Universidad de **Valladolid**

Facultad de Ciencias

Trabajo fin de grado

Grado en Matemáticas

TEORÍA DE INVARIANTES DE GRUPOS FINITOS

Autora: Sara Aguado Delgado
Tutor: Santiago Encinas Carrión
2023-2024

Resumen: En este trabajo se aborda un estudio sobre la teoría de invariantes de grupos finitos y se incluye una revisión de conceptos básicos de álgebra conmutativa necesarios para el desarrollo de los resultados de interés. Entre estos resultados se destacan los teoremas que relacionan el anillo invariante con un anillo de polinomios, los conceptos relacionados con el álgebra simétrica, el desarrollo de las series de Hilbert y la fórmula de Molien y, finalmente el teorema de Shephard-Todd.

Palabras clave: Representaciones de grupos, anillo invariante, cota de Noether, fórmula de Molien, pseudorreflexiones, teorema de Shephard-Todd.

Abstract: In this work, a study on the theory of invariants of finite groups is presented, including a review of basic concepts in commutative algebra necessary for the development of the relevant results. Among these results, notable highlights include theorems that relate the invariant ring to a polynomial ring, concepts related to the symmetric algebra, the development of Hilbert series and Molien's formula, and finally, the Shephard-Todd theorem.

Keywords: Group representations, invariant ring, Noether's bound, Molien's formula, pseudoreflections, Shephard-Todd's theorem.

Índice general

Capítulo 1

Introducción

La teoría de invariantes es una rama del álgebra abstracta que nació como resultado de la curiosidad humana de obtener una descripción explícita de expresiones polinómicas que se mantenían intactas, o invariantes, ante las transformaciones de un grupo lineal.

Los primeros estudios sobre esta rama se remontan a los comienzos del siglo XIX y se asocian al nombre de Arthur Cayley(1821–1895) quien en su primer escrito, *On the Theory of Linear Transformations* (Acerca de la teoría de transformaciones lineales) datado en 1845, inició el estudio de formas algebraicas y sus propiedades invariantes bajo transformaciones lineales, siendo su estudio más destacado el método de derivación hiperdeterminante. Gracias a Cayley surgió el concepto de invariante como una función que permanece inalterada bajo ciertas transformaciones.

El trabajo en invariantes continuó de esta manera bajo la mano de matemáticos como James Joseph Sylvester, que hizo contribuciones significativas al estudio de formas binarias y polinomios invariantes, o como Paul Gordan, que conocido informalmente por ser el Rey de los Invariantes sus escritos se centraron en la clasificación y construcción de invariantes de formas algebraicas y en 1868 logró demostrar que el anillo de invariantes de formas binarias de grado fijo es finitamente generado.

La teoría de invariantes es muy extensa y por ello vamos a centrarnos en los resultados que abarcan únicamente a grupos finitos. La teoría de invariantes comenzó a relacionarse más estrechamente con la teoría de grupos a finales del siglo XIX gracias al matemático Felix Klein que promovió el estudio de geometrías a través de sus grupos de simetría en su Erlanger Programm en 1872.

Después de Klein, fue David Hilbert quien revolucionó la teoría de invariantes en 1890 al probar que para cualquier grupo lineal G actuando sobre un anillo de polinomios $K[X_1, \ldots, X_n]$, el anillo de invariantes $K[X_1, \ldots, X_n]^G$ es finitamente generado. Y después de él, en el siglo XX, destacamos los estudios de Emmy Noether que ayudó con el desarrollo conjunto de teoría de invariantes con teoría de representaciones de grupos.

La teoría de invariantes de grupos finitos guarda una gran conexión con la teoría de Galois y ha evolucionado desde sus inicios en el siglo XIX hasta convertirse en una parte integral de las matemáticas modernas.

Este trabajo con título *Teoría de invariantes de grupos finitos* tiene como objetivo el desarrollo de las notas de Jürgen Müller con el mismo nombre, de los capítulos 1 al 5. Puede obtenerse más información de dicho autor y de sus notas en su página web [11].

En estas notas vamos a tratar distintos temas relacionados con teoría invariante incluyendo una serie de conceptos que nos van a permitir llegar a analizar el teorema de Shephard-Todd que indica el final de este estudio.

Para ello vamos a definir lo que son los polinomios simétricos y vamos a poder establecer una caracterización que nos va a ser útil para poder trabajar con ellos.

También tendrá mucha importancia en este trabajo el concepto de álgebra simétrica que será muy redundante a lo largo de los capítulos finales y nos será muy útil para la constitución de las series de Hilbert, que introduciremos en los capítulos relacionados con la cota de Noether y la fórmula de Molien.

Hablaremos de ciertas estructuras algebraicas que nos servirán como continuación de lo estudiado en el resto de asignaturas de álgebra tratadas en la carrera y terminaremos hablando de pseudorreflexiones, el último concepto que nos permitirá por fin introducir el teorema de Shephard-Todd que marca el final del trabajo.

Capítulo 2

Polinomios simétricos

Este capítulo va a estar destinado al estudio de polinomios simétricos que van a resultar clave para la comprensión de la teoría de invariantes de grupos finitos. Para ello vamos a asumir a lo largo de todo el capítulo que los anillos son unitarios.

2.1. Primeras definiciones y conceptos

En esta primera sección nuestro objetivo es dar a conocer al lector la definición de polinomio simétrico, así como añadir algunas propiedades básicas y aportar una serie de ejemplos que sirvan como ayuda para entender bien todos los conceptos.

Como primera instancia queremos hacer referencia al álgebra libre, pues nos va a ser útil para poder presentar el resto de conceptos que nos conducen al tema de interés. Informalmente hablando, el álgebra libre es el análogo no conmutativo del anillo de polinomios.

Definición 2.1.1. Sea R un anillo, el **álgebra libre** en n indeterminadas $X_1, \ldots, X_n$ es el anillo generado por todas las combinaciones lineales de los productos no conmutativos de las variables y es denotado por $R\langle X_1, \ldots X_n\rangle$. Más aún, sobre un cuerpo, el álgebra libre en n indeterminadas se puede construir como el álgebra tensorial de un espacio vectorial n-dimensional, pero esto último lo abordaremos con mayor profundidad en la Definición 3.1.8 y en la Proposición 3.1.13.

Partiendo de esto queremos aportar una pequeña observación que servirá al lector como recordatorio de algunas nociones necesarias para la comprensión del tema a tratar.

Observación 2.1.2. Sea F un cuerpo, sea $X := \{X_1, \ldots, X_n\}$, con $n \geq 1$, un conjunto finito de indeterminadas algebraicamente independientes sobre F, ver la Definición 2.2.3, y sea $F[X] := F[X_1, \ldots, X_n]$ el anillo de polinomios correspondiente. Nótese que, como veremos en la Proposición 3.1.13, $F[X]$ es la álgebra libre conmutativa de F con $X = (X_1, \ldots, X_n)$ por generadores libres.

Recordatorio: Una **acción por la izquierda** ρ de un grupo G sobre un conjunto X es una operación externa

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

satisfaciendo las siguiente propiedades

1. $(g \cdot g') \cdot x = g \cdot (g' \cdot x)$, para todos $g, g' \in G$, $x \in X$.
2. $e \cdot x = x$, para todo $x \in X$, donde e es el elemento neutro de G.

Denotemos por $\mathcal{S}_n \cong S_X$ al grupo simétrico sobre X, actuando por la izquierda en X. Como $\sigma \in S_X$ permuta X, esto induce un automorfismo entre F-álgebras $\sigma : F[X] \longrightarrow F[X]$, y por lo tanto una acción por la izquierda de S_X en $F[X]$. Dado un polinomio $f \in F[X] = F[X_1, \ldots, X_n]$, definimos σf como

$$\sigma f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

Nótese que, si $f \in F[X]$ es homogéneo de grado $deg_X(f) = d \in \mathbb{N}_0$, entonces $\sigma f \in F[X]$ es también homogéneo y $deg_X(\sigma f) = d$.

Ejemplo 2.1.3. Para $X = (X_1, X_2, X_3)$, consideremos la permutación $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ y el polinomio $f(X_1, X_2, X_3) = X_1 + X_2^2 + 2X_3$, entonces siguiendo la definición

$$\sigma f(X_1, X_2, X_3) = f(X_{\sigma(1)}, X_{\sigma(2)}, X_{\sigma(3)}) = f(X_2, X_1, X_3) = X_2 + X_1^2 + 2X_3$$

Teniendo esta observación en mente ya podemos introducir los conceptos de polinomio simétrico y de anillo invariante.

Definición 2.1.4. Un polinomio $f \in F[X]$ se llama **simétrico**, si $\sigma f = f$ para todo $\sigma \in S_X$.

Sea $F[X]^{S_X} := \{ f \in F[X] \ / \ f \text{ es simétrico } \} \subseteq F[X]$. Como S_X actúa por automorfismos de F-álgebras de $F[X]$, como vimos en la Observación 2.1.2, el subconjunto $F[X]^{S_X}$ es un subanillo de $F[X]$, que contiene a los polinomios constantes $1 \cdot F \cong F$, por lo que $F[X]^{S_X}$ es una F-subálgebra de $F[X]$. Llamamos a $F[X]^{S_X}$ el **anillo invariante** de S_X.

A lo largo de este capítulo, trataremos de describir la estructura del anillo invariante $F[X]^{S_X}$.

Ilustremos el concepto de polinomio simétrico con algunos ejemplos básicos pero visuales.

Ejemplo 2.1.5. Los polinomios $f = X_1^2 + X_2^2 + 3$, $g = X_1^3 X_2 + X_1^2 X_2^2 + (X_1 + X_2)^2 + X_1 X_2^3$ son polinomios simétricos pues al intercambiar sus variables se obtienen de nuevo los mismos polinomios, pero, sin embargo, el polinomio $h = X_1 - X_2$ no es simétrico ya que al intercambiar sus variables se obtiene $X_2 - X_1 \neq h$.

La existencia de los polinomios simétricos puede llevar a uno a cuestionarse la existencia de una "base"de polinomios que sean de este tipo o que sean sencillos de construir. Es por esto que consideramos los polinomios simétricos elementales.

Definición 2.1.6. Los **polinomios simétricos elementales** $e_0^{(n)}, e_1^{(n)}, \ldots, e_n^{(n)} \in F[X]$ de $X_1, X_2, \ldots, X_n$ se definen como

$$e_j^{(n)}(X_1, X_2, \ldots, X_n) = \sum_{\substack{J \subset [n] \\ |J| = j}} \prod_{i \in J} X_i \ ,$$

donde $[n] = \{1, 2, \ldots, n\}$.

Ejemplo 2.1.7. Los polinomios simétricos elementales de X_1, X_2, X_3 son los siguientes

- $e_0^{(3)}(X_1, X_2, X_3) = 1$
- $e_1^{(3)}(X_1, X_2, X_3) = X_1 + X_2 + X_3$

- $e_2^{(3)}(X_1, X_2, X_3) = X_1X_2 + X_1X_3 + X_2X_3$
- $e_3^{(3)}(X_1, X_2, X_3) = X_1X_2X_3$

En el caso general para $X_1, X_2, \ldots, X_n$ algunos polinomios simétricos elementales son

- $e_0^{(n)}(X_1, X_2, \ldots, X_n) = 1$
- $e_1^{(n)}(X_1, X_2, \ldots, X_n) = X_1 + X_2 + \ldots + X_n$
- $e_2^{(n)}(X_1, X_2, \ldots, X_n) = X_1X_2 + X_1X_3 + \ldots + X_1X_n + X_2X_3 + \ldots + X_2X_n + \ldots + X_{n-1}X_n$
- $e_3^{(n)}(X_1, X_2, \ldots, X_n) = X_1X_2X_3 + X_1X_2X_4 + \ldots + X_{n-2}X_{n-1}X_n$

Observación 2.1.8. El polinomio $e_j^{(n)}(X)$ es homogéneo de grado $deg_X(e_j^{(n)}) = j$

Los polinomios simétricos elementales tienen algunas propiedades muy útiles para obtener expresiones de coeficientes de ecuaciones algebraicas o para relacionar indeterminadas.

Teorema 2.1.9. ***(Fórmulas de Cardano-Vieta)*** *Sea Y una indeterminada sobre $F[X]$. Entonces*

$$(Y - X_1)\cdots(Y - X_n) = \prod_{j=1}^{n}(Y - X_j) = Y^n + \sum_{j=1}^{n}(-1)^j e_j^{(n)}(X)Y^{n-j} \in F[X][Y].$$

Demostración.

Denotemos $f_n = (Y - X_1)\cdots(Y - X_n)$. Por inducción sobre $n = deg_X(f_n)$.

Si $n = 1$, $f_1 = (Y - X_1)$ y $Y + (-1)e_1^{(1)}(X_1) = Y - X_1$ por lo tanto se verifica que $f_1 = Y + (-1)e_1^{(1)}$.

Supongamos que el resultado es cierto para $n - 1$. Denotamos $X' = (X_1, \ldots, X_{n-1})$, por hipótesis de inducción,

$$f_{n-1} = (Y - X_1)\cdots(Y - X_{n-1}) = Y^{n-1} + \sum_{j=1}^{n-1}(-1)^j e_j^{(n-1)}(X')Y^{n-1-j}$$

Entonces

$$f_n = f_{n-1}(Y - X_n) = \left(Y^{n-1} + \sum_{j=1}^{n-1}(-1)^j e_j^{(n-1)}(X')Y^{n-1-j}\right)(Y - X_n) = Y^n - Y^{n-1}X_n +$$

$$+Y\sum_{j=1}^{n-1}(-1)^j e_j^{(n-1)}(X')Y^{n-1-j} + (-1)\sum_{j=1}^{n-1}(-1)^j e_j^{(n-1)}(X')X_nY^{n-1-j}$$

Teniendo en cuenta que $e_n^{(n-1)}(X') = 0$ y que $(-1)^{j+1}e_j^{(n-1)}(X')X_nY^{n-1-j}\Big|_{j=0} = -X_nY^{n-1}$ podemos escribir

$$f_n = Y^n + \sum_{j=1}^{n}(-1)^j e_j^{(n-1)}(X')Y^{n-j} + \sum_{j=0}^{n-1}(-1)^{j+1}e_j^{(n-1)}(X')X_nY^{n-1-j}$$

Ahora, haciendo un cambio de índice en el segundo sumatorio

$$f_n = Y^n + \sum_{j=1}^{n}(-1)^j e_j^{(n-1)}(X')Y^{n-j} + \sum_{j=1}^{n}(-1)^j e_{j-1}^{(n-1)}(X')X_nY^{n-j}$$

Y entonces podemos agrupar todo en una única suma para obtener

$$f_n = Y^n + \sum_{j=1}^{n}(-1)^j(e_j^{(n-1)}(X') + X_n e_{j-1}^{(n-1)}(X'))Y^{n-j} = Y^n + \sum_{j=1}^{n}(-1)^j e_j^{(n)}(X)Y^{n-j}$$

Como queríamos probar. □

Observación 2.1.10. En la demostración anterior hemos hecho uso de la expresión

$$e_j^{(n-1)}(X') + X_n e_{j-1}^{(n-1)}(X') = e_j^{(n)}(X).$$

Esta surge de la propia definición de polinomio simétrico elemental en n variables

$$e_j^{(n)}(X_1, X_2, \ldots, X_n) = \sum_{\substack{J\subset[n]\\|J|=j}} \prod_{i\in J} X_i \ ,$$

al separar los términos de la suma en aquellos en los que no aparece X_n, que son precisamente

$$\sum_{\substack{J\subset[n-1]\\|J|=j}} \prod_{i\in J} X_i,$$

y agrupando aquellos en los que sí aparece X_n tomando este término como factor común, de modo que lo agrupado se convierte en el polinomio simétrico elemental en $n-1$ variables de orden uno menos que el orden inicial

$$X_n \sum_{\substack{J\subset[n-1]\\|J|=j-1}} \prod_{i\in J} X_i.$$

De esta forma,

$$\sum_{\substack{J\subset[n]\\|J|=j}} \prod_{i\in J} X_i = \sum_{\substack{J\subset[n-1]\\|J|=j}} \prod_{i\in J} X_i + X_n \sum_{\substack{J\subset[n-1]\\|J|=j-1}} \prod_{i\in J} X_i$$

que es precisamente la expresión usada.

Ejemplo 2.1.11. En relación a la observación anterior, para $X = (X_1, X_2, X_3)$ por ejemplo observamos que

$$e_2^{(3)}(X) = X_1X_2 + X_2X_3 + X_1X_3 = X_1X_2 + X_3(X_1 + X_2) = e_2^{(2)}(X_1, X_2) + X_3(e_1^{(2)}(X_1, X_2))$$

Observación 2.1.12. Si $\zeta_1, \zeta_2, \ldots, \zeta_n$ son las raíces de la ecuación algebraica $a_0 + a_1Y + \ldots + a_nY^n = 0$. Entonces

$$a_{n-j} = (-1)^j e_j^{(n)}(\zeta_1, \zeta_2, \ldots, \zeta_n)a_n$$

esto es resultado de las fórmulas de Vieta, procedentes del Teorema 2.1.9, que vienen dadas por

$$\zeta_1 \cdots \zeta_n = \frac{a_0}{a_n} \qquad \zeta_1 + \ldots + \zeta_n = -\frac{a_{n-1}}{a_n}$$

cuando es posible dividir por a_n. Observemos que precisamente se tratan de los polinomios simétricos $e_n^{(n)}(\zeta_1, \ldots, \zeta_n)$ y $e_1^{(n)}(\zeta_1, \ldots, \zeta_n)$.

Por último, el peso de un monomio o un polinomio va a tener alta influencia en los siguientes resultados que vamos a tratar así que vamos a hablar de ellos.

Definición 2.1.13. Para un monomio $X^\alpha := \prod_{i=1}^n X_i^{\alpha_i} \in F[X]$, con $\alpha = [\alpha_1, \ldots, \alpha_n] \in \mathbb{N}_0^n$, definimos por $pe_X(X^\alpha) := \sum_{i=1}^n i\alpha_i \in \mathbb{N}_0$ a su **peso**. Para $f \in F[X]$, definimos como $pe_X(f) \in \mathbb{N}_0$ al máximo peso de los monomios de f.

