UNIVERSIDAD AUTÓNOMA DE ZACATECAS

"Francisco García Salinas"

UNIDAD ACADÉMICA DE MATEMÁTICAS

ACCIÓN DE GRUPOS FINITOS SOBRE ESPACIOS AFINES

T E S I S

QUE PARA OBTENER EL GRADO DE

MAESTRA EN MATEMÁTICAS

PRESENTA

YURIKO PITONES AMARO

ASESOR

Dr. ALEXIS GARCÍA ZAMORA

ZACATECAS, ZAC. OCTUBRE 2015

AGRADECIMIENTOS

Quiero agradecer de manera especial al *Dr. Alexis García Zamora*, por aceptar dirigir esta tesis, por el trabajo y tiempo dedicado a la misma. Sus conocimientos, su manera de trabajar, su persistencia, su paciencia y su motivación han sido fundamentales para mi formación, ganándose mi admiración. Gracias por todo lo recibido durante este tiempo.

Quiero agradecer a los sinodales:

Dra. Claudia Reynoso

Dr. Rafael H. Villarreal

Dr. Andrés Daniel Duarte

Dr. Hernán de Alba Casillas

Por revisar esta tesis, por sus correcciones y sugerencias, por todas las observaciones realizadas. Todas sus contribuciones mejoraron este trabajo.

DEDICATORIA

A mi familia, quienes siempre han estado en los buenos y malos momentos, incluso en los que nadie quisiera enfrentar. A mis padres, *Juan Luis y Josefa*, pilares fundamentales en mi vida, quienes han hecho de mi lo que ahora soy, les agradezco por ser los mejores padres, y les dedico este logro que no solo ha sido mío, sino mucho de él es de ustedes. ¡Los amo y gracias!.

A mis hermanos, *Yoshio y Cain*, por siempre apoyarme, porque a nuestra manera sabemos que siempre podemos contar uno con el otro y nunca nos fallaremos.

A mi cuñada, *Naty*, porque desde que llegaste a nuestra familia te convertiste en una hermana para mí, gracias por todo el apoyo y amistad. A mis sobrinos *Brayan y Zairy*, pues con pequeñas cosas me han dado grandes alegrías y son un motivo para lograr mis metas.

Acción de Grupos Finitos Sobre Espacios Afines

Yuriko Pitones Amaro

Asesor: Dr. Alexis García Zamora

Octubre 2015

Índice general

Introducción

La teoría de invariantes es una rama del álgebra abstracta que estudia las acciones de grupos de transformaciones en variedades. Clásicamente la teoría hace una descripción explícita de funciones polinomiales que permanecen invariantes bajo las transformaciones de un grupo lineal dado. A mediados del siglo XIX se desarrollan los métodos algebraicos formales para la construcción de invariantes, y se presenta el problema de saber si el anillo de invariantes es finitamente generado, si lo es, quiénes son sus generadores. Hilbert [10] trabajó en esta cuestión, y es ahí donde se comienza a desarrollar mucha de la teoría de invariantes.

Una gran parte del álgebra conmutativa se formula en forma no constructiva. Un ejemplo típico es el teorema de la base de Hilbert. Sin embargo, el álgebra conmutativa también tiene una gran parte computacional, el cual se ha convertido en un campo de investigación propio. En la presente tesis se introduce una pequeña visión de este campo, específicamente en el capítulo 1 se desarrolla la teoría de Bases de Gröbner, particularmente estamos interesados en utilizar este método para encontrar relaciones entre polinomios.

En el capítulo 2 veremos la teoría básica de Representaciones de grupos finitos pues estamos interesados en el anillo de invariantes $K[V]^G$ donde V es una representación de dimensión finita de un grupo G de orden p.

El principal objetivo que abordaremos en esta tesis es describir una forma explicita de cómo son las relaciones entre los generadores del anillo de invariantes $K[V]^G$. Para esto a partir del capítulo 3 nos enfocaremos en teoría de invariantes.

En el capítulo 4 se describe un método para calcular las relaciones de los

generadores de $K[V]^G$ en el caso donde V es una representación de G dos dimensional, dado por John C. Harris y David L. Wehlau en [9].

En los capítulos 5 y 6 consideramos G un grupo cíclico finito y V una representación dimensionalmente finita de G. Daremos algunos resultados que en conjunto nos proporcionan un método para el cálculo de generadores de $K[V]^G$ y de las relaciones entre ellos. Por último en el capítulo 7 calculamos las relaciones de los generadores de un grupo cíclico de orden p (p no necesariamente primo) y $dim(V) = n$, generalizaremos la fórmula dada por Harris y Wehlau en [9], para conocer de forma explicita como son las relaciones, además de dar algunos ejemplos donde emplearemos los diferentes métodos antes mencionados.

Capítulo 1

Bases de Gröbner

Las bases de Gröbner se introdujeron en 1965, junto con un algoritmo para calcularlas (el algoritmo de Buchberger), por Bruno Buchberger en su tesis doctoral [3]. El objetivo de este capítulo es introducir la noción de Base de Gröbner y presentar este algoritmo [15], [5].

1.1. Algoritmo de Buchberger

Fijemos las siguientes convenciones.

K denotará un campo y $K[x_1, ..., x_n]$ el anillo de polinomios en n variables.

Un polinomio de la forma $t = x_1^{e_1} \cdot ... \cdot x_n^{e_n}$ con $e_i \in \mathbb{N}_0$ se llama *monomio*.

Un polinomio de la forma ct con $c \in K \setminus \{0\}$ y t un monomio se llama *término*.

Para $f \in K[x_1, ..., x_n]$ un polinomio $T(f)$ denota el conjunto de todos los términos en f. Entonces $f = \sum_{ct \in T(f)} ct$.

$Mon(f)$ denota el conjunto de todos los monomios en f. En particular $f = 0$ si y sólo si $Mon(f) = \emptyset$.

Con polinomios de una variable, podemos comparar monomios, lo que conduce a nociones como grado, coeficiente principal, división (con residuo);

para polinomios de varias variables no hay una forma canónica para comparar monomios. Para resolver este problema damos la siguiente definición.

Definición 1.1. *Sea M el conjunto de todos los monomios en $K[x_1, ..., x_n]$.*

a) Un orden monomial en $K[x_1, ..., x_n]$ es un orden "$\leq$" con las siguientes propiedades.

(1) "$\leq$" es un orden total, es decir si $s, t \in M$ entonces $s \leq t$ o $t \leq s$.

(2) Si $t \in M$, entonces $1 \leq t$.

(3) Si $s, t_1, t_2 \in M$ con $t_1 \leq t_2$, entonces $st_1 \leq st_2$.

b) Supongamos que "$\leq$" es un orden monomial, si $f \in K[x_1, ..., x_n]$ es un polinomio no cero denotamos $LM(f)$ al elemento más grande de $Mon(f)$, $LC(f) \in K$ el coeficiente de $LM(f)$ en f y $LT(f) := LC(f)LM(f)$.
$LM(f)$ se llama el monomio líder de f.
$LC(f)$ se llama el coeficiente líder de f.
$LT(f)$ se llama el término líder de f.

Para $f = 0$, $LM(f) = LT(f) = LC(f) = 0$ y extendemos "$\leq$" por la convención $0 < 1$.

Veamos algunos ejemplos de órdenes monomiales.

Ejemplo 1.1. *Sea $t = x_1^{e_1} \cdot ... \cdot x_n^{e_n}$ y $t' = x_1^{e'_1} \cdot ... \cdot x_n^{e'_n}$ monomios.*

1. *El orden lexicográfico (lex)*
   $t \leq t'$ si $t = t'$ o $e_i < e'_i$ para el índice más pequeño tal que $e_i \neq e'_i$.

2. *El orden lexicográfico graduado inverso (grevlex)*
   $t \leq t'$ si $t = t'$ o $deg(t) = \sum_{i=1}^{n} e_i < deg(t') = \sum_{i=1}^{n} e'_i$ o $deg(t) = deg(t')$ y $e_i > e'_i$ para el mayor índice tal que $e_i \neq e'_i$.

3. *Supongamos que tenemos dos órdenes monomiales $\leq_1$ y $\leq_2$ en $K[x_1, ..., x_k]$ y en $K[x_{k+1}, ..., x_n]$ respectivamente. Entonces el orden bloque (orden producto) $\leq$ está definido como un orden en $K[x_1, ..., x_n]$ como*
   $t \leq t'$ si $x_1^{e_1} \cdot ... \cdot x_k^{e_k} <_1 x_1^{e'_1} \cdot ... \cdot x_k^{e'_k}$ o $x_1^{e_1} \cdot ... \cdot x_k^{e_k} = x_1^{e'_1} \cdot ... \cdot x_k^{e'_k}$ y $x_{k+1}^{e_{k+1}} \cdot ... \cdot x_n^{e_n} \leq_2 x_{k+1}^{e'_{k+1}} \cdot ... \cdot x_n^{e'_n}$.
   En este caso $\leq_1$ se dice dominante (análogamente podemos definir el orden con $\leq_2$ dominante).

Recordemos que un conjunto M con un orden se dice bien ordenado si todo subconjunto no vacío $N \subseteq M$ tiene elemento mínimo $y \in N$, es decir, $y \leq x \ \forall x \in N$.

Lema 1.1. *(Los órdenes monomiales son buenos órdenes)*
El conjunto M de todos los monomios en $K[x_1, ..., x_n]$ es bien ordenado por el orden monomial $\leq$.

Demostración. Sea $N \subseteq M$ un subconjunto no vacío, por el Lema de Dickson [[5],Cap. 2.4, Teorema 5], existen $t_1, ..., t_m \in N$ que generan el ideal $\langle N \rangle_{K[x_1,...,x_n]}$.

Como $\leq$ es un orden total, existe i tal que $t_i \leq t_j$ para $1 \leq j \leq m$.

Sea $t \in N$, entonces $t = f_1 t_1 + ... + f_m t_m$ con $f_i \in K[x_1, ..., x_n]$, notemos que t aparece como un monomio en al menos uno de los $f_j t_j$, se sigue que t es múltiplo de t_j, de la Definición 1.1 (2), tenemos que, $t \geq t_j \geq t_i$. Por lo tanto t_i es el elemento mínimo de N.

□

Definición 1.2. *a) Sea $S \subseteq K[x_1, ..., x_n]$ un conjunto de polinomios, el ideal*

$$L(S) := \langle LM(f) | f \in S \rangle_{K[x_1,...,x_n]}$$

Se llama el Ideal Líder de S.

b) Sea $I \subseteq K[x_1, ..., x_n]$ un ideal. Un subconjunto finito $G \subseteq I$ se llama una G-base (Base de Gröbner) con respecto a la elección del orden monomial $\leq$, de I si

$$L(I) = L(G)$$

equivalentemente, G es G-bases si para cada $f \in I$ no cero existe un $g \in G$ tal que $LM(g)$ divide a $LM(f)$.

Ejemplo 1.2. *$K[x_1, ..., x_n]$ (como un ideal en sí mismo) con el orden lexicográfico tiene la G-base $G = \{1\}$, sin embargo el conjunto $S := \{x_1, x_1 + 1\}$ no es G-base pues $L(S) = \langle x_1 \rangle_{K[x_1,...,x_n]}$.*

Definición 1.3. *Sea $S = \{g_1, ..., g_r\} \subset K[x_1, ..., x_n]$ un conjunto finito de polinomios, $f \in K[x_1, ..., x_n]$ y $\leq$ un orden monomial en $K[x_1, ..., x_n]$.*

1. *Decimos que f es una forma normal con respecto a S si no hay $t \in Mon(f)$ divisible por el monomio líder $LM(g_i)$ de cualquier $g_i \in S$.*

2. *Un polinomio $f^* \in K[x_1, ..., x_n]$ se dice que es una forma normal de f con respecto a S si satisface las siguientes condiciones:*

   1) f^* es forma normal con respecto a S.

   2) Existen $h_1, ..., h_r \in K[x_1, ..., x_n]$ tal que

$$f - f^* = \sum_{i=1}^{r} h_i g_i \text{ y } LM(h_i g_i) \leq LM(f) \ \forall i. \tag{1.1}$$

   En particular f y f^* son congruentes módulo el ideal generado por S.

Ejemplo 1.3. *Sean $S = \{x_1, x_1 + 1\}$ y $\leq$ el orden lexicográfico.*

$f = x_1$ tiene dos formas normales 0 y -1, tenemos que 0 es forma normal con respecto a S y $x_1 - 0 = x_1 + 0(x_1 + 1)$ y además $LM(x_1) = x_1 \leq LM(f)$ y $LM(0) = 0 \leq LM(f)$, entonces 0 es forma normal de f con respecto a S. Por otro lado tenemos que $Mon(-1) = 1$ y entonces $LM(x_1) = LM(x_1 + 1) = x_1$ no divide a 1, además tenemos que $x_1 - 1 = 2x_1 - (x_1 + 1)$ y $LM(2x_1) \leq LM(x_1)$ y $LM(-x_1 + 1) \leq LM(x_1)$, se sigue que -1 es una forma normal de f respecto a S.

0 no es forma normal de 1,ya que 1 es congruente con 0 módulo $\langle S \rangle$, pues $1 - 0 = 1 = -x_1 + x_1 + 1$, sin embargo, $LM(-x_1) \leq LM(1) = 1$ y $LM(x_1 + 1) \leq LM(1)$ lo cual contradice la definición de orden monomial.

Entonces en general las formas normales no están determinadas de manera única.

Veremos ahora un algoritmo para calcular la forma normal de un polinomio respecto a un conjunto finito de polinomios.

Algoritmo 1.1. *(Forma Normal)*
Entrada: Un conjunto finito de polinomios $S = \{g_1, ..., g_r\} \subseteq K[x_1, ..., x_n]$ y un polinomio $f \in K[x_1, ..., x_n]$.
Salida: Una forma normal f^* de f con respecto a S y polinomios $h_1, ..., h_r \in$

$K[x_1, ..., x_n]$ que satisfacen (1.1).
Pasos:

1. *Definimos $f^* := f$ y $h_i = 0 \ \forall i \in \{1, ..., r\}$.*

2. *Definir $\mu = \{(t, i) | t \in Mon(f^*) \ i \in \{1, ..., r\}$ tal que $LM(g_i)$ divide a $t\}$.*

3. *Si $\mu = \emptyset$ termina y regresa f^* y los h_i.*

4. *Elija $(t, i) \in \mu$ con t máximo y sea $c \in K$ el coeficiente de t en f^*.*

5. *Defina*

$$f^* := f^* - \frac{ct}{LT(g_i)} g_i \quad y \quad h_i := h_i + \frac{ct}{LT(g_i)}.$$

En el paso (5) el término ct se elimina de f^* y sólo los monomios que son más pequeños que t pueden añadirse a f^*.

Ejecución en SINGULAR [8] (Forma Normal)

```
> ring r=0, (x(1),x(2),  ...  ), orden;
> poly f1=   ;
> poly f2=   ;
  ⋮
> poly fn=   ;
> poly f=   ;
> ideal i=f1,f2,..., fn;
> ideal j=groebner(i);
> reduce (f,j);
```

Ejemplo 1.4. *Sean $K[x, y]$ el anillo de polinomios en dos variables, $f = x^2y + xy^2 + y^2$ y $S = \{f_1 = xy - 1, f_2 = y^2 - 1\}$, queremos encontrar una forma normal de f con respecto a S con el orden lexicográfico inverso ($y < x$).*

El monomio líder de cada polinomio es el siguiente:

$$LM(f) = x^2y \quad LM(f_1) = xy \quad LM(f_2) = y^2.$$

Ordenamos los polinomios según el orden monomial y dividimos f entre el primer polinomio, dividimos el primer monomio de f entre el monomio líder de f_1, y realizamos el proceso de división.

$$\begin{array}{lll} & & x+y \\ & & \\ xy-1 & y^2-1 \Big| & x^2y+xy^2+y^2 \\ & & -x^2y+x \\ & & \hline xy^2+x+y^2 \\ & & -xy^2+y \\ & & \hline x+y^2+y=g_1 \end{array} \qquad \begin{array}{l} \textit{residuo} \\ \\ \\ \\ \\ \\ x \end{array}$$

Notamos que $LM(g_1)$ ya no se puede dividir por $LM(f_1)$, así que lo consideramos como residuo. Consideramos el resto del polinomio g_1 y lo dividimos entre $f_2 = y^2 - 1$.

$$\begin{array}{lll} & & 1 \\ & & \\ y^2-1 & \Big| & y^2+y \\ & & -y^2+1 \\ & & \hline y+1=g_2 \end{array} \qquad \begin{array}{l} \textit{residuo} \\ \\ \\ \\ y+1 \end{array}$$

Aquí también observamos que $LM(g_1)$ ya no se puede dividir por $LM(f_1)$ entonces lo pasamos a la columna de residuo. Se sigue que;

$$f = (x+y)f_1 + (1)f_2 + (x+y+1).$$

Entonces la forma normal de f con respecto a S es $x+y+1$.

Teorema 1.1. *(La aplicación de la forma normal)*
Sea G una G-base de un ideal $I \subseteq K[x_1, ..., x_n]$.

(a) Todo $f \in K[x_1, ..., x_n]$ tiene precisamente una forma normal con respecto a G. Por lo tanto, hay una aplicación $NF_G : K[x_1, ..., x_n] \to K[x_1, ..., x_n]$ que asigna a cada polinomio su forma normal con respecto a G.

(b) La aplicación NF_G es K-lineal y $\ker(NF_G) = I$.

(c) Si $\bar{G}$ es otra G-base de I (con respecto al mismo orden monomial) entonces $NF_{\bar{G}} = NF_G$. Entonces la aplicación NF_G depende sólo de I y de la elección del orden monomial.

Demostración. Primero probaremos (a) y (c). Sean f^* y $\bar{f}$ formas normales de f con respecto a G y $\bar{G}$ G-bases respectivamente, de (1.1) tenemos que $f - \bar{f} \in \langle \bar{G} \rangle \subset I$ y $f - f^* \in \langle G \rangle \subset I$, lo que implica que

$f - \bar{f} - (f - f^*) = f^* - \bar{f} \in I$, entonces $LM(f^* - \bar{f}) \in L(I) = L(G) = L(\bar{G})$.

Ahora supongamos que $f^* \neq \bar{f}$, por la definición de G-base tenemos que para $f^* - \bar{f} \in I$ existe $g \in G$ tal que $LM(g)$ divide a $LM(f^* - \bar{f})$ y también existe $\bar{g} \in \bar{G}$ tal que $LM(\bar{g})$ divide a $LM(f^* - \bar{f})$. Pero $LM(f^* - \bar{f}) \in Mon(f^*)$ o bien $LM(f^* - \bar{f}) \in Mon(\bar{f})$, si sucede lo primero tenemos una contradicción, pues f^* es una forma normal con respecto a G y tendría que suceder que $LM(g_i)$ no divide a t para todo $t \in Mon(f^*)$ y algún $g_i \in G$, análogamente si $LM(f^* - \bar{f}) \in Mon(\bar{f})$. Por lo tanto $f^* = \bar{f}$.

Para probar (b) sea $f, g \in K[x_1, ..., x_n]$ y $c \in K$, definimos $h := NF_G(f + cg) - NF_G(f) - cNF_G(g)$, luego h es congruente con $f + cg - f - cg = 0$ módulo $\langle G \rangle$, entonces $h \in \langle G \rangle$, como $G \subseteq I$ tenemos que $\langle G \rangle \subseteq I$, así en particular $h \in I$.

Si $h \neq 0$ entonces $LM(h)$ debería ser divisible por $LM(g)$ para algún $g \in G$, contradiciendo el hecho de que h es forma normal con respecto a G, así $h = 0$ y la linealidad se satisface.

Veamos ahora que $\ker(NF_G) = I$. Sea $f \in \ker(NF_G)$ entonces $f = f - NF_G(f) \in I$, pues $f - NF_G(f) \in \langle G \rangle \subseteq I$.

Inversamente si $f \in I$ entonces $f^* := NF_G(f) \in I$, pues $f - f^* \in \langle G \rangle \subseteq I$ y $f \in I$. Si $f^* \neq 0$ debería existir $g \in G$ tal que $LM(g)$ divida a $LM(f^*)$ contradiciendo la definición de forma normal, y por lo tanto $f^* = 0$ y $f \in \ker(NF_G)$.

□

Corolario 1.1. *Sea G una G-base de un ideal $I \subseteq K[x_1, ..., x_n]$, entonces $I = \langle G \rangle_{K[x_1,...,x_n]}$.*

Demostración. Por definición de G-base $G \subseteq I$, entonces $\langle G \rangle \subseteq I$. Inversamente, sea $f \in I$ entonces $NF_G(f) = 0$ por el teorema anterior, por (1.1) existen $h_1, ..., h_r$ tal que $f = f - 0 = \sum_{i=1}^{r} h_i g_i$ con $g_i \in G$ lo que implica que $f \in \langle G \rangle$.

□

Observación 1.1. *(G-bases sobre anillos). Parte de lo que hemos hecho hasta ahora se translada al caso en el que K es un anillo arbitrario, y no un campo. Primero la definición (1.1) no involucra las propiedades de K. Entonces el Lema (1.1) se satisface para anillos de polinomios sobre anillos arbitrarios. Podemos tambien utilizar las definiciones (1.2) y (1.3) en la situación más general.*

Definición 1.4. *Para $f, g \in K[x_1, ..., x_n]$ dos polinomios no cero, sea t el m.c.m de $LM(f)$ y $LM(g)$, definimos el s-polinomio de f y g como:*

$$spol(f, g) := \frac{t}{LT(f)} f - \frac{t}{LT(g)} g.$$

Ejemplo 1.5. *Si $f = x_1^2 + x_2^2$ y $g = x_1 x_2$, con el orden lexicográfico inverso $(x_1 > x_2)$, tenemos que $LM(f) = x_1^2$, $LM(g) = x_1 x_2$, $t = x_1^2 x_2$, $LT(f) = x_1^2$ y $LT(g) = x_1 x_2$, entonces,*

$$spol(f, g) = \frac{x_1^2 x_2}{x_1^2}(x_1^2 + x_2^2) - \frac{x_1^2 x_2}{x_1 x_2}(x_1 x_2) = x_2^3.$$

El siguiente teorema es la base del algoritmo de Buchberger, además nos garantiza que este algoritmo se realiza en un número finito de pasos.

Teorema 1.2. *(Criterio de Buchberger) Sea $G \subseteq K[x_1, ..., x_n]$ un conjunto finito de polinomios no cero. Entonces las siguientes afirmaciones son equivalentes:*

(a) G es una G-base del ideal $I \subseteq K[x_1, ..., x_n]$ generado por G.

(b) Para todo polinomio $g, h \in G$, 0 es una forma normal del $spol(g, h)$ con respecto a G.

Para la demostración del Criterio de Buchberger necesitamos el siguiente lema.

Lema 1.2. *Supongamos que $f_1, ..., f_s \in K[x_1, ..., x_n]$ tienen el mismo monomio líder $LM(f_i) = X \neq 0$, si $f = \sum c_i f_i$ con $c_i \in K$ satisface $LM(f) < X$, entonces hay $d_{ij} \in K$ tales que*

$$f = \sum_{i<j} d_{ij} spol(f_i, f_j).$$

Demostración. Sea $LT(f_i) = a_iX$, de modo que $LT(f_i) = a_iX$, $LT(f_j) = a_jX$ y $m.c.m(LM(f_i), LM(f_j)) = X$ y entonces $spol(f_i, f_j) = \frac{1}{a_i}f_i - \frac{1}{a_j}f_j$. Luego el coeficiente de X en f, $\sum_{i=1}^{s} c_i a_i$ es cero pues $LM(f) < X$, así tenemos

$$\begin{aligned} f &= c_1f_1 + ... + c_sf_s \\ &= c_1a_1(\frac{1}{a_1}f_1) + ... + c_sa_s(\frac{1}{a_s}f_s) \\ &= c_1a_1(\frac{1}{a_1}f_1 - \frac{1}{a_2}f_2) + (c_1a_1 + c_2a_2)(\frac{1}{a_2}f_2 - \frac{1}{a_3}f_3) + \\ &+ ... + (c_1a_1 + ... + c_{s-1}a_{s-1})(\frac{1}{a_{s-1}}f_{s-1} - \frac{1}{a_s}f_s) + (c_1a_1 + ... + c_sa_s)(\frac{1}{a_s}f_s) \\ &= c_1a_1spol(f_1, f_2) + ... + (c_1a_1 + ... + c_sa_s)spol(f_{s-1}, f_s). \end{aligned}$$

□

Demostración Teorema 1.2. (a)⇒(b) Todo s-polinomio de elementos de G es un elemento de $I = \langle G \rangle$, entonces, si G es una G-base el s-polinomio tiene forma normal 0 pues $\ker(NF_G) = I$.

