.1:

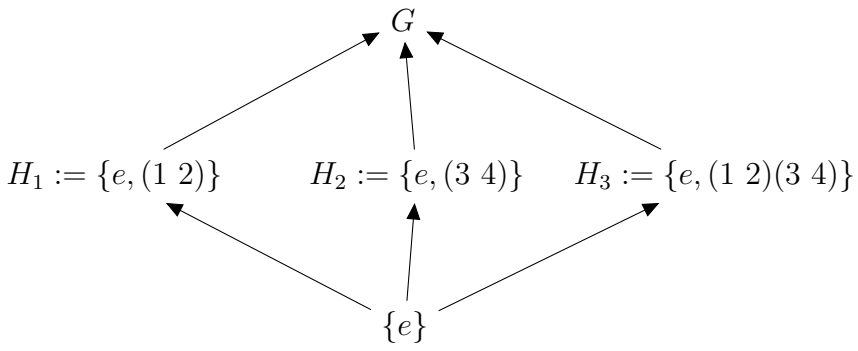


Figura 3.1: Estructura del grupo de Klein de orden 2

Sin pérdida de generalidad podemos suponer que $Gal(f) \leq G$, y tomaremos a $H_1 \leq G$. A continuación calcularemos un polinomio $F \in \mathbb{Q}[x_1, x_,x_3, x_4]^{H_1}$ tal que $\sigma F \neq F\ \forall \sigma \in G - H_1$. Para calcular dicho polinomio, haremos uso del **Algoritmo 1**.

En primer lugar calcularemos las series de Hilbert $H(R^{H_1}, z)$ y $H(R^G, z)$, donde $R = \mathbb{Q}[x_1, x_2, x_3, x_4]$.
La representación matricial de G es:

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

Llegamos a:

$$H(R^G, z) = 1 + 2z + 5z^2 + 8z^3 + 14z^4 + \mathcal{O}(z^5) \tag{3.1.1}$$
$$H(R^{H_1}, z) = 1 + 3z + 7z^2 + 13z^3 + 22z^4\mathcal{O}(z^5) \tag{3.1.2}$$

El algoritmo nos sugiere tomar el grado más pequeño tal que los coeficientes son distintos; al observar las dos series, tenemos que el grado más pequeño cumpliendo dichas restricciones es $d = 1$.
Ahora, calcularemos todos los invariantes homogéneos bajo la acción de H_1 de grado 1. Los monomios de grado 1 son: x_1, x_2, x_3, x_4.
Utilizando el operador de Reynold, tenemos: $x_1^* = \frac{1}{2}(x_1 + x_2)$, $x_2^* = \frac{1}{2}(x_2 + x_1)$
Donde:
$\left.\begin{array}{l} x_3^* = \frac{1}{2}(x_3 + x_3) = x_3 \\ x_4^* = \frac{1}{2}(x_4 + x_4) = x_4 \end{array}\right\}$ Son G-relativos H_1-invariantes

Luego se deben remover aquellos polinomios que no son G-relativos, esto es para todos aquellos que no cumplan que: $\forall \sigma \in (G - H_1)$, $\sigma \circ g \neq g$ con g un H_1 invariante.
Para $x_1^* = x_2^*$, con $\sigma_1 = (3\ 4)$, se tiene $\sigma_1 \circ x_1^* = x_1^*$. Con $\sigma_2 = (1\ 2)(3\ 4)$, se tiene $\sigma_2 \circ x_2^* = x_2^*$, y son los únicos $\sigma \in (G - H)$, luego $x_1^* = x_2^*$ no son G-relativos.
Para $x_3^* = x_3$, con $\sigma_1 = (3\ 4)$, tenemos $\sigma_1 \circ x_3^* = \sigma_1 \circ x_4 \neq x_3$.
Con $\sigma_2 = (1\ 2)(3\ 4)$, tenemos $\sigma_2 \circ x_3 = x_4 \neq x_3$, lo mismo sucede con x_4^*, por lo tanto $I = x_3$ y $J = x_4$ son G-relativos. Elegiremos a I, el cual consideraremos nuestro polinomio G-relativo H_1-invariante, entonces $F(x_1, x_2, x_3, x_4) = x_3$.
Verificando las hipótesis de la **Proposición 3.1**:
$G - H_1 = \{(3\ 4), (1\ 2)(3\ 4)\}$ y observemos que $F(-\sqrt{\alpha}, \sqrt{\alpha}, -\sqrt{\beta}, \sqrt{\beta}) = -\sqrt{\beta}$.

$(3\ 4) \circ F(-\sqrt{\alpha}, \sqrt{\alpha}, -\sqrt{\beta}, \sqrt{\beta}) = \sqrt{\beta}$.
$(1\ 2)(3\ 4) \circ F(-\sqrt{\alpha}, \sqrt{\alpha}, -\sqrt{\beta}, \sqrt{\beta}) = \sqrt{\beta}$.
Así $\forall \sigma \in G - H_1$, se cumple:

$$\sigma \circ F(-\sqrt{\alpha}, \sqrt{\alpha}, -\sqrt{\beta}, \sqrt{\beta}) \neq F(-\sqrt{\alpha}, \sqrt{\alpha}, -\sqrt{\beta}, \sqrt{\beta}).$$

Luego observemos que $\sqrt{\beta} = \sqrt{5 + 2\sqrt{6}} \notin \mathbb{Q}$.
Entonces debe suceder: $Gal(f) \nleq H_1$
Por otro lado si tomamos al subgrupo maximal $H_2 \leq G$, su serie de Hilbert coincide con la serie de Hilbert de H_1 (3.1.2), y tenemos:

$$H(R^{H_2}, z) = 1 + 3z + 7z^2 + 13z^3 + 22z^4\mathcal{O}(z^5)$$

al compararla con (3.1.1), resulta $d = 1$, luego calcularemos todos los invariantes homogéneos bajo la acción de H_2 de grado 1, con el uso del operador de Reynold, tenemos: $x_3^* = \dfrac{1}{2}(x_3 + x_4)$, $x_4^* = \dfrac{1}{2}(x_4 + x_3)$

Donde: $\left.\begin{array}{l} x_1^* = x_1 \\ x_2^* = x_2 \end{array}\right\}$ Son G-relativos H_2-invariantes.
Tomaremos $I = x_1 = F_2(x_1, x_2, x_3, x_4)$, se considerará nuestro polinomio G-relativo H_2-invariante. Se satisfacen las hipótesis de la **Proposición 3.1**.
Luego como $F_2(-\sqrt{\alpha}, \sqrt{\alpha}, -\sqrt{\beta}, \sqrt{\beta}) = -\sqrt{\alpha} \notin \mathbb{Q}$. Llegamos a que $Gal(f) \nleq H_2$.

