Invariantes de grupos finitos

Autor: Guillermo Sanmarco
Director:Nicolás Andruskiewitsch

UNIVERSIDAD NACIONAL DE CÓRDOBA

Marzo de 2015

Resumen

En este trabajo se realiza un repaso por la teoría de invariantes de grupos finitos y de grupos racionales. Se introducen las nociones básicas de geometría algebraica y los preliminares de álgebra conmutativa necesarios. Entre los resultados se destacan los teoremas que prueban que para grupos finitos y grupos algebraicos reductivos, el álgebra de invariantes es finitamente generada. En el caso finito, se analiza la dimension de Krull del álgebra de invariantes y se muestra una cota para el grado de los generadores.

Palabras claves:

- Teoría de invariantes
- Representaciones de grupos finitos
- Representaciones de grupos racionales

Código de clasificación: 13A50.

Índice general

Resumen 1

Capítulo 1. Introducción 5

Capítulo 2. Preliminares 7
1. Conceptos básicos de geometría algebraica 7
2. El Nullstellensatz 9
3. Equivalencia álgebra-geometría 10
4. Grupos algebraicos afines 11
5. Representaciones de grupos 13
6. Anillos noetherianos y el teorema de la base de Hilbert 15

Capítulo 3. Nociones generales de invariantes 17
1. Invariantes de grupos algebraicos reductivos 19

Capítulo 4. Invariantes de grupos finitos 21
1. Ejemplo: Invariantes de los grupos simétricos 21
2. Ejemplo: Invariantes de los grupos alternantes 23
3. Primera noción de finitud del álgebra de invariantes 24
4. Dimensión de Krull 26
5. Cota de Noether 34

Bibliografía 39

Capítulo 1

Introducción

(. . .) has been pronounced dead several times, and like the phoenix it has been again and again rising from its ashes.

- Jean Dieuddoné, *Invariant Theory, Old and New.*

La teoría de invariantes toma como punto de partida una representación de un grupo algebraico sobre un espacio vectorial, y luego la representación que ésta induce sobre las funciones polinomiales en ese espacio vectorial. El principal objeto de estudio es el álgebra formada por los polinomios que permanecen invariantes por dicha acción. Uno de los resultados que darían inicio al estudio de esta teoría fue el *Teorema fundamental de los polinomios simétricos*, enunciado por primera vez por Lagrange. Sin embargo, existen indicios de que, un siglo antes, Isaac Newton (1643, 1727) ya conocía dicho teorema. A lo largo de los últimos 150 años el desarrollo de la teoría de invariantes supo alternar su importancia en la escena mundial, tomando un papel protagónico en algunos casos, y también aguardando en silencio el próximo resultado que la colocara de vuelta en los primeros planos.

A lo largo del siglo XIX el foco estaba puesto en probar que el álgebra de invariantes es finitamente generada, y se probaron algunos casos particulares. Ya en esos momentos, la teoría empezó a generar lenguaje y métodos propios.

Ya mas cerca del siglo XX, Emmy Noehter y David Hilbert usaron las herramientas existentes del álgebra abstracta para poner en contexto y en palabras precisas los problemas que la teoría intentaría resolver en los años siguientes. Esas preguntas resultaron ser estímulos fundamentales para el origen del álgebra conmutativa moderna. En 1890, Hilbert resolvió el problema de generación finita para una familia muy particular de representaciones de $GL(n, \mathbb{C})$. Su demostración tuvo como argumento central el *Teorema de la base de Hilbert*, que establece que los anillos de polinomios sobre un cuerpo son noetherianos.

En el Congreso Internacional de Matemáticos de 1890 Hilbert postuló su problema número 14, indagando si las álgebras de invariantes son siempre finitamente generadas. Recién en 1959, y después de algunos intentos fallidos de demostración por parte de Maurer, Nagata exhibió un contraejemplo.

En este trabajo se realiza un breve repaso de los resultados básicos de la teoría de invariantes de grupos finitos, y algunos pocos resultados sobre la teoría de invariantes de grupos algebraicos reductivos.

Capítulo 2

Preliminares

En este capítulo se fija lenguaje y se introducen nociones básicas de geometría algebraica, álgebra conmutativa, y grupos algebraicos.

1. Conceptos básicos de geometría algebraica

En esta sección, k denota un cuerpo algebraicamente cerrado, y por lo tanto infinito.

Cada polinomio $f \in k[x_1, x_2, ..., x_n]$ puede ser visto como una función

$$f\colon k^n \to k.$$

Las funciones así obtenidas se llaman *funciones polinomiales* del espacio vectorial k^n a k. Si una función polinomial es nula, entonces es la asociada al polinomio nulo (esto sucede porque el cuerpo es infinito). Por lo tanto, polinomios distintos tienen asociadas funciones polinomiales distintas. Esto permite identificar a $k[x_1, x_2, ..., x_n]$ con una subálgebra del álgebra de funciones $k^n \to k$.

Definición 2.1. Dado un subconjunto $T \subset k[x_1, x_2, ..., x_n]$, se define el *conjunto de ceros* de T por

$$Z(T) = \{P \in k^n\colon f(P) = 0 \text{ para todo } f \in T\}.$$

Los subconjuntos de k^n obtenidos de esta forma se llaman *conjuntos algebraicos*, o también *subconjuntos algebraicos de* k^n.

De la definición se desprende que si dos subconjuntos T_1 y T_2 generan el mismo ideal en $k[x_1, x_2, ..., x_n]$, entonces $Z(T_1) = Z(T_2)$. Como $k[x_1, x_2, ..., x_n]$ es un anillo noetheriano, todo ideal es finitamente generado, y por lo tanto todo conjunto algebraico se puede escribir como el conjunto de ceros de una cantidad finita de polinomios.

Proposición 2.2. *(a). La unión de dos conjuntos algebraicos es un conjunto algebraico.*

(b). La intersección de una familia arbitraria de conjuntos algebraicos es un conjunto algebraico.

(c). El vacío y el total son conjuntos algebraicos.

Demostración. Sean T_1 y T_2 subconjuntos de $k[x_1, x_2, ..., x_n]$, y sea T_1T_2 el conjunto de todos los productos de elementos de T_1 con elementos de T_2. Si $P \in Z(T_1) \cup Z(T_2)$, entonces P está en $Z(T_1)$ o en $Z(T_2)$, y por lo tanto P es un cero de cualquier polinomio de T_1T_2. Recíprocamente, si P es un elemento de $Z(T_1T_2)$, y $P \notin Z(T_1)$, digamos $f(P) \neq 0$ con $f \in T_1$, entonces para todo $g \in T_2$, se tiene $fg(P) = 0$, y por lo tanto $g(P) = 0$. Así $Z(T_1) \cup Z(T_2) = Z(T_1T_2)$. Del mismo modo, si $Z(T_\alpha)$ es una familia de conjuntos algebraicos, entonces $\bigcap_\alpha Z(T_\alpha) = Z(\bigcup_\alpha T_\alpha)$. Finalmente, el conjunto vacío es $Z(1)$ y el total es $Z(0)$. □

DEFINICIÓN 2.3. Por la proposición anterior, los complementos (en k^n) de los conjuntos algebraicos determinan una topología en k^n. Esta se denomina *topología de Zariski*.

EJEMPLO 2.4. En $k[x]$, todos los ideales son principales. Así, todo conjunto algebraico es el conjunto de ceros de un polinomio en una variable, y por lo tanto es finito o todo k. Luego, los abiertos de Zariski en k son los complementos de los conjuntos finitos y el conjunto vacío.

DEFINICIÓN 2.5. Sea X un espacio topológico, y sea $Y \subset X$. Se dice que Y es *irreducible* si no existen subconjuntos cerrados propios $Y_1, Y_2 \subset X$ tales que $Y = Y_1 \cup Y_2$. El conjunto vacío no se considera irreducible.

EJEMPLO 2.6. Con la topologia de Zariski, k es irreducible, porque los subconjuntos cerrados propios son finitos, y k es infinito.

DEFINICIÓN 2.7. Una *variedad algebraica afín* es un subconjunto algebraico irreducible de k^n, dotado de la topología inducida.

En este trabajo, se usan indistintamente *variedad algebraica* y *variedad algebraica afín*.

Una construcción inversa a la construcción de conjuntos algebraicos. Ahora se obtienen ideales de $k[x_1, x_2, ..., x_n]$ a partir de subconjuntos de k^n.

DEFINICIÓN 2.8. Sea $Y \subset k^n$. Se define el *ideal* de Y en $k[x_1, x_2, ..., x_n]$ por

$$I(Y) \coloneqq \{f \in k[x_1, x_2, ..., x_n] \colon f(P) = 0 \text{ para todo } P \in Y\}.$$

Es inmediato que *I(Y)* es en efecto un ideal de $k[x_1, x_2, ..., x_n]$. Así, se define el *anillo de coordenadas* de Y como la k-álgebra

$$A(Y) \coloneqq k[x_1, x_2, ..., x_n]/I(Y)$$

PROPOSICIÓN 2.9. *Sea $Y \subset k^n$. Entonces* A(Y) *es una* k*-álgebra reducida y finitamente generada.*

DEMOSTRACIÓN. *A(Y)* es finitamente generada porque $k[x_1, x_2, ..., x_n]$ lo es. Ahora se ve que es reducida. Sea $f \in k[x_1, x_2, ..., x_n]$ tal que la clase de f es nilpotente en *A(Y)*, digamos $f^d = 0$ en A(Y). Ahora, para cada $p \in Y$, la evaluación en p es un morfismo de anillos de *A(Y)*. Por lo tanto, $f(p)^d = f^d(p) = 0$ para todo $p \in Y$. Así, la clase de f en *A(Y)* es nula. □

Ahora se cuenta con una función Z que asigna a cada subconjunto de $k[x_1, x_2, ..., x_n]$ un conjunto algebraico de k^n y con una función I que asigna a cada subconjunto de k^n un ideal de $k[x_1, x_2, ..., x_n]$. A continuación se detallan algunas de sus propiedades.

PROPOSICIÓN 2.10. *(a). Si $T_1 \subset T_2$ son subconjuntos de $k[x_1, x_2, ..., x_n]$, entonces $Z(T_1) \supset Z(T_2)$.*
(b). Si $Y_1 \subset Y_2$ son subconjuntos de k^n, entonces $I(Y_1) \supset I(Y_2)$.
(c). Dados $Y_1, Y_2 \subset k^n$, se tiene $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.
(d). Dado $Y \subset k^n$, se tiene $Z(I(Y)) = \bar{Y}$, la clausura de Y.

DEMOSTRACIÓN. Las primeras dos afirmaciones son inmediatas.

Sean $Y_1, Y_2 \subset k^n$, y sea $f \in k[x_1, x_2, ..., x_n]$. Entonces f está en $I(Y_1 \cup Y_2)$ si y sólo si se anula en todos los elementos de $I(Y_1)$ y en todos los elementos de $I(Y_2)$; es decir, si y solo si f esta en $I(Y_1) \cap I(Y_2)$. Esto prueba *(c)*.

Sea $Y \subset k^n$ Es inmediato que $Y \subset Z(I(Y))$, y como este último es cerrado, se sigue $\bar{Y} \subset Z(I(Y))$. Recíprocamente, sea W un cerrado que contiene a Y, digamos $W = Z(T) \supset Y$. Por b, $I(Z(T)) \subset I(Y)$. Por otro lado, $T \subset I(Z(T))$, luego $T \subset I(Z(T)) \subset I(Y)$. Así, por a, $Z(T) \supset Z(I(Y))$. Esto prueba d. □

2. El Nullstellensatz

El Teorema de los ceros de Hilbert es la herramienta con la que terminamos de delinear la primera conexión entre objetos algebraicos (ideales de k^n) y objetos geométricos (conjuntos algebraicos, conjuntos de ceros).

TEOREMA 2.11. *(Nullstellensatz). Sea* k *un cuerpo algebraicamente cerrado. Si* $\mathfrak{a}$ *es un ideal de* k^n*, entonces*

$$I(Z(\mathfrak{a})) = rad(\mathfrak{a}).$$

Por lo tanto, las aplicaciones $\mathfrak{a} \mapsto Z(\mathfrak{a})$ *y* $X \mapsto I(X)$ *inducen una biyección entre las familias de conjuntos algebraicos de* k^n *y de ideales radicales de* $k[x_1, x_2, ..., x_n]$*.* □

Para una demostración de este resultado, ver la sección 4.5 de [**5**]. La correspondencia establecida por el *Nullstellensatz* tiene la siguiente propiedad.

PROPOSICIÓN 2.12. *Bajo la correspondencia* $\mathfrak{a} \mapsto Z(\mathfrak{a})$ *y* $X \mapsto I(X)$*, un conjunto algebraico es irreducible si, y sólo si, su ideal es primo.*

DEMOSTRACIÓN. Sea X un conjunto algebraico irreducible. Veo que $I(X)$ es un ideal primo. Sean $f, g \in k[x_1, x_2, ..., x_n]$ tales que $fg \in I(X)$. Entonces

$$X \subset Z(fg) = Z(f) \cup Z(g),$$

y por lo tanto $X = (Z(f) \cap X) \cup (Z(g) \cap X)$, siendo estos dos cerrados. Como X es irreducible, debe ser $X = Z(f) \cap X$ o bien $X = Z(g) \cap X$. En el primer caso se tiene $X \subset Z(f)$, y por lo tanto $f \in X$, y en el segundo caso $X \subset Z(g)$, y por lo tanto $g \in X$.

Recíprocamente, sea $\mathfrak{p}$ un ideal primo. Sean X_1, X_2 cerrados de manera tal que que $Z(\mathfrak{p}) = X_1 \cup X_2$. Entonces $\mathfrak{p} = I(X_1 \cup X_2) = I(X_1) \cap I(X_2)$. Por lo tanto, $\mathfrak{p} = I(X_1)$ o $\mathfrak{p} = I(X_2)$, es decir, $Z(\mathfrak{p}) = X_1$ o $Z(\mathfrak{p}) = X_2$, y por lo tanto $Z(\mathfrak{p})$ es irreducible. □

El Nullstellensatz dice que los ideales radicales de $k[x_1, x_2, ..., x_n]$ son precisamente los *I(X)* para X conjunto algebraico. Esto, junto con la correspondencia $\mathfrak{a} \mapsto Z(\mathfrak{a})$ y $X \mapsto I(X)$, son herramientas que permiten transferir el estudio geométrico de variedades algebraicas al álgebra. En una primera instancia, caracteriza a las k-álgebras que se obtienen como anillos de coordenadas.