(b)⇒ (a) Sea $f \in I$, debemos probar que $LM(g_i)$ divide a $LM(f)$ para algún i. Escribimos

$$f = h_1g_1 + ... + h_sg_s.$$

Sea $X = \text{máx}\{LM(h_ig_i) | i = 1, ..., s\}$, podemos suponer que X es mínimo entre todas las expresiones de f como elemento de I con respecto a un orden monomial.

Si $X = LM(f)$ hemos terminado pues existe $j \in \{1, ..., s\}$ tal que $X = LM(h_jg_j) = LM(h_j)LM(g_j) = LM(f)$, así $LM(g_i)$ divide a $LM(f)$.

Supongamos que no, sea $S_X = \{i \in \{1, ..., s\} \, | LM(h_ig_i) = X\}$. Para $i \in S_X$ escribimos $h_i = c_iX_i + h_i'$ donde $c_i \in K$ y $LT(h_i') < X$. Definamos $g = \sum_{i \in S_X} c_iX_ig_i$, entonces, $LM(X_ig_i) = X \ \forall i \in S_X$ y $LM(g) < X$, por el Lema (1.2), existen $d_{ij} \in K$ tales que

$$g = \sum_{i,j \in S_X i \neq j} d_{ij}spol(X_ig_i, X_jg_j).$$

Necesitamos probar que estos s-polinomios tienen forma normal cero respecto a G y así tendremos una expresión de f con monomio líder más pequeño que X, contradiciendo la minimalidad de X. Tenemos que

$$\begin{aligned} spol(X_i g_i, X_j g_j) &= \frac{X}{LT(X_i g_i)} X_i g_i - \frac{X}{LT(X_j g_j)} X_j g_j \\ &= \frac{X}{LT(g_i)} g_i - \frac{X}{LT(g_j)} g_j \\ &= \frac{X}{m.c.m(LM(g_i), LM(g_j))} spol(g_i, g_j). \end{aligned}$$

Se sigue que $NF_G(spol(X_i g_i, X_j g_j)) = 0$, entonces $spol(X_i g_i, X_j g_j) \in I$, así podemos escribirlo como $spol(X_i g_i, X_j g_j) = \sum_l h_{ijl} g_l$ satisfaciendo que $\max\{LM(h_{ijl})\} = LM(spol(X_i g_i, X_j g_j)) < X$. Entonces concluimos que

$$\begin{aligned} f &= \sum_{i \in S_X} h_i g_i + \sum_{i \notin S_X} h_i g_i \\ &= \sum_{i \in S_X} (c_i X_i + h_i') g_i + \sum_{i \notin S_X} h_i g_i \\ &= \sum_{i \in S_X} c_i X_i g_i + \sum_{i \in S_X} h_i' g_i + \sum_{i \notin S_X} h_i g_i \\ &= \sum_{i,j \in S_X i<j} d_{ij} spol(X_i g_i, X_j g_j) + \sum_{i \in S_X} h_i' g_i + \sum_{i \notin S_X} h_i g_i \\ &= \sum_{i,j \in S_X i<j} d_{ij} \sum_l h_{ijl} g_l + \sum_{i \in S_X} h_i' g_i + \sum_{i \notin S_X} h_i g_i \\ &= \sum_l (\sum_{i,j \in S_X i<j} d_{ij} h_{ijl}) g_l + \sum_{i \in S_X} h_i' g_i + \sum_{i \notin S_X} h_i g_i. \end{aligned}$$

Ahora cada expresión $p_l g_l$ en el lado derecho tiene monomio líder menor que X, entonces tenemos una expresión de $f = \sum q_i g_i$ con $max\{LM(q_i g_i)\} < X$ contradiciendo la minimalidad de X.

□

Daremos ahora un algoritmo el cual nos permite calcular G-bases de un ideal

Algoritmo 1.2. *(Algoritmo de Buchberger)*
Entrada: Un conjunto finito de polinomios S.

Salida: Una G-base G (con respecto a la elección del orden monomial $\leq$) del ideal $I \subseteq K[x_1, ..., x_n]$ generado por S.

Pasos

1) Definir $G := S \setminus 0$.

2) Para todo $g, h \in G$ realizar los pasos (3)-(4).

3) Calcular el s-polinomio $s := spol(g, h)$ y una forma normal s^* de s con respecto a G.

4) Si $s^* \neq 0$, defina $G := G \cup s^*$ y realice el paso (2).

5) Si $s^* = 0$ termina el cálculo y regresar G.

Cada vez que un nuevo polinomio s^* es agregado en G en el Algoritmo 1.2, el ideal $L(G)$ aumenta estrictamente. Por lo tanto la terminación del algoritmo está garantizada por el Teorema de la base de Hilbert ([13], Corolario 2.13). Como todo s^* es un elemento de I la exactitud del algoritmo se sigue del criterio de Buchberger.

Ejecución en SINGULAR [8] (Base de Gröbner)

```
> ring r=0, (x(1),x(2),    ), orden;
> poly f1=    ;
> poly f2=    ;
  ⋮
> poly fn=    ;
> ideal i=f1,f2,..., fn;
> ideal h=groebner(i);
> h;
```

Ejemplo 1.6. *Sean $\mathbb{C}[x, y]$ el anillo de polinomios en dos variables, $f_1 = x^2 - 1$, $f_2 = y^2 - 1$, $f_3 = x^2 - y$ e $I = \langle f_1, f_2, f_3 \rangle$, queremos encontrar una G-base del ideal I con respecto al orden lexicográfico.*

Veamos si $G = \{f_1 = x^2 - 1, f_2 = y^2 - 1, f_3 = x^2 - y\}$ *ya es G-base.*

Obtenemos los s-polinomios de los elementos de G por parejas, y calculamos su forma normal con respecto a G, si ésta es cero, entonces significa que el s-polinomio es una combinación de los elementos de G.

Tenemos que $spol(x^2 - 1, y^2 - 1) = x^2 - y^2$ *y ahora calculamos su forma normal respecto a G.*

$$
\begin{array}{cccc|c|c|c|l}
 & & & & f_1 & f_3 & f_2 & \\
 & & & & 1 & 0 & -1 & \\
\hline
x^2-1 & x^2-y & y^2-1 & x^2-y & & & & \text{residuo} \\
 & & & -x^2+1 & & & & \\
\cline{4-4}
 & & & -y^2+1 & & & & \\
 & & & y^2-1 & & & & \\
\cline{4-4}
 & & & 0 & & & & 0
\end{array}
$$

Tenemos que la forma normal de $spol(x^2 - 1, y^2 - 1) = x^2 - y^2$ *con respecto a G es* 0 *y* $spol(x^2 - 1, y^2 - 1) = x^2 - y^2 = 1f_1 - 1f_2 + 0f_3$*, entonces* $spol(x^2 - 1, y^2 - 1)$ *no se añade al conjunto G.*

Ahora $spol(x^2 - 1, x^2 - y) = y - 1$ *y calculamos su forma normal con respecto a G.*

$$
\begin{array}{cccc|c|c|c|l}
 & & & & f_1 & f_3 & f_2 & \\
 & & & & 0 & 0 & 0 & \\
\hline
x^2-1 & x^2-y & y^2-1 & y-1 & & & & \text{residuo} \\
 & & & & & & & y-1
\end{array}
$$

Notamos que $LM(spol(x^2 - 1, x^2 - y))$ *no puede dividirse por ningún* $LM(f_i)$ $i = 1, 2, 3$*, y entonces tenemos que la forma normal de* $spol(x^2 - 1, x^2 - y)$ *es* $y - 1$*, en este caso como la forma normal fue distinta de cero se agrega al conjunto G, entonces tenemos que:*

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

Ahora el $spol(y^2 - 1, x^2 - y) = -x^2 + y^3$*, calculamos su forma normal con respecto al nuevo conjunto G.*

$$
\begin{array}{cccc|cccc}
 & & & & f_1 & f_3 & f_2 & f_4 \\
 & & & & -1 & 0 & y & 1 \\
\hline
x^2-1 & x^2-y & y^2-1 & y-1 & -x^2+y^3 & & & \\
 & & & & x^2-1 & & & \\
\hline
 & & & & y^3-1 & & & \\
 & & & & -y^3+y & & & \\
\hline
 & & & & y-1 & & & \\
 & & & & -y+1 & & & \\
\hline
 & & & & 0 & & &
\end{array}
$$

Tenemos entonces que la forma normal de $spol(y^2-1, x^2-y) = -x^2+y^3$ *es cero y* $spol(y^2-1, x^2-y) = -1f_1 + yf_2 + 0f_3 + 1f_4$.

Tenemos ahora que $spol(x^2-1, y-1) = -x^2-y,\ y$

$$
\begin{array}{cccc|cccc}
 & & & & f_1 & f_3 & f_2 & f_4 \\
 & & & & 1 & 0 & 0 & -1 \\
\hline
x^2-1 & x^2-y & y^2-1 & y-1 & x^2-y & & & \\
 & & & & -x^2+1 & & & \\
\hline
 & & & & -y+1 & & & \\
 & & & & y-1 & & & \\
\hline
 & & & & 0 & & &
\end{array}
$$

Entonces la forma normal de $spol(x^2-1, y-1)$ *es cero y* $spol(x^2-1, y-1) = 1f_1 + 0f_2 + 0f_3 - 1f_4$.

El $spol(y^2-1, y-1) = y-1,\ y$

$$
\begin{array}{cccc|cccc}
 & & & & f_1 & f_3 & f_2 & f_4 \\
 & & & & 0 & 0 & 0 & 1 \\
\hline
x^2-1 & x^2-y & y^2-1 & y-1 & y-1 & & & \\
 & & & & -y+1 & & & \\
\hline
 & & & & 0 & & &
\end{array}
$$

La forma normal de $spol(y^2-1, y-1)$ *es cero y* $spol(y^2-1, y-1) = 0f_1 + 0f_2 + 0f_3 + 1f_4$.

Por último tenemos que $spol(x^2 - y, y - 1) = x^2 - y^2$, y

$$
\begin{array}{cccc|cccc}
 & & & & f_1 & f_3 & f_2 & f_4 \\
 & & & & 1 & 0 & -1 & 0 \\
\hline
x^2-1 & x^2-y & y^2-1 & y-1 & x^2-y^2 & & & \\
 & & & & -x^2+1 & & & \\
\hline
 & & & & -y^2+1 & & & \\
 & & & & y^2-1 & & & \\
\hline
 & & & & 0 & & &
\end{array}
$$

Así la forma normal de $spol(x^2 - y, y - 1)$ *es cero y* $spol(x^2 - y, y - 1) = 1f_1 - 1f_2 + 0f_3 + 0f_4$.

Entonces podemos concluir que $G = \{f_1, f_2, f_3, f_4\}$ *es una G-base para* I. *(En este ejemplo realizamos la división en un solo paso).*

1.2. Aplicaciones

Una G-base permite deducir fácilmente muchas propiedades importantes de un ideal y de la variedad algebraica asociada, tales como la dimensión y el número de ceros de la variedad (cuando es finito). El cálculo de la G-base es una de las principales herramientas prácticas para la resolución de sistemas de ecuaciones polinomiales. En nuestro caso, estamos interesados en utilizar las G-bases para calcular el kernel de una aplicación entre K- álgebras afines. En [1] se describen ésta y otras aplicaciones de las G-bases.

1.2.1. Eliminación de ideales

Definición 1.5. *Sea* $S = \{x_{i1}, ..., x_{ik}\}$ *un conjunto de indeterminadas.*

a) Para un ideal $I \subseteq K[x_1, ..., x_n]$ *el ideal de* S*-eliminación de* I *es definido como la intersección:*

$$I_S := K[x_{i1}, ..., x_{ik}] \cap I$$

(donde $I_\emptyset$ *es el conjunto de constantes que yacen en* I*).*

b) Un orden monomial $\leq$ en $K[x_{i1}, ..., x_{ik}]$ se llama orden de S- eliminación si:

$$t \leq x_j \text{ para todos los monomios } t \in K[x_{i1}, ..., x_{ik}] \text{ y para todo } x_j \in \bar{S}, \text{ donde } \bar{S} = \{x_1, ..., x_n\} \setminus S.$$

Ejemplo 1.7. *1) Sea $\leq$ un orden monomial arbitrario en $K[x_1, ..., x_n]$ y sea S el conjunto de indeterminadas con complemento*

$$\{x_1, ..., x_n\} \setminus S = \{x_{j1}, ..., x_{jr}\}.$$

Definimos un nuevo orden monomial como sigue:

$$t = x_1^{e_1} \cdot ... \cdot x_n^{e_n} \preccurlyeq t' = x_1^{e'_1} \cdot ... \cdot x_n^{e'_n} \quad si \quad e_{j1} + ... + e_{jr} < e'_{j1} + ... + e'_{jr} \quad o \text{ si } e_{j1} + ... + e_{jr} = e'_{j1} + ... + e'_{jr} \quad y \quad t \leq t'.$$

Entonces $\preccurlyeq$ es un orden de S-eliminación.

2) El orden bloque es un orden de $\{x_{k+1}, ..., x_n\}$-eliminación.

3) El orden lexicográfico es un orden de $\{x_{k+1}, ..., x_n\}$- eliminación para todo k.

Teorema 1.3. *Sea $I \subseteq K[x_1, ..., x_n]$ un ideal y $S = \{x_{i1}, ..., x_{ik}\}$ un conjunto de indeterminadas. Sea G una G-base de I con respecto a un orden de S-eliminación. Entonces*

$$G_S := K[x_{i1}, ..., x_{ik}] \cap G$$

es una G-base para el ideal de S- eliminación de I con respecto al orden monomial restringido.

Demostración. Claramente $G_S \subseteq I_S$.

Para probar que $L(I_S) = L(G_S)$ sea $f \in I_S$ no cero, tenemos que $LM(f) \in L(I)$, pues $f \in I$, entonces existe $g \in G$ tal que $LM(g)$ divide a $LM(f)$ ($LM(f) = hLM(g)$ con $h \in K[x_1, ..., x_n]$), luego como $f \in K[x_{i1}, ..., x_{ik}]$ tenemos que $LM(f) = x_{i1}^{e_1} \cdot ... \cdot x_{ik}^{e_k}$ con posiblemente algunos $e_i = 0$ y se sigue que $LM(g) \in K[x_{i1}, ..., x_{ik}]$.

Pero entonces todo $t \in Mon(g)$ es un elemento de $K[x_{i1}, ..., x_{ik}]$ ya que de lo contrario la definición de orden de S-eliminación implicaría que $LM(g) \leq t$ lo cual es una contradicción. Así g es un polinomio que depende sólo de $x_{i1}, ..., x_{ik}$ y entonces $g \in G_S$.

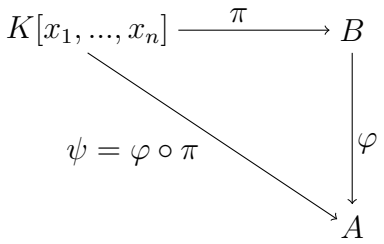
□

Ejecución en SINGULAR [8] (Eliminación)

> ring r=0, (x,y, ,z(1..n)), orden;
> poly f1= ;
> poly f2= ;
⋮
> poly fn= ;
> ideal i=f1-z1,f2-z2,..., fn-zn;
> ideal j=eliminate(i,xy);
> j;
Usando la G-base
> ideal g=groebner(i);
> g;
> ideal k=eliminate(g,xy);
> k;

Una aplicación de los ideales de eliminación es el cálculo de los *kernel* de homomorfismos entre K-álgebras afines [13].

Sean $A := K[y_1, ..., y_m]/I$ y $B := K[x_1, ..., x_n]/J$ dos K-álgebras afines con I, J ideales en los anillos de polinomios, sea $\varphi : B \to A$ un homomorfismo de K-álgebras. Componiendo φ con la aplicación canónica $\pi : K[x_1, ..., x_n] \to B$ obtenemos un homomorfismo $\psi : K[x_1, ..., x_n] \to A$, como lo muestra el siguiente diagrama:



Observamos que $\ker(\varphi) = \ker(\psi)/J$, así que es suficiente calcular $\ker(\psi)$.

Podemos suponer que la primera álgebra es un anillo de polinomios, entonces, la siguiente proposición nos dice que en esta situación el *kernel* puede ser calculado como un ideal de eliminación.

Antes de dar una caracterización del kernel del homomorfismo φ, veamos un lema técnico [1].

Lema 1.3. *Sean $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n$ elementos de un anillo conmutativo R sobre un campo K, entonces el elemento $a_1a_2 \cdot ... \cdot a_n - b_1b_2 \cdot ... \cdot b_n$ está en el ideal $\langle a_1 - b_1, ..., a_n - b_n\rangle$.*

Demostración. Haremos la prueba por inducción en n.
Para $n = 1$ es claro.

Para $n = 2$ tenemos $a_1a_2 - b_1b_2 = a_1(a_2 - b_2) + b_2(a_1 - b_1)$.

Supongamos que el lema es válido para $n > 2$, esto es

$$a_1a_2 \cdot ... \cdot a_n - b_1 \cdot ... \cdot b_n \in \langle a_1 - b_1, ..., a_n - b_n\rangle$$

y mostremos que se satisface para $n + 1$.

De nuestra hipótesis de inducción se sigue que

$$a_{n+1}(a_1a_2 \cdot ... \cdot a_n - b_1 \cdot ... \cdot b_n) \in \langle a_1 - b_1, ..., a_n - b_n\rangle$$

y

$$b_{n+1}(a_1a_2 \cdot ... \cdot a_n - b_1 \cdot ...b_n) \in \langle a_1 - b_1, ..., a_n - b_n\rangle$$

de donde,

$$a_1 \cdot ... \cdot a_n a_{n+1} - b_1 \cdot ... \cdot b_n a_{n+1} + a_1 \cdot ... \cdot a_n b_{n+1} - b_1 \cdot ... \cdot b_n b_{n+1} \in \langle a_1 - b_1, ..., a_n - b_n\rangle$$

entonces,

$$\begin{aligned} a_1 \cdot ... \cdot a_{n+1} - b_1 \cdot ... \cdot b_{n+1} &= \alpha_1(a_1 - b_1) + ... + \alpha_n(a_n - b_n) \\ &+ b_1 \cdot ... \cdot b_n a_{n+1} - a_1 \cdot ... \cdot a_n b_{n+1} \end{aligned}$$

con $\alpha_i \in K$. Ahora observemos que

$$b_1 \cdot ... \cdot b_n a_{n+1} - a_1 \cdot ... \cdot a_n b_{n+1} = a_{n+1}(b_1 \cdot ... \cdot b_n - a_1 \cdot ... \cdot a_n) - a_1 \cdot ... \cdot a_n(a_{n+1} - b_{n+1})$$

por lo tanto

$$a_1 \cdot ... \cdot a_{n+1} - b_1 \cdot ... \cdot b_{n+1} \in \langle a_1 - b_1, ..., a_{n+1} - b_{n+1} \rangle.$$

□

Proposición 1.1. *Sea* $\varphi : K[x_1, ..., x_n] \longrightarrow A = K[y_1, ..., y_m]/I$ *un homomorfismo de* K*-álgebras dado por* $\varphi(x_i) = g_i + I$ *con* $g_i \in K[y_1, ..., y_m]$*, considere el ideal* $J := \langle I \cup \{g_1 - x_1, ..., g_n - x_n\} \rangle_{K[x_1,...,x_n,y_1,...,y_m]}$*, entonces*

$$\ker(\varphi) = K[x_1, ..., x_n] \cap J.$$

Demostración. Se sigue de la definición de J y del Lema (1.3) que para todo $f \in K[x_1, ..., x_n]$ tenemos

$$f(g_1, ..., g_n) - f \in J. \tag{1.2}$$

Supongamos que $f \in \ker(\varphi)$, entonces, $f(g_1, ..., g_n) \in I$, pues $\varphi(x_i) = g_i + I$, de (1.2) obtenemos que $f \in J$.

Si $f \in K[x_1, ..., x_n] \cap J$, entonces de (1.2) obtenemos que $f(g_1, ..., g_n) \in J$, entonces podemos escribir $f(g_1, ..., g_n) = \sum_{i=1}^{r} h_i f_i + \sum p_j(g_i - x_i)$ con $h_i, p_i \in K[x_1, ..., x_n, y_1, ..., y_m]$ y $f_i \in I$. Ahora consideremos la aplicación $\chi : K[x_1, ..., x_n, y_1, ..., y_m] \longrightarrow K[y_1, ..., y_m]$ dada como $\chi(x_i) = g_i$ y $\chi(y_j) = y_j$, entonces aplicando χ a nuestra última expresión tenemos que $f(g_1, ..., g_n) = \sum_{i=1}^{r} \chi(h_i) f_i$, y así tenemos que $f(g_1, ..., g_n) \in I$ y se sigue que $f \in \ker(\varphi)$.

□

Esta proposición nos muestra que $\ker \varphi$ es siempre un ideal de eliminación, luego podemos definir el ideal de relaciones o módulo de Sizigias como $\ker(\varphi) = Syzy(g_1, ..., g_n)$, esta definición nos permite saber si los polinomios son algebraicamente independientes o no.

Ejemplo 1.8. *(SINGULAR [8]) Determinar si los polinomios* $f_1 = x + y$*,* $f_2 = s + t$*,* $f_3 = xy - st$*,* $f_4 = xt + ys$ *son algebraicamente independientes.*

Usaremos el algoritmo para calcular ideales de eliminación, si éste ideal sólo tiene el elemento 0 *esto significará que los polinomios son algebraicamente independientes, de lo contrario implicaría que existe una relación no*

cero la cual ellos satisfacen.

> *ring* $r = 0$, $(x, y, s, t, z\,(1..4))$, *lp;*
> *poly* $f1 = x + y$;
> *poly* $f2 = s + t$;
> *poly* $f3 = x * y - s * t$;
> *poly* $f4 = x * t + y * s$;
> *ideal* $i = f1 - z(1), f2 - z(2), f3 - z(3), f4 - z(4)$;
> *ideal j=eliminate(i,xyst);*
> *j;*
$j[1] = 0$
> *ideal g=groebner(i);*
> *ideal k=eliminate(g,xyst);*
> *k;*
$k[1] = 0$

Veamos ahora que si añadimos el polinomio $f_5 = xy$*, éstos ya no son algebraicamente independientes pues en este caso existe una relación distinta de cero que ellos satisfacen.*

> *ring* $r = 0$, $(x, y, s, t, z(1..5))$, *lp;*
> *poly* $f1 = x + y$;
> *poly* $f2 = s + t$;
> *poly* $f3 = x * y - s * t$;
> *poly* $f4 = x * t + y * s$;
> *poly* $f5 = x * y$;
> *ideal* $i = f1 - z(1), f2 - z(2), f3 - z(3), f4 - z(4), f5 - z(5)$;
> *ideal j=eliminate*$(i, xyst)$*;*
> *j;*
$j[1] = z(1)^2 * z(3) - z(1)^2 * z(5) + z(1) * z(2) * z(4) - z(2)^2 * z(5) - 4 * z(3) * z(5) - z(4)^2 + 4 * z(5)^2$
> *ideal g=groebner*(i)*;*
> *ideal k=eliminate*$(g, xyst)$*;*
> *k;*
$k[1] = z(1)^2 * z(3) - z(1)^2 * z(5) + z(1) * z(2) * z(4) - z(2)^2 * z(5) - 4 * z(3) * z(5) - z(4)^2 + 4 * z(5)^2$

Si juntamos el Teorema (1.3) y la Proposición (1.1), obtenemos el siguiente algoritmo para obtener una G-base del $\ker(\varphi)$.

1) Formamos el ideal $J \subseteq K[x_1, ..., x_n, y_1, ..., y_m]$ y elegimos un orden monomial de $\{x_1, ..., x_n\}$-eliminación $\leq$ en $K[x_1, ..., x_n, y_1, ...y_m]$.

2) Calcular una G-base de J con respecto a $\leq$ y definir $G_x := K[x_1, ..., x_n] \cap G$.

3) Entonces G_x es una G-base de $\ker(\varphi)$.

Una pregunta natural que surge en este momento es qué pasa con la otra parte de la G-base, la siguiente proposición responde a esta pregunta.

Proposición 1.2. *(Kemper, [13], Proposición 9.18). Sea $\varphi : K[x_1, ..., x_n] \to A := K[y_1, ..., y_m]/I$ un homomorfismo de K-álgebras dado por $\varphi(x_i) = g_i + I$ con $g_i \in K[y_1, ..., y_m]$.*

Sea $R := im(\varphi) \subseteq A$ consideremos el homomorfismo de R-álgebras, $\psi : R[y_1, ..., y_m] \longrightarrow A$ dado por $\psi(y_i) = y_i + I$.