2.2. Caracterización de los polinomios simétricos

En esta sección veremos los primeros resultados importantes relacionados con polinomios simétricos y aportaremos algún ejemplo que nos permita visualizar su funcionamiento de una forma más clara.

El siguiente resultado nos va a permitir expresar cualquier polinomio simétrico en términos de los polinomios simétricos elementales.

Teorema 2.2.1. *Sea $f \in F[X]$ un polinomio simétrico con $deg_X(f) = d$. Entonces existe un polinomio $g \in F[X]$ tal que $pe_X(g) \leq d$ y $f = g(e_1^{(n)}, \ldots, e_n^{(n)})$.*

Demostración.

Por inducción sobre n.

El teorema es obvio si $n = 1$, basta con ver que si $f(X) = a_d X^d + \ldots + a_1 X + a_0$, como $e_1(X) = X$, podemos tomar $g = f$.

Así que supongamos que $n > 1$. Hacemos ahora inducción sobre d, para el caso $d = 0$, f es constante, y basta tomar $g = f$, así que pongamos $d > 0$.

Consideremos el Teorema 2.1.9 y hagamos la sustitución $X_n \mapsto 0$. Como

$$e_j^{(n)}(X_1, \ldots, X_{n-1}, 0) = e_j^{(n-1)}(X_1, \ldots, X_{n-1}),$$

igualdad procedente de la expresión discutida en la Observación 2.1.10, obtenemos la expresión siguiente

$$Y \cdot \prod_{i=1}^{n-1}(Y - X_i) = Y^n + \sum_{j=1}^{n-1}(-1)^j e_j^{(n-1)}(X_{1:n-1})Y^{n-j} \in F[X][Y],$$

para $j \in \{1, \ldots, n-1\}$. Observemos además que $f(X_1, \ldots, X_{n-1}, 0)$ es simétrico en $X_1, \ldots, X_{n-1}$.

Por inducción en n, existe $g' \in F[X]$ tal que $pe_X(g') \leq d$ y

$$f(X_1, \ldots, X_{n-1}, 0) = g'(e_1^{(n-1)}, \ldots, e_{n-1}^{(n-1)}).$$

Como los $e_j^{(n)}$ son homogéneos y $deg_X(e_j^{(n)}) = j$, concluimos que $\deg_X(g'(e_1^{(n)}, \ldots, e_{n-1}^{(n)})) \leq d$.

Sea $f' := f - g'(e_1^{(n)}, \ldots, e_{n-1}^{(n)}) \in F[X]$, entonces $\deg_X(f') \leq d$ también. Puesto que $f'(X_1, \ldots, X_{n-1}, 0) = 0$, concluimos que $f' \in F[X_1, \ldots, X_{n-1}][X_n]$ es divisible por X_n.

Como X_n divide a f' en $F[X_1, \ldots, X_n]$ y f' es simétrico por ser suma de dos polinomios simétricos, entonces, permutando i, n, tenemos que X_i divide a f'. Con este razonamiento deducimos que X_i divide a f' para $i = 1, \ldots, n$. Ahora bien, recordemos que $F[X_1, \ldots, X_n]$ es un dominio de factorización única y puesto que los elementos $X_1, \ldots, X_n$ son primos, finalmente obtenemos que $X_1 \cdot X_2 \cdots X_n$ divide a f'. De esta forma podemos escribir $f' = f'' \cdot e_n^{(n)} \in F[X]$.

Entonces $f'' \in F[X]$ es simétrico y tenemos que $\deg_X(f'') \leq d - n < d$. De esta forma, por inducción, existe $g'' \in F[X]$ tal que $\mathrm{pe}_X(g'') \leq d - n$ y $f'' = g''(e_1^{(n)}, \ldots, e_n^{(n)})$. Concluimos así que

$$f = g'(e_1^{(n)}, \ldots, e_{n-1}^{(n)}) + e_n^{(n)} \cdot g''(e_1^{(n)}, \ldots, e_n^{(n)}),$$

donde $\mathrm{pe}_X(g' + X_n g'') \leq d$. □

Exponemos un ejemplo que nos permite ilustrar este resultado.

Ejemplo 2.2.2. Consideremos el polinomio $f(X_1, X_2) = X_1^2 + X_2^2$, entonces podemos escribir

$$f(X_1, X_2) = X_1^2 + X_2^2 = (X_1 + X_2)^2 - 2(X_1X_2) = e_1(X_1, X_2)^2 - 2e_2(X_1, X_2)$$

Por lo tanto $f(X_1, X_2) = g(e_1, e_2)$ con $g(X_1, X_2) = X_1^2 - 2X_2$

Para el siguiente resultado a desarrollar, vamos a recordar la definición de elementos algebraicamente independientes.

Definición 2.2.3. Decimos que los elementos $a_1, \ldots, a_n \in F$ son **algebraicamente independientes** si no existe ningún polinomio no nulo

$$P(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$$

tal que $P(a_1, \ldots, a_n) = 0$. En caso contrario, decimos que $a_1, \ldots, a_n$ son **algebraicamente dependientes**.

Teorema 2.2.4. *El conjunto* $\{e_1^{(n)}, \ldots, e_n^{(n)}\} \subseteq F[X]$ *es algebraicamente independiente.*

Demostración.

Hacemos inducción sobre n. El caso $n = 1$ es evidente, así que consideremos $n > 1$. Razonamos por reducción al absurdo y elegimos $f \in F[X]$ de grado mínimo tal que $f(e_1^{(n)}, \ldots, e_n^{(n)}) = 0$.

Sea

$$f = \sum_{i=0}^{d} f_i(X_1, \ldots, X_{n-1}) X_n^i \in F[X_1, \ldots, X_{n-1}][X_n]$$

Si $f_0 = 0$, entonces tenemos que $f = X_n \cdot f'$ y entonces $f'(e_1^{(n)}, \ldots, e_n^{(n)}) = 0$, donde f' es no nulo y $\deg_X(f') < \deg_X(f)$, entrando en contradicción con cómo habíamos considerado f.

Por lo tanto, necesariamente $f_0 \neq 0$. Sustituyendo $X_n \mapsto 0$ como en la demostración del Teorema 2.2.1, obtenemos que

$$0 = f(e_1^{(n-1)}, \ldots, e_{n-1}^{(n-1)}, 0) = f_0(e_1^{(n-1)}, \ldots, e_{n-1}^{(n-1)})$$

Por inducción, esto contradice la independencia algebraica de $\{e_1^{(n-1)}, \ldots, e_{n-1}^{(n-1)}\}$. □

Como consecuencia de los Teoremas 2.2.1 y 2.2.4 obtenemos el siguiente corolario.

Corolario 2.2.5. *El anillo invariante* $F[X]^{S_X}$ *es un anillo de polinomios en las indeterminadas* $e_1, \ldots, e_n$*, es decir, tenemos* $F[X]^{S_X} \cong F[e_1, \ldots, e_n]$.

Capítulo 3

Anillos invariantes

En este capítulo vamos a formalizar el álgebra simétrica que es isomorfa a un anillo de polinomios cuyas indeterminadas son los elementos de una base de un espacio vectorial. Nuevamente vamos a considerar que todos los anillos mencionados tienen unidad.

3.1. El álgebra simétrica

Para entrar en el tema vamos a comenzar introduciendo una serie de definiciones que servirán como apoyo al lector interesado.

Definición 3.1.1. Sea R un anillo, un **módulo por la izquierda** A sobre R es un grupo abeliano $(A, +)$, dotado de una operación (multiplicación escalar)

$$\begin{aligned} R \times A &\longrightarrow A \\ (r, a) &\longmapsto r \cdot a \end{aligned}$$

verificando que para todos $r, r_1, r_2 \in R$, $a, a_1, a_2 \in A$ se satisface

1. $1 \cdot a = a$
2. $(r_1 r_2)a = r_1(r_2 a)$
3. $(r_1 + r_2)a = r_1 a + r_2 a$
4. $r(a_1 + a_2) = r a_1 + r a_2$

Análogamente podemos definir un **módulo por la derecha** sobre A, sin embargo trataremos únicamente con módulos por la izquierda de ahora en adelante, a no ser que indique lo contrario, y les denotaremos simplemente por A**-módulos** o directamente **módulos** en caso de que la referencia sea clara.

Veamos algunos ejemplos básicos de módulos.

Ejemplo 3.1.2.

a) Dado A un grupo abeliano, es un módulo sobre $\mathbb{Z}$ con el producto por escalares

$$na = \begin{cases} a + a + \ldots + a \ (n \ veces) \ n \geq 0 \\ -a - a - \ldots - a \ (n \ veces) \ n < 0 \end{cases}$$

b) Si R es unitario, entonces $R[X]$ es un módulo sobre R con el producto usual de polinomios con elementos del anillo.

c) R es un R-módulo sobre sí mismo. Realmente, si I es un ideal en R, entonces es un R-módulo.

d) Dado un grupo abeliano A, sabemos que la familia de endomorfismos de A es un anillo (respecto a la composición y a la suma). Entonces, si para $f \in End(A)$ definimos $f \cdot a := f(a)$, A es un $End(A)$-módulo.

e) Sea S un anillo. Dado A un S-módulo y dado un homomorfismo de anillos $R \xrightarrow{\varphi} S$, entonces A es un R-módulo al definir $r \cdot a := \varphi(r)a$.

f) Si I es un ideal sobre el anillo R, entonces R/I es un R-módulo, con la definición $r_1(r + I) := r_1 r + I$

Definición 3.1.3. Dados un anillo R y dos R-módulos A, B, un **homomorfismo de R-módulos** es una aplicación $\varphi : A \longrightarrow B$ que es un homomorfismo de grupos A y B satisfaciendo

$$\varphi(ra) = r\varphi(a), \quad r \in R,\ a \in A$$

Partiendo de la noción de módulos vamos a introducir lo que es una categoría y la definición de producto tensorial que nos será útil para la definición de álgebra simétrica que es el concepto de interés de esta parte del capítulo.

Definición 3.1.4. Una **categoría $\mathcal{C}$** consiste en una familia de objetos (usualmente escritos A, B, C) y flechas entre ellos, llamadas morfismos (escritas f, g, h) tales que si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son morfismos, entonces $g \circ f : A \longrightarrow C$ es un morfismo; tal que, cuando tenga sentido, la composición de morfismos f, g, h satisface

$$h \circ (g \circ f) = (h \circ g) \circ f$$

y para todo objecto A en la categoría tenemos el morfismo identidad $1_A : A \longrightarrow A$ que por definición satisface $1_A \circ f = f$ y $g \circ 1_A = g$ (cuando estas composiciones tengan sentido).

El lector puede acudir a [10, Cap. 1] para profundizar más en las definiciones relativas a las categorías así como en sus axiomas característicos.

Definición 3.1.5. Sea R un anillo conmutativo, si $E_1, E_2 \ldots, E_n, F$ son módulos, entonces denotamos por

$$L^n(E_1, \ldots, E_n; F)$$

al módulo de n aplicaciones multilineales

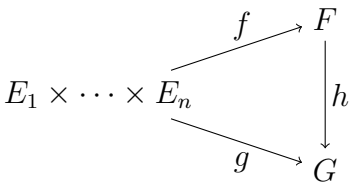
$$f : E_1 \times \cdots \times E_n \longrightarrow F$$

(Recordemos que una aplicación multilineal es una aplicación lineal en cada factor del producto $E_1 \times \cdots \times E_n$)

Uno puede entender las aplicaciones multilineales de un conjunto fijo de módulos $E_1, \ldots, E_n$ como objetos de una categoría. Fijados un conjunto de R-módulos $E_1, \ldots, E_n$, los objetos de la categoría mencionada son aplicaciones multilineales

$$f : E_1 \times \cdots \times E_n \longrightarrow F,$$

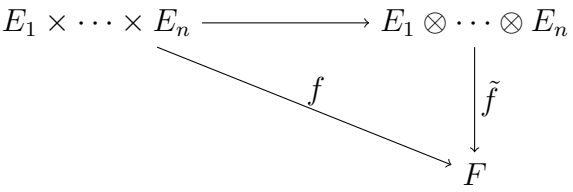
donde F es un R-módulo. Dados dos objetos de la categoría, $f : E_1 \times \cdots \times E_n \longrightarrow F$, $g : E_1 \times \cdots \times E_n \longrightarrow G$, con F, G ambos R-módulos, un morfismo de esta categoría es un homomorfismo de R-módulos $h : F \longrightarrow G$ que hace conmutativo el siguiente diagrama



El **producto tensorial** es un objeto inicial en esta categoría, una explicación más detallada sobre este tema puede ser encontrada en [10, 1.2], y lo denotamos $E_1 \otimes \cdots \otimes E_n$. Es conocido que este siempre existe y es único.

$$E_1 \times \cdots \times E_n \longrightarrow E_1 \otimes \cdots \otimes E_n$$
$$(e_1, \ldots, e_n) \longmapsto (e_1 \otimes \cdots \otimes e_n)$$

De esta forma, podemos enunciar una "propiedad universal" asociada a $E_1, E_2, \ldots, E_n$. Para todo $f : E_1 \times \cdots \times E_n \longrightarrow F$ objeto en la categoría, existe un único homomorfismo entre R-módulos $\tilde{f} : E_1 \otimes \cdots \otimes E_n \longrightarrow F$ de tal forma que el siguiente diagrama se vuelve conmutativo.



Encontramos que si $e_i, e_i' \in E_i$ y $a \in R$, el producto tensorial verifica para todo i lo siguiente

- $e_1 \otimes \cdots \otimes ae_i \otimes \cdots \otimes e_n = a(e_1 \otimes \cdots \otimes e_n)$
- $e_1 \otimes \cdots \otimes (e_i + e_i') \otimes \cdots \otimes e_n = (e_1 \otimes \cdots \otimes e_n) + (e_1 \otimes \cdots \otimes e_i' \otimes \cdots \otimes e_n)$

Si tenemos dos factores, $E \otimes F$ por ejemplo, entonces cada elemento de $E \otimes F$ se puede escribir como una suma de términos $x \otimes y$ con $x \in E$, $y \in F$, porque tales términos generan $E \otimes F$ y $a(x \otimes y) = ax \otimes y$ para todo $a \in R$. Ver [9, 16.1].

Vamos ahora a introducir algunas nociones necesarias para poder entender el álgebra simétrica.

Definición 3.1.6. Una **representación matricial de grado** $n \leq 1$ de un grupo finito G sobre un anillo conmutativo A es un homomorfismo de grupos

$$\rho : G \longrightarrow GL_n(A)$$

donde el **grupo lineal general** es el grupo de las matrices invertibles de orden $n \times n$ con coeficientes en A. Diremos que A es el **anillo de coeficientes** de la representación.

Definición 3.1.7. Sea F un cuerpo y sea G un grupo. El **álgebra de grupo** $F[G] = FG$ es el F-espacio vectorial con base $\{g : g \in G\}$ con la estructura de álgebra dada por el producto

$$\left(\sum_{g \in G} \lambda_g g\right) \cdot \left(\sum_{h \in G} \mu_h h\right) = \sum_{g,h \in G} \lambda_g \mu_h (gh).$$

Una vez vistos estos conceptos, veamos lo que es una potencia simétrica un álgebra simétrica y hablemos del anillo invariante.

Definición 3.1.8. Sea F un cuerpo y sea V un espacio vectorial sobre F con $n = \dim_F(V) \in \mathbb{N}_0$. Para $d \in \mathbb{N}$, definimos la **d-ésima potencia simétrica** de V como el F-espacio cociente del d-ésimo espacio tensorial potencia $V \otimes \overset{d}{\cdots} \otimes V$, donde los productos tensoriales se toman sobre F, con respecto al F-subespacio V'_d. Esto es,

$$S[V]_d := \frac{V \otimes \overset{d}{\cdots} \otimes V}{V'_d}$$

donde

$$V'_d := \langle v_1 \otimes \cdots \otimes v_d - \sigma(v_1 \otimes \cdots \otimes v_d) \ / \ v_i \in V,\ \sigma \in S_d \rangle_F \subseteq V \otimes \overset{d}{\cdots} \otimes V$$

Definimos el **álgebra simétrica** $S[V]$ sobre V como

$$S[V] := \oplus_{d \in \mathbb{N}_0} S[V]_d, \text{ donde } S[V]_0 := 1 \cdot F \cong F.$$

$S[V]$ es una F-álgebra conmutativa finitamente generada, donde la multiplicación es heredada de la concatenación de productos tensoriales. Dada una F-base de $\{b_1, \ldots, b_n\} \subseteq V = S[V]_1$ de V, es un conjunto generador de $S[V]$ como F-álgebra.

Mediante las observaciones siguientes vamos a poder mostrar al lector de dónde procede la razón de la construcción de la potencia y álgebra simétricas, explicando el sentido del cociente.

Observación 3.1.9. Dados G un grupo y $D_V : G \to GL(V) \cong GL_n(F)$ una F-representación de G, podemos observar que V como F-espacio vectorial se convierte en un $F[G]$-módulo.

Para $g \in G$, $v \in V$ tenemos que $g \cdot v = D_V(g)(v)$ como aplicación de $G \times V$ en V, como los D_V son lineales y $\sum_{g \in G} \lambda_g g \in F[G]$ actúa de forma lineal, entonces V es un $F[G]$-módulo mediante la aplicación

$$\begin{aligned} F[G] \times V &\longrightarrow V \\ \alpha \cdot v &\longmapsto \textstyle\sum_{g \in G} \lambda_g \cdot g \cdot v \end{aligned}$$

donde $\alpha = \sum_{g \in G} \lambda_g g \in F[G]$.

Observación 3.1.10. Por otro lado, mediante la G-acción diagonal, $V \otimes \overset{d}{\cdots} \otimes V$, con $d \in \mathbb{N}$, se convierte en un $F[G]$-módulo. Para analizar esto es suficiente hacer actuar un g del grupo sobre un elemento del producto tensorial. Sean $g \in G$, $v_1 \otimes \cdots \otimes v_d \in V \otimes \overset{d}{\cdots} \otimes V$, entonces tiene sentido escribir

$$g(v_1 \otimes \cdots \otimes v_d) = gv_1 \otimes \cdots \otimes gv_d,$$

pues los gv_i, $i = 1, \ldots, d$ son todos vectores y de esta forma la acción recibe el nombre de diagonal debido a que actúa de igual forma sobre todos los factores. Por lo tanto, si ahora tomamos un elemento del álgebra de grupo, $\alpha = \sum_{g \in G} \lambda_g g \in F[G]$, $\alpha(v_1 \otimes \cdots \otimes v_d)$ toma sentido por linealidad.

