UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMATICA

SECCIÓN DE MATEMÁTICA

INFORME FINAL DEL CURSO DE ESPECIALIZACIÓN:

VARIEDADES TORICAS Y ACCIONES DE GRUPOS ALGEBRAICOS

TÍTULO DEL INFORME FINAL:

ÁLGEBRA DE INVARIANTES FINITAMENTE GENERADOS BAJO ACCIONES DE GRUPOS FINITOS

PARA OPTAR AL GRADO ACADÉMICO DE:

LICENCIATURA EN MATEMÁTICA

PRESENTADO POR:

JENNIFER ALEXANDRA LÓPEZ HERNÁNDEZ N° CARNET LH17017
YONY ALEXANDER GUEVARA REYES N° CARNET GR15040

DOCENTE ASESOR:

DR. TOBIAS HUMBERTO MARTÍNEZ LOVO

SEPTIEMBRE DE 2025

SAN MIGUEL, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES

M.SC. JUAN ROSA QUINTANILLA

RECTOR

DRA. EVELYN BEATRIZ FARFÁN

VICERRECTORA ACADÉMICA

M.SC. ROGER ARIAS

VICERRECTOR ADMINISTRATIVO

LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA

SECRETARIO GENERAL

LIC. CARLOS AMÍLCAR SERRANO RIVERA

FISCAL

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

AUTORIDADES

M.SC. CARLOS IVÁN HERNÁNDEZ FRANCO

DECANO

DRA. NORMA AZUCENA FLORES RETANA

VICEDECANA

LIC. CARLOS DE JESÚS SÁNCHEZ

SECRETARIO

ING. DOLORES BENEDICTO SARAVIA MARTÍNEZ

JEFE DEL DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

LIC. SONIA DEL CARMEN MARTÍNEZ DE LÓPEZ

COORDINADORA DEL PROCESO DE GRADO DEL DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

Índice general

Resumen

En este trabajo se presenta un estudio sobre las acciones de grupos finitos sobre k-álgebras finitamente generadas. Tomando temas fundamentales como lo son acciones de grupos, k-algebras, anillos y módulos noetherianos así mismo como el teorema de la base de Hilbert. Posteriormente se estudia la teoría de álgebra de invarinates analizando propiedades básicas y ejemplos de la misma. El resultado central, muestra que si un grupo finito actúa mediante automorfismos sobre una k-álegbra finitamente generada entonces el subanillo de invariantes también es finitamente generado.

Palabras clave: Grupos finitos, k-álgebras finitamnete generadas, Acciones de grupos, Anillos y Modulos Noetherianos, Teorema de la base de Hilbert, Teoría de álgebra de invariantes, Subanillos de invariantes.

Abstract

This work presents a study on the actions of finite groups on finitely generated k-algebras. It covers fundamental topics such as group actions, k-algebras, Noetherian rings and modules, as well as Hilbert's basis theorem. Subsequently, the theory of invariant algebra is studied, analyzing its basic properties and examples. The central result shows that if a finite group acts by automorphisms on a finitely generated k-algebra, then the subring of invariants is also finitely generated.

Keywords: Finite groups,initely generated k-algebras,Group actions, Noetherian rings and modules, Hilbert's basis theorem, Invariant algebra theory, Subring of invariants.

1. Introducción

El desarrollo del álgebra moderna ha estado profundamente influenciado por el estudio de las acciones de grupos y su interacción con diversas estructuras algebraicas, tales como anillos, módulos y espacios vectoriales. Una de las áreas donde esta interacción adquiere especial relevancia es el *álgebra de invariantes*, cuyo propósito es comprender cómo ciertos elementos permanecen fijos bajo la acción de grupos. Este campo, iniciado con las preguntas planteadas por Hilbert a finales del siglo XIX, ha evolucionado hasta convertirse en una herramienta central tanto en el álgebra conmutativa como en la geometría algebraica.

El problema de la *finita generabilidad de los invariantes* surge de manera natural en este contexto. Dado un grupo G actuando sobre una k-álgebra A, interesa determinar si el subanillo de invariantes A^G conserva la propiedad de ser finitamente generado. Esta cuestión, que conecta directamente con el Problema XIV de Hilbert, no solo es de interés teórico, sino que también tiene implicaciones en la comprensión de espacios afines, variedades algebraicas y cocientes geométricos.