También consideremos el homomorfismo $\phi : K[x_1, ..., x_n, y_1, ...y_m] \longrightarrow R[y_1, ..., y_m]$ determinado por la aplicación φ coeficiente a coeficiente.

Sea $\preceq$ un orden de $\{x_1, ..., x_n\}$ -eliminación en $K[x_1, ..., x_n, y_1, ..., y_m]$ y sea G una G-base con respecto a $\preceq$ del ideal

$$J := \langle I \cup \{g_1 - x_1, ..., g_n - x_n\}\rangle_{K[x_1,...,x_n,y_1,...,y_m]}$$

Si $G_x := K[x_1, .., x_n] \cap G$ y $G_y := G \setminus G_x$ (el resto de G), entonces:

a) G_x es una G-base de $\ker(\varphi)$ *respecto a la restricción de $\preceq$ a $K[x_1, ..., x_n]$.*

b) $\ker(\psi) = \langle \phi(G_y)\rangle_{R[y_1,...,y_m]}$.

c) Si $\leq$ es el orden bloque de los órdenes monomiales $\leq_x$ en $K[x_1, ..., x_n]$ y $\leq_y$ en $K[y_1, ..., y_m]$ con $\leq_y$ dominando, entonces $\phi(G_y)$ es una G-base de $\ker(\psi)$ *con respecto a $\leq_y$. (Ver observación (1.1) para G-bases sobre un anillo).*

Capítulo 2

Representaciones

En este capítulo V denotará un espacio vectorial de dimensión n, $K = \mathbb{C}$, el campo de números complejos, $GL(V)$ es el grupo de automorfismos de V sobre sí mismo. Daremos una introducción a la teoría de representaciones de grupos finitos; podemos encontrar una descripción más detallada en [11] y [21].

$GL(V)$ como grupo es identificable con el grupo de matrices invertibles cuadradas de orden n, es decir, $GL(V) \simeq GL(n, K)$ donde $n = dim(V)$.

Supongamos ahora que G es un grupo finito con elemento neutro 1.

Definición 2.1. *Una representación lineal de G en V es un homomorfismo $\rho : G \to GL(V)$ definido como $s \mapsto \rho(s) = \rho_s$ tal que $\rho(st) = \rho(s)\rho(t)$ $\forall s, t \in G$. El grado de la representación es definido como la dimensión de V como espacio vectorial sobre K.*

Se sigue además que $\rho(1) = 1$ y $\rho(s^{-1}) = \rho(s)^{-1}$.

Si $\rho : G \to GL(V)$ es una representación lineal de G en V decimos que V es un espacio de representación para G o simplemente representación.

Definición 2.2. *Sean ρ y ρ' dos representaciones del mismo grupo G en espacios vectoriales V y V' respectivamente. Decimos que son equivalentes (isomorfas o similares) si existe un isomorfismo lineal $\tau : V \to V'$ el cual transforma ρ en ρ', esto es que satisface la identidad:*

$$\tau\rho(s) = \rho'(s)\tau \ \forall s \in G$$

y lo denotamos por $\rho \sim \rho'$.

Nota: Cuando ρ y ρ' están dadas en forma matricial R_s y R'_s respectivamente, la definición anterior es equivalente a que existe una matriz invertible T tal que $TR_s = R'_s T \ \forall s \in G$.

Ejemplo 2.1 (Representaciones equivalentes)**.** *Sean* $G = C_2 = \langle a : a^2 = 1 \rangle$ *y* $A = \begin{pmatrix} -5 & 12 \\ -2 & 5 \end{pmatrix}$.

Tenemos que $A^2 = I_2$*, definimos entonces una representación*

$$\begin{gathered} \rho : G \to GL(2, \mathbb{C}) \\ 1 \mapsto I_2 \\ a \mapsto A. \end{gathered}$$

Sea $T = \begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}$*, es tal que* $T^{-1}AT = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Entonces podemos definir otra representación para G *sobre* $\mathbb{C}$

$$\begin{gathered} \rho' : G \to GL(2, \mathbb{C}) \\ 1 \mapsto I_2 \\ a \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{gathered}$$

Se sigue que ρ *y* ρ' *son equivalentes.*

2.1. Subrepresentaciones

Definición 2.3. *Sea* $\rho : G \to GL(V)$ *una representación lineal y sea* $W < V$ *(un subespacio de* V*). Supóngase que* W *es estable bajo la acción de* G*, es decir,* $\forall x \in W$ *tenemos que* $\rho_s(x) \in W \ \forall s \in G$*. La restricción* $\rho^W : W \to W$ *es un isomorfismo de* W *sobre sí mismo y tenemos* $\rho^W_{st} = \rho^W_s \rho^W_t$*, así* ρ^W *es una representación lineal de* G *en* W*.* W *se dice que es una subrepresentación de* V*.*

Definición 2.4. *Sean* V *un espacio vectorial y* $W, W' < V$*.* V *es suma directa de* W *y* W' *si cada* $x \in V$ *se expresa como* $x = w + w'$ *con* $w \in W$ *y* $w' \in W'$*,* $W \cap W' = 0$ *y* $dim(V) = dim(W) + dim(W')$*, decimos además que* W' *es un complemento de* W *en* V*.*

Teorema 2.1. *Sea $\rho : G \to GL(V)$ una representación lineal de G en V y sea W un subespacio vectorial de V estable bajo la acción de G, entonces existe un complemento W^0 de W en V que también es G-estable.*

Demostración. Sea W^0 un complemento arbitrario de W en V, y sea p la proyección correspondiente de V sobre W, consideremos la siguiente aplicación:

$$p^0 = \frac{1}{g} \sum_{t \in G} \rho_t p \rho_t^{-1} \text{ (g es el orden de G)}$$

Luego se sigue que $\rho_t^{-1} x \in W$ para $x \in W$, de donde $p\rho_t^{-1} x = \rho_t^{-1} x$, $\rho_t p \rho_t^{-1} x = x$ y $p^0 x = x$. Así p^0 es una proyección de V sobre W, correspondiente a algún complemento W^0 de W. Tenemos además $\rho_s p^0 = p^0 \rho_s \; \forall s \in G$.

Si $x \in W^0$ y $s \in G$ tenemos $p^0 x = 0$, por lo tanto $p^0 \rho_s x = \rho_s p^0 x = 0$ esto es $\rho_s x \in W^0$, esto prueba que W^0 es estable bajo G.

□

Definición 2.5. *Sea $\rho : G \to GL(V)$ una representación lineal de G. Decimos que es irreducible o simple si V no es 0 y si no hay subespacios de V estables bajo la acción de G (excepto por supuesto 0 y V). Por el Teorema (2.1), esta segunda condición es equivalente a decir que V no es la suma directa de dos subrepresentaciones (excepto para la descomposición trivial $V = 0 \oplus V$).*

Observación 2.1. *Una representación de grado 1 es evidentemente irreducible.*

Teorema 2.2. *Toda representación es una suma directa de representaciones irreducibles.*

Demostración. Sea V una representación lineal de G. Procedemos por inducción en $dim(V)$.

Si $dim(V) = 0$ tenemos que 0 es la suma directa de la familia vacía de representaciones irreducibles.

Supongamos que $dim(V) \geq 1$. Si V es irreducible no hay nada que probar, en otro caso, por el Teorema 2.1, V puede ser descompuesto en una suma directa $V' \oplus V''$, con $dim(V') < dim(V)$ y $dim(V'') < dim(V)$. Por la hipótesis

de inducción V' y V'' son suma directa de representaciones irreducibles y entonces V también lo es.

□

2.2. Lema de Schur

Proposición 2.1. *(Lema de Schur) Sean $\rho^1 : G \to GL(V_1)$ y $\rho^2 : G \to GL(V_2)$ dos representaciones irreducibles de G y sea f una aplicación lineal de V_1 a V_2,*

$$f : V_1 \to V_2 \text{ tal que}$$

$$\rho_s^2 \circ f = f \circ \rho_s^1 \ \forall s \in G$$

entonces:

1) Si ρ^1 y ρ^2 son no isomorfas (no equivalentes) tenemos $f = 0$.

2) Si $V_1 = V_2$ y $\rho^1 = \rho^2$, f es una homotecia (es decir, un múltiplo escalar de la identidad).

Demostración. 1) Si $f = 0$ no hay nada que probar. Supongamos que $f \neq 0$ y sea $W_1 = ker(f)$, entonces para $x \in W_1$ tenemos $f\rho_s^1 x = \rho_s^2 f x = 0$, de donde $\rho_s^1 x \in W_1$ y W_1 es estable bajo G, como V_1 es irreducible, W_1 es igual a V_1 o 0, el primer caso es imposible pues implica que $f = 0$, entonces $W_1 = 0$.

Ahora sea $W_2 = im(f)$ para $x \in V_1$, $f\rho_s^1 x \in W_2$, entonces $\rho_s^2 f x \in W_2$, así W_2 es estable bajo G, como V_2 es irreducible tenemos que W_2 es igual a cero o V_2, el primer caso implica que $f = 0$, lo cual es una contradicción, entonces $W_2 = V_2$.

Se sigue que f es un isomorfismo lo cual contradice la hipótesis, así que $f = 0$.

2) Supongamos ahora que $V_1 = V_2$ y $\rho^1 = \rho^2$, y sea λ un eigenvalor de f (existe al menos uno, pues el campo de los escalares es el campo de los números complejos).

Sea $f' = f - \lambda$, como λ es un eigenvalor de f entonces existe $v \in V_1$, con $v \neq 0$, tal que $f(v) = \lambda v$, luego $f'(v) = f(v) - \lambda v = 0$; se sigue que $v \in ker(f')$ y por lo tanto $ker(f') \neq 0$.

Por otro lado $\rho_s^2 \circ f' = f' \circ \rho_s^1$, para $s \in G$, así $\forall\ x \in ker(f')$ se tiene que $\rho_s^1(x) \in ker(f')\ \forall\ s \in G$, esto es, $ker(f')$ es estable bajo la acción de G, luego como V_1 es irreducible tenemos $ker(f') = V_1$, y entonces $f'(v) = 0\ \forall\ v \in V_1$, por lo tanto f es una homotecia. □

Corolario 2.1. *Sea G un grupo abeliano, entonces cualquier representación irreducible de G es de grado 1.*

Demostración. Sea $\rho : G \to GL(V)$ una representación irreducible, sean $s \in G$ y ρ_s, entonces para todo $t \in G$,

$$\rho_s \rho_t = \rho_{st} = \rho_{ts} = \rho_t \rho_s.$$

Por el Lema de Schur (Proposición (2.1)) tenemos que $\rho_s = \lambda_s I$, $\lambda_s \in \mathbb{C}$.

Sean $v \in V$ $v \neq 0$, $k \neq 0 \in \mathbb{C}$, entonces $\rho_s(kv) = \lambda_s kv \in \langle v \rangle$, luego $\langle v \rangle$ es un subespacio $G-$estable de V, como s es arbitrario y V es irreducible, se sigue que $\langle v \rangle = V$, entonces $dim(V) = 1$. □

Proposición 2.2. *Sea G el grupo cíclico de orden m, $G = \langle a : a^m = 1 \rangle$, supongamos que $A \in GL(n, \mathbb{C})$ y definimos*

$$\rho : G \to GL(n, \mathbb{C})$$

$$a^r \to A^r\ 0 \leq r \leq m - 1.$$

Entonces ρ es una representación de G sobre $\mathbb{C}$ si y sólo si $A^m = I$.

Demostración. ($\Rightarrow$) $I_n = \rho 1 = \rho a^m = (\rho a)^m = (A)^m = A^m$.

($\Leftarrow$) Si $A^m = I$, entonces $\rho a^i = A^i$, por lo tanto, $\rho(a^i a^j) = \rho(a^{i+j}) = A^{i+j} = A^i A^j = (\rho a^i)(\rho a^j)$. Se sigue que ρ es una representación. □

Corolario 2.2. *Sea G un grupo cíclico de orden m y $A \in GL(1, \mathbb{C})$, entonces $\rho : G \to GL(1, \mathbb{C})$ dada por $a^r \mapsto (\lambda)^r$ $(0 \leq r \leq m-1)$ es una representación si y sólo si $\lambda^m = 1$, es decir, λ es una raíz m-ésima de la unidad.*

Corolario 2.3. *El número de representaciones no equivalentes de grado 1 de $G = \langle a : a^m = 1 \rangle$ es igual a m.*

2.3. Grupos abelianos finitos

Todo grupo abeliano finito es isomorfo a un producto directo de grupos cíclicos, $G = C_{n_1} \times ... \times C_{n_r}$, donde n_i es el orden de C_{n_i}.

Sea G un grupo abeliano finito, entonces $|G| = n_1 \cdot ... \cdot n_r$, para $1 \leq i \leq r$ sea c_i un generador de C_{n_i}. Escribimos $g_i = (1, ..., c_i, .., 1)$ con c_i en la i-ésima posición, entonces $G = \langle g_1, ..., g_r \rangle$ con $g_i^{n_i} = 1$ y $g_i g_j = g_j g_i \ \forall i, j$.

Sea ahora una representación irreducible de G sobre $\mathbb{C}$

$$\rho : G \to GL(V) \simeq \mathbb{C}^\star.$$

Entonces para $1 \leq i \leq r$ existe $\lambda_i \in \mathbb{C}$ tal que $\rho(g_i) = \lambda_i$, como g_i tiene orden n_i tenemos que $\lambda_i^{n_i} = 1$, es decir, λ_i es una raíz n_i-ésima de la unidad.

Para $g \in G$, $g = (g_1^{i_1}, ..., g_r^{i_r})$ para algunos $i_1, ..., i_r \in \mathbb{Z}$, entonces

$$\rho(g) = \rho((g_1^{i_1}, ..., g_r^{i_r})) = \lambda_1^{i_1} \cdot ... \cdot \lambda_r^{i_r}$$

denotamos ρ por $\rho_{\lambda_1^{i_1}, ..., \lambda_r^{i_r}}$.

Tenemos ahora que dada una raíz n_i-ésima de la unidad λ_i, $1 \leq i \leq r$, la función $(g_1^{i_1}, ..., g_r^{i_r}) \mapsto \lambda_1^{i_1} \cdot ... \cdot \lambda r^{i_r}$ es una representación de G. Hay $n_1 \cdot ... \cdot n_r = |G|$ representaciones de este tipo y ninguna de ellas es equivalente.

Teorema 2.3. *Sea G un grupo abeliano finito $C_{n_1} \times ... \times C_{n_r}$, las representaciones $\rho_{\lambda_1^{i_1}, ..., \lambda_r^{i_r}}$ construidas anteriormente son irreducibles, tienen grado 1 y hay $|G|$ representaciones.*

Capítulo 3

Teoría de Invariantes

En este capítulo definiremos el anillo de invariantes y daremos algunas propiedades de éste. Supondremos a partir de aquí que K es un campo algebraicamente cerrado, a menos de que se indique lo contrario, y G es un grupo finito.

3.1. Anillo de invariantes

Necesitamos introducir algunas nociones básicas de grupos algebraicos.

Definición 3.1. *Un grupo algebraico lineal es una variedad afín G la cual tiene una estructura de grupo tal que la multiplicación $\mu : G \times G \to G$ y la inversión $\nu : G \to G$ son morfismos de álgebras afines.*

Decimos que un grupo algebraico lineal G actúa regularmente en una variedad afín X si una acción de G en X es dada por un morfismo $G \times X \to X$.

Definición 3.2. *Una representación de G es un K-espacio vectorial dimensionalmente finito V junto con un homomorfismo de grupos $G \to GL(V)$. Una representación V se llama racional si G actúa regularmente en V (considerado como un espacio afín).*

Supongamos que G es un grupo algebraico lineal actuando regularmente en una variedad afín X. Si $f \in K[X]$ y $\sigma \in G$, entonces definimos $\sigma \cdot f \in K[X]$ como:

$$(\sigma \cdot f)(x) := f(\sigma \cdot x) \text{ para todo } x \in X.$$

Esto define una acción izquierda en el anillo de coordenadas de X.

Definición 3.3. *Si $f \in K[X]$ y $\sigma \cdot f = f$ para todo $\sigma \in G$, entonces f se llama invariante.*

En general estamos interesados en el conjunto

$$K[X]^G = \{f \in K[X] : \sigma \cdot f = f \text{ para todo } \sigma \in G\}$$

de todos los G-invariantes. El conjunto $K[X]^G$ es un subanillo de $K[X]$ y es llamado el anillo de invariantes de G. Posteriormente nos enfocaremos en el caso donde $X = V$ es una representación de G, entonces $K[V]$ es isomorfo al anillo de polinomios $K[x_1, ..., x_n]$, donde n es la dimensión de V como K-espacio vectorial. El anillo polinomial $K[V] = \bigoplus_{d=0}^{\infty} K[V]_d$ es graduado con respecto al grado total. La G-acción en $K[V]$ preserva el grado y $K[V]^G \subseteq K[V]$ hereda la graduación.

Un problema fundamental en la teoría de invariantes es encontrar generadores del anillo de invariantes $K[V]^G$. Entonces una pregunta natural es: ¿Se puede siempre encontrar un número finito de generadores $f_1, ..., f_r$ tal que $K[V]^G = K[f_1, .., f_r]$?.

Con el fin de responder esta pregunta, veamos la siguiente proposición, la cual demuestra que el anillo de invariantes es finitamente generado.

Proposición 3.1. *(Noether [19]). Sea R un álgebra finitamente generada sobre un anillo Noetheriano conmutativo K, y sea G un grupo finito actuando en R fijando K por automorfismo. Entonces R^G es finitamente generado como una K-álgebra.*

Demostración. Sean $x_1, ..., x_n$ generadores para R. El polinomio

$$\prod_{\sigma \in G}(T - \sigma \cdot x_i) = T^m + a_{i,1}T^{m-1} + ... + a_{i,m-1}T + a_{i,m} \in R^G[T]$$

proporciona una ecuación entera para x_i sobre R^G. Por lo tanto R es finitamente generado como un módulo sobre la subálgebra $A := K[a_{1,1}, ..., a_{n,m}]$ generada por los coeficientes de ésta ecuación. Como A es Noetheriana, R es Noetheriano como un A-módulo, y por lo tanto lo mismo es cierto para el submódulo R^G. Así que R^G es un módulo finitamente generado sobre A. □

Note que la demostración anterior no es constructiva, así que en los siguientes capítulos veremos resultados que nos ayudarán a encontrar un conjunto de generadores.

3.2. Existencia de un sistema homogéneo de parámetros

Definición 3.4. *Supóngase que $R = \bigoplus_{d=0}^{\infty} R_d$ es un álgebra graduada sobre un campo K tal que $R_0 = K$. Un conjunto $f_1, ..., f_n \in R$ de elementos homogéneos se llama un sistema homogéneo de parámetros si:*

a) $f_1, ..., f_n$ son algebraicamente independientes y

b) R es un módulo finitamente generado sobre $K[f_1, ..., f_n]$.

Supongamos ahora que G es un grupo finito y V una representación de dimensión finita de G. Si $f_1, ..., f_n \in K[V]^G$ es un sistema homogéneo de parámetros, llamamos a los f_i *invariantes primarios* de $K[V]^G$. El anillo de invariantes $K[V]^G$ es un $K[f_1, ..., f_n]$-módulo finitamente generado, digamos

$$K[V]^G = Fg_1 + ... + Fg_s$$

donde F es el anillo de polinomios $K[f_1, ..., f_n]$ y $g_1, ..., g_n \in K[V]^G$ homogéneos. Los invariantes $g_1, ..., g_s$ son llamados invariantes secundarios.

Veamos que los sistemas homogéneos de parámetros existen para anillos graduados, para esto necesitamos el Lema de Normalización de Noether (ver Mumford [17], pag. 2, Eisenbud [7],Teorema 13.3).

Lema 3.1. *Supóngase que $R = \bigoplus_{d=0}^{\infty} R_d$ es un anillo graduado con $R_0 = K$. Supóngase que $f_1, ..., f_r \in R_d$ para algún d, y R es un F-módulo finito donde $F = K[f_1, ..., f_r]$. Entonces existen $g_1, ..., g_r \in R_d$ los cuales son combinaciones lineales de $f_1, ..., f_r$, tal que $g_1, ..., g_r$ es un sistema homogéneo de parámetros.*

Los anillos graduados finitamente generados tienen sistemas homogéneos de parámetros como lo muestra el siguiente corolario. En particular los anillos de invariantes de grupos finitos tienen sistemas homogéneos de parámetros.

Corolario 3.1. *Si $R = \bigoplus_{d=0}^{\infty} R_d$ es un álgebra graduada finitamente generada con $R_0 = K$, entonces R tiene un sistema homogéneo de parámetros.*

Demostración. Tomemos generadores homogéneos $f_1, ..., f_r \in R$, sea $d_i = deg(f_i)$ para todo i. Sea d el mínimo común múltiplo de $d_1, ..., d_r$, y definamos $f_i' = f_i^{\frac{d}{d_i}}$. Entonces $f_1', ..., f_r'$ son homogéneos de grado d. Ahora aplicamos el Lema anterior y obtenemos el resultado. □

En particular tenemos que existen sistemas homogéneos de parámetros para los anillos de invariantes.

3.3. La propiedad Cohen-Macaulay

Definición 3.5. *Sea R un anillo Noetheriano y M un R-módulo finitamente generado.*

a) Una sucesión $f_1, ..., f_k \in R$ se llama M-regular si $M/(f_1, ..., f_k)M \neq 0$ y multiplicación por f_i induce una aplicación inyectiva en $M/(f_1, ..., f_{i-1})M$ para $i = 1, ..., k$.

b) Sea $I \subseteq R$ un ideal con $IM \neq M$. Entonces la profundidad de I en M es la longitud máxima k de una M-sucesión regular $f_1, ..., f_k$ con $f_i \in I$, denotado por $depth(I, M) = k$.

c) Si R es un anillo local graduado con ideal maximal (homogéneo) m, escribimos $depth(M)$ por $depth(m, M)$.

d) Si R es un anillo local Noetheriano con ideal maximal m, entonces M se llama Cohen-Macaulay si $depth(M) = dim(M)$, donde $dim(M)$ es la dimensión de Krull de $R/Ann(M)$. Si R no es necesariamente local, entonces M es llamado Cohen-Macaulay si para todo ideal maximal $m \in Supp(M)$, M_m es Cohen-Macaulay como un R_m-módulo.

e) R es llamado Cohen-Macaulay si es Cohen-Macaulay como un módulo sobre si mismo.

Lema 3.2. *El anillo de polinomios en n variables es Cohen-Macaulay.*

Una demostración de este lema la encontramos en Kemper ([6], Lema 2.5.2).

La siguiente proposición nos da una caracterización importante de la propiedad Cohen- Macaulay para álgebras graduadas.

Proposición 3.2. *Sea R un álgebra graduada Noetheriana sobre un campo K con $K = R_0$ la parte homogénea de grado 0. Entonces las siguientes condiciones son equivalentes:*

a) R es Cohen-Macaulay.

b) Todo sistema homogéneo de parámetros es R-regular.

c) Si $f_1, ..., f_n$ es un sistema homogéneo de parámetros, entonces R es un módulo libre sobre $K[f_1, ..., f_n]$.

d) Existe un sistema homogéneo de parámetros $f_1, ..., f_n$ tal que R es un módulo libre sobre $K[f_1, ..., f_n]$.

Una prueba de la Proposición 3.2 puede ser encontrada en Benson ([2], Teorema 4.3.5).

3.4. Serie de Hilbert de anillos de invariantes

Una importante herramienta para el cálculo de invariantes es la serie de Hilbert. La serie de Hilbert de un anillo contiene mucha información acerca del anillo en sí mismo, por ejemplo, la dimensión.

En muchos casos conocemos la serie de Hilbert $H(K[V]^G, t)$ antes de conocer los generadores de $K[V]^G$. Para grupos finitos, $H(K[V]^G, t)$ puede ser calculada usando la fórmula de Molien (ver Teorema (6.1)).

Definición 3.6. *Para un espacio vectorial graduado $V = \bigoplus_{d=k}^{\infty} V_d$ con V_d dimensionalmente finito para todo d, definimos la Serie de Hilbert de V como la serie formal de Laurent*

$$H(V, t) := \sum_{d=k}^{\infty} dim(V_d) t^d.$$

Ejemplo 3.1. *Calculemos la serie de Hilbert de* $K[x_1, ..., x_n]$. *Hay* $\binom{n+d-1}{n-1}$ *monomios de grado* d, *por lo tanto la serie de Hilbert es:*

$$H(K[x_1, ..., x_n], t) = \sum_{d=0}^{\infty} \binom{n+d-1}{n-1} t^d.$$

Ésta es exactamente la expansión formal en serie de potencias de $(1-t)^{-n}$.

