GRUPOS ALGEBRAICOS REDUCTIVOS

TOBÍAS MARTÍNEZ

RESUMEN. Se presentan métodos simbólicos de la Teoría de Invariantes y se usan para demostrar el Primer Teorema Fundamental de la Teoría de Invariantes y el Teorema de Gordan-Hilbert. Se introducen los conceptos de grupos linealmente reductivos y geométricamente reductivos y como aplicación de ellos se demuestra el Teorema de Nagata que afirma que el álgebra de invariantes de la acción de un grupo geométricamente reductivo sobre una álgebra finitamente generada, es finitamente generada. Se demuestra también que si G es un grupo reductivo actuando sobre una variedad algebraica afín X, entonces existe el cociente categórico X/G.

ÍNDICE

1. INTRODUCCIÓN

Consideremos una k-álgebra A finitamente generada y sea G un subgrupo de sus automorfismos. El conjunto $A^G := \{a \in A : g(a) = a, \forall g \in G\}$ es una k-álgebra. Sea $X = \mathrm{Specm}(A)$ la variedad algebraica afín sobre k tal-que $\mathcal{O}(X) = A$. Sea Y otra variedad algebraica afín con $\mathcal{O}(Y) = B$ y $f : X \to Y$ un morfismo invariante, luego f define un homomorfismo de k-álgebras $f^* : B \to A$ tal que $g(f^*(b)) = f^*(b)$ para todo $g \in G$ y $b \in B$. Tenemos por tanto que f^* es la composición de un homomorfismo $B \to A^G$ y la inclusión $A^G \hookrightarrow A$. Sea $Z = \mathrm{Specm}(A^G)$, así obtenemos una función $X \to Z$ definida por la inclusión $A^G \hookrightarrow A$ toma el rol de función universal para el cociente X/G (cf. [2, p. 123]). Vemos que es razonable asumir que $A^G = \mathcal{O}(X/G)$, sin embargo, el primer problema que se encuentra es que A^G no necesariamente es finitamente generada. El segundo problema, es que $\mathrm{Specm}(A^G)$ rara vez coincide con el conjunto de órbitas de X por G, es decir, $\mathrm{Specm}(A^G)$ no es el cociente categórico.

Luego, eso motiva las siguientes preguntas

- ¿Qué características debe tener G y cómo debe ser la acción sobre una k-álgebra A finitamente generada de manera tal que A^G sea finitamente generada?.
- ¿Bajo qué condiciones el conjunto de órbitas coincide con $\mathrm{Spec}(A^G)$?.

Elegantemente, los grupos reductivos son la respuesta. Nagata demostró en 1964 que si G es geométricamente reductivo, entonces A^G es finitamente generada. En 1916, Noether había demostrado este resultado en el caso de grupos finitos. Mostraremos también que dichos grupos nos proporcionan los cocientes deseados.

El interés en estudiar los invariantes, va más allá del ejemplo que hemos presentado. La Teoría de Invariantes tiene aplicaciones en el estudio de Cohomología de grupos finitos, Teoría de Grafos, Teoría de Codificación, Ciencia de Materiales, Visión por computadora, etc (ver [10, Cap. 5]).

El problema de determinar A^G tiene casi dos siglos y sólo en pocos casos se han obtenido resultados completos.

1.1. Estructura del artículo. Primero se establecen algunos convenios y terminología, luego se presentan algunos métodos simbólicos de la Teoría de Invariantes y se usan luego para demostrar el Primer Teorema de la Teoría de Invariantes y el Teorema de Gordan-Hilbert.

Luego se introduce la noción de grupo algebraico y grupo algebraico afín; se muestran varios ejemplos.

Introducimos las nociones de grupos linealmente reductivos, geométricamente reductivos y reductivos y muchas de sus propiedades, así como una serie de ejemplos entre los cuales mencionamos el Teorema que Haboush demostró en 1975 correspondiente a la Conjetura de Mumford; que todo grupo reductivo es geométricamente reductivo.

Se demuestra el Teorema de Nagata y se demuestra la existencia de buenos cocientes geométricos que a su vez son cocientes categóricos. Finalmente se resuelva un problema de ecuaciones funcionales adaptado de un ejemplo de [17] usando el Teorema de Nagata.

2. Notación

Como cuerpo base, se tomará un cuerpo k algebraicamente cerrado y de característica, $\operatorname{car}(k)$ arbitraria. Las variedades algebraicas afines a menudo estarán dadas como $X = \operatorname{Specm}(A)$ donde A es una k-álgebra finitamente generada reducida.

Dada una variedad algebraica X denotamos por $\mathcal{O}(X)$ su álgebra de funciones regulares.

Si A es un conjunto con una estructura algebraica, (k-álgebra, grupo, anillo, etc) denotamos por 1_A al elemento identidad de la operación de A (operación producto en el caso de que A sea un anillo) y denotamos por Id_A a la función identidad $A \to A$.

Una *acción* de un grupo G sobre un conjunto X es una aplicación $\alpha : G \times X \to X$ tal que

1. $\alpha(1_G, x) = x$ para todo $x \in X$ y
2. $\alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 g_2, x)$ para cualesquiera $g_1, g_2 \in G$ y cualquier $x \in X$.

A menudo denotamos $g(x) := \alpha(g, x)$.

Un elemento $x \in X$ se dice *G-invariante* si $g(x) = x$ para todo $g \in G$. Denotamos por X^G al conjunto de todos los elementos de X que son G-invariantes. Un subconjunto $Y \subset X$ se dice *G-invariante* (G-estable) si para todo $y \in Y$, $g(y) \in Y$. Si G actúa sobre dos conjuntos X, Z y $f : X \to Z$ ese una función, diremos que f es *G-equivariante* si $f(g(x)) = g(f(x))$ para todo $x \in X$ y se dice que es *G-invariante* si $f(g(x)) = f(x)$ para todo $x \in X$.

3. Métodos simbólicos

Definición 3.1. Sea E un k-espacio vectorial de dimensión finita $n \geq 1$. Una *función polinomial* f sobre E es una función $f : E \to k$ talque para cualquier base $\{b_1, \ldots, b_n\}$ de E y para cualquier $v = \sum_{i=1}^n \beta_i b_i \in E$, $f(v)$ es un polinomio en los coeficientes β_i, *i.e.,* existe un polinomio $\overline{f} \in k[X_1, \ldots, X_n]$ tal que $f\left(\sum_{i=1}^n \beta_i b_i\right) = \overline{f}(\beta_1, \ldots, \beta_n)$.

Ser función polinomial no depende de la elección de la base, tal como lo probamos en la siguiente proposición.

Proposición 3.2. *Sean $B = \{b_1, \ldots, b_n\}$ y $C = \{c_1, \ldots, c_n\}$ bases para de E y $f : E \to k$ una función. Entonces para todos los vectores $v = \sum_{i=1}^n \beta_i b_i = \sum_{i=1}^n \gamma_i c_1 \in E$, $f(v)$ es un polinomio en β_i si y sólo si lo es en las γ_i.*

Demostración:
Notar que por simetría, ambas direcciones de la proposición son idénticas salvo un cambio de notación. Supongamos que $f(v)$ es un polinomio en las β_i. Sea $M = (a_{ij}) \in \mathrm{GL}_n(k)$ la matriz de cambio de base de C a B. Tenemos que $\beta_i = \sum_{j=1}^n a_{ij} \gamma_j$. Luego, $f(v)$ es un polinomio en las β_i y cada β_i es un polinomio en las γ_i, por tanto, $f(v)$ es también un polinomio en las γ_i. ■

Ejemplo 3.3. La función determinante $\det : \operatorname{End}(E) \to k$ es una función polinomial sobre el el espacio de endomorfismos de E, $\operatorname{End}(E)$.

Denotamos por $\mathrm{Pol}(E)$ al conjunto de todas las funciones polinomiales sobre E, tenemos entonces que $\mathrm{Pol}(E)$ es isomorfo a $k[X_1,\dots,X_n]$.

Definición 3.4. Una función polinomial $f:E\to k$ se dice *homogénea de grado d* si cumple que $f(\lambda v)=\lambda^d f(v)$ para todo, $\lambda\in k$ y todo $v\in E$. Denotamos por $\mathrm{Pol}_d(E)$ al conjunto de funciones polinomiales homogéneas de grado d sobre E.

Tenemos que $\mathrm{Pol}(E)=\bigoplus_{d\geq 0}\mathrm{Pol}_d(E)$, por tanto, $\mathrm{Pol}(E)$ es una k-álgebra graduada.
Notar que $E^\vee\cong \mathrm{Pol}_1(E)$, luego si $\{b_1,\dots,b_n\}$ es una base de E, entonces la base dual $\{b_1^\vee,\dots,b_n^\vee\}$, es una base para $\mathrm{Pol}_1(E)$ y por tanto generan a $\mathrm{Pol}(E)$ como k-álgebra. Así, $\mathrm{Pol}(E)$ es una k-álgebra graduada finitamente generada.

Como $\mathrm{Pol}_m(E)$ es naturalmente isomorfa a la *m-ésima potencia simétrica* $\mathrm{S}^mE^\vee$ mediante la función que a cada elemento $v_1v_2\cdots v_n\in \mathrm{S}^mE^\vee$ le asigna $f\in\mathrm{Pol}_m(E)$ dada por $f(b_i)=v_1(b_1)\cdots v_n(b_i)$ y extendida por linealidad a las sumas finitas, resultando en un isomorfismo de k-álgebras. Luego, $\mathrm{Pol}(E)$ es isomorfa al álgebra simétrica de $E^\vee$, $\mathrm{S}E^\vee$ como k-álgebras graduadas. De manera similar, $\mathrm{Pol}(E^\vee)$ es isomorfa a $\mathrm{S}E$.

Asumamos $\mathrm{car}(k)=0$. Dado $P\in\mathrm{Pol}_m(E)$, tenemos que P induce una aplicación multilineal simétrica $\mathrm{pol}(P):E^n\to k$ dada por

$$\mathrm{pol}(P)(v_1,\dots,v_m)=\sum_{I\subset[m]}(-1)^{m-\#I}P\left(\sum_{i\in I}v_i\right),$$

donde $[m]:=\{1,\dots,m\}$.

Denotemos por $\mathrm{Sym}_m(E)$ el espacio vectorial de *m-formas multilineales simétricas* sobre E^m, entonces tenemos que la función $\mathrm{pol}:\mathrm{Pol}_m(E)\to\mathrm{Sym}_m(E)$ dada por $P\mapsto\mathrm{pol}(P)$ es lineal.

Para cualquier forma multilineal simétrica $F:E^m\to k$, la función $\mathrm{res}(F):E\to k$ definida por

$$\mathrm{res}(F)(v)=F(v,\dots,v);$$

llamada la *restitución* de F y tenemos que $\mathrm{res}:\mathrm{Sym}_n(E)\to\mathrm{Pol}(E)$ dada por $F\mapsto\mathrm{res}(F)$ es una función lineal. Más aún, tenemos que $\mathrm{res}(F)\in\mathrm{Pol}_m(E)$ y $\mathrm{pol}(\mathrm{res}(F))=m!F$ (cf. [9, p. 34])

Como $\mathrm{car}(k)=0$, tenemos que cada $P\in\mathrm{Pol}_m(E)$ es igual a la restitución de una única m-forma multilineal simétrica, llamada $\frac{1}{m!}\mathrm{pol}(P)$, lo que significa que $\mathrm{Pol}_m(E)\cong\mathrm{Sym}_m(E)$.
Supongamos que P es igual al producto de formas lineales $P=L_1\cdots L_m$. Entonces tenemos que

$$\begin{aligned}\mathrm{pol}(P)(v_1,\dots,v_m)&=\sum_{I\subset[m]}(-1)^{m-\#I}L_1\dots L_m\left(\sum_{i\in I}v_i\right)\\&=\sum_{I\subset[m]}(-1)^{m-\#I}L_1\left(\sum_{i\in I}v_i\right)\dots L_m\left(\sum_{i\in I}v_i\right)\\&=\sum_{I\subset[m]}(-1)^{m-\#I}\left(\sum_{i\in I}L_1\left(v_i\right)\right)\dots\sum_{i\in I}\left(L_m\left(v_i\right)\right)\\&=\sum_{\sigma\in S_n}L_1(v_{\sigma(1)})\dots L_m(v_{\sigma(m)})\\&=\sum_{\sigma\in S_n}L_{\sigma(1)}(v_1)\dots L_{\sigma(m)}(v_m).\end{aligned}\tag{3.1}$$

Sea $(\xi_1,\dots,\xi_n)$ una base de E y $(t_1,\dots,t_n)$ la base dual de $E^\vee$, luego, cualquier elemento $v\in E$ puede ser escrito como $v=\sum_{i=1}^n t_i(v)\xi_i$.