COROLARIO 2.13. *Sea* k *un cuerpo algebraicamente cerrado y sea* A *una* k*-álgebra. Entonces* A *es el anillo de coordenadas de algún conjunto algebraico si, y sólo si,* A *es reducida y finitamente generada como* k*-álgebra.*

DEMOSTRACIÓN. Si $A = A(X)$ para algún conjunto algebraico $X \subset k^n$, lo vimos en la Proposición 2.9.

Recíprocamente, si A es reducida y finitamente generada como k-álgebra, escogiendo generadores se sabe que $A = k[x_1, x_2, ..., x_n]/\mathfrak{a}$ para algún ideal $\mathfrak{a}$. Como A es reducida, $\mathfrak{a}$ debe ser un ideal radical. Del Nullstellensatz se sigue que $\mathfrak{a} = I(Z(\mathfrak{a}))$. □

Observación 2.14. El Nullstellensatz nos permite también calcular los ideales maximales de los anillos de coordenadas. Para poder hacerlo, mejor tener a mano lo siguiente. Si $p = (a_1, a_2, ..., a_n) \in k^n$, entonces *I(p)* es el ideal

$$\mathfrak{m}_p \coloneqq (x_1 - a_1, x_2 - a_2, ..., x_n - a_n).$$

Primero notar que $\mathfrak{m}_p$ es un ideal maximal. En efecto, en la proyección

$$k[x_1, x_2, ..., x_n] \to k[x_1, x_2, ..., x_n]/\mathfrak{m}_p,$$

la variable x_i se identifica con a_i, luego el cociente es isomorfo a k. La inclusión $\mathfrak{m}_p \subset I(p)$ es inmediata y la igualdad sigue de la maximalidad de $\mathfrak{m}_p$.

Corolario 2.15. *Sea* k *un cuerpo algebraicamente cerrado y sea* $X \subset k^n$ *un conjunto algebraico. Entonces todo ideal maximal del anillo de coordenadas* A(X) *es de la forma* $\mathfrak{m}_p \coloneqq (x_1 - a_1, x_2 - a_2, ..., x_n - a_n)/I(X)$ *para algún*

$$p = (a_1, a_2, ..., a_n) \in X.$$

En particular, los puntos de X *están en correspondencia biyectiva con los ideales maximales de* A(X).

Demostración. Todo ideal maximal de $A(X)$ se obtiene cocientando un ideal maximal de $k[x_1, x_2, ..., x_n]$ que contiene a $I(X)$ por este último. Luego, basta probar el corolario cuando $X = k^n$ y por lo tanto $A(X) = k[x_1, x_2, ..., x_n]$.

Ahora bien, si $\mathfrak{m}$ es un ideal maximal, entonces es radical (por ser primo), y por lo tanto $I(Z(\mathfrak{m})) = \mathfrak{m}$. Luego, si $p \in Z(\mathfrak{m})$ (este último es no vacío porque $\mathfrak{m}$ es propio por consecuencia del *Nullstellensatz*), entonces $\mathfrak{m} \subset \mathfrak{m}_p$. Y como $\mathfrak{m}$ es maximal, se sigue la igualdad. □

3. Equivalencia álgebra-geometría

En esta sección se establece la correspondencia categórica que se empezó a delinear. Se describe la conexión entre objetos algebraicos y objetos geométricos dada por el Teorema de los ceros de Hilbert.

Observación 2.16. Otra interpretación del anillo de coordenadas. Sea $X \subset k^n$ un conjunto algebraico. Denotamos por k^X a la k-álgebra de funciones de X a k. Sea $R\colon k[x_1, x_2, ..., x_n] \to k^X$ la restricción de funciones, $f \mapsto f_{|X}$. El núcleo de R coincide con $I(X)$. Por lo tanto, la imagen de R es isomorfa al álgebra $A(X)$. Así interpretamos a los elementos del anillo de coordenadas como funciones en X.

Definición 2.17. Sea $X \subset k^n$ un conjunto algebraico. Se dice que una función $f \in k^X$ es una *función regular* si es la restricción a X de una función polinomial de k^n, es decir, si f está en la imagen de R. El conjunto de funciones regulares se denota por $k[X]$.

Observación 2.18. Ya se probó que $k[X]$ es isomorfo a $A(X)$.

Definición 2.19. Sean $X \subset k^n$ e $Y \subset k^m$ dos conjuntos algebraicos. Un *morfismo de conjuntos algebraicos* $F\colon X \to Y$ es una función de X a Y para la cual existen $f_1, f_2, ..., f_m \in k[x_1, x_2, ..., x_n]$ tales que F es la restricción a X de la aplicación

$$\begin{aligned} k^n &\to k^m \\ (a_1, a_2, ..., a_n) &\mapsto (f_1(a_1, a_2, ..., a_n), f_2(a_1, a_2, ..., a_n), ..., f_m(a_1, a_2, ..., a_n)). \end{aligned}$$

Los morfismos de conjuntos algebraicos también se llaman *aplicaciones polinomiales*.

Siguiendo con la notación de la definición, se pueden usar los polinomios $f_1, f_2, ..., f_m$ para definir una morfismo de k-álgebras

$$\begin{aligned} F^*\colon k[y_1, y_2, ..., y_m] &\to k[x_1, x_2, ..., x_n] \\ y_i &\mapsto f_i(x_1, x_2, ..., x_n). \end{aligned}$$

Ahora bien, como la restricción de F a X tiene imagen en Y, para g en $I(Y)$, se tiene $F^*(g) = g(f_1(x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n), ..., f_m(x_1, x_2, ..., x_n))$ se anula en todo X, es decir $F^*(g) \in I(X)$. Por lo tanto F^* induce un morfismo de k-álgebras

$$F^*\colon A(Y) = k[y_1, y_2, ..., y_m]/I(Y) \to k[x_1, x_2, ..., x_n]/I(X) = A(X).$$

Viendo a los anillos de coordenadas como anillos de funciones, F^* es la composición con F. Por lo tanto, si $F_1, F_2\colon X \to Y$ son morfismos de conjuntos algebraicos tales que $F_1^* = F_2^*$, entonces $F_1 = F_2$.

Este procedimiento se puede invertir. Si $\psi\colon A(Y) \to A(X)$ es un morfismo de k-álgebras, se puede obtener un morfismo de conjuntos algebraicos $F\colon X \to Y$ tal que $F^* = \psi$. Se bosqueja la construcción. Para cada $i = 1, 2, ..., m$ se elige un representante f_i en $k[y_1, y_2, ..., y_m]$ de la clase $\psi(y_i) \in k[y_1, y_2, ..., y_m]/I(Y)$. Luego, se define

$$\begin{aligned} F\colon k^n &\to k^m \\ (a_1, a_2, ..., a_n) &\mapsto (f_1(a_1, a_2, ..., a_n), f_2(a_1, a_2, ..., a_n), ..., f_m(a_1, a_2, ..., a_n)), \end{aligned}$$

cuya restricción a X es un morfismo de conjuntos algebraicos $X \to Y$ tal que $F^* = \psi$.

TEOREMA 2.20. *Sea k un cuerpo algebraicamente cerrado. La categoría de conjuntos algebraicos afines sobre k es equivalente a la categoría de las k-álgebras afines con las flechas intercambiadas.*

Existe una forma equivalente de definir los morfismos.

DEFINICIÓN 2.21. Sean X e Y conjuntos arbitrarios. Si $F\colon X \to Y$ es una función, se define $F^*\colon k^Y \to k^X$ por $F^*(f) \coloneqq f \circ F$. Es claro que F^* es un morfismo de álgebras.

OBSERVACIÓN 2.22. Sean $X \subset k^n$ e $Y \subset k^m$ dos conjuntos algebraicos. Se puede probar que un *morfismo de conjuntos algebraicos* $F\colon X \to Y$ es equivalente a una función de X a Y tal que $F^*(k[Y]) \subset k[X]$.

4. Grupos algebraicos afines

En esta sección se construye el producto directo en la categoría de conjuntos algebraicos. Se introduce el concepto de grupo algebraico afín.

LEMA 2.23. *Sean $X \subset k^n$ e $Y \subset k^m$ dos conjuntos algebraicos.*

1. *$X \times Y$ es un subconjunto cerrado de k^{n+m}.*
2. *$X \times Y$, con la topología inducida de k^{n+m} es el producto directo (en la categoría de conjuntos algebraicos sobre k) de X con Y.*
3. *$A(X \times Y) = A(X) \otimes_k A(Y)$.*

DEMOSTRACIÓN. Para probar *1*, se recuerda que, como k-álgebras, $k[x_1, x_2, ..., x_n] \otimes_k k[y_1, y_2, ..., y_m] \simeq k[x_1, ..., x_n, y_1, ..., y_m]$. Ahora, con esa identificación, se ve que $X \times Y = Z(I(X) \otimes 1 + 1 \otimes I(Y))$. Es inmediato que $X \times Y$ está contenido en ese conjunto de ceros. Para la inclusión recíproca, sea $(x, y) \in Z(I(X) \otimes 1 + 1 \otimes I(Y))$. Entonces (x, y) es un cero de todos los elementos de $I(X) \otimes 1$, y por lo tanto x está en $Z(I(X)) = X$. Del mismo modo, y está en $Z(I(Y)) = Y$.

Para probar *2*, se ve primero *3*. Se define

$$\psi \colon A(X) \otimes_k A(Y) \to A(X \times Y)$$
$$\psi \left(\sum_i f_i \otimes g_i \right) (x, y) = \sum_i f_i(x) g_i(y).$$

Es claro que esta aplicación es regular en $X \times Y$. Es sobreyectiva, porque tiene en su imagen a las coordenadas $x_1, x_2, ..., x_n, y_1, y_2, ..., y_m$ que generan $A(X \times Y)$. Resta ver que es invectiva. Para eso, basta probar que, si $\{f_i\}$ son linealmente independientes en $A(X)$ y $\{g_j\}$ son linealmente independientes en $A(Y)$, entonces $\{\psi(f_i \otimes g_j)\}$ son linealmente independientes en $A(X \times Y)$. Sean c_{ij} tales que

$$\sum_{i,j} c_{ij} f_i(x) g_j(y) = 0.$$

Sea $y \in k^m$ fijo pero arbitrario. Se tiene

$$\sum_i \left(\sum_j c_{ij} g_j(y) \right) f_i(x) = 0$$

para todo $x \in k^n$. Por lo tanto,

$$\sum_j c_{ij} g_j(y) = 0 \text{ para todo } i.$$

Pero esto vale para todo $y \in k^m$, de donde se concluye que $c_{ij} = 0$ para todo i, j.

Ahora, sabiendo la equivalencia de categorías dada por el teorema de los ceros de Hilbert, se sigue que $X \times Y$ es el producto directo de X con Y en la categoría de conjuntos algebraicos sobre k, y eso prueba *2*. □

La subcategoría de conjuntos algebraicos irreducibles hereda el producto directo.

PROPOSICIÓN 2.24. *Sean $X \subset k^n$ e $Y \subset k^m$ dos conjuntos algebraicos irreducibles. Entonces $X \times Y$ es irreducible en k^{n+m}.*

DEMOSTRACIÓN. Sean $Z_1, Z_2 \subset k^{n+m}$ cerrados tales que $X \times Y \subset Z_1 \cup Z_2$. Para cada $x \in X$, $\{x\} \times Y$ es irreducible, por ser homeomorfo a Y. Por lo tanto, para cada $x \in X$, $\{x\} \times Y$ es un subconjunto de Z_1 o de Z_2. Sean, para $i = 1, 2$, $X_i \coloneqq \{x \in X \colon \{x\} \times Y \subset Z_i\}$. Se sabe que $X = X_1 \cup X_2$. Ahora se ve que estos dos son cerrados. Fijo $y \in Y$, la aplicación $X \to X \times Y$, $x \mapsto (x, y)$ es continua. Así, como Z_i es cerrado, la preimagen $\{x \in X \colon (x, y) \in Z_i\}$ es cerrada. Luego, $X_i = \bigcap_{y \in Y} \{x \in X \colon (x, y) \in Z_i\}$ es cerrado. Como X es irreducible, se tiene $X \subset X_1$ o $X \subset X_2$. Es decir, $X \times Y \subset Z_1$ o $X \times Y \subset Z_2$. □

OBSERVACIÓN 2.25. Este resultado permite afirmar que en la categoría de variedades algebraicas afines existen los productos directos. Ahora se incorpora la definición principal de esta sección.

DEFINICIÓN 2.26. Sea k un cuerpo algebraicamente cerrado. Un *grupo algebraico afín sobre* k es un variedad algebraica afín G definida sobre k que cuenta además con una estructura de grupo tal que la multiplicación $G \times G \to G$ y la inversión $G \to G$ son morfismos de variedades algebraicas.

5. Representaciones de grupos

DEFINICIÓN 2.27. Sean G un grupo y X un conjunto no vacío. Una *acción* de G en X es una aplicación $G \times X \to X$, $(g, x) \mapsto g \cdot x$ tal que:

- Si e denota a la identidad de G, entonces $e \cdot x = x$ para todo $x \in X$.
- Para $g, h \in G$ y para $x \in X$, se cumple $g \cdot (h \cdot x) = gh \cdot x$.

En este caso, la aplicación $\psi_g \colon X \to X, x \mapsto g \cdot x$ es una biyección, con inverso $\psi_{g^{-1}}$. Además, la condición $g \cdot (h \cdot x) = gh \cdot x$ se traduce en $\psi_g \circ \psi_h = \psi_{gh}$.

Si G actúa en un espacio vectorial V, se dice que G *actúa linealmente* si, para cada $g \in G$, la aplicación ψ_g es lineal (y, por lo tanto, un automorfismo de V).

DEFINICIÓN 2.28. Sean G un grupo y V un espacio vectorial. Una *representación* de G en V es un morfismo de grupos $G \to GL(V)$.

En este caso, se dice que V es un G-módulo.

OBSERVACIÓN 2.29. Si V es un k-espacio vectorial de dimensión finita, digamos n, fijando una base se tiene un isomorfismo de grupos de $GL(V)$ en el grupo $GL(n, k)$ de matrices inversibles $n \times n$ con coeficientes en k. Si $G \to GL(V)$ es una representación, se dice que la aplicación $G \to GL(V) \simeq GL(n, k)$ es la *representación matricial* asociada.