En este trabajo se abordan los fundamentos necesarios para construir dicho marco teórico. En primer lugar, se revisan los conceptos básicos de acciones de grupos, destacando su correspondencia con homomorfismos hacia grupos de permutaciones. Posteriormente, se introducen las *k-álgebras* y el caso particular de las álgebras finitamente generadas, cuya estructura permite representar sistemas algebraicos a partir de un número finito de generadores. A continuación, se examina el papel de los anillos y módulos noetherianos, cuya relevancia radica en controlar el crecimiento de ideales y submódulos, garantizando condiciones de finitud en contextos generales. Estos resultados culminan en la exposición del Teorema de la base de Hilbert, piedra angular para demostrar la finita generabilidad en diferentes entornos.

Finalmente, se estudia con detalle la teoría del álgebra de invariantes, analizando propiedades esenciales, ejemplos ilustrativos y resultados clásicos como los invariantes simétricos bajo la acción de grupos finitos. El aporte central de este trabajo consiste en demostrar que, cuando un grupo finito actúa mediante automorfismos sobre una k-álgebra finitamente generada, el subanillo de invariantes A^G también es finitamente generado. Este resultado confirma la estabilidad de la finitud bajo acciones de grupos finitos y refuerza la importancia de la teoría en el marco del álgebra conmutativa y la geometría algebraica contemporánea.

2. Acciones de Grupos

En esta sección se estudiará sobre acciones de grupos la cual es una herramienta fundamnetal para poder relacionar grupos con diversos objetos como anillos, espacios vectoriales, conjuntos etc.

Definición 1. *Una acción de grupo de un grupo G sobre un conjuto A es una función de $G \times A \to A$, cuya imagen se denota $g \cdot a$ con $g \in G \quad y \quad a \in A$ que satisfacen las siguientes propiedades:*

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ *para todo* $g_1, g_2 \in G, \quad a \in A$
2. $1 \cdot a = a$ *para todo* $a \in A$

Proposición 1. *Para cualquier grupo G y conjunto no vacío A, hay una biyección entre acciones de G sobre A y homomorfismos $\phi : G \to Sym(A)$.*

Demostración. Supongamos que G actúa sobre A, es decir, tenemos una aplicación

$$\cdot : G \times A \to A, \quad (g, a) \mapsto g \cdot a$$

que satisface:

1. $e \cdot a = a$ para todo $a \in A$;
2. $(gh) \cdot a = g \cdot (h \cdot a)$ para todos $g, h \in G$ y $a \in A$.

Para cada $g \in G$ definimos la aplicación $\sigma_g : A \to A$ por

$$\sigma_g(a) := g \cdot a.$$

Entonces σ_g es biyectiva, con inversa $\sigma_{g^{-1}}$, pues

$$\sigma_{g^{-1}}\big(\sigma_g(a)\big) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = e \cdot a = a,$$

y análogamente $\sigma_g \circ \sigma_{g^{-1}} = \mathrm{id}_A$. Por lo tanto $\sigma_g \in \mathrm{Sym}(A)$.
Definimos

$$\phi : G \to \mathrm{Sym}(A), \quad \phi(g) := \sigma_g.$$

Para $g, h \in G$ y $a \in A$,

$$\phi(gh)(a) = (gh) \cdot a = g \cdot (h \cdot a) = \sigma_g\big(\sigma_h(a)\big) = (\sigma_g \circ \sigma_h)(a),$$

lo que implica que $\phi(gh) = \phi(g)\phi(h)$. Además $\phi(e) = \mathrm{id}_A$. Así, ϕ es un homomorfismo.

Recíprocamente, dado un homomorfismo $\phi : G \to \mathrm{Sym}(A)$, definimos

$$g \cdot a := \phi(g)(a), \quad g \in G,\ a \in A.$$

Entonces:

1. $e \cdot a = \phi(e)(a) = \mathrm{id}_A(a) = a$;
2. $(gh) \cdot a = \phi(gh)(a) = \phi(g)\phi(h)(a) = \phi(g)\big(\phi(h)(a)\big) = g \cdot (h \cdot a)$.

Por lo tanto, esto define una acción de G sobre A.

Si partimos de una acción, construimos ϕ como en (1) y luego definimos la acción correspondiente mediante (2), obtenemos la misma acción original. Si partimos de un homomorfismo y luego definimos una acción como en (2) para después obtener $\tilde{\phi}$ como en (1), resulta que $\tilde{\phi} = \phi$.
Esto prueba que las correspondencias son inversas y, por tanto, existe una biyección entre el conjunto de acciones de G sobre A y $\mathrm{Hom}(G, \mathrm{Sym}(A))$. □

Ejemplo 1. *Para cualquier conjunto no vacio A el grupo simetrico S_A actua sobreA mediante $\sigma \cdot a = \sigma(a)$ para todo $\sigma \in S_A$ $a \in A$. La representación de permutación es la función identidad S_A sobre si misma.*