Para cualesquiera $v_1, \dots, v_m \in E$ y para cualquier $F \in \mathrm{Sym}_m(E)$, tenemos que

$$\begin{aligned} F(v_1, \dots, v_m) &= F\left(\sum_{i=1}^n t_i(v_1)\xi_i, \dots, \sum_{i=1}^n t_i(v_m)\xi_i\right) \\ &= \sum_{i_1,\dots,i_m=1}^n t_{i_1}(v_1)\dots t_{v_m} F(\xi_{i_1}, \dots, \xi_{i_m}). \end{aligned}$$

Tomando $v_1 = \dots = v_m = v$, obtenemos que

$$\mathrm{res}(F)(v) = \left(\sum_{i_1,\dots,i_m=1}^n a_{i_1\dots i_m} t_{i_1}\dots t_{i_m}\right)(v).$$

Dado que cualquier polinomio es la restitución de alguna m-forma multilineal simétrica, tenemos que cualquier $P \in \mathrm{Pol}_m(E)$ puede ser escrito de manera única como una suma de monomios $t_{i_1}\dots t_{i_m}$. Debido al isomorfismo $\mathrm{pol} : \mathrm{Pol}_m(E) \to \mathrm{Sym}_m(E)$, tenemos que $\mathrm{Sym}_m(E)$ tiene una base formada por la polarización de monomios $t_{i_1}\dots t_{i_m}$. Como los t_i son lineales, aplicando (3.1), tenemos que considerando el producto de m formas lineales sobre E como una m-forma multilineal sobre E^n, se cumple

$$\mathrm{pol}(t_{i_1}\dots t_{i_m})(v_1, \dots, v_m) = \sum_{\sigma\in S_n} t_{i_{\sigma(1)}}(v_1)\dots, t_{i_{\sigma(m)}}(v_m).$$

Luego, tenemos que

$$\mathrm{pol}(t_{i_1}\dots t_{i_m})(\xi_{j_1}, \dots, \xi_{j_m}) = \#\{\sigma \in S_n : (j_1, \dots, j_m) = (i_{\sigma(1)}, \dots, i_{\sigma(m)})\}. \tag{3.2}$$

Si escribimos $t_{i_1}\dots t_{i_m} = t_i^{k_1}\dots t_n^{k_n}$, entonces el lado derecho de la ecuación anterior es igual $k_1!\dots k_n!$ si $\{i_1, \dots, i_m\} = \{j_1, \dots, j_m\}$ y cero en otro caso.

Escojamos una base para $\mathrm{Pol}_m(E^\vee)$ formada por monomios $\xi_{i_1}\cdots\xi_{i_m}$. Para cualquier $F \in \mathrm{Sym}_m(E)$ podemos definir $F(\xi_{i_1}\cdots\xi_{i_m}) := F(\xi_{i_1}, \dots\xi_{i_m})$ y extender el dominio de F por linealidad a todos los polinomios homogéneos de grado m. Aplicando, (3.2), obtenemos que

$$\mathrm{pol}(t_1^{k_1}\dots t_n^{k_n})(\xi_1^{l_1}\dots\xi_n^{l_n}) = \begin{cases} k_1!\dots k_n!, & si\,(k_1, \dots, k_n) = (l_1, \dots, l_n), \\ 0, & \text{en otro caso.} \end{cases}$$

Esto muestra que la función $\mathrm{Pol}_m(E) \times \mathrm{Pol}_m(E^\vee) \to k$ definida por

$$(P, Q) \mapsto \frac{1}{m!}\mathrm{pol}(P)(Q),$$

es un emparejamiento perfecto, *i.e.,* define los isomorfismos $\psi_1 : \mathrm{Pol}_m(E^\vee) \to \mathrm{Pol}_m(E)^\vee$ y $\psi_2 : \mathrm{Pol}_m(E) \to \mathrm{Pol}_m(E^\vee)^\vee$ Luego,

$$\mathrm{Pol}_m(E)^\vee \cong \mathrm{Pol}_m(E^\vee),\ \mathrm{Pol}_m(E^\vee)^\vee \cong \mathrm{Pol}_m(E). \tag{3.3}$$

Si $f \in \mathrm{Pol}_m(E)$ y escogemos una base $(\xi_1, \dots\xi_r)$ de E, dado $v \in E$, $v = \sum_{i=1}^r t_i\xi_i$ y tendremos que

$$f(t_1, \dots, t_r) = \sum_{\substack{i_1,\dots,i_r\geq 0 \\ i_1+\dots+i_r=m}} a_{i_1\dots i_r} t_1^{i_1}\cdots t_r^{i_r},$$

o en notación vectorial

$$f(\mathbf{t}) = \sum_{\mathbf{i}\in\mathbb{Z}^r_{\geq 0},\ |\mathbf{t}|=m} a_{\mathbf{i}}\mathbf{t}^{\mathbf{i}}. \tag{3.4}$$

Podemos tomar coordenadas para E las funciones $A_{\mathbf{i}}$ que asignan a cada $f \in E$ en la forma (3.4) su coeficiente $a_{\mathbf{i}}$. Así, cualquier elemento de $\mathrm{Pol}(\mathrm{Pol}_d(V))$ es un polinomio en las $A_{\mathbf{t}}$.

En (3.3,la base monomial $(\boldsymbol{\xi}^{\mathbf{k}}) = (\xi_1^{k_1}\cdots\xi_n^{k_n})$ de $\mathrm{Pol}_m(E^\vee)$ es la base dual $(\frac{m!}{k_1!\cdots k_n!}t_n^{k_n}) = (\frac{m!}{\mathbf{k}!}\mathbf{t}^{\mathbf{k}})$. Por tanto, cualquier $P \in \mathrm{Pol}_m(E)$ se escribe como

$$P = \sum_{|\mathbf{k}|=m} \frac{m!}{\mathbf{k}!} a_{\mathbf{k}}\mathbf{t}^{\mathbf{k}}. \tag{3.5}$$

Notar que los $a_{\mathbf{k}}$ son iguales a los valores de $A_{\mathbf{k}} = \boldsymbol{\xi}^{\mathbf{k}} = \xi_1^{k_1} \cdots \xi_n^{k_n}$ en P. Podemos ver la expresión $P_{\text{general}} = P = \sum_{|\mathbf{k}|=m} \frac{m!}{\mathbf{k}!} A_{\mathbf{k}} \mathbf{t}^{\mathbf{k}}$ como un polinomio homogéneo de grado m general.

Sea $E = \mathrm{Pol}_d(V)$ donde V es un k-espacio vectorial de dimensión r. Una *función multihomogénea de multigrado* $(d_1, \ldots, d_m)$, sobre V, es una función sobre V^m que es homogénea de grado d_i en cada variable. Notar que las funciones multihomogéneas de multigrado $(1, \ldots, 1)$ son las funciones multilineales. Denotamos por $\mathrm{Pol}_{d_1,\ldots,d_m}(V)$ *espacio lineal de funciones multihomogéneas de multigrado* $(d_1, \ldots, d_m)$. Tenemos que el grupo simétrico S_m actúa naturalmente sobre $\mathrm{Pol}_{d,\ldots,d}(V)$ permutando las variables y definimos subespacio S_m-invariante $\mathrm{Sym}_{d,\ldots,d}(V) := \mathrm{Pol}_{d,\ldots,d}(V)^{S_m}$ que serán efectivamente funciones simétricas. En particular, tenemos que $\mathrm{Sym}_{1,\ldots,1}(V) = \mathrm{Sym}_m(V)$.

Lema 3.5. *Tenemos un isomorfismo natural de espacios lineales*

$$\mathrm{symb} : \mathrm{Pol}_m(\mathrm{Pol}_d(V)) \to \mathrm{Sym}_{d,\ldots,d}(V^\vee).$$

Demostración:
Tenemos que la polarización define un isomorfismo

$$\mathrm{Pol}_m(\mathrm{Pol}_d(V)) \cong \mathrm{Sym}_m(\mathrm{Pol}_d(V)).$$

Usando la polarización, de manera similar a como se obtuvieron los isomorfismos en (3.3), obtenemos que $\mathrm{Pol}_d(V)^\vee \cong \mathrm{Pol}_d(V^\vee)$. Así, cualquier función lineal sobre $\mathrm{Pol}_d(V)$ es una función polinomial homogénea de grado d sobre $V^\vee$. Por tanto, las funciones multilineales sobre $\mathrm{Pol}_d(V)$ pueden identificarse con funciones multihomogéneas de multigrado $(d, \ldots, d)$ sobre $V^\vee$. ∎

Podemos hacer el isomorfismo del Lema anterior más explícito usando una base $(\xi_1, \ldots, \xi_r)$ de V y su base dual $(t_1, \ldots, t_r)$ en $V^\vee$. Sea $A_{\mathbf{k}}$ con $|\mathbf{k}| = d$ las funciones coordenadas sobre $\mathrm{Pol}_d(V)$, donce cada $P \in \mathrm{Pol}_d(V)$ está escrito en la forma (3.5) con m reemplazado por d, así, que $A_{\mathbf{k}}(P) = a_{\mathbf{k}}$ y por tanto, cualquier $F \in \mathrm{Pol}_m(\mathrm{Pol}_d(V))$ es una expresión polinomial en las $A_{\mathbf{k}}$ de grado m. Sea $(A_{\mathbf{k}}^{(1)}), \ldots, (A_{\mathbf{k}}^{(m)})$ las funciones coordenadas en cada copia de $\mathrm{Pol}_d(V)$, tenemos que la polarización $\mathrm{pol}(F)$ es una expresión multilineal en $A_{\mathbf{k}}^{(j)}$ y si reemplazamos $A_{\mathbf{k}}^{(j)}$ con el monomio $(\boldsymbol{\xi}^{(j)})^{\mathbf{k}} = (\xi_1^{(j)})^{k_1} \cdots (\xi_r^{(j)})^{k_n}$ en la base $(\xi_1^{(j)}, \ldots, \xi_r^{(j)})$ de la j-ésima copia de V, obtenemos la *expresión simbólica* de F

$$\mathrm{symb}(F)(\boldsymbol{\xi}^{(1)}, \ldots, \boldsymbol{\xi}^{(m)}) \in \mathrm{Pol}_{d,\ldots,d}(V^\vee).$$

Denotamos por $\mathrm{Mat}_{r,m}$ al espacio de matrices de tamaño $r \times m$.

Organizamos ahora a las variables $\xi_1^{(1)}, \ldots, \xi_r^{(1)}, \ldots, \xi_1^{(m)}, \ldots, \xi_r^{(m)}$ como una matriz de tamaño $r \times m$

$$A = \begin{pmatrix} \xi_1^{(1)} & \cdots & \xi_1(m) \\ \vdots & \ddots & \vdots \\ \xi_r^{(1)} & \cdots & \xi_r^{(m)} \end{pmatrix}.$$

Primero identificamos el espacio $\mathrm{Pol}_{d,\ldots,d}(V^\vee)$ con el subespacio del álgebra de polinomios

$$k[\xi_1^{(1)}, \ldots, \xi_r^{(1)}, \ldots, \xi_1^{(m)}, \ldots, \xi_r^{(m)}]$$

que consiste de polinomios homogéneos de grado d en cada conjunto de variables $\xi_1^{(j)}, \ldots, \xi_r^{(j)}$. Luego, identificamos el álgebra $\mathrm{Pol}(\mathrm{Mat}_{r,m})$ de las funciones polinomiales sobre el espacio de matrices $\mathrm{Mat}_{r.m}$. El valor de cada variable $\xi_i^{(j)}$ en una matriz A es la ij-ésima entrada de la matriz.
El grupo $(k^*)^m$ actúa naturalmente sobre el espacio $\mathrm{Mat}_{r,m}$ mediante

$$(\lambda_1, \ldots, \lambda_m) \cdot [C_1, \ldots, C_m] := [\lambda_1 C_1, \ldots, \lambda_m C_m],$$

donde la matriz $A = [C_1, \ldots, C_m]$. De manera similar, $(k^*)^r$ actúa sobre $\mathrm{Mat}_{r,m}$ multiplicando las filas. Diremos que un polinomio $P \in \mathrm{Pol}(\mathrm{Mat}_{r,m})$ es *multihomogéno de multigrado* $(d_1, \ldots, d_m)$ si para cualquier $\lambda \in k^*$ y cualquier $A = [C_1, \ldots, C_m] \in \mathrm{Mat}_{r,m}$,

$$P([C_1, \ldots, C_{j-1}, \lambda C_j, C_{j+1}, \ldots, C_m] = \lambda^{d_j} P([C_1, \ldots, C_j, \ldots, C_m]).$$

Diremos que P es *multiisobárico* de multipeso $(w_1, \ldots, w_r)$ si la función polinomial $A \to P(A^t)$ sobre el espacio $Mat_{r,m}$ es multihomogéna de multigrado $(w_1, \ldots, w_r)$. Denotemos por $\mathrm{Pol}(\mathrm{Mat}_{r,m})_{d_1,\ldots,d_m;w_1,\ldots,w_r}$ el subespacio de funciones polinomiales de $\mathrm{Mat}_{r,m}$ que son multihomogéneas de multigrado $(d_1, \ldots, d_m)$ y multisobáricas de multipeso $(w_1, \ldots, w_r)$. Si $d_1 = \ldots = d_m = d$, escribimos $d^m = (d_1, \ldots, d_m)$ y de manera similar $w^r = (w_1, \ldots, w_r)$ cuando los pesos $w_1 = \ldots = w_r = w$.