Puesto que la G-acción es diagonal, entonces la G-acción y la $\mathcal{S}_d$-acción conmutan en $V \otimes \overset{d}{\cdots} \otimes V$. Para $\sigma \in \mathcal{S}_d$, $g \in G$,

$$\sigma(g(v_1 \otimes \cdots \otimes v_d)) = g(\sigma(v_1 \otimes \cdots \otimes v_d))$$

Por lo tanto concluimos que $V'_d \subseteq V \otimes \overset{d}{\cdots} \otimes V$ es un $F[G]$-submódulo, y por lo tanto, el F-espacio cociente $S[V]_d = \frac{V \otimes \overset{d}{\cdots} \otimes V}{V'_d}$ tiene sentido pues estamos cocientando un módulo sobre el mismo anillo y es también un $F[G]$-módulo. Nótese que dejamos que G actúe trivialmente en $S[V]_0 = 1 \cdot F$. Por otro lado, G actúa mediante automorfismos de álgebras de F en $S[V]$.

Esta construcción ayuda al lector a entender cómo partiendo de una representación $D_V : G \to GL(V)$, G actúa sobre $S[V]$.

Definición 3.1.11. Nuevamente, el **anillo invariante** correspondiente se define como

$$S[V]^G := \{f \in S[V] \ / \ \sigma f = f \text{ para todo } \sigma \in G\}$$

Partiendo de esto, podemos abordar el primer resultado del tema que nos relaciona el álgebra simétrica con un anillo de polinomios. Para ello primero vamos a tratar una caracterización de los productos tensoriales que va a ser necesaria para la prueba del resultado.

Observación 3.1.12. Fijada una base $\{b_1, \ldots, b_n\}$ de V, tenemos que para cada $d \in \mathbb{N}_0$ definimos la aplicación multilineal

$$\begin{array}{c} \tilde{\beta}_d : V \times \overset{d}{\cdots} \times V \longrightarrow F[X] \\ (b_{i_1}, \ldots, b_{i_d}) \longmapsto X_{i_1} \cdots X_{i_d}. \end{array}$$

Entonces, por la Definición 3.1.5, podemos considerar la siguiente aplicación lineal que se obtiene por la propiedad universal del producto tensorial

$$\begin{array}{c} \beta_d : V \otimes \overset{d}{\cdots} \otimes V \longrightarrow F[X] \\ b_{i_1} \otimes b_{i_2} \otimes \cdots \otimes b_{i_d} \longmapsto \prod_{k=1}^{d} X_{i_k} \end{array}$$

que nos proporciona un polinomio de grado d.

Proposición 3.1.13. *Sea $S[V]$ como en la Definición 3.1.8. Entonces $S[V] \cong F[X]$ como álgebras sobre F, donde $F[X]$ es como en la Observación 2.1.2.*

Demostración.
Sea $\{b_1, \ldots, b_n\} \subseteq V$ una base sobre F de V. Como $F[X]$ es el álgebra libre de F en X, existe un homomorfismo de álgebras de F,

$$\begin{array}{c} \alpha : F[X] \longrightarrow S[V] \\ X_i \longmapsto b_i \end{array} \qquad \text{para } i \in \{1, \ldots, n\}$$

Recíprocamente, por la Observación 3.1.12, para $d \in \mathbb{N}_0$, sabemos que existe una aplicación lineal

$$\begin{array}{c} \beta_d : V \otimes \overset{d}{\cdots} \otimes V \longrightarrow F[X] \\ b_{i_1} \otimes b_{i_2} \otimes \cdots \otimes b_{i_d} \longmapsto \prod_{k=1}^{d} X_{i_k} \end{array}$$

donde $i_k \in \{1, 2, \ldots, n\}$. Dado que $F[X]$ es conmutativo, tenemos $V'_d \subseteq ker(\beta_d)$, y por lo tanto, existe una aplicación F-lineal

$$\beta := \sum_{d \geq 0} \beta_d : S[V] \longrightarrow F[X]$$

Además, β, así definido, es un homomorfismo de anillos compatible con el producto, luego es un homomorfismo de álgebras y, finalmente, tenemos que $\alpha\beta = id_{F[X]}$ y $\beta\alpha = id_{S[V]}$. □

Observación 3.1.14. Sea $F[X]$ como en la observación 2.1.2, y sea

$$V := F[X]_1 := \{f \in F[X] \ / \ deg_X(f) = 1\} \cup \{0\}$$

Por la Proposición 3.1.13, obtenemos $S[V] \cong F[X]$ como F-álgebras. Más aún, dado que $V = F[X]_1$ es un $F[\mathcal{S}_X]$-módulo, por la Definición 3.1.8 tenemos una acción de $\mathcal{S}_X$ en $S[V]$, que de hecho coincide con la acción de $\mathcal{S}_X$ en $F[X]$ dada en la Observación 2.1.2.

Observación 3.1.15. Ahora, fijada $\{b_1, \ldots, b_n\}$ una base de V, vamos a identificar cada elemento del grupo G con una matriz

$$\begin{aligned} G &\longrightarrow GL_n(F) \\ g &\longmapsto Mg \end{aligned}$$

Acabamos de ver que $S[V] \cong F[X]$ como F-álgebras, lo que nos proporciona la siguiente identificación

$$X_{i_1} \cdots X_{i_d} \longleftrightarrow b_{i_1} \otimes \cdots \otimes b_{i_d}$$

Esto nos lleva a considerar que hay una identificación entre $F[X]^G$ y $S[V]^G$. Ya sabemos que $F[X]^G$ se define de la siguiente manera

$$F[X]^G = \{p(X) \in F[X] \ / \ g \cdot p(X) = p(X), \ \forall \ g \in G\},$$

y para poder considerar esta última identificación, tenemos que entender cómo actúa una matriz sobre un polinomio.

Cómo ya hemos visto en las Observaciones 3.1.9 y 3.1.10

$$g(b_{i_1} \otimes \cdots \otimes b_{i_d}) = gb_{i_1} \otimes \cdots \otimes gb_{i_d} = D_V(g)(b_{i_1}) \otimes \cdots \otimes D_V(g)(b_{i_d})$$

La construcción para matrices no va a diferir mucho de esta expresión. Tomando un elemento cualquiera de la base tenemos que g actúa de la siguiente manera

$$g \cdot b_i = Mg \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

tomando coordenadas en la base $\{b_1, \ldots, b_n\}$.

Por lo tanto, obtenemos que g actúa sobre una variable de la manera siguiente

$$g \cdot X_i = (X_1, \ldots, X_n)Mg \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

y sobre un producto entonces

$$g(X_{i_1} \cdots X_{i_d}) = (gX_{i_1}) \cdots (gX_{i_d})$$

obteniendo un polinomio homogéneo de grado d.

3.2. Algunas nociones estructurales

A continuación, introducimos algunas nociones estructurales que resultarán importantes para los anillos conmutativos. A pesar de ser aplicables a anillos conmutativos en general, originalmente fueron introducidas por Hilbert y Noether para el estudio de anillos invariantes.

Definición 3.2.1. Sea $R \subset S$ una extensión de anillos conmutativos. Un elemento $s \in S$ se llama **entero** sobre R si existe un polinomio no nulo $f \in R[X]$ mónico, tal que $f(s) = 0$.

En otras palabras, $s \in S$ es entero sobre R, si satisface una ecuación mónica con la siguiente forma

$$x^n + r_1 x^{n-1} + \ldots + r_n = 0, \quad n \geq 1$$

con $r_i \in R$ para $i = 1, \ldots, n$.

La extensión de anillos $R \subset S$ se llama **entera** si cada elemento de S es entero sobre R.

Consultar [2, Ch. 5] o [4, Ch. 3.1] para ver más sobre estas definiciones.

Ejemplo 3.2.2. Veamos ahora algunos ejemplos de elementos y extensiones enteras.

- Todo cuerpo F que sea extensión algebraica de un cuerpo K, es un anillo de extensión entera.
- Todo anillo R es entero sobre sí mismo, pues para todo $r \in R$ existe

  $$f_r(X) = X - r \in R[X]$$

  polinomio no nulo y mónico satisfaciendo que $f_r(r) = 0$.
- En la extensión de $\mathbb{Z}$ por el cuerpo real $\mathbb{R}$, $1/\sqrt{3}$ es algebraico sobre $\mathbb{Z}$

  $$3\left(\frac{1}{\sqrt{3}}\right)^2 - 1 = 0,$$

  pero no entero.

  Sin embargo, $1/\sqrt{3}$ es entero sobre $\mathbb{Q}$ ya que

  $$f(X) = X^2 - \frac{1}{3} \in \mathbb{Q}[X]$$

  es no nulo, mónico y satisface $f(1/\sqrt{3}) = 0$.

Veamos ahora una caracterización de los elementos enteros.

Proposición 3.2.3. *Un elemento $s \in S$ es entero sobre R si, y solo si, existe un R-submódulo finitamente generado de S que contiene a s. Más generalmente, finitos elementos $s_1, s_2, \ldots, s_n \in S$ son enteros sobre R si, y solo si, el R-módulo $R[s_1, \ldots, s_n]$ es finitamente generado.*

Demostración.

$\boxed{\Longrightarrow}$

Sea $s \in S$ un elemento entero sobre R, entonces sabemos que existe un polinomio mónico $f \in R[X]$ de grado $n \geq 1$ tal que $f(s) = 0$.

Dado $g \in R[X]$, por la división euclídea (gracias a que f es mónico) tenemos que existen $q, r \in R[X]$ con $deg(r) < n$ tales que

$$g(X) = q(X)f(X) + r(X)$$

por lo tanto tenemos

$$g(s) = r(s) = r_0 + r_1 s + \ldots + r_{n-1}s^{n-1}$$

De esta forma obtenemos que $R[s]$ es generado como R-módulo por los elementos $1, s, \ldots, s^{n-1}$.

La segunda afirmación se obtiene al aplicar inducción a la primera afirmación que acabamos de desarrollar.

Para $n = 1$, acabamos de ver que si s_1 es entero sobre R, entonces existe un R-submódulo finitamente generado de S que contiene a s_1, concretamente $R[s_1]$.

Para $n = 2$, si s_1, s_2 son enteros sobre R, en particular, s_2 es entero sobre $R[s_1]$ y por lo tanto $R[s_1][s_2] = R[s_1, s_2]$ es un R-submódulo finitamente generado de S que contiene a s_1 y s_2.

Supongamos ahora que esta afirmación es cierta para $n-1$, es decir, que $T = R[s_1, \ldots, s_{n-1}]$ es un R-módulo finitamente generado conteniendo a los enteros $s_1, \ldots, s_{n-1}$ sobre R. Si $s_1, \ldots, s_n \in S$ son enteros sobre R, entonces s_n es entero sobre T, por hipótesis de inducción tenemos que $T[s_n] = R[s_1, \ldots, s_n]$ está finitamente generado sobre T, y por lo tanto también sobre R.

$\boxed{\Longleftarrow}$

Supongamos que el R-módulo $R[s_1, \ldots, s_n]$ es finitamente generado, entonces existen $m_1, m_2, \ldots, m_r$ de forma que para todo $s \in R[s_1, \ldots, s_n]$ se tiene una representación

$$sm_i = \sum_{j=1}^{r} r_{ij}m_j, \quad i = 1, \ldots, r, \ r_{ij} \in R.$$

En términos matriciales, este sistema de ecuaciones se transforma en

$$\Delta \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix} = 0$$

donde $\Delta = (\delta_{ij}s - r_{ij})_{i,j=1,\ldots,r}$, y δ_{ij} es la delta de Kronecker definida como

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

.

Consideremos entonces la regla de Cramer para obtener la relación

$$\Delta^{ad} \cdot \Delta = det(\Delta) \cdot I$$

con Δ^{ad} la matriz adjunta de Δ e I la matriz identidad de tamaño r. Esta ecuación está definida para matrices con coeficientes en un cuerpo, pero se aplica también a anillos en general. En efecto, comparando los coeficientes de las matrices en ambos lados de la regla de Cramer, obtenemos un sistema de identidades polinómicas para los coeficientes de Δ. Para justificar estas identidades, es posible visualizar los coeficientes c_{ij} de Δ como variables y trabajar sobre el anillo $\mathbb{Z}[c_{ij}]$, caso que puede ser reducido a la situación de coeficientes en un cuerpo pasando al cuerpo de fracciones $\mathbb{Q}(c_{ij})$.

Por lo tanto, usando la fórmula de Cramer obtenemos

$$det(\Delta) \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix} = \Delta^{ad} \cdot \Delta \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix} = 0$$

y entonces, $det(\Delta) \cdot m_i = 0$, $i = 1, \ldots, r$. Como $1 = t_1 m_1 + \ldots + t_r m_r \in R[s_1, \ldots, s_n]$, entonces, necesariamente $det(\Delta) = 0$, y así obtenemos una ecuación mónica para s con coeficientes en R lo que muestra que s es entero sobre R.

□

Observación 3.2.4. En general en $R[X]$ no hay división euclídea, pero sí es posible la división por polinomios mónicos.

De acuerdo con esta proposición, si $s_1, \ldots, s_n \in S$ son enteros sobre R, entonces también lo es cualquier elemento s de $R[s_1, \ldots, s_n]$, porque $R[s_1, \ldots, s_n, s] = R[s_1, \ldots, s_n]$ es un R-módulo finitamente generado.

Definición 3.2.5. Sea $R \subset S$ una extensión de anillos conmutativos. La extensión de anillos $R \subset S$ se llama **finita** si S es una R-álgebra finitamente generada y es entera sobre R.

La extensión de anillos $R \subset S$ es finita si, y solo si, S es un R-módulo finitamente generado. Consultar [13, Pg. 31]

La siguiente proposición nos va a permitir ver que el conjunto de elementos enteros sobre un anillo forma una extensión de anillos.

Proposición 3.2.6. *Sean $R \subseteq S \subseteq T$ dos extensiones de anillos, si T es entero sobre S y S es entero sobre R, entonces T es entero sobre R.*

Demostración.

Sea $t \in T$, como T es entero sobre S existe

$$t^n + s_1 t^{n-1} + \ldots + s_n = 0$$

con $s_i \in S$ para $i = 1, \ldots, n$.

Definimos $A = R[s_1, \ldots, s_n]$, entonces $A[t]$ es un A-módulo finitamente generado. Si S es entero sobre R, entonces $A[t]$ es también finitamente generado sobre R, pues A es finitamente generado sobre R y por lo tanto t es entero sobre R. De esta forma concluimos que T es entero sobre R. □

Definición 3.2.7. Sea $R \subset S$ una extensión de anillos conmutativos. El conjunto de todos los elementos de S que son enteros sobre R

$$\overline{R}^S := \{s \in S \ / \ s \text{ entero sobre } R\} \subseteq S$$

es un anillo, deducido de los resultados anteriores, $R \longrightarrow \overline{R}^S$ es extensión entera y $\overline{R}^S$ contiene todos los subanillos de S enteros sobre R, y se denota como la **clausura entera** de R en S.

Si $\overline{R}^S = R$, entonces R se dice **íntegramente cerrado en** S.

Si R es un dominio entero y es íntegramente cerrado en su cuerpo de fracciones $Quot(R)$, entonces R se dice **íntegramente cerrado**.

Ejemplo 3.2.8. El dominio $\mathbb{Z}$ es íntegramente cerrado en $\mathbb{Q}$, sin embargo, no lo es en el cuerpo complejo $\mathbb{C}$ ya que $i \in \mathbb{C}$ es entero sobre $\mathbb{Z}$.

Una vez conocidos estos conceptos podemos probar la siguiente proposición que hace alusión a los términos recién introducidos. Para ello necesitamos introducir algunos recordatorios relacionados con un resultado que nos va a servir para la demostración de la proposición.

Definición 3.2.9. Sea L un cuerpo y G un subgrupo del grupo de automorfismos

$$Aut(L) = \{g : L \longrightarrow L \ / \ g \text{ es isomorfismo}\}.$$

Al subcuerpo de L

$$L^G = \{x \in L \ / \ \sigma(x) = x, \text{ para todo } \sigma \in G\}$$

se le llama **cuerpo fijo** de G. Ver el lema [1, Ch. 2.F] o acudir a [5, Ch. 5.5].

Teorema 3.2.10. ***Teorema de Artin.*** *Sea L un cuerpo y G un subgrupo finito del grupo*

$$Aut(L) = \{g : L \to L \ / \ g \text{ es isomorfismo}\}$$

Sea $K = L^G$ el cuerpo fijo de G. Entonces la extensión $L \mid K$ es normal, separable y su grado coincide con el cardinal de G. Consultar [1, Th. 14] o nuevamente [5, Ch. 5.5].

A continuación, vamos a ver un resultado que involucra al cuerpo de fracciones de $S[V]$. En el momento en que un grupo finito G actúa sobre $S[V]$, también lo hará sobre su cuerpo de fracciones y podremos considerar la construcción de cuerpo invariante de $S(V)$ sobre dicho grupo.

Proposición 3.2.11. *Denotemos $S(V) := Quot(S[V])$ y sea G un grupo finito.*

a) Sea $S(V)^G \subset S(V)$ el cuerpo invariante de $S(V)$ sobre G, entonces $S(V)^G = Quot(S[V]^G)$. Además, la extensión de cuerpos $S(V)|S(V)^G$ es una extensión finita de Galois con grupo de Galois $G = ker(D_V)$.

b) El anillo invariante $S[V]^G$ es íntegramente cerrado.