Para H_3 la serie de Hilbert es

$$H(R^{H_3}, z) = 1 + 2z + 6z^2 + 10z^3 + 19z^4\mathcal{O}(z^5)$$

y comparándola con (3.1.1), es necesario buscar invariantes de grado dos, los cuales se muestran a continuación

$$\left\{\frac{1}{2}(x_1^2 + x_2^2), \frac{1}{2}(x_3^2 + x_4^2), x_1x_2, \frac{1}{2}(x_1x_3 + x_2x_4), \frac{1}{2}(x_1x_4 + x_2x_3), x_3x_4\right\}$$

eligiendo convenientemente a $F_3(x_1, x_2, x_3, x_4) := x_1x_2 + x_1x_3 + x_2x_4$, el cual es G-relativo H_3-invariante y $F_3(-\sqrt{\alpha}, \sqrt{\alpha}, -\sqrt{\beta}, \sqrt{\beta}) = -\alpha + 2 \notin \mathbb{Q}$. Por lo que $Gal(f) \nleq H_3$, así por el **Algoritmo 3.1** debe suceder que

$$Gal(f) = G = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

además G es conocido como el grupo de Klein de orden 2.

□

3.2. Teoría de invariantes en Geometría Proyectiva

Sea $X := (x_{ij})$ una matriz de orden $n \times d$ cuyas entradas son indeterminadas, y sea $\mathbb{C}[x_{ij}]$ el anillo de polinomios en dn variables. A lo largo de este capítulo tendremos en cuenta a X como una configuración de n vectores en el espacio vectorial $\mathbb{C}^n$. Estos vectores representan una configuración de n puntos en el espacio proyectivo $\mathbb{P}^{d-1}$ de dimensión $d-1$.
El objetivo es estudiar las funciones polinomiales en $\mathbb{C}[x_{ij}]$ que corresponden a las propiedades geométricas de la configuración proyectiva de los puntos X.
Consideremos el conjunto $\Lambda(n,d) := \{[\lambda_1\lambda_2\ldots\lambda_d] \mid 1 \leq \lambda_1 < \lambda_2 < \ldots < \lambda_d \leq n\}$ de las d-uplas ordenadas en $[n] := \{1, 2, \ldots, n\}$. Los elementos $\Lambda(n,d)$ les llamaremos soportes y nos servirán como indeterminadas sobre $\mathbb{C}$.
Se define a $\mathbb{C}[\Lambda(n,d)]$ como el anillo de polinomios generado por los $\binom{n}{d}$ elementos del conjunto $\Lambda(n,d)$. Además, se abrevia a $[\lambda] := [\lambda_1\lambda_2\ldots\lambda_d]$ y $[\lambda_{\pi_1}\lambda_{\pi_2}\ldots\lambda_{\pi_d}] := sing(\pi)\cdot[\lambda]$, para toda permutación π del conjunto $\{1, 2, \ldots, d\}$.
Consideremos el homomorfismo de álgebras

$$\Phi_{n,d} : \mathbb{C}[\Lambda(n,d)] \longrightarrow \mathbb{C}[x_{ij}]$$

$$[\lambda] \longmapsto \Phi_{n,d}([\lambda]) = \det \begin{pmatrix} x_{\lambda_1 1} & x_{\lambda_1 2} & \cdots & x_{\lambda_1 d} \\ x_{\lambda_2 1} & x_{\lambda_2 2} & \cdots & x_{\lambda_2 d} \\ \vdots & \vdots & \vdots & \vdots \\ x_{\lambda_d 1} & x_{\lambda_d 2} & \cdots & x_{\lambda_d d} \end{pmatrix}.$$

el cual aplica el soporte $[\lambda]$ en el subdeterminante de X de dimensión $d \times d$ cuyas filas están indexadas por λ. A la aplicación $\Phi_{n,d}$ le llamaremos *coordinatización genérica.*

Ejemplo 3.2
Para $d = 3$ y $n = 6$ las filas de la matriz X son

$$X = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ \vdots & \vdots & \vdots \\ x_{61} & x_{62} & x_{63} \end{pmatrix}$$

X puede ser pensado como seis puntos en $\mathbb{CP}^2$. Ahora, el determinante $\Phi_{6,3}([146]) = x_{11}x_{42}x_{63} - x_{11}x_{62}x_{43} - x_{41}x_{12}x_{63} + x_{41}x_{62}x_{13} + x_{61}x_{12}x_{43} - x_{61}x_{42}x_{13}$ se anula si y sólo si los puntos "1", "4" y "6" están alineados.

La imagen de $\Phi_{n,d}$ coincide con el subanillo $\mathcal{B}_{n,d}$ de $\mathbb{C}[x_{ij}]$ generado por los menores de $d \times d$ de X. Al anillo $\mathcal{B}_{n,d}$ se le llama el anillo soporte.
La aplicación $\Phi_{n,d}$ en general no es inyectiva. Denotaremos por $I_{n,d} \subset \mathbb{C}[\Lambda(n,d)]$ el núcleo de $\Phi_{n,d}$. Este es el ideal de las dependencias algebraicas o sicigias entre los menores de las matrices genéricas de dimensión $n \times d$.

Observación 1
En virtud del primer del primer teorema de isomorfía tenemos que $\mathcal{B}_{n,d}$ es isomorfo al anillo cociente $\mathbb{C}[\Lambda(n,d)]/I_{n,d}$.