Por definición, la expresión simbólica de un polinomio invariante de $\mathrm{Pol}_m(\mathrm{Pol}_d(V))$ es multihomogénea. Probaremos ahora que es multiisobárica.

Proposición 3.6. *Hay una inclusión*

$$\mathrm{symb}(\mathrm{Pol}_m(\mathrm{Pol}_d(V))^{\mathrm{SL}(V)}) \subset \mathrm{Pol}(\mathrm{Mat}_{r,m})_{d^m;w^r},$$

donde $rw = md$.

Demostración:
Consideremos $F \in \mathrm{Pol}_m(\mathrm{Pol}_d(V))^{\mathrm{SL}(V)}$ como un polinomio en los coeficientes A_i del polinomio general $\sum_{\mathbf{i}} \binom{d}{\mathbf{i}} \mathbf{t}^{\mathbf{i}} \in \mathrm{Pol}_d(V)$. Como para cada $g \in \mathrm{GL}_r(k)$ y cualquier $\tilde{g} \in \mathrm{SL}(V)$, se cumple que $\det(\det(g)\tilde{g}) = \det(g)^r$, entonces dada $g \in \mathrm{GL}_r(k)$ tendremos que

$$g^r = \det(g)\tilde{g},$$

para alguna $\tilde{g} \in \mathrm{SL}(V)$.

Además, las matrices escalares λI_r actúan sobre cada ξ_i de la base de V multiplicando por λ. Por tanto, actúa sobre cada función coordenada t_i multiplicando por λ^{-1} y sobre $\mathrm{Pol}_d(V)$ multiplicando por λ^{-d}. En consecuencia, como $g \cdot F(P) = F(g^{-1}P)$, λI_r actúa sobre $\mathrm{Pol}_m(\mathrm{Pol}_d(V))$ multiplicando por λ^{md}. Luego,

$$g^r \cdot F = (\det(g))^{md}\tilde{g} \cdot F = \det(g)^{md}F,$$

ya que F es $\mathrm{SL}(V)$-invariante.

Como k es algebraicamente cerrado con $car(k) = 0$, tenemos que cualquier $g' \in \mathrm{GL}_r(k)$ puede escribirse como g^r para alguna $g \in \mathrm{GL}(V)$, y por tanto, tenemos

$$g' \cdot F = g^r \cdot F = (\det(g))^{md}F = \chi(g')F$$

para algún homomorfismo $\chi : \mathrm{GL}_r(k) \to k^*$.

Si fijamos $F \in \mathrm{Pol}_m(\mathrm{Pol}_d(V))^{\mathrm{SL}(V)}$ y $P \in \mathrm{Pol}_d(V)$, tenemos que la función $g \mapsto g \cdot F(P)$ es una función polinomial homogénea de grado md en las entradas de la matriz g. Como $g^r \cdot F = \chi(g^r)F = (\det(g))^{md}F$, tenemos que $\chi(g)^r = \det(g)^{md}$ y como $\det(g)$ es un polinomio irreducible de grado r, tenemos que $\chi(g) = \det(g)^w$ para algún entero no negativo w y en consecuencia

$$g \cdot F = \det(g)^w F.$$

Por construcción de $\mathrm{symb} : \mathrm{Pol}_m(\mathrm{Pol}_d) \to \mathrm{Pol}(\mathrm{Mat}_{r,m})$ tenemos que symb es G-equivariante, *i.e.,* para todo $g \in \mathrm{GL}_r(k)$,

$$g \cdot \mathrm{symb}(F) = \det(g)^w \mathrm{symb}(F).$$

Tomando $g = \mathrm{diag}(1, \ldots, \lambda, 1, \ldots, 1)$, obtenemos que $\mathrm{symb}(F)$ es multiisobárica de multipeso w^r y por definición $\mathrm{symb}(F)$ es multihomogénea de multigrado d^m, con lo cual $F \in \mathrm{Pol}(\mathrm{Mat}_{r,m})_{d^m;w^r}$. ■

Corolario 3.7. *Si $r \nmid md$. Entonces para $m > 0$, tenemos que*

$$\mathrm{Pol}_m(\mathrm{Pol}_d(V))^{\mathrm{SL}(V)} = \{0\}.$$

Demostración:
Si existiera $F \in \mathrm{Pol}_m(\mathrm{Pol}_d(V))^{\mathrm{SL}(V)}$ con $F \neq 0$, entonces la relación $\chi(g)^r = (\det(g))^{md}$ debería cumplirse para todo $g \in \mathrm{GL}_r(k)$ pero esto implica que $r|md$. ■

Un ejemplo de una función de $\mathrm{Pol}(\mathrm{Mat}_{r,r})_{1^r;1^r}$ es la función determinante $\mathcal{D}_r : \mathrm{Mat}_{r,r} \to k$ dada por $A \mapsto \det(A)$. De manera más general, tenemos la siguiente definición.

Definición 3.8. Sea $J \subset [m] := \{1, \ldots, m\}$. Una *función corchete* $\det_J$ sobre $\mathrm{Mat}_{r,m}$ es una función que a cada matriz $A \in \mathrm{Mat}_{r,m}$ le asigna el máximo menor formado por las columnas indexadas por J. Si $J = \{j_1, \ldots, j_r\}$ usaremos la definición clásica para menores

$$\det_J = (j_1 \ldots j_r) = [j_1, \ldots, j_r].$$

Sea $P(X_1, \ldots, X_N) \in k[X_1, \ldots, X_N]$, denotemos por $\tilde{P}$ el operador diferencial formal obtenido al reemplazar cada X_i por la derivada parcial formal $\frac{\partial}{\partial X_i}$.

Definición 3.9. Sea $N = r^2$ e incógnitas X_{ij}, con $i, j = 1, \ldots, r$ y sea P el polinomio resultante de evaluar la función determinate $\mathcal{D}_r$ en la matriz con entradas X_{ij}. El correspondiente operador diferencial $\tilde{P}$ lo denotamos por Ω y es llamado el *operador omega* o *operador de Cayley.*

Enunciamos los siguientes lemas técnicos sin demostración, (ver [1, pp. 17-19]).

Lema 3.10. *Se cumple la relación*

$$\Omega(\mathcal{D}_r^s) = s(s+1)\cdots(s+r-1)\mathcal{D}_r^{s-1}.$$

Lema 3.11. *Sea* $F = P_1 \cdots P_r \in k[x_{11}, \ldots, X_{rr}]$, *donde cada* P_i *es igual al producto de* m_i *formas lineales* $L_i^{(j)} = \sum_{s=1}^{r} a_{is}^{(j)} X_{is}$, $j = 1, \ldots, m_i$. *Entonces*

$$\Omega(F) = \sum \det \begin{pmatrix} a_{11}^{(j_1)} & \ldots & a_{1r}^{(j_r)} \\ \vdots & \ddots & \vdots \\ a_{r1}^{(j_1)} & \ldots & a_{rr}^{(j_r)} \end{pmatrix} (P_1/L_1^{(j_1)} \cdots (P_r/L_r^{(j_r)}),$$

donde la suma es tomada sobre el conjunto $S = \{(j_1, \ldots, j_r) : 1 \leq j_i \leq m_i\}$.

4. Primer Teorema Fundamental de la Teoría de Invariantes y Teorema de Gordan-Hilbert

Probamos ahora el Primer Teorema Fundamental de la Teoría de Invariantes.

Teorema 4.1. *El álgebra de invariantes* $\mathrm{Pol}(\mathrm{Mat}_{r,m})^{\mathrm{SL}_r(k)}$ *es finitamente generada por las funciones corchete* $[j_1, \ldots, j_r]$.

Demostración:
Sea $\mathrm{Pol}(\mathrm{Mat}_{r,m})_w$ el subespacio de polinomios multiisobáricos de multi peso w^r. Tenemos entonces que

$$\mathrm{Pol}(\mathrm{Mat}_{r,m})^{\mathrm{SL}_r(k)} = \bigoplus_{w \geq 0} \mathrm{Pol}(\mathrm{Mat}_{r,m})^{\mathrm{SL}_r(k)}.$$

Luego podemos asumir que un polinomio invariante $F \in \mathrm{Pol}(\mathrm{Mat}_{r,m})^{\mathrm{SL}_r(k)}$ pertenece a $\mathrm{Pol}(\mathrm{Mat}_{r,m})_w$. Fijemos un $A \in \mathrm{Mat}_{r,m}$, por la demostración de la Proposición 3.6 que

$$F(g \cdot A) = \det(g)^w F(A).$$

Como F es multiisobárico, entonces $F(g \cdot A)$ puede ser escrito como producto de polinomios lineales como en el Lema 3.10 con $m_i = w$. Aplicando el operador omega w veces al lado izquierdo de la identidad podemos deshacernos de las variables g_{ij} y obtenemos así un polinomio en las funciones corchete. Por otra parte, por el Lema 3.10, obtenemos un múltiplo escalar de F, con lo cual, F es un polinomio en las funciones corchetes. ■

Asumimos ahora que el cuerpo k es de característica arbitraria a menos que se especifique lo contrario.

Teorema 4.2. *Sea* G *un grupo finito de automorfismos de una* k*-álgebra finitamente generada* A. *Entonces* A^G *es finitamente generada sobre* k.

Demostración:
Sean $x_1, \ldots, x_n$ generadores de A sobre k. Notar que cada x_i es raíz del polinomio $p_i(x) = \prod_{g \in G}(x - g(x_i))$ que tiene coeficientes G-invariantes. Sea R la k-álgebra generada por los coeficientes de los $p_i(x)$, luego, R es una k-álgebra finitamente generada sobre k. El anillo A es un R-módulo finitamente generado, ya que los monomios en las cuales todas las x_i que aparecen tienen exponente menor que $|G|$ forman un conjunto finito de generadores como R-módulo. Como R es noetheriano y

$$R \subset A^G \subset A,$$

entonces A^G es un R-módulo finitamente generado y por tanto es una k-álgebra finitamente generada ya que basta tomar los generadores de R como k-álgebra y los generadores de S^G como R-módulo y la unión de estos conjuntos de generadores, generan a A^G como k-álgebra. ■

Daremos una prueba alternativa en el caso especial de que el orden $d = |G|$ de G es primo a la característica de k y G actúa sobre $A = \mathrm{Pol}(E)$ mediante su acción lineal sobre E.

Tenemos que el espacio de polinomios homogéneos de grado m, queda invariante bajo la acción de G, (si $P \in \mathrm{Pol}(E)$ es homogéneo de grado m, entonces $g \cdot P$ es homogéneo de grado m), luego,

$$\mathrm{Pol}(E)^G = \bigoplus_{m=0}^{\infty} \mathrm{Pol}_m(E)^G.$$

Sea I el ideal de A generado por polinomios homogéneos de grado positivo invariantes que se anulan en cero. Por el Teorema de la base de Hilbert, I es finitamente generado por un conjunto finito de polinomios $F_1, \ldots, F_n \in A^G$. Podemos asumir que cada F_i es homogéneo de grado $m_i > 0$. Entonces cualquier función poliniomial $F \in A^G$ de grado m se puede escribir como

$$F = P_1F_1 + \cdots + P_nF_n \tag{4.1}$$

para algunos polinomios homogéneos P_i de grado $m - m_i$.
Consideremos el operador $\mathbb{E} : A \to A$ dado por

$$\mathbb{E}(P) = \frac{1}{d}\sum_{g\in G} g(P).$$

Tenemos entonces que $\mathbb{E}|_{A^G} = \mathrm{Id}_{A^G}$ y $\mathbb{E}(A) = A^G$. Aplicando $\mathbb{E}$ a ambos lados de la ecuación (4.1) obtenemos

$$F = \mathbb{E}(P_1)F_1 + \cdots + \mathbb{E}(P_n)F_n.$$

Asumamos por inducción que cada polinomio invariante de grado menor que m puede ser escrito como un polinomio en las F_i. Como $\mathbb{E}(P_i)$ es homogéneo de grado menor que m ya que cada P_i lo es, tenemos $\mathbb{E}(P_i)$ se puede escribir como un polinomio en las F_i y en consecuencia F se puede escribir como un polinomio en las F_i.