PROPOSICIÓN 2.30. *Sean G un grupo y V un espacio vectorial. Hay una biyección*

$$\{\textit{Acciones lineales de } G \textit{ en } V\} \to \{\textit{Representaciones de } G \textit{ en } V\}.$$

DEMOSTRACIÓN. Sea $G \times V \to V$ una acción lineal, y para cada $g \in G$ sea $\psi_g \colon V \to V, v \mapsto g \cdot v$. Se define $\rho \colon G \to GL(V)$, $g \mapsto \psi_g$. Se sabe que $\psi_g \in GL(V)$, y también que $\psi_g \circ \psi_h = \psi_{gh}$ para todos $g, h \in G$. Es decir, ρ es una representación de G en V.

Recíprocamente, si $\rho \colon G \to GL(V)$ es un morfismo de grupos, entonces se define $G \times V \to V$, $g \cdot v := \rho(g)v$. Como ρ aplica la identidad de G en la identidad de $GL(V)$, se tiene $e \cdot v = v$ para todo $v \in V$. Al ser $\rho(gh) = \rho(g) \circ \rho(h)$, se tiene $g \cdot (h \cdot v) = gh \cdot v$. Así, $G \times V \to V$ es una acción lineal de G en V. Resta ver que las construcciones son recíprocas.

Empezando con una acción lineal $G \times V \to V$, sea ρ su representación, se denota por $\alpha \colon G \times V \to V$ a la acción que se obtiene de ρ. Entonces, para $g \in G$ y $v \in V$ arbitrarios, se tiene $\alpha(g, v) = \rho(g)v = g \cdot v$. Es decir, α es la acción con la que se empezó. Recíprocamente, sea $\rho \colon G \to GL(V)$ una representación. Se denota por $G \times V \to V$ su acción lineal asociada, y sea $\pi \colon G \to GL(V)$ la representación que se obtiene de esa acción. Entonces, para $g \in G$ y $v \in V$ arbitrarios, se tiene $\pi(g)v = g \cdot v = \rho(g)v$. Así, $\rho = \pi$. □

A partir de ahora, se hablará indistintamente de acciones lineales y de representaciones.

DEFINICIÓN 2.31. Sea $\rho\colon G \to GL(V)$ un G-módulo de dimensión finita. Se define el *caracter* de ρ por

$$\begin{aligned}\chi_\rho\colon G &\to k\\ g &\mapsto tr(\rho_g).\end{aligned}$$

5.1. Restricción de representaciones.

DEFINICIÓN 2.32. Sea $\rho\colon G \to GL(V)$ un G-módulo y sea W un subespacio de V. Se dice que W es G-*invariante* si para cada $g \in G$, se tiene $g \cdot W \subset W$.

Notar que toda representación tiene siempre dos subespacios G-invariantes, el 0 y todo el espacio.

OBSERVACIÓN 2.33. Si W es un subespacio G-invariante de V, entonces para cada g la aplicación $\psi_g|_W$ está en $GL(W)$, y por lo tanto, ρ induce una representación de G en W. Si además V es de dimensión finita, y $\{v_1, ..., v_n\}$ es una base de V que contiene a una base $\{v_1, ..., v_d\}$ de W, entonces la representación matricial asociada tiene la forma

$$\psi_g = \begin{bmatrix} \psi_g|_W & * \\ 0 & * \end{bmatrix}.$$

DEFINICIÓN 2.34. Una representación se dice *irreducible* si no admite subespacios invariantes propios.

5.2. Suma directa de G-módulos.

Si $\rho\colon G \to GL(V)$ y $\eta\colon G \to GL(W)$ son G-módulos sobre k, se puede dotar a la suma directa $V \oplus W$ de la misma estructura. Se define $\rho \oplus \eta\colon G \to GL(V \oplus W)$ por

$$\rho \oplus \eta(g)(v + w) \coloneqq \rho(g)v + \eta(g)w.$$

Notar que si V y W son de dimensión finita, con bases $\{v_1, ..., v_n\}$ y $\{w_1, ..., w_m\}$ respectivamente, entonces la representación matricial asociada a $\rho \oplus \eta$ en la base $\{v_1, ..., v_n, w_1, ..., w_m\}$ resulta

$$\rho \oplus \eta(g) = \begin{bmatrix} \rho_g & 0 \\ 0 & \eta_g \end{bmatrix}.$$

Por lo tanto, $\chi_{\rho\oplus\eta} = \chi_\rho + \chi_\eta$.

DEFINICIÓN 2.35. Un G-módulo V se dice *descomponible* si existen V_1, V_2 G-submódulos de V tales que $V = V_1 \oplus V_2$.

V se dice *semisimple* o *completamente reducible* si existen $V_1, ..., V_n$ G-submódulos irreducibles de V tales que $V = V_1 \oplus ... \oplus V_n$.

5.3. Producto tensorial de G-módulos.

Si se tienen $\rho\colon G \to GL(V)$ y $\eta\colon G \to GL(W)$ G-módulos sobre k, también es un G-módulo $V \otimes W$: Se define $\rho \otimes \eta\colon G \to GL(V \otimes W)$ por

$$\rho \otimes \eta(g)(v \otimes w) \coloneqq \rho_g(v) \otimes \eta_g(w).$$

Y resulta $\chi_{\rho\otimes\eta} = \chi_\rho\chi_\eta$.

5.4. Representación contragradiente.

Si $\rho\colon G \to GL(V)$ es un G-módulo, entonces V^* también. Se define $\rho^*\colon G \to GL(V^*)$ por $\rho^*(g)(\phi)(v) \coloneqq \phi(\rho(g^{-1})v)$, para $g \in G$, $\phi \in V^*$ y $v \in V$.

Resulta $\chi_{\rho^*}(g) = \chi_\rho(g^{-1})$.

Por lo tanto, si $\rho\colon G \to GL(V)$ y $\eta\colon G \to GL(W)$ son G-módulos sobre k, el espacio $\mathrm{Hom}(V, W) = V^* \otimes W$ también es un G-módulo.

5.5. Álgebra de grupo. Sea G un grupo finito. Si A es un anillo conmutativo, se define el *álgebra de grupo* AG como el A-módulo libre con base $\{e_g \colon g \in G\}$, con la estructura de álgebra dada por las reglas $e_g e_h = e_{gh}$ para g y h en G.

PROPOSICIÓN 2.36. *Sean G un grupo finito y k un cuerpo. Hay una biyección*

$$\{k\text{-representaciones de } G\} \leftrightarrow \{kG\text{-módulos}\}.$$

DEMOSTRACIÓN. Sea $\rho \colon G \to GL(V)$ una representación de G. Entonces V admite estructura de kG-módulo con la acción $\alpha(\rho)$ dada por

$$\left(\sum_{g\in G} a_g e_g\right) \cdot_{\alpha(\rho)} v \coloneqq \sum_{g\in G} a_g \rho(g) v$$

para $\sum_{g\in G} a_g e_g \in kG$ y $v \in V$. Se denotará por $\alpha(\rho)$ a este kG-módulo.

Recíprocamente, si V es un kG-módulo, se define $\beta(V) \colon G \to GL(V)$ por $\beta(V)(g)v \coloneqq e_g \cdot_V v$ para $g \in G$ y $v \in V$. Es evidente que $\rho(g)$ está en $GL(V)$. Además ρ es un morfismo de grupos porque

$$\beta(V)(gh)v = e_{gh} \cdot_V v = (e_g e_h) \cdot_V v = e_g \cdot_V (e_h \cdot_V v) = \beta(V)(g) \circ \beta(V)(h)v$$

para $g, h \in G$ y $v \in V$.

Las construcciones son recíprocas:

Si $\rho \colon G \to GL(V)$ una representación de G, para todo $g \in G$ y todo $v \in V$ se tiene

$$\beta(\alpha(\rho))(g)v = e_g \cdot_{\alpha(\rho)} v = \rho(g)v$$

y por lo tanto $\beta(\alpha(\rho)) = \rho$.

Del mismo modo, si V es un kG-módulo, entonces para todo $\sum_{g\in G} a_g e_g \in kG$ y todo $v \in V$ se tiene

$$\left(\sum_{g\in G} a_g e_g\right) \cdot_{\alpha(\beta(V))} v = \sum_{g\in G} a_g \beta(V)(g)v = \sum_{g\in G} a_g e_g \cdot_V v = \left(\sum_{g\in G} a_g e_g\right) \cdot_V v$$

y por lo tanto $\alpha(\beta(V) = V$.

□

6. Anillos noetherianos y el teorema de la base de Hilbert

DEFINICIÓN 2.37. Sea A un anillo con unidad. Un A-módulo se dice *noetheriano* si toda cadena ascendente de submódulos es eventualmente constante. Se dice que A es un *anillo noetheriano* si es un A-módulo noetheriano sobre si mismo. Es decir, si toda cadena ascendente de ideales de A es eventualmente constante.

OBSERVACIÓN 2.38. La suma directa de una cantidad finita de módulos noetherianos, al igual que los cocientes y submódulos de módulos noetherianos, son también noetherianos.

PROPOSICIÓN 2.39. *Un módulo M sobre un anillo noetheriano A es noetheriano si, y sólo si, es finitamente generado.*

DEMOSTRACIÓN. Si M es finitamente generado, entonces es un cociente de una suma directa de una cantidad finita de copias del A-módulo A, y por lo tanto es noetheriano.

Recíprocamente, si M es noetheriano, comenzando por un v_1 arbitrario de M se elige inductivamente una sucesión $v_1, v_2, ..., v_n, ...$ de elementos de M tal que, para cada $i \geq 2$, v_i no está en el submódulo generado por $v_1, ..., v_{i-1}$. Como M es noetheriano, la cadena ascendente de ideales $(v_1, ..., v_i), i \in \mathbb{N}$ es eventualmente constante, y así la sucesión se debe terminar. Por lo tanto, M es finitamente generado. □

Corolario 2.40. *Todo submódulo de un módulo finitamente generado sobre un anillo noetheriano es también finitamente generado.*

Lema 2.41. *Un anillo con unidad es noetheriano si, y sólo si, todo ideal es finitamente generado.*

Demostración. Si A es un anillo noetheriano, por el corolario todo ideal a izquierda es finitamente generado. Recíprocamente, se asume que todo ideal a izquierda de A es finitamente generado. Sea $(\mathfrak{a}_i)_{i\in\mathbb{N}}$ una cadena ascendiente de ideales a izquierda de A. Como la cadena es ascendente, la unión $\bigcup_{i\in\mathbb{N}} \mathfrak{a}_i$ es un ideal a izquierda, y por lo tanto es finitamente generado, digamos que es generado por $x_1, ..., x_n$. Ahora bien, ese subconjunto finito está incluido en la unión de la cadena ascendente, y por lo tanto está incluido en alguno de los ideales de la cadena. La cadena resulta constante a partir de ese ideal. □

Teorema 2.42. *Teorema de la base de Hilbert. Si A es un anillo conmutativo y con unidad noetheriano, entonces el anillo de polinomios $A[x]$ también lo es.*

Demostración. Por el lema, es suficiente probar que, si $\mathfrak{a}$ es un ideal de $A[x]$, entonces es finitamente generado. Inductivamente, se construye una sucesión $f_1, ..., f_n, ...$ en $\mathfrak{a}$. Sea f_1 un elemento de grado mínimo de $\mathfrak{a}$. Para $i \geq 1$, si $(f_1, ..., f_i) \neq \mathfrak{a}$, se elige f_{i+1} un elemento de grado mínimo de $\mathfrak{a} - (f_1, ..., f_i)$. Si $(f_1, ..., f_i) = \mathfrak{a}$, se deja de elegir elementos. Sea a_j el coeficiente principal de f_j. Como A es noetheriano, el ideal $(a_1, ..., a_i, ...)$ es finitamente generado, digamos que por $a_1, ..., a_m$.

Ahora se prueba que $f_1, ..., f_m$ generan $\mathfrak{a}$. Suponiendo que no es así, se elige un f_{m+1} de grado mínimo en $\mathfrak{a} - (f_1, ..., f_m)$, y se tiene

$$a_{m+1} = \sum_{j=1}^{m} c_j a_j$$

para algunos $c_1, ..., c_m$. Ahora bien, para $j \in \{1, ..., m\}$, el grado de f_{m+1} es menor que el grado de f_j, y así $d_j \coloneqq deg(f_{m+1}) - deg(f_j)$ es un entero positivo. Se considera

$$g \coloneqq \sum_{j=1}^{m} c_j f_j x^{d_j}$$

Este g está en el ideal generado por $f_1, ..., f_m$ y tiene el mismo coeficiente principal y grado que f_{m+1}. Entonces $f_{m+1} - g \in \mathfrak{a} - (f_1, ..., f_m)$ y tiene grado menor que f_{m+1}, contradiciendo la elección de f_{m+1}.

□

Capítulo 3

Nociones generales de invariantes

DEFINICIÓN 3.1. Sean G un grupo algebraico afín y X una variedad algebraica. Una *acción regular a izquierda* de G en X es una acción $G \times X \to X$ que es, además, un morfismo de variedades algebraicas.

En este caso, se dice que X es una G-variedad.

OBSERVACIÓN 3.2. Si X es una G-variedad, entonces para cada $g \in G$, la aplicación $\psi_g \colon X \to X, x \mapsto g \cdot x$ es un isomorfismo de variedades algebraicas, con inverso $\psi_{g^{-1}}$.

En efecto, ψ_g es la composición

$$X \to G \times X \to X$$
$$x \mapsto (g, x) \mapsto g \cdot x$$

de morfismos de variedades algebraicas.

Para $x \in X$ se denota por G_x al conjunto de los $g \in G$ tales que $g \cdot x = x$. Es inmediato que G_x es un subgrupo cerrado de G, y se llama *grupo de isotropía de* x.

Se denota por X^G al conjunto de los $x \in X$ cuyo grupo de isotropía es todo G. Estos se llaman los *elementos invariantes* por la acción.

DEFINICIÓN 3.3. Sea G un grupo algebraico afín, y sean X e Y G-variedades. Un *morfismo de G-variedades* es un morfismo de variedades algebraicas $f \colon X \to Y$ tal que $f(g \cdot x) = g \cdot f(x)$ para todo $x \in X$ y para todo $g \in G$.

DEFINICIÓN 3.4. Sea G un grupo algebraico afín y sea V un k-espacio vectorial de dimensión finita. Una *representación racional de G en V* es una acción regular y lineal de G en V.