Daremos ahora una base de Groebner explícita para el ideal $I_{n,d}$. La variedad proyectiva definida por la sicigia del ideal $I_{n,d}$ es la variedad *Grassmaniana* de dimensión $(n-d)d$ cuyos puntos corresponden a los subespacios vectoriales de dimensión d de $\mathbb{C}^n$. En lo que sigue necesitaremos de las siguientes notaciones. El *complemento* de una upla $\lambda \in \Lambda(n,d)$ es la única $(n-d)$-upla $\lambda^* \in \Lambda(n, n-d)$, con $\lambda \cup \lambda^* = \{1, 2, \ldots, n\}$. El *signo* del par (λ, λ^*) se define como el signo de la permutación π, la cual mapea λ_i en i, para $i = 1, 2, \ldots, d$ y λ^*_j a $j+d$, para $j = 1, 2, \ldots, n-d$.
Sea $s \in \{1, 2, \ldots, d\}$ y $\alpha \in \Lambda(n, s-1)$, $\beta \in \Lambda(n, d+1)$ y $\gamma \in \Lambda(n, d-s)$.
Se define la sicigia de *van der Waerden* $[[\alpha\dot{\beta}\gamma]]$ para ser el siguiente polinomio cuadrático en $\mathbb{C}[\Lambda(n,d)]$.

$$[[\alpha\dot{\beta}\gamma]] := \sum_{\tau \in \Lambda(d+1,s)} sig(\tau, \tau^*) \cdot [\alpha_1, \ldots, \alpha_{s-1}\beta_{\tau^*_1}, \ldots, \beta_{\tau^*_{d+1-s}}] \cdot [\beta_{\tau_1}, \ldots, \beta_{\tau_s}\gamma_1, \ldots, \gamma_{d-s}]$$

Lema 3.2
El polinomio $[[\alpha\dot{\beta}\gamma]]$ pertenece al ideal $I_{n,d}$.

Demostración. Necesitamos mostrar que $\Phi_{n,d}([[\alpha\dot{\beta}\gamma]]) \in \mathbb{C}[x_{ij}]$ es cero para cada matriz X de dimensión $n \times d$.

Consideremos los vectores filas $x_{\alpha_1}, \ldots, x_{\alpha_{s-1}}, x_{\beta_1}, \ldots, x_{\beta_{d+1}}, x_{\gamma_1}, \ldots, x_{\gamma_{d-s}}$ de X los cuales son indexados por las uplas α, β, γ respectivamente. Los $d-1$ vectores fila x_{α_i} y x_{γ_i} son elementos arbitrarios de $\mathbb{C}^d$, mientras que los $d+1$ vectores x_{β_k} se dejan como indeterminadas por lo que la expresión $\Phi_{n,d}([[\alpha\dot{\beta}\gamma]])$ define una familia multilineal en $\mathbb{C}^d$. Además observemos que esta forma multilineal es antisimétrica porque la suma definida en el polinomio de Van der Waerden es alternante por definición. Un teorema bien conocido del álgebra lineal establece la existencia de una $d+1$-forma multilineal no antisimétrica en el espacio vectorial de dimensión d, excepto la forma cero. Ya que la especialización anterior fue arbitraria entonces podemos concluir que $\Phi_{n,d}([[\alpha\dot{\beta}\gamma]]) = 0$ en $\mathbb{C}[x_{ij}]$. □

En lo que sigue demostraremos dos teoremas importantes. Primero consideremos el orden lexicográfico en los elementos de $\Lambda(n,d)$, en donde $|\lambda| \prec |\mu|$ si existe m con $1 \leq m \leq d$, tal que $\lambda_j = \mu_j$, para $1 \leq j \leq m-1$, $\lambda_m < \mu_m$. Esto nos da un orden total en el conjunto de variables en el anillo $\mathbb{C}[\Lambda(n,d)]$. El orden monomial "$\prec$" es llamado el *orden tabular*. Escribiremos los monomios $\mathbb{C}[\Lambda(n,d)]$ como matrices rectangulares o tablas.
Dado $[\lambda^1], \ldots, [\lambda^k] \in \Lambda(n,d)$, con el orden $[\lambda^1] \preceq, \ldots, \preceq [\lambda^k]$, entonces el monomio $T := [\lambda^1] \cdots [\lambda^k]$ queda escrito como la siguiente tabla:

$$T = \begin{bmatrix} \lambda_1^1 & \cdots & \lambda_d^1 \\ \lambda_1^2 & \cdots & \lambda_d^2 \\ \vdots & \ddots & \vdots \\ \lambda_1^k & \cdots & \lambda_d^k \end{bmatrix}$$

Definición 3.1
Una tabla T se dice estándar si sus columnas están ordenadas, es decir: $\lambda_s^1 \leq \lambda_s^2 \leq, \ldots, \leq \lambda_s^k$, $\forall s = 1, 2, \ldots, d$, de los contrario se dirá que T es no estándar.

La sicigia de Van der Waerden $[[\alpha\dot{\beta}\gamma]]$ es llamada sicigia de enderezamiento, si cumple que $\alpha_{s-1} < \beta_{s+1}$ y $\beta_s \leq \gamma_1$.

Teorema 3.1
El conjunto $S_{n,d}$ de las sicigias de enderezamiento forman una base de Groebner para $I_{n,d}$, con respecto al orden tabular. Una tabla T es estándar si y sólo sí T no esta en el ideal inicial $init_{\prec}(I_{n,d})$.