Demostración.

a) Claramente, $Quot(S[V]^G) \subset S(V)^G$, luego sólo necesitamos ver que $S(V)^G \subset Quot(S[V]^G)$. Sea $f = \frac{g}{h} \in S(V)^G$, con $g, h \in S[V]^G$. Al multiplicar y dividir por $\prod_{1 \neq \pi \in G} h\pi \in S[V]$, podemos asumir que $h \in S[V]^G$, y por lo tanto, $g \in S[V]^G$ también, lo que implica que $f \in Quot(S[V]^G)$. Luego, $S(V)^G = Quot(S[V]^G)$.

Para la segunda parte del resultado, por el Teorema de Artin, obtenemos directamente que la extensión de cuerpos $S(V)|S(V)^G$ es de Galois.

b) Sea $f \in S(V)^G \subset S(V)$ un elemento entero sobre $S[V]^G$, entonces también es entero sobre $S[V]$. Ahora, veamos que $S[V]$ es íntegramente cerrado en $S(V)$. Dado que $S[V]$ es un dominio de factorización única, vamos a ver que todo dominio de factorización única es íntegramente cerrado.

Sea R un dominio de factorización única. Sea, $u \in Quot(R)$ entero sobre R, entonces existen $c_0, \ldots, c_{n-1} \in R$ tales que

$$u^n + c_{n-1}u^{n-1} + \ldots + c_0 = 0$$

Escribamos $u = \frac{a}{b}$, con $a, b \in R$ y asumamos que son primos entre sí. Multiplicando la ecuación anterior por b^n obtenemos

$$a^n + c_{n-1}ba^{n-1} + \ldots + c_0b^n = 0$$

Ahora, sea d un divisor irreducible de b, tenemos que, como R es dominio de factorización única, d es primo. Observemos que $d \mid a^n$ dado que d divide a todos los otros términos y como d es primo, $d|a$. Pero a, b son coprimos por lo que d es una unidad y entonces $u \in R$.

Por lo tanto, hemos visto que todo dominio de factorización única es íntegramente cerrado, luego $S[V]$ es íntegramente cerrado en $S(V)$, por lo que $f \in S[V]$ y por ende $f \in S[V]^G$.

□

3.3. Anillos y módulos noetherianos

Como última parte de este tema queremos tratar los anillos y los módulos noetherianos dando a conocer sus respectivas caracterizaciones y teoremas de Hilbert pues tienen un gran peso en el estudio de anillos conmutativos.

Comenzamos aportando el concepto de anillo noetheriano.

Definición 3.3.1. Un anillo conmutativo unitario es **noetheriano** si, y solo si, todo ideal es finitamente generado.

El siguiente teorema nos permite aportar una caracterización a los anillos noetherianos.

Teorema 3.3.2. ***Caracterización de anillos noetherianos.*** *Sea R un anillo conmutativo y unitario, las siguientes afirmaciones son equivalentes:*

1. *Todo ideal I en R es finitamente generado.*
2. *Toda cadena ascendente de ideales*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

es estacionaria, es decir, existe un m tal que $I_m = I_{m+1}$

3. *Cualquier familia no vacía de ideales en R contiene un elemento maximal (con respecto a la inclusión).*

Para sumergirse en una exploración más profunda acerca de los anillos noetherianos, se sugiere consultar [2, Ch. 7].

Ahora que el lector ya conoce lo que es un anillo noetheriano, lo lógico es introducir el concepto de módulo noetheriano.

Definición 3.3.3. Sea R un anillo conmutativo y unitario. Un R-módulo M es **noetheriano** si todo R-submódulo de M es finitamente generado (en particular M es finitamente generado). Ver [14, Ch. 4.2] o [2, Prop. 6.2].

Observación 3.3.4.

a) El anillo R es noetheriano si el R-módulo R_R es noetheriano.

b) Si M es noetheriano, entonces también lo son los submódulos de R y los cocientes de R con respecto a M. Si R es noetheriano, entonces M es noetheriano si, y solo si, M es un R-módulo finitamente generado.

El teorema más importante y con más peso en relación a anillos noetherianos es el teorema de la base de Hilbert que nos permite relacionar un anillo con el correspondiente anillo de polinomios.

Teorema 3.3.5. ***Teorema de la base de Hilbert.*** *Sea R un anillo conmutativo noetheriano. Entonces, el anillo de polinomios $R[X]$ también es noetheriano. Ver [2, Th. 7.5] para la demostración del resultado.*

Corolario 3.3.6. *Una F-algebra conmutativa finitamente generada es noetheriana. Consultar [2, Cor. 7.7].*

Como uno puede deducir, para módulos noetherianos existe un análogo al teorema de la base de Hilbert. La demostración de esta versión del teorema puede ser utilizada para probar la versión simple para anillos y es que, en general, el submódulo de un módulo finitamente generado no es finitamente generado por lo que es interesante conocer el siguiente teorema.

Teorema 3.3.7. *Un módulo finitamente generado sobre un anillo noetheriano es noetheriano. Consultar [14, Ch. 4.2]*

Para cerrar esta sección veamos un último teorema que nos añade un par de características sobre la extensión invariante de anillos.

Teorema 3.3.8. *Sea G un grupo finito.*

a) La extensión de anillos $S[V]^G \subset S[V]$ es finita.

b) El anillo invariante $S[V]^G$ es un álgebra sobre F finitamente generada.

Demostración.

a) Sea $S := S[V]$. Si $s \in S$, entonces para

$$f_s := \prod_{\pi \in G} (Y - \pi s) \in S^G[Y]$$

tenemos que $f_s(s) = 0$.

Dado que f_s es mónico, la extensión de anillos $S^G \subset S$ es entera. Como S está finitamente generado, incluso como un F-álgebra, la extensión $S^G \subset S$ es finita.

b) Sea $\{s_1, \ldots, s_k\} \subset S$ un conjunto generador de S como álgebra sobre F. Definimos $R \subset S^G \subset S$ como el álgebra sobre F generada por los coeficientes de los polinomios $\{f_{s_1}, \ldots, f_{s_k}\} \subseteq S^G[Y]$.

Puesto que R es un álgebra finitamente generada, por el Corolario 3.3.6, es noetheriana. Debido a la elección de R tomada, el módulo S es finitamente generado como módulo sobre R y, por lo tanto, es un módulo noetheriano.

Entonces, por la definición de módulo noetheriano, Definición 3.3.3, el R-submódulo $S^G \subseteq S$ también es noetheriano, lo que implica que S^G es un módulo finitamente generado sobre R.

Como R es un álgebra finitamente generada sobre F, S^G es un álgebra finitamente generada sobre F también.

□

La demostración expuesta del Teorema 3.3.8 es puramente no constructiva. En tiempos de Hilbert esto llevó a la famosa frase de Gordan, que en ese momento era el principal experto en teoría invariante y era un defensor dogmático de la idea de que las matemáticas debían ser constructivas: *Das ist Theologie und nicht Mathematik!* (¡Esto es teología y no matemáticas!) En realidad, el trabajo pionero de Hilbert ahora es reconocido como el inicio y el pilar sobre el que reside la álgebra conmutativa abstracta moderna.

Observación 3.3.9. La afirmación sobre la generación finita en el Teorema 3.3.8 no es válida para grupos arbitrarios. Existe un famoso contraejemplo presentado por Nagata en 1959.

Sean $K = \mathbb{C}$ y a_{ij} números complejos algebraicamente independientes sobre $\mathbb{Q}$ con $i = 1, 2, 3$, $j = 1, 2, \ldots, 16$. Sea $G \subset GL_{32}$ el grupo de todas las matrices diagonales por bloques

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_{16} \end{pmatrix}$$

donde

$$A_j = \begin{pmatrix} c_j & c_j b_j \\ 0 & c_j \end{pmatrix}$$

para $j = 1, \ldots, 16$, con c_j, b_j números complejos arbitrarios tales que

$$c_1 c_2 \cdots c_{16} = 1 \quad y \quad \sum_{j=1}^{16} a_{ij} b_j = 0$$

para $i = 1, 2, 3$.

Entonces $K[x_1, \ldots, x_{32}]^G$ no es finitamente generado. Ver [6, Ex. 2.1.4] y [12].

Sin embargo, esta afirmación es válida para los llamados grupos linealmente reductivos, para ello hay que avanzar a las observaciones que se encuentran después de la Definición 4.1.13. Un grupo G se llama **linealmente reductivo** si para toda representación racional V y todo $v \in V^G \setminus \{0\}$, existe una función lineal invariante $f \in (V^*)^G$ tal que $f(v) \neq 0$.

De hecho, Hilbert trabajó en grupos linealmente reductivos, aunque esta noción no se acuñó hasta más tarde en el tiempo, mientras que Noether desarrolló la maquinaria para grupos finitos.

Además, la afirmación sobre la generación finita en el Teorema 3.3.8 está relacionada con el **problema número 14 de Hilbert**, sean K un cuerpo y $X_1, \ldots, X_n$ indeterminadas, si F es un cuerpo tal que $K \subseteq F \subseteq K(X_1, \ldots, X_n)$ ¿la K-álgebra $F \cap K[X_1, \ldots, X_n]$ es necesariamente finitamente generada?

De otra forma, si $K \subset S(V)$ es un subcuerpo, ¿es $K \subset S[V]$ un álgebra finitamente generada? Dado que, por definición, $S(V)^G \subset S[V] = S[V]^G$ para cualquier grupo G, el contraejemplo de Nagata da una respuesta negativa a este problema también.

Capítulo 4

Cota del grado de Noether

En este capítulo vamos a dirigir nuestra atención a la pregunta de si es posible limitar los grados de los elementos de un sistema de generadores del anillo de invariantes como álgebra.

4.1. Estructuras graduadas, funciones de transferencia relativas e ideales de invariantes

Para poder tratar la pregunta de interés de este capítulo, vamos a ir introduciendo una serie de herramientas necesarias que son nociones derivadas del álgebra conmutativa. Comenzamos esta sección por lo tanto hablando de los primeros conceptos, álgebras y módulos graduados. Para esta parte se puede consultar a mayores [2, Pg. 106].

Definición 4.1.1. Una F-álgebra conmutativa R se llama **graduada** si tenemos

$$R = \bigoplus_{d \geq 0} R_d$$

como espacios vectoriales sobre F, tal que $R_0 = 1 \cdot F \cong F$ y $\dim_F(R_d) \in \mathbb{N}_0$, así como $R_d R_{d'} \subseteq R_{d+d'}$ para $d, d' \geq 0$.

Nótese que R es una suma directa, es decir, para $0 \neq r = [r_d \ / \ d \geq 0] \in \bigoplus_{d \geq 0} R_d$ existe $k \in \mathbb{N}_0$ mínimo tal que $r_d = 0$ para todo $d > k$, y el **grado** de r se define como $deg(r) = k \in \mathbb{N}_0$. El F-subespacio $R_d \subseteq R$ se llama el d-ésimo **componente homogéneo** de R.

Por último, consideremos el **ideal irrelevante** de R, $R+$, que se define como

$$R_+ = \bigoplus_{d > 0} R_d \lhd R,$$

es decir, el conjunto de todos los elementos homogéneos de R que no son invertibles.

El siguiente resultado es un apoyo al ideal irrelevante que acabamos de introducir.

Proposición 4.1.2. *El ideal irrelevante R_+ de una F-álgebra conmutativa graduada R es el único ideal maximal de R.*

Demostración.

Claramente $R_+ \subsetneq R$, pues R_+ no contiene elementos de grado cero. Supongamos que existe un ideal maximal $I \lhd R$, tal que $R_+ \subsetneq I$. El ideal I debe contener al menos un elemento de grado mayor que cero y como $R_+ \subsetneq I$, entonces existe al menos un elemento y de grado cero

tal que $y \in I$. Si tenemos un elemento $y \in I,\ y \neq 0 \in I$ tal que $y \in R_0 = F$ entonces $y^{-1} \in R$ y por lo tanto $1 \in I$ implicando que $I = R$, en contra de que I era un ideal maximal. Por lo tanto, R_+ es el único ideal maximal de R. □

Análogamente a las álgebras graduadas podemos introducir el concepto de módulos graduados que poseen una estructura muy similar.

Definición 4.1.3. Sea R una F-álgebra graduada. Un módulo M sobre R se llama **graduado** si tenemos

$$M = \bigoplus_{d \geq n_M} M_d$$

como espacios vectoriales sobre F, para algún $n_M \in \mathbb{Z}$, tal que $\dim_F(M_d) \in \mathbb{N}_0$, así como $M_d R_{d'} \subseteq M_{d+d'}$ para $d \geq n_M$ y $d' \geq 0$. Para $0 \neq m \in M$, existe $k \geq n_M$ mínimo tal que $m_d = 0$ para todo $d > k$, y el **grado** de m se define como $deg(m) = k \in \mathbb{Z}$. El F-subespacio $M_d \subseteq M$ se llama el **d-ésimo componente homogéneo** de M.

Definición 4.1.4. Si M y N son R-módulos graduados, un **homomorfismo de R-módulos graduados** es un homomorfismo de R-módulos

$$f : M \longrightarrow N$$

tal que $f(M_d) \subseteq N_d$ para todo $d \geq n_M$

Para estas estructuras graduados es conveniente hablar de ideales homogéneos pues son los que toman parte en este tipo de construcciones.

Definición 4.1.5. Decimos que un ideal $I \subset R$ es un **ideal homogéneo** si

$$I = \bigoplus_d I_d, \text{ donde } I_d = I \cap R_d$$

Proposición 4.1.6. *Un ideal I es homogéneo si, y solo si, puede ser generado por elementos homogéneos.*

Demostración.

$\boxed{\Longrightarrow}$

Si I es un ideal homogéneo, entonces por definición

$$I = \bigoplus_d I \cap R_d,$$

luego I está generado por los conjuntos $\{I \cap R_d\}_{d \in \mathbb{Z}_{\geq 0}}$.

$\boxed{\Longleftarrow}$

Supongamos que I está generado por elementos homogéneos $\{h_\alpha\}$. Sea $x \in I$, podemos descomponer de manera única x como una suma de elementos homogéneos,

$$x = \sum_d x_d,$$

donde $x_d \in R_d$. Necesitamos ver que cada $x_d \in I$.

Notemos que $x = \sum_\alpha q_\alpha h_\alpha$ con $q_\alpha \in R$. Si tomamos las componentes homogéneas d-ésimas, encontramos que

$$x_d = \sum_\alpha (q_\alpha)_{d-deg(h_\alpha)} h_\alpha,$$

donde $(q_\alpha)_{d-deg(h_\alpha)}$ hace referencia a la componente homogénea de q_α concentrada en el grado $d - deg(h_\alpha)$.

De esto se deduce fácilmente que cada x_d es una combinación lineal de los h_α y, en consecuencia, pertenece a I.

□

Por lo tanto, si I es un ideal homogéneo, tenemos que $f \in I$ si, y solo si, $f_d \in I_d$ donde

$$f = \sum_d f_d \in \bigoplus_d R_d$$

En relación a las álgebras y módulos graduados y a sus dimensiones tenemos las series de Hilbert, también conocidas como series de Poincaré.

Definición 4.1.7. La **serie de Hilbert** (**serie de Poincaré**) $H_R \in \mathbb{C}[[T]] \subseteq \mathbb{C}((T))$ de una F-álgebra graduada R es la serie de potencias formal definida por

$$H_R(T) := \sum_{d \geq 0} dim_F(R_d) T^d$$

Definición 4.1.8. La **serie de Hilbert** (**serie de Poincaré**) $H_M \in \mathbb{C}((T))$ de un R-módulo graduado M es la serie de Laurent formal definida por

$$H_M(T) := \sum_{d \geq n_M} dim_F(M_d) T^d$$

A continuación, vamos a enunciar una serie de ejemplos y observaciones que nos serán de gran utilidad para ilustrar los conceptos recién introducidos.

Ejemplo 4.1.9. Veamos una serie de ejemplos de estructuras graduadas de las que ya hemos hablado en esta lectura.

- El álgebra simétrica
$$S[V] := \bigoplus_{d \in \mathbb{N}_0} S[V]_d,$$
introducida en la Definición 3.1.1, está graduada.
- El anillo de polinomios $F[X]$, del cual hablamos en la Observación 2.1.2, también está graduado, donde la graduación viene dada por el grado deg_X.
- Como muestra la demostración de la Proposición 3.1.13, el isomorfismo $\beta : S[V] \to F[X]$ de F-álgebras es realmente un isomorfismo de anillos graduados, es decir, para $f \in S[V]$, tenemos $deg_X(f\beta) = deg(f)$.

Observación 4.1.10. Dado que los componentes homogéneos $S[V]_d$, para $d \in \mathbb{N}_0$, son $F[G]$-submódulos de $S[V]$, como vimos en la Observación 3.1.10, el anillo invariante $S[V]^G$ también está graduado, y entonces tenemos

$$S[V]^G = \bigoplus_{d\geq 0} S[V]^G_d,$$

donde de hecho $S[V]_0 = 1 \cdot F$.

Observación 4.1.11. Si $F[X] := F[X_1, \ldots, X_n]$ y $F[X]_d := \{f \in F[X] \ / \ deg_X(f) = d\}$, con $d \in \mathbb{N}_0$, tenemos que

$$dim_F(F[X]_d) = \binom{n+d-1}{d}.$$

La base estándar de este espacio es de la forma $X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$, con $a_1 + \ldots + a_n = d$. Ahora, el número de n-uplas de enteros no negativos cuya suma es d es un problema conocido y es igual a

$$\binom{n+d-1}{n-1} = \binom{n+d-1}{n+d-1-(n-1)} = \binom{n+d-1}{d},$$

este recibe el nombre de d-composiciones débiles de n y su resultado es obtenido mediante el empleo del método del gráfico de estrellas y barras. Este sistema consiste en representar n estrellas por cada elemento de la n-upla necesario y utilizar $d-1$ barras para separar cada n-upla. Con este método el problema se traduce en averiguar de cuántas formas es posible escoger $k-1$ elementos (las barras) de entre $n+k-1$ símbolos (estrellas y barras). Por ejemplo, para $n = 10$ y $d = 3$ una posible combinación es

★★|★★★★|★★★★

y obtenemos que

$$\binom{n+d-1}{d} = \binom{10+3-1}{3} = \binom{12}{3} = \frac{12!}{3!9!} = 220$$

Por otro lado, por inducción obtenemos que

$$\binom{d+k}{k} = \binom{k-1}{k-1} + \binom{k}{k-1} + \cdots + \binom{d+k-1}{k-1}$$

Esto nos lleva a deducir que, por la Definición 4.1.7,

$$H_{F[X]}(T) = \sum_{d\geq 0} dim_F(F[X]_d)T^d = \sum_{d\geq 0} \binom{n+d-1}{d} T^d = \sum_{d\geq 0} \frac{(n+d-1)!}{d!(n-1)!} T^d =$$

$$= \sum_{d\geq 0} \frac{(-1)^d(n+d-1)!}{d!(n-1)!}(-T)^d = \sum_{d\geq 0} \binom{-n}{d}(-T)^d = \frac{1}{(1-T)^n} \in \mathbb{C}((T)).$$

Observación 4.1.12. Análogamente, si $X' := \{X'_1, \ldots, X'_m\} \subseteq F[X]$, para $m \in \mathbb{N}_0$, es algebraicamente independiente, donde X'_i es homogéneo de tal forma que $\deg_X(X'_i) = d_i$, entonces obtenemos de manera similar que

$$H_{F[X']}(T) = \prod_{i=1}^{m} \frac{1}{1-T^{d_i}} \in \mathbb{C}((T)).$$

Se puede consultar [7, Prop. 3.8].