Observación 3.1. *Si* V *y* W *son dos espacios vectoriales graduados, entonces el producto tensorial* $V \otimes W$ *también tiene una graduación natural:*

$$(V \otimes W)_d = \bigoplus_{d_1+d_2=d} V_{d_1} \otimes W_{d_2}.$$

Es obvio de esta fórmula que $H(V \otimes W, t) = H(V, t)H(W, t)$. *Supongamos que* $R = K[x_1, ..., x_n]$ *y* x_i *tiene grado* $d_i > 0$. *Entonces tenemos* $R = K[x_1] \otimes K[x_2] \otimes ... \otimes K[x_n]$ *como álgebras graduadas y* $H(K[x_i], t) = (1 - t^{d_i})^{-1}$. *Se sigue que,*

$$H(R, t) = \textstyle\prod_{i=1}^{n} (1 - t^{d_i})^{-1}.$$

Si $H(K[V]^G, t)$ es conocida, la podemos comparar término a término con $H(K[f_1, ..., f_r], t)$ para algún conjunto de invariantes homogéneos $f_1, ..., f_r$. Si son iguales tenemos que como K-espacios vectoriales las componente homogeneas son iguales respectivamente. Así tenemos un criterio para determinar un conjunto de invariantes homogéneos $f_1, ..., f_r$ que generan a $K[V]^G$:

$$K[V]^G = K[f_1, ..., f_r] \Leftrightarrow H(K[V]^G, t) = H(K[f_1, ..., f_r], t).$$

Investigaremos la estructura de $H(K[V]^G, t)$ cuando G es un grupo finito y V es una representación dimensionalmente finita de G. Primero que todo, sabemos que existe un sistema homogéneo de parámetros $f_1, ..., f_r$ (invariantes primarios) de $K[V]^G$. Entonces $K[V]^G$ es un F-módulo libre, donde $F \cong K[f_1, ..., f_r]$, ya que $K[V]^G$ es Cohen-Macaulay. Entonces existe una descomposición

$$K[V]^G = Fg_1 \oplus Fg_2 \oplus .... \oplus Fg_s$$

Con $g_1, ..., g_s \in K[V]^G$ homogéneos. La descomposición anterior es llamada una **descomposición de Hironaka**.

Por ejemplo la serie de Hilbert de $K[f_1, ..., f_r]$ es igual a $\prod_{i=1}^{r} (1 - t^{d_i})^{-1}$, donde $d_i := deg(f_i)$ para todo i.

Lema 3.3. *La serie de Hilbert del anillo de invariantes $K[V]^G$ esta dada por*

$$H(K[V]^G, t) = \frac{\sum_{j=1}^{s} t^{e_j}}{\prod_{i=1}^{r}(1 - t^{d_i})} \tag{3.1}$$

donde $d_i = deg(f_i)$ y $e_j = deg(g_j)$.

Demostración. con la notación de arriba, tenemos lo siguiente, $Fg_j \simeq F \otimes_K g_j K$, además $H(g_j K, t) = t^{e_j}$, con $e_j = deg(g_j)$, así se sigue que:

$$H(Fg_j, t) = \frac{t^{e_j}}{\prod_{i=1}^{n}(1 - t^{d_i})}$$

De la descomposición de Hironaka tenemos:

$$H(K[V]^G, t) = \frac{\sum_{j=1}^{s} t^{e_j}}{\prod_{i=1}^{r}(1 - t^{d_i})}$$

donde $e_j = deg(g_j)$ para todo j. □

Capítulo 4

Relaciones de un Anillo de Invariantes 2 Dimensional de un Grupo Cíclico

Sean G un grupo cíclico de orden n y K un campo el cual contiene una raíz n-ésima primitiva de la unidad. Consideramos el anillo de invariantes $K[V]^G$ de una representación dos dimensional de G. En este capítulo describiremos un método para calcular las relaciones de los generadores de $K[V]^G$ dado por John C. Harris y David L. Whelau en [9]. Demostraremos además que el conjunto de relaciones forman una G-base. Para más detalles vea [4].

4.1. Relación entre resolución de A/J y resolución de A/I

Sea $A = K[y_1, ..., y_s]$ y $deg(x_i) = 1$, fijemos un orden monomial en $Mon(A)$.

Sea $J = \left\langle z_{0_1}, ..., z_{0_{\beta_1}} \right\rangle$ con $z_{0_j} \in A$, $j = 1, ..., \beta_1$ e $I = \left\langle y_{0_1}, ..., y_{0_{\beta_1}} \right\rangle$ con y_{0_j} el término líder de z_{0_j}.

Supongamos que $\left\{z_{0_j}\right\}_{1 \leq j \leq \beta_1}$ es una G-base para J.

Sea M un A-módulo libre con base $\{x_j | j = 1, ..., \beta\}$. La K-base de M es

el conjunto de monomios de M $\{\alpha x_j | \alpha \in Mon(A)\}$.

Definimos una $Mon(A)$-graduación llamada tipo en los elementos no cero de M, y un orden en los monomios de M.

Sea $p \in A$ mónico, definimos $type(p) = LT(p)$, y para $p \neq 0$ definnimos $type(p) = type(kp)$ donde $k \in K$ y kp es mónico. Para cada $j = 1, ..., \beta$ elijamos un elemento $type(x_j) \in Mon(A)$, y para $x = \sum p_j x_j$ sea $type(x) = max_j \{type(p_j)type(x_j)\}$.

Ahora definimos el orden en los monomios de M. Decimos $\alpha x_j > \alpha' x_{j'}$ si una de las siguientes condiciones se satisface:

I) $type(\alpha x_j) > type(\alpha' x_{j'})$.

II) $type(\alpha x_j) = type(\alpha' x_{j'})$ y $type(x_j) > type(x_{j'})$.

III) $type(\alpha x_j) = type(\alpha' x_{j'})$ y $type(x_j) = type(x_{j'})$ y $j > j'$.

El monomio maximal de un elemento $x = \sum p_j x_j$ en M se llama el término líder de x denotado por $lt(x)$.

La suma de todos los monomios de x que tienen tipo α se llama el término-tipo α denotado por x_α. Si $x_\alpha = 0$ tenemos que no hay monomios en x que tienen tipo α.

El término-tipo de x que tiene el mismo tipo que el término líder se llama el término-tipo líder y se denota por $ltt(x)$.

Escribimos M^α para el K-espacio de monomios en M de tipo $\leq \alpha$ y $M^{(\alpha)}$ para el K-espacio de monomios de tipo exactamente α.

Sea $0 \to M_s \to ... \to M_1 \to M_0 = A$ con $e_s : M_s \to M_{s-1}$, una sucesión de A-módulos libres y A-aplicaciones lineales, y para cada i, sea $\{x_{ij} | j = 1, ..., \beta_i\}$ una A-base para M_i. Decimos que $(M_\star, e_\star)$ tiene una tipo-graduación si cada M_i tiene una $Mon(A)$-graduación como arriba. Por convención siempre tomamos $x_{01} = 1$ y $type(x_{01}) = 1$.

Definición 4.1. *Una sucesión tipo graduada $(M_\star, e_\star)$ se dice que es filtrada por tipo si $e_i(M_i^\alpha) \subseteq M_{i-1}^\alpha$, y que preserva tipo si $e_i(M_i^{(\alpha)}) \subseteq M_{i-1}^{(\alpha)}$.*

Definimos la sucesión asociada a una sucesión tipo graduada $(M_\star, e_\star)$ como $0 \to M_s \to ... \to M_0 = A$, con $d_s : M_s \to M_{s-1}$ aplicaciones A-lineales, cada d_i manda x_{ij} al término-tipo(x_{ij}) de $e_i(x_{ij})$.

Claramente la sucesión asociada $(M_\star, d_\star)$ preserva el tipo, pues $d_i(x_{ij}) = e_i(x_i j)_{x_{ij}}$.

Lema 4.1. *Sea $(M_\star, e_\star)$ una sucesión filtrada por tipo y $(M_\star, d_\star)$ su sucesión asociada. Si $x \in M_i$ tiene tipo α, entonces,*

$$d_i(x_\alpha) = (e_i(x_\alpha))_\alpha = (e_i(x))_\alpha.$$

En particular si $e_i(x) = 0$ entonces $d_i(x_\alpha) = 0$

Demostración. Sea $x = \sum_{j\in S} p_j x_{ij}$ y sea $T = \{j \in S | type(p_j)type(x_{ij}) = \alpha\}$ y $U = \{j \in S | type(p_j)type(e_i(x_{ij})) = \alpha\}$ entonces $x_\alpha = \sum_{j\in T} lt(p_j)x_{ij}$ y

I) $d_i(x_\alpha) = \sum_{j\in T} lt(p_j)d_i(x_{ij}) = \sum_{j\in U} lt(p_j)ltt(e_i(x_{ij}))$.

II) $(e_i(x_\alpha))_\alpha = (\sum_{j\in T} lt(p_j)e_i(x_{ij}))_\alpha = \sum_{j\in U} lt(p_j)ltt(e_i(x_{ij}))$.

III) $(e_i(x))_\alpha = (\sum_{j\in S} p_j e_i(x_{ij}))_\alpha = \sum_{j\in U} lt(p_j)ltt(e_i(x_{ij}))$.

□

Sea $(M_\star, e_\star)$ una sucesión de A-módulos y A-aplicaciones lineales como arriba tal que $e_i(x_{ij}) \neq 0$ para cada i, j. Podemos definir una tipo-graduación inducida en $M_\star$ tal que $(M_\star, e_\star)$ es filtrada por tipo.

Recordemos que $x_{01} = 1$, $type(x_{01}) = 1$, para $p \neq 0 \in M_0 = A$ definimos $type(p)$ como antes, $type(p) = lt(p)$.

Una vez definido el tipo en M_{i-1} defina $type(x_{ij}) = type(e_i(x_{ij}))$ y extendemos al resto de M_i de forma natural.

Definición 4.2. *Llamamos resolución libre sobre un módulo M a una sucesión $(M_\star, e_\star)$ tal que cada M_i es un módulo libre finitamente generado y*

$$... \to M_k \to M_{k-1} \to ... \to M_1 \to M_0 \to 0$$

es exacta.

Si además los M_i son graduados, entonces se llama resolución libre graduada de M.

Definición 4.3. *Sean M un R-módulo graduado finitamente generado y $(M_\star, e_\star)$ una resolución libre graduada sobre M. Decimos que $(M_\star, e_\star)$ es minimal si, dada una base $\{m_1, ..., m_s\}$ de M_{i+1} formada por elementos homogéneos, las imágenes $e_{i+1}(m_1), ..., e_{i+1}(e_s) \in M_i$, forman un sistema de generadores minimal de $ker(e_i) \subset M_i$, para cada $i \geq 0$.*

Criterio de minimalidad 4.1([4], Criterio 1.2). Una resolución $(M_\star, e_\star)$ es minimal si y sólo si las entradas no cero de cada e_i tienen grado positivo.

Proposición 4.1. *Sea $(M_\star, e_\star)$ una resolución libre de A/J con $e_0 : M_0 = A \to A/J$ la proyección y con la graduación inducida definida anteriormente. Si cada subcomplejo $(M^\alpha_\star, e_\star)$ es exacto, entonces el complejo asociado $(M_\star, d_\star)$ es una resolución de A/I. Además si $(M_\star, d_\star)$ es una resolución mínima de A/J entonces $(M_\star, d_\star)$ es una resolución mínima de A/I.*

Demostración. Tenemos que $\to M_s \xrightarrow{e_s} ... \to M_1 \xrightarrow{e_1} M_0 = A \xrightarrow{e_0} A/J \to 0$ es exacta, entonces $im(e_{i+1}) = ker(e_i)$, en particular $im(e_1) = ker(e_0) = J$ y $\left\{z_{0_j}\right\}$ es una G-base, es decir $L(J) = I$. Tenemos que $d_1(x_{1j})$ es el término tipo (x_{1j}) de $e_1(x_{1j})$ y $e_1(x_{1j}) \in J$, entonces, se sigue que $im(d_1) = I$. Lo que implica que $M_1 \xrightarrow{d_1} M_0 \xrightarrow{d_0} A/I$ es exacta.

Para $i \geq 1$ tenemos $d_i d_{i+1} = 0$ pues

$$d_i d_{i+1}(x_{i+1,j}) = d_i((e_{i+1}(x_{i+1,j}))_{x_{i+1}}) = (e_i(e_{i+1}(x_{i+1,j})))_{x_{i+1,j}} = 0.$$

Supongamos que $d_i(x) = 0$ para algún $x \neq 0 \in M_i$, podemos suponer que x es de tipo homogéneo digamos con tipo α. Tenemos que $d_i(x) = (e_i(x))_\alpha = 0$, es decir, la suma de los términos de x que tienen tipo α es cero (no hay monomios en x que tienen tipo α), entonces $\beta = type(e_i(x)) < \alpha$, pues $(M_\star, e_\star)$ es filtrada por tipo.

Como $e_{i-1}e_i(x) = 0$ tenemos que $e_i(x) \in ker(e_{i-1})$, y por hipótesis $(M^\beta_\star, e_\star)$ es exacta, así que $e_i(x) \in im(e_i)$ por lo que existe $y \in M_i$ con $type(y) \leq \beta$ y $e_i(y) = e_i(x)$, así que $e_i(x - y) = 0$ y entonces $x - y \in ker(e_i) = im(e_{i+1})$, así que existe $z \in M^\alpha_{i+1}$ tal que $x - y = e_{i+1}(z)$. Del

Lema (4.1) tenemos que $d_{i+1}(z_\alpha) = (e_{i+1}(z))_\alpha = (x-y)_\alpha = x$, por lo tanto $ker(d_i) \subset im(d_{i+1})$, y entonces $(M_\star, d_\star)$ es exacta.

Por el criterio de minimalidad (4.1), $(M_\star, e_\star)$ minimal implica que las matrices de los e_i relativas a las bases $\{x_{ij}\}$ y $\{x_{i-1,j}\}$ no involucran constantes no cero. Pero las matrices de d_i provienen de las matrices de los e_i, entonces no tienen entradas constantes no cero.

□

Nuestro siguiente resultado construye una resolución de A/J a partir de una de A/I. Como I es un ideal monomial podemos elegir una resolución minimal $(M_\star, d_\star)$ de A/I que preserva tipo (construyendo los d_i inductivamente escribiendo los elementos de $ker(d_{i-1})$ como sumas de términos homogéneos).

Proposición 4.2. *Sea $(M_\star, d_\star)$ una resolución libre de A/I que preserva tipo con $M_1 = \oplus_{j=1}^{\beta_1} A x_{1j}$, $M_0 = A$ y $d_1(x_{1,j}) = y_{0,j}$ entonces hay una resolución $(M_\star, e_\star)$ de A/J comenzando con $e_1(x_{1,j}) = z_{0j}$ la cual satisface las siguientes propiedades:*

(I) $(M_\star, e_\star)$ es filtrada por tipo.

(II) $(M_\star, d_\star)$ es la resolución asociada a $(M_\star, e_\star)$,

(III) Para cada $\alpha \in Mon(A)$, el subcomplejo $(M_\star^\alpha, e_\star)$ es exacto.

Demostración. Podemos construir inductivamente los e_i's. Primero chequemos que $M_1 \to M_0 \to A/J$ satisface $(I) - (III)$.

(I)

$$\begin{aligned} type(e_1(\sum p_j x_{1j})) &= type(\sum p_j z_{0j}) \leq max\,\{type(p_j z_{0j})\} \\ &= max\,\{type(p_j y_{0j})\} \leq max\,\{type(p_j x_{1j})\} \\ &= type(\sum p_j x_{1j}) = \alpha \end{aligned}$$

Por lo tanto $e_1(M_1^\alpha) \subseteq M_0^\alpha$.

(II) Se sigue de la hipótesis.

(III) Debemos mostrar que $M_1^\alpha \to M_0^\alpha \to A/J$ es exacta.

Para $\alpha = 1$ tenemos que $M_1^\alpha \to M_0^\alpha \to A/J$ es exacta, pues $e_1(x_{1j}) = z_{0j}$ y $ker(e_0) = J$.

Sea $\alpha \in Mon(A)$ y supongamos que hemos probado que $M_1^\beta \to M_0^\beta \to A/J$ es exacta en M_0^β para $\beta < \alpha$.

Supongamos que $p \in M_0^\alpha$ tiene tipo α y $e_0(p) = 0$, entonces $p \in J$ y $lt(p) = k\alpha$ para algún $k \in K$, como $\{z_{0j}\}$ es G-base, entonces $k\alpha = qy_{0j_0}$ para algún $q \in Mon(A)$ y algún j_0.

Sea $x = qx_{1j_0} \in M_1$, entonces $e_1(x) = qz_{0j_0}$ tiene término líder $k\alpha$, luego $e_0(p - e_1(x)) = 0$ y $type(p - e_1(x)) < \alpha$, por hipótesis de inducción existe $y \in M_1^\beta$ con $e_1(y) = p - e_1(x)$, entonces $e_1(x + y) = p$ con $type(x + y) = \alpha = type(p)$, se sigue que $M_1^\alpha \to M_0^\alpha \to A/J$ es exacta.

Ahora, supongamos que e_{i-1} esta bien definida y tiene las propiedades (I)-(III).

Entonces

$$e_{i-1}(d_i(x_{ij})) = d_{i-1}(d_i(x_{ij})) + y = y$$

con $type(y) \leq type(x_{ij})$ y $e_{i-2}(y) = 0$. Como e_{i-1} satisface (III), esto es, $M_{i-1}^\alpha \to M_{i-1}^\alpha \to ... \to M_1^\alpha \to M_0^\alpha \to A/J \to 0$ es exacta, tenemos $ker(e_{i-2}) = im(e_{i-1})$, de donde $y \in ker(e_{i-2}) = im(e_{i-1})$, así que existe $z \in M_{i-1}$ con $e_{i-1}(z) = y$ y $type(z) \leq type(y)$.

Sea $e_i(x_{ij}) = d_i(x_{ij}) - z$, extendemos e_i linealmente a M_i y notemos que $e_{i-1}e_i = 0$, e_i satisface (I) y (II), veamos que satisface (III).

Supongamos que hemos probado que $M_i^\beta \to M_{i-1}^\beta \to M_{i-2}^\beta$ es exacta en M_{i-1}^β para todo $\beta < \alpha$ y supongamos que $e_{i-1}(x) = 0$ para algún $x \in M_{i-1}^\alpha$ que tiene tipo α. Por el Lema 4.1, $d_{i-1}(x_\alpha) = 0$, así que $x_\alpha \in ker(d_{i-1}) = im(d_i)$, luego existe $y \in M_i^\alpha$ con $d_i(y) = x_\alpha$, sea $z = e_i(y) - x$, entonces $e_{i-1}(z) = e_{i-1}(e_i(y)) - e_{i-1}(x) = 0$ y $type(z) < \alpha$. Por inducción existe $w \in M_i$ con $e_i(w) = z$ y $type(w) < \alpha$, se sigue que $e_i(y - w) = x$ con $y - w \in M_i^\alpha$, por lo tanto $x \in im(e_1)$, es decir, $ker(e_{i-1}) \subset im(e_i)$. □

4.2. Resoluciones mínimas y números graduados de Betti

Sea $n \geq 3$, G un grupo cíclico de orden n, K un campo que contiene una raíz n-ésima primitiva de la unidad ξ, σ denota un generador de G.

En el capítulo 2 vimos que hay n representaciones no equivalentes de G sobre K de dimensión 1, las denotamos por W_b, $b = 1, ..., n$, donde G actúa en W_b vía $\sigma w = \xi^b w \ \forall w \in W_b$.

Ahora sea $R = K[x_1, ..., x_m]$, con cada $deg(x_i)$ un entero positivo, I un ideal homogéneo en R, la resolución mínima graduada libre de R/I tiene la forma

$$0 \to M_k \to M_{k-1} \to ... \to M_1 \to M_0 = R \to R/I \to 0$$

donde $k \leq m$, $M_i = \bigoplus_j R(-j)^{\beta_{ij}(R/I)}$ y $R(-j)$ son R-módulos libres. El número $\beta_{ij}(R/I)$ es el $(i,j)-$ésimo número de Betti graduado de R/I, que es igual al número de generadores de grado j en el i-ésimo módulo de sizigias (el cual definiremos en el capítulo 6) de R/I. Los números de Betti $\beta_{ij}(I)$ de un ideal I se definen como sigue, si

$$... \to M_1 \to M_0 \to R/I \to 0$$

es una resolución mímima graduada libre de R/I, entonces

$$... \to M_1 \to M_0 \to I \to 0$$

es una resolución mínima graduada libre de I.

Por convención $\beta_{-1,0}(I) = 1$, $\beta_{-1,j}(I) = 0 \ \forall j > 0$ y $\beta_{i-1,j}(I) = \beta_{ij}(R/I)$.

De la Proposición (4.1) y la Proposición (4.2) tenemos el siguiente lema:

Lema 4.2. *Sea I un ideal homogéneo en R generado mínimamente por una G-base $\{z_1, ..., z_k\}$ donde para cada i el grado del término líder de z_i es menor o igual que el grado de los otros términos de z_i. Si (M_*, d_*) es una resolución mínima graduada libre de $R/LT(I)$ que es pura, entonces existen diferenciales $\bar{d}_*$ tal que $(M_*, \bar{d}_*)$ es una resolución mínima graduada libre de R/I. En particular los números de Betti graduados para R/I y $R/LT(I)$ son los mismos.*

Ahora estamos particularmente interesados en los números graduados de Betti para anillos de invariantes $K[W]^G$ los cuales son definidos como sigue: si $\{b_1, ..., b_m\}$ es un conjunto minimal de generadores para $K[W]^G$, entonces hay un homomorfismo de R sobre $K[W]^G$, donde $deg(x_i) = deg(b_i)$ y bajo el homomorfismo x_i va a b_i. El kernel de este homomorfismo, digamos I, es homogéneo y se llama el ideal de relaciones para $K[W]^G$. Luego como $K[W]^G \simeq R/I$ como anillos graduados, definimos $\beta_{i,j}(K[W]^G) = \beta_{i,j}(R/I)$.

4.2.1. Caso dos dimensional

Considerar $W = W_b \oplus W_c$ una representación 2 dimensional de G con $0 < b, c < n$, tenemos $K[W] = K[x, y]$ donde $\sigma x = \xi^b x$ y $\sigma y = \xi^c y$.

Tenemos que $K[W]^G$ tiene un conjunto de generadores minimal que consiste de monomios

$$x^k y^l \text{ tal que } bk + cl \equiv 0 \mod n.$$

Observemos que estos monomios son invariantes

$$\begin{aligned} \sigma(x^k y^l) &= (\sigma x)^k (\sigma y)^l = (\xi^b x)^k (\xi^c y)^l \\ &= \xi^{bk} x^k \xi^{cl} y^l = \xi^{bk+cl} x^k y^l = x^k y^l. \end{aligned}$$

Consideremos el siguiente conjunto minimal de generadores como K-álgebra para $K[W]^G$

$$\left\{ u_i = x^{a_i} y^{b_i} : i = 1, ..., m \right\}$$

entonces como K-álgebra $K[W]^G = K[u_1, ..., u_m]$.

Podemos suponer que $a_1 > a_2 > ... > a_{m-1} > a_m$, notemos que si u_i divide a u_j, entonces $u_j = qu_i$ para algún $q \in K[x, y]$, y además $u_j = \sigma u_j = \sigma(qu_i) = \sigma q \sigma u_i = \sigma q u_i$, entonces $qu_i = \sigma q u_i$ lo cual implica que $q = \sigma q$, luego de la minimalidad de m se sigue que u_i no divide a u_j para $i \neq j$, lo que implica que $b_1 < b_2 < ... < b_{m-1} < b_m$, en efecto, pues si suponemos que $b_1 = b_2 = \beta$, entonces $u_1 = x^{a_1} y^\beta$ y $u_2 = x^{a_2} y^\beta$ lo cual implica que u_2 divide a u_1 lo que es imposible. La misma contradicción se tiene si suponemos que $b_2 > b_1$ y $a_1 > a_2$, y esto para cada par de índices.

Considerar ahora la resolución exacta corta

$$0 \to J \to S = K[U_1, ..., U_m] \xrightarrow{\pi} K[W]^G \to 0$$

donde U_i son indeterminadas, $\pi(U_i) = u_i \ \forall i = 1, ..., m$ y J es el ideal de relaciones para $K[W]^G$.