Ejemplo 2. *Sea G un grupo cualquiera y sea $A = G$. Definamos una función de $G \times A$ a A mediante $g \cdot a = ga$ para cualquier $g \in G$ y $a \in A$ dónde ga en el lado derecho es el producto de g y a en el grupo G. Esto da una acción de grupo G sobre si misma donde cada $g \in G$*

Ejemplo 3. *Sea $ga = a$ para todo $g \in G$ $a \in A$. Esta acción se denomina acción trivial y se dice que G actúa trivialmente sobre A. Nótese que distintos elementos de G inducen la misma permutación sobre A*
La representación de la permutación asociada

$$G \longrightarrow S_A$$

Para profundisar más sobre este tema ver ([1], capítulo 1,seccion 1.7, pag 41)

3. k-Álgebras

Las k-álgebras son estructuras algebraicas que combinan las propiedades de un anillo con unidad y de un espacio vectorial sobre un cuerpo k. Este concepto permite extender operaciones algebraicas dentro de un contexto más general, útil tanto en álgebra como en geometría. En particular, las K-álgebras finitas, es decir, aquellas de dimensión finita como espacios vectoriales, presentan una rica estructura interna. Su estudio incluye la clasificación, los homomorfismos y la descomposición en álgebras locales. Además, ciertos ejemplos clásicos sobre $\mathbb{R}$ revelan conexiones con geometrías fundamentales del plano.

Definición 2. *Sea k un cuerpo. Una k-álgebra A con unidad es un par $(A, +, \cdot)$ que cumple las siguientes condiciones:*

- *Es un anillo con unidad.*
- *Es un k-espacio vectorial.*
- *Para todo $\alpha \in k$ y para todos $a, b \in A$, se cumple que:*

$$\alpha(ab) = (\alpha a)b = a(\alpha b)$$

Decimos que A es una k-álgebra finita si es una k-álgebra conmutativa con unidad y de dimensión finita como k-espacio vectorial. Denotaremos por $\dim_k A$ a su dimensión como k-espacio vectorial.

Definición 3. *Un homomorfismo de k-álgebras es una aplicación lineal*

$$\varphi : A \to B$$

entre dos k-álgebras tal que:

$$\varphi(1_A) = 1_B \quad y \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \textit{para todo } a, b \in A.$$

El homomorfismo estructural es el siguiente:

$$k \to A, \quad 1_k \mapsto 1_A$$

Es inyectivo, ya que k es un cuerpo. Por lo tanto, 1_k es parte libre en el k-espacio vectorial A, y se puede extender $\{1_A\}$ a una base de A.

Si $\dim_k A = 2$, tomamos $\gamma \in A \setminus k$, entonces $\{1_A, \gamma\}$ es parte libre en A y, por tanto, $\{1_A, \gamma\}$ es una base del k-espacio vectorial A.
Además, como $1 \cdot \gamma = \gamma \cdot 1$, se tiene que el anillo A es conmutativo. Sin embargo, para dimensiones superiores, las k-álgebras no son necesariamente conmutativas.
Existen, salvo isomorfismos, tres álgebras de dimensión 2 sobre $\mathbb{R}$:

- $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$
- $\mathbb{P} = \mathbb{R}[x]/(x^2 - 1)$
- $\mathbb{D} = \mathbb{R}[x]/(x^2)$

Esto se debe a que, en una extensión de grado 2 de $\mathbb{R}$,

$$A = \mathbb{R}[x]/(x^2 + bx + c),$$

se pueden dar tres casos, según si el polinomio $x^2 + bx + c$ tiene dos raíces imaginarias, dos raíces reales distintas o una raíz doble. Los conjuntos $\mathbb{C}$, $\mathbb{P}$ y $\mathbb{D}$ son, respectivamente, los números complejos, los números paracomplejos y los números duales.
Para más detalles sobre k-álgebras ver ([2] capítulo 1, pag. 32)

Ejemplos de k-Álgebras

Ejemplo 4. *Un anillo conmutativo que contiene a k, cómo una extensión de cuerpo, el anillo de polinomios $k[X, Y]$, o la serie de potencias formales $k[[X]]$, es una k-álgebra.*

Ejemplo 5. *El anillo $M_d(k)$, bajo la suma y multiplicación de matrices, es una k-álgebra. Esto se llama un* álgebra de matrices sobre k.