Demostración. Por el **Lema 3.2** tenemos que $S_{n,d} \subset I_{n,d}$. Sea $\mathcal{M} \subseteq init_{\prec}(I_{n,d})$ el conjunto que denota el ideal inicial generado por la tabla inicial de elementos en $S_{n,d}$. Nos hace falta probar que $init_{\prec}(I_{n,d}) \subseteq \mathcal{M}$.
Sea $T = [\lambda^1] \cdots [\lambda^k]$, cualquier tabla no estándar, es decir, existe $i \in \{2, \ldots, k\}$ y $s \in \{2, \ldots, d\}$, tal que $\lambda^i_s > \lambda^{i-1}_s$. El factor $[\lambda^i_s][\lambda^{i-1}_s]$ es la tabla inicial de la sicigia de enderezamiento $[[\alpha\dot{\beta}\gamma]]$, donde $\alpha := [\lambda^{i-1}_1 \lambda^{i-1}_2 \ldots \lambda^{i-1}_{s-1}]$ y $\beta := [\lambda^i_1 \lambda^i_2 \ldots \lambda^i_s \lambda^{i-1}_s \ldots \lambda^{i-1}_d]$, $\gamma := [\lambda^i_{s+1} \lambda^i_{s+2} \ldots \lambda^i_d]$. Por lo tanto $T \in \mathcal{M}$.
Consideremos el anillo de polinomios $\mathbb{C}[x_{ij}]$, y el orden monomial lexicográfico "$<$" inducido de las variables $x_{11} > x_{12} > \ldots > x_{1d} > x_{21} > \ldots > x_{n1} > \ldots > x_{nd}$. Al orden "$<$" le llamaremos "*orden monomial diagonal*" en $\mathbb{C}[x_{ij}]$.

Sea $T = [\lambda^1] \cdots [\lambda^k] \in \Lambda(n, d)$, cualquier tabla, consideramos su imagen $\Phi_{n,d}(T) \in \mathbb{C}[x_{ij}]$ bajo la coordinatización genérica. El monomio inicial de este producto de los k menores en el orden monomial diagonal es igual a

$$lt(\Phi_{n,d}(T)) = \prod_{i=1}^{k} x_{\lambda^i_1 1} x_{\lambda^i_2 2} \cdots x_{\lambda^i_d d}.$$

□

Lema 3.3
Sean $\{\lambda^1, \ldots, \lambda^k\}$ cualquier conjunto de $\Lambda(n, d)$. Entonces existe una tabla estándar única T' tal que

$$lt(\Phi_{n,d}(T')) = \prod_{i=1}^{k} x_{\lambda^i_1 1} x_{\lambda^i_2 2} \cdots x_{\lambda^i_d d}.$$

Demostración. La tabla T' se obtiene de la tabla $T = [\lambda^1] \cdots [\lambda^k]$ por cada columna ordenada.
Ahora supongamos que la tabla estándar T esta en el ideal inicial $init_{\prec}(I_{n,d})$

es decir $T = lt(F)$ donde $F \in I_{n,d}$. Sin pérdida de generalidad asumamos que todas las tablas que están en F son estándar. Cualquier tabla no estándar puede ser reemplazada por su forma normal (la cual no necesariamente es única) con respecto a $S_{n,d}$. Cualquier forma normal es una combinación lineal de tablas estándar por la primera parte de esta prueba.
Ya que F no es cero pero $\Phi_{n,d}(F) = 0$, existe una tabla estándar no trivial T' en la expansión de F tal que $\Phi_{n,d}(T)$ y $\Phi_{n,d}(T')$ tienen el mismo monomio inicial en el orden monomial diagonal en $\mathbb{C}[x_{ij}]$. Pero esto es una contradicción según las hipótesis del lema por lo que se completa la prueba. □

Corolario 3.1
(Ley de enderezamiento). La tabla estándar de un $\mathbb{C}$-espacio vectorial es una base para el anillo de soporte $\mathcal{B}_{n,d}$.

El grupo $SL(\mathbb{C}^d)$ de las matrices de $d \times d$ cuyo determinante es 1, actúa por multiplicación derecha en el anillo $\mathbb{C}[x_{ij}]$ de las funciones polinomiales de la matriz genérica $X = (x_{ij})$. Es claro que cada $d \times d$ menor de la matriz X es invariante bajo la acción de $SL(\mathbb{C}^d)$, por lo que $\mathbb{C}[x_{ij}]^{SL(\mathbb{C}^d)}$ contiene el anillo de soporte $\mathcal{B}_{n,d}$ el cual es generado por todos los $d \times d$ menores.
Para probar un resultado muy importante de la teoría de invariantes se necesitara del "multigrado" en el anillo de polinomios $\mathbb{C}[x_{ij}]$. Sea $m \in \mathbb{C}[x_{ij}]$ cualquier monomio. Para cada índice de las columnas $j \in \{1, 2, \ldots, d\}$, se define $deg_j(m)$ como el grado total de m en el subconjunto de variables $\{x_{ij} : 1 \leq i \leq n\}$. El vector $deg(m) := (deg_1(m), deg_2(m), \ldots, deg_d(m))$ es llamado el multigrado de m. Note que si un polinomio $f \in \mathbb{C}[x_{ij}]$ es multihomogéneo de multigrado $(\delta_1, \delta_2, \ldots, \delta_d)$, entonces f es homogéneo de grado total $\delta_1 + \delta_2 + \ldots + \delta_d$.
Un polinomio Q se dice *invariante relativo* del grupo general lineal $GL(\mathbb{C}^d)$ si existe un entero $0 \leq p$ tal que $Q \circ A = \det(A)^p \cdot Q$, $\forall A \in GL(\mathbb{C}^d)$. El entero p es llamado el índice de Q.