Definimos $deg(U_i) = deg(u_i)$ y el siguiente orden monomial en S, para monomios $\alpha = \prod_{i=1}^m U_i^{e_i}$ y $\beta = \prod_{i=1}^m U_i^{f_i}$ decimos que $\alpha < \beta$ si

1) $deg(\alpha) < deg(\beta)$.

2) $deg(\alpha) = deg(\beta)$ y $e_i < f_i$ para el i más grande tal que $e_i \neq f_i$.

Ahora describimos un conjunto de generadores minimal para el ideal de relaciones J:

Para cada par i, j con $1 \leq i, j \leq m$ y $j - i \geq 2$ considerar el producto $u_i u_j \in K[W]^G$. El monomio u_{i+1} divide propiamente a $u_i u_j$, y entonces $\alpha := \frac{u_i u_j}{u_{i+1}} = x^{a_i + a_j - a_{i+1}} y^{b_i + b_j - b_{i+1}} \neq 1$ esta en $K[W]^G$, así podemos escribir $\alpha = \frac{u_i u_j}{u_{i+1}} = \prod_{k=1}^m u_k^{d_{ijk}}$ para algunos enteros no negativos d_{ijk}.

La condición $j - i \geq 2$ implica que $j \geq 1 + (i + 1)$, entonces $a_j < a_{i+2}$, pero tenemos que $a_{i+1} > a_{i+2} > a_j$, similarmente $b_i < b_{i+1} < b_{i+2} < b_j$.

Si $u_r | \alpha$ para $r \leq i$ tenemos que $\frac{u_i u_j}{u_{i+1}} = q u_r$, de donde $a_r < a_i + a_j - a_{i+1}$ y $b_r < b_i + b_j - b_{i+1}$.

Si $a_r < a_i + a_j - a_{i+1}$, entonces $a_i \leq a_r < a_i + a_j - a_{i+1}$ lo cual es una contradicción, por lo tanto $u_r \nmid \alpha$ para $r \leq i$. Similarmente $u_r \nmid \alpha$ para $r \geq j$.

Se sigue que $\alpha = \prod_{k=i+1}^{j-1} u_k^{d_{ijk}}$, y definimos

$$R_{ij} := U_i U_j - U_{i+1} \prod_{k=i+1}^{j-1} U_k^{d_{ijk}}$$

Tenemos que $R_{ij} \in J$ y $LT(R_{ij}) = U_i U_j$.

Proposición 4.3. *Los* $\binom{m-1}{2}$ *elementos* $\{R_{ij} : 1 \leq i, j \leq m, i - j \geq 2\}$ *forman una G-base para* J *y generan mínimamente a* J.

Demostración. Supongamos por contradicción que los R_{ij} no forman una G-base para J .

Elijamos un elemento $f \in J$ homogéneo con $\beta := LM(f)$ mínimo tal que β no es divisible por $LT(R_{ij})$ $\forall i, j$, podemos suponer que f es mónico y como $K[W]^G$ es generado por monomios, también podemos suponer que f es una diferencia de dos términos $f = \prod_{k=1}^{m} U_k^{c_k} - \prod_{k=1}^{m} U_k^{d_k}$ (ver Lema A.1).

Luego algún $\prod_{k=1}^{m} U_k^{c_k}$ o $\prod_{k=1}^{m} U_k^{d_k}$ será el monomio líder de f, como $LT(R_{ij})$ no divide a β, entonces $\beta = U_i^p U_{i+1}^q$ para algún $1 \leq i \leq m$, algún entero positivo p y algún entero no negativo q, donde $U_{i+1} := 1$ si $i = m$.

Tenemos que $f = U_i^p U_{i+1}^q - \prod_{k=1}^{i+1} U_k^{d_k}$ para algunos enteros no negativos d_k. Ya que ni U_i ni U_{i+1} puede dividir a f (por la minimalidad de β) se sigue que $f = U_i^p U_{i+1}^q - \prod_{k=1}^{i-1} U_k^{d_k}$.

Aplicando π a f tenemos

$$0 = \pi(U_i^p U_{i+1}^q) - \pi(\prod_{k=1}^{i-1} U_k^{d_k}) = x^{pa_i+qa_{i+1}} y^{pb_i+qb_{i+1}} - x^{\sum_{k=1}^{i-1} d_k a_k} y^{\sum_{k=1}^{i-1} d_k b_k}$$

y por lo tanto $pa_i + qa_{i+1} = \sum_{k=1}^{i-1} d_k a_k$ y $pb_i + qb_{i+1} = \sum_{k=1}^{i-1} d_k b_k$, por lo tanto

$$\frac{pb_i + qb_{i+1}}{pa_i + qa_{i+1}} = \frac{\sum_{k=1}^{i-1} d_k b_k}{\sum_{k=1}^{i-1} d_k a_k}.$$

Ahora, como $b_1 < b_2 < ... < b_k < ...$, se sigue que $\sum_{k=1}^{i-1} d_k b_k \leq (\sum_{k=1}^{i-1} d_k) b_{i-1}$. Similarmente $\sum_{k=1}^{i-1} d_k a_k \geq (\sum_{k=1}^{i-1} d_k) a_{i-1}$, entonces tenemos que

$$\frac{\sum_{k=1}^{i-1} d_k b_k}{\sum_{k=1}^{i-1} d_k a_k} \leq \frac{(\sum_{k=1}^{i-1} d_k) b_{i-1}}{(\sum_{k=1}^{i-1} d_k) a_{i-1}} = \frac{b_{i-1}}{a_{i-1}}$$

y también como $a_i > a_{i+1}$ tenemos $qa_i \geq qa_{i+1}$, entonces

$$pa_i + qa_i \geq qa_{i+1} + pa_i;$$

$$(p+q)a_i \geq pa_i + qa_{i+1}$$

y como $b_i < b_{i+1}$, se sigue que

$$(p+q)b_i \leq pb_i + qb_{i+1},$$

entonces

$$\frac{pb_i + qb_{i+1}}{pa_i + qa_{i+1}} \geq \frac{(p+q)b_i}{(p+q)a_i} = \frac{b_i}{a_i}.$$

Entonces tenemos que $\frac{b_{i-1}}{a_{i-1}} \geq \frac{b_i}{a_i}$.

Lo cual es una contradicción. Así los elementos $LT(R_{ij})$ forman una G-base para J. Finalmente como los términos líder de R_{ij} son distintos y cuadráticos y sus otros términos no líder tienen grado polinomial más grande o igual que 2, entonces ellos generan mínimamente.

□

Proposición 4.4. *(Harris y Wehlau, [9], Proposición 3.2). Los números de Betti polinomiales para $LT(J)$ son*

$$\beta_{ij} = \begin{cases} 1 & i = -1 \quad j = 0 \\ (i+1)\binom{m}{i+2} - (m-1)\binom{m-2}{i} & i = 0, ..., m-3 \quad j = i+2 \\ 0 & \textit{en otro caso} \end{cases}$$

Proposición 4.5. *(Harris y Wehlau, [9], Proposición 3.3). Sea $W = W_b \oplus W_c$. Entonces la resolución mínima libre de $K[W]^G \cong S/J$ como un S-módulo es de la forma*

$$0 \to M_{m-2} \to ... \to M_1 \to M_0 \to K[W]^G \to 0$$

donde $rank(M_0) = 1$ y para $1 \leq i \leq m-2$ $rank(M_i) = i\binom{m}{i+1} - (m-1)\binom{m-2}{i-1}$.

Capítulo 5

El Teorema de la Cota de Noether

En este capítulo se demuestra el Teorema de la cota de Noether [18], [23], el cual además de acotar los grados de los invariantes, nos dice que $K[V]^G$ tiene un conjunto de generadores de a lo más $\binom{n+k}{n}$ elementos, donde k es el orden del grupo y $n = dim(V)$. Para ello veamos antes algunos resultados.

5.1. Polinomios simétricos

Sea K un campo de característica cero. Un polinomio $f \in K[x_1, ..., x_n]$ se dice que es *simétrico* si es invariante bajo toda permutación de las variables $x_1, ..., x_n$. Por ejemplo, el polinomio $f_1 := x_1x_2 + x_1x_3$ no es simétrico porque $f_1(x_1, x_2, x_3) \neq f_1(x_2, x_1, x_3) = x_1x_2 + x_2x_3$, por otro lado $f_2 := x_1x_2 + x_1x_3 + x_2x_3$ es simétrico.

Los polinomios

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

son simétricos en las variables $x_1, ..., x_n$.

Los polinomios $\sigma_1, ..., \sigma_n \in K[x_1, ..., x_n]$ son llamados polinomios simétricos elementales.

Como la propiedad de ser simétricos se preserva bajo la adición y la multiplicación de polinomios, los polinomios simétricos forman un subanillo de $K[x_1, ..., x_n]$, esto implica que toda expresión polinomial $p(\sigma_1, ..., \sigma_n)$ en los polinomios simétricos elementales es simétrico en $K[x_1, ..., x_n]$.

Teorema 5.1. *Todo polinomio simétrico $f \in K[x_1, ..., x_n]$ puede ser escrito de manera única como un polinomio*

$$f(x_1, ..., x_n) = p(\sigma_1(x_1, ..., x_n), ..., \sigma_n(x_1, ..., x_n))$$

en los polinomios simétricos elementales.

Demostración. Sea $f \in K[x_1, ..., x_n]$ un polinomio simétrico. Comparamos los monomios de f usando el orden lexicográfico graduado.

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} < x_1^{\beta_1} \cdots x_n^{\beta_n} \text{ si}$$

$$\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \text{ o tienen grado total igual y la primera diferencia no nula}$$

$$\alpha_i - \beta_i \text{ es negativa.}$$

Para cualquier monomio $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ que aparece en el polinomio simétrico f, también aparecen todas sus imágenes bajo cualquier permutación σ,

$$x_{\sigma(1)}^{\alpha_1} \cdots x_{\sigma(n)}^{\alpha_n} \text{ también aparece en } f.$$

Esto implica que el monomio inicial $init(f) = cx_1^{\gamma_1} \cdots x_n^{\gamma_n}$ de f satisface $\gamma_1 \geq ... \geq \gamma_n$ (el monomio inicial es el monomio más grande de f con respecto a un orden monomial, el cual aparece con un coeficiente no cero en f, y es denotado por $init(f)$), en efecto, tenemos

$$init(f) = cx_1^{\gamma_1} \cdots x_n^{\gamma_n} > cx_1^{\gamma_2} x_2^{\gamma_1} x_3^{\gamma_3} \cdots x_n^{\gamma_n}, \text{ de donde } \gamma_1 \geq \gamma_2$$

luego

$$init(f) = cx_1^{\gamma_1} \cdots x_n^{\gamma_n} > cx_1^{\gamma_1} x_2^{\gamma_3} x_3^{\gamma_2} \cdots x_n^{\gamma_n}, \text{ de donde } \gamma_2 \geq \gamma_3.$$

Así aplicando la permutación correspondiente a cada par de índices (i, j), $\sigma(i, j) = (j, i)$ sucesivamente, obtenemos $\gamma_1 \geq ... \geq \gamma_n$.

El algoritmo para escribir a f como un polinomio en los polinomios simétricos elementales es el siguiente:

1. Reemplazamos f por $\bar{f}$, donde

$$\bar{f} := f - c\sigma_1^{\gamma_1-\gamma_2}\sigma_2^{\gamma_2-\gamma_3}\cdots\sigma_{n-1}^{\gamma_{n-1}-\gamma_n}\sigma_n^{\gamma_n}.$$

2. Si $\bar{f} \neq 0$ aplicamos (1) a $\bar{f}$.

3. Si $\bar{f} = 0$, f está escrito como un polinomio en los polinomios simétricos elementales.

Veamos que el proceso termina. Por construcción el monomio inicial de $c\sigma_1^{\gamma_1-\gamma_2}\sigma_2^{\gamma_2-\gamma_3}\cdots\sigma_{n-1}^{\gamma_{n-1}-\gamma_n}\sigma_n^{\gamma_n}$ es igual al monomio inicial de f.

La afirmación anterior se sigue de que para cualesquiera f_1, f_2 polinomios, el monomio inicial de un producto de polinomios es el producto de los monomios iniciales respecto a un orden monomial, esto es, $init(f_1f_2) = init(f_1)init(f_2)$. Para mostrar esto veamos el siguiente argumento, para un orden monomial dado, se tiene que si m_1, m_2 son monomios tales que $m_1 > m_2$, tenemos $mm_1 > mm_2$ para todo m monomio. Así, como $init(f_1) \geq m_1$ para todo m_1 monomio de f_1, entonces $init(f_1)init(f_2) \geq m_1 init(f_2)$, y como $init(f_2) \geq m_2$, para todo m_2 monomio de f_2, entonces $m_1 init(f_2) \geq m_1m_2$, de donde $init(f_1)init(f_2) \geq m_1m_2$ para todo m_1m_2 monomio de f_1f_2, por lo tanto, $init(f_1f_2) = init(f_1)init(f_2)$.

Se sigue que en la diferencia que define a $\bar{f}$, los monomios iniciales se cancelan y obtenemos $init(\bar{f}) < init(f)$. El conjunto de monomios m con $m < init(f)$ es finito, pues sus grados están acotados.

El algoritmo entonces tiene que terminar porque de lo contrario se generaría una cadena decreciente infinita de monomios.

Demostraremos la unicidad. Veamos que los polinomios simétricos elementales son algebraicamente independientes sobre K.

Supongamos lo contrario. Entonces, hay un polinomio no cero $p(y_1, ..., y_n)$ tal que $p(\sigma_1, ..., \sigma_n) = 0$ en $K[x_1, ..., x_n]$.

Dado cualquier monomio $y_1^{\alpha_1}\cdots y_n^{\alpha_n}$ de p, tenemos que

$$x_1^{\alpha_1+\alpha_2+...+\alpha_n}x_2^{\alpha_2+...+\alpha_n}\cdots x_n^{\alpha_n}$$

es el monomio inicial de $\sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n}$.

Ahora como la aplicación lineal $(\alpha_1, \alpha_2, ..., \alpha_n) \mapsto (\alpha_1+\alpha_2+...+\alpha_n, ..., \alpha_n)$ es inyectiva, tenemos que todos los monomios $\sigma_1^{\beta_1} \cdots \sigma_n^{\beta_n}$ en la expansión de $p(\sigma_1, ..., \sigma_n)$ tienen un monomio inicial diferente.

Entonces el monomio lexicográficamente más grande

$$x_1^{\alpha_1+\alpha_2+...+\alpha_n} x_2^{\alpha_2+...+\alpha_n} \cdots x_n^{\alpha_n}$$

no se cancela y por lo tanto $p(\sigma_1, ..., \sigma_n) \neq 0$ lo cual es una contradicción, lo cual termina la demostración.

□

Ejemplo 5.1. *Sea* $f = x_1^3 + x_2^3$, *entonces* $init(f) = x_1^3$, $\gamma_1 = 3$, $\gamma_2 = 0$

$$\begin{aligned} \bar{f} &= x_1^3 + x_2^3 - \sigma_1^3\sigma_2^0 \\ &= x_1^3 + x_2^3 - (x_1 + x_2)^3 \\ &= x_1^3 + x_2^3 - (x_1^3 + x_2^3 + 3x_1x_2^2 + 3x_1^2x_2) \\ &= -3x_1^2x_2 - 3x_1x_2^2 \\ &= -3(x_1x_2)(x_1 + x_2) \end{aligned}$$

$\bar{f} \neq 0$, *entonces* $init(\bar{f}) = -3x_1^2x_2$, $\gamma_1 = 2$, $\gamma_2 = 1$ *y* $\gamma_3 = 0$
Entonces tenemos que $\bar{f}_1 = -3x_1^2x_2 - 3x_1x_2^2 + 3(x_1 + x_2)(x_1x_2) = 0$
Así que del paso anterior tenemos que $f = \sigma_1^3 - 3\sigma_1\sigma_2$

Ahora describiremos otro conjunto generador para los polinomios simétricos. El polinomio $p_k := x_1^k + x_2^k + ... + x_n^k$ es llamada la k-ésima suma de potencia.

Proposición 5.1. *El anillo de polinomios simétricos es generado por las primeras n sumas de potencia, es decir,*

$$K[x_1, ..., x_n]^{S_n} = K[\sigma_1, ..., \sigma_n] = K[p_1, p_2, ..., p_n].$$

Demostración. Una partición de un entero positivo d es un $\mathbb{Z}$-vector $\lambda = (\lambda_1, \lambda_2, .., \lambda_n)$ tal que $\lambda_1 \geq ... \geq \lambda_n \geq 0$ y $\lambda_1 + ... + \lambda_n = d$.

Asignamos al monomio $x_1^{i_1}x_2^{i_2} \cdots x_n^{i_n}$ de grado d la partición $\lambda(i_1, ..., i_n)$, la cual es la cadena decreciente de sus exponentes.

Esto da lugar al siguiente orden total en el conjunto de monomios de grado d en $K[x_1, ..., x_n]$. Decimos que

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} < x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

si la partición

$$\lambda(i_1, ..., i_n) >_{lex} \lambda(j_1, ..., j_n)$$

o si

$$\lambda(i_1, ..., i_n) = \lambda(j_1, ..., j_n) \text{ y } (i_1, ..., i_n) <_{lex} (j_1, ..., j_n).$$

Por ejemplo, para $n = 3$ y $d = 4$ tenemos $x_3^4 < x_2^4 < x_1^4 < x_2 x_3^3 < x_2^3 x_3 < x_1 x_3^3 < x_1 x_2^3$.

Ahora consideremos un producto de sumas de potencias $p_{i_1} p_{i_2} \cdots p_{i_n}$. En la expansión de este producto tenemos que los monomios con n elementos son mayores a los que tienen menos elementos respecto al orden antes definido, esto es, si $m < n$ tenemos $x_{j_1}^{k_1} x_{j_2}^{k_2} \cdots x_{j_m}^{k_m} < x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n}$, en efecto, como todos los monomios en $p_{i_1} p_{i_2} \cdots p_{i_n}$ tienen grado $i_1 + i_2 + ... + i_n$, entonces $k_1 + ... + k_m = l_1 + ... + l_n$, como $m < n$ tenemos que existe j tal que $k_j > l_i$ para $i = 1, ..., n$, así $\lambda(k_1, ..., k_m) = (k_j, ..., k_{r_m}, 0, ..., 0)$ en la cual aparecen $n - m$ ceros, se sigue que $(k_j, ..., k_{r_m}, 0, ..., 0) >_{lex} \lambda(l_1, ..., l_n)$.

Tenemos entonces que $init(p_{i_1} p_{i_2} \cdots p_{i_n}) = c_{i_1 i_2 ... i_n} x_1^{i_1} \cdots x_n^{i_n}$ siempre que $i_1 \geq i_2 \geq ... \geq i_n$, donde $c_{i_1 i_2 ... i_n}$ es un entero positivo.

Ahora podemos describir un algoritmo que pruebe la proposición. Este reescribe un polinomio simétrico dado $f \in K[x_1, ..., x_n]$ como una función polinomial en $p_1, ..., p_n$, por el Teorema (5.1) podemos suponer que f es uno de los polinomios simétricos elementales. En particular el grado d de f es menor o igual a n.

Su monomio inicial $init(f) = x_1^{i_n} \cdots x_n^{i_n}$ satisface $n \geq i_1 \geq i_2 \geq ... \geq i_n$ (aquí los i_k son ceros o unos).

Reemplazar f por $\bar{f}$ donde

$$\bar{f} := f - \frac{c}{c_{i_1 i_2 ... i_n}} p_{i_1} p_{i_2} \cdots p_{i_n}.$$

Por la observación anterior el monomio inicial de esta diferencia se cancela y obtenemos $init(\bar{f}) < init(f)$. Como ambos f y $\bar{f}$ tienen el mismo grado d, este proceso termina con el resultado deseado.

□

5.2. El teorema de la cota de Noether

Ahora regresemos al caso de un grupo finito G para demostrar el siguiente teorema de E. Noether (1916) [18].

Teorema 5.2 (La cota del grado de Noether)**.** *El anillo de polinomios invariantes $K[x_1, ..., x_n]^G$ de un grupo finito tiene un conjunto de generadores como K-álgebra de a lo más $\binom{n+|G|}{n}$ invariantes cuyos grados están acotados por arriba por el orden del grupo $|G|$.*

Demostración. A cada vector $e = (e_1, e_2, ..., e_n)$ de enteros no negativos le asociamos el invariante homogéneo $J_e(x) := (x_1^{e_1} \cdots x_n^{e_n})^*$, el cual es obtenido considerando la imagen del monomio con exponente e bajo la siguiente aplicación:

$$\begin{aligned} * : K[x_1, ..., x_n] &\to K[x_1, ..., x_n]^G \\ f &\mapsto \tfrac{1}{|G|} \sum_{\pi \in G} f \circ \pi \end{aligned}$$

esto es:

$$\begin{aligned} J_e(x) &:= (x_1^{e_1} \cdots x_n^{e_n})^* \\ &= \frac{1}{|G|} \sum_{\pi \in G} (x_1^{e_1} \cdots x_n^{e_n}) \circ \pi \\ &= \frac{1}{|G|} \sum_{\pi \in G} (x_1 \circ \pi)^{e_1} \cdots (x_n \circ \pi)^{e_n} \end{aligned}$$

El orden del vector e es $|e| = e_1 + e_2 + ... + e_n$.

Consideremos un nuevo conjunto de variables $u_1, ..., u_n$ y definamos el polinomio

$$\begin{aligned} S_{|e|}(u, x) &:= ((u_1 x_1 + ... + u_n x_n)^{|e|})^* \\ &= \frac{1}{|G|} \sum_{\pi \in G} (u_1 (x_1 \circ \pi) + ... + u_n (x_n \circ \pi))^{|e|} \end{aligned}$$

$S_{|e|}(u,x)$ es un polinomio en las variables $u_1,...,u_n$ con coeficientes en las variables $x_1,...,x_n$. El operador de Reynolds $*$ actúa en estos polinomios considerando las variables u_i $i=1,...,n$ como constantes.

En la expansión completa de la expresión de arriba encontramos que el coeficiente de $u_1^{e_1}\cdots u_n^{e_n}$ en $S_{|e|}$, es igual al invariante J_e multiplicando por un entero positivo.

Ahora definamos $y_i := \sum_{l=1}^{n} u_l(x_l \circ \pi_i)$, con $\pi_i \in G$ y sea $k=|G|$, tenemos $S_{|e|}(u,x) = y_1^{|e|}+y_2^{|e|}+...+y_k^{|e|}$, entonces es claro que $S_{|e|}(u,x) \in \mathbb{C}[y_1,...,y_k]^{S_k}$, por la Proposición (5.1) tenemos que, $S_{|e|}(u,x) \in K[S_1,...,S_k]$. Esta representación de $S_{|e|}$ prueba que todos los u-coeficientes son funciones polinomiales en los u-coeficientes de $S_1, S_2, ..., S_{|e|}$. Veamos como son los polinomios $S_{|e|}$, describiremos el polinomio S_1.

$$\begin{aligned} S_1 &= \frac{1}{|G|}\sum_{\pi\in G} u_1(x_1\circ\pi)+...+u_n(x_n\circ\pi) \\ &= u_1(\frac{1}{|G|}\sum_{\pi\in G} x_1\circ\pi)+...+u_n(\frac{1}{|G|}\sum_{\pi\in G} x_n\circ\pi) \\ &= J_{(1,0,0,...,0)}u_1+...+J_{(0,0,...,1)}u_n. \end{aligned}$$

Este argumento prueba que los invariantes J_e con $|e|>|G|$ están contenidos en el subanillo $\mathbb{C}[\{J_e : |e|>|G|\}]$.

Además notamos que todo invariante es una $\mathbb{C}$-combinación lineal de los invariantes especiales J_e, por lo tanto tenemos que

$$\mathbb{C}[x_1,...,x_n]^G = \mathbb{C}[\{J_e : |e|>|G|\}].$$

Por último tenemos que el conjunto de vectores $e\in\mathbb{N}^n$ con $|e|\leq|G|$ tiene cardinalidad $\binom{n+|G|}{n}$.

□

La aplicación $*$ usada en la demostración anterior, se llama el operador de Reynolds, el cual será definido en el siguiente capítulo.

Capítulo 6

Teoría de Invariantes de Grupos Finitos

En este capítulo K es un campo y G es un grupo finito actuando en un espacio vectorial V dimensionalmente finito. Observe que si consideramos G como un grupo algebraico lineal, entonces toda acción lineal en un espacio vectorial es racional. En el capítulo 3, en la Proposición (3.1) demostramos que el anillo de invariantes $K[V]^G$ es finitamente generado, ahora nuestro objetivo central es calcular un conjunto finito de generadores. Hemos visto además en el capítulo anterior que el número de generadores es a lo más $\binom{n+|G|}{n}$ y que sus grados están acotados por $|G|$.