En este caso, se dice que V es un G-módulo racional.

DEFINICIÓN 3.5. Sea G un grupo y $G \to GL(V)$ una representación de G en un k-espacio vectorial V. Para $v \in V$ y $\alpha \in V^*$, se define $\alpha|v \colon G \to k$ por $(\alpha|v)(g) \coloneqq \alpha(g \cdot v)$.

La función $\alpha|v$ se llama el *coeficiente matricial* asociado a α, v.

OBSERVACIÓN 3.6. Si V es de dimensión finita y $v_1, v_2, ..., v_n$ es una base de V con base dual $\alpha_1, \alpha_2, ..., \alpha_n$, entonces las funciones $\alpha_j|v_i$ son los coeficientes de la representación matricial asociada. Mas aún, éstas generan el espacio de coeficientes matriciales.

PROPOSICIÓN 3.7. *Sean G un grupo algebraico sobre k y V un k-espacio vectorial de dimensión finita. Sea $\rho \colon G \to GL(V)$ una representación abstracta de G en V. Entonces la acción $G \times V \to V$ es regular si, y sólo si, ρ es un morfismo de grupos algebraicos.*

DEMOSTRACIÓN. Sea $v_1, v_2, ..., v_n$ una base de V con base dual $\alpha_1, \alpha_2, ..., \alpha_n$. Entonces ρ es un morfismo de variedades algebraicas si, y sólo si, los coeficientes de la representación matricial asociada son funciones polinomiales en G. Pero, por la observación anterior, los coeficientes de la representación matricial son $\alpha_j|v_i$, que generan el espacio de las coeficientes matriciales. Por lo tanto, estos últimos son funciones polinomiales si, y sólo si, la acción $G \times V \to V$ es regular. Esto prueba el resultado. □

OBSERVACIÓN 3.8. Sean $\rho\colon G \to GL(V)$ y $\eta\colon G \to GL(W)$ G-módulos racionales, es decir, ρ y η son morfismos de grupos algebraicos. Entonces $\rho^*\colon G \to GL(V^*)$ y $\rho\otimes\eta\colon G \to GL(V\otimes W)$ también son racionales. Por lo tanto, $Hom(V, W) = V^*\otimes W$ es un G-módulo racional. Mas aún, $\mathrm{Hom}(V, W)^G = \mathrm{Hom}_G(V, W)$.

DEFINICIÓN 3.9. Sean G un grupo y V un k-espacio vectorial (no necesariamente de dimensión finita). Sea $\rho\colon G \to GL(V)$ una representación abstracta de G en V. Se dice que V es un G-módulo *localmente finito* si para cada $v \in V$ existe un subespacio vectorial G-invariante de dimensión finita que contiene a v.

DEFINICIÓN 3.10. Sean G un grupo algebraico sobre k y V un k-espacio vectorial. Sea $\rho\colon G \to GL(V)$ una representación abstracta de G en V. Se dice que la representación es *racional* si se satisfacen las siguientes condiciones:

(a). V es un G-módulo localmente finito.
(b). Para cada $v \in V$ y cada $\alpha \in V^*$, el coeficiente matricial $\alpha|v$ está en $k[G]$.

COROLARIO 3.11. *Sean G un grupo algebraico sobre k y V un k-espacio vectorial. Sea $G \to GL(V)$ una acción abstracta de G en V. Entonces V es un G-módulo racional si, y sólo si, existe una familia $\{V_i\colon i \in I\}$ de subespacios G-estables de dimensión finita de V tales que*

(a). $V = \sum_{i\in I} V_i$
(b). Para cada $i \in I$ la acción restringida $G \to GL(V_i)$ es un morfismo de grupos algebraicos afines.

En otras palabras, V es un G-módulo racional si, y sólo si es unión filtrante de G-módulos racionales de dimensión finita.

DEFINICIÓN 3.12. Un grupo algebraico G se dice *reductivo* si todo G-módulo racional es semisimple.

LEMA 3.13. *Sea G un grupo algebraico reductivo y sea V un G-módulo racional. Si existe un morfismo de G-módulos $V \to V$ que proyecta V sobre V^G, entonces es único (y se llama el operador de Reynolds de V).*

DEMOSTRACIÓN. Se considera la descomposición $V = \oplus_{S\in\widehat{G}} V_S$ en componentes isotípicas, de modo que V= $V_{trivial} \oplus V_2$, donde $V_2 = \oplus_{S\in\widehat{G}:S\neq\ trivial} V_S$. Claramente la proyección $\pi_1 : V \to V_{trivial} = V^G$ de núcleo V_2 es un operador de Reynolds.

Sea ahora $\pi_2\colon V \to V^G$ otro operador de Reynolds. Para ver que $\pi_1 = \pi_2$ basta ver que $V_2 \subset \ker \pi_2$. Para esto, basta ver que $\pi_{2|V_s} = 0$ para todo $S \in \widehat{G}$. Pero V_S es una suma directa de módulos simples isomorfos a S que es no trivial. Si W es un tal módulo, consideramos la restricción $\pi_2 : W \to V^G$ que es un morfismo de G-módulos. Como W es simple, este morfismo es trivial, es decir 0, o un isomorfismo; pero esto es absurdo pues $S \not\cong k$ (el módulo trivial).

Luego $\pi_2(W) = 0$, de donde se deduce $\pi_2(V_2) = 0$ y así, $\pi_1 = \pi_2$.

□

COROLARIO 3.14. *Sea G un grupo algebraico y sea $T\colon V \to W$ un morfismo de G-módulos racionales. Si V y W admiten operadores de Reynolds $\pi_V\colon V \to V$ y $\pi_W\colon W \to W$, entonces $\pi_W \circ T = T \circ \pi_V$. En particular, si T es sobreyectivo, entonces su restricción $T^G\colon V^G \to W^G$ también lo es.*

DEMOSTRACIÓN. Es consecuencia del lema anterior, porque $\pi_W \circ T$ y $T \circ \pi_V$ proyectan $Im(T)$ sobre sus G-invariantes. □

LEMA 3.15. *Sea G un grupo algebraico. Son equivalentes:*

(a) G es reductivo.

(b) Para todo G-módulo racional V, existe un morfismo de G-módulos $V \to V$ que proyecta V sobre V^G.

DEMOSTRACIÓN. (a) $\implies$ (b): Sea V un G-módulo racional. Como G es reductivo, V es semisimple. Sea $V = \bigoplus_{i\in I} V_i$ la descomposición en componentes isotípicas de V, y digamos que la componente de tipo trivial es V_0. Esta componente es el mayor subespacio de V donde G actúa trivialmente, es decir, $V_0 = V^G$. Sea $\pi\colon V \to V^G$ la proyección sobre la componente de tipo trivial. Ésta es un morfismo de G-módulos, y es una retracción de la inclusión $V^G \hookrightarrow V$, y por lo tanto proyecta V sobre V^G.

(b) $\implies$ (a):

Recordar que, para G módulos arbitrarios W, W', la estructura usual de G-módulo de $\mathrm{Hom}(W, W')$, dada por $(g \cdot \phi)w = g \cdot \phi(g^{-1} \cdot w)$ es racional, y por lo tanto $\mathrm{Hom}(W, W')$ admite un operador de Reynolds.

Se prueba en primera instancia que todo G-módulo racional de dimensión finita es semisimple. Sea V un G-módulo racional de dimensión finita, y sea U un G-submódulo racional de V. Se mostrará que U tiene un G-módulo complementario.

La inclusión $i\colon U \hookrightarrow V$ es un morfismo de G-módulos. Se considera el morfismo de G-módulos que éste induce

$$\begin{aligned} i^*\colon \mathrm{Hom}(V, U) &\to \mathrm{Hom}(U, U) \\ T &\mapsto T \circ i. \end{aligned}$$

Es decir, la restricción. Esta aplicación es sobreyectiva, porque todo operador de $U \to U$ se puede extender trivialmente a $V \to U$. Por el corolario anterior, se sigue que la inclusión $i\colon U \hookrightarrow V$ (que es G-invariante) es la imagen por i^* de algún $\rho \in \mathrm{Hom}(V, U)^G$. Es decir, $i\colon U \hookrightarrow V$ es la restricción a U de un morfismo de G módulos $\rho\colon V \to U$. Ahora el núcleo de ρ es un G-submódulo racional de V, que es claramente un complemento de U.

Esto prueba que todo G-módulo racional de dimensión finita es semisimple. Ahora bien, si V es un G-módulo racional de dimensión no necesariamente finita, entonces es suma de G-módulos racionales de dimensión finita, y por lo tanto semisimples, y así V es semisimple.

□

1. Invariantes de grupos algebraicos reductivos

Sea G un grupo algebraico reductivo, y sea V un G-módulo racional. Entonces el operador de Reynolds $\pi_V\colon V \to V$ induce una aplicación $\pi\colon k[V] \to k[V]$.

LEMA 3.16. *La aplicación $\pi\colon k[V] \to k[V]$ es un morfismo de $k[V]^G$-módulos.*

DEMOSTRACIÓN. Sea $x \in k[V]^G$. Entonces las aplicaciones $k[V] \to k[V]$ dadas por $y \mapsto x\pi(y)$, y por $y \mapsto \pi(xy)$ proyectan $k[V]$ sobre los invariables $k[V]^G$, y por 3.13, son iguales. □

TEOREMA 3.17. *(Hilbert, Nagata). Sea G un grupo algebraico reductivo. Para todo G-módulo racional V de dimensión finita, el álgebra de funciones polinomiales G-invariantes es finitamente generada.*

DEMOSTRACIÓN. Sea I el ideal de $k[V]$ generado por los invariantes homogéneos de grado positivo. Por el Teorema de la base de Hilbert, $k[V]$ es noetheriano, y por lo tanto I es generado por una cantidad finita de invariables, digamos $f_1, \ldots, f_s$.

Afirmación: $\{f_1, \ldots, f_s\}$ genera $k[V]^G$ como k-álgebra.

Sea f un invariante homogéneo de grado positivo. Como f está en I, se puede escribir $f = \sum_{i=1}^{s} h_i f_i$ para algunos $h_1, \ldots, h_s$ en $k[V]$. Por el lema anterior, aplicando a esta igualdad el morfismo de $k[V]^G$-módulos $\pi\colon k[V] \to k[V]$, se tiene

$$f = \sum_{i=1}^{s} \pi(h_i) f_i.$$

Ahora bien, por definición de π, cada $\pi(h_i)$ es un invariante de grado menor que f. Inductivamente, se asume que $\pi(h_1), \ldots, \pi(h_s)$ están en la subálgebra de $k[V]^G$ generada por $\{f_1, \ldots, f_s\}$, y se deduce que f también pertenece a esa subálgebra.

Esto prueba la afirmación, y por lo tanto el álgebra de invariantes es finitamente generada.

□

COROLARIO 3.18. *Sean G un grupo algebraico reductivo y X una variedad algebraica afín donde G actúa racionalmente. El álgebra de funciones polinomiales G-invariantes $k[X]^G$ es finitamente generada.*

DEMOSTRACIÓN. Por hipótesis, G actúa en $k[X]$ por automorfismos de álgebras de forma localmente finita (esto es, todo vector pertenece a un G-submódulo de dimensión finita). Luego, existe un G-submódulo V de dimensión finita que genera $k[X]$ como álgebra. Se considera la proyección canónica $\pi : k[V] \to k[X]$ inducida por la inclusión de V en $k[X]$; entonces π es un morfismo de G-módulos y por lo tanto induce $\pi^G : k[V]^G \to k[X]^G$; esta π^G es suryectiva y aplicar el teorema 3.17. □

Capítulo 4

Invariantes de grupos finitos

Sea G un grupo finito. Dado un k-espacio vectorial V, el álgebra de funciones polinomiales sobre V se puede interpretar de otro modo:

Si $x_1, ..., x_n$ es una base de V^*, y $S^m(V^*)$ denota el *producto simétrico* de m copias de V^*, que está formado por los polinomios homogéneos de grado m en $x_1, ..., x_n$, entonces

$$k[V] = k \oplus V^* \oplus S^2(V^*) \oplus S^3(V^*) \oplus ...$$

Si V es un G-módulo, entonces G actúa en $k[V]$ vía $(g \cdot f)(v) \coloneqq f(g^{-1} \cdot v)$.

Por definición, esta acción envía polinomios homogéneos a polinomios homogéneos.

En este capítulo se plantea la pregunta: existe un conjunto finito $f_1, \ldots, f_s$ de invariantes tales que todo invariante pueda ser escrito como polinomio en $f_1, \ldots, f_s$. También se analizan algunos aspectos de la dimensión del álgebra de invariantes.

1. Ejemplo: Invariantes de los grupos simétricos

En esta sección, $V = k^n$ y G es el grupo simétrico $\mathbb{S}_n$, que actúa en V permutando los vectores de la base canónica, que denotamos $\alpha_1, \ldots, \alpha_n$; la base dual se denota $x_1, \ldots, x_n$, y es un sistema de generadores de $k[V]$.

En este caso, la acción que G induce en $k[V]$ permuta las variables de los polinomios, y está dada por

$$\sigma \cdot f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Así, los elementos invariantes de esta acción son los polinomios $f(x_1, \ldots, x_n)$ tales que $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ para cada σ en $\mathbb{S}_n$. Estos polinomios se llaman simétricos.

Ahora se introduce una nueva variable X. Se consideran los polinomios $e_i \in k[x_1, \ldots, x_n]$ definidos por

$$\prod_{i=1}^{n}(X + x_i) = \sum_{i=0}^{n} e_i X^{n-i}.$$

El producto $\prod_{i=1}^{n}(X + x_i)$ permanece invariante bajo cualquier permutación de sus factores, y por lo tanto $e_i \in k[x_1, \ldots, x_n]$ son simétricos. Se llaman *polinomios simétricos elementales en* $x_1, \ldots, x_n$.

Ahora se demuestra en términos elementales que el álgebra de polinomios simétricos es finitamente generada.

Proposición 4.1. *Todo polinomio simétrico de* $k[x_1, \ldots, x_n]$ *puede ser escrito como un polinomio en los polinomios simétricos elementales* $e_1, \ldots, e_n$.