Lema 3.4
Sea $Q \in \mathbb{C}[x_{ij}]$ un invariante homogéneo de $SL(\mathbb{C}^d)$. Entonces existe un entero $0 \leq p$ tal que

I) *Q tiene multigrado $(p, p, \ldots, p)$ y*

II) *Q es un invariante relativo de $GL(\mathbb{C}^d)$ de índice p.*

Demostración. Fijemos los índices de dos filas $j_1, j_2 \in \{1, \ldots, d\}$. Sea $D(j_1, j_2)$ la matriz de dimensión $d \times d$, cuya j_1-ésima entrada diagonal es 2 y j_2-ésima entrada diagonal igual a $\frac{1}{2}$ y todas sus otras entradas diagonales son iguales a 1. Note que $D(j_1, j_2) \in SL(\mathbb{C}^d)$. Esta matriz transforma un monomio m en $m \circ D(j_1, j_2) = m \cdot 2^{deg_{j_1}(m) - deg_{j_2}(m)}$.
Pero como Q es invariante entonces $Q = Q \circ D(j_1, j_2)$. Esto implica que cada monomio de m el cual esta en la expansión de I satisface que $deg_{j_1}(m) = deg_{j_2}(m)$ y ya que los índices j_1, j_2 fueron escogidos arbitrarios entonces se cumple la condición I).
Ahora sea A una matriz arbitraria de $GL(\mathbb{C}^d)$, definimos la matriz diagonal $D_A := diag(\det(A), 1, 1, \ldots, 1)$, y se observa que $A \cdot D_A^{-1} \in SL(\mathbb{C}^d)$. Ahora la primera parte implica
$Q \circ A = Q \circ (A\ D_A^{-1} \cdot D_A) = (Q \circ A \cdot D_A^{-1}) \cdot D_A = Q \circ D_A = \det(A)^p \cdot Q$, lo que completa la prueba. □

Extendemos la matriz de dimensión $n \times d$, X a la matriz genérica de dimensión $(n + 2d) \times d$ como sigue

$$\begin{pmatrix} A \\ X \\ B \end{pmatrix} := \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & \ddots & \vdots \\ a_{d1} & \cdots & a_{dd} \\ x_{11} & \cdots & x_{1d} \\ x_{21} & \cdots & x_{2d} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nd} \\ b_{11} & \cdots & b_{1d} \\ \vdots & \ddots & \vdots \\ b_{d1} & \cdots & b_{dd} \end{pmatrix}$$

El anillo de polinomios $\mathbb{C}[a_{ij}, x_{ij}, b_{ij}]$ en $(n + 2d)d$ variables lo llamaremos un

súper anillo. Las filas de matriz $\begin{pmatrix} A \\ X \\ B \end{pmatrix}$ están ordenadas de la siguiente forma

$$a_1 < \ldots < a_d < x_1 < x_2 < \ldots < x_n < b_1 < \ldots < b_d.$$

El correspondiente anillo de soporte $\mathbb{C}[\Lambda(n+2d,d)]$ es generado por los soportes de la forma $[a_{j_1} \ldots a_{j_s} x_{j_1} \ldots x_{j_t} b_{k_1} \ldots b_{k_{d-s-t}}]$. La idea más importante para demostrar el resultado principal de esta sección es definir dos homomorfismos de $\mathbb{C}$-álgebras $\mathbb{C}[x_{ij}] \to \mathbb{C}[\Lambda(n+2d,d)]$. Estos homomorfismos son definidos por

$$x_{ij} \mapsto [a_1 \ldots a_{j-1} x_i a_{j+1} \ldots a_d] \quad \text{y} \quad x_{ij} \mapsto [b_1 \ldots b_{j-1} x_i b_{j+1} \ldots b_d].$$

Lema 3.5
Sea $Q = Q(x_{ij}) \in \mathbb{C}[x_{ij}]$ cualquier $GL(\mathbb{C}^d)$-invariante relativo de indice p. Entonces el polinomio de soporte

$$\begin{array}{c} [b_1 b_2 \ldots b_d]^{p(d-1)} \cdot Q([a_1 \ldots a_{j-1} x_i a_{j+1} \ldots a_d] \\ -[a_1 a_2 \ldots a_d]^{p(d-1)} \cdot Q([b_1 \ldots b_{j-1} x_i b_{j+1} \ldots b_d]) \end{array}$$

pertenece al ideal de sicigias $I_{n+2d,d} \subset \mathbb{C}[\Lambda(n+2d,d)]$.

Demostración. Necesitamos mostrar que la imagen del polinomio de soporte anterior bajo la especialización genérica $\Phi_{n+2d,d}$ es cero. Para simplificar la notación se abreviará el determinante $\Phi_{n+2d,d}([\lambda])$ con el correspondiente soporte $[\lambda]$. Sea $Adj(A)$ la matriz adjunta de A. Las entradas $Adj(A)_{jk}$ es el menor de dimensión $(d-1)(d-1)$ de A, el cual es obtenido eliminando la j-ésima fila y la k-ésima columna de A. Por la expansión de Laplace obtenemos

$$[a_1 \ldots a_{j-1} x_i a_{j+1} \ldots a_d] = \sum_{k=1}^{d} Adj(A)_{jk},$$

y por lo tanto

$$\begin{aligned}[a_1a_2\dots a_d]^{p(d-1)}\cdot Q(x_{ij}) &= \det(A)^{p(d-1)}\cdot Q(x_{ij})\\ &= \det(Adj(A))^{p}\cdot Q(x_{ij})\\ &= (Q\circ Adj(A))(x_{ij})\\ &= Q\left(\sum_{k=1}^{d} Adj(A)_{jk}\right)\\ &= Q\left([a_1\dots a_{j-1}x_ia_{j+1}\dots a_d]\right)\end{aligned}$$

El mismo argumento se puede usar para la matriz B. Esto implica la identidad deseada en $\mathcal{B}_{n+2d,d}$:

$$\begin{aligned}[b_1b_2\dots b_d]^{p(d-1)}[a_1a_2\dots a_d]^{p(d-1)}\cdot Q(x_{ij}) &= [b_1b_2\dots b_d]^{p(d-1)}\cdot Q\left([a_1\dots a_{j-1}x_ia_{j+1}\dots a_d]\right)\\ &= [a_1a_2\dots a_d]^{p(d-1)}\cdot Q([b_1\dots b_{j-1}x_ib_{j+1}\dots b_d])\end{aligned}$$

□

Teorema 3.2
*(***Primer teorema fundamental de teoría invariantes.)** */4, pág. 85 , cap. 3/ El anillo invariante* $\mathbb{C}[x_{ij}]^{SL(\mathbb{C}^d)}$ *está generado por los* $d\times d$ *menores de la matriz* $X=(x_{ij})$ *es decir:*

$$\mathbb{C}[x_{ij}]^{SL(\mathbb{C}^d)}\cong \mathbb{C}[\Lambda(n,d)]/I_{n,d}\cong \mathcal{B}_{n,d}.$$