Ejemplo 6. *El anillo de grupo $k[G]$, para un grupo finito G, es una k-álgebra.*

Ejemplo 7. *El conjunto* $\mathrm{Hom}_k(V, V)$ *de aplicaciones k-lineales de un espacio vectorial k-vectorial V en sí mismo, es una k-álgebra bajo la suma y la composición de aplicaciones lineales.*

4. k-Álgebras finitamente generadas

Se estudiara un caso importante dentro de las k-álgebras, como lo es las k-álgebras finitamente generadas. Son aquellas que pueden construirse mediante de un número

finito de elementos, a partir operaciones como suma, multiplicación por escalar k y producto, es decir toda estructura esta determinada por un conjunto finito de generadores.

Definición 4. *Decimos que A es una k-**álgebra finitamente generada** si existen elementos $a_1, a_2, \ldots, a_n \in A$ tales que*

$$A = k[a_1, a_2, \ldots, a_n],$$

donde $k[a_1, a_2, \ldots, a_n]$ denota la subálgebra de A generada por k y los elementos $a_1, \ldots, a_n$. Equivalente y más constructivamente,

$$A \cong k[x_1, x_2, \ldots, x_n]/I,$$

para algún ideal $I \subseteq k[x_1, \ldots, x_n]$.
En otras palabras, toda k-álgebra finitamente generada puede obtenerse como un cociente de un álgebra de polinomios en un número finito de variables sobre k.

Ejemplo 8. *Si k es un campo y A es una k-álgebra no trivial es decir $A \neq 0$, el morfismo de $k \to A$ es inyectivo y así se puede identificar a k como su imagen en A y pensar que k es un subanillo de A.*

5. Anillos Noetherianos

En está sección veremos un poco acerca de los anillos Noetherianos, el cual en el álgebra es un concepto fundamental, su nombre es en honor a Emmy Noether quien fue una pionera en álgebra moderna.
La noción de los que es un anillo noetheriano que controla el creciemiento de ideales dentro de un anillo. De manera formal un anillo se dice noetheriano si todo ideal es finitamente generado.
Ahora daremos una definión más formal.

Definición 5. *Un anillo A es noetheriano sí todos sus ideales son finitamente generados.*

Proposición 2. *Sí A es un anillo son equivalentes:*

1. *A es noetheriano*
2. *Toda cadena ascendente de ideales propios*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

se estaciona es decir existe un entorno m tal que $I_m = I_{m+1} = \ldots$

3. *Todo conjunto no vacio de ideales propios A tiene un elemento máximo es decir un ideal que no esta contenido en ninguno de los ideales de la familia dada.*

Demostración. **(1) ⇒ (2).** Sea

$$I_1 \subseteq I_2 \subseteq \cdots$$

una cadena ascendente de ideales. Considere $I := \bigcup_{n\geq 1} I_n$, que es un ideal de A. Cómo A es noetheriano, I es finitamente generado: existen $a_1, \ldots, a_r \in I$ tales que $I = (a_1, \ldots, a_r)$. Para cada i hay n_i con $a_i \in I_{n_i}$. Tome $m = \text{máx}\{n_1, \ldots, n_r\}$. Entonces $a_1, \ldots, a_r \in I_m$, de modo que

$$I = (a_1, \ldots, a_r) \subseteq I_m \subseteq I,$$

y por tanto $I = I_m$. De la inclusión $I_m \subseteq I_{m+1} \subseteq I$ se deduce $I_{m+1} = I$, y por inducción $I_k = I$ para todo $k \geq m$. La cadena se estaciona.

(2) ⇒ (3). Sea $\mathcal{F}$ un conjunto no vacío de ideales propios de A. Supongamos que $\mathcal{F}$ no tiene elementos máximos. Elija $I_1 \in \mathcal{F}$. Cómo no es máximo, existe $I_2 \in \mathcal{F}$ con $I_1 \subsetneq I_2$. De nuevo, I_2 no es máximo, así que hay $I_3 \in \mathcal{F}$ con $I_2 \subsetneq I_3$, y así sucesivamente. Esto construye una cadena estrictamente ascendente de ideales propios que, por hipótesis (2), debería estacionarse, contradicción. Por lo tanto, $\mathcal{F}$ debe tener un elemento máximo.

(3) ⇒ (1). Sea I un ideal de A. Consideremos

$$\mathcal{S} := \{\, J \subseteq I : J \text{ es un ideal finitamente generado} \,\}.$$

Observamos que $\mathcal{S}$ es no vacío (contiene al ideal cero). Por (3) aplicado al conjunto de ideales propios de I (o directamente a $\mathcal{S}$, ordenado por inclusión), existe $J \in \mathcal{S}$ maximal por inclusión. Afirmamos que $J = I$. En efecto, si $J \neq I$, existe $x \in I \setminus J$ y entonces $J' := J + (x)$ es un ideal de I que contiene propiamente a J; pero J' es finitamente generado (si $J = (a_1, \ldots, a_r)$, entonces $J' = (a_1, \ldots, a_r, x)$), contradiciendo la maximalidad de J en $\mathcal{S}$. Luego $I = J$ es finitamente generado. Cómo I fue arbitrario, todo ideal de A es finitamente generado, es decir, A es noetheriano.