Visto esto, podemos continuar introduciendo herramientas que nos serán útiles para la prueba de la cota del grado de Noether. Vamos a hablar por lo tanto, a partir de ahora, de aplicaciones transversales y, lo más importante, del operador relativo de Reynolds que se trata de un operador muy útil para trabajar entre anillos invariantes. Si el lector desea conocer más al respecto puede consultar [13, Ch. 2.2]

Definición 4.1.13. Sea $H \subseteq G$ tal que $[G : H] < \infty$, y sea V un G-módulo de dimensión finita. La **función de transferencia relativa de H en G**, Tr_H^G, se define como la aplicación F-lineal

$$Tr_H^G : S[V]^H \longrightarrow S[V]^G$$

donde

$$Tr_H^G(f) = \sum_{gH \in G/H} (g \cdot f)$$

La notación significa que la suma se realiza sobre un conjunto de representantes de las clases a izquierda de G sobre H.

Si $|G| < \infty$, entonces la aplicación F-lineal $Tr^G := Tr_1^G : S[V] \to S[V]^G$ se llama **función de transferencia**, en este caso

$$Tr^G(f) = \sum_{g \in G} g \cdot f, \quad f \in S[V]$$

Observación 4.1.14. Es fácil comprobar que Tr_H^G está bien definida y es independiente de la elección de los elementos en G representando las clases a izquierda G/H. Si $g_1H = g_2H$, entonces $g_2^{-1}g_1 \in H$ y por lo tanto

$$\sum_{g_1H \in G/H} g_1 f = \sum_{g_1H \in G/H} g_2 g_2^{-1} g_1 f = \sum_{g_2H \in G/H} g_2 f$$

Observación 4.1.15. Más aún, puesto que para un $g' \in G$ fijo tenemos que

$$g' \cdot Tr_H^G(f) = \sum_{g''H \in G/H} g'g''(f) = \sum_{g'g''H \in G/H} g'g''(f) = Tr_H^G(f),$$

entonces observamos que $Tr_H^G(f) \in S[V]^G$ para cualquier $f \in S[V]$ y además $Tr_H^G\big|_{S[V]_d^H} : S[V]_d^H \to S[V]_d^G$, para $d \in \mathbb{N}_0$.

Lema 4.1.16. *Sean $f \in S[V]^G \subseteq S[V]^H$ y $h \in S[V]^H$, entonces*

$$Tr_H^G(fh) = f \cdot Tr_H^G(h)$$

Demostración.

Usando la propia definición desarrollamos

$$Tr_H^G(fh) = \sum_{gH \in G/H} g(fh) = \sum_{gH \in G/H} (gf) \cdot (gh) =$$

$$= \sum_{gH \in G/H} f \cdot (gh) = f \sum_{gH \in G/H} (gh) = f \cdot Tr_H^G(h)$$

□

Observación 4.1.17. Estos resultados nos permiten deducir que Tr_H^G es un homomorfismo de $S[V]^G$-módulos, y dado que $\mathrm{Tr}_H^G(1) = 1 \cdot [G : H]$, concluimos que

$$Tr_H^G\big|_{S[V]^G} : f \longmapsto f \cdot [G : H]$$

Los elementos en la imagen por la función de transferencia son invariantes bajo la acción de G, lo que nos lleva a deducir que la transferencia proporciona una herramienta para construir formas invariantes de grado arbitrariamente grande.

La siguiente proposición nos aporta una caracterización de las transferencias. Para entender su demostración vamos a enunciar un lema previo debido a Dedekin.

Lema 4.1.18. *Sean A un dominio conmutativo, $F \subseteq A$ un cuerpo y $\alpha_1, \ldots, \alpha_n \in Aut(A)$ automorfismos distintos de A. Entonces $\alpha_1, \ldots, \alpha_n$ son linealmente independientes en $Hom_F(A, A)$. Ver [8, Ch. 1.3, Th. 3].*

Proposición 4.1.19. *Sea $\rho : G \longrightarrow GL_n(F)$ una representación de un grupo finito G sobre el cuerpo F, entonces $Tr^G : S[V] \longrightarrow S[V]^G$ es no nula.*

Demostración.

Por reducción al absurdo, si $Tr^G = 0$, entonces el conjunto $\{\rho(g) \ / \ g \in G\} \subseteq Aut(S[V])$ de automorfismos distintos,

$$\begin{gathered} \rho : S[V] \longrightarrow S[V], \\ f \longrightarrow g \cdot f \end{gathered}$$

es linealmente dependiente en $End_F(S[V]) = End_S(V)$, ya que

$$0 = Tr^G = \sum_{g \in G} 1 \cdot g \Longleftrightarrow \sum_{g \in G} \rho(g) = 0,$$

lo que contradice el Lema 4.1.18. □

Esta proposición nos lleva a una observación referente a la función de transferencia.

Observación 4.1.20. Tenemos que $Im(Tr_H^G) \trianglelefteq S[V]^G$. Para G finito, por la Proposición 4.1.19, tenemos $Im(Tr^G) \neq \{0\}$, pero es posible que $Im(Tr^G) \neq S[V]^G$.

Proposición 4.1.21. *Sea $\rho : G \to GL_n(F)$ una representación de un grupo finito G sobre el cuerpo F, y $H \subseteq G$ un subgrupo. Si $|G : H|$ es invertible sobre el cuerpo F, entonces el homomorfismo de transferencia $Tr_H^G : S[V]^H \to S[V]^G$ es un epimorfismo.*

Esta última proposición es consecuencia de la Observación 4.1.17 ya que si $|G : H|$ es invertible en F, entonces

$$S[V]^G \longrightarrow S[V]^H \longrightarrow S[V]^G$$

es un isomorfismo que consiste en multiplicar por $|G : H| \in F$.

Según la propiedad que verifique la característica de F vamos a poder identificar dos casos bien diferenciados que nos va a llevar a proporcionar la definición de operador de Reynolds normal y relativo.

Definición 4.1.22. Si $char(F) \nmid [G : H]$, entonces el **operador relativo de Reynolds** $\mathcal{R}_H^G$ es el homomorfismo de $S[V]^G$-módulos definido como

$$\mathcal{R}_H^G := \frac{1}{[G : H]} \cdot Tr_H^G : S[V]^H \to S[V]^G,$$

que por lo visto anteriormente es una proyección sobre $S[V]^G$.

Si $char(F) \nmid |G| < \infty$, usando el **operador de Reynolds**, que es sobreyectivo,

$$\mathcal{R}^G := \mathcal{R}_1^G : S[V] \to S[V]^G$$

obtenemos en particular $S[V] = S[V]^G \bigoplus ker(\mathcal{R}^G)$ como módulos sobre $S[V]^G$.

Observación 4.1.23. Para G finito, el caso $char(F) \nmid |G|$ se llama el **caso no modular**, de lo contrario, se llama el **caso modular**. Nosotros vamos a centrarnos exclusivamente en el caso no modular.

Para obtener una mayor comprensión de los últimos conceptos recién introducimos veamos un sencillo ejemplos del cálculo del operador de Reynolds de un polinomio.

Ejemplo 4.1.24. Sea $f = X^2 + YZ + 3Z$, y consideremos $G = S_3$. Como

$$Tr^G(f) = \sum_{g \in G} g \cdot f,$$

entonces, tenemos que

$$\begin{aligned} Tr^G(f)(X,Y,Z) &= (X^2 + YZ + 3Z) + (X^2 + ZY + 3Y) + (Y^2 + XZ + 3Z) + \\ &+ (Y^2 + ZX + 3X) + (Z^2 + XY + 3Y) + (Z^2 + YX + 3X) = \\ &= 2X^2 + 2Y^2 + 2Z^2 + 2XY + 2XZ + 2YZ + 6X + 6Y + 6Z \end{aligned}$$

Y por lo tanto concluimos que

$$R^G(f)(X,Y,Z) = \frac{1}{|G|} \sum_{g \in G} (g \cdot f)(X,Y,Z) = \frac{1}{6} \sum_{g \in G} (g \cdot f)(X,Y,Z) =$$

$$= \frac{1}{6}(2(X^2 + Y^2 + Z^2 + YZ + XZ + XY) + 6(X + Y + Z))$$

Para acabar con las definiciones introductorias de este capítulo vamos a hablar de los ideales generados por invariantes homogéneos.

Definición 4.1.25. El ideal de $S[V]$ generado por todos los invariantes homogéneos de grado estrictamente positivo,

$$\mathcal{I}_G[V] := S[V]_+^G \cdot S[V] = (S[V]_+ \cap S[V]^G) \cdot S[V] \lhd S[V]$$

se llama el **ideal de Hilbert** de $S[V]$ con respecto a G.

Por el Corolario 3.3.6, la F-álgebra $S[V]$ es noetheriana, de esta forma concluimos, por la Definición 3.3.3, que el ideal de Hilbert $\mathcal{I}_G[V] \lhd S[V]$ está generado por un conjunto finito de invariantes homogéneos. Nótese que $\mathcal{I}_G[V] \lhd S[V]$ es un ideal homogéneo, es decir, para $f \in S[V]$ tenemos que $f \in \mathcal{I}_G[V]$ si, y solo si, $f_d \in \mathcal{I}_G[V]$ para todo $d \in \mathbb{N}_0$, donde $f = \sum_d f_d$ es la suma de partes homogéneas de f.

Observación 4.1.26. Expresado en otras palabras, sea $\rho : G \longrightarrow GL_n(F)$ una representación de un grupo finito G sobre el cuerpo F, el ideal de Hilbert es el ideal en $S[V]$ generado por las formas, aplicaciones de un espacio vectorial al cuerpo de escalares en el que está definido, G-invariantes de grado positivo. Generalmente ρ se entiende por el contexto en el que aparece y por eso no lo mencionamos.

Ahora que ya somos conocedores de los conceptos necesarios para este capítulo, como último tópico de esta sección vamos a tratar un teorema que nos va a permitir pasar a la siguiente sección del capítulo y hablar de la cota de Noether que es el tema de verdadero interés.

Teorema 4.1.27. *Sea G un grupo finito tal que $char(F) \nmid |G|$. Sea*

$$\mathcal{I}_G[V] = \sum_{i=1}^{r} f_i S[V] \lhd S[V],$$

donde $f_i \in S[V]^G$ es homogéneo para $i = 1, \ldots, r$. Entonces, $\{f_1, \ldots, f_r\}$ es un conjunto generador de la F-álgebra de $S[V]^G$.

Demostración.

Sea $h \in S[V]^G$ homogéneo tal que $deg(h) = d$. Razonamos por inducción en d. El caso $d = 0$ es claro, por lo tanto, asumamos $d > 0$.

Supongamos que

$$h = \sum_{i=1}^{r} f_i g_i, \quad con\ g_i \in S[V]_{d-deg(f_i)} \quad pues\ h \in I_G[V].$$

Por la Definición 4.1.22 y el Lema 4.1.16, tenemos

$$h = \mathcal{R}^G(h) = \sum_{i=1}^{r} f_i \cdot \mathcal{R}^G(g_i).$$

Entonces, puesto que $deg(R^G(g_i)) = d - deg(f_i) < d$ y $R^G(g_i) \in S[V]^G$, teníamos lo que buscábamos por inducción. □

4.2. Cota de Noether

Con lo visto en la sección anterior, estamos ya preparados para demostrar el límite de grado de Noether, que se cumple en el caso no modular. De hecho, Noether estableció el resultado solo para el caso $char(F) = 0$, pero su prueba es válida para el caso $|G|! \neq 0 \in F$. Finalmente, Fleischmann cerró la brecha para todos los casos no modulares. Presentamos aquí una prueba basada en una simplificación dada por Benson.

Primero vamos a introducir una noción necesaria para el Lema de Benson que vamos a tratar a continuación.

Definición 4.2.1. Sea G un grupo finito, un **ideal de grupo** I es un subconjunto de $F[G]$ satisfaciendo las siguientes propiedades.

1. Si $\sum_{g\in G} \alpha_g g, \sum_{h\in G} \beta_h h \in I$, entonces $\sum_{g,h\in G}(\alpha_g g + \beta_h h) \in I$
2. Para cada $\sum_{g\in G} \alpha_g g \in I$ y $\sum_{h\in G} \lambda_h h \in F[G]$, entonces

$$\left(\sum_{h\in G} \lambda_h\right)\left(\sum_{g\in G} \alpha_g g\right) = \sum_{h,g\in G} \lambda_h \alpha_g (hg) \in I$$

Con este concepto ya podemos presentar el lema de Benson.

Proposición 4.2.2. ***Lema de Benson.*** *Sea G un grupo finito tal que $char(F) \nmid |G|$, y sea $\mathcal{I} \trianglelefteq S[V]$ un $F[G]$-ideal invariante. Entonces, tenemos*

$$\mathcal{I}^{|G|} \subseteq (\mathcal{I} \cap S[V]^G) \cdot S[V] \trianglelefteq S[V].$$

Demostración.

Sea $S := S[V]$ y $\{f_\pi \ / \ \pi \in G\} \subseteq \mathcal{I}$. Entonces tenemos

$$\prod_{\pi \in G} (\sigma\pi f_\pi - f_\pi) = 0,$$

para $\sigma \in G$. Expandiendo el producto y sumando sobre $\sigma \in G$ esto deriva en

$$\sum_{M \subseteq G} (-1)^{|G \setminus M|} \cdot \left(\sum_{\sigma \in G} \prod_{\pi \in M} \sigma\pi f_\pi \right) \cdot \left(\prod_{\pi \in G \setminus M} f_\pi \right) = 0$$

donde la suma se realiza sobre todos los subconjuntos $M \subseteq G$. Si $M \neq \emptyset$, entonces tenemos

$$\left(\sum_{\sigma \in G} \prod_{\pi \in M} \sigma\pi f_\pi \right) \in \mathcal{I} \cap S^G,$$

y de tal manera el sumando correspondiente de la suma anterior es un elemento de $(\mathcal{I} \cap S^G) \cdot S$. Por lo tanto, para $M = \emptyset$, obtenemos de aquí que

$$\pm |G| \cdot \left(\prod_{\pi \in G} f_\pi \right) \in (\mathcal{I} \cap S^G) \cdot S,$$

por lo que finalmente

$$\left(\prod_{\pi \in G} f_\pi \right) \in (\mathcal{I} \cap S^G) \cdot S.$$

□

Como consecuencia del lema de Benson obtenemos el siguiente teorema que nos proporciona la cota del grado de Noether.

Teorema 4.2.3. *Sea G un grupo finito tal que $char(F) \nmid |G|$. Entonces existe un conjunto generador del ideal de Hilbert $I_G[V] \lhd S[V]$ tal que sus elementos son homogéneos de grado no superior a $|G|$.*

Demostración.

Sea $S := S[V]$. Utilizando la identificación de la Proposición 3.1.13, sea $X^\alpha \in S$ un monomio de grado $\geq |G|$. Por la Proposición 4.2.2, aplicada al ideal irrelevante $S_+ \lhd S$, tenemos

$$X^\alpha \in (S_+ \cap S^G) \cdot S = \mathcal{I}_G[V] \lhd S.$$

Si $deg(X^\alpha) > |G|$, sea $X^\alpha = X^{\alpha'} \cdot X^{\alpha''}$, de tal forma que $\deg(X^{\alpha'}) = |G|$. Por lo tanto, ya tenemos $X^{\alpha'} \in \mathcal{I}_G[V]$.

Consideremos ahora

$$\mathcal{I}_G[V] = \sum_{i=1}^{r} f_i S \lhd S$$

un conjunto generador minimal y homogéneo. Si algún $deg(f_r) > |G|$, por ejemplo, por lo anterior, concluimos que

$$f_r \in \sum_{j, deg(f_j) \leq |G|} f_j S \lhd S,$$

lo cual es una contradicción. □

Corolario 4.2.4. *Existe un conjunto generador del F-álgebra $S[V]^G$ donde todos sus elementos son homogéneos de grado $\leq |G|$.*

Observación 4.2.5. Según los Teoremas 4.1.27 y 4.2.3, existe un conjunto generador de la F-álgebra $S[V]^G$ en

$$\bigoplus_{d=1}^{|G|} S[V]_d^G.$$

Utilizando el operador de Reynolds, que es sobreyectivo y conserva los grados como vimos en la Definición 4.1.22, tenemos que

$$\mathcal{R}^G\left(\bigoplus_{d=1}^{|G|} S[V]_d\right) = \bigoplus_{d=1}^{|G|} S[V]_d^G.$$

Por lo tanto, evaluando el operador de Reynolds en los monomios X^α, donde $deg(X^\alpha) \leq |G|$, se obtiene un conjunto, no necesariamente minimal, que genera la F-álgebra $S[V]^G$.