Sea $F \in \mathrm{Pol}_m(E)^{\mathrm{SL}(V)}$, por Proposición 3.6, existe un entero e tal que para cualquier $v \in E$,

$$F(g \cdot v) = \det(g)^e F(v).$$

El número e es llamado el *peso* de F. Probaremos ahora el teorema de Gordan-Hilbert que es otra aplicación del Teorema de la base de Hilbert, de hecho, Hilbert probó dicho Teorema en su artículo de 1980 (ver[5]) para demostrar este teorema. Para ello necesitaremos el siguiente lema.

Lema 4.3. *Sean $r > q$ enteros no negativos. Para cualquier $P \in \mathrm{Pol}(E)$ y cualquier $v \in E$, sea*

$$F(g, v) = \Omega^r(\det(g)^q P(g \cdot v)).$$

Entonces $F(0, v)$ es cero o un invariante de peso $r - q$.

Teorema 4.4. *(Gordan-Hilbert) El álgebra de invariantes $\mathrm{Pol}(\mathrm{Pol}_d(V))^{\mathrm{SL}(V)}$ es finitamente generada sobre k.*

Demostración:
Sea $E = \mathrm{Pol}_d(V)$. Usaremos la misma idea de la segunda prueba del Teorema 6,7, sólo que en vez de usar el operador $\mathbb{E}$, usaremos el operador omega Ω. Sea $F \in \mathrm{Pol}_m(E)^{\mathrm{SL}(V)}$, escribimos

$$F = P_1F_1 \cdots + P_nF_n$$

para algún $P_i \in \mathrm{Pol}_{m-m_i}(E)$ y $F_i \in \mathrm{Pol}_{m_i}(E)^{\mathrm{SL}(V)}$. Por la prueba de la Proposición 3.6, tenemos que existe un entero e tal que para cada $v \in E$,

$$F(g \cdot v) = \det(g)^e F(V).$$

Luego, para un $g \in \mathrm{GL}(V)$ tenemos que

$$F(g \cdot v) = \det(g)^e F(v) = \sum_{i=1}^{n} \det(g)^{e_i} P_i(g \cdot v) F_i(v).$$

Aplicando e veces el operador omega Ω a ambos lados obtenemos, por Lema 3.10 que

$$cF(v) = \sum_{i=1}^{n} \Omega^e(\det(g)^{e_i} P_i(g \cdot v))F_i(v),$$

donde c es una constante no nula. Por el Lema 4.3 tenemos que en $g = 1_{\mathrm{GL}(V)}$, $\Omega^e(\det(g)^{e_i} P_i(g \cdot v))$ es $\mathrm{SL}(V)$-invariante y si suponemos que todos los polinomios de grado menor que m se escriben como un polinomio en las F_i, entonces $\Omega^e(\det(g)^{e_i} P_i(g \cdot v))$ se escribe como un polinomio en las F_i y por tanto, F se escribe como un polinomio en las F_i. ■

5. Grupos Algebraicos

Definición 5.1. Un *grupo algebraico* es una variedad algebraica G tales que la función producto $\mu : G\times G \to G$ y la función inversión $\beta : G \to G$ son morfismos regulares. Si G es una variedad algebraica afín, entonces se dice que G es un *grupo algebraico afín.*

Dado que si X, Y son variedades algebraicas afines, entonces hay una biyección entre los morfismos regulares $X \to Y$ y homomorfismos de k-álgebras $\mathcal{O}(Y) \to \mathcal{O}(X)$ y luego la multiplicación e inversión que definen un grupo algebraico afín G pueden ser definidas por homomorfismos de k-álgebras

$$\mu^* : \mathcal{O}(G) \to \mathcal{O}(G\times G) \cong \mathcal{O}(G)\otimes_k \mathcal{O}(G),\ \beta^* : \mathcal{O}(G) \to \mathcal{O}(G)$$

que serán llamados *coproducto* y *coinverso*. Luego, dada una k-álgebra A finitamente generada, se puede definir un grupo algebraico afín $G := \mathrm{Specm}(A)$ junto con homomorfismos de k-álgebras

$$\mu^* : A \to A\otimes_k A,\ \beta^* : A \to A,$$

satisfaciendo:

(i) El diagrama

$$\begin{tikzcd} A \arrow[r, "\alpha^*"] \arrow[d, "\mu^*"'] & A\otimes_k A \arrow[d, "\mathrm{Id}_A\otimes\mu^*"] \\ A\otimes_k A \arrow[r, "\mu^*\otimes \mathrm{Id}_A"] & A\otimes_k A\otimes_k A \end{tikzcd}$$

conmuta.

(ii) Las dos composiciones

$$\begin{tikzcd} & & k\otimes_k A \arrow[dr, "\sim"] & \\ A \arrow[r, "\mu^*"] & A\otimes_k A \arrow[ur, "\epsilon\otimes\mathrm{Id}_A"] \arrow[dr, "\mathrm{Id}_A\otimes\epsilon"'] & \cdot & A \\ & & A\otimes_k k \arrow[ur, "\sim"'] & \end{tikzcd}$$

son iguales a la identidad, donde $\epsilon : A \to k$ es el homomorfismo *coidentidad* dado por $\epsilon(f) = f(1_G)$.

(iii) La composición, (donde la última función m es la multiplicación en A)

$$A \xrightarrow{\mu^*} A\otimes_k A \xrightarrow{\mathrm{Id}_A\otimes\beta^*} A\otimes_k A \xrightarrow{m} A$$

coincide con ϵ.

Estos tres requerimientos coinciden respectivamente a la asociatividad, existencia de elemento identidad y existencia de inversos (por la derecha).

Para cualquier k-álgebra K denotamos por $X(K)$, llamado el conjunto de K puntos de X, al conjunto de homomorfismos de k-álgebras $\mathcal{O}(X) \to K$. En particular, si $K = \mathcal{O}(Y)$ para alguna variedad algebraica afín Y, entonces $X(K)$ puede identificarse con el conjunto de morfismos de Y a X.

5.1. Ejemplos de grupos algebraicos afines.

1. El grupo aditivo $\mathbb{G}_a$, es el grupo $(k, +)$, i.e., la variedad afín $\mathbb{A}^1$ bajo la suma. Tenemos en este caso que $\mathcal{O}(\mathbb{G}_a) = k[x]$.
2. El grupo multiplicativo $\mathbb{G}_m$ es el grupo $(k^\times, \times)$, i.e., el conjunto abierto $\mathbb{A}^1 \setminus \{0\}$ bajo la multiplicación. Se tiene que $\mathcal{O}(\mathbb{G}_m) = k[x, x^{-1}]$.
3. El grupo $\mathrm{GL}_n = \mathrm{GL}_n(k)$ es el grupo de matrices $n \times n$ sobre k con determinante distinto de cero. $\mathrm{GL}_n = \mathbb{A}^{n^2} \setminus \{M \in \mathbb{A}^{n^2} : \det(M) = 0\}$ y por tanto G_n es abierto y en consecuencia una variedad algebraica afín ya que es isomorfa como variedad a
$$\left\{(X, x_{n^2+1}) \in \mathbb{A}^{n^2+1} : \det(X)x_{n^2+1} = 1\right\},$$
donde se toma a la matriz X como un elemento de $\mathbb{A}^{n^2}$.
El producto $\mathrm{GL}_n \times \mathrm{GL}_n \to \mathrm{GL}_n$ es regular pues está dado por polinomios sobre k y recordemos que $A \in \mathrm{GL}_n$,
$$A^{-1} = \frac{1}{\det A}\mathrm{Adj}(A)$$
donde $\mathrm{Adj}(A)$ es la transpuesta de la matriz de cofactores (cuya entrada ij se obtiene como $(-1)^{i+j}\det(A_{ij})$ donde A_{ij} se obtiene de A eliminando la fila i y la columna j.) Por lo que también es regular. Se tiene que $\mathcal{O}(\mathrm{GL}_n(k)) = k[x_1, \dots, x_{n^2}, \det(x_{ij})^{-1}]$.
4. $\mathrm{PGL}_n := \mathrm{PGL}_n(k) = \mathrm{GL}_n / \mathrm{Z}(\mathrm{GL}_n)$ donde $\mathrm{Z}(\mathrm{GL}_n)$ es el centro de GL_n es decir, el conjunto de matrices escalares, es una variedad y para ver que el producto y la inversión son regulares, se procede análogo a GL_n.
5. Cualquier subgrupo cerrado de un grupo algebraico, es un grupo algebraico.
6. El *el grupo especial lineal* $\mathrm{SL}_n(k)$ formado por los elementos de $\mathrm{GL}_n(k)$ con determinante igual a 1, es un subgrupo y es cerrado debido a que está definido por una condición cerrada, por tanto, $\mathrm{SL}_n(k)$ es un grupo algebraico afín.
7. El producto finito de grupos algebraicos, también es un grupo algebraico.
8. El *toro algebraico afín sobre* k, denotado por $\mathbb{T}_k^n := \mathbb{G}_m^n$ para algún entero positivo n, es también un grupo algebraico afín.

Para variedades algebraicas suaves, sabemos que son irreducibles si y sólo si son conexas. En el caso de grupos algebraicos, esto siempre es cierto.

Proposición 5.2. *Un grupo algebraico es irreducible si y sólo si es conexo.*

Demostración:
Toda variedad algebraica irreducible es conexa. Recíprocamente, supongamos que G es un grupo algebraico conexo. Basta probar que existe una única componente irreducible que contiene a 1_G ya que por homogeneidad esto implica que sólo hay una componente irreducible conteniendo a cada punto y por la hipótesis de conexidad, esto significa que G tiene una única componente irreducible, con lo cual, G es irreducible.

Por contradicción, supongamos que hay más de una y sean $X_1, \dots, X_r$ las componentes irreducibles que contienen a 1_G. Definamos $\varphi : X_1 \times \ldots \times X_R \to G$ mediante el producto. Como las X_i son irreducibles, también lo es el producto de ellas y por tanto también la imagen de φ. Como $1_G \in \mathrm{Im}(\varphi)$ que es irreducible, entonces $\mathrm{Im}(\varphi) \subseteq X_i$ para algún $i \in \{1, \dots, r\}$. Como todas las X_j contienen a 1_G, entonces $X_j \subset X_i$ para todo $j = 1, \dots, r$, lo que es una contradicción, luego, sólo hay una componente irreducible que contiene a 1_G. ■

Definición 5.3. La *componente identidad* de un grupo algebraico G es la única componente irreducible que contiene a 1_G y se denota por G^0.

Definición 5.4. Un subconjunto $B \subset X$ de una variedad algebraica X se dice *constructible* si se puede escribir como unión finita de conjuntos localmente cerrados.

Lema 5.5. *Sean U, V dos subconjuntos abiertos densos de un grupo algebraico G. Entonces $G = U \cdot V$.*

Demostración:
Tenemos que $U \cdot V \subset G$. Recíprocamente sea $x \in G$. Como la inversión es un homeomorfismo, V^{-1} es un conjunto abierto y luego xV^{-1} también es abierto. Como U es denso, $xV^{-1} \cap U \neq \emptyset$ con lo cual $x \in U \cdot V$. ■

Proposición 5.6. *Sea H un subgrupo de un grupo algebraico G y $\overline{H}$ su clausura.*
1. *$\overline{H}$ es un subgrupo de G y en consecuencia un grupo algebraico.*
2. *Si H es constructible, entonces $H = \overline{H}$.*

Demostración:

1. Como la inversión es un homeomorfismo,
$$\overline{H}^{-1} = \overline{H^{-1}} = \overline{H},$$
con lo cual $\overline{H}$ es estable bajo inversiones.
Como la traslación por $x \in H$ es un homeomorfismo de H,
$$x\overline{H} = \overline{xH} = \overline{H},$$
con lo cual $H\overline{H} \subset \overline{H}$. Además, si $x \in \overline{H}$, $Hx \subset \overline{H}$, así
$$\overline{H}x = \overline{Hx} \subset \overline{H}.$$
Por tanto, $\overline{H}$ es un subgrupo de G.
2. Si H es constructible, entonces contiene un subconjunto abierto denso (cf. [16, p. 8]). Como $\overline{H}$ es un grupo, por el Lema 5.5 tenemos que $\overline{H} = U \cdot U \subset H \cdot H = H$.