Hemos probado (1)⇒(2)⇒(3)⇒(1), y por tanto las tres condiciones son equivalentes. □

Teorema 1. *Teorema de la base de Hilbert: Si A es un anillo noetheriano entonces $A[x]$ también lo es. En particulas si Kes un campo entonces el anillo de polinomios $K[x_1, .., x_n]$ es noetheriano.*

Demostración. Para ver una demostración (ver [4], teorema 4.2 pag. 86) □

Ejemplo 9. *Si k un campo los unicos ideales en k son (0) y (1)=k por lo que k es noetheriano*

Ejemplo 10. *Si R es un PID, entonces R es noetheriano. Todo ideal se genera finitamente.*

Ejemplo 11. *Un anillo que no es noetheriano es un anillo de polinomial en un numero infinito de variables sobre un campo K. La cadena ascendente de ideales* $(x_1) \subseteq (, x_1x_2) \subseteq (x_1, x_2, x_3) \subseteq \ldots$ *no se estabiliza.*

Para ver más ejemplos sobre anillos noeterianos ver ([5], capítulo 1, sección 1.3, pag. 10)

6. Módulos Noetherianos

En esta sección se analizará en qué casos la propiedad de un módulo de ser finitamente generado puede ser hereditaria; es decir, en qué circunstancias los submódulos de un módulo finitamente generado también son finitamente generados. Para motivar el estudio y evidenciar que no se trata de una cuestión trivial, se considerará el siguiente ejemplo. Sea $A = \mathbb{R}^{[0,1]} = \{f : [0,1] \to \mathbb{R}\}$, con la estructura usual de anillo de funciones, esto es:

$$\forall x \in [0,1],\ f, g \in \mathbb{R}^{[0,1]} :$$

$$(f+g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Sea $M = \mathbb{R}^{[0,1]}$ y

$$S = \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; f(x) \neq 0 \text{ sólo para una cantidad finita de valores } x \right\}.$$

El conjunto S es un ideal de M. En efecto, si considero

$$(f \cdot g)(x) = f(x) \cdot g(x), \quad f \in S,\ g \in M,$$

entonces $f \cdot g$ será distinta de cero a lo sumo en los finitos x_i donde lo era f. Luego, S es un A-submódulo de M.

El módulo M está generado por la función constante 1, pero S no es un A-módulo finitamente generado. Para ver esto, consideremos $f_1, \ldots, f_n \in S$ tales que

$$\langle f_1, \ldots, f_n \rangle = S,$$

y sea $\{x_1, \ldots, x_s\} \subset [0,1]$ la unión de todos los puntos x tales que existe alguna f_i con $f_i(x) \neq 0$ (el cual es finito).
Sea $x_0 \in [0,1] \setminus \{x_1, \ldots, x_s\}$. Si definimos $\varphi : [0,1] \to \mathbb{R}$ dada por

$$\varphi(x) = \begin{cases} 1, & \text{si } x = x_0, \\ 0, & \text{si } x \neq x_0, \end{cases}$$

entonces $\varphi \in S$, pero φ nunca puede pertenecer a $\langle f_1, \ldots, f_n \rangle$, pues
$x_0 \in [0,1] \setminus \{x_1, \ldots, x_s\}$.

Proposición 3. *Sea A un anillo y M un A-módulo. Son equivalentes:*

1. *Todo conjunto no vacío de submódulos de M tiene un elemento maximal.*
2. *Toda sucesión (no vacía) creciente de submódulos se estaciona.*

Demostración. Para una demostración (ver [6], proposición 2.3, pag. 6) □

Definición 6. *Sea M un A-módulo, se dice noetheriano si cumple al menos una de las dos propiedades anteriores de la Proposición 3.*

Ejemplo 12. *Los A-módulos con un número finito de submódulos son noetherianos, por la proposición anterior, ya que cualquier sucesión no vacía de submódulos creciente se estaciona dado que es finita.*

Ejemplo 13. *Dado un cuerpo K, un espacio vectorial V es noetheriano si y sólo si $\dim_K(V) < \infty$. Esto se ve también con la proposición anterior, dado que cualquier cadena de subespacios creciente se estaciona porque la base es finita.*

Por otro lado, los submódulos del cociente M/S están en correspondencia con los submódulos de M que contienen a S. Por lo tanto, un cociente de un módulo noetheriano también es noetheriano.