6.1. Componentes homogéneas

La tarea más básica de la teoría de invariantes computacional es calcular invariantes de algún grado dado d. Recordemos que el anillo de invariantes $K[V]^G$ es un álgebra graduada, donde $K[V]^G_d$ es el espacio de invariantes homogéneos de grado d. Los monomios de grado d en las variables $x_1, ..., x_n$ forman una base de $K[V]_d$, por lo tanto $dim(K[V]_d) = \binom{n+d-1}{n-1}$, donde $n = dim(V)$.

6.1.1. El método de álgebra lineal

Sea $H \leq G$ un subgrupo de G cuyos invariantes de grado d son conocidos y tomemos un conjunto $S(G \setminus H) \subseteq G$ tal que H junto con $S(G \setminus H)$ generan

a G.

Consideremos la suma directa de $K[V]$ cuyos componentes están indexados por los elementos de $S(G \setminus H)$, y consideremos la siguiente aplicación.

$$\begin{aligned} \phi : K[V]^H &\to \bigoplus_{\sigma \in S(G\setminus H)} K[V] \\ f &\mapsto \phi(f) = (\sigma \circ f - f)_{\sigma \in S(G\setminus H)} \end{aligned}$$

Y observemos que $f \in \ker \phi$ si y sólo si $\sigma \circ f = f \ \forall \sigma \in S(G \setminus H)$, esto pasa si y sólo si $f \in K[V]^{S(G\setminus H)}$, se sigue que $f \in K[V]^G$, por lo tanto $\ker \phi = K[V]^G$.

Además tenemos que ϕ es K-lineal y preserva el grado.

Ahora restringiendo a la componente de grado d obtenemos una aplicación lineal

$$K[V]_d^H \to K[V]_d^{|S(G\setminus H)|}$$

cuyo kernel es $K[V]_d^G$. Esta aplicación está explícitamente dada, entonces su kernel puede ser calculado resolviendo un sistema de ecuaciones lineales sobre K.

Para $H = 1$ tenemos que $K[V]_d^H = K[V]_d$, entonces el número de incógnitas es $\binom{n+d-1}{n-1}$ y el número de ecuaciones es $|S(G \setminus H)| \cdot \binom{n+d-1}{n-1}$.

6.1.2. El operador de Reynolds

Definición 6.1. *Supongamos que X es una G-variedad afín, donde G es un grupo algebraico lineal.*

Un operador de Reynolds es una G-proyección invariante, es decir, una aplicación lineal

$$\mathcal{R} : K[X] \to K[X]^G$$

tal que

a) $\mathcal{R}(f) = f \ \forall f \in K[X]^G$.

b) $\mathcal{R}$ *es G-invariante, es decir* $\mathcal{R}(\sigma \circ f) = \mathcal{R}(f) \ \forall f \in K[X]$ *y* $\forall \sigma \in G$.

Supongamos que G es un grupo finito tal que $char(K)$ no divide a $|G|$. Si X es una variedad afín en la cual actúa G, entonces un operador de Reynolds es definido por:

$$\mathcal{R}(f) = \tfrac{1}{|G|} \sum_{\sigma \in G} \sigma \circ f.$$

Ahora describamos el siguiente algoritmo el cual es aplicable si $char(K)$ no divide al orden del grupo $|G|$.

Algoritmo 6.1. *Aplicar el operador de Reynolds a todos los monomios en $K[V]$ de grado d.*

Con esto se obtiene un conjunto de generadores de $K[V]_d^G$. Por álgebra lineal una base puede ser extraída de éste.

Más generalmente, sea $H \leq G$ un subgrupo de G tal que el índice $[G : H]$ no es divisible por la característica p de K, entonces definimos el operador de Reynolds relativo como:

$$\begin{gathered} \mathcal{R}_{G/H} : K[V]^H \to K[V]^G \\ f \mapsto \tfrac{1}{[G:H]} \sum_{\sigma \in G/H} \sigma \circ f \end{gathered}$$

donde G/H es el conjunto de representantes de clases laterales izquierdas. Es claro que $\mathcal{R}_{G/H}$ es independiente de la elección de los representantes de clase lateral y que es una proyección de módulos sobre $K[V]^G$. En particular, las imágenes bajo $\mathcal{R}_{G/H}$ de una base de $K[V]_d^H$ generan el espacio vectorial deseado $K[V]_d^G$, y entonces podemos seleccionar una base para $K[V]_d^G$.

6.2. Fórmula de Molien

Teorema 6.1 (Teorema de Molien [16])**.** *El anillo de invariantes $S^G \subset S = \mathbb{C}[x_1, ., x_n]$ de cualquier grupo finito $G \subset GL(n)$ tiene una serie de Hilbert dada por*

$$\tfrac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I_n - tA)}.$$

Antes de probar este Teorema, recordemos algunos hechos de la teoría de representaciones de grupos finitos.

Una representación de un grupo G es un homomorfismo $\rho : G \to GL(V)$ de G al grupo de automorfismos de un espacio vectorial V. Si V es una representación dimensionalmente finita, su *carácter* es la aplicación:

$$\begin{array}{c} \chi : G \to \mathbb{C} \\ g \mapsto tr(\rho(g)). \end{array}$$

Consideramos el subespacio invariante

$$V^G := \{v \in V | \rho(g)v = v, \forall g \in G\}.$$

La dimensión de este subespacio es

$$dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Demostración. (Fórmula de Molien). Tomemos un elemento $A \in G$, y sea $\{x_1, ..., x_n\}$ una base de eigenvectores de A en S_1, correspondientes a los eigenvalores $a_1, ..., a_n$.

Note que A es diagonalizable ya que tiene orden finito y el campo es algebraicamente cerrado.

Se sigue que el polinomio característico inverso de A es:

$$\det(I_n - tA) = (1 - a_1 t)(1 - a_2 t) \cdots (1 - a_n t).$$

Ahora consideremos la expansión formal en serie de potencias de

$$\frac{1}{(1 - x_1)(1 - x_2) \cdots (1 - x_n)}$$

cuyos términos son precisamente los monomios del anillo $\mathbb{C}[x_1, ..., x_n]$.

La acción de A en esta serie nos da

$$\frac{1}{(1 - a_1 x_1)(1 - a_2 x_2) \cdots (1 - a_n x_n)}.$$

Entonces si tomamos la sustitución $x_1 = ... = x_n = t$ vemos que el caracter $\chi_d(A)$ en $\mathbb{C}[x_1, ..., x_n]$ es precisamente el coeficiente de t^d en la expansión de

$$\frac{1}{(1-a_1t)\cdots(1-a_nt)}.$$

En decir, obtenemos

$$\sum_d \chi_d(A)t^d = \frac{1}{\det(I_n - tA)}.$$

Si ahora dividimos por $\frac{1}{|G|}$ y aplicamos la fórmula de la dimensión (ver [16], Fórmula (1.11))

$$dimV^G = \frac{1}{|G|}\sum_{g\in G}\chi(g)$$

obtenemos la fórmula de Molien

$$H(\mathbb{C}[x_1,...,x_n]^G,t) = \frac{1}{|G|}\sum_{A\in G}\frac{1}{\det(I_n - tA)}.$$

□

6.3. Invariantes primarios

El primer paso para calcular un anillo de invariantes de un grupo finito, es la construcción de un sistema homogéneo de parámetros (ver sección 3.2). Los invariantes que aparecen en un sistema homogéneo de parámetros son llamados *invariantes primarios*. La existencia de un sistema homogéneo de parámetros es garantizado por el Teorema de Normalización de Noether 3.1. Antes de ver un criterio para invariantes primarios, demostraremos el lema graduado de Nakayama.

Lema 6.1. *(Lema Graduado de Nakayama) Sea R una álgebra graduada (no negativa), sobre un campo $K = R_0$ y M un R-módulo graduado no negativo. Entonces para un subconjunto $S \subseteq M$ de elementos homogéneos, las siguientes dos condiciones son equivalentes.*

a) S genera a M como un R-módulo.

b) S genera a M/R_+M como un espacio vectorial sobre K, aquí $R_+M \subset M$ es el submódulo de M generado por los elementos $a \cdot g$ con $a \in R_+$.

En particular un conjunto generador S para M es de cardinalidad mínima si no existe un subconjunto propio de S que genera a M.

Demostración. $(a) \Rightarrow (b)$

Claramente si S genera a M también genera a M/R_+M como un K-espacio vectorial.

$(b) \Rightarrow (a)$

Supongamos que S genera a M/R_+M y sea $g \in M$ homogéneo de algún grado d.

Si $d = 0$, tenemos $g = \sum_{i=1}^{m} \alpha_i g_i$ con $\alpha \in K$ y $g_i \in S$ de grado cero.

Supongamos $d > 0$, por hipótesis

$$g = \sum_{i=1}^{m} \alpha_i g_i + \sum_{j=1}^{r} a_j h_j$$

con $g_i, ..., g_m \in S$, $\alpha_i \in K$, $a_j \in R_+$ y $h_j \in M$.

Podemos suponer que a_j y h_j son homogéneos con $deg(a_j h_j) = d$, por lo tanto, $deg(h_j) < d$ y h_j está en el submódulo generado por S por inducción en d, entonces g pertenece al submódulo generado por S.

La observación de minimalidad se sigue de la propiedad correspondiente de espacios vectoriales.

□

Ahora veremos el siguiente criterio para invariantes primarios.

Proposición 6.1. *Sean $f_1, ..., f_n \in K[V]_+^G$ invariantes homogéneos de grado positivo con $n = dim_K(V)$. Entonces las siguientes afirmaciones son equivalentes:*

a) $f_1, ..., f_n$ forman un sistema homogéneo de parámetros.

b) $V_{\bar{K}}(f_1, ..., f_n) = \{0\}$ donde $V_{\bar{K}}(f_1, ..., f_n)$ es definido como

$$\left\{ v \in \bar{K} \otimes_K V | f_i(v) = 0 \text{ para } i = 1, ..., n \right\}$$

y $\bar{K}$ una cerradura algebraica de K.

c) La dimensión de Krull, $dim(K[V]/\langle f_1, ..., f_n\rangle)$ es cero.

d) La dimensión de Krull, $dim(K[V]/\langle f_1, ..., f_i\rangle) = n - i$ para $i = 1, ..., n$.

Demostración. Veamos que $K[V]$ es entero sobre $K[V]^G$, como $K[V]$ es un álgebra finitamente generada sobre K, sean $x_1, ..., x_n$ generadores para $K[V]$ y sea $f_i(t) = \prod_{\sigma\in G}(t - \sigma x_i)$ con coeficientes en $K[V]^G$, entonces $f_i(x_i) = 0$ para todo $i = 1, ..., n$, así $f_i(t)$ es una ecuación entera para x_i sobre $K[V]^G$, se sigue que $K[V]$ es entero sobre $K[V]^G$.

Luego $dimK[V] = dimK[V]^G = n$ (ver Kemper [[13], Corolario 8.13]).

Por lo tanto cualquier sistema homogéneo de parámetros en $K[V]^G$ tiene a lo más n elementos y (a) es equivalente a la condición de que $K[V]^G$ es un módulo finitamente generado sobre la subálgebra $A := K[f_1, ..., f_n]$, que a su vez es equivalente a la condición que $K[V]$ es un módulo finitamente generado sobre A. Esta última afirmación es clara, pues por un lado tenemos que $K[V]$ es un $K[V]^G-$módulo finitamente generado y $K[V]^G$ es un A-módulo finitamente generado se sigue que $K[V]$ es un A-módulo finitamente generado, inversamente usamos que $K[V]$ es noetheriano.

Por la versión graduada del lema de Nakayama (Lema (6.1)), esto es equivalente a $dim_K(K[V]/\langle f_1, ..., f_n\rangle) < \infty$.

Una K-álgebra es de K-dimensión finita si y sólo si su dimensión de Krull es cero.

Así hemos probado la equivalencia de (a) y (c).

Por el Teorema del ideal principal de Krull (ver Eisenbud [[7], Teorema 10.2])(c) y (d) son equivalentes.

Finalmente (b) es equivalente a (c) pues el ideal $\langle f_1, ..., f_n\rangle$ es homogéneo. □

6.3.1. Algoritmo de Dade

Un algoritmo para la construcción de un sistema homogéneo de parámetros para $K[V]^G$ fue dado por Dade (Stanley [22], Reiner y Smith [20]). Este

ésta basado en la siguiente observación.

Proposición 6.2. *Sea $n = dim(V)$ y supongamos que $l_1, ..., l_n \in V^* \setminus \{0\}$ son formas lineales tales que*

$$l_i \notin \bigcup_{\sigma_1,...,\sigma_{i-1} \in G} \langle \sigma_1 l_1, ..., \sigma_{i-1} l_{i-1} \rangle \text{ para } i = 1, ..., n.$$

Sea f_i el producto sobre todos los l en la G-órbita de l_i. Entonces $\{f_1, ..., f_n\}$ es un sistema homogéneo de parámetros de $K[V]^G$.

Demostración. Veamos que se satisface la condición (b) de la proposición anterior. Tomemos $v \in V_{\bar{K}}(f_1, ..., f_n)$, como $f_i = \prod_{\sigma \in G} \sigma l_i$, entonces $\sigma l_i(v) = 0$ para algún $\sigma \in G$, y le llamamos σ_i, así $(\sigma_i l_i)(v) = 0$.

Luego por hipótesis tenemos que $\sigma_1 l_1, ..., \sigma_n l_n$ forma una base para V^*, consideremos la base $e_1, ..., e_n$ de V determinada por $\sigma_j l_j(e_i) = \delta_{ij}$, ahora escribimos $v = \lambda_1 e_1 + ... + \lambda_n e_n$, entonces $\sigma_i l_i(v) = \lambda_i$, se sigue que $\lambda_i = 0$ para todo $i = 1, ..., n$, por lo tanto, $v = 0$. □

6.3.2. Un algoritmo para un sistema homogéneo de parámetros óptimo

A continuación se proporciona un criterio para la existencia de invariantes primarios de grados dados.

Teorema 6.2. *Sea $A = \bigoplus_{d=0}^{\infty} A_d$ un álgebra graduada conmutativa sobre un campo infinito $K = A_0$ y sea $n \in \mathbb{N}_0$ y $d_1, ..., d_k \in \mathbb{N}$. Entonces las siguientes condiciones son equivalentes:*

a) Existen homogéneos $f_1, ..., f_k$ con $deg(f_i) = d_i$ tal que

$$\dim(A/(f_1, ..., f_k)) \leq n - k.$$

b) Para cada subconjunto $M \subset \{1, ..., k\}$ tenemos que

$$\dim(A/(\textstyle\bigcup_{i \in M} A_{d_i})) \leq n - |M|.$$

Si K es un campo finito entonces la implicación $(a) \Rightarrow (b)$ se satisface.

Una prueba de este Teorema la podemos encontrar en Kemper ([12], Teorema 2). Tenemos ahora el siguiente algoritmo para la construcción de un sistema homogéneo de parámetros óptimo.

Algoritmo 6.2. *1. Recorrer todos los vectores grado* $(d_1, ..., d_n) \in \mathbb{N}^n$ *ordenados de forma creciente por el valor* $\prod_{i=1}^{n} d_i$ *hasta que se encuentre uno que satisfaga las condiciones en (b) del Teorema (6.2).*

2. Recorrer todos los $f_1 \in K[V]_{d_1}^G$ *hasta encontrar un* f_1 *tal que* $(d_2, ..., d_n)$ *satisface las condiciones en (b) del Teorema (6.2) con* $K[V]$ *reemplazado por* $K[V]/(f_1)$*.*

3. Por recursión obtenemos $f_2, ..., f_n$ *de grados* $d_2, ..., d_n$*, tal que* $f_1, ..., f_n$ *es el sistema homogéneo de parámetros deseado.*

4. Si el ciclo en $K[V]_{d_i}^G$ *falla en algún nivel de la recursividad (que por el teorema anterior sólo puede suceder si* K *es finito), volver a (1) y elegir un nuevo vector grado* $(d_1, ..., d_n)$*.*

6.4. Cohen- Macaulay

La propiedad Cohen-Macaulay ya fue definida anteriormente en la sección 3.3, y probamos en la Proposición (3.2) que un álgebra es Cohen- Macaulay si y sólo si es libre como un módulo sobre la subálgebra generada por un sistema homogéneo de parámetros. En esta sección demostraremos que el anillo de invariantes $K[V]^G$ es Cohen- Macaulay, y usando los resultados de la sección 6.3 podemos calcular los invariantes primarios. En caso de grupos finitos tenemos:

Teorema 6.3. *Si* $char(K)$ *no divide al orden del grupo* $|G|$*, entonces* $K[V]^G$ *es Cohen-Macaulay.*

Demostración. Sean $f_1, ..., f_n$ invariantes primarios $K[V]$. Por la Proposición (6.1) $f_1, ..., f_n$ también es un sistema homogéneo de parámetros de $K[V]$, por lo tanto, $f_1, ..., f_n$ es una sucesión $K[V]-$regular por el Lema (3.2) y la Proposicón (3.2).

Supongamos que para algún $i \in \{1, ..., n\}$ tenemos

$$g_i f_i = g_1 f_1 + ... + g_{i-1} f_{i-1}$$

con $g_1, ..., g_{i-1} \in K[V]^G$. Entonces g_i pertenece ideal generado por $f_1, ..., f_{i-1}$ en $K[V]$, entonces

$$g_i = h_1 f_1 + ... + h_{i-1} f_{i-1}$$

con $h_j \in K[V]$. Ahora aplicamos el operador de Reynolds y obtenemos

$$g_i = \mathcal{R}(g_i) = \mathcal{R}(h_1) f_1 + ... + \mathcal{R}(h_{i-1}) f_{i-1}$$

Por lo tanto, g_i esta en el $K[V]^G$-ideal generado por $f_1, ..., f_{i-1}$. Como $K[V]$ es Noetheriano tenemos que $K[V]^G$ es un $K[V]$-módulo finitamente generado, entonces se sigue que $K[V]^G$ es un $K[f_1, ..., f_n]$-módulo finitamente generado. Así $K[V]^G$ es Cohen- Macaulay por la Proposición (3.2). □

Del Teorema (6.3) y de la Proposición (3.2) se sigue el siguiente resultado:

Teorema 6.4. *Sean G un grupo finito y V una representación finita de G. Entonces el anillo de invariantes $K[V]^G$ es Cohen- Macaulay y $K[V]^G$ es un módulo libre sobre $K[f_1, ..., f_n]$, donde $f_1, ..., f_n$ es un sistema homogéneo de parámetros, esto es $f_1, ..., f_n$ son invariantes primarios.*

6.5. Invariantes secundarios

En esta sección supondremos que hemos calculado los invariantes primarios $f_1, ..., f_n$, entonces $K[V]^G$ es generado por invariantes homogéneos $g_1, ..., g_m$ como un módulo sobre $A := K[f_1, ..., f_n]$, tales g_i se llaman invariantes secundarios, junto con los invariantes primarios los g_i generan a $K[V]^G$ como un álgebra sobre K.

De la versión graduada del Lema de Nakayama (Lema 6.1) tenemos que un conjunto de invariantes homogéneos generan a $K[V]^G$ como un módulo sobre A si y sólo si sus imágenes generan al cociente $K[V]^G/A_+K[V]^G$ como un espacio vectorial sobre K.

Sabemos que existe un sistema homogéneo de parámetros $f_1, ..., f_r$, y además tenemos que $K[V]^G$ es Cohen- Macaulay y $K[V]^G$ es un F-módulo libre donde $F := K[f_1, ..., f_r]$.

Por lo tanto hay una descomposición $K[V]^G = Fg_1 \oplus ... \oplus Fg_s$, con $g_1, ..., g_s$ invariantes homogéneos.

Hemos visto además que la serie de Hilbert de $K[V]^G$ es:

$$H(K[V]^G, t) = \frac{\sum_{j=1}^{s} t^{e_j}}{\prod_{i=1}^{r}(1 - t^{d_i})}$$

donde $d_i = deg(f_i)$ y $e_j = deg(g_j)$.

De la fórmula de Molien tenemos

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I_n - tA)}$$

Comparando las dos series obtendremos información completa acerca de los grados de los invariantes.

Sean $g_1, ..., g_m \in K[V]^G$ invariantes homogéneos con $m = \frac{\prod_{i=1}^{n} d_i}{|G|}$ (ver apéndice B). Entonces los g_i son invariantes secundarios si y sólo si generan a $K[V]^G / A_+K[V]^G$ como espacio vectorial sobre K.

El ideal $A_+K[V]^G$ en $K[V]^G$ es generado por $f_1, ..., f_n$. Consideremos la aplicación

$$\begin{array}{c} K[V]^G \longrightarrow K[V]/\langle f_1, ..., f_n \rangle K[V] \\ f \longmapsto f + \langle f_1, ..., f_n \rangle K[V] \end{array}$$

claramente $A_+K[V]^G$ pertenece al kernel de esta aplicación. Un elemento f en el kernel tiene la forma

$$f = h_1 f_1 + ... + h_n f_n$$

y aplicando el operador de Reynolds obtenemos

$$f = \mathcal{R}(h_1)f_1 + ... + \mathcal{R}(h_n)f_n \in A_+K[V]^G.$$

Por lo tanto tenemos el encaje

$$K[V]^G/A_+K[V]^G \hookrightarrow K[V]/\langle f_1, ..., f_n\rangle K[V]$$

Entonces $g_1, ..., g_m$ son invariantes secundarios si y sólo si son linealmente independientes módulo el ideal $I := \langle f_1, ..., f_n\rangle$ en $K[V]$.

Sea G una G-base de I con respecto a algún orden monomial y denotamos la forma normal con respecto a G por NF_G, entonces para $\alpha_1, ..., \alpha_m \in K$ tenemos $\alpha_1 g_1 + ... + \alpha_m g_m \in I$ si y sólo si $\alpha_1 NF_G(g_1) + ... + \alpha_m NF_G(g_m) = 0$.

Así que todo lo que tenemos que hacer es comprobar la independencia de las formas normales de los g_i.

Algoritmo 6.3. *(Invariantes Secundarios)*

1) Sea G una G-base del ideal

$$\langle f_1, ..., f_n\rangle \subseteq K[V]$$

generado por los invariantes primarios.

2) Calcular los grados $e_1, ..., e_m$ usando la fórmula de Molien y comparándola con la serie de Hilbert (ecuación (3.1)) del $K[V]^G$.

3) Para $i = 1, ..., m$ realizar los siguientes pasos.

4) Calcular una base de la componente homogénea $K[V]^G_{e_i}$ usando los métodos ya vistos (ver sección 6.1).

5) Seleccionar un elemento g_i de esta base tal que $NF_G(g_i)$ no esté en el K-espacio vectorial generado por los polinomios $NF_G(g_1), ..., NF_G(g_{i-1})$.

6) Los invariantes $g_1, ..., g_m$ son los invariantes secundarios.

6.6. Sizigias

Comencemos con algunas nociones sobre el módulo sizigias de un anillo de polinomios.

Escribimos $R := K[x_1, ..., x_n]$ para el anillo de polinomios en n variables, y R^k para un R-módulo libre de rango k. La base estándar de vectores de R^k

son denotados por $e_1, ..., e_k$. Dados polinomios $f_1, ..., f_k \in R$, nos preguntamos por el conjunto de todos los $(h_1, ..., h_k) \in R^k$ tal que $h_1 f_1 + ... + h_k f_k = 0$. Este conjunto es un submódulo de R^k, llamado el **módulo de sizigias** de $f_1, ..., f_k$ y es denotado por $Syz(f_1, ..., f_k)$. Más generalmente, nos preguntamos por el kernel de un R-homomorfismo $\phi : R^k \to R^l$ entre dos R-módulos libres. Si $f_i := \phi(e_i) \in R^l$, entonces el kernel de ϕ consiste de todos los $(h_1, ..., h_k) \in R^k$ con $h_1 f_1 + ... + h_k f_k = 0$. Una vez más $Syz(f_1, ..., f_k) := ker(\phi)$ es llamado el módulo de sizigias de f_i [6].

Ahora supongamos que tenemos generadores $h_1, ..., h_r$ de una K-álgebra R. Consideremos el homomorfismo

$$\begin{aligned} \psi : K[t_1, ..., t_r] &\to R \\ t_i &\mapsto h_i \end{aligned}$$

donde las t_i son indeterminadas. Nos interesa encontrar generadores de $I = ker(\psi)$ como un ideal en el anillo de polinomios. Esto lo podemos hacer mediante diferentes métodos.