■

Definición 5.7. Un morfismo de grupos algebraicos es un homomorfismo de grupos $\varphi : G \to G'$ que es un morfismo de variedades algebraicas.

Proposición 5.8. *Sea $\varphi : G \to G'$ un morfismo de grupos algebraicos. Entonces*
1. $\mathrm{Ker}(\varphi)$ *es un subgrupo cerrado de G.*
2. $\mathrm{Im}(\varphi)$ *es un subgrupo cerrado de G'.*

Demostración:

1. Como φ es continua y $\mathrm{Ker}(\varphi) = \varphi^{-1}(1_{G'})$, tenemos que $\mathrm{Ker}(\varphi)$ es cerrado.
2. $\varphi(G)$ es un subgrupo de G' que es constructible (cf. [11, p. 33]) y por Proposición 5.6, tenemos que $\varphi(G)$ es cerrado.

■

Definición 5.9. Un grupo algebraico lineal es un subgrupo cerrado de $\mathrm{GL}_n(k)$.

Ejemplo 5.10. El grupo simétrico S_n es isomorfo al grupo de matrices de permutaciones P_n. Por el Teorema de Cayley, todo grupo finito es isomorfo a un subgrupo de S_n para algún entero positivo n y por tanto, un subgrupo de P_n, con lo cual, si G es un grupo finito entonces es un subgrupo cerrado de GL_n, por tanto, todo grupo finito es un grupo algebraico lineal.

Ejemplo 5.11. Las curvas elípticas son ejemplos de grupos algebraicos que no son grupos algebraicos lineales. (cf. [15, p. 23])

Definición 5.12. Una *acción racional o acción regular* de un grupo algebraico G sobre una variedad X como un morfismo regular $\alpha : G \times X \to X$ tal que $\alpha(1_G, x) = x$ y $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ para todo, $g, h \in G$ y todo $x \in X$.

Definición 5.13. Una *representación racional* de un grupo algebraico afín G es una representación lineal $\rho : G \to \mathrm{GL}_n(V) \cong \mathrm{GL}_n(k)$ que está dada por funciones regulares. Una *subrepresentación* es un subespacio lineal de V que es G-invariante. Una representación racional se dice *simple* si tiene exactamente dos subrepresentaciones y se dice *semisimple* si cualquier subrepresentación tiene un complemento G-invariante.

Ejemplo 5.14. Sean $\rho : G \to \mathrm{GL}(V)$ y $\sigma : G \to \mathrm{GL}(W)$ dos representaciones racionales de G. Entonces el espacio lineal $\mathrm{Hom}_k(V, W)$ es una representación racional, llamada la *representación* Hom mediante la acción lineal de G dada por $g \cdot \varphi := \sigma(g) \circ \varphi \circ \rho(g^{-1})$. $\mathrm{Hom}_k(V, W)^G$ está conformado por la funciones lineales $V \to W$ que son G-invariantes.

Ejemplo 5.15. Si $G \subset \mathrm{GL}(V)$, entonces $G \hookrightarrow \mathrm{GL}(V)$ es una representación racional.

Ejemplo 5.16. Sea $\rho : G \to \mathrm{GL}(V)$ una representación racional de un grupo algebraico afín G. Definamos una acción $\alpha : G \times \mathrm{Pol}(V) \to \mathrm{Pol}(V)$ mediante $g(f)(v) := f(g^{-1}v)$ para todo $v \in V$ y $f \in \mathrm{Pol}(V)$. Esta acción preserva la graduación de $\mathrm{Pol}(V)$. Si $f \in Pol_d(V)$ y $g \in G$, entonces para $\lambda \in k$, tenemos que $g(f)(\lambda v) = f(g^{-1}(\lambda v)) = f(\lambda g^{-1}(v)) = \lambda^d f(g^{-1}(v)) = \lambda^d g(f)(v)$. Por tanto, α es una acción llamada la *acción regular* de G sobre $\mathrm{Pol}(V)$.

Sea G un grupo algebraico afín actuando sobre una variedad algebraica afín $X = \mathrm{Specm}(A)$. Como $\mathcal{O}(G \times X) \cong \mathcal{O}(G) \otimes_k A$, entonces la acción de G sobre X puede ser descrita por el homomorfismo de coacción

$$\alpha^* : \mathcal{O}(G) \to \mathcal{O}(G) \otimes_k A,$$

satisfaciendo que

(i) La composición

$$A \xrightarrow{\alpha^*} \mathcal{O}(G) \otimes_k A \xrightarrow{\epsilon \otimes \mathrm{Id}_A} k \otimes_k A \xrightarrow{\sim} A$$

es igual a Id_A la identidad en A donde $\epsilon : \mathcal{O}(G) \to k$ es el homomorfismo de k-álgebra *coidentidad*, dado por $g \mapsto \epsilon(g) = g(1)$.

(ii) El siguiente diagrama es conmutativo:

$$\begin{tikzcd} A \arrow[r, "\alpha^*"] \arrow[d, "\alpha^*"'] & \mathcal{O}(G) \otimes_k A \arrow[d, "\mathrm{Id}_{\mathcal{O}(G)} \otimes \alpha^*"] \\ \mathcal{O}(G) \otimes_k A \arrow[r, "\beta^* \otimes \mathrm{Id}_A"] & \mathcal{O}(G) \otimes_k \mathcal{O}(G) \otimes_k A \end{tikzcd} \tag{5.1}$$

donde $\beta^* : \mathcal{O}(G) \to A \otimes_k \mathcal{O}(G)$ es el homomorfismo de k-álgebras inducido por el producto $\beta : G \times G \to G$ en G.

Para cualquier $a \in A$, tenemos que

$$\alpha^*(a) = \sum_i f_i \otimes a_i,$$

donde $f_i \in \mathcal{O}(G)$, $a_i \in A$. Cada elemento de $g \in G$ puede interpretarse como un homomorfismo $\mathcal{O}(G) \to k$, $f \mapsto f(g)$, y definamos

$$g(a) := (g \otimes \mathrm{Id}_A) \circ \alpha^*(a) = \sum_i f_i(g) a_i. \tag{5.2}$$

Un homomorfismo $\alpha : G \to \mathrm{Aut}(A)$ que surge de (5.2) es llamada una *acción racional* de G sobre una k-álgebra A.

Una importante propiedad de las acciones racionales es la siguiente.

Lema 5.17. *Para cualquier $a \in A$, el subespacio lineal de A generado por las traslaciones $g(a)$, $g \in G$, es de dimensión finita.*

Demostración:
Notar que en la ecuación (5.2), los a_i forman conjunto finito y de dicha ecuación se tiene que el subespacio lineal generado por los G-traslados de a está contenido en el subespacio generado por los a_i, con lo cual es subespacio lineal generado por los trasladados de a es de dimensión finita. ∎

Como una consecuencia, tenemos el siguiente resultado que puede pensarse como el análogo al Teorema de Cayley, que afirma que todo grupo finito de orden n es isomorfo a un subgrupo del grupo simétrico S_n.

Proposición 5.18. *Todo grupo algebraico afín G es un grupo algebraico lineal.*

Demostración:
Como el producto en G, $\mu : G \times G \to G$ es una acción de G en G, entonces $\mu^* : \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$ es una coacción y por tanto tenemos una acción racional de G sobre $\mathcal{O}(G)$,

$$\rho : G \to \mathrm{Aut}(\mathcal{O}(G)) \subset \mathrm{GL}(\mathcal{O}(G)),\ g \mapsto \rho_g,$$

donde

$$\rho_g(f)(k) = f(kg),$$

para todo $f \in \mathcal{O}(G), k \in G$. Luego, por la ecuación (5.2), tenemos que para todo $x \in G$,

$$x(f) = \rho(x) = \sum_j g_j(x) h_j,$$

donde $\mu^*(f) = \sum_j g_j \otimes h_j$. Sean $f_1, \ldots, f_n$ generadores de $\mathcal{O}(G)$ como k-álgebra y sea E el subespacio lineal de generado por los G-trasladados de los f_i's. Se sigue del Lema 5.17 que E es finito dimensional. Sin pérdida de generalidad, podemos suponer que los f_i son una base de E. Consideremos

$$\psi : G \to \mathrm{GL}(E),$$

dado por $x \mapsto \rho_x|_E$.

Para cada i, escribamos $\mu^*(f_i) := \sum_j g_j \otimes h_j \in \mathcal{O}(G) \otimes \mathcal{O}(G)$. Luego, por ecuación (5.2), tenemos que para todo $x \in G$,

$$x(f_i) = \sum_j g_j(x) h_j.$$

Lo cual implica que $h_j \in E$ y así podemos escribir

$$\mu^*(f_i) = \sum_j g_{ij} \otimes f_j,$$

para todo $i = 1, \ldots, n$.

Luego, la matriz de coordenadas de $\psi(x)$ con respecto a la base $f_i, \ldots, f_j$ es $g_{ij}(x)$. Por tanto, ψ es un morfismo de variedades. Notar que para todo $x \in G$, $f_i(x) = f_i(1_G \cdot x) = \rho_x(f_i)(1_G) = \sum_j g_{ij}(x) f_j(1_G)$, es decir,

$$f_i = \sum_j g_{ij} f_j(1_G). \tag{5.3}$$

Si $\psi(x) = 1_{\mathrm{GL}(E)}$, entonces $g_{ij}(x) = \delta_{ij}$ la delta de Kronecker, y por tanto $f_i(x) = f_i(1_G)$ lo cual implica que $x = 1_G$ ya que los f_i generan a $\mathcal{O}(G)$. Por la Proposición 2 , $G' := \mathrm{Im}(\psi)$ es un subgrupo cerrado de $\mathrm{GL}(E)$. Nos falta probar que ψ es un morfismo de variedades, i.e., $\psi^* : \mathcal{O}(G') \to \mathcal{O}(G)$ es un isomorfismo de k-álgebras. Como $\psi : G \to G'$ es sobreyectivo, tenemos que ψ^* es inyectivo. Sean t_{ij} las funciones coordenadas de $\mathrm{GL}(E)$ restringidas a G'. Tenemos entonces que $\psi^*(t_{ij}) = g_{ij}$ y por la ecuación (5.3), tenemos que los g_{ij} generan $\mathcal{O}(G)$, lo cual implica que ψ^* es sobreyectiva. ■

Ejemplo 5.19. Sea $G = \mathbb{G}_m$ actuando sobre una variedad algebraica afín $X = \mathrm{Specm}(A)$. Sea $\alpha^* : A \to \mathcal{O}(G) \otimes A = k[T, T^{-1}] \otimes A$ el correspondiente homomorfismo de coacción. Entonces para cada $a \in A$, podemos escribir

$$\alpha^*(a) = \sum_{i \in \mathbb{Z}} T^i \otimes a_i.$$

La función $p_i : A \to A$ dada por $a \mapsto a_i$ cumple en virtud del diagrama conmutativo (5.1) que p_i es una proyección para cada $i \in \mathbb{Z}$, *i.e.*, $p(a_i) = a_i$ y denotando por $A_i := p_i(A)$, tenemos que $A_i A_j \subset A_{i+j}$ y

$$A = \bigoplus_{i \in \mathbb{Z}} A_i. \tag{5.4}$$

Esto define una graduación en A. Recíprocamente, dada una graduación de A, podemos definir α^* mediante $\alpha^*(a) = \sum_{i \in \mathbb{Z}} T^i \otimes a_i$, donde a_i es la i-ésima parte graduada de a. Notar que esto da una interpretación geométrica de una graduación de una k-álgebra A, *i.e.*, una graduación sobre una k-álgebra A corresponde a una acción de $\mathbb{G}_m$ sobre la variedad $X = \mathrm{Specm}(A)$.

Si la graduación dada en (5.4) cumple que $A_i = \{0\}$ para todo $i < 0$, $A_0 = k$, entonces a dicha graduación se le llama una *graduación geométrica* y la acción inducida se dice que es una *buena* $\mathbb{G}_m$*-acción*. En este caso tendremos que el ideal $\mathfrak{m}_0 = \sum_{i>0} A_i$ es un ideal maximal pues al sumar el ideal de A generado por cualquier elemento de k nos da A, y por tanto corresponde a punto $p_0 \in X$ llamado el *vértice*.