Demostración. Por el **Lema 3.4**, podemos asumir que dado un invariante Q existe $p\geq 0$ tal que Q es $GL(\mathbb{C}^d)$-invariante relativo de índice p. Podemos aplicar el algoritmo de enderezamiento al polinomio

$$[b_1b_2\dots b_d]^{p(d-1)}\cdot Q([a_1\dots a_{j-1}x_ia_{j+1}\dots a_d])\in\mathbb{C}[\Lambda(n+2d,d)]$$

es decir, hemos calculado su forma normal módulo la Base de Groebner dada en el **Teorema 3.1**. Dado que todos los índices de la fila $b_1,b_2,\dots,b_d$ son mayores que los índices de la fila $a_1,\dots,a_d,x_1,x_2,\dots x_n$, el resultado es una combinación lineal de la tabla estándar de la forma:

$$\sum_j T_j(a_1\dots a_d,x_1,x_2,\dots,x_n)\cdot[b_1b_2\dots b_d]^{p(d-1)}$$

Donde los T_j son ciertas tablas estándar en los índices de las filas $a_1, \ldots, a_d$ y $x_1, x_2, \ldots x_n$. Similarmente, el polinomio

$$[a_1 a_2 \ldots a_d]^{p(d-1)} \cdot Q([b_1 \ldots b_{j-1} x_i b_{j+1} \ldots b_d])$$

se endereza a un polinomio

$$\sum_k [a_1 a_2 \ldots a_d]^{p(d-1)} \cdot T'_k(x_1, x_2, \ldots x_n, b_1, \ldots, b_d)$$

Donde los T'_k son tablas estándar en los índices $x_1, \ldots, x_n, b_1, \ldots, b_d$. Por el **Lema 3.5** y la ley de enderezamiento (**Corolario 3.1**), estas dos expansiones de tablas estándar deben ser iguales en $\mathbb{C}[\Lambda(n+2d, d)]$. Pero esto es solamente posible si ambas sumas son de la forma

$$\sum_l [a_1 \ldots a_d]^{p(d-1)} \cdot T''_l(x_1, x_2, \ldots, x_n) \cdot [b_1 b_2 \ldots b_d]^{p(d-1)}$$

Donde los T''_l son ciertas tablas estándar solamente en los índices anteriores $x_1, x_2, \ldots, x_n$. Por otro lado, por la prueba del **Lema 3.5**, ambos polinomios son iguales a

$$[a_1 \ldots a_d]^{p(d-1)} [b_1 \ldots b_d]^{p(d-1)} \cdot I(x_{ij})$$

Esto implica la expansión deseada

$$Q(x_{ij}) = \sum_l T''_l(x_1, x_2, \ldots, x_n).$$

□

Nuestra prueba del Primer Teorema Fundamental implica el siguiente algoritmo para reescribir un polinomio $Q \in \mathbb{C}[x_{ij}]^{SL(\mathbb{C}^d)}$-invariante en términos de soportes.

Algoritmo 2 Representación de soporte

Input: Un polinomio $Q \in \mathbb{C}[x_{ij}]^{SL(\mathbb{C}^d)}$-invariante

Out: Un polinomio de soporte $P \in \mathbb{C}[\Lambda(n,d)]$ cuya expansión es igual a $Q(x_{ij})$.

1: Reemplazaremos cada variable x_{ij} en $Q(x_{ij})$ por el soporte correspondiente $[a_1 \dots a_{j-i} x_i a_{j+i} \dots a_d]$.

2: Aplicamos el algoritmo de enderezamiento para el anillo de soporte extendido $\mathbb{C}[\Lambda(n+d,d)]$, con respecto al orden $a_1 < \ldots < a_d < x_1 < x_2 < \ldots < x_n$ en los índices de las filas.

3: Si Q es un relativo invariante de índice p, entonces $[a_1 \dots a_d]^{p(d-1)}$ aparece como factor en la representación estándar. Dividiendo este factor, obtenemos la expansión única de $Q(x_{ij})$ en términos de la tabla estándar en los índices de las filas x_i.

Sea "$\prec$" denota el orden monomial lexicográfico en $\mathbb{C}[x_{ij}]$ inducido del orden de las variables $x_{11} \prec x_{12} \prec \ldots \prec x_{1d} \prec x_{21} \prec x_{22} \prec \ldots \prec x_{2d} \prec \ldots \prec x_{n1} \prec x_{n2} \prec \ldots \prec x_{nd}$. Esto es llamado *el orden diagonal*. Un monomio $m \in \mathbb{C}[x_{ij}]$ se dice que es *diagonal* si su grado es divisible por d y si puede ser escrito en la forma:

$$m = \prod_{i=1}^{k} (x_{\lambda_1^i 1} x_{\lambda_2^i 2} \cdots x_{\lambda_d^i d}) \tag{3.2.1}$$

Donde $\lambda_1^i < \lambda_2^i < \ldots < \lambda_d^i$ para todo $i = 1, 2, \ldots, k$. Es fácil ver que el monomio inicial de cualquier tabla (expandida) es un monomio diagonal.

Lema 3.6
Sea T la tabla $[\lambda^1][\lambda^2] \cdots [\lambda^k] \in \mathbb{C}[\Lambda(n,d)]$. Entonces el monomio inicial en la expansión de $\Phi_{n,d}(T) \in \mathbb{C}[x_{ij}]$ con respecto a "$\prec$" es igual al monomio diagonal m en la ecuación (3.2.1).

Recíprocamente, cada monomio diagonal es el monomio inicial de alguna tabla.

Lema 3.7
Sea m el monomio diagonal en (3.2.1). *Entonces existe una única tabla T_m tal que $lt_{\prec}(\Phi_{n,d}(T_m)) = m$.*

La tabla T_m en la que hace referencia el **Lema 3.7** es construida a partir del monomio diagonal como sigue. Considerando la tabla

$$T = \begin{bmatrix} \lambda_1^1 & \cdots & \lambda_d^1 \\ \lambda_1^2 & \cdots & \lambda_d^2 \\ \vdots & \ddots & \vdots \\ \lambda_1^k & \cdots & \lambda_d^k \end{bmatrix}$$

entonces la tabla estándar T_m resulta ser la única tabla estándar que se obtiene de T ordenando las d columnas.