En nuestra situación tenemos $R = K[V]^G$, el cual está contenido en el anillo de polinomios $K[V]$. Por lo tanto podemos usar los métodos de las G-bases para calcular las relaciones entre los polinomios h_i. En este caso tenemos que $ker(\psi)$ es un ideal de eliminación, entonces aplicamos los resultados descritos en la sección 1.2.

Otra forma de calcular $ker(\psi)$ es usando la homogeneidad de los generadores invariantes. De hecho, I se convierte en un ideal homogéneo si establecemos $deg(t_i) = deg(h_i)$. También usamos que en nuestra situación el conjunto $\{h_1, ..., h_r\}$ es la unión de un sistema homogéneo de parámetros $\{f_1, ..., f_n\}$ y un conjunto de invariantes secundarios $\{g_1, ..., g_m\}$. Como los f_i son algebraicamente independientes, estamos buscando el kernel I de la aplicación:

$$\begin{aligned} A[t_1, ..., t_m] &\to K[V]^G \\ t_i &\mapsto g_i \end{aligned}$$

donde $A = K[f_1, ..., f_n]$ y las t_i son otra vez indeterminadas.

Afirmación: Supongamos que $S \subseteq I$ es un conjunto de relaciones que contiene

a) Generadores para el A-módulo $I \cap (\oplus_{i=1}^{m} A \cdot t_i)$ de relaciones A-lineales entre los g_i, y

b) Para cada $1 \leq i \leq j \leq m$ una relación de la forma $t_i t_j - f_{i,j}$ con $f_{i,j} \in \oplus_{k=1}^{m} A \cdot t_k$.

Entonces tenemos que S genera a I. En otras palabras, todo lo que tenemos que saber son las relaciones lineales entre los g_i con coeficientes en A y la representación de cada producto $g_i g_j$ como en elemento de $\oplus_{k=1}^{m} A \cdot g_k$[14]. Veamos la prueba de esta afirmación.

Demostración. Sea J el ideal generado por S. Para un producto p de los t_k sea t_i el elemento maximal con respecto a i de p, el cual es uno de los t_k, y sea $D(p)$ la longitud (número de t_k) de $\dfrac{p}{t_i}$. Probaremos por inducción en $D(p)$ que p es congruente a un elemento de $\bigoplus_{k=1}^{m} At_k$ módulo J.

Si $D(p) = 0$, significa que $p = t_i$, entonces $t_i \equiv t_i \mod J$ con $t_i \in \bigoplus_{k=1}^{m} At_k$. Supongamos que $D(p) > 0$, entonces $p = t_i t_j q$ para algún j. Por la hipótesis de inducción $t_i t_j$ es congruente a un elemento de $\bigoplus_{k=1}^{m} At_k$ módulo J. Además, para todo k tenemos $D(t_k q) = length(q) < D(p)$. Por lo tanto por inducción todo $t_j q$ está en $\bigoplus_{k=1}^{m} At_k$ módulo J, y por lo tanto p también.

Ahora sea $f \in A[t_1, ..., t_m]$ un polinomio en el kernel I de la siguiente aplicación

$$A[t_1, ..., t_m] \to K[V]^G$$

por lo anterior $f \equiv g \mod J$ con $g \in \bigoplus_{k=1}^{m} At_k$, entonces $f - g \in J \subset I$. Como $f \in I$, tenemos, $g \in I$, se sigue que $g \in I \cap \bigoplus_{k=1}^{m} At_k$, de (a) se sigue que $g \in J$, entonces $f \in J$.

□

Capítulo 7

Cálculo de Relaciones

En este capítulo describiremos el conjunto de relaciones del anillo de invariantes $K[V]^G$ de una representación de dimensión finita V bajo la acción de un grupo cíclico de orden p, haremos esto utilizando los diferentes métodos descritos en las secciones anteriores.

7.1. Caso $|G| = p$ y $dim(V) = n$

En esta sección sean G un grupo cíclico de orden p, σ un generador de G, V un $K-$espacio vectorial dimensionalmente finito, $dim(V) = n$ y ξ una raíz p-ésima primitiva de la unidad, en esta situación describiremos las relaciones del anillo de invariantes $K[V]^G$ enfocándonos en los resultados descritos en el Capítulo 6.

Existe una base de V en la que la acción de G sobre V está dada de la siguiente manera

$$A = diag(I_{n_0}, \xi I_{n_1}, ..., \xi^{p-1} I_{n_{p-1}})$$

donde $n_0 + n_1 + ... + n_{p-1} = n = dim(V)$. Entonces tenemos que $K[V] \simeq K[X_{01}, ..., X_{0n_0}, X_{11}, ..., X_{1n_1}, ..., X_{p-11}, ..., X_{p-1n_{p-1}}]$. Escribimos entonces la acción como $\sigma X_{ij} = \xi^i X_{ij}$, con $0 \leq i \leq p-1$ y $1 \leq j \leq n_i$.

Por lo tanto los monomios invariantes de esta acción tienen la forma $\prod_{i,j} X_{ij}^{k_{ij}}$ tales que $\sum_{i,j} ik_{ij} \equiv 0 \mod p$ con $0 \leq i \leq p-1$ y $1 \leq j \leq n_i$. Se sigue

que $\prod_{i,j} X_{ij}^{k_{ij}}$ están en el kernel de la siguiente aplicación.

Sean $H = 1$ y $S(G \setminus H) = \{\sigma, ..., \sigma^{p-1}\}$. $S(G \setminus H)$ junto con H genera a G, consideremos la aplicación

$$\begin{array}{c} \varphi : K[V]^H \to \bigoplus_{\sigma \in S(G\setminus H)} K[V] \\ f \longmapsto (\sigma f - f)_{\sigma \in S(G\setminus H)} \end{array}$$

cuyo kernel es $K[V]^G$, restringiendo a grado d tenemos

$$\varphi_d : K[V]_d^G \to K[V]_d^{|S(G\setminus H)|}$$

cuyo kernel es $K[V]_d^G$. Escribimos entonces

$$ker(\varphi_d) = \left\langle \prod_{i,j} X_{ij}^{k_{ij}} : \sum_{i,j} k_{ij} = d \ , \ \sum ik_{ij} \equiv 0 \mod p \right\rangle.$$

Lema 7.1. *Con la notación anterior. El kernel de la aplicación φ_d está generado por los polinomios invariantes de grado d*

$$ker(\varphi_d) = \left\langle \prod_{i,j} X_{ij}^{k_{ij}} : \sum_{i,j} k_{ij} = d \ , \ \sum ik_{ij} \equiv 0 \mod p \right\rangle.$$

Como $V\left(\left\{X_{ij}^p\right\}_{\substack{0\le i\le p-1 \\ 1\le j\le n_i}}\right) = (0)$ se sigue que $\left\{X_{ij}^p\right\}_{\substack{0\le i\le p-1 \\ 1\le j\le n_i}}$ es un sistema homogéneo de parámetros y entonces es un conjunto de invariantes primarios. Como los invariantes primarios son monomios, entonces son una G-base con el orden lexicográfico del ideal que generan.

Lema 7.2. *Con la notación anterior. $\left\{X_{ij}^p\right\}_{\substack{0\le i\le p-1 \\ 1\le j\le n_i}}$ es un conjunto de invariantes primarios y una G-base con el orden lexicográfico para el ideal generado por ellos. Además*

$$NF_G(\prod_{i,j} X_{ij}^{k_{ij}}) = \begin{cases} \prod X_{ij}^{k_{ij}} & \forall ij \text{ con } k_{ij} < p \\ 0 & si\ \exists ij \text{ con } k_{ij} \ge p \end{cases}$$

respecto a esta G-base.

Ahora describiremos las relaciones de los generadores del anillo de invariantes $K[V]^G$.

Sea $A = K[X_{ij}^p]_{\substack{0\le i\le p-1\\ 1\le j\le n_i}}$ y definamos las siguientes indeterminadas

$$t_{\underline{a}_0\underline{a}_1\cdots\underline{a}_{p-1}}$$

donde $\underline{a}_i = (a_{i1}, ..., a_{in_i})$ con $\sum_{i,j} ia_{ij} \equiv 0 \mod p$ y $0 \le a_{ij} \le p-1$.

Consideremos ahora la siguiente aplicación

$$\begin{aligned}\psi : A[t_{\underline{a}_0\cdots\underline{a}_{p-1}}] &\to K[V]^G\\ t_{\underline{a}_0\cdots\underline{a}_{p-1}} &\longmapsto \prod_{i,j} X_{ij}^{\underline{a}_i}\end{aligned}$$

El número de índices $\underline{a}_0...\underline{a}_{p-1}$ es p^{n-1} y los comparamos como sigue, decimos que $\underline{a}_0...\underline{a}_{p-1} < \underline{a}'_0...\underline{a}'_{p-1}$ si $\underline{a}_i <_{lex} \underline{a}'_i$, o si $\underline{a}_i = \underline{a}'_i$ y $\underline{a}_{i+1} <_{lex} \underline{a}'_{i+1}$, para $i = 0, 1, ..., p-1$.

De acuerdo con la Afirmación (6.6) para cada par $\underline{a}_0...\underline{a}_{p-1}$ y $\underline{a}'_0...\underline{a}'_{p-1}$ con $\underline{a}_0...\underline{a}_{p-1} < \underline{a}'_0...\underline{a}'_{p-1}$ debemos encontrar una relación de la forma

$$t_{\underline{a}_0\cdots\underline{a}_{p-1}}t_{\underline{a}'_0\cdots\underline{a}'_{p-1}} - f_{\underline{a}_0\cdots\underline{a}_{p-1},\underline{a}'_0\cdots\underline{a}'_{p-1}}$$

con $f_{\underline{a}_0\cdots\underline{a}_{p-1},\underline{a}'_0\cdots\underline{a}'_{p-1}} \in \bigoplus_{\underline{b}_0\cdots\underline{b}_{p-1}} K[X_{ij}^p]_{\substack{0\le i\le p-1\\ 1\le j\le n_i}} t_{\underline{b}_0\cdots\underline{b}_{p-1}}$.

Debemos tener entonces

$$\begin{aligned}\psi(f_{\underline{a}_0\cdots\underline{a}_{p-1},\underline{a}'_0\cdots\underline{a}'_{p-1}}) &= \psi(t_{\underline{a}_0\cdots\underline{a}_{p-1}}t_{\underline{a}'_0\cdots\underline{a}'_{p-1}})\\ &= \prod_{i,j} X_{ij}^{\underline{a}_i}\prod_{i,j} X_{ij}^{\underline{a}'_i}\\ &= \prod_{i,j} X_{ij}^{\underline{a}_i+\underline{a}'_i}\end{aligned}$$

donde $\underline{a}_i + \underline{a}'_i = (a_{i1} + a'_{i1}, ..., a_{in_i} + a'_{in_i})$.

Para cada i, j escribimos

$$a_{ij} + a'_{ij} = q_{ij}p + r_{ij} \text{ con } 0 \le r_{ij} \le p-1$$

Sean $\underline{q}_i = (pq_{i1}, ..., pq_{in_i})$ y $\underline{r}_i = (r_{i1}, ..., r_{in_i})$, es claro que $\sum_{i,j} ipq_{ij} \equiv 0 \mod p$ y $\sum_{i,j} ir_{ij} \equiv 0 \mod p$.

Entonces $\prod_{i,j} X_{ij}^{\underline{a}_i + \underline{a'}_i} = \prod_{i,j} X_{ij}^{\underline{q}_i} \prod_{i,j} X_{ij}^{\underline{r}_i}$.

Proposición 7.1. *Bajo las hipótesis anteriores, las relaciones de los generadores del anillo de invariantes $K[V]^G$ para cada par de indices $\underline{a}_0 ... \underline{a}_{p-1}$, $\underline{a'}_0 ... \underline{a'}_{p-1}$ están dadas por*

$$\mathcal{R}_{\underline{a}_0 \cdots \underline{a}_{p-1}, \underline{a'}_0 \cdots \underline{a'}_{p-1}} = t_{\underline{a}_0 \cdots \underline{a}_{p-1}} t_{\underline{a'}_0 \cdots \underline{a'}_{p-1}} - \prod_{i,j} X_{ij}^{\underline{q}_i} t_{\underline{r}_0 \cdots \underline{r}_{p-1}}.$$

7.1.1. Ejemplos

1. Caso $p = 2$ y $dim(V) = n$

Sean V un K-espacio vectorial tal que $dim(V) = n$, G el grupo cíclico de orden 2 y σ un generador para G.

Consideramos la acción

$$G \times V \to V$$

dada por $A = diag(I_{n_0}, \xi I_{n_1})$, donde $n_0 + n_1 = n$ y ξ es una raíz 2-ésima primitiva de la unidad. Tenemos que $K[V] \simeq K[X_{01}, ..., X_{0n_0}, X_{11}, ..., X_{1n_1}]$ y

$$\sigma X_{0j} = X_{0j} \ , \ 1 \leq j \leq n_0$$
$$\sigma X_{1i} = \xi X_{1i}, \ 1 \leq i \leq n_1.$$

Los invariantes de esta acción tienen la forma $\prod X_{ij}^{k_{ij}}$ tal que $\sum ik_{ij} \equiv 0$ mód 2.

Luego del Lema (7.2) se sigue que $\left\{X_{ij}^2\right\}$ donde $0 \leq i \leq 1$ y $1 \leq j \leq n_i$ es un conjunto de invariantes primarios.

El número de invariantes secundarios es $m = \frac{2^n}{2} = 2^{n-1}$ (ver Apéndice B). Calculemos entonces los invariantes secundarios con el Algoritmo 6.3.

- Tenemos que $G = \left\{X_{ij}^2\right\}$ es una $G-$base con el orden lexicográfico para el ideal generado por los invariantes primarios.

- Calcular los grados de los invariantes secundarios comparando la serie de Hilbert (ecuación (3.1)) con la fórmula de Molien.

  De la fórmula de Molien tenemos

$$\begin{aligned} H(K[V]^G,t) &= \frac{1}{2}\left(\frac{1}{(1-t)^{n_0}(1+t)^{n_1}}+\frac{1}{(1-t)^{n_0+n_1}}\right) \\ &= \frac{1}{2}\left(\frac{(1-t)^{n_0+n_1}+(1-t)^{n_0}(1+t)^{n_1}}{(1-t)^{n_0+n_0+n_1}(1+t)^{n_1}}\right) \\ &= \frac{1}{2}\left(\frac{(1-t)^{n_1}+(1+t)^{n_1}}{(1-t)^{n_0+n_1}(1+t)^{n_1}}\right) \end{aligned}$$

  Comparamos con la serie de Hilbert (ecuación (3.1)) y obtenemos

$$\frac{1}{2}\left(\frac{(1-t)^{n_1}+(1+t)^{n_1}}{(1-t)^{n_0+n_1}(1+t)^{n_1}}\right)=\frac{\sum_{j=1}^{2^{n-1}} t^{e_j}}{(1-t^2)^n}$$

  entonces tenemos

$$\begin{gathered} \tfrac{1}{2}\left(\frac{(1-t)^{n_1}+(1+t)^{n_1}}{(1-t)^{n_0+n_1}(1+t)^{n_1}}\right)(1-t)^n(1+t)^n=\sum_{j=1}^{2^{n-1}} t^{e_j} \\ \tfrac{1}{2}\left((1-t)^{n_1}+(1+t)^{n_1}\right)(1+t)^{n_0}=\sum_{j=1}^{2^{n-1}} t^{e_j} \end{gathered}$$

  Observemos en el lado izquierdo de la igualdad anterior lo siguiente:

$$(1-t)^{n_1}=\sum_{k=0}^{n_1}\tbinom{n_1}{k}(-t)^k,\ (1+t)^{n_1}=\sum_{k=0}^{n_1}\tbinom{n_1}{k}t^k \text{ y } (1+t)^{n_0}=\sum_{l=0}^{n_0}\tbinom{n_0}{l}t^l.$$

  Entonces

$$\begin{aligned} (1-t)^{n_1}+(1+t)^{n_1} &= (1-t)^{n_1}=\sum_{k=0}^{n_1}\binom{n_1}{k}(-t)^k+\sum_{k=0}^{n_1}\binom{n_1}{k}t^k \\ &= \begin{cases} 2\sum_{k=0}^{\frac{n_1-1}{2}}\tbinom{n_1}{2k}t^{2k} & si\ n_1\ es\ impar \\ 2\sum_{k=0}^{\frac{n_1}{2}}\tbinom{n_1}{2k}t^{2k} & si\ n_1\ es\ par \end{cases} \end{aligned}$$

luego para n_1 impar el polinomio $\sum_{j=1}^{2^{n-1}} t^{e_j}$ está dado por:

$$\begin{aligned}\sum_{j=1}^{2^{n-1}} t^{e_j} &= \tfrac{1}{2}\left(2\sum_{k=0}^{\frac{n_1-1}{2}}\tbinom{n_1}{2k}t^{2k}\right)\left(\sum_{l=0}^{n_0}\tbinom{n_0}{l}t^{l}\right)\\ &= \left(\sum_{k=0}^{\frac{n_1-1}{2}}\tbinom{n_1}{2k}t^{2k}\right)\left(\sum_{l=0}^{n_0}\tbinom{n_0}{l}t^{l}\right)\end{aligned}$$

Se sigue que:

$$\begin{aligned}\sum_{j=1}^{2^{n-1}} t^{e_j} &= 1+n_0t+\left(\binom{n_1}{0}\binom{n_0}{2}+\binom{n_1}{2}\binom{n_0}{0}\right)t^2\\ &+ \left(\binom{n_1}{0}\binom{n_0}{3}+\binom{n_1}{2}\binom{n_0}{1}\right)t^3\\ &+ \left(\binom{n_1}{0}\binom{n_0}{4}+\binom{n_1}{2}\binom{n_0}{2}+\binom{n_1}{4}\binom{n_0}{0}\right)t^4\\ &+ \left(\binom{n_1}{0}\binom{n_0}{5}+\binom{n_1}{2}\binom{n_0}{3}+\binom{n_1}{4}\binom{n_0}{1}\right)t^5\\ &+ \left(\binom{n_1}{0}\binom{n_0}{6}+\binom{n_1}{2}\binom{n_0}{4}+\binom{n_1}{4}\binom{n_0}{2}+\binom{n_1}{6}\binom{n_0}{0}\right)t^6\\ &+ \ldots+\binom{n_1}{\frac{n_1-1}{2}}t^{n_1-1+n_0}\end{aligned}$$

Análogamente, para el caso n_1 par, tenemos que el polinomio está dado como sigue:

$$\begin{aligned}\sum_{j=1}^{2^{n-1}} t^{e_j} &= 1 + n_0 t + \left(\binom{n_1}{0}\binom{n_0}{2} + \binom{n_1}{2}\binom{n_0}{0}\right) t^2 \\ &+ \left(\binom{n_1}{0}\binom{n_0}{3} + \binom{n_1}{2}\binom{n_0}{1}\right) t^3 \\ &+ \left(\binom{n_1}{0}\binom{n_0}{4} + \binom{n_1}{2}\binom{n_0}{2} + \binom{n_1}{4}\binom{n_0}{0}\right) t^4 \\ &+ \left(\binom{n_1}{0}\binom{n_0}{5} + \binom{n_1}{2}\binom{n_0}{3} + \binom{n_1}{4}\binom{n_0}{1}\right) t^5 \\ &+ \left(\binom{n_1}{0}\binom{n_0}{6} + \binom{n_1}{2}\binom{n_0}{4} + \binom{n_1}{4}\binom{n_0}{2} + \binom{n_1}{6}\binom{n_0}{0}\right) t^6 \\ &+ \ldots + \binom{n_1}{\frac{n_1}{2}} t^{n_1+n_0}\end{aligned}$$

Vemos entonces que en ambos casos el coeficiente de la k-ésima potencia es:

$$\sum_{l=0}^{\frac{k}{2}} \tbinom{n_1}{2l}\tbinom{n_0}{k-2l} t^k \text{ si } k \text{ es par, o}$$
$$\sum_{l=0}^{\frac{k-1}{2}} \tbinom{n_1}{2l}\tbinom{n_0}{k-2l} t^k \text{ si } k \text{ es impar}$$

para $k = 1, ..., n_1 - 1 + n_0$ si n_1 es par, y $k = 1, ..., n_1 + n_0$ si n_1 es par.

- Calculemos ahora una base para la componente homogénea $K[V]_k^G$, para $k = 0$ tenemos que $K[V]_0^G = K$. Para $k = 1$, $K[V]_1^G = \{X_{0j}\}_{j=1,...,n_0}$.

  Del Lema (7.1) se sigue que

$$ker(\varphi_l) = \left\langle \prod_{i=0,1 j=n_0,n_1} X_{ij}^{k_{ij}} : \sum k_{ij} = l \ y \ \sum i k_{ij} \equiv 0 \mod 2 \right\rangle$$

- Sabemos que $G = \left\{ \prod_{i=0,1 j=n_0,n_1} X_{ij}^{k_{ij}} \right\}$ es una $G-$base con el orden lexicográfico para el ideal generado por los invariantes primarios, del Lema

(7.2) tenemos que $NF_G\left(\prod_{i=0,1 j=n_0,n_1} X_{ij}^{k_{ij}}\right) = \prod_{i=0,1 j=n_0,n_1} X_{ij}$.

Ahora estamos interesados en encontrar las relaciones del conjunto de generadores de $K[V]^G$.

Sea $A = K[X_{ij}^2]$, con $0 \leq i \leq 1$, $1 \leq j \leq n_i$, definimos las siguientes indeterminadas $t_{\underline{a}_0\underline{a}_1}$, donde $\underline{a}_i = (a_{i1}, ..., a_{in_0})$ con $\sum_{i,j} i a_{ij} \equiv 0 \mod 2$ y $0 \leq a_{ij} \leq 1$.

Consideremos entonces la aplicación

$$\psi : A[t_{\underline{a}_0\underline{a}_1}] \to K[V]^G$$
$$t_{\underline{a}_0\underline{a}_1} \mapsto \prod_j X_{0j}^{\underline{a}_0} \prod_j X_{1j}^{\underline{a}_1}$$

Por lo tanto tenemos de la Proposición (7.1) que las relaciones para cada par $\underline{a}_0\underline{a}_1$ y $\underline{a'}_0\underline{a'}_1$ están dadas por:

$$\mathcal{R}_{\underline{a}_0\underline{a}_1,\underline{a'}_0\underline{a'}_1} = t_{\underline{a}_0\underline{a}_1} t_{\underline{a'}_0\underline{a'}_1} - \prod_j X_{0j}^{\underline{q}_0} \prod_j X_{1j}^{\underline{q}_1} t_{\underline{r}_0\underline{r}_1}.$$

2. Caso $p = 2$ **y** $dim(V) = 2$

1) Calculemos un conjunto de generadores del anillo de invariantes usando el método descrito en el Capítulo 4.

Sea G un grupo cíclico de orden $p = 2$ y $V = V_b \oplus V_c$ una representación 2-dimensional de G. Tenemos entonces que $K[V] \simeq K[x, y]$. Sea ξ una raíz 2-ésima primitiva de la unidad, tenemos entonces que la acción de G sobre $K[V]$ está dada por

$$\sigma x = -x$$
$$\sigma y = y$$

con σ un generador para G.

Luego los monomios invariantes son $x^k y^l$ tales que $k + 2l \equiv 0 \mod 2$. De esto se sigue que k debe ser un número par o cero y $l \in \mathbb{N}$, así que el conjunto de generadores para $K[V]^G$ es:

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

Describir el conjunto de relaciones siguiendo este método no es posible pues debemos considerar $p \geq 3$.

2) Ahora calculemos un conjunto de generadores, así como las relaciones entre ellos usando los resultados del Capítulo 6.

Tenemos que la acción de G sobre $K[V]$ está dada por la siguiente matriz:

$$A = diag(I_{n_0}, \xi I_{n_1})$$

con $n_0 + n_1 = 2$, en este caso $n_0 = 1$ y $n_1 = 1$.

Luego del Lema (7.2) se sigue que $\{x^2, y^2\}$ es un conjunto de invariantes primarios.

El número de invariantes secundarios es $m = 2$. Ahora calculemos los invariantes secundarios usando el Algoritmo 6.3.