El grupo $\mathbb{G}_a$ también tiene su interpretación. Dada una k-álgebra A y supongamos que $\mathrm{car}(k) = 0$. Una *derivación en* A es una función $D : A \to A$ tal que para cualesquiera $a, b \in A$,

1. $D(a + b) = D(a) + D(b)$
2. $D(ab) = aD(b) + bD(a)$.

El kernel de D es $\mathrm{Ker}\, D = \{b \in A : D(b) = 0\}$ y denotemos por $\mathrm{Der}(A)$ al conjunto de todas las derivaciones de A. Si B es un subanillo de A, definimos el conjunto $\mathrm{Der}_B(A) = \{D \in \mathrm{Der}(A) : D(a) = 0, \forall a \in B\}$. Una derivación $D \in \mathrm{Der}(A)$ es llamada *localmente nilpotente* si para cada $f \in A$ existe un entero positivo $n = n(f)$ tal que $D^n(f) = 0$. Denotamos por $\mathrm{DLN}(A)$ al conjunto de derivaciones localmente nilpotentes en A y para un subanillo B definamos $\mathrm{DLN}_B(A) := \mathrm{Der}_B(A) \cap \mathrm{DLN}(A)$.

Dado $D \in \mathrm{DLN}(A)$, la *función exponencial* determinada por D, $e^D : A \to A$ está dada por

$$e^D(f) := \sum_{i \geq 0} \frac{1}{i!} D^i(f).$$

Notar que como D es localmente nilpotente y $\mathrm{car}(k) = 0$, e^D está bien definida y satisface que $e^{D_1+D_2} = e_1^D e_2^D$. Tenemos también que para $D \in \mathrm{Der}_k(A)$, $fD \in \mathrm{DLN}(A)$ si y sólo si $D \in \mathrm{DLN}(A)$ y $f \in \mathrm{Ker}(D)$ y además la derivada formal $\frac{d}{dt} : B[t] \to B[t]$ donde $t \in A$ es trascendente sobre el subanillo $B \subset A$, cumple que $\frac{d}{dt} \in \mathrm{DLN}_B(B[t])$ y $\mathrm{Ker}\left(\frac{d}{dt}\right) = B$ y también para $D \in \mathrm{DLN}(A)$ se tiene que $D \in \mathrm{Aut}(A)$, (cf. [18, pp. 24-25]). Luego, dada $D \in \mathrm{DLN}(A)$, obtenemos un isomorfismo de grupos $\eta : (\mathrm{Ker}(D), +) \to \mathrm{Aut}(A)$ dado por

$$\eta(a) = e^{aD},$$

el cual es inyectivo si $D \neq 0$.

Dado $H \subset \mathrm{Ker}(D)$ tenemos que $H \cong \mathbb{G}_a$ si y sólo si $H = kf$ para algún $f \in \mathrm{Ker}(D)$ no nulo y por tanto, en este caso, tenemos una representación

$$\eta|_H : \mathbb{G}_a \to \mathrm{Aut}(A),$$

i.e., una derivación localmente nilpotente corresponde a una acción de $\mathbb{G}_a$ sobre $X = \mathrm{Specm}(A)$.

Recíprocamente, dada una acción $\alpha : \mathbb{G}_a \times X \to X$, podemos definir una derivación localmente nilpotente dada por la composición

$$A \xrightarrow{\quad \alpha^* \quad} A[t] \xrightarrow{\quad \frac{d}{dt} \quad} A[t] \xrightarrow{\quad \mathrm{eval} \quad} A,$$

donde eval es el homomorfismo evaluación en $t = 0$. Luego, $\delta := \mathrm{eval} \circ \frac{d}{dt} \circ \alpha^* \in \mathrm{DLN}(A)$ (cf. [18, Proposición 1.36]).

Explicamos la noción de grupos geométricamente reductivos.

Definición 5.20. Un grupo algebraico lineal G es llamado *linealmente reductivo* si para cualquier representación racional $\rho : G \to \mathrm{GL}(V)$ y cualquier $v \in V^G$ no nulo, existe una función lineal G-invariante f sobre V tal que $f(v) \neq 0$.

Proposición 5.21. *Para cualquier grupo algebraico lineal G, son equivalentes*

(i) *El grupo G es linealmente reductivo.*
(ii) *Cualquier representación racional de G es semisimple.*
(iii) *Para cualquier función sobreyectiva G-invariante $\varphi : V \to W$ de representaciones racionales, la función inducida de subespacios de invariantes es sobreyectiva.*

Demostración:
(i) $\Rightarrow$ *(ii)*
Sea $U \subset V$ una subrepresentación propia. Como cada subespacio complementario de U es la imagen del algún

homomorfismo $\sigma : V/U \to V$ tal que $\pi \circ \sigma = \mathrm{Id}_{V/U}$ donde $\pi : V \to V/U$ es la proyección canónica y si σ es G-invariante, entonces la imagen es G-invariante. Luego, basta probar que existe un homomorfismo $\tau : V/U \to V$ G-invariante tal que $\pi \circ \tau = \mathrm{Id}_{V/U}$.

Sea $\sigma : V/U \to V$ un homomorfismo tal que $\pi \circ \sigma = \mathrm{Id}_{V/U}$. Sea $T := \mathrm{Vect}_k(G_\sigma)$ donde $G_\sigma := \{g(\sigma) : g \in G\}$ la subrepresentación de $\mathrm{Hom}(V/U, V)$ (cf. Ejemplo 5.14) generada por la *órbita* de σ y $T' \subset T$ el subespacio generado por $\{g(\sigma) - \sigma : g \in G\}$.

Para cualquier $g \in G$ y cualquier $v \in V$ tenemos

$$\begin{aligned} \pi \circ (g(\sigma) - \sigma)(v + U) &= \pi(g\sigma(g^{-1}v + U)) - \pi(\sigma(v + U)) \\ &= g\pi(\sigma(g^{-1}v + U)) - \pi(\sigma(v + U)) \\ &= gg^{-1}v - v + U \\ &= U. \end{aligned}$$

Luego, $T' \subset \mathrm{Ker}(\pi)$. Si $\sigma \in T'$, entonces $\mathrm{Id}_{V/U} = \pi \circ \sigma = 0$ pero esto es imposible ya que $U \subsetneq V$. Por tanto, $\sigma \in T \setminus T'$ y $T = T' + \mathrm{Vect}_k(\sigma)$. Escogemos una función lineal $\ell : T \to k$ tal que $\ell|_{T'} = 0$. Luego para todo $v \in T$, $(g(\ell) - \ell)(v) = 0$, lo cual implica que ℓ es G-invariante. Como G es linealmente reductivo, existe $\tau' \in T^G = (T^{\vee\vee})^G$ tal que $\ell(\tau') \neq 0$. Así, $\tau' \notin T'$ y por tanto, $\tau' = a\sigma + \sum_{g \in G} a_g(g(\sigma) - \sigma)$ para algunos $a, a_\sigma \in k$ con $a \neq 0$. Tomemos $\tau := a^{-1}\tau'$. Tenemos que τ es G-invariante y además tomando $b_g = a^{-1}a_g$, tenemos

$$\pi \circ \tau = \tau \circ \left(\sigma + \sum_{g \in G} b_g(g(\sigma) - \sigma) \right) = \pi \circ \sigma = \mathrm{Id}_{V/U}.$$

(ii) $\Rightarrow$ *(iii)*
Sea $\varphi : V \to W$ una función lineal sobreyectiva G-invariante. Como V es semisimple, existe un subespacio lineal complementario G-invariante V' del $\mathrm{Ker}(\varphi) \subset V$. La representación V' es isomorfa a W mediante una función G-invariante, por tanto, el subespacio de invariantes V'^G es isomorfo a W^G mediante una función G-invariante. Como $V'^G \subset V^G$, entonces, tenemos que existe una función G-invariante sobreyectiva de V^G a W^G.

(iii) $\Rightarrow$ *(i)*
Consideremos la acción trivial de G sobre k y sea $v \in V^G \setminus \{0\}$. Entonces la evaluación $\mathrm{eval}_v : V^\vee \to k$ es lineal, sobreyectiva y G-equivariante. Por hipótesis, $\mathrm{eval}_v|_{(V^\vee)^G} : (V^\vee)^G \to k^G = k$ es sobreyectivo. Tomando una preimagen $\ell \in (V^\vee)^G$ de $1 \in k$ tenemos que $\ell(v) = \mathrm{eval}_v(\ell) = 1$, por tanto G es linealmente reductivo. ■

Lema 5.22. *Un grupo algebraico es linealmente reductivo si y sólo si para cualquier representación racional $\rho : G \to V$ y para cualquier función lineal G-invaraínte $f : V \to k$, existe un $w \in V^G$ tal que $f(w) \neq 0$*

Demostración:
La equivalencia se obtiene reemplazando V por su dual $V^\vee$ y notando que el espacio lineal de funciones G-invariantes sobre $V^\vee$, $\mathrm{Hom}_G(V^\vee, k) = \mathrm{Hom}_G(V, k) = V^G$ con G actuando trivialmente sobre k. ■

Ejemplo 5.23. Si G es un grupo finito tal que $\mathrm{car}(k) \nmid |G|$. Entonces G es linealmente reductivo.

Demostración:
Sea $\rho : G \to \mathrm{GL}(V)$ una representación racional, sea $v \in V^G \setminus \{0\}$. Luego, existe un función lineal $\ell : V \to k$ tal que $\ell(v) \neq 0$. Definamos $f : V \to k$ mediante $u \mapsto f(u) := \ell\left(\frac{1}{|G|}\sum_{g \in G} \rho(g)(u)\right)$. Así, f es lineal, G-invariante y $f(v) = \ell\left(\frac{1}{|G|}\sum_{g \in G} \rho(g)(v)\right)$ y como $v \in V^G$, tenemos que $f(v) = \ell(v) \neq 0$. Con lo cual, G es reductivo. ■

Ejemplo 5.24. $\mathbb{G}_m$ es linealmente reductivo.

Demostración:
Sea $\rho : G \to \mathrm{GL}(V)$ una representación racional, sea $v \in V^{\mathbb{G}_m} \setminus \{0\}$. Definamos $f : V \to k$ mediante $f(v) = 1$ y $f(u) = 0$ para todo $u \in V$ con $u \neq v$. Luego, f es lineal y $f(v) \neq 0$. En el ejemplo 5.19, vimos que $\mathbb{G}_m$ induce

una graduación de $V = \bigoplus_{i\in\mathbb{Z}} V_i$ donde $V_i = \{u \in V : \alpha^*(u) = \sum_j T^j \otimes v_j$ con $v_i = u_i\}$, de acá que $V^{\mathbb{G}_m} = V_0$ y por tanto, f es $\mathbb{G}_m$-invariante y así $\mathbb{G}_m$ es linealmente reductivo. ■

Ejemplo 5.25. El producto directo de grupos algebraicos linealmente reductivos es un grupo linealmente reductivo, en consecuencia el toro algebraico $\mathbb{G}_m^n$ es linealmente reductivo.

Ejemplo 5.26. Si $\mathrm{car}(k) = 0$, entonces $\mathrm{SL}_2(k)$ es linealmente reductivo.