DEMOSTRACIÓN. La acción de $\mathbb{S}_n$ en $k[x_1,\dots,x_n]$ envía polinomios homogéneos en polinomios homogéneos. Por lo tanto, un polinomio de $k[x_1,\dots,x_n]$ es simétrico si, y sólo si, todas sus componentes homogéneas son simétricas. Basta con probar que todo polinomio homogéneo simétrico de $k[x_1,\dots,x_n]$ puede ser escrito como un polinomio en los polinomios simétricos elementales $e_1,\dots,e_n$.

Se introduce el *orden lexicográfico* en monomios, que es un orden parcial determinado por

$$x_1^{a_1}\cdots x_n^{a_n} \prec x_1^{b_1}\cdots x_n^{b_n}$$

si, y sólo si, la primera diferencia no nula $b_i - a_i$ es positiva.

Sea $f(x_1,\dots,x_n)$ un polinomio homogéneo simétrico. Sea $x_1^{a_1}\cdots x_n^{a_n}$ el mayor monomio que aparece con coeficiente no nulo, digamos a, en $f(x_1,\dots,x_n)$. Como éste es el mayor monomio, para ningún i puede ocurrir $a_{i+1} > a_i$. En efecto, si eso ocurre para algún i, se considera el menor índice para el que ocurre esa desigualdad. La transposición que intercambia i con $i+1$ está en $\mathbb{S}_n$ y como f es invariante, se deduce que el monomio $x_1^{a_1}\cdots x_i^{a_{i+1}}x_{i+1}^{a_i}\cdots x_n^{a_n}$ también ocurre en f con coeficiente a, pero este es un monomio mayor que $x_1^{a_1}\cdots x_n^{a_n}$. Por lo tanto, $a_{i+1} \leq a_i$ para todo i. Además, el producto

$$e_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n}$$

también tiene al monomio $x_1^{a_1}\cdots x_n^{a_n}$ como mayor monomio. Por lo tanto,

$$f(x_1,\dots,x_n) - ae_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n}$$

es un polinomio simétrico cuyo monomio mayor es menor que el mayor de f, que era $x_1^{a_1}\cdots x_n^{a_n}$.

Inductivamente, asumiendo que

$$f(x_1,\dots,x_n) - ae_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n}$$

es un polinomio en los simétricos elementales, se deduce que $f(x_1,\dots,x_n)$ también lo es.

□

Los polinomios simétricos elementales no sólo generan el álgebra de invariantes, sino que además se tiene la siguiente unicidad.

PROPOSICIÓN 4.2. *Los polinomios simétricos elementales $e_1,\dots,e_n$ son algebraicamente independientes.*

DEMOSTRACIÓN. Sea $f(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$ un polinomio que cumple que $f(e_1,\dots,e_n) = 0$ como polinomio en $x_1,\dots,x_n$. Se probará, que $f(x_1,\dots,x_n)$ es el polinomio nulo. Este polinomio es suma de monomios, y se los escribe de la siguiente forma

$$x_1^{a_1-a_2}x_2^{a_2-a_3}\cdots x_n^{a_n}$$

para enteros $a_1 \geq a_2 \geq \cdots \geq a_n$.

Si $f \neq 0$, sea

$$ax_1^{a_1-a_2}x_2^{a_2-a_3}\cdots x_n^{a_n}$$

con $a \neq 0$, el mayor monomio en el orden lexicográfico entre todas las posibilidades para $(a_1, \ldots, a_n)$. Entonces $f(e_1, \ldots, e_n)$, considerado como polinomio en $x_1, \ldots, x_n$, tiene a $ax_1^{a_1-a_2}x_2^{a_2-a_3}\cdots x_n^{a_n}$ como mayor monomio en el orden lexicográfico, y por lo tanto $a = 0$, contradiciendo lo anterior.

Se deduce $f = 0$.

□

Las dos últimas proposiciones constituyen el Teorema fundamental de los polinomios simétricos. Como se dijo en la introducción, este resultado se debe a Lagrange (1770), aunque aparece en los trabajos de Newton 100 años antes.

En resumen, el anillo de invariantes es un anillo de polinomios; y cada polinomio simétrico se escribe de forma única como polinomio en los simétricos elementales.

Las siguientes secciones abordan esta pregunta en un marco más general.

2. Ejemplo: Invariantes de los grupos alternantes

En esta sección se muestra que no es necesario hacer un análisis demasiado exhaustivo para encontrar grupos con anillos de invariantes que no son anillos de polinomios.

Antes de ver el ejemplo que ocupa esta sección, se muestra un caso más sencillo.

EJEMPLO 4.3. Sea $G = \mathbb{Z}_2$, considerar $V = \mathbb{C}^2$, donde el elemento no trivial de G actúa vía $v \mapsto -v$. Entonces el anillo de invariantes es la suma de las componentes homogéneas de grado par. Por lo tanto, tiene como sistema minimal de generadores a x_1^2, x_2^2, x_1x_2. Así, $\mathbb{C}[V]^G$ no es un anillo de polinomios, porque sus generadores satisfacen $x_1^2x_2^2 = (x_1x_2)^2$.

En esta sección, el grupo en cuestión será el grupo alternante A_n, que está formado por todas las permutaciones pares del grupo simétrico $\mathbb{S}_n$. La representación a estudiar será la misma que en el ejemplo anterior, pero restringida a A_n. Se añade una restricción sobre la característica del cuerpo de base.

Sea k un cuerpo que no tiene característica 2. Sea V el espacio vectorial k^n. Entonces A_n actúa en V permutando los vectores de la base canónica. Sea $x_1, \ldots, x_n$ la base dual. Los invariantes de esta acción se llaman *polinomios alternantes*.

Por otro lado se tiene $sgn\colon \mathbb{S}_n \to k^\times$, la representación *signo* de $\mathbb{S}_n$ que asigna a cada permutación su signo. Entonces A_n es justamente el núcleo de sgn.

Se considera el anillo $k[V]^{\mathbb{S}_n}_{sgn}$ formado por los f en $k[V]$ tales que $g \cdot f = sgn(g)f$ para todo g en $\mathbb{S}_n$. Este anillo se suele llamar el anillo de invariantes con respecto al carácter sgn.

Con este vocabulario, los polinomios alternantes son exactamente los elementos de $k[V]^{\mathbb{S}_n}_{sgn}$.

El siguiente resultado describe a $k[V]^{\mathbb{S}_n}_{sgn}$ como $k[V]^{\mathbb{S}_n}$-módulo.

PROPOSICIÓN 4.4. *En anillo $k[V]^{\mathbb{S}_n}_{sgn}$ como $k[V]^{\mathbb{S}_n}$-módulo es libre y generado por un solo elemento. Mas aún,*

$$k[V]^{\mathbb{S}_n}_{sgn} = k[V]^{\mathbb{S}_n} \cdot \Delta$$

donde Δ *se define como el determinante de la matriz de Vandermonde*

$$\Delta := det \begin{bmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_n \\ \vdots & \dots & \vdots \\ x_1^{n-1} & \dots & x_n^{n-1} \end{bmatrix}$$

Es decir,

$$\Delta = \prod_{j<i}(x_i - x_j)$$

Demostración. Es claro que Δ está en $k[V]^{\mathbb{S}_n}_{sgn}$. Por lo tanto, basta con probar que si f está en $k[V]^{\mathbb{S}_n}_{sgn}$, entonces Δ divide a f. Ahora bien, como $k[V]$ es un dominio de factorización única, basta probar que cada $x_i - x_j$ divide a f. Es decir, ver que f se anula en el subespacio de V determinado por la ecuación $x_i = x_j$. La permutación que intercambia i con j actúa en f multiplicandola por -1. Por lo tanto, $f = -f$ en ese subespacio. Como k no tiene característica 2, se sigue que f es nula en ese subespacio. □

Este resultado es de gran ayuda para calcular $k[V]^{A_n}$. Primero, notar que se tienen extensiones de anillos

$$k[V]^{\mathbb{S}_n} \subset k[V]^{A_n} \subset k[V].$$

Además, A_n es un subgrupo normal de $\mathbb{S}_n$, y por lo tanto el grupo cociente $\mathbb{Z}_2$ actúa en $k[V]^{A_n}$. Como la característica de k no es 2, se sigue que el elemento no nulo de $\mathbb{Z}_2$ es diagonalizable con autovalores ± 1; que $k[V]^{\mathbb{S}_n}$ es el autoespacio de 1 y $k[V]^{\mathbb{S}_n}_{sgn}$ el de -1.

Corolario 4.5. *Sean k un cuerpo de característica distinta de 2, $V = k^n$ la representación permutación de $\mathbb{S}_n$, y $sgn\colon \mathbb{S}_n \to k^\times$ la representación signo de $\mathbb{S}_n$. Entonces el anillo de invariantes $k[V]^{A_n}$ es un módulo libre de rango 2 sobre $k[V]^{\mathbb{S}_n}$,*

$$k[V]^{A_n} = k[V]^{\mathbb{S}_n} \oplus k[V]^{\mathbb{S}_n}_{sgn} = k[e_1, \dots, e_n] \oplus k[e_1, \dots, e_n] \cdot \Delta.$$

Observación 4.6. Notar que $e_1, \dots, e_n, \Delta$ es un conjunto minimal de generadores de $k[V]^{A_n}$. Sin embargo, no son algebraicamente independientes, porque $\Delta^2 \in k[e_1, \dots, e_n]$.

En resumen, $k[V]^{A_n}$ no es un anillo de polinomios, pero es un módulo finitamente generado sobre su subálgebra $k[e_1, \dots, e_n]$, que si es un álgebra de polinomios.

Para una demostración del Teorema si A es un dominio de factorización única, entonces el anillo de polinomios $A[X]$ también es dominio de factorización única, ver [**4**], pp.304.

3. Primera noción de finitud del álgebra de invariantes

Si G es un grupo finito y k un cuerpo cuya característica no divide al orden de G, sea $\int_G = \frac{1}{|G|}\sum_{g\in G} g \in kG$.

Se considera para cada G-módulo $\rho : G \to GL(V)$, la aplicación

$$\rho\left(\int_G\right) : V \to V^G,$$

que está dada por $\rho(\int_G)(v) = \frac{1}{|G|}\sum_{g\in G}\rho(g)(v)$. Este es un morfismo de G-módulos. Además, todos los elementos de la imagen de $\rho(\int_G)$ están en V^G: dados $v \in V$ y $h \in G$, se tiene

$$\rho(h)\left(\rho\left(\int_G\right)(v)\right) = \frac{1}{|G|}\sum_{g\in G}\rho(hg)(v) = \frac{1}{|G|}\sum_{g\in G}\rho(g)(v) = \rho\left(\int_G\right)(v).$$

Con una idea similar, se prueba el siguiente resultado.

COROLARIO 4.7. *(Teorema de Maschke). Si G es un grupo finito y k un cuerpo cuya característica no divide al orden de G, entonces G es reductivo.*

DEMOSTRACIÓN. Sea V un G-módulo con representación $\rho : G \to GL(V)$. Sea $\iota\colon V^G \hookrightarrow V$ la inclusión. Se considera $\rho(\int_G)\colon V \to V^G$. Entonces, para todo $v \in V^G$, se tiene

$$\rho\left(\int_G\right)\circ\iota(v) = \frac{1}{|G|}\sum_{g\in G}\rho(g)(v) = \frac{1}{|G|}\sum_{g\in G}v = v.$$

Por lo tanto, $\rho(\int_G)\colon V \to V^G$ es una retracción de G-módulos de la inclusión $V^G \hookrightarrow V$, y así V se proyecta sobre V^G. □

Cuando el grupo en cuestión es finito, el siguiente resultado garantiza que el álgebra de invariantes es finitamente generada.

TEOREMA 4.8. *(Hilbert, Noether) Sean k un cuerpo y A una k-álgebra conmutativa finitamente generada. Si G actúa por automorfismos en A, entonces el álgebra de G-invariantes A^G también es finitamente generada sobre k y A es finitamente generado como A^G-módulo.*

DEMOSTRACIÓN. Primero, se remarca que A es una extensión íntegra de A^G. En efecto, dado a en A, a es una raíz del polinomio mónico

$$\prod_{g\in G}(X - g\cdot a)$$

que está en $A^G[X]$.

Sea $\{a_1, ..., a_m\}$ un conjunto que genera a A como k-álgebra, y para cada i sea p_i un polinomio mónico en A^G que tiene a a_i como raíz. Se denota por B a la subálgebra de A^G generada por los coeficientes de $p_1, ..., p_n$. Entonces B es una k-álgebra finitamente generada, y por lo tanto noetheriana. Como A es un B-módulo finitamente generado, se sigue que A^G también lo es. Por lo tanto, A^G es finitamente generada como k-álgebra. □

La última prueba está muy lejos de ser constructiva. Hay dos aspectos que se destacan:

(1) No se conoce A^G, pero se necesitan generadores de A sobre A^G y peor aún, polinomios que los tengan como raíces.
(2) Como no se conoce A^G, tampoco se sabe qué es B, y sin embargo se necesitan generadores de A^G como B-módulos.

COROLARIO 4.9. *Si G es un grupo finito y V es un G-módulo de dimensión finita sobre el cuerpo k, entonces $k[V]^G$ es una k-álgebra finitamente generada.*

DEMOSTRACIÓN. Es consecuencia inmediata del teorema anterior, porque G actúa por automorfismos de k-álgebras en $k[V]$, que es una k-álgebra finitamente generada. □

4. Dimensión de Krull

Ya se estableció que $k[V]$ es una extensión finita de la k-álgebra finitamente generada $k[V]^G$. Ahora se usa esto para establecer una relación entre los ideales primos de $k[V]$ y los de $k[V]^G$.

DEFINICIÓN 4.10. Sea A un anillo conmutativo. Se define la *dimensión de Krull* como la longitud máxima n de las cadenas de inclusiones propias de ideales primos de A

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

Si no existe tal n natural, se dice que la dimensión de Krull de A es infinita.

La *dimensión de Krull* de un A-módulo M se define como la dimensión de Krull del anillo $A/Ann_A(M)$.

Dado x en A, se considera el conjunto

$$S_x \coloneqq x^{\mathbb{N}}(1+xA) = \{x^n(1+xa) \colon n \in \mathbb{N}, a \in A\}$$

que es multiplicativamente cerrado. Y se define la *frontera* de x en A como la localización

$$A_x \coloneqq S_x^{-1}A.$$

Notar que si x es nilpotente o inversible, entonces la frontera A_x es trivial. El paso de A a A_x elimina los elementos nilpotentes y los elementos inversibles.