- Tenemos que $G = \{x^2, y^2\}$ con el orden lexicográfico es una G-base para el ideal $I = \langle x^2, y^2 \rangle$.
- Calculemos los grados e_1, e_2 de los invariantes secundarios, de la

fórmula de Molien tenemos:

$$\begin{aligned} H(K[V]^G,t) &= \frac{1}{2}\left(\frac{1}{(1-t)(1-\xi t)}+\frac{1}{(1-t)^2}\right) \\ &= \frac{1}{2}\left(\frac{1}{(1-t)(1+t)}+\frac{1}{(1-t)^2}\right) \\ &= \frac{1}{2}\left(\frac{1}{(1-t^2)}+\frac{1}{(1-t)^2}\right) \\ &= \frac{1}{2}\left(\frac{(1-t)^2+(1-t^2)}{(1-t^2)(1-t)^2}\right) \\ &= \frac{1}{2}\left(\frac{1-t+1+t}{(1+t)(1-t)^2}\right) \\ &= \frac{1}{2}\left(\frac{2}{(1+t)(1-t)^2}\right) \\ &= \frac{1}{(1+t)(1-t)^2} \end{aligned}$$

comparando con la serie (ecuación (3.1)) tenemos

$$\frac{1}{(1+t)(1-t)^2} = \frac{t^{e_1}+t^{e_2}}{(1-t^2)^2}$$

se sigue que

$$\frac{(1-t^2)(1-t^2)}{(1+t)(1-t)^2} = \frac{(1-t)^2(1+t)^2}{(1+t)(1-t)^2} = 1-t$$

así tenemos que $1+t = t^{e_1}+t^{e_2}$, de donde, $e_1 = 0$ y $e_2 = 1$.

- Ahora calculemos una base de las componentes homogéneas $K[V]_0^G$ y $K[V]_1^G$.
  Sea $H = 1$ y $S(G \setminus H) = \{\sigma\}$, entonces $S(G \setminus H)$ junto con H genera a G, consideremos el homomorfismo

$$\begin{gathered} \phi_i : K[V]_{e_i}^H \to K[V]_{e_i} \\ f \mapsto \sigma f - f,\ \sigma \in S(G \setminus H) \end{gathered}$$

  cuyo kernel es $K[V]_{e_i}^G$. Entonces tenemos que

$$\ker(\phi_0) = K \text{ y } \ker(\phi_1) = \{y\}.$$

- Seleccionamos un elemento g_i de estas bases tal que su forma normal $NF_G(g_i)$ no esté contenida en el K-espacio vectorial generado por $NF_G(g_1)$, ..., $NF_G(g_{i-1})$.

  Tenemos entonces que los invariantes secundarios son $\{1, y\}$.

Ahora encontremos las relaciones de los generadores.

Sea $A = K[x^2, y^2]$, y consideremos

$$\begin{aligned} \varphi : A[t_1, t_2] &\to K[V]^G \\ t_1 &\mapsto 1 \\ t_2 &\mapsto y \end{aligned}$$

Entonces para cada $1 \leq i \leq j \leq 2$ debemos encontrar una relación de la forma $t_i t_j - f_{i,j}$ con $f_{i,j} \in K[x^2, y^2]t_1 \oplus K[x^2, y^2]t_2$.

Para $t_1 t_2$, necesitamos $f_{1,2}$ tal que $\varphi(t_1 t_2 - f_{1,2}) = 0$, entonces $\varphi(f_{1,2}) = y$, se sigue que $f_{1,2} = t_2 = 0t_1 + 1t_2$.

Para $t_1 t_1$, necesitamos $f_{1,1}$ tal que $\varphi(t_1 t_1 - f_{1,1}) = 0$, entonces $\varphi(f_{1,1}) = 1$, se sigue que $f_{1,1} = t_1 = 1t_1 + 0t_2$.

Para $t_2 t_2$, necesitamos $f_{2,2}$ tal que $\varphi(t_1 t_2 - f_{2,2}) = 0$, entonces $\varphi(f_{2,2}) = y^2$, se sigue que $f_{2,2} = y^2 t_1 + 0t_2$.

Se sigue que el conjunto de relaciones de $K[V]^G$ en $K[x^2, y^2][t_1, t_2]$ es generado por

$$\{t_1^2 - t_1, t_1 t_2 - t_2, t_2^2 - y^2 t_1\}.$$

3) Método de G-bases (eliminación)

Hemos calculado con los métodos anteriores los generadores para el anillo de invariantes $K[V]^G$ los cuales son $\{x^2, y\}$. Ahora consideremos la siguiente aplicación:

$$\psi : K[t_1, t_2] \to A = K[x^2, y]$$
$$t_1 \mapsto x^2$$
$$t_2 \mapsto y$$

Notemos que $A = K[x^2, y] = K[x, y]/(x - x^2)$. Entonces de la Proposición (1.1) tenemos que si definimos $J := ((x - x^2) \cup x^2 - t_1, y - t_2)$, $ker(\psi) = K[t_1, t_2] \cap J$, esto es $ker(\psi)$ es un ideal de $\{t_1, t_2\}$-eliminación.

La ejecución en SINGULAR [8] es la siguiente

> ring $r = 0$, $(x, y, t(1), t(2))$, lp;
> poly $f1 = x^2$;
> poly $f2 = y$;
> poly $f3 = x - x^2$;
> ideal $i = f1 - t(1), f2 - t(2)$;
> ideal $j = f3, i$;
> j;
$j[1] = -x^2 + x$
$j[2] = x^2 - t(1)$
$j[3] = y - t(2)$
> ideal e=eliminate(j, xy);
> e;
$e[1] = t(1)^2 - t(1)$
> ideal g=groebner(e);
> g;
$g[1] = t(1)^2 - t(1)$
> ideal k=eliminate(g, xy);
> k;
$k[1] = t(1)^2 - t(1)$

Entonces tenemos que el conjunto de relaciones de $K[V]^G$ en $K[t_1, t_2]$ es generado por $t_1^2 - t_1$.

3. Caso $p = 3$ **y** $dim(V) = 2$

1) Usaremos el método del Capítulo 4 para encontrar un conjunto de generadores y las relaciones entre ellos.

Sea G un grupo cíclico de orden $p = 3$ y $V = V_b \oplus V_c$ una representación 2-dimensional de G. Tenemos entonces que $K[V] \simeq K[x, y]$. Sea ξ una raíz 3-ésima primitiva de la unidad, consideremos la siguiente acción de G sobre $K[V]$

$$\sigma x = \xi x$$
$$\sigma y = \xi^2 y$$

con σ un generador para G.

Luego los invariantes consisten de monomios $u_i = x^{k_i} y^{l_i}$ tales que $k_i + 2l_i \equiv 0 \mod 3$.

Tenemos que $k_1 = \frac{3}{mcd(3,1)} = 3$, entonces $3 + 2l_1 \equiv 0 \mod 3$ así que $l_1 = 0$, se sigue que $u_1 = x^3$.

Luego debemos tener que $k_1 = 3 > k_2 > k_3 > ...$ y $0 = l_1 < l_2 < l_3 < ....$, así que $k_2 = 2, 1, 0$ y $l_2 = 1, 2, 3$.

Si $k_2 = 2$ entonces $2 + 2l_2 \equiv 0 \mod 3$, así que $l_2 = 2$ y $u_2 = x^2 y^2$

Si $k_2 = 1$ tenemos $1 + 2l_2 \equiv 0 \mod 3$, y entonces $l_2 = 1$ y $u_2 = xy$.

Como buscamos un conjunto minimal de generadores y dado que $x^2 y^2 = (xy)^2$ tenemos que $u_2 = xy$.

Por otro lado $l_m = \frac{3}{mcd(3,2)} = 3$, entonces $0 = l_1 < 1 = l_2 < l_3$, se sigue que $l_3 = 3$ y entonces $k_3 = 0$, de donde $u_3 = y^3$. Por lo tanto el conjunto de generadores es

$$\{x^3, xy, y^3\}$$

Encontremos ahora las relaciones entre estos generadores. Consideremos la sucesión exacta corta:

$$0 \to J \to K[U_1, U_2, U_3] \to^{\pi} K[V]^G \to 0$$

con U_i indeterminadas, J el ideal de relaciones de $K[V]^G$ y $\pi(U_1) = x^3$, $\pi(U_2) = xy$ y $\pi(U_3) = y^3$.

Para cada par i, j con $1 \leq i, j \leq 3$ y $j - i \geq 2$ consideremos el producto $u_i u_j \in K[V]^G$. Así que sólo consideramos $i = 1$ y $j = 3$, entonces tenemos lo siguiente.

$u_1 u_3 = x^3 y^3 \in K[V]^G$, el monomio $u_2 = xy$ divide propiamente a $u_1 u_3$, definimos ahora $\alpha := \frac{u_1 u_3}{u_2} = \frac{x^3 y^3}{xy} = x^2 y^2$, podemos escribir entonces $\alpha = u_1^0 u_2^2 u_3^0$.

Se sigue que la relación es: $R_{13} = U_1 U_3 - U_2 U_2^2 = U_1 U_3 - U_2^3$.

2) Ahora usaremos los resultados del Capítulo 6 para encontrar generadores y las relaciones del anillo de invariantes.

Tenemos que la acción de G sobre $K[V]$ esta dada por la siguiente matriz

$$A = diag(I_{n_0}, \xi I_{n_1}, \xi^2 I_{n_2})$$

con $n_0 + n_1 + n_2 = 2$, en este caso $n_0 = 1$, $n_1 = 1$ y $n_2 = 2$.

Luego del Lema (7.2) se sigue que $\{x^3, y^3\}$ es un conjunto de invariantes primarios.

El número de invariantes secundarios es $m = 3$ (ver apéndice B). Ahora calculemos los invariantes secundarios usando el Algoritmo 6.3.

- Tenemos que $G = \{x^3, y^3\}$ con el orden lexicográfico es una G-base para el ideal $I = \langle x^3, y^3 \rangle$.
- Calculemos los grados e_1, e_2, e_3 de los invariantes secundarios, de la

fórmula de Molien tenemos:

$$\begin{aligned} H(K[V]^G,t) &= \frac{1}{3}\left(\frac{1}{(1-t)^0(1-\xi t)(1-\xi^2 t)}\right. \\ &+ \left.\frac{1}{(1-t)^0(1-\xi^2 t)(1-\xi t)}+\frac{1}{(1-t)^2}\right) \\ &= \frac{1}{3}\left(\frac{2}{(t^2+t+1)}+\frac{1}{(1-t)^2}\right) \\ &= \frac{1}{3}\left(\frac{2(1-t)^2+(t^2+t+1)}{(t^2+t+1)(1-t^2)}\right) \\ &= \frac{1}{3}\left(\frac{2-4t+2t^2+t^2+t+1}{(t^2+t+1)(1-t)^2}\right) \\ &= \frac{1-t+t^2}{(t^2+t+1)(1-t)^2} \end{aligned}$$

comparando con la serie (ecuación (3.1)) tenemos

$$\frac{1-t+t^2}{(t^2+t+1)(1-t)^2}=\frac{t^{e_1}+t^{e_2}+t^{e_3}}{(1-t^3)^2}$$

se sigue que

$$\frac{(t^2+t+1)(1-t)^2(1-t+t^2)}{(t^2+t+1)(1-t)^2}=t^{e_1}+t^{e_2}+t^{e_3}$$

así tenemos que $1+t^2+t^4=t^{e_1}+t^{e_2}+t^{e_3}$, de donde, $e_1=0$, $e_2=2$ y $e_3=4$.

- Calculemos una base de las componentes homogéneas $K[V]_0^G$, $K[V]_2^G$ y $K[V]_4^G$.

  Sea $H=1$ y $S(G\setminus H)=\{\sigma\}$, entonces $S(G\setminus H)$ junto con H genera a G, consideremos el homomorfismo

  $$\begin{gathered} \phi_i : K[V]_{e_i}^H \to K[V]_{e_i} \\ f \mapsto \sigma f - f,\ \sigma \in S(G\setminus H) \end{gathered}$$

  cuyo kernel es $K[V]_{e_i}^G$. Entonces tenemos que $\ker(\phi_0)=K$, $\ker(\phi_2)=\{xy\}$ y $\ker(\phi_4)=\{x^2y^2\}$.

- Seleccionamos un elemento g_i de estas bases tal que su forma normal $NF_G(g_i)$ no está contenida en el K-espacio vectorial generado por

$NF_G(g_1)$, ..., $NF_G(g_{i-i})$.

Tenemos entonces que los invariantes secundarios son $\{1, xy, x^2y^2\}$.

Ahora encontremos las relaciones de los generadores.

Sea $A = K[x^3, y^3]$, y consideremos

$$\begin{gathered}\varphi : A[t_1, t_2, t_3] \to K[V]^G \\ t_1 \mapsto 1 \\ t_2 \mapsto xy \\ t_3 \mapsto x^2y^2\end{gathered}$$

Entonces para cada $1 \leq i \leq j \leq 3$ debemos encontrar una relación de la forma $t_it_j - f_{i,j}$ con $f_{i,j} \in K[x^3, y^3]t_1 \oplus K[x^3, y^3]t_2 \oplus K[x^3, y^3]t_3$.

Para t_1t_2, necesitamos $f_{1,2}$ tal que $\varphi(t_1t_2 - f_{1,2}) = 0$, entonces $\varphi(f_{1,2}) = xy$, se sigue que $f_{1,2} = t_2 = 0t_1 + 1t_2 + 0t_3$.

Para t_1t_1, necesitamos $f_{1,1}$ tal que $\varphi(t_1t_1 - f_{1,1}) = 0$, entonces $\varphi(f_{1,1}) = 1$, se sigue que $f_{1,1} = t_1 = 1t_1 + 0t_2 + 0t_3$.

Para t_2t_2, necesitamos $f_{2,2}$ tal que $\varphi(t_2t_2 - f_{2,2}) = 0$, entonces $\varphi(f_{2,2}) = x^2y^2$, se sigue que $f_{2,2} = 0t_1 + 0t_2 + 1t_3$.

Para t_1t_3, necesitamos $f_{1,3}$ tal que $\varphi(t_1t_3 - f_{1,3}) = 0$, entonces $\varphi(f_{1,3}) = x^2y^2$, se sigue que $f_{1,3} = 0t_1 + 0t_2 + 1t_3$.

Para t_2t_3, necesitamos $f_{2,3}$ tal que $\varphi(t_2t_3 - f_{2,3}) = 0$, entonces $\varphi(f_{2,3}) = x^3y^3$, se sigue que $f_{2,3} = x^3y^3t_1 + 0t_2 + 0t_3$.

Para t_3t_3, necesitamos $f_{3,3}$ tal que $\varphi(t_3t_3 - f_{3,3}) = 0$, entonces $\varphi(f_{3,3}) = x^4y^4$, se sigue que $f_{3,3} = 0t_1 + x^3y^3t_2 + 0t_3$.

Se sigue que el conjunto de relaciones de $K[V]^G$ en $K[x^3, y^3][t_1, t_2, t_3]$ es generado por:

$$\{t_1^2 - t_1, t_1t_2 - t_2, t_2^2 - t_3, t_1t_3 - t_3, t_2t_3 - x^3y^3t_1, t_3^2 - x^3y^3t_2\}.$$

3) Método de G-bases (eliminación)

Hemos calculado con los métodos anteriores los generadores para el anillo de invariantes $K[V]^G$ los cuales son $\{x^3, xy, y^3\}$. Ahora consideremos la siguiente aplicación

$$\begin{gathered}\psi : K[t_1, t_2, t_3] \to A = K[x^3, xy, y^3] \\ t_1 \mapsto x^3 \\ t_2 \mapsto xy \\ t_3 \mapsto y^3\end{gathered}$$

Veamos cuales son las relaciones del conjunto de generadores. Usaremos la siguiente ejecución en SINGULAR [8]:

> ring $r = 0$, $(x, y, t(1), t(2), t(3))$, lp;
> poly $f1 = x^3$;
> poly $f2 = x * y$;
> poly $f3 = y^3$;
> ideal $i = f1 - t(1), f2 - t(2), f3 - t(3)$;
> ideal e=eliminate(i, xy);
> e;
$e[2] = t(1) * t(3) - t(2)^3$

Entonces tenemos que el conjunto de relaciones de $K[V]^G$ en $K[t_1, t_2]$ esta dado por $\langle t_2^3 - t_2, t_1t_3 - t_2^3 \rangle$.

Apéndice A

Ideal Tórico

Estudiaremos un caso especial de ideales en $K[X] := K[x_1, ..., x_n]$. Fijemos un subconjunto $\mathcal{A} = \{a_1, ..., a_n\}$ de $\mathbb{Z}^d$. Cada vector a_i es identificado con un monomio t^{a_i} en el anillo de polinomios de Laurent $K[t^{\pm 1}] := K[t_1, ..., t_d, t_1^{-1}, ..., t_d^{-1}]$. Considerar el homomorfismo de semigrupo

$$\begin{gathered}\pi : \mathbb{N}^n \to \mathbb{Z}^d \\ u = (u_1, ..., u_n) \mapsto u_1 a_1 + ... + u_n a_n.\end{gathered}$$

La imagen de π es el semigrupo

$$\mathbb{N}\mathcal{A} = \{\lambda_1 a_1 + ... + \lambda_n a_n : \lambda_1, ..., \lambda_n \in \mathbb{N}\}.$$

Luego podemos considerar el siguiente homomorfismo

$$\begin{gathered}\bar{\pi} : K[x] \to K[t^{\pm 1}] \\ x_i \mapsto t^{a_i}.\end{gathered}$$

El kernel de $\bar{\pi}$ es denotado por $I_{\mathcal{A}}$ y se llama el *ideal tórico* de $\mathcal{A}$. Claramente $I_{\mathcal{A}}$ es un ideal primo, y por lo tanto su variedad afín $V(I_{\mathcal{A}})$ de ceros en K^n es irreducible. Esto es la cerradura de Zariski del conjunto de puntos $(t^{a_1}, ..., t^{a_n})$, donde $t \in (K^\star)^d$, aquí $K^\star$ denota $K \setminus \{0\}$. El grupo multiplicativo $(K^\star)^d$ es llamado el toro (d-dimensional algebraico). Una variedad de la forma $V(I_{\mathcal{A}})$ es una variedad afín tórica. El siguiente lema da un conjunto infinito de generadores para un ideal tórico [24].

Lema A.1. *El ideal tórico I_A es generado como un k-espacio vectorial por el conjunto de binomios*

$$\ker(\bar{\pi}) = \{x^u - x^v : u, v \in \mathbb{N}^n, \pi(u) = \pi(v)\}.$$

Demostración. Un binomio $x^u - x^v \in \ker(\bar{\pi})$ si y sólo si $\pi(u) = \pi(v)$, entonces si $x^u - x^v \in \ker(\bar{\pi})$ entonces $\pi(u) = \pi(v)$.

Supongamos que $\pi(u) = \pi(v)$ y fijemos un orden $<$ en $K[x_1, ..., x_n]$, supongamos además que $f \in \ker(\bar{\pi})$ no puede ser escrito como una combinación k-lineal de estos binomios tal que $LM(f) = x^u$ es minimal con respecto al orden. En particular $t^{\pi(u)} = \bar{\pi}(x^u)$ se cancela en esta expresión pues de lo contrario $f(t^{a_1}, ..., t^{a_n}) \neq 0$, por lo tanto hay algún otro monomio x^v que aparece en f, tal que $x^v < x^u$ y $\pi(u) = \pi(v)$.

Tampoco el polinomio $f' := f - x^u + x^v$ puede ser escrito como una K-combinación lineal de binomios en $\ker(\bar{\pi})$, se sigue que $f' \in \ker(\bar{\pi})$, pero $LM(f') < LM(f)$, lo cual es una contradicción pues $LM(f)$ es mínimo con esta propiedad.

Por lo tanto

$$\ker(\bar{\pi}) = \{x^u - x^v : u, v \in \mathbb{N}^n, \pi(u) = \pi(v)\}.$$

□

Apéndice B

Número de Invariantes Secundarios

Para calcular el número de invariantes secundarios consideremos la definición de la serie de Hilbert del anillo de invariantes y la fórmula de Molien.

Sean $d_i = deg(f_i)$ donde f_i $i = 1, ..., n$ son los invariantes primarios y $e_j = deg(g_j)$ con g_j $j = 1, ..., m$ los invariantes secundarios. Entonces tenemos

$$\frac{1}{|G|} \sum_{\pi \in G} \frac{1}{det(I_n - t\pi)} = \frac{\sum_{j=1}^{m} t^{e_j}}{\prod_{i=1}^{n} (1 - t^{d_i})}$$

multiplicando por $(1-t)^n$ tenemos

$$\frac{1}{|G|} \sum_{\pi \in G} \frac{(1-t)^n}{det(I_n - t\pi)} = \frac{\sum_{j=1}^{m} t^{e_j}}{\prod_{i=1}^{n} (1 + t + t^2 + ... + t^{d_i - 1})}$$

Ahora tomamos el límite cuando $t \to 1$.

Observamos que en $\frac{(1-t)^n}{det(I_n - t\pi)}$ todos los sumandos convergen a cero, excepto en el sumando cuando $\pi = Id$, para este sumando obtenemos que el límite es 1, entonces para el lado izquierdo, obtenemos que converge a $\frac{1}{|G|}$, y

el lado derecho a $\frac{m}{d_1 \cdot ... \cdot d_n}$.

Se sigue que:

$$m = \frac{d_1 \cdot ... \cdot d_n}{|G|}.$$

Bibliografía

[1] Adams, William W and Loustaunau, Philippe, An introduction to Gröbner bases, *American Mathematical Soc.*, Graduate Studies in Mathematics vol. 3, (1994).

[2] Benson, David J, Polynomial invariants of finite groups, *Cambridge University Press* **(190)** (1993).

[3] Buchberger, Bruno, Bruno Buchberger PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal, *Journal of symbolic computation, Elsevier* **(3)** (2006) 41, 475-511.

[4] Campbell, HEA and Harris, JC and Wehlau, David L, Internal Duality for Resolution of Rings,*Journal of Algebra* **(1)** (1999) vol. 215, 1-33.

[5] Cox, David and Little, John and O'shea, Donal, Ideals, varieties and algorithms, *Springer* (1992).

[6] Derksen, Harm and Kemper, Gregor, Computational invariant theory, *Springer Science & Business Media* (2013) vol. 130.

[7] Eisenbud, David, Commutative Algebra: with a view toward algebraic geometry, *Springer- Verlag, New York* (1995).

[8] Gerrt-Martin, Greuel, Gerhard Pfister, Hannes Schönemann,Singular version 1.2 user manual, *Reports On Computer Algebra* **(21)**, Centre for Computer Algebra, University of Kaiserslautern, (1998), available at http://www.mathematik.uni-kl.de/∼zca/Singular.

[9] Harris, John C. and Wehlau, David L., Resolutions of 2 and 3 dimensional rings of invariants for cyclic groups, *Communications in Algebra* **(11)** (2013) vol. 41, 4278-4289.

[10] Hilbert, David and Sturmfels, Bernd, Theory of algebraic invariants, *Cambridge University Press* (1993).

[11] James, Gordon and Liebeck, Martin W, Representations and characters of groups, *Cambridge University Press* (2001).

[12] Kemper, Gregor, An algorithm to calculate optimal homogeneous systems of parameters, *Journal of Symbolic Computation* **(2)** (1999) vol. 27, 171-184.

[13] Kemper, Gregor, A course in Commutative Algebra, *Springer Science & Business Media* (2010) vol. 256.

[14] Kemper, Gregor and Steel, Allan, Some algorithms in invariant theory of finite groups, in *Computational methods for representations of groups and algebras Springer* (1999),267-285.

[15] Mishra, Bhubaneswar, Algorithmic algebra, *Springer Science & Business Media* (2012).

[16] Mukai, Shigeru and Oxbury, WM, An introduction to invariants and moduli, *Cambridge University Press* (2003) vol. 81.

[17] Mumford, David, The red book of varieties and schemes: includes the Michigan lectures (1974) on curves and their Jacobians, *Springer Science & Business Media*, (1999) 1358.

[18] Noether, Emmy, Der endlichkeitssatz der invarianten endlicher gruppen, *Mathematische Annalen, Springer* **(1)** (1915) 77, 89-92.

[19] Noether, Emmy, Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p, *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* (1926), 28-35.

[20] Reiner, Victor and Smith, Larry, Systems of parameters for rings of invariants, *preprint, Göttingen* (1996).

[21] Serre, Jean-Pierre, Linear representations of finite groups, *Springer-Verlag, New York* (1977).

[22] Stanley, Richard P, Invariants of finite groups and their applications to combinatorics, *Bulletin of the American Mathematical Society* **(3)** (1979) 1, 475-511.

[23] Sturmfels, Bernd, Algorithms in invariant theory, *Springer- Verlag, Wien, New York* (1993).

[24] Sturmfels, Bernd, Gröbner bases and convex polytopes, *American Mathematical Soc.* (1996) vol. 8.