Proposición 4. *Sea A un anillo noetheriano y M un A-módulo de tipo finito, entonces M es noetheriano.*

Demostración. Como M es de tipo finito existen $m_1, ..., m_n \in M$ que lo generan como un A-módulo. Ahora definimos un homomorfismo de A-módulos

$$f : A^n \to M \text{ para algún } \quad n \in \mathbb{N}$$

Este mapa es sobreyectivo, es decir es un epimorfismo.

Como A es noetheriano cómo anillo, lo es también cómo A-módulo sobre si mismo. Además la suma directa finita de módulos noetheriano es noetheriana por lo que

$$A^n : \bigoplus_{i=1}^{n} A$$

y A es un A-módulo noetheriano.
Finalmente ser noetheriano se preserva por sumas directas finitas, luego A^n es noetheriano y cómo f es un epimorsmo, M es noetheriano. □

Ejemplo 14. *Sea $d \in \mathbb{Z}$ un número que no es cuadrado, $\sqrt{d}$ una raíz compleja de d, y sea*

$$\mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Z} \right\}.$$

Este subconjunto de $\mathbb{C}$ es, de hecho, un subanillo de $\mathbb{C}$. En efecto, si

$$\alpha = a + b\sqrt{d}, \quad \beta = a' + b'\sqrt{d},$$

entonces al multiplicar se obtiene:

$$\alpha \cdot \beta = (a + b\sqrt{d})(a' + b'\sqrt{d}) = aa' + (ab' + ba')\sqrt{d} + bb'd.$$

Cómo $d \in \mathbb{Z}$, se concluye que $\alpha \cdot \beta \in \mathbb{Z}[\sqrt{d}]$, por lo tanto, $\mathbb{Z}[\sqrt{d}]$ es un subanillo de $\mathbb{C}$. Por otro lado, existe un epimorfismo de anillos

$$Z[x] \longrightarrow \mathbb{Z}[\sqrt{d}]$$

determinado por $x \mapsto \sqrt{d}$. Como $\mathbb{Z}$ es noetheriano, entonces $\mathbb{Z}[x]$ también lo es, y al ser $\mathbb{Z}[\sqrt{d}]$ cociente de un anillo noetheriano, se concluye que $\mathbb{Z}[\sqrt{d}]$ es un anillo noetheriano.

Definición 7. *[7] Sea A un anillo y sea G un grupo que actúa sobre A mediante automorfismos de anillo. El* ***subanillo de invariantes*** *de A bajo la acción de G se denota por*

$$A^G = \{\, a \in A \mid g \cdot a = a \;\; \text{para todo } g \in G \,\}.$$

7. Subanillo de Ivariantes

Proposición 5 (**Propiedades del subanillo de invariantes**). *[8] Sea A un anillo conmutativo y G un grupo que actúa sobre A por automorfismos de anillo. Denotemos*

$A^G = \{\, a \in A : g \cdot a = a \ \forall g \in G \,\}$.

1. A^G ***es un subanillo unitario de*** A**.**

   Demostración. Si $a, b \in A^G$, entonces para todo $g \in G$ se tiene $g \cdot (a \pm b) = (g \cdot a) \pm (g \cdot b) = a \pm b$ y $g \cdot (ab) = (g \cdot a)(g \cdot b) = ab$. Además $1 \in A^G$. □

2. ***Caracterización:*** *los elementos de* A^G *son exactamente los fijos por la acción.*

   Demostración. Es tautológico por la definición de A^G. □

3. ***Cociente afín:*** *si* $X = \mathrm{Spec}(A)$*, la inclusión* $A^G \hookrightarrow A$ *induce un morfismo*

   $$\pi : X \to X/\!/G := \mathrm{Spec}(A^G)$$

   llamado cociente afín*.*

   Demostración. Todo morfismo de anillos induce un morfismo de esquemas contravariante; aquí usamos la inclusión $A^G \hookrightarrow A$. □

   Definición 8 (**Elemento integral**)**.** *Sea* A *un anillo conmutativo con unidad y* B *una* A*-álgebra. Un elemento* $b \in B$ *se dice* ***integral sobre*** A *si existe un polinomio mónico*

   $$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0,$$

   con coeficientes $a_i \in A$*.*

4. ***Integralidad para acciones finitas:*** *si* G *es finito, entonces* A *es integral sobre* A^G*.*

   Demostración. Fijado $a \in A$, consideramos el polinomio

   $$P(T) = \prod_{g \in G} \big(T - g \cdot a\big) \in A[T].$$

   Sus coeficientes son polinomios simétricos en el conjunto $\{\, g \cdot a : \ g \in G \,\}$, por tanto son invariantes bajo G y pertenecen a A^G. Además P es mónico y $P(a) = 0$. Así, cada $a \in A$ es integral sobre A^G. □

5. ***Finita generación (Hilbert) para grupos linealmente reductivos:*** *si* $A = k[x_1, \ldots, x_n]$ *y* $G \subset \mathrm{GL}_n(k)$ *es linealmente reductivo, entonces* A^G *es de tipo finito sobre* k.