PROPOSICIÓN 4.11. *Sean A un anillo conmutativo con unidad y m un entero no negativo. Los siguientes son equivalentes:*

(a) La dimensión de Krull de A es a lo sumo m.
(b) Para cada x en A, la dimensión de Krull de A_x es a lo sumo $m-1$.

DEMOSTRACIÓN. Recordar que los ideales primos de una localización $S^{-1}A$ son de la forma $S^{-1}\mathfrak{p}$ donde $\mathfrak{p}$ es un ideal primo de A que no interseca a S. Se prueban dos afirmaciones:

Afirmación 1: Para cada x en A, todos los ideales maximales de A intersecan a S_x.

Sea $\mathfrak{m}$ es un ideal maximal de A. Sea x en A. Si x está en $\mathfrak{m}$, es inmediato. Si ese no es el caso, entonces x es inversible módulo $\mathfrak{m}$, y por lo tanto $1+xA$ interseca a $\mathfrak{m}$.

Afirmación 2: Si $\mathfrak{m}$ es un ideal maximal de A y $\mathfrak{p}$ es un ideal primo contenido en $\mathfrak{m}$, entonces para todo x en $\mathfrak{m} \setminus \mathfrak{p}$ se cumple que $\mathfrak{p}$ no interseca a S_x.

En efecto, si $x^k(1+xa) \in \mathfrak{p}$, como $x \notin \mathfrak{p}$ se tiene $1+xa \in \mathfrak{p} \subset \mathfrak{m}$, y por lo tanto $1 \in \mathfrak{m}$, contradiciendo que $\mathfrak{m}$ es maximal.

Ahora se prueba la equivalencia. Por la Afirmación 1, toda cadena de ideales primos terminando con un ideal maximal pierde un término cuando se pasa a A_x. Mientras que por la Afirmación 2, una cadena de largo máximo m se puede reducir a una de largo $m-1$ eligiendo un x adecuado. □

Más generalmente, se tiene:

PROPOSICIÓN 4.12. *Sean A un anillo conmutativo con unidad y m un entero no negativo. Los siguientes son equivalentes:*

(a) La dimensión de Krull de A es a lo sumo m.
(b) Para cada $x_0, \dots, x_m$ en A existen $a_0, \dots a_m$ en A y $n_0, \dots, n_m$ en $\mathbb{N}$ tales que

$$x_0^{n_0}(\dots(x_m^{n_m}(1 + a_m x_m) + \dots) + a_0 x_0) = 0.$$

DEMOSTRACIÓN. Se procede por inducción en m. El caso $m = 0$ es el enunciado de la proposición anterior. Se supone que el resultado es cierto para todos los anillos conmutativos con unidad y todos los enteros no negativos menores que m. Se deduce que la dimensión de una localización $S^{-1}A$ es menor que m si, y sólo si, para cada $x_0, \dots, x_{m-1} \in A$ existen $a_0, \dots, a_{m-1} \in R$, $s \in S$, y $n_0, \dots, n_{m-1} \in \mathbb{N}$ tales que

$$x_0^{n_0}(x_1^{n_1} \dots (x_{m-1}^{n_{m-1}}(s + a_{m-1}x_{m-1}) + \dots + a_1 x_1) + a_0 x_0) = 0.$$

Aplicando esta igualdad a la localización A_{x_m}, y cambiando $s \in S$ por un elemento $x_m^{n_m}(1 + a_m x_m)$ de S_{x_m} se obtiene la igualdad buscada.

□

PROPOSICIÓN 4.13. *Sean k un cuerpo y A una k-álgebra conmutativa. Si cada conjunto $x_0, \dots, x_m$ de A es algebraicamente dependiente sobre k, entonces la dimensión de Krull de A es a lo sumo m.*

DEMOSTRACIÓN. Sea $Q(x_0, \dots, x_m) = 0$ una relación algebraica sobre k. Los monomios de Q son de la forma $\alpha_{p_0,\dots,p_m} x_0^{p_0} x_1^{p_1} \dots x_m^{p_m}$. Se los ordena según el orden lexicográfico en las palabras $p_0 p_1 \dots p_m$. Se asume que el primer monomio tiene coeficiente 1, y que dicho monomio es $x_0^{n_1} x_1^{n_1} \dots x_m^{n_m}$. Respetando el orden lexicográfico, Q se puede escribir de la forma

$$x_0^{n_0} \cdots x_m^{n_m} + x_0^{n_0} \cdots x_m^{1+n_m} R_m + x_0^{n_0} \cdots x_{m-1}^{1+n_{m-1}} R_{m-1} + \cdots + x_0^{n_0} x_1^{1+n_1} R_1 + x_0^{1+n_0} R_0,$$

donde $R_j \in k[x_i \colon i \geq j]$. El resultado se sigue de la proposición anterior. □

PROPOSICIÓN 4.14. *La dimension de Krull de $k[x_1, \dots, x_n]$ es n.*

DEMOSTRACIÓN. La dimension de Krull de $k[x_1, \dots, x_n]$ es mayor o igual que n. En efecto,

$$(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, x_2, \dots, x_n)$$

es una cadena ascendente de inclusiones propias de ideales primos de $k[V]$.

Por otro lado, como cualquier conjunto de $n + 1$ elementos de $k[x_1, \dots, x_n]$ satisface relaciones algebraicas, de la proposición anterior se sigue que la dimensión de Krull de $k[x_1, \dots, x_n]$ no supera a n. □

COROLARIO 4.15. *Si V es un espacio vectorial sobre el cuerpo k, entonces la dimension de Krull del anillo $k[V]$ coincide con $dim_k(V)$.* □

4.1. Dependencia algebraica.

DEFINICIÓN 4.16. Sean B un anillo conmutativo con unidad y A un subanillo que contiene a la identidad del anillo. Un elemento x en B se dice *íntegro* sobre A si es raíz de un polinomio mónico con coeficientes en A.

LEMA 4.17. *Sean A un anillo conmutativo con unidad, $\mathfrak{a}$ un ideal de A y M un A-módulo finitamente generado.*

Si ϕ es un endomorfismo de A-módulos de M tal que $\phi(M) \subset \mathfrak{a} \cdot M$, entonces existen $a_1, \ldots, a_n$ en $\mathfrak{a}$ tales que

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0.$$

DEMOSTRACIÓN. Sean $x_1, \ldots, x_n$ generadores de M. Para $i = 1, \ldots, n$, como $\phi(x_i)$ está en $\mathfrak{a} \cdot M$, existen $a_{i1}, \ldots a_{in}$ en $\mathfrak{a}$ tales que

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j.$$

Y por lo tanto

$$\sum_{j=1}^{n}(\delta_{ij}\phi - a_{ij})x_j = 0.$$

Así, multiplicando ambos lados de la última igualdad por la matríz adjunta de $(\delta_{ij}\phi - a_{ij})_{i,j}$, se deduce que cada $x_1, \ldots, x_n$ son raíces de $det(\delta_{ij}\phi - a_{ij})_{i,j}$. Por lo tanto, $(\delta_{ij}\phi - a_{ij})_{i,j}$ es el endomorfismo nulo de M. Desarrollando el determinante, se tiene la igualdad requerida.

□

PROPOSICIÓN 4.18. *Sea A un subanillo de B, y x en B. Los siguientes son equivalentes.*

(a) x es íntegro sobre A.
(b) $A[x]$ es un A-módulo finitamente generado.
(c) Existe un subanillo C de B que contiene a $A[x]$ y es finitamente generado como A-módulo.
(d) Existe un $A[x]$-módulo fiel M que es finitamente generado como A-módulo.

DEMOSTRACIÓN. (a) $\implies$ (b). Sean $a_1, \ldots, a_n$ en A tales que

$$x^n + a_1x^{n-1} + \cdots + a_n = 0.$$

Entonces, para cada entero no negativo r, se tiene

$$x^{n+r} = -(a_1x^{n+r-1} + \cdots + a_nx^r).$$

Por lo tanto, inductivamente, todas las potencias positivas de x están en el A-módulo generado por $1, x, \ldots, x^{n-1}$. Así, como A-módulo, $A[x]$ está generado por $1, x, \ldots, x^{n-1}$.

(b) $\implies$ (c). Inmediato, tomando $C = A[x]$.

(c) $\implies$ (d). Tomar $M = C$ que es un $A[x]$-módulo, y es fiel porque si $y \cdot C = 0$, entonces $y \cdot 1 = 0$.

(d) $\implies$ (a). Es consecuencia del lema anterior. Sea ϕ la multiplicación por x, y $\mathfrak{a} = A$. Se tiene $x \cdot M \subset M$ porque M es un $A[x]$-módulo. Como M es fiel, si $a_1, \ldots, a_n$ en $\mathfrak{a}$ son tales que

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

entonces

$$x^n + a_1x^{n-1} + \cdots + a_n = 0$$

□

COROLARIO 4.19. *Sean $x_1, \ldots, x_n$ elementos de B, todos íntegros sobre A. Entonces $A[x_1, \ldots, x_n]$ es finitamente generado como A-módulo.*

DEMOSTRACIÓN. Se procede por inducción en n.

El caso $n = 1$ ya fue probado anteriormente.

Se asume $n < 1$. Para $i = 1, \ldots, n$, sea $A_i \coloneqq A[x_1, \ldots, x_r]$. Por el caso $n = 1$, se tiene que $A_n = A_{n-1}[x_n]$ es finitamente generado como A_{n-1}-módulo. Por hipótesis inductiva, A_{n-1} es finitamente generado como A-módulo. Por lo tanto, A_n es finitamente generado como A-módulo, como consecuencia del siguiente lema. □

LEMA 4.20. *Sea $A \subset B \subset C$ una extensión de anillos. Si C es finitamente generado como B-módulo y B es finitamente generado como A-módulo, entonces C es finitamente generado como A-módulo.*

DEMOSTRACIÓN. Sean $y_1, \ldots, y_m$ generadores de C sobre B, y sean $x_1, \ldots, x_n$ generadores de B sobre A. Entonces $x_i y_j$, $1 \leq i \leq n$, $1 \leq j \leq m$ generan C sobre A. □

COROLARIO 4.21. *El conjunto C de elementos de B que son íntegros sobre A es un subanillo de B.*

DEMOSTRACIÓN. Sean x, y en B íntegros sobre A. Por el corolario anterior, $A[x, y]$ es finitamente generado como A-módulo. Por (c) de 4.18, se sigue que $x+y$, $x - y$, xy son íntegros sobre A.

□

DEFINICIÓN 4.22. Sea A un subanillo de B. El anillo C de 4.21 se llama *clausura íntegra de A en B*. Si $C = A$ se dice que A es *íntegramente cerrado en B*. Si $C = B$ se dice que B es íntegro sobre A.

COROLARIO 4.23. *Transitividad de la dependencia íntegra. Sean $A \subset B \subset C$ anillos. Si C es íntegro sobre B y B es íntegro sobre A, entonces C es íntegro sobre A.*

DEMOSTRACIÓN. Dado x en C, sean $b_1, \ldots, b_n$ en B tales que

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0.$$

Se denota por B' al anillo $A[b_1, \ldots, b_n]$. Como B es íntegro sobre A, se probó que B' es finitamente generado como A-módulo. Además, como x es íntegro sobre B', $B'[x]$ es finitamente generado como B'-módulo. Por lo tanto, $B'[x]$ es finitamente generado como A-módulo. Por (c) de 4.18, se sigue que x es íntegro sobre A. □

COROLARIO 4.24. *Sea A un subanillo de B. Si C es la clausura íntegra de A en B, entonces C es íntegramente cerrado en B.*

DEMOSTRACIÓN. Sea x en B íntegro sobre C. Por el corolario anterior, como C es íntegro sobre A, se deduce que x es íntegro sobre A. Por lo tanto, x está en C. □

PROPOSICIÓN 4.25. *Sea $A \subset B$ una extensión íntegra de anillos.*

(1) Si $\mathfrak{b}$ es un ideal de B y $\mathfrak{a} \coloneqq A \cap \mathfrak{b}$ es la contracción *de $\mathfrak{b}$, entonces $B/\mathfrak{b}$ es íntegro sobre $A/\mathfrak{a}$.*

(2) Si S es un subconjunto multiplicativamente cerrado de A, entonces $S^{-1}B$ es íntegro sobre $S^{-1}A$.

DEMOSTRACIÓN. (1) Dado y en $B/\mathfrak{b}$, digamos $y = x + \mathfrak{b}$, existen $a_1, \ldots, a_n$ en A tales que

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

Reduciendo esa ecuación módulo $\mathfrak{b}$, se obtiene una ecuación en y con coeficientes en $A/\mathfrak{a}$.

(2) Dado x/s en $S^{-1}B$, con x en B y s en S, la ecuación de arriba se transforma en

$$(x/s)^n + a_1/s(x/s)^{n-1} + \cdots + a_n/s^n = 0.$$

Y por lo tanto x/s es íntegro sobre $S^{-1}A$.

□

4.2. Teorema de ascenso.

PROPOSICIÓN 4.26. *Sea $A \subset B$ una extensión íntegra de dominios íntegros. Entonces A es un cuerpo si, y sólo si, B es un cuerpo.*

DEMOSTRACIÓN. Se supone primero que A es un cuerpo. Sea x en B no nulo, y sea n el menor natural tal que

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

para ciertos $a_1, \ldots, a_n$ en A. Por minimalidad de n y por ser B un dominio íntegro, se sigue $a_n \neq 0$. Por lo tanto,

$$x^{-1} = -a_n^{-1}(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) \in B.$$

Y así, B es un cuerpo.