Observación 4.2.6. La cota del grado de Noether es óptima en el sentido en que no se puede mejorar solo considerando el orden del grupo: Sea $G = \langle \pi \rangle \cong C_n$ el grupo cíclico de orden n, sea F un cuerpo tal que $char(F) \nmid n$, sea $\zeta \in F$ una raíz primitiva n-ésima de la unidad, y sea $G \to GL_1(F) : \pi \mapsto \zeta$. Entonces, el anillo de invariantes es

$$S[V]^G \cong F[X_1^n] \subseteq F[X_1] \cong S[V].$$

Observación 4.2.7. En el caso modular, la cota del grado de Noether no siempre se cumple. Un contraejemplo de esto puede ser encontrado en [6, Ex. 3.3.1].

Capítulo 5

La fórmula de Molien

A lo largo de las próximas secciones vamos a considerar G como un grupo finito y $F \subseteq \mathbb{C}$. El objetivo de este capítulo es determinar la serie de Hilbert de anillos invariantes, para ello vamos a hacer uso de la teoría que trata sobre la característica de grupos finitos.

5.1. Desarrollos previos

Vamos a comenzar definiendo algunos conceptos que nos van a ser de ayuda a la hora de evaluar la fórmula de Molien.

Definición 5.1.1. Sea V un módulo de dimensión finita sobre el grupo de anillos $F[G]$, consideramos la **sigma-serie** dada por

$$\sigma_T(V) := \sum_{d=0}^{\infty} S[V]_d \cdot T^d,$$

que es una serie formal de potencias con $K[G]$-módulos como coeficientes. Ver [6, Ch. 3.2.1]

Definición 5.1.2. Sea π una acción de G sobre V y sean $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ los autovalores asociados a $D_V(\pi)$, definimos el **carácter de Brauer** como

$$\Phi_\pi(V) := \lambda_1 + \ldots + \lambda_n,$$

y más aun

$$det_V(1 - \pi T) := (1 - \lambda_1 T) \cdots (1 - \lambda_n T) \in F[T],$$

donde $1 - D_V(\pi)\dot{T} \in F[T]^{n \times n}$ y $\det_V(1 - \pi T) := \det_{F[T]^{n\times n}}(1 - D_V(\pi)T) \in F[T]$. Para una explicación más detallada se puede consultar [15, Ch. 10.1].

En este capítulo, nuestro principal objetivo es desarrollar la fórmula de Molien y estudiar el comportamiento de su estructura. Para entenderlo de una forma más generalizada, la fórmula de Molien es un teorema para las series de Poincaré de los invariantes de característica cero, $H_R \in \mathbb{C}[[T]] \subseteq \mathbb{C}((T))$, concepto introducido en 4.1.7.

Si F es un cuerpo de característica cero y $\rho : G \longrightarrow GL_n(F)$ una representación del grupo finito G, la aplicación

$$\pi^G = \frac{1}{|G|} \sum_{g \in G} g$$

es una proyección sobre $S[V]$ con imagen $S[V]^G$. Por lo tanto, la dimensión de $S[V]^G_j$ es igual a la traza de la matriz representando π en $S[V]_j$. Tenemos de esta forma

$$H_{S[V]^G}(T) = \frac{1}{|G|}\sum_{g\in G}\sum_{j=0}^{\infty} Tr_{S[V]_j}(g)T^j$$

Observación 5.1.3. En muchos casos es posible computar la serie de Poincaré de un álgebra graduada conmutativa directamente. Por ejemplo, para el álgebra polinómica $\mathbb{F}[z]$ sobre un único generador z de grado d, encontramos que

$$H_{\mathbb{F}[z]}(T) = \sum_{i=0}^{\infty} T^{d_i} = \frac{1}{1-T^d}$$

y entonces por la regla del producto de tensores

$$H_{\mathbb{F}[z_1,\ldots,z_n]}(T) = \prod_{i=1}^{n}\frac{1}{(1-T^{d_i})}, \quad deg(z_i) = d_i,\ i = 1,\ldots,n,$$

como vimos en la Observación 4.1.12.

La siguiente fórmula para la traza funciona independientemente de la característica de F.

Proposición 5.1.4. *Para $\pi \in G$ tenemos*

$$\sum_{d\geq 0} Tr_{S[V]_d}(\pi)\cdot T^d = \frac{1}{\det_V(1-\pi T)} \in F((T)),$$

donde $Tr_{S[V]_d}(\pi) \in F$ es la traza usual de una matriz.

Demostración.

Podemos asumir que $\mathbb{Q}[\zeta_{|G|}] \subseteq F$, donde $\zeta_{|G|} := \exp\frac{2\pi i}{|G|} \in \mathbb{C}^*$ es una raíz primitiva de la unidad de orden $|G|$-ésimo. Puesto que $\pi \in G$, podemos considerar la representación $D_V(\pi)$ sobre el espacio vectorial V, que es diagonalizable. En particular, sean $\lambda_1,\ldots,\lambda_n \in F$ los autovalores de $D_V(\pi)$, por la Definición 5.1.2 sabemos que podemos escribir el determinante de la matriz $1-\pi T$ en términos de los autovalores $\lambda_1,\ldots,\lambda_n$,

$$det_V(1-\pi T) = \prod_{i=1}^{n}(1-\lambda_i T) \in F[T].$$

Ahora, los autovalores de la representación $D_{S[V]_d}(\pi)$ son

$$\prod_{i=1}^{n}\lambda_i^{\alpha_i} \in F,$$

donde $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}_0^n$ tal que $\sum_{i=1}^n \alpha_i = d$. Entonces, como la traza de una matriz diagonal es la suma de sus autovalores, tenemos que

$$Tr_{S[V]_d}(\pi) = \sum_{\alpha\in\mathbb{N}_0^n,\sum_{i=1}^n \alpha_i = d}\ \prod_{i=1}^{n}\lambda_i^{\alpha_i}$$

por lo tanto

$$\sum_{d\geq 0} Tr_{S[V]_d}(\pi)\cdot T^d = \sum_{\alpha\in\mathbb{N}_0^n}\prod_{i=1}^{n}(\lambda_i T)^{\alpha_i} = \prod_{i=1}^{n}\sum_{j\geq 0}(\lambda_i T)^j = \prod_{i=1}^{n}\frac{1}{1-\lambda_i T} =$$

$$= \frac{1}{\prod_{i=1}^{n}(1-\lambda_i T)} = \frac{1}{\det_V(1-\pi T)} \in F((T)),$$

donde hemos usado la suma de una serie geométrica. □

Ejemplo 5.1.5. Para $g = 1$ se cumple que

$$\sum_{j=0}^{\infty} T^j dim_K S[V]_j = \frac{1}{(1-T)^n}$$

Como ya comprobamos en la Observación 4.1.11. También es posible consultar [3, Pg. 22].

5.2. La fórmula de Molien

Los resultados vistos en la sección anterior nos permiten finalmente introducir la fórmula de Molien al lector.

Teorema 5.2.1. ***Fórmula de Molien, 1897.*** *Tenemos que*

$$H_{S[V]^G} = \frac{1}{|G|}\sum_{\pi\in G}\frac{1}{\det_V(1-\pi T)} \in F((T)).$$

Demostración.

El operador de Reynolds $\mathcal{R}^G$, introducido en la Definición 4.1.22, proyecta $S[V]_d$ en $S[V]_d^G$, para $d \in \mathbb{N}_0$. Usando esto obtenemos

$$\dim_F(S[V]_d^G) = Tr_{S[V]_d}(\mathcal{R}^G) = \frac{1}{|G|}\sum_{\pi\in G} Tr_{S[V]_d}(\pi) \in F.$$

Por lo tanto, la afirmación se sigue de la Proposición 5.1.4. □

Las siguientes observaciones son muy útiles para entender el contexto en el cual puede hacerse uso de esta fórmula. A su misma vez, vamos a poder analizar una aplicación más práctica de la fórmula de Molien.

Observación 5.2.2. El lado izquierdo de la expresión de la fórmula de Molien reside en $\mathbb{Q}(T)$, mientras que el lado derecho reside en $F(T)$, por lo que la ecuación toma sentido si F posee característica cero.

Para la siguiente observación vamos a necesitar introducir el concepto de carácter de una representación y también es preciso hacer uso de las identidades de Newton, así que vamos a introducir esto primero.

Definición 5.2.3. El **carácter** de una representación $\rho : G \longrightarrow GL_n(V)$ es una función $\chi_V : G \longrightarrow F$ definida como

$$\chi(g) = Tr(\rho(g))$$

El carácter de una representación conserva mucha información sobre dicha representación y es una herramienta muy útil a la hora de trabajar con representaciones de grupos finitos.

Por otro lado, las identidades de Newton nos van a permitir relacionar los polinomios simétricos elementales $e_i^{(n)}$ con las sumas de potencias de los autovalores $p_{n,j}$. Para esta sección puede consultarse [13, Pg. 81].

Teorema 5.2.4. ***Identidades de Newton.*** *Sean $X_1, \ldots, X_n$ variables, para $k \geq 1$ denotamos por $p_{n,k}(X_1, \ldots, X_n)$ la k-ésima suma de potencias en n variables*

$$p_{n,k}(X_1, \ldots, X_n) = \sum_{i=1}^{n} X_i^k = X_1^k + \ldots + X_n^k,$$

entonces las identidades de Newton se establecen como

$$ke_k^{(n)} = \sum_{i=1}^{k} (-1)^{i-1} p_{n,i} e_{k-i}^{(n)}, \quad \textit{con } k \in \{1, \ldots, n\},$$

donde $e_k^{(n)}$ son los polinomios simétricos elementales, recordar la Definición 2.1.6.

Demostración.

Vamos a probar el caso especial en que $k = n$. Por el Teorema 2.1.9 de las fórmulas de Cardano-Vieta tenemos que

$$\prod_{i=1}^{k} (T - X_i) = \sum_{i=0}^{k} (-1)^{k-i} e_{k-i}^{(k)} T^i.$$

Al evaluar T en X_j con $1 \leq j \leq k$ obtenemos

$$0 = \prod_{i=1}^{k} (X_j - X_i) = \sum_{i=0}^{k} (-1)^{k-i} e_{k-i}^{(k)} X_j^i, \ 1 \leq j \leq k.$$

Y finalmente sumando sobre todas las j

$$0 = (-1)^k k e_k^{(k)} + \sum_{i=1}^{k} (-1)^{k-i} e_{k-i}^{(k)} p_{k,i}.$$

Es decir,

$$(-1)^{k+1} k e_k^{(k)} = \sum_{i=1}^{k} (-1)^{k-i} e_{k-i}^{(k)} p_{k,i}.$$

Lo que nos lleva a concluir, una vez que hemos simplificado y agrupado, que

$$ke_k^{(k)} = \sum_{i=1}^{k} (-1)^{-(i+1)} e_{k-i}^{(k)} p_{k,i} = \sum_{i=1}^{k} (-1)^{i-1} p_{k,i} e_{k-i}^{(k)},$$

como queríamos probar. □

Observación 5.2.5. La fórmula de Molien es muy fácil de evaluar en la práctica. Para esto, nótese que

$$det_V(1-\pi T)=\prod_{i=1}^{n}(1-\lambda_i T)=T^n\cdot\prod_{i=1}^{n}\left(T^{-1}-\lambda_i\right),$$

para $\pi\in G$. Por lo tanto, por la Definición 2.1.6, podemos expandir usando los polinomios simétricos elementales

$$det_V(1-\pi T)=T^n\cdot\left(T^{-n}+\sum_{i=1}^{n}(-1)^i e_i^{(n)}(\lambda_1,\ldots,\lambda_n)T^{i-n}\right)=$$

$$=1+\sum_{i=1}^{n}(-1)^i e_i^{(n)}(\lambda_1,\ldots,\lambda_n)T^i\in F[T].$$

Usando las identidades de Newton, Teorema 5.2.4,

$$ke_k=\sum_{i=1}^{k}(-1)^{i-1}p_{n,i}e_{k-i},\quad con\ k\in\{1,\ldots,n\},$$

los polinomios simétricos elementales $e_i^{(n)}(\lambda_1,\ldots,\lambda_n)\in F$, para $i\in\{1,\ldots,n\}$, se pueden determinar a partir de las sumas de potencias $p_{n,j}(\lambda_1,\ldots,\lambda_n)\in F$, para $j\in\{1,\ldots,n\}$.

Finalmente, tenemos

$$p_{n,j}(\lambda_1,\ldots,\lambda_n)=\sum_{i=1}^{n}\lambda_i^j=Tr_V(\pi^j)=\chi_V(\pi^j),$$

donde $\chi_V\in\mathbb{Z}Irr_{\mathbb{C}}(G)$ denota el carácter ordinario de G inducido por V y $\mathbb{Z}Irr_{\mathbb{C}}(G)$ representa el conjunto de combinaciones lineales de carácteres irreducibles, es decir, carácteres de representaciones sin subrepresentaciones propias no triviales, con coeficientes enteros.

Por lo tanto, la Fórmula de Molien se puede evaluar una vez que χ_V y las llamadas **aplicaciones de potencia**

$$p_j:\mathcal{C}l(G)\longrightarrow\mathcal{C}l(G),$$

para $j\in\{1,\ldots,n\}$, en las clases de conjugación $\mathcal{C}l(G)$ de G son conocidas. En otras palabras, podemos evaluar la fórmula de Molien en el momento en que conocemos el carácter de Brauer asociado a V y las aplicaciones de potencia de G, sin que sea necesaria la computación de ningún determinante.

Esta información suele poder encontrarse en las bibliotecas de tablas de carácteres, por ejemplo, en la del sistema algebraico computacional GAP, y de hecho, la Fórmula de Molien también está implementada allí.

Debido a la gran importancia del teorema de Molien, la serie de Hilbert de un anillo invariante a veces también se denomina serie de Molien.

Para finalizar este capítulo veamos ahora con un ejemplo cómo es el funcionamiento de la fórmula de Molien.

Ejemplo 5.2.6. Para $k\in\mathbb{N}$, sea $G=\langle\delta,\sigma\rangle\cong D_{2k}$ el grupo diedral de orden $2k$. Sea $\zeta_k:=\exp\frac{2\pi i}{k}\in\mathbb{C}^*$ una raíz primitiva k-ésima de la unidad, y sea

$$D_V:G\to GL_2(\mathbb{C}):\delta\mapsto\begin{bmatrix}\zeta_k & 0\\ 0 & \zeta_k^{-1}\end{bmatrix},\ \sigma\mapsto\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

Tenemos que $G = \{\delta^i, \sigma\delta^i \ / \ i \in \{0, 1, \ldots, k-1\}\}$, donde $\delta^i \in G$ es una rotación teniendo los autovalores $\zeta_k^{\pm i} \in \mathbb{C}$, y donde $\sigma\delta^i \in G$ es una reflexión, por lo tanto teniendo los autovalores $\pm 1 \in \mathbb{C}$.

Entonces, mediante la Fórmula de Molien 5.2.1, la serie de Hilbert de $S[V]^G$ viene dada por

$$H_{S[V]^G} = \frac{1}{2k} \cdot \left(\frac{k}{(1-T)\cdot(1+T)} + \sum_{i=0}^{k-1} \frac{1}{(1-\zeta_k^i T)\cdot(1-\zeta_k^{-i}T)} \right) \in \mathbb{C}((T)).$$

Desarrollando esta expresión obtenemos que

$$H_{S[V]^G} = \frac{1}{2k} \cdot \left(\frac{k}{(1-T^2)} + \sum_{i=0}^{k-1} \frac{1}{1-\zeta_k^i T - \zeta_k^{-i}T + \zeta_k^i\zeta_k^{-i}T^2} \right) =$$

$$= \frac{1}{2k} \cdot \left(\frac{k}{(1-T^2)} + \sum_{i=0}^{k-1} \frac{1}{1-(\zeta_k^i + \zeta_k^{-i})T + T^2} \right) = \cdots$$

$$\cdots = \frac{1}{(1-T^2)\cdot(1-T^k)} \in \mathbb{C}((T)).$$

Por lo tanto, por la Observación 4.1.11, estamos tentados a conjeturar que $S[V]^G$ es un anillo de polinomios en dos indeterminadas de grados 2 y k. De hecho, mediante la identificación de la Proposición 3.1.13, tenemos

$$f_1 := X_1X_2 \in S[V]^G \quad y \quad f_2 := X_1^k + X_2^k \in S[V]^G.$$

Por el Criterio Jacobiano, ver Proposición 6.3.6 en el siguiente capítulo, fácilmente concluimos que $\{f_1, f_2\} \subseteq \mathbb{C}[X_1, X_2]$ es algebraicamente independiente, y por lo tanto, la serie de Hilbert de $\mathbb{C}[f_1, f_2] \subseteq S[V]^G$ viene dada por

$$H_{\mathbb{C}[f_1,f_2]} = \frac{1}{(1-T^2)\cdot(1-T^k)} \in \mathbb{C}((T)).$$

Así que finalmente concluimos que $\mathbb{C}[f_1, f_2] = S[V]^G$, que de hecho es efectivamente un anillo de polinomios.

Capítulo 6

Anillos de polinomios invariantes

En este capítulo nuestro principal objetivo es obtener una respuesta a la pregunta de si podemos caracterizar aquellas representaciones cuyo anillo invariante es un anillo de polinomios. De esta forma, el resultado principal a tratar es el Teorema 6.3.7 de Shephard-Todd.

Para poder estudiar esta pregunta, vamos a comenzar considerando la expansión de Laurent de $H_{S[V]^G}$ en $T = 1$, lo que nos lleva directamente a considerar pseudorreflexiones, la primera noción a definir en este capítulo.

Para un análisis más profundo y complementar este capítulo es posible consultar [7, Ch. 3], [3, Ch. 2.5, Ch.7] o también [13, Ch. 7.1].

A lo largo de este capítulo vamos a considerar que G es un grupo finito, $F \subseteq \mathbb{C}$, y D_V es una **representación fiel** de F, es decir, tenemos $ker(D_V) = \{1\} \subseteq G$.

6.1. Pseudorreflexiones

Abordamos esta sección introduciendo el concepto que le da nombre así como otras nociones relacionadas.