El **Lema 3.6** y el **Lema3.7** implican la correctitud del siguiente algoritmo para calcular las representaciones descritas en el Primer Teorema Fundamental de la teoría de invariantes.

Algoritmo 3 Representación de soporte

Input: Un polinomio $Q \in \mathbb{C}[x_{ij}]$ el cual es un invariante de $SL(\mathbb{C}^d)$
Out: Un polinomio de soporte $P \in \mathbb{C}[\Lambda(n,d)]$ cuya expansión es igual a $Q(x_{ij})$.

1: Si $Q = 0$, entonces el algoritmo devuelve la representación de soporte con el valor $P = 0$.
2: Sea $m := lt_{\prec}(Q)$.
3: Si m no es diagonal, entonces el algoritmo termina y devuelve: "*Q no es un invariante*".
4: Por otro lado, sea c el coeficiente de $lt_{\prec}(Q)$ de Q, el algoritmo devuelve el sumando $c \cdot T_m$, reemplazar Q por $Q - c \cdot \phi_{n,d}(T_m)$, y retornar al paso 1.

Ejemplo 3.3
Una proyección de seis puntos $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$, $\boldsymbol{E}$ *y* $\boldsymbol{F}$ *del plano proyectivo* $\mathbb{CP}^2$ *se dice que es un conjunto cuadrilátero si las triplas* $\boldsymbol{AFD}, \boldsymbol{ACE}, \boldsymbol{BCF}$ *y* $\boldsymbol{BED}$ *son colineales. Ver la* **Figura 3.2**.

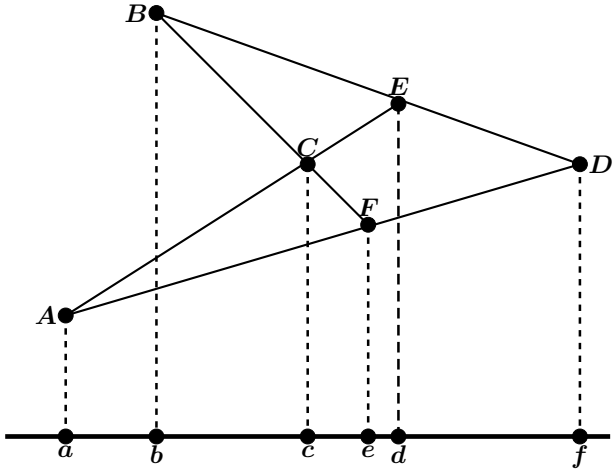


Figura 3.2: La proyección de un conjunto cuadrilátero.

Diremos que los seis puntos $\boldsymbol{a} = (a_1 : a_2), \ldots, \boldsymbol{f} = (f_1 : f_2)$ *son la proyección de un conjunto cuadrilátero si y sólo si existen números complejos* $a_3, b_3, c_3, d_3, e_3, f_3$ *tal que los puntos* $\boldsymbol{A} = (a_1 : a_2 : a_3), \ldots, \boldsymbol{F} = (f_1 : f_2 : f_3)$ *formen un conjunto cuadrilátero. Veremos que la propiedad geométrica "ser conjunto cuadrilátero" es equivalente a la propiedad algebraica "*$Q = 0$*", donde:*

$$\begin{aligned} Q = &- a_1b_1c_1d_2e_2f_2 - a_1b_1c_2d_1e_2f_2 + a_1b_1c_2d_2e_1f_2 + a_1b_1c_2d_2e_2f_1 \\ &+ a_1b_2c_1d_1e_2f_2 - a_1b_2c_2d_2e_1f_1 + a_2b_1c_1d_1e_2f_2 - a_2b_1c_2d_2e_1f_1 \\ &- a_2b_2c_1d_1e_1f_2 - a_2b_2c_1d_1e_2f_1 + a_2b_2c_1d_2e_1f_1 + a_2b_2c_2d_1e_1f_1. \end{aligned}$$

Solución. Primero demostraremos que si los seis puntos $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{d}$, $\boldsymbol{e}$ y $\boldsymbol{f}$ forman la proyección de un conjunto cuadrilátero, entonces $Q = 0$.

En efecto, supongamos que los seis puntos $\boldsymbol{a} = (a_1 : a_2), \ldots, \boldsymbol{f} = (f_1 : f_2)$ son la proyección de un conjunto cuadrilátero entonces existen números com-

plejos $a_3, b_3, c_3, d_3, e_3, f_3$ tales que los puntos:
$\boldsymbol{A} = (a_1 : a_2 : a_3), \ldots, \boldsymbol{F} = (f_1 : f_2 : f_3)$ son un conjunto cuadrilátero, entonces $\boldsymbol{AFD}, \boldsymbol{ACE}, \boldsymbol{BCF}$ y $\boldsymbol{BED}$ son colineales, por lo que $\det(A, F, D) = 0$, y así sucesivamente para los demás puntos colineales formando el siguiente sistema de ecuaciones en las variables $a_3, b_3, c_3, d_3, e_3, f_3$

$$\begin{cases} \det(A, F, D) = 0 \\ \det(A, C, E) = 0 \\ \det(B, C, F) = 0 \\ \det(B, E, D) = 0 \end{cases}$$

cuya matriz de coeficientes es de 4×6, la cual no puede tener rango cuatro porque la solución de ese sistema no debe ser la trivial. Así, pues debe tener rango como máximo 3, de donde cada subdeterminante de 4×4 debe anularse y uno de esos determinantes es el siguiente:

$$\begin{vmatrix} (a_1 f_2 - a_2 f_1) & -(a_1 d_2 - a_2 d_1) & 0 & 0 \\ (b_1 e_2 - b_2 e_1) & 0 & (d_1 e_2 - d_2 e_1) & 0 \\ 0 & (b_1 c_2 - b_2 c_1) & (c_1 f_2 - c_2 f_1) & -(b_1 f_2 - b_2 f_1) \\ 0 & 0 & 0 & -(a_1 e_2 - a_2 e_1) \end{vmatrix} = 0$$

$$= -\underbrace{(a_1 e_2 - a_2 e_1)}_{\neq 0} \cdot Q = 0$$
$$\Rightarrow Q = 0$$