Demostración:
Como $\mathbb{G}_m$ es linealmente reductivo, y $\mathbb{G}_m \cong T \subset \mathrm{SL}_2(k)$ donde (T son las matrices diagonales), podemos encotrar una función lineal T-invariante $e : V \to k$ tal que $e(w) = 1$ y podemos usarla para definir una función

$$\varphi : V \to \mathcal{O}(\mathrm{SL}_2(k))$$

dada por $\varphi(x)(g) = e(g(x))$ para todo $x \in V$ y todo $g \in \mathrm{SL}_2(k)$.
Equivalentemente, φ es la composición del homomorfismo coacción con $e \otimes \mathrm{Id}_{\mathcal{O}(\mathrm{SL}_2(k))}$,

$$V \xrightarrow{\alpha^*} V \otimes_k \mathcal{O}(\mathrm{SL}_2(k)) \xrightarrow{e\otimes \mathrm{Id}_{\mathcal{O}(\mathrm{SL}_2(k))}} k \otimes_k \mathcal{O}(\mathrm{SL}_2(k)) \xrightarrow{\sim} \mathcal{O}(\mathrm{SL}_2(k)).$$

Tenemos que

$$\mathcal{O}(\mathrm{SL}_2(V)) = k[x, y, z, t]/(xt - yz - 1),$$

Por tanto, tenemos acciones de $\mathrm{SL}_2(k)$ por la derecha y por la izquierda. Consideremos la acción derecha de T sobre $\mathcal{O}(\mathrm{SL}_2(k))$ y la acción izquierda de $\mathrm{SL}_2(k)$ sobre $\mathcal{O}(\mathrm{SL}_2(k))^T$. Como para cualquier $\begin{pmatrix} q & 0 \\ 0 & q^{-1}\end{pmatrix} \in \mathrm{SL}_2(k)$, tenemos que

$$\begin{pmatrix} x & y \\ z & t\end{pmatrix}\begin{pmatrix} q & 0 \\ 0 & q^{-1}\end{pmatrix} = \begin{pmatrix} qx & q^{-1}y \\ qz & q^{-1}t\end{pmatrix}$$

tenemos que

$$k[x, y, z, t]^T = k[xy, xt, zy, zt]$$

y como el polinomio $xt - yz - 1$ es T-invariante, tenemos que

$$\mathcal{O}(\mathrm{SL}_2(k))^T = k[xy, xt, zy, zt]/(xt - yz - 1).$$

Por tanto, tenemos que para toda $x \in V$, la función $\varphi(x)$ es invariante bajo la acción derecha de T, esto es $\varphi(V) \subset \mathcal{O}(\mathrm{SL}_2(k))^T$, φ es un homomorfismo de representaciones de $\mathrm{SL}_2(k)$ y $\varphi(w) = 1_{\mathcal{O}(\mathrm{SL}_2(k))}$.
Demos otra descripción de $\mathcal{O}(\mathrm{SL}_2(k))^T$. Para cada $n \in \mathbb{N}$, sea R_n el conjunto de funciones racionales en variables u, v

$$R_n = \left\{ \frac{f(u, v)}{(u - v)^n} : \deg_u f(u, v) \le n, \deg_v f(u, v) \le n \right\}.$$

Este es un espacio vectorial de dimensión $(n + 1)^2$ y $R_n \subset R_{n+1}$. La unión

$$R := \bigcup_{n\ge 0} R_n$$

es una subálgebra de $k[u, v, 1/(u - v)] \subset k(u, v)$, mientras que el cuerpo $k(u, v)$ es una representación de $\mathrm{SL}_2(k)$ mediante a $g = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{SL}_2(k)$, $g \mapsto \rho(g)$ con $\rho(g)(u) = \frac{au+b}{cu+d}, \rho(g)(v) = \frac{av+b}{cv+d}$.
Con esta acción

$$u - v \mapsto \frac{au + b}{cu + d} - \frac{av + b}{cv + d} = \frac{u - v}{(cu + d)(cv + d)},$$

con lo cual $R_n \subset k(u, v)$ es una subrepresentación.

La función $\sigma : R \to k[xy, xt, zy, zt]$ dado por $\sigma(u) = \frac{x}{z}, \sigma(v) = \frac{y}{t}, \sigma(1/(u - v)) = zt$ induce un isomorfismo $R \cong \mathcal{O}(\mathrm{SL}_2(k))^T = k[xy, xt, zy, zt]/(xt - yz - 1)$.

Tenemos que la imagen de $\varphi : V \to \mathcal{O}(\mathrm{SL}_2(k)) \cong R$ está contenida en un espacio vectorial de dimensión finita R_n para algún n. Por definición, un elemento general es de la forma $\frac{f(u,v)}{(u-v)}$ donde $f(u, v) = \sum_{i,j=0}^n a_{ij} u^i v^j$.

El determinante de la matriz de coeficientes (a_{ij}) define una función $\det : R_n \to k$ homogénea de grado $n+1$ $\mathrm{SL}_2(k)$-invariante. La función constante

$$1 = \frac{(u-v)^n}{(1-v)^n} = \frac{u^n - nu^{n-1} + \binom{n}{2}u^{n-2}v^2 - \cdots + (-v)^n}{(u-v)^n} \in R_n \subset \mathcal{O}(\mathrm{SL}_2(k))^T,$$

luego

$$\det(1) = \det \begin{pmatrix} & & & & 1 \\ & & & -n & \\ & & \binom{n}{2} & & \\ & \cdots & & & \\ (-1)^{n-1}n & & & & \\ (-1)^n & & & & \end{pmatrix} = \prod_{i=0}^{n} \binom{n}{i}.$$

Sea $h : R_n \to k$ la función lineal $\mathrm{SL}_2(k)$-invariante definida por

$$\frac{f(u,v)}{(u-v)^n} \mapsto \sum_{i=0}^{n} (-1)^{n-i} a_{i,n-i} \prod_{j\neq i} \binom{n}{j}.$$

Luego,

$$h(1) = (-1)^{(n+1)} \prod_{j=0}^{n} \binom{n}{j} \neq 0.$$

Por tanto,

$$f := h \circ \varphi : V \to k$$

es una función lineal $\mathrm{SL}_2(k)$-invariante y $f(w) = h(\varphi(w)) = h(1) \neq 0$. Con lo cual $\mathrm{SL}_2(k)$ es linealmente reductivo. ■

El siguiente ejemplo aparece en la introducción de [6],

Ejemplo 5.27. Si $\mathrm{car}(k) = 2$, entonces $\mathrm{SL}_2(k)$ no es linealmente reductivo.

Ejemplo 5.28. $\mathbb{G}_a$ no es linealmente reductivo.

Demostración:
Consideremos la representación $\rho : \mathbb{G}_a \to \mathbb{A}^2$ dada por

$$\rho(g) = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}.$$

Si ρ fuera semisimple, existiría una base en $\mathbb{A}^2$ donde en dicha base

$$\rho(g) = \begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix}.$$

Con lo cual, ρ no puede ser semisimple. ■

Definición 5.29. Un grupo algebraico lineal G se dice *geométricamente reductivo* si para cualquier representación racional $\rho : G \to \mathrm{GL}(V)$ y para cualquier $v \in V^G$ no nulo, existe un polinomio homogéneo f sobre V que es G-invariante y tal que $f(v) \neq 0$.

Ejemplo 5.30. Cualquier grupo linealmente reductivo es geométricamente reductivo.

Ejemplo 5.31. Si G es un grupo finito, entonces G es geométricamente reductivo.

Demostración:
Sea G un grupo finito y V una representación racional de G. Sea $v \in V^G$ no nulo. Tomemos una función lineal G-invariante $\ell \in V^\vee$ tal que $\ell(v) \neq 0$.

Sea $f := \prod_{g\in G} g(\ell)$, luego f es un polinomio homogéneo de grado $|G|$ sobre V y

$$f(v) = \prod_{g\in G} g(\ell)(v) = \prod_{g\in G} \ell(g^{-1}v) = \ell(v)^{|G|} \neq 0.$$

Con lo cual, G es geométricamente reductivo. ■

Proposición 5.32. *Si* $\operatorname{car}(k) = 0$*, entonces un grupo algebraico lineal es geométricamente reductivo si y sólo si es linealmente reductivo.*

Demostración:
Si es linealmente reductivo, es geométricamente reductivo. Recíprocamente, sea $\rho : G \to \mathrm{GL}_n(V)$ una representación racional que induce una acción de G sobre V. Sea $w \in V^G$ no nulo. Por ser G geométricamente reductivo, existe un polinomio G-invariante homogéneo f de grado d tal que $f(w) \neq 0$.

Para cada $v_1, \ldots, v_d \in V$ y $\lambda_1, \ldots, \lambda_d \in k$ tenemos que

$$f(\lambda_1 v_1 + \cdots + \lambda_d v_d) = \sum_{i_1+\ldots+i_d=d} \lambda_1^{i_1} \cdots \lambda_d^{i_d} f_{i_1,\ldots,i_d}(v_1, \ldots, v_d),$$

donde cada función $f_{i_1,\ldots,i_d} : V^d \to k$, es multihomogéna de multigrado $(i_1, \ldots, i_d)$.

Poniendo $v_1 = \ldots = v_d = v$, obtenemos

$$\begin{aligned}\sum_{i_1+\ldots+i_d=d} \lambda_1^{i_1} \cdots \lambda_d^{i_d} f_{i_1,\ldots,i_d}(v, \ldots, v) &= \sum_{i_1+\ldots+i_d=d} f_{i_1,\ldots,i_d}(\lambda_1 v, \ldots, \lambda_d v)\\ &= f(\lambda_1 v + \ldots + \lambda_d v)\\ &= (\lambda_1 + \ldots + \lambda_d)^d f(v)\end{aligned}$$

Por el Teorema del multinomio,

$$(\lambda_1 + \ldots + \lambda_d)^d = \sum_{k_1+\ldots+k_d=d} \binom{n}{k_1, \ldots, k_d} x_1^{k_1} \ldots x_d^{k_d},$$

con

$$\binom{n}{k_1, \ldots, k_d} = \frac{d!}{k_1! \cdots k_d!}.$$

Así, tenemos que

$$\begin{aligned}\sum_{i_1+\ldots+i_d=d} \lambda_1^{i_1} \cdots \lambda_d^{i_d} f_{i_1,\ldots,i_d}(v, \ldots, v) &= \sum_{k_1+\ldots+k_d=d} \binom{n}{k_1, \ldots, k_d} x_1^{k_1} \ldots x_d^{k_d}\\ &= (\lambda_1^d + \ldots + d!\lambda_1 \cdots \lambda_d) f(v).\end{aligned}$$

Comparando los coeficientes de los monomios $\lambda_1^{i_1} \cdots \lambda_d^{i_d}$ tenemos que

$$f_{1,\ldots,1}(v, \ldots, v) = d! f(v),$$

para todo $v \in V$. Definamos $\ell : V \to k$ mediante $\ell(v) = f_{1,\ldots,1}(v, w, \ldots, w)$. Como $f_{1,\ldots,1}$ es multilineal, tenemos que ℓ es lineal. Como f es G-invariante y la acción respecta los multigrados, tenemos que la función $f_{1,\ldots,1}$ es G-invariante, *i.e.*, $g(f_{1,\ldots,1})(v_1, \ldots, v_d) = f_{1,\ldots,1}(g^{-1}v_1, \ldots, g^{-1}v_d) = f_{1,\ldots,1}(v_1, \ldots, v_d)$. La G- invarianza de w y $f_{1,\ldots,1}$ implica que ℓ es G-invariante y tenemos que

$$\ell(w) = d! f(w) \neq 0.$$

Luego, G es linealmente reductivo. ∎

Definición 5.33. Sea $\rho : G \to \mathrm{GL}(V)$ una representación racional de un grupo algebraico G. Diremos que $g \in G$ es

1. **Nilpotente** si $\rho(g)^n = 0$ para algún entero no negativo n.
2. **Unipotente** si $\rho(g) - \mathrm{Id}_V$ es nilpotente. Se dice que G es unipotente si todos sus elementos son unipotentes.

Definición 5.34. Un grupo algebraico lineal T es llamado un *toro algebraico* (o simplemente un toro) si es isomorfo a $\mathbb{G}_m^n$ para algún $n \in \mathbb{Z}^+$. Un grupo algebraico es *resoluble* si admite un serie de composición de subgrupos normales cerrados cuyos cocientes sucesivos forman un grupo abeliano.

Cualquier grupo algebraico G posee un único subgrupo resoluble normal $S \subset G$ el cual es automáticamente un cerrado de Zariski. Su componente identidad $R(G) := S^0$ es entonces un subgrupo de G normal, conexo, resoluble maximal llamado el *radical de G*.
Un grupo G es llamado **reductivo** si su radical es un toro. Un grupo algebraico lineal conexo G es llamado

semisimple si su radical es trivial.

Observación 5.35. Si G es linealmente reductivo, entonces G es geométricamente reductivo, tomando $d = 1$

Ejemplo 5.36. Si $\mathrm{car}(k) = p > 0$, entonces $\mathrm{SL}_2(k)$ es geométricamente reductivo.

Demostración:
En la prueba del Ejemplo 5.26, podemos tomar $n = p^\nu - 1$ para ν suficientemente grande. Luego

$$(u-v)^n = \frac{(u-v)^{p^\nu}}{u-v} = \frac{u^{p^\nu} - v^{p^\nu}}{u-v} = \sum_{i=0} u^{n-i}v^i.$$

En particular, la función $\det : R_n \to k$ toma el valor 1 en $1 \in R_n$. Así en este caso la composición

$$f := \det \circ \varphi : V \to k$$

es un polinomio homogéneo $\mathrm{SL}_2(k)$-invariante y $f(w) = \det(\varphi(w)) = \det(1) = 1 \neq 0$. ■

Como consecuencia de los ejemplos 5.26 y 5.36 se tiene que

Ejemplo 5.37. SL_2 es geométricamente reductivo en cualquier característica

Observación 5.38. Por los ejemplos 5.27 y 5.37, tenemos que hay grupos geométricamente reductivos que no son linealmente reductivos.