Definición 6.1.1. Un elemento $1 \neq \pi \in G$ se llama **pseudorreflexión** si, para el espacio vectorial $Fix_V(\pi) \subseteq V$ de puntos fijos de $\pi \in G$, identificando π con $D_V(\pi)$, tenemos $dim_F(Fix_V(\pi)) = n - 1$, y si además $\pi^2 = 1$, entonces π se llama **reflexión**. El F-espacio $Fix_V(\pi) \subseteq V$ de puntos fijos de una pseudorreflexión se llama su **hiperplano reflectante**. Vamos a denotar por $N_G \in \mathbb{N}_0$ al **número de pseudorreflexiones** en G.

Nótese que estos conceptos dependen de la representación D_V escogida y toman sentido para cualquier cuerpo arbitrario F.

Definición 6.1.2. Para una función racional

$$0 \neq H = \frac{H'}{H''} \in \mathbb{C}(T),$$

donde $H', H'' \in \mathbb{C}[T]$ son coprimos, consideremos $c \in \mathbb{C}$ y sea $k \in \mathbb{Z}$ tal que

$$\left((T-c)^{-k} \cdot H\right)(c) \neq \begin{cases} 0 \\ \infty \end{cases}$$

Entonces, $ord_c(H) := k \in \mathbb{Z}$ es el **orden** de H en $T = c$. Si $H = 0$, entonces consideramos $ord_c(H) := \infty$.

La siguiente observación nos permite ilustrar el concepto de orden.

Observación 6.1.3. Como en la demostración de la Proposición 5.1.4, sean $\lambda_1, \ldots, \lambda_n \in F$ los autovalores de $D_V(\pi)$, para $\pi \in G$. Gracias a la expresión

$$det_V(1 - \pi T) = \prod_{i=1}^{n}(1 - \lambda_i T) \in F[T],$$

podemos observar que $ord_1(det_V(1 - \pi T)) \leq n$. Además tenemos que $ord_1(\det_V(1 - \pi T)) = n$ si, y solo si, $\pi = 1$. Para $\pi = 1$ todos los autovalores son 1 y por la expresión anterior deducimos que

$$det_V(1 - \pi \cdot T) = (1 - T)^n$$

obteniendo que $ord_1(\det_V(1 - \pi T)) = n$. Para $\pi \neq 1$, necesariamente $ord_1(\det_V(1 - \pi T)) \leq n - 1$.

Por lo tanto, por la Fórmula de Molien, recordar el Teorema 5.2.1, podemos determinar que $ord_1(H_{S[V]^G}) = -n$. Además,

$$\left((T-1)^n \cdot H_{S[V]^G}\right)(1) = \frac{(-1)^n}{|G|}.$$

Ahora si consideramos la expansión

$$H_{S[V]^G} = \frac{(-1)^n}{|G|} \cdot (T-1)^{-n} + H'_{S[V]^G} \in F(T),$$

obtenemos que $ord_1(H'_{S[V]^G}) \geq -(n-1)$.

Por otro lado, $ord_1(\det_V(1 - \pi T)) = n - 1$ si, y solo si, $\pi \neq 1$ tiene el autovalor 1 con multiplicidad $n-1$, es decir, si, y solo si, π es una pseudorreflexión como vimos en la Definición 6.1.1. En este caso, sea $1 \neq \lambda \in F$ el autovalor no trivial de π, entonces tenemos

$$\frac{(T-1)^{n-1}}{\det_V(1 - \pi T)}(1) = \frac{(-1)^{n-1}}{(1-\lambda)}.$$

Dado que se verifica que

$$\frac{1}{1-\lambda} + \frac{1}{1-\lambda^{-1}} = 1,$$

al emparejar cada pseudorreflexión con su inverso y sumar sobre todas las pseudorreflexiones en G obtenemos como resultado

$$\left((T-1)^{n-1} \cdot H'_{S[V]^G}\right)(1) = \frac{(-1)^{n-1} \cdot N_G}{2 \cdot |G|}.$$

Así, finalmente, concluimos que

$$H_{S[V]^G} := \frac{(-1)^n}{|G|} \cdot (T-1)^{-n} + \frac{(-1)^{n-1} \cdot N_G}{2 \cdot |G|} \cdot (T-1)^{-(n-1)} + H''_{S[V]^G} \in F(T),$$

donde $ord_1(H''_{S[V]^G}) \geq -(n-2)$.

Como anunciamos previamente en la introducción el verdadero resultado de interés que trataremos en este capítulo es el Teorema de Shephard-Todd, Teorema 6.3.7. Debido a su dificultad, para poder estudiarlo vamos a ir encaminando algunos resultados previos comenzando con el Lema 6.1.4.

Lema 6.1.4. *Supongamos que G está generado por pseudorreflexiones, y sea*

$$R := S[V]^G \subseteq S[V] =: S.$$

Además, sean $h_1, \dots, h_r \in R$ y $h \in R \setminus (\sum_{i=1}^r h_i R)$, y sean $p, p_1, \dots, p_r \in S$ homogéneos tales que

$$hp = \sum_{i=1}^r h_i p_i.$$

Entonces, tenemos que $p \in \mathcal{I}_G[V]$, donde $\mathcal{I}_G[V] \lhd S$ denota el ideal de Hilbert, introducido en la Definición 4.1.25.

Demostración.

Vamos a realizar la demostración por inducción sobre $\deg(p)$.

Supongamos que $\deg(p) = 0$ y $p \neq 0$. Entonces tenemos que

$$hp = \mathcal{R}^G(hp) = \sum_{i=1}^r h_i \cdot \mathcal{R}^G(p_i) \in \sum_{i=1}^r h_i R,$$

donde $\mathcal{R}^G$ denota el operador de Reynolds, puede consultar la definición 4.1.22. Esto contradice la elección de h pues $h \in R \setminus (\sum_{i=1}^r h_i R)$ y por reducción al absurdo concluimos que $p = 0$.

Ahora, supongamos que $\deg(p) > 0$. Sea $\pi \in G$ una pseudorreflexión, y supongamos que su hiperplano de reflexión viene dado por $Fix_V(\pi) = \langle b_2, \dots, b_n \rangle_F$, donde $\{b_1, \dots, b_n\} \subseteq V$ es una F-base de V.

Usando la identificación de la Proposición 3.1.13, obtenemos que $\pi X_i = X_i$, para $i \geq 2$. Por lo tanto, tenemos que $(\pi - 1)X^\alpha = 0$ para todos los monomios $X^\alpha \in F[X]$, donde $\alpha \in \mathbb{N}_0^n$ tal que $\alpha_1 = 0$. De esto concluimos que existen $p', p_i' \in S$ homogéneos tales que

$$(\pi - 1)p = X_1 p' \in S \quad y \quad (\pi - 1)p_i = X_1 p_i' \in S,$$

para $i \in \{1, \dots, r\}$. En particular, $\deg(p') < \deg(p)$.

Aplicando $\pi - 1$ a la ecuación $hp = \sum_{i=1}^r h_i p_i$ obtenemos

$$X_1 hp' = X_1 \sum_{i=1}^r h_i p_i'.$$

Por lo tanto, por inducción, tenemos $p' \in \mathcal{I} := \mathcal{I}_G[V]$, y así $(\pi - 1)p = X_1 p' \in \mathcal{I}$ también.

Ahora, sea $^-\colon S \to S/\mathcal{I}$ el epimorfismo natural de F-álgebras. Dado que $\mathcal{I} \lhd S$ es un $F[G]$-submódulo, el grupo G actúa sobre la F-álgebra cociente $S/\mathcal{I}$. Por lo anterior, tenemos $\pi\bar{p} = \bar{p}$ para todas las pseudorreflexiones $\pi \in G$, y como G está generado por pseudorreflexiones, tenemos $\pi\bar{p} = \bar{p}$ para todas las $\pi \in G$, es decir, $\bar{p}$ es invariante por G.

Dado que $\mathcal{R}^G(p) \in R_+ \subseteq \mathcal{I}$, concluimos que $p + \mathcal{I} = \mathcal{R}^G(p) + \mathcal{I} = 0 + \mathcal{I} \in S/\mathcal{I}$, por lo tanto, $p \in \mathcal{I}$. □

6.2. Pseudorreflexiones y anillos de polinomios

El objetivo en esta sección es obtener una serie de resultados que nos aporten ciertas relaciones entre pseudorreflexiones y anillos de polinomios, todo encaminado para poder realizar la prueba del Teorema de Shephard-Todd 6.3.7.

El siguiente teorema a estudiar nos da una implicación del mencionado Teorema 6.3.7.

Teorema 6.2.1. *Sea G generado por pseudorreflexiones. Entonces, $S[V]^G$ es un anillo de polinomios.*

Demostración.

Mantenemos la notación del Lema 6.1.4, y consideramos

$$\mathcal{I} := \mathcal{I}_G[V] = \sum_{i=1}^{r} f_i S \lhd S,$$

donde $f_i \in R$ es homogéneo tal que $d_i := deg(f_i)$, y $r \in \mathbb{N}_0$ es mínimo.

Por el Teorema 4.1.27 sabemos que el conjunto $\{f_1, \ldots, f_r\} \subseteq R$ es un sistema de generadores como F-álgebra de R y por lo tanto es suficiente demostrar que $\{f_1, \ldots, f_r\}$ es algebraicamente independiente.

Supongamos, por reducción al absurdo, que existe $0 \neq h \in F[Y] := F[Y_1, \ldots, Y_r]$ tal que $h(f_1, \ldots, f_r) = 0$. Podemos suponer también que h es homogéneo, es decir, que hay un $d \in \mathbb{N}_0$ tal que para todos los monomios de la forma $Y^\alpha \in F[Y]$, donde $\alpha \in \mathbb{N}_0^r$, que aparecen en h se tiene que

$$\sum_{i=1}^{r} \alpha_i d_i = d.$$

A continuación vamos a definir

$$h_i := \frac{\partial h}{\partial Y_i}(f_1, \ldots, f_r) \in R,$$

para $i \in \{1, \ldots, r\}$, de modo que $\deg(h_i) = d - d_i$. Reordenando las variables podemos suponer que

$$\sum_{i=1}^{r'} h_i R = \sum_{i=1}^{r} h_i R \lhd R,$$

para $\{h_1, \ldots, h_r'\} \subseteq \{h_1, \ldots, h_r\}$ donde $1 \leq r' \leq r$ es mínimo.

De esta forma, para $j > r'$, existe $g_{ij} \in R$, para $i \in \{1, \ldots, r'\}$, homogéneo tal que

$$deg(g_{ij}) = \deg(h_j) - \deg(h_i) = d_i - d_j \quad y \quad h_j = \sum_{i=1}^{r'} h_i g_{ij}.$$

Ahora consideramos la derivada parcial respecto a X_k, $\frac{\partial}{\partial X_k}$, para $k \in \{1, \ldots, n\}$. Utilizando la regla de la cadena llegamos a la expresión

$$0 = \frac{\partial}{\partial X_k} h(f_1, \ldots, f_r) = \sum_{i=1}^{r} \frac{\partial h}{\partial Y_i}(f_1, \ldots, f_r) \cdot \frac{\partial f_i}{\partial X_k} = \sum_{i=1}^{r} h_i \cdot \frac{\partial f_i}{\partial X_k}$$

Y puesto que para $j > r'$ podemos expresar h_j en términos de los h_i con $i \leq r'$ tenemos que

$$0 = \sum_{i=1}^{r'} h_i \cdot \left(\frac{\partial f_i}{\partial X_k} + \sum_{j=r'+1}^{r} g_{ij} \cdot \frac{\partial f_j}{\partial X_k} \right) \in S.$$

Ahora consideremos

$$p_i := \frac{\partial f_i}{\partial X_k} + \sum_{j=r'+1}^{r} g_{ij} \cdot \frac{\partial f_j}{\partial X_k} \in S,$$

para $i \in \{1, \ldots, r'\}$. De esta forma, p_i es homogéneo con, o bien $deg(p_i) = d_i - 1$, o bien $p_i = 0$. Por construcción, podemos suponer que $p_1 \neq 0$ y $h_1 \notin h_2R + \cdots + h_rR$, y así por el Lema 6.1.4 concluimos que $p_1 \in \mathcal{I}$, y por lo tanto,

$$p_1 = \sum_{i=1}^{r} f_i q_i,$$

para algún $q_i \in S$ homogéneo.

Por otro lado teníamos que

$$p_1 = \frac{\partial f_1}{\partial X_k} + \sum_{j=r'+1}^{r} g_{1j} \cdot \frac{\partial f_j}{\partial X_k}.$$

Al multiplicar por X_k y sumar sobre todos los $k \in \{1, \ldots, n\}$, mediante la identidad de Euler que viene dada por

$$\sum_{k=1}^{n} X_k \cdot \frac{\partial f}{\partial X_k} = deg_X(f) \cdot f, \text{ para } f \in S,$$

deducimos la igualdad

$$d_1 \cdot f_1 + \sum_{j=r'+1}^{r} d_j \cdot g_{1j} f_j = \sum_{i=1}^{r} f_i q_i',$$

donde $\deg(q_i') > 0$ o $q_i' = 0$.

Dado que el lado izquierdo de esta ecuación es homogéneo de grado d_1, el lado derecho también lo es. Si $q_1' \neq 0$, entonces tenemos que $\deg(f_1 q_1') > d_1$, y por lo tanto, el término $f_1 q_1'$ se cancela con otros términos del mismo grado en el lado derecho. De esto finalmente concluimos que

$$f_1 \in \sum_{i=2}^{r} f_i S \lhd S,$$

lo que es una contradicción. □

Introducimos a continuación el concepto de representación de pseudorreflexión aunque no será hasta después del Teorema 6.3.7 que tomará sentido al completo.

Definición 6.2.2. Las representaciones $\rho : G \longrightarrow GL_n(F)$ en las que $S[V]^G$ es un álgebra polinómica son precisamente aquellas en las que $\rho(G)$ es generado por pseudorreflexiones, estas representaciones reciben el nombre de **representación de pseudorreflexión**. Se dice que G es un **grupo de pseudorreflexión** cuando existe alguna representación de pseudorreflexión.

Para la demostración de la siguiente proposición necesitamos recordar el concepto de conjunto algebraicamente independiente, Definición 2.2.3, pues vamos a hacer uso de una nueva caracterización. Es posible introducir un orden entre los subconjuntos algebaricamente independientes de un cuerpo por inclusión existiendo elementos maximales. Teniendo esto en cuenta estudiamos el siguiente concepto.

Definición 6.2.3. Sea S un subconjunto de F algebraicamente independiente sobre a. Supongamos que la cardinalidad de S es máxima entre todos los subconjuntos de F, entonces esta cardinalidad recibe el nombre de **grado de trascendencia o dimensión** de F sobre a. Se puede consultar [9, Ch. 8.1].

Observación 6.2.4. Sólo vamos a necesitar distinguir entre grado de trascendencia finito e infinito. Obsérvese que la noción de grado de trascendencia guarda con la independencia algebraica la misma relación que la noción de dimensión guarda con la de independencia lineal.

Proposición 6.2.5. *Supongamos que $S[V]^G = F[f_1, \dots, f_r]$ es un anillo de polinomios, donde $f_i \in S[V]$ es homogéneo y $deg(f_i) = d_i$, y sea $N_G \in \mathbb{N}_0$ el número de pseudorreflexiones en G, ver Definición 6.1.1. Entonces $r = n$ y tenemos que*

$$\prod_{i=1}^{n} d_i = |G| \quad y \quad \sum_{i=1}^{n} (d_i - 1) = N_G.$$

Demostración.

Puesto que $S[V]^G \cong F[Y] := F[Y_1, \dots, Y_r]$, para el cuerpo invariante tenemos que $S(V)^G \cong F(Y)$, donde según la Proposición 3.2.11,

$$r = tr.deg(S(V)^G) = tr.deg(S(V)) = n.$$

Por la Observación 4.1.12, la serie de Hilbert de $S[V]^G$ viene dada por

$$H_{S[V]^G} = \prod_{i=1}^{n} \frac{1}{1 - T^{d_i}} = (-1)^n \cdot (T-1)^{-n} \cdot \prod_{i=1}^{n} \frac{1}{\sum_{j=0}^{d_i - 1} T^j} \in F((T)).$$

Utilizando la Observación 6.1.3, al multiplicar por $(-1)^n \cdot (T-1)^n$ obtenemos

$$\frac{1}{|G|} - \frac{N_G}{2 \cdot |G|} \cdot (T-1) + (-1)^n \cdot (T-1)^n \cdot H''_{S[V]^G} = \prod_{i=1}^{n} \frac{1}{\sum_{j=0}^{d_i - 1} T^j} \in F((T)),$$

donde $ord_1((T-1)^n \cdot H''_{S[V]^G}) \geq 2$. Evaluando en $T = 1$ se obtiene

$$\frac{1}{|G|} = \prod_{i=1}^{n} \frac{1}{d_i}.$$

Al aplicar $\frac{\partial}{\partial T}$ sobre el lado derecho de la ecuación anterior obtenemos

$$- \left(\prod_{i=1}^{n} \frac{1}{\sum_{j=0}^{d_i - 1} T^j} \right) \cdot \left(\sum_{i=1}^{n} \frac{\sum_{j=1}^{d_i - 1} j T^{j-1}}{\sum_{j=0}^{d_i - 1} T^j} \right),$$

y nuevamente evaluando en $T = 1$ llegamos a la expresión

$$- \left(\prod_{i=1}^{n} \frac{1}{d_i} \right) \cdot \sum_{i=1}^{n} \frac{d_i(d_i - 1)}{2 d_i}.$$

En el lado izquierdo de la ecuación anterior obtenemos $-\frac{N_G}{2|G|}$. De esta manera, usando $\prod_{i=1}^{n} d_i = |G|$, obtenemos

$$N_G = \sum_{i=1}^{n} (d_i - 1).$$

□

6.3. Anillos polinómicos e invariantes

En esta última sección del capítulo vamos a hablar de conjuntos de invariantes y concluiremos el trabajo con la demostración del importante Teorema de Shephard-Todd.

Definición 6.3.1. Supongamos que $S[V]^G = F[f_1, \ldots, f_r]$ es un anillo polinómico, donde $f_i \in S[V]$ es homogéneo y tal que $deg(f_i) = d_i$. El conjunto $\{f_1, \ldots, f_n\} \subseteq S[V]^G$ recibe formalmente el nombre de conjunto de **invariantes básicos**.