Para la otra implicación veremos que el polinomio Q es invariante bajo la acción del grupo $SL(\mathbb{C}^2)$ y podemos calcular una representación de soporte usando cualesquiera de los **Algoritmos 2** y **3**.
Escribimos las coordenadas homogéneas de los seis puntos como columnas para formar la matriz

$$\mathbf{X} := \begin{pmatrix} a_1 & b_1 & c_1 & d_1 & e_1 & f_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 & f_2 \end{pmatrix}$$

En la aproximación del enderezamiento reemplazamos $\mathbf{X}$ por la matriz extendida.

$$\mathbf{X}' := \begin{pmatrix} a_1 & b_1 & c_1 & d_1 & e_1 & f_1 & 0 & -1 \\ a_2 & b_2 & c_2 & d_2 & e_2 & f_2 & 1 & 0 \end{pmatrix}$$

cuyas últimas dos columnas son etiquetadas como 1 y 2. Expresamos cada matriz entrante de $\mathbf{X}$ como un maximal menor de $\mathbf{X}'$ por $a_1 = [a1], b_1 = [b1], \ldots, f_2 = [f2]$.
Esto transforma el invariante Q en el siguiente polinomio de soporte:

$$\begin{aligned} &-[a1][b1][c1][d2][e2][f2] - [a1][b1][c2][d1][e2][f2] \\ &+[a1][b1][c2][d2][e1][f2] + [a1][b1][c2][d2][e2][f1] \\ &+[a1][b2][c1][d1][e2][f2] - [a1][b2][c2][d2][e1][f1] \\ &+[a2][b1][c1][d1][e2][f2] - [a2][b1][c2][d2][e1][f1] \\ &-[a2][b2][c1][d1][e1][f2] - [a2][b2][c1][d1][e2][f1] \\ &+[a2][b2][c1][d2][e1][f1] + [a2][b2][c2][d1][e1][f1] \end{aligned}$$

Aplicamos el algoritmo de enderezamiento para $\mathbb{C}[\Lambda(8,2)]$ con respecto al orden de los índices de las columnas $a < b < c < d < e < f < 1 < 2$. En la estrategia específica utilizada en la implementación por el autor del algoritmo de enderezamiento, este cálculo requiere de 58 pasos. La salida es la siguiente combinación lineal de la tabla estándar:

$$\begin{aligned} &-[ab][cd][ef][12][12][12] + [ab][ce][df][12][12][12] \\ &+[ac][bd][ef][12][12][12] - [ac][be][df][12][12][12] \\ &-[ad][be][cf][12][12][12] \end{aligned}$$

Por lo tanto el invariante Q tiene la siguiente representación en soporte:

$$Q = -[ab][cd][ef] + [ab][ce][df] + [ac][bd][ef] - [ac][be][df] - [ad][be][cf] \tag{3.2.2}$$

Para el mismo polinomio Q. El **Algoritmo 3** se implementa como sigue. El monomio inicial de Q con el orden monomial diagonal es $m = a_1b_1c_1d_2e_2f_2$. La correspondiente tabla estándar es $T_m = -[ad][be][cf]$ y reemplazamos Q por $Q - \Phi_{(6,3)}(T_m)$. Ahora el monomio inicial es igual a $a_1b_1 \times c_2d_1e_2f_2$

y lo restamos de la expansión de $-[ad][be][df]$. El nuevo monomio inicial es $a_1b_1c_2d_2e_1f_2$ y se resta de $[ac][bd][ef]$. El nuevo monomio inicial es $a_1b_2c_1d_1e_2f_2$ y se resta de $[ab][ce][df]$. El nuevo monomio inicial es $a_1b_2c_1d_2e_1f_2$ y se resta de $-[ab][cd][ef]$. El número de pasos necesarios en el **Algoritmo 3** son cinco, donde este número siempre es igual al tamaño de la salida.
Notar que la representación en soportes encontrada por ambos métodos no es en general mínima.
En nuestro ejemplo, la representación mínima de soporte de Q sólo tiene dos tablas:

$$Q = -[ad][cf][be] - [af][bc][de].$$

□

En general para invariantes de $SL(\mathbb{C}^d)$, sigue siendo un problema interesante encontrar un buen algoritmo para calcular una representación de soporte teniendo un número mínimo de tablas.

Conclusiones

⋆ Dado un grupo finito de matrices, el anillo invariante está generado por un conjunto finito de invariantes algebraicamente independientes.

⋆ Las bases de Groebner dan una herramienta computacional para determinar si un conjunto de invariantes es completo i.e. genera todo el anillo invariante.

⋆ El Grupo de Galois de un polinomio mónico irreducible se puede calcular usando métodos computacionales fundamentados en la teoría de invariantes.

⋆ En Geometría Proyectiva los polinomios invariantes bajo la acción del Grupo Especial Lineal se corresponden a propiedades geométricas en el espacio proyectivo.

Bibliografía

[1] D.A. Cox, J. Little y D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer New York, 2008. ISBN: 9780387356501.

[2] H. Derksen y G. Kemper. *Computational Invariant Theory*. Encyclopaedia of Mathematical Sciences. Springer Berlin Heidelberg. ISBN: 9783540434764.

[3] J.B. Fraleigh. *A First Course in Abstract Algebra*. Pearson Education, 2003. ISBN: 9788177589009.

[4] P. Paule y B. Sturmfels. *Algorithms in Invariant Theory*. Texts & Monographs in Symbolic Computation. Springer Vienna, 2008. ISBN: 9783211774175.

[5] B. Steinberg. *Representation Theory of Finite Groups: An Introductory Approach*. Universitext. Springer New York, 2011. ISBN: 9781461407768.