   Demostración. Se gradúa A y se considera el ideal homogéneo J generado por invariantes de grado positivo; una vez que J es finitamente generado, la reductividad lineal asegura que los generadores de J bastan para generar el anillo de invariantes por inducción en el grado. □

6. ***Separación de órbitas cerradas y sobreyectividad de*** π***:*** *si* $x, y \in X$ *tienen órbitas* $G \cdot x$ *y* $G \cdot y$ *cerradas y disjuntas, existe* $f \in A^G$ *con* $f(x) \neq f(y)$*; además,* π *es sobreyectiva y establece biyección entre órbitas cerradas y puntos de* $X/\!/G$.

   Demostración. La aplicación cociente afín π identifica cada órbita con la clausura-equivalencia correspondiente; las órbitas cerradas forman exactamente una sección de fibras, y los invariantes separan sus clases. □

7. ***Fracciones e invariantes:*** *Sea* A *un dominio con cuerpo de fracciones* $K = \mathrm{Frac}(A)$. *Siempre se tiene la inclusión*

$$\mathrm{Frac}(A^G) \subseteq K^G.$$

   Si, además, G *es finito (y* A *es dominio), entonces* $\mathrm{Frac}(A^G) = K^G$.

   Demostración. La inclusión es inmediata de la definición. Si G es finito, la integralidad de A/A^G implica que toda fracción en K^G satisface una ecuación monica con coeficientes en A^G, y por tanto pertenece al cuerpo de fracciones de A^G. □

Ejemplo 15 (**Ejemplos básicos de** A^G**).**

1. ***Acción trivial.*** *Si* G *actúa trivialmente sobre* A*, entonces todo elemento es invariante y*

$$A^G = A.$$

2. ***Acción de*** $\mathbb{Z}/2\mathbb{Z}$ ***en*** $k[x, y]$**.** *Sea* $A = k[x, y]$ *y* $G = \mathbb{Z}/2\mathbb{Z}$ *que actúa intercambiando* x *y* y*. Los invariantes son los polinomios simétricos:*

$$A^G = k[x + y,\ xy].$$

3. ***Acción de*** $\mathbb{Z}/n\mathbb{Z}$ ***en*** $k[x]$**.** *Sea* $A = k[x]$ *y* $G = \mathbb{Z}/n\mathbb{Z}$ *actuando por* $g \cdot x = \zeta x$*, donde* ζ *es una raíz n-ésima de la unidad. Entonces*

$$A^G = k[x^n].$$

4. ***Acción de*** S_n ***en*** $k[x_1, \ldots, x_n]$**.** *El grupo simétrico* S_n *actúa permutando las variables. El subanillo de invariantes es el anillo de polinomios simétricos:*

$$A^G = k[e_1(x_1, \ldots, x_n),\ e_2(x_1, \ldots, x_n),\ \ldots,\ e_n(x_1, \ldots, x_n)],$$

donde e_i *son los polinomios simétricos elementales.*

5. ***Acción de*** $\mathbb{G}_m$ ***en*** $k[x, y]$**.** *Sea el grupo multiplicativo* $\mathbb{G}_m = k^\times$ *actuando por* $t \cdot (x, y) = (tx, t^{-1}y)$*. Entonces los invariantes son generados por* xy*:*

$$A^G = k[xy].$$

Ejemplo 16. *Un resultado clásico de Hilbert establece que si G es un grupo lineal reductivo actuando sobre un anillo de polinomios* $A = k[x_1, \ldots, x_n]$*, entonces el anillo de invariantes* A^G *es de tipo finito sobre k. Sin embargo, en 1959 Nagata construyó un contraejemplo para el caso de grupos no reductivos.*

Más precisamente, existe una acción de un grupo conmutativo afín de dimensión 13 *sobre el anillo de polinomios en* 32 *variables*

$$A = k[x_1, \ldots, x_{32}],$$

tal que el anillo de invariantes

$$A^G$$

no es finitamente generado *como álgebra sobre k.*

Este ejemplo respondió negativamente al Problema XIV de Hilbert*, que preguntaba si todo anillo de invariantes* A^G *es finitamente generado.*