La siguiente proposición nos permite afirmar que los grados $d_i = deg(f_i)$ de un conjunto de invariantes básicos están definidos de manera única, salvo reordenamiento. Ver [7, Prop. 3.7].

Proposición 6.3.2. *Sea R una F-álgebra graduada finitamente generada y sean $\{f_1, \ldots, f_n\} \subseteq R$ y $\{f'_1, \ldots, f'_n\} \subseteq R$ conjuntos algebraicamente independientes de elementos homogéneos tales que*

$$R = F[f_1, \ldots, f_n] = F[f'_1, \ldots, f'_n].$$

Sean $d_i = deg(f_i)$ y $d'_i = deg(f'_i)$, donde $d_1 \leq \cdots \leq d_n$ y $d'_1 \leq \cdots \leq d'_n$. Entonces $d_i = d'_i$ para $i = 1, \ldots, n$.

Demostración.

Cada conjunto de polinomios puede ser escrito como polinomios en el otro conjunto, es decir, para $i = 1, \ldots, n$,

$$f_i = \sum_{j=1}^{n} a'_j f'_j \quad y \quad f'_i = \sum_{j=1}^{n} a_j f_j.$$

Para cada par de índices (i, j) con $i, j \in \{1, \ldots, n\}$, podemos usar la regla de la cadena para evaluar la derivada parcial $\frac{\partial f_i}{\partial f_j}$ y así obtener

$$\frac{\partial f_i}{\partial f_j} = \sum_{k=1}^{n} \frac{\partial f_i}{\partial f'_k} \frac{\partial f'_k}{\partial f_j} = \delta_{ij} = \begin{cases} 1, & si\ i = j \\ 0, & si\ i \neq j \end{cases}$$

lo que muestra que las matrices

$$\left(\frac{\partial f_i}{\partial f'_j}\right) \quad y \quad \left(\frac{\partial f'_i}{\partial f_j}\right)$$

son inversa una de la otra, concluyendo que cada una tiene determinante no nulo por ser invertibles.

Como los determinantes son no nulos, la expansión del primero de ellos debe incluir un producto no nulo de la forma

$$\prod_{i=1}^{n} \frac{\partial f_i}{\partial f'_{\pi(i)}}$$

para alguna permutación π. Por la ordenación de los grados, podemos suponer que esa permutación es la identidad, es decir $\pi(i) = i$. De esta forma, como

$$\prod_{i=1}^{n} \frac{\partial f_i}{\partial f'_i} \neq 0,$$

entonces $\frac{\partial f_i}{\partial f_i'} \neq 0$ para $i = 1, \ldots, n$. Por lo tanto cuando expresamos f_i como un polinomio en $f_1', \ldots, f_n'$, el término f_i' debe aparecer con un coeficiente no nulo.

Una vez hemos descartado los términos redundantes, podemos asumir que cada monomio

$$f_1'^{k_1}, \ldots, f_n'^{k_n}$$

que toma lugar en f_i satisface $d_i = \sum_{j=1}^{n} d_j' k_j$. Por la construcción, sabemos que f_i' debe aparecer en la expansión de f_i y puesto que los grados están ordenados concluimos que $d_i \geq d_i'$. Recíprocamente,

$$\sum_{i=1}^{n} d_i \geq \sum_{i=1}^{n} d_i'.$$

Al intercambiar los roles de f_i y f_i', el mismo razonamiento nos lleva a obtener que $d_i' \geq d_i$ lo que nos permite concluir que $d_i = d_i'$ para todo i. □

Definición 6.3.3. A los grados $d_i = deg(f_i)$ de un conjunto de invariantes básicos se les llama los **grados polinómicos** de G, donde podemos asumir que $d_1 \leq d_2 \leq \cdots \leq d_n$.

La siguiente observación nos permite ilustrar el hecho de que los invariantes básicos no son únicos.

Observación 6.3.4. A diferencia de los grados polinómicos, los invariantes básicos generalmente no están definidos de manera única, ni siquiera salvo reordenamiento y multiplicación por escalares. Sea $G = \mathcal{S}_n = \langle (1,2), \ldots, (n-1,n) \rangle$ el grupo simétrico como en el Capítulo 1, que actúa sobre el anillo de polinomios $F[X]$ al permutar las indeterminadas. Encontramos entonces que G está generado por reflexiones. Por las identidades de Newton, vistas en el Teorema 5.2.4, el Corolario 2.2.5 y la independencia algebraica de $p_{n,1}, \ldots, p_{n,n}$, que quedará probada por la Proposición 6.3.6, tenemos $F[X]^{\mathcal{S}_n} = F[e_1, \ldots, e_n] = F[p_{n,1}, \ldots, p_{n,n}]$.

Demostramos a continuación un criterio general para decidir si un subconjunto de n elementos de un anillo polinómico $F[X] = F[X_1, \ldots, X_n]$, donde $char(F) = 0$, es algebraicamente independiente. Esto ya ha sido utilizado en el Ejemplo 5.2.6.

En la Definición 6.3.5 y la Proposición 6.3.6 permitimos cuerpos F más generales.

Definición 6.3.5. Para $\{f_1, \ldots, f_n\} \subseteq F[X] = F[X_1, \ldots, X_n]$, la **matriz Jacobiana** se define como

$$J(f_1, \ldots, f_n) := \left[\frac{\partial f_i}{\partial X_j} \right]_{i,j=1,\ldots,n} \in F[X]^{n \times n},$$

y su determinante, $det(J(f_1, \ldots, f_n)) \in F[X]$ se llama el **determinante Jacobiano**.

Proposición 6.3.6. ***Criterio Jacobiano.*** *Si $char(F) = 0$, entonces $\{f_1, \ldots, f_n\} \subseteq F[X] = F[X_1, \ldots, X_n]$ es algebraicamente independiente si, y solo si, $det(J(f_1, \ldots, f_n)) \neq 0 \in F[X]$.*

Demostración.

$\boxed{\Longleftarrow}$

Sea $0 \neq h \in F[X]$ de grado mínimo tal que $h(f_1, \ldots, f_n) = 0$. Al aplicar la derivada parcial $\frac{\partial}{\partial X_j}$, mediante la regla de la cadena, obtenemos el sistema de ecuaciones lineales sobre $F(X) = Quot(F[X])$,

$$\left[\frac{\partial h}{\partial X_i}(f_1, \ldots, f_n) \right]_{i=1,\ldots,n} \cdot J(f_1, \ldots, f_n) = 0.$$

Dado que $deg_X(h) > 0$ y $char(F) = 0$, existe $i \in \{1, \dots, n\}$ tal que $\frac{\partial h}{\partial X_i} \neq 0 \in F[X]$. Como $deg_X\left(\frac{\partial h}{\partial X_i}\right) < deg_X(h)$, también tenemos que $\frac{\partial h}{\partial X_i}(f_1, \dots, f_n) \neq 0 \in F[X]$. Por lo tanto, el sistema de ecuaciones lineales anterior tiene una solución no trivial, y de esta forma concluimos que $\det(J(f_1, \dots, f_n)) = 0 \in F[X]$.

$\boxed{\Longrightarrow}$

Supongamos ahora que $\{f_1, \dots, f_n\}$ es un conjunto algebraicamente independiente. Dado que $tr.deg(F(X)) = n$, para $k \in \{1, \dots, n\}$ los conjuntos $\{X_k, f_1, \dots, f_n\}$ son algebraicamente dependientes.

Sea $0 \neq h_k \in F[X_0, X_1, \dots, X_n] = F[X^+]$ de grado mínimo tal que $h_k(X_k, f_1, \dots, f_n) = 0$. Diferenciando por $\frac{\partial}{\partial X_j}$ obtenemos

$$\left[\frac{\partial h_k}{\partial X_i}(X_k, f_1, \dots, f_n)\right]_{k,i=1,\dots,n} \cdot J(f_1, \dots, f_n) = diag\left[-\frac{\partial h_k}{\partial X_0}(X_k, f_1, \dots, f_n)\right]_{k=1,\dots,n}.$$

Dado que $\{f_1, \dots, f_n\}$ es algebraicamente independiente, tenemos que $deg_{X_0}(h_k) > 0$. Ahora, como $char(F) = 0$, obtenemos $\frac{\partial h_k}{\partial X_0} \neq 0 \in F[X^+]$, y como $\deg_{X^+}\left(\frac{\partial h_k}{\partial X_0}\right) < deg_{X^+}(h_k)$, tenemos

$$\frac{\partial h_k}{\partial X_0}(X_k, f_1, \dots, f_n) \neq 0 \in F[X^+].$$

De esta manera llegamos a que

$$det\left(diag\left[-\frac{\partial h_k}{\partial X_0}(X_k, f_1, \dots, f_n)\right]\right) \neq 0 \in F[X^+],$$

y así concluimos que $\det(J(f_1, \dots, f_n)) \neq 0 \in F[X]$.

□

Demostramos finalmente el teorema para el que nos llevamos preparando todo el capítulo.

Teorema 6.3.7. ***Shephard-Todd.*** *El anillo invariante $S[V]^G$ es un anillo de polinomios si, y solo si, G está generado por pseudorreflexiones.*

Demostración.

Por el Teorema 6.2.1, sólo es necesario ver que que si $S[V]^G$ es un anillo de polinomios, entonces G está generado por pseudorreflexiones.

Mediante la Proposición 6.2.5, sea $S[V]^G = F[f_1, \dots, f_n]$, donde $f_i \in S[V]$ es homogéneo tal que $d_i := deg(f_i)$. Sea $H \subseteq G$ el subgrupo generado por las pseudorreflexiones en G. Por lo tanto, nuevamente por el Teorema 6.2.1, tenemos

$$S[V]^G \subseteq S[V]^H = F[g_1, \dots, g_n] \subseteq S[V],$$

donde $g_i \in S[V]$ es homogéneo tal que $e_i := deg(g_i)$.

De esta manera, existen $h_i \in F[X]$ tales que $f_i = h_i(g_1, \dots, g_n)$, para $i \in \{1, \dots, n\}$. Como todos los elementos son homogéneos podemos suponer que para todos los monomios $X^\alpha \in F[X]$, con $\alpha \in \mathbb{N}_0^n$, que aparecen en h_i se tiene que

$$\sum_{i=1}^{n} \alpha_i e_i = d_i.$$

Al diferenciar por $\frac{\partial}{\partial X_k}$, para $k \in \{1, \ldots, n\}$, y aplicar la regla de la cadena a $f_i = h_i(g_1, \ldots, g_n)$ obtenemos la expresión

$$J(f_1, \ldots, f_n) = \left[\frac{\partial h_i}{\partial X_j}(g_1, \ldots, g_n)\right]_{i,j=1,\ldots,n} \cdot J(g_1, \ldots, g_n) \in F[X]^{n\times n}.$$

Por el Criterio del Jacobiano, véase la Proposición 6.3.6, tenemos que $detJ(f_1, \ldots, f_n) \neq 0 \in F[X]$, y por lo tanto

$$det\left(\left[\frac{\partial h_i}{\partial X_j}(g_1, \ldots, g_n)\right]\right) \neq 0 \in F[X]$$

también.

Partiendo de esto y reordenando $\{f_1, \ldots, f_n\}$ podemos suponer que

$$\prod_{i=1}^{n} \frac{\partial h_i}{\partial X_j}(g_1, \ldots, g_n) \neq 0 \in F[X].$$

Así que tenemos $d_i \geq e_i$, para $i \in \{1, \ldots, n\}$. Así, por la Proposición 6.2.5, tenemos

$$\sum_{i=1}^{n}(d_i - 1) = N_G = N_H = \sum_{i=1}^{n}(e_i - 1),$$

de donde concluimos que $e_i = d_i$ para $i \in \{1, \ldots, n\}$. Por tanto, obtenemos que

$$|G| = \prod_{i=1}^{n} d_i = \prod_{i=1}^{n} e_i = |H|,$$

es decir, $G = H$. □

Observación 6.3.8. Shephard-Todd demostró el Teorema 6.3.7 primero clasificando los grupos finitos generados por pseudorreflexiones. Luego analizó caso por caso con lo que pudo verificar el Teorema 6.2.1. Más tarde, Chevalley proporcionó una demostración conceptual.

Los grupos finitos generados por pseudorreflexiones juegan un papel importante no solo en la teoría de invariantes, sino también en la teoría de representaciones de grupos finitos de tipo Lie.

Ejemplo 6.3.9. Un ejemplo de representación por reflexiones irreducible es la acción del grupo diedral D_{2k} que consideramos en el Ejemplo 5.2.6.

Ejemplo 6.3.10. Otro ejemplo de este tipo de representaciones puede visualizarse mediante el grupo de permutaciones $\mathcal{S}_n$. Consideremos la representación

$$\begin{aligned} \mathcal{S}_n &\longrightarrow GL_n(K) \\ \sigma &\longrightarrow M \end{aligned}$$

donde M es una matriz de permutación que actúa permutando las columnas de I_n.

Puesto que S_n está generado por trasposiciones $\tau_{ij} = (i, j)$ y la matriz de permutación de τ_{ij} es una reflexión deducimos que $S[V]^{\mathcal{S}_n}$ es un anillo de polinomios en n variables y $S[V]^{\mathcal{S}_n} = K[\text{polinomios simétricos}]$, que ya vimos en el capítulo de anillos invariantes que era un anillo de polinomios.

Por otro lado existe la representación de $\mathcal{S}_n$ en dimensión $n-1$

$$D_v(\sigma) : K^{n-1} \longrightarrow K^{n-1}$$
$$e_i \longrightarrow e_{\sigma(i)}$$

donde $e_n = -(e_1 + \ldots + e_{n-1})$. Puesto que

$$K^n/\langle e_1 + \ldots + e_n \rangle \cong K^{n-1}$$

existen polinomios invariantes algebraicamente independientes $\{f_1, \ldots, f_{n-1}\} \subseteq S[V]^{\mathcal{S}_n}$ tales que $S[V]^{\mathcal{S}n} = K[f_1, \ldots, f_{n-1}]$. Partiendo de $X_1 + \ldots + X_n = 0$ y de los primeros n-ésimos polinomios simétricos elementales obtenemos

- $X_1X_2 + X_1X_3 + \ldots + X_{n-1}X_n = -(X_2 + \ldots + X_n)X_2 - (X_2 + \ldots + X_n)X_3 - \ldots - (X_2 + \ldots + X_n)X_n + X_2X_3 + \ldots + X_{n-1}X_n$
- $X_1X_2X_3 + X_1X_2X_4 + \ldots + X_{n-2}X_{n-1}X_n = -(X_2 + \ldots + X_n)X_2X_3 - (X_2 + \ldots + X_n)X_2X_4 - \ldots - (X_2 + \ldots + X_n)X_{n-1}X_n + X_2X_3X_4 + \ldots + X_{n-2}X_{n-1}X_n$

$$\vdots$$

- $X_1X_2 \cdots X_n = -(X_2 + \ldots + X_n)X_2 \cdots X_n$

Y de esta forma

- $f_1 = X_2^2 + X_3^2 + \ldots + X_n^2 + (n-2)X_2X_3 + (n-2)X_2X_4 + \ldots + (n-2)X_{n-1}X_n$
- $f_2 = (X_2 + X_3)X_2X_3 + (X_2 + X_4)X_2X_4 + \ldots + (X_{n-1} + X_n)X_{n-1}X_n + (n-2)X_2X_3X_4 + (n-2)X_2X_3X_5 + \ldots + (n-2)X_{n-2}X_{n-1}X_n$

$$\vdots$$

- $f_n = (X_2 + \ldots + X_n)X_2 \cdots X_n$

Después del análisis del Teorema de Shephard-Todd y su aplicación en la teoría de representación, hemos llegado a la conclusión de que sí es posible caracterizar aquellas representaciones cuyo anillo invariante es un anillo de polinomios. Además, esta caracterización nos abre nuevas vías de investigación para poder explorar las propiedades de estas representaciones otros contextos más generales.

Bibliografía

[1] Emil Artin. *Galoissche Theorie*, volume 28 of *Math.-Naturwiss. Bibl.* Teubner Verlagsgesellschaft, Leipzig, 1959.

[2] Michael F. Atiyah and I. G. Macdonald. Introduction to commutative algebra. Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969)., 1969.

[3] D. J. Benson. *Polynomial invariants of finite groups*, volume 190 of *Lond. Math. Soc. Lect. Note Ser.* Cambridge: Cambridge University Press, 1993.

[4] Siegfried Bosch. *Algebraic geometry and commutative algebra*. Universitext. London: Springer, 2nd edition edition, 2022.

[5] Félix Delgado, Concha Fuertes, and Sebastián Xambó. *Introducción al Álgebra*. Paraninfo, Madrid, 2ª ed. edition, 2021.

[6] Harm Derksen and Gregor Kemper. *Computational invariant theory*, volume 130 of *Encycl. Math. Sci.* Berlin: Springer, 2002.

[7] James E. Humphreys. *Reflection groups and Coxeter groups*, volume 29 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, 1992.

[8] Nathan Jacobson. *Lectures in abstract algebra. III: Theory of fields and Galois theory. 3rd corr. printing*, volume 32 of *Grad. Texts Math.* Springer, Cham, 1980.

[9] Serge Lang. Algebra. Reading, Mass.: Addison-Wesley Publishing Company, Inc., XVIII, 508 p. (1965)., 1965.

[10] Saunders Mac Lane. *Categories for the working mathematician.*, volume 5 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed edition, 1998.

[11] Jürgen Müler. https://www.math.rwth-aachen.de/ juergen.mueller/, 2024.

[12] M. Nagata. On the 14th problem of Hilbert. Sugaku 12 (1960/61), 203-209 (1961)., 1961.

[13] Mara D. Neusel and Larry Smith. *Invariant theory of finite groups*, volume 94 of *Math. Surv. Monogr.* Providence, RI: American Mathematical Society (AMS), 2002.

[14] D. G. Northcott. *Lessons on rings, modules and multiplicities*. Cambridge: Cambridge University Press, reprint of the 1968 hardback ed. edition, 2008.

[15] Peter Webb. *A course in finite group representation theory*, volume 161 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, 2016.