Recíprocamente, si B es un cuerpo, dado x en A no nulo, x tiene un inverso x^{-1} en B. Como B es íntegro sobre A, existen $a_1, \ldots, a_m$ en A tales que

$$x^{-m} + a_1 x^{-m+1} + \cdots + a_m = 0.$$

Multiplicando por x^{m-1}, y pasando de término, se tiene

$$x^{-1} = -(a_1 + a_2 x + \cdots + a_m x^{m-1}) \in A.$$

Y por lo tanto A es un cuerpo. □

COROLARIO 4.27. *Sea $A \subset B$ una extensión íntegra, y sea $\mathfrak{q}$ un ideal primo de B. Sea $\mathfrak{p} \coloneqq A \cap \mathfrak{q}$ la* contracción *de $\mathfrak{q}$. Entonces $\mathfrak{p}$ es maximal si, y sólo si, $\mathfrak{q}$ es maximal.*

DEMOSTRACIÓN. Como $\mathfrak{p}$ resulta ser un ideal primo de A, tanto $B/\mathfrak{q}$ como $A/\mathfrak{p}$ son dominios íntegros. Además, $A/\mathfrak{p} \subset B/\mathfrak{q}$ es una extensión íntegra. Por la proposición anterior, $A/\mathfrak{p}$ es un cuerpo si, y sólo si, $B/\mathfrak{q}$ es un cuerpo. Es decir, $\mathfrak{p}$ es maximal si, y sólo si, $\mathfrak{q}$ es maximal. □

PROPOSICIÓN 4.28. *Sea $A \subset B$ una extensión íntegra, y sean $\mathfrak{q}$, $\mathfrak{q}'$ ideales primos de B. Si $\mathfrak{q} \subset \mathfrak{q}'$ y $A \cap \mathfrak{q} = A \cap \mathfrak{q}'$, entonces $\mathfrak{q} = \mathfrak{q}'$.*

DEMOSTRACIÓN. Sea $\mathfrak{p} \coloneqq A \cap \mathfrak{q} = A \cap \mathfrak{q}'$, que es primo. Ya se probó que $B_\mathfrak{p}$ es íntegro sobre $A_\mathfrak{p}$. Sea $\mathfrak{m}$ la extensión de $\mathfrak{p}$ en $A_\mathfrak{p}$, y sean $\mathfrak{n}$ y $\mathfrak{n}'$ las extensiónes de $\mathfrak{q}$ y $\mathfrak{q}'$ en $B_\mathfrak{p}$, respectivamente. Entonces $\mathfrak{m}$ es el ideal maximal de $A_\mathfrak{p}$. Por otro lado, $\mathfrak{n} \subset \mathfrak{n}'$, y las contracciones de estos ideales coinciden con $\mathfrak{m}$. Por el corolario anterior, $\mathfrak{n}$ y $\mathfrak{n}'$ son maximales. Por lo tanto, $\mathfrak{n} = \mathfrak{n}'$ y se sigue $\mathfrak{q} = \mathfrak{q}'$.

□

TEOREMA 4.29. *Sea $A \subset B$ una extensión íntegra y sea $\mathfrak{p}$ un ideal primo de A. Entonces existe un ideal primo $\mathfrak{q}$ de B tal que $\mathfrak{p} = A \cap \mathfrak{q}$.*

DEMOSTRACIÓN. Se probó que $B_\mathfrak{p}$ es íntegro sobre $A_\mathfrak{p}$. Además, el diagrama

$$\begin{array}{ccc} A & \to & B \\ \downarrow & & \downarrow \\ A_\mathfrak{p} & \to & B_\mathfrak{p} \end{array}$$

es conmutativo. Sea $\mathfrak{n}$ el ideal maximal de $B_\mathfrak{p}$. Entonces $\mathfrak{m} \coloneqq A_\mathfrak{p} \cap \mathfrak{n}$ es maximal, y por lo tanto es el único ideal maximal de $A_\mathfrak{p}$. Además, $\mathfrak{q} \coloneqq \beta^{-1}(\mathfrak{n})$ es primo, y se deduce que $\mathfrak{q} \cap A = \alpha^{-1}(\mathfrak{m}) = \mathfrak{p}$.

□

TEOREMA 4.30. *(Teorema de ascenso) Sea $A \subset B$ una extensión íntegra. Sean $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ una cadena de ideales primos de A y $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ una cadena de ideales primos de B con $m < n$ tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $i = 1, \ldots, m$.*

Entonces la cadena $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ puede extenderse a una cadena $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ de ideales primos de B tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $i = 1, \ldots, n$.

DEMOSTRACIÓN. Vía un razonamiento inductivo, se deduce que basta con probar sólo el caso $m = 1$, $n = 2$. Sean $\overline{A} \coloneqq A/\mathfrak{p}_1$ y $\overline{B} \coloneqq A/\mathfrak{q}_1$. Entonces $\overline{A} \subset \overline{B}$ es una extensión íntegra. Se denota por $\overline{\mathfrak{p}_2}$ a la imagen de $\mathfrak{p}_2$ en $\overline{A}$. Por el teorema anterior, existe un ideal primo $\overline{\mathfrak{q}_2}$ de $\overline{B}$ tal que $\overline{\mathfrak{q}_2} \cap \overline{A} = \overline{\mathfrak{p}_2}$. Sea $\mathfrak{q}_2 \subset B$ la preimagen de $\overline{\mathfrak{q}_2}$. Entonces $\mathfrak{q}_2$ es un ideal primo de B, y cumple $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

□

4.3. Dominios íntegros algebraicamente cerrados. Existe un análogo al Teorema de ascenso pero con cadenas de primos descendentes, conocido como Teorema de descenso. Ese resultado requiere hipótesis más finas, y en esta sección se las detalla y analiza.

Se puede dar una versión más precisa de 4.25, (2).

PROPOSICIÓN 4.31. *Sean $A \subset B$ una extensión de anillos y C la clausura íntegra de A en B. Sea S un subconjunto multiplicativamente cerrado de A. Entonces $S^{-1}C$ es la clausura íntegra de $S^{-1}A$ en $S^{-1}B$.*

DEMOSTRACIÓN. Se probó en 4.25, (2) que $S^{-1}C$ es íntegro sobre $S^{-1}A$. Sea b/s en $S^{-1}B$ íntegro sobre $S^{-1}A$. Sean $a_1, \ldots, a_n$ en A y $s_1, \ldots, s_n$ en S tales que

$$(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \cdots + (a_n/s_n) = 0.$$

Sea $t = \prod_{i=1}^n s_i \in S$.

Ahora mutiplicando el polinomio en b/s por $(st)^n$, se ve que bt es raíz de un polinomio mónico con coeficientes en A. Por lo tanto, bt está en C. Luego, $b/s = bt/st$ está en $S^{-1}C$.

□

DEFINICIÓN 4.32. Un dominio íntegro se dice *íntegramente cerrado* (sin referencia a ninguna extensión) si es íntegramente cerrado sobre su anillo de fracciones.

Recordar el siguiente resultado.

PROPOSICIÓN 4.33. *Sea A un anillo y $f\colon M \to N$ un morfismo de A-módulos. Son equivalentes:*

(1) $f\colon M \to N$ es suryectiva.
(2) $f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ es suryectiva para todo ideal primo $\mathfrak{p}$ de A.
(3) $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ es suryectiva para todo ideal maximal $\mathfrak{m}$ de A.

PROPOSICIÓN 4.34. *Sea A un dominio íntegro. Son equivalentes:*

(1) A es íntegramente cerrado.
(2) $A_{\mathfrak{p}}$ es íntegramente cerrado para todo ideal primo $\mathfrak{p}$ de A.
(3) $A_{\mathfrak{m}}$ es íntegramente cerrado para todo ideal maximal $\mathfrak{m}$ de A.

DEMOSTRACIÓN. Sea F el anillo de fracciones de A, y sea C la clausura íntegra de A en F. Se denota por $f\colon A \to C$ a la inclusión, que es un morfismo de A-módulos. Dado $\mathfrak{p}$ un ideal primo de A, se probó que $C_{\mathfrak{p}}$ es la clausura íntegra de $A_{\mathfrak{p}}$, y que f induce un mapa $f_{\mathfrak{p}}\colon A_{\mathfrak{p}} \to C_{\mathfrak{p}}$ que coincide con la inclusión.

Ahora bien, A es íntegramente cerrado si, y sólo sí, f es suryectiva. Y dados un ideal primo $\mathfrak{p}$ y un maximal $\mathfrak{m}$ de A, $A_{\mathfrak{p}}$ (respectivamente, $A_{\mathfrak{m}}$) es íntegramente cerrado si, y sólo sí, $f_{\mathfrak{p}}$ (respectivamente $f_{\mathfrak{m}}$) es suryectiva.

□

DEFINICIÓN 4.35. Sean $A \subset B$ una extensión de anillos, y sea $\mathfrak{a}$ un ideal de A. Un elemento de B se dice *íntegro sobre* $\mathfrak{a}$ si es raíz de un polinomio mónico con coeficientes en $\mathfrak{a}$.

La *clausura íntegra de* $\mathfrak{a}$ *en* B es el conjunto de elementos de B que son íntegros sobre $\mathfrak{a}$.

LEMA 4.36. *Sean $A \subset B$ una extensión de anillos y C la clausura íntegra de A en B. Sea $\mathfrak{a}$ un ideal de A y sea $\mathfrak{a}^e$ su extensión a C. Entonces la clausura íntegra de $\mathfrak{a}$ en B es el radical de $\mathfrak{a}^e$. En particular, es cerrado por suma y multiplicación.*

DEMOSTRACIÓN. Se denota por $r(\mathfrak{a}^e)$ al radical de $\mathfrak{a}^e$. Sea x en B integral sobre $\mathfrak{a}$. Existen $a_1, \dots, a_n$ en $\mathfrak{a}$ tales que

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

Entonces x está en C, y $x^n = -(a_1 x^{n-1} + \cdots + a_n)$ está en $\mathfrak{a}^e$. Por lo tanto, $x \in r(\mathfrak{a}^e)$. Recíprocamente, dado x en $r(\mathfrak{a}^e)$, existen $a_1, \dots, a_m$ en $\mathfrak{a}$ y $x_1, \dots, x_m$ en C tales que, para algún n,

$$x^n = a_1 x_1 + \cdots + a_m c_m.$$

Como cada x_i es íntegro sobre A, se sigue que $M \coloneqq A[x_1, \dots, x_n]$ es finitamente generado como A-módulo. Además, $x^n M \subset \mathfrak{a}M$. Por 4.17, tomando como ϕ la multiplicación por x^n, se sigue que x^n es íntegro sobre A, y por lo tanto x es íntegro sobre A.

□

PROPOSICIÓN 4.37. *Sean $A \subset B$ dominios íntegros, A íntegramente cerrado. Sea F el cuerpo de fracciones de A. Si $x \in B$ es íntegro sobre un ideal $\mathfrak{a}$ de A, entonces x es íntegro sobre F. Y mas aún, el polinomio minimal de x sobre F tiene coeficientes en $r(\mathfrak{a})$.*

DEMOSTRACIÓN. Si x satisface una ecuación polinomial mónica con coeficientes en $\mathfrak{a}$, ciertamente satisface una ecuación con coeficientes en F. Se denota por $p(t)$ al polinomio minimal de x sobre F, y sea n su grado. Sea L una extensión (de cuerpos) de F que contiene a todas las raíces $x_1, \ldots, x_n$ de $p(t)$. Cada $x_1, \ldots, x_n$ satisface la ecuación polinomial que satisface x sobre $\mathfrak{a}$, y por lo tanto todos ellos son íntegros sobre $\mathfrak{a}$. Ahora bien, como $p(t) = (t - x_1) \ldots (t - x_n)$, los coeficientes de $p(t)$ son polinomios en $x_1, \ldots, x_n$. Por el resultado anterior, los coeficientes son íntegros sobre $\mathfrak{a}$. Como A es íntegramente cerrado, nuevamente por el resultado anterior, se sigue que los coeficientes de $p(t)$ están en $r(\mathfrak{a})$.

□

4.4. Teorema de descenso. Para una demostración del siguiente resultado básico de álgebra conmutativa ver por ejemplo [**1**], pp.43.

LEMA 4.38. *Sea $f\colon A \to B$ un morfismo de anillos, y sea $\mathfrak{p}$ un ideal primo de A. Entonces $\mathfrak{p}$ es la contracción de un ideal primo de B si, y sólo si, $\mathfrak{p}^{ec} = \mathfrak{p}$.*

□

TEOREMA 4.39. *Teorema de descenso. Sea $A \subset B$ una extensión íntegra, con A íntegramente cerrado. Sean $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$ una cadena de ideales primos de A y $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ una cadena de ideales primos de B con $m < n$ tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $i = 1, \ldots, m$.*

Entonces la cadena $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ puede extenderse a una cadena $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_n$ de ideales primos de B tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $i = 1, \ldots, n$.

DEMOSTRACIÓN. Como en el Teorema de ascenso, la prueba se reduce al caso $m = 1$, $n = 2$. En este caso, hay que probar que $\mathfrak{p}_2$ es la contracción de un ideal primo del anillo $B_{\mathfrak{q}_1}$. Por el lema anterior, eso es equivalente a que $\mathfrak{p}_2^{ec} = \mathfrak{p}_2$. Ahora bien, la extensión de $\mathfrak{p}_2$ en $B_{\mathfrak{q}_1}$ es $B_{\mathfrak{q}_1}\mathfrak{p}_2$; y la contracción de este último en A es $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$. Se probará entonces que $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$.

Sea x en $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$. Como x está en $B_{\mathfrak{q}_1}\mathfrak{p}_2$, es de la forma y/s para ciertos y en $B\mathfrak{p}_2$ y s en $B \setminus \mathfrak{q}_1$. Por el lema 4.36, y es íntegro sobre $\mathfrak{p}_2$. Sea F el cuerpo de fracciones de A. Por la proposición 4.37, si la ecuación minimal de y sobre F es

$$y^r + u_1 y^{r-1} + \cdots + u_r = 0, \tag{4.1}$$

entonces $u_1, \ldots, u_r$ están en $\mathfrak{p}_2$. Además, como x está en A, si se denota por x^{-1} al inverso de x en F, entonces $s = yx^{-1}$. Por lo tanto, la ecuación polinomial minimal de s sobre F se obtiene dividiendo *(1)* por x^r. Así, si se define $v_i \coloneqq u_i/x^i$ para $i = 1, \ldots, r$, entonces la ecuación minimal de s es

$$s^r + v_1 s^{r-1} + \cdots + v_r = 0. \tag{4.2}$$

Evidentemente, para $i = 1, \ldots, r$, se tiene

$$v_i = x^i u_i \in \mathfrak{p}_2. \tag{4.3}$$

Por otro lado, s es íntegro sobre A. Así, por la proposición 4.37 (aplicada a $\mathfrak{a} = A$), se deduce que $v_1, \ldots, v_r$ están en A.

Ahora, suponiendo que $x \notin \mathfrak{p}_2$, por *(3)* se deduce que $v_1, \ldots, v_r$ están en $\mathfrak{p}_2$. Y luego, por *(2)*, se tiene $s^r \in B\mathfrak{p}_2 \subset B\mathfrak{p}_1 \subset \mathfrak{q}_1$. Por lo tanto, s está en $\mathfrak{q}_1$, lo cual es una contradicción. Se sigue que $x \in \mathfrak{p}_2$.