Teorema 2. *Sea G un grupo finito de automorfismos de una k-álgebra finitamente generada A. Entonces* A^G *es finitamente generada sobre k.*

Demostración. De acuerdo con la Definición 1, G actúa sobre A mediante $g \cdot a := g(a)$ para $g \in G$ y $a \in A$, lo que corresponde a un homomorfismo $G \to \mathrm{Sym}(A)$. El subanillo

de invariantes se define como

$$A^G := \{a \in A : g(a) = a \ \forall g \in G\}.$$

Sea $\{x_1, \ldots, x_n\}$ un conjunto de generadores de A como k-álgebra. Para cada i se considera el polinomio

$$p_i(x) := \prod_{g \in G} \big(x - g(x_i)\big) \ \in A[x].$$

Dado que G permuta las raíces $\{g(x_i) : g \in G\}$, los coeficientes de $p_i(x)$ son invariantes, es decir, pertenecen a A^G. Además, como x_i es raíz de $p_i(x)$, es integral sobre la subálgebra generada por dichos coeficientes.
Sea R la k-álgebra generada por los coeficientes de todos los polinomios $p_1(x), \ldots, p_n(x)$. Por construcción, $R \subseteq A^G$ y R es finitamente generada sobre k según la Definición 4.

Cada x_i es integral sobre R, por lo que $A = R[x_1, \ldots, x_n]$ es integral sobre R. En consecuencia, A es un R-módulo de tipo finito: en efecto, de $p_i(x_i) = 0$ se deduce

$$x_i^{d_i} = c_{i,0} + c_{i,1}x_i + \cdots + c_{i,d_i-1}x_i^{d_i-1},$$

con $c_{i,j} \in R$ y $d_i = |G|$. Iterando este procedimiento para cada una de las variables, cualquier monomio $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ se reduce R-linealmente a combinación de monomios con $0 \leq \alpha_i < d_i$, formando así un conjunto generador finito de A como R-módulo. La integralidad implica que A es un R-módulo finitamente generado. En efecto, cada ecuación $p_i(x_i) = 0$ permite expresar $x_i^{|G|}$ como combinación R-lineal de potencias menores de x_i. Repitiendo este procedimiento para cada x_i, se deduce que A es generado como R-módulo por el conjunto finito de monomios

$$\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \ : \ 0 \leq \alpha_i < |G|\}.$$

Por el Teorema 1 (Base de Hilbert), si B es una k-álgebra finitamente generada, entonces B es noetheriana. Aplicando este resultado, R es noetheriana ya que es cociente de un anillo de polinomios $k[t_1, \ldots, t_m]$ (véase también el Ejemplo 14).
De acuerdo con la Proposición 4, si R es noetheriano y M es un R-módulo de tipo finito, entonces todo submódulo de M es también de tipo finito. Aplicando esto con $M = A$, se concluye que el submódulo A^G de A (considerado como R-módulo mediante la inclusión $R \subseteq A^G$) es un R-módulo finitamente generado.

Finalmente, si $\{r_1, \ldots, r_s\}$ genera R como k-álgebra y $\{y_1, \ldots, y_\ell\}$ genera A^G como R-módulo, entonces el conjunto finito $\{r_1, \ldots, r_s, y_1, \ldots, y_\ell\}$ genera A^G como k-álgebra. Por lo tanto, A^G es finitamente generada sobre k. □

Referencias Bibliográficas

[1] David Steven Dummit, Richard M Foote et al. *Abstract algebra*. Vol. 3. Wiley Hoboken, 2004.

[2] Caludia Granados Pinzon y Wilson Olaya Leon. «K-algebras finitas Conmutativas con unidad». En: (2016).

[3] Michael Francis Atiyah y Ian Grant Macdonald. *Introducción al álgebra conmutativa*. Reverté, 1989.

[4] Felipe Zaldivar. «Introduccion al Algebra Conmutativa». En: *Capitulo 4 : Anillos noetherianos y artinianos* (2011).

[5] Jack Jeffries. «Notas de algebra Conmutativa».

[6] Sebastian Zarete. «Estructuras Alegbraicas». En: *Modulos Noetherianos y Artinianos* (2015).

[7] Igor Dolgachev. *Lectures on Invariant Topology*. Cambridge University Press, 2003.

[8] Shigeru Mukai. *An introduction to Invariants and Moduli*. Cambridge University Press, 2003.

[9] TOBÍAS MARTÍNEZ. «GRUPOS ALGEBRAICOS REDUCTIVOS». En: ().