Se probó la inclusión $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A \subset \mathfrak{p}_2$. La recíproca es inmediata.

□

4.5. Dimensión de Krull. Como consecuencia inmediata del Teorema de ascenso, se tiene.

COROLARIO 4.40. *Si $A \subset B$ es una extensión íntegra de anillos, entonces las dimensiones de Krull de A y B son iguales.*

TEOREMA 4.41. *Sean G un grupo finito y V un G-módulo de dimensión finita sobre el cuerpo k.*

Entonces la dimensión de Krull del anillo $k[V]^G$ coincide con $dim_k(V)$.

DEMOSTRACIÓN. Se probó que la extensión $k[V]^G \subset k[V]$ es íntegra. Por el corolario anterior, se deduce que la dimensión de Krull del anillo $k[V]^G$ coincide con la dimensión de Krull de $k[V]$. Pero, por 4.15, la dimensión de Krull de $k[V]$ es $dim_k(V)$.

□

5. Cota de Noether

En esta sección se establece una cota para el grado de los generadores del álgebra de invariantes. Se impone una restricción en la característica del cuerpo.

Sean G un grupo finito y V un G-módulo de dimensión finita sobre el cuerpo k. Sea H un subgrupo arbitrario de G. Se considera la *transferencia*

$$Tr_H^G \colon k[V]^H \to k[V]^G$$

dada por

$$Tr_H^G(f)(x) \coloneqq \sum_{gH \in G/H} g(f)(x) = \sum_{gH \in G/H} f(g^{-1}x),$$

donde la suma se toma sobre una familia de representantes de coclases de G/H. Si g, g' pertenecen a la misma coclase, $gH = g'H$, para $f \in k[V]^H$ se tiene $g^{-1}g' \in H$ y por lo tanto $g^{-1}g'(f) = f$, es decir, $g'(f) = g(f)$. Así, la definición no depende de la familia de representantes que se escoja.

Además, dados $g' \in G$ y $f \in k[V]^H$, se tiene

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

(la penúltima igualdad se debe a que si $g_1, \ldots g_r$ es una clase de representantes de coclases, entonces $g'g_1, \ldots, g'g_r$ también).

Por lo tanto $Tr_H^G(f)$ está en $k[V]^G$. Esto prueba la buena definición de

$$Tr_H^G \colon k[V]^H \to k[V]^G.$$

A continuación se resumen algunas propiedades de esta aplicación.

(1) La composición $k[V]^G \hookrightarrow k[V]^H \xrightarrow{Tr_H^G} k[V]^G$ es la multiplicación por $|G : H|$. Simplemente porque, para $f \in k[V]^G$, $Tr_H^G(f) = \sum_{gH \in G/H} f = |G : H|f$.
(2) Si $|G : H|$ es invertible en k, entonces Tr_H^G es suryectivo. Mas aún, la aplicación

$$\pi_H^G \coloneqq \frac{1}{|G : H|} Tr_H^G \colon k[V]^H \to k[V]^G \hookrightarrow k[V]^H$$

proyecta $k[V]^H$ sobre $k[V]^G$.
(3) $k[V]^H = k[V]^G \oplus ker(\pi_H^G)$.
(4) Si f está en $k[V]^G$ y h en $k[V]^H$ no es constante, entonces

$$Tr_H^G(f) = |G : H|f$$
$$Tr_H^G(f \cdot h) = f \cdot Tr_H^G(h).$$

Por lo tanto, si $|G : H|$ es invertible en k, entonces π_H^G es un morfismo de $k[V]^G$-módulos (la estructura de $k[V]^G$-módulo de $k[V]^H$ es la que proviene de la inclusión $k[V]^G \subset k[V]^H$).

Un resultado previo antes de encarar el tema principal de esta sección. Ver [**8**], pp. 29 para su demostración.

LEMA 4.42. *Sea V un espacio vectorial sobre el cuerpo k, y sean $u_1, \dots, u_j$ en $k[V]$. Si $j!$ es inversible en k, entonces el monomio $u_1 \dots u_j$ se puede escribir como combinación lineal de sumas elevadas a la potencia j de elementos de $\{u_1, \dots, u_j\}$. Mas aún*

$$(-1)^j j! u_1 \dots u_j = \sum_{I \subset \{1,\dots,j\}} (-1)^{|I|} \left(\sum_{i \in I} u_i \right)^j,$$

donde I varía en todos los subconjuntos de $\{1, \dots, j\}$, $|I|$ es el cardinal de I.

TEOREMA 4.43. *(Noether). Sean G un grupo finito, H un subgrupo de G y V un G-módulo de dimensión finita sobre el cuerpo k. Si $|G : H|!$ es inversible en k y $k[V]^H$ es generado por elementos de grado a lo sumo m, entonces $k[V]^G$ es generado por elementos de grado a lo sumo $m \cdot |G : H|$.*

DEMOSTRACIÓN. Se denota por d a $|G : H|$. Sea B la subálgebra de $k[V]^G$ generada por todos los elementos de grado a lo sumo md. Se probará que $B = k[V]^G$. Sea N el subespacio vectorial de $k[V]^H$ generado por los elementos de $k[V]^H$ de grado a lo sumo m, y sea M el subespacio de $k[V]^H$ generado por $\{f_1^{e_1} \dots f_k^{e_k} \colon k, e_1, \dots, e_k \in \mathbb{N}, e_1 + \dots + e_n < d; f_1, \dots, f_k \in N\}$.

Afirmación: M genera a $k[V]^H$ como B-módulo. Es decir, $B \cdot M = k[V]^H$.

Dada f en $k[V]^H$, es raíz del polinomio

$$\prod_{gH \in G/H} (x - gf),$$

donde el producto se toma sobre una familia de representantes de coclases de H en G. Este polinomio se escribe de la forma

$$\prod_{gH \in G/H} (x - gf) = x^d + b_1 x^{d-1} + \dots + b_d,$$

donde b_i es el valor que toma la i-ésima función simétrica elemental en d variables cuando es evaluada en los d elementos de $\{gf\colon g \in G/H\}$. Entonces, se tiene

$$f^d = -(b_1 f^{d-1} + \cdots + b_d). \tag{5.1}$$

Parte 1: si f tiene grado a lo sumo m, entonces

$$deg(b_1) \leq deg(b_2) \leq \cdots \leq deg(b_d) \leq dm,$$

y por lo tanto $b_1, \ldots, b_d$ están en B. Como $f, f^2, \ldots, f^{d-1}$ están en M, por *(4.1)* se sigue que $f \in B \cdot M$, y esto para toda $f \in N$.

Parte 2: si f^E denota a un monomio $f^E = f_1^{e_1} \ldots f_k^{e_k}$ con $f_1, \ldots, f_k$ en N y $e_1 + \cdots + e_k = d$, por el lema anterior se tiene

$$(-1)^d d! f^E = \sum_{I \subset \{1,\ldots,j\}} (-1)^{|I|} \left(\sum_{i \in I} f_i \right)^d = \sum_{I \subset \{1,\ldots,j\}} (-1)^{|I|} h_I^d, \tag{5.2}$$

donde los h_I están en N. Como $d!$ es inversible en k, se sigue que $f^E \in B \cdot M$.

Éste fue el caso base del siguiente razonamiento inductivo.

Parte 3: Supóngase que todos los monomios $f^E = f_1^{e_1} \ldots f_k^{e_k}$ para algunos $k, e_1, \ldots, e_k \in \mathbb{N}$, $f_1, \ldots, f_k$ en N y $e_1 + \cdots + e_k \leq d + i$ están en $B \cdot M$. Se considera un monomio $f^E = f_1^{e_1} \ldots f_k^{e_k}$ con $k, e_1, \ldots, e_k \in \mathbb{N}$, $f_1, \ldots, f_k$ en N y $e_1 + \cdots + e_k = d + i + 1$. Se asume sin pérdida de generalidad que $f^E = f^{E'} f_k$. Por hipótesis inductiva, se tiene $f^{E'} \in B \cdot M$, y por lo tanto existen $h_1, \ldots, h_l \in N$, $d_1, \ldots, d_l \in \mathbb{N}$ con $d_1 + \cdots + d_l < d$ y $c_D \in B$ tales que

$$f^{E'} = \sum c_D h^D = \sum_{|D| < d-1} c_D h^D + \sum_{|D| = d-1} c_D h^D,$$

donde

$$h^D \coloneqq \prod_{i=1}^{l} h_i^{d_i}.$$

Si $|D| < d-1$, entonces $h^D f_k \in M$ porque el grado de sus términos no supera d, y por lo tanto

$$\sum_{|D| < d-1} c_D h^D f_k \in B \cdot M.$$

Si $|D| = d-1$, entonces por la ecuación *(4.2)* $h^D f_k \in B \cdot M$, y por lo tanto

$$\sum_{|D| = d-1} c_D h^D f_k \in B \cdot M.$$

Combinando estos dos casos,

$$f^E = f^{E'} f_k = \sum c_D h^D f_k = \sum_{|D| < d-1} c_D h^D f_k + \sum_{|D| = d-1} c_D h^D f_k \in B \cdot M.$$

Por lo tanto, por inducción, todo monomio $f^E = f_1^{e_1} \dots f_k^{e_k}$ con $f_1, \dots f_k \in N$ pertenece a $B \cdot M$. Como N genera al álgebra $k[V]^H$, esto prueba la afirmación.

Ahora sólo resta usar la proyección π_H^G. Como la característica de k es coprima con $|G : H|$, se sabe que π_H^G es un morfismo suryectivo de $k[V]^G$-módulos. Por lo tanto, usando que $\pi_H^G(M) \subset B$,

$$k[V]^G = \pi_H^G(k[V]^H) = \pi_H^G(B \cdot M) = B \cdot \pi_H^G(M) = B.$$

□

Aplicando el resultado anterior al subgrupo trivial $H = \{e\}$, se tiene

COROLARIO 4.44. *(Noether) Sean G un grupo finito, y V un G-módulo de dimensión finita sobre el cuerpo k. Si $|G|!$ es inversible en k (es decir, k tiene característica cero o mayor que $|G|$), entonces $k[V]^G$ es generado por elementos de grado a lo sumo $\binom{dim_k(V)+|G|}{|G|}$.*

Si la característica del cuerpo no divide a $|G|$, la prueba del último teorema de Noether adaptada al caso que se trata en el corolario anterior proporciona un algoritmo para calcular un sistema de generadores del álgebra de invariantes:

(1) Exhibir una base de los polinomios de grado a lo sumo $|G|$.
(2) Aplicar a esa base la proyección π^G.
(3) Los polinomios resultantes están en $k[V]^G$ y la generan como álgebra.

En el siguiente ejemplo se ilustran estos pasos.

EJEMPLO 4.45. El grupo cíclico de orden 3 actúa en k^3 permutando cíclicamente los vectores de la base canónica E_1, E_2, E_3. El subespacio de k^3 formado por los (a, b, c) tales que $a + b + c = 0$ es invariante por esta acción de $\mathbb{Z}_3$. Se fija para ese subespacio la base $E_1 - E_2, E_3 - E_2$. En esa base, la matriz del generador de $\mathbb{Z}_3$ es

$$A \coloneqq \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \in GL(2, k).$$

Ahora, si $\{x, y\}$ es la base dual de V^*, se tienen las siguientes bases para las componentes homogéneas de $k[x, y]$ de grados 1, 2 y 3 respectivamente:

$$x, y \in S^1(V^*)$$
$$x^2, xy, y^2 \in S^2(V^*)$$
$$x^3, x^2y, xy^2, y^3 \in S^3(V^*).$$

La acción de A en V^* está dada por

$$Ax = -y$$
$$Ay = x - y$$

Por la prueba del teorema de Noether, se puede obtener una familia de generadores de $k[x, y]^{\mathbb{Z}_3}$ aplicando la proyección

$$\pi^{\mathbb{Z}_3} \colon k[x, y] \to k[x, y]^{\mathbb{Z}_3}$$

a esos 9 polinomios que forman una base de los polinomios de grado a lo sumo 3. Esos valores se resumen en la siguiente tabla

ψ	$\pi^{\mathbb{Z}_3}(\psi)$
x	0
y	0
x^2	$\frac{1}{3}(2x^2 - 2xy + 2y^2)$
xy	$\frac{1}{3}(x^2 - xy + y^2)$
y^2	$\frac{1}{3}(2x^2 - 2xy + 2y^2)$
x^3	$x^2y - xy^2$
x^2y	$\frac{1}{3}(-x^3 + 3x^2y - y^3)$
xy^2	$\frac{1}{3}(-x^3 + 3xy^2 - y^3)$
y^3	$-x^2y + xy^2$

Y de esta tabla se deduce que los polinomios

$$\begin{aligned} f &= x^2 - xy + y^2 \\ g &= x^2y - xy^2 \\ h &= x^3 - 3xy^3 + y^3 \end{aligned}$$

son un sistema de generadores del álgebra de invariantes $k[x, y]^{\mathbb{Z}_3}$. Notar que g y h tienen grado 3, justo el máximo posible con este método.

Bibliografía

[1] Atiyah, Michael; MacDonald, Ian. *"Introduction to Commutative Algebra",* Addison-Wesley, 1969.

[2] Benson, David. *"Polynomial Invariants of Finite Groups",* London Mathematical Society Lecture Notes Series 190, Cambridge University Press, 1993.

[3] Dieuddoné, Jean; Carrell, James. *"Invariant Theory Old and New",* Advances in Mathematics, Academic Press, Vol.4, 1970.

[4] Dummit, David; Foote, Richard. *.ᴬbstract Algebra",* Third edition, Wiley, 2004.

[5] Eisenbud, David. *Çommutative Algebra with a View Toward Algebraic Geometry",* Graduate Texts in Mathematics, Springer, 1995.

[6] Hartshorne, Robin. *"Algebraic Geometry",* Graduate Texts in Mathematics, Springer, 1997.

[7] Serre, Jean-Pierre. *"Linear Representations of Finite Groups",* Graduate Texts in Mathematics, Springer, 1977.

[8] Smith, Larry. *"Polynomial Invariants of Finite Groups",* Research Notes in Mathematics, Vol.6, A. K. Peters, 1995.

[9] Smith, Larry. *"Polynomial Invariants of Finite Groups. A Survey of Recent Developments",* Bulletin of the American Mathematical Society, Vol.34, Number 3, pp 211-250, July 1997.