Ejemplo 5.39. $\mathbb{G}_a$ no es geométricamente reductivo.

Teorema 5.40. *(Nagata-Miyata (1963)) Si G es un grupo geométricamente reductivo, entonces es reductivo.*

Este teorema fue probado en [7] usando la noción de grupos semi-reductivos la cual introdujo en [8] y que es equivalente a la noción de grupos geométricamente reductivos.

Teorema 5.41. *(Conjetura de Munford, Teorema de Haboush (1975)) cf. [4] Si G es reductivo, entonces G es geométricamente reductivo.*

6. Teorema de Nagata

Necesitaremos el siguiente resultado del álgebra conmutativa.

Lema 6.1. *Sean $R \subset S$ k-álgebras tales que S es integral sobre R. Si S es finitamente generada sobre k, entonces R es finitamente generada sobre k.*

Demostración:
Sean $b_1, \ldots, b_n$ generadores de S como k-álgebra. Como S es integral sobre R, para cada $i = 1, \ldots, n$, existe $f_i \in R[X]$ mónico tal que $f_i(b_i) = 0$ y sea $A \subset R$ la k-álgebra finitamente generada por los coeficientes de todos los f_i. Luego, tendremos que los b_i generan a S como una A-álgebra y S es integral sobre A por tanto, S es A-módulo finitamente generado y en como A es un k-módulo noetheriano al igual que S, entonces S es un A-módulo noetheriano. Luego, R debe ser un A-módulo finitamente generado y por tanto es finitamente generado sobre k como k-álgebra. ■

Lema 6.2. *Sea $A = \bigoplus_{d \geq 0} A_d$ una k-álgebra graduada con $A_0 = k$. Entonces el ideal $A_+ := \sum_{d>0} A_d$ es finitamente generado si y sólo si A es finitamente generada como k-álgebra.*

Demostración:
Supongamos que A es finitamente generada sobre k y sean $a_1, \ldots, a_n \in A_+$ un conjunto de generadores e $I = (a_1, \ldots, a_n)$ el ideal de A generado por los a_i. Sea $x \in A_+$. Escribamos $x = \sum_{i \in J} \lambda_i a^{i_1} \ldots a_1^{i_n}$ donde J es un subconjunto finito de los enteros no negativos y los $i_k = i_k(x)$ con $\lambda_i \in k$. Así, cada sumando de x debe contener al menos una potencia de alguna de las a_i con lo cual $x \in I$ con lo cual $A_+ \subseteq I$ y la otra inclusión es trivial.

Recíprocamente, supongamos que $A_+ = (a_1, \ldots, a_n)$ y sea $x \in A$. Escribamos $x = x_+ + x_0$ para ciertos $x_+ \in A_+$ y $x_0 \in k$. Tenemos que x_+ es una combinación lineal sobre A de los a_i digamos $x = \sum_{i=1}^n x_i a_i$ con $x_i \in A$. Como los a_i tienen grado positivo, tenemos que los x_i tienen grado estrictamente menor que x_+. Por inducción sobre el grado, podemos asumir que x_+ es una combinación lineal sobre k de los a_i y así x es un polinomio lineal en las a_i con coeficientes en k. Por tanto, A es finitamente generada. ■

Lema 6.3. *Sea G un grupo algebraico geométricamente reductivo actuando racionalmente sobre una k-álgebra A dejando invariante a un ideal I de A. Considere $A^G/I\cap A^G$ con una sub álgebra de $(A/I)^G$ mediante el homomorfismo inyectivo inducido por la inclusión $A^G\subset A$, (i.e., $A^G/I\cap A^G\ni a+(U\cap A^G)\mapsto a+I\in(A/I)^G$). Entonces para cualquier $a\in(A/I)^G$, existe $d>0$ tal que $a^d\in A^G/I\cap A^G$. Más aún, si G es linealmente reductivo, entonces se puede tomar $d=1$.*

Demostración:
Sea $\overline{a}$ un elemento en $(A/I)^G$ no nulo y a un representante de $\overline{a}$ en A. Sea $\mu^*(a)=\sum_i\alpha_i\otimes a_i$. Sea V un el subespacio lineal G-invariante de A generado por los G trasladados de a. Por el Lema 5.17, V es de dimensión finita y está contenido en el subespacio generado por los a_i. Sea $v=g(a)\in V$ para algún $g\in G$. Como $\overline{a}\in(A/I))^G$, entonces $\overline{g(a)-a}=g(\overline{a})-\overline{a}=I\cap A^G$. Luego, $g(a)-a\in I\cap A^G$.

Sea $W=I\cap V$ y sean $v_2,\ldots,a_n$ una base de W. Como $\overline{a}\neq 0$, entonces $a\notin W$ y $v=g(a)=a+g(a)-a=a+w$ con $w=g(a)-a\in W$. Por tanto todo elemento $v\in V$ pertenece a $W+\mathrm{Vect}_k\{a\}$ con lo cual $\{v_1,\ldots,v_n\}$ con $v_1=a$ es una base para V y así cualquier elemento $v\in V$ se puede escribir como

$$v=\lambda a+w$$

para algún $\lambda\in k$ y algún $w\in W$.

Sea $\ell:V\to k$ la función lineal dada por $v=\lambda a+w\mapsto\lambda$. Entonces tendremos que $\ell\in V^\vee$ y que para todo $g\in G$,

$$g(v)=\ell(g(v))a+w'$$

para algún $w'\in W$ y

$$g(v)=g(\ell(v)a+w)=\ell(v)g(a)+g(w)=\ell(v)a+w''=\ell(g(v))a+w'$$

con $w''=g(w)$. Por tanto, $\ell(g(v))=\ell(v)$ y $w''=w'$ y esto implica en particular que la función lineal $\ell:V\to k$ es G-invariante y G actúa linealmente sobre $V^\vee$. Como tenemos que $\{v_1,\ldots,v_n\}$ es una base de V, podemos identificar a $V^\vee$ con A^n mediante la base dual y de esta forma $\ell=(1,0,\ldots,0)\in A^n$. Por definición de ser geométricamente reductivo, podemos encontrar un polinomio homogéneo G-invariante $F(Z_1,\ldots,Z_n)$ de grado d tal que $F(1,0,\ldots,0)\neq 0$ y por tanto, podemos asumir que $F=Z_1^d+\cdots$.. Con lo cual, podemos identificar v_i con el polinomio lineal Z_i y así $(F-Z_i^d)(v_1,\ldots,v_n)=F(v_1,\ldots,v_n)-a^d$ pertenece al ideal J de A generado por $v_2,\ldots,v_n$. Como cada generador de J pertenece a $W\subset I$, tenemos que $a^d\equiv F(v_1,\ldots,v_n)$ mód I. Como F es G-invariante, entonces $F(v_1,\ldots,v_n)\in A^G$, luego $a^d\in A^G/I\cap A^G$. Además, si G es linealmente reductivo, entonces F se puede escoger lineal sobre V en consecuencia $d=1$. ■

Observación 6.4. Notar que esto implica también que $(A/I)^G$ es integral sobre $A^G/I\cap A^G$.

Necesitaremos el siguiente teorema del álgebra conmutativa que enunciamos sin demostración (ver [19, Corolario 13.13, p. 293]).

Teorema 6.5. *(Emmy Noether) Para cualquier k-álgebra A finitamente generada sin divisores de cero, la clausura integral de A en una extensión de cuerpos finita del cuerpo de fracciones de A es un A-módulo finitamente generado.*

Teorema 6.6. *(Teorema de Nagata) Sea G un grupo geométricamente reductivo actuando sobre una variedad afín* $\mathrm{Specm}(A)$*. Entonces A^G es una k-álgebra finitamente generada.*

Demostración:
Paso 1:
Por inducción noetheriana, podemos asumir que para cualquier ideal I de A no trivial que es G-invariante, se tiene que $(A/I)^G$ es finitamente generada.

Paso 2:
Asumamos primero que $A=\sum_{n\geq 0}A_n$ es k-álgebra geométricamente graduada (*i.e.*, $A_0=k$) y que la acción de G preserva la graduación. Por ejemplo, A podría ser una álgebra polinomial sobre la cual G actúa linealmente. La subálgebra A^G hereda esta graduación ya que $A_0=k$ es G-invariante. Supongamos que A^G es un dominio entero y tomemos un elemento homogéneo $f\in A^G$ de grado positivo.

Afirmamos que $fA\cap A^G = fA^G$. En efecto, si $y \in fA\cap A^G$, entonces $y = fx$ con $x \in A$ y tal que $g(fx) = fx$. Luego,

$$g(fx) - fx = f(g(x) - x) = 0$$

y por estar en un dominio entero tenemos que $g(x) = x$ con lo cual $x \in A^G$ y así $y = fx \in fA^G$. Recíprocamente si $y \in fA^G$, entonces $y = fx$ con $x \in A^G$ y por tanto, $g(xf) = xf$ y así $y \in fA \cap A^G$. Tenemos entonces que $(A/fA)^G$ es finitamente generada y por Observación 6.4 tenemos que $(A/fA)^G$ es integral sobre $A^G/fA^G = A^G/fA \cap A^G$ y en consecuencia A^G/fA^G es finitamente generada y como A^G es graduado y fA^G es un ideal graduado, tenemos que A^G/fA^G es una k-álgebra graduada. Entonces, por el Lema 6.2, su ideal maximal $(A^G/fA^G)_+$ generado por los elementos de grado positivo, es finitamente generado. Tomemos un conjunto finito de representantes en A^G de los generadores del ideal $(A^G/fA^G)_+$ y agreguemos f a este conjunto, de esta forma obtenemos un conjunto de generadores para el ideal $(A^G)_+$ en A^G. Usando inducción sobre el grado como en la segunda demostración del Teorema 6.7, obtenemos que A^G es una k-álgebra finitamente generada.

Asumamos ahora que A^G contiene un divisor de cero f. El ideal fA y el ideal aniquilador de f definido por $R = (0 : f) = \{a \in A : fa = 0\}$, son ideales G invariantes no nulos. Luego, como antes, $A^G/fA \cap A^G$ y $A^G/R\cap A^G$ son finitamente generadas. Sea B el subanillo de A^G generado por los generadores de estas dos álgebras y por tanto existen homomorfismos sobreyectivos $B \to A^G/fA \cap A^G$ y $B \to A^G/r \cap A^G$. Por Observación 6.4, $(A/R)^G$ es integral sobre $B/R\cap B$ y por tanto $(A/R)^G$ es un $B/R\cap B$ finitamente generado. Sean $c_1, \dots, c_n$ representantes en A de los generadores de $(A/R)^G$ como un $B/R\cap A^G$ módulo. Como $c_i + R \in (A/R)^G$, tenemos que para todo $g \in G$, se cumple que $g(c_i) + R = c_i + R$, entonces $g(c_i) - c_i \in R$ y por tanto, $f(g(c_i) - c_i)) = 0$ y así $fc_i \in A^G$. Afirmamos que $A^G = B[fc_i, \dots, fc_n]$. En efecto, claramente $B[fc_i, \dots, fc_n] \subset A^G$. Por otra parte, si $a \in A^G$, como B se mapea sobreyectivamente a $A^G/fA \cap A^G$, existe $b \in B$ tal que $a - b \in fA$. Luego, $a - b = fr$ con $r \in A$ y $g(fr) = fr$. Por tanto, $g(r + R) = r + R$ y así $r + R \in (A/R)^G$. Luego, por definición de los c_i, $r + R \in \sum_i B/R \cap B(c_i + R)$ y esto implica $r - \sum_i b_i c_i \in R \cap B$ con los $b_i \in B \cap R$ y así $r = \sum_i b_i c_i + b'$ con $b' \in R \cap B$. Luego, $a = b + fr = b + f(\sum_i b_i c_i + b') \in B[fc_1, \dots, fc_n]$.
Con esto probamos el caso graduado.

Paso 3:
Consideremos ahora el caso general. Sean $t_1, \dots, t_n$ los generadores de A. Considere el k-espacio vectorial $V \subset A$ generado por los G-trasladados de los t_i que por el Lema 5.17, es finito dimensional. Sin pérdida de generalidad podemos asumir que $(t_1, \dots, t_n)$ son una base dicho espacio. Sea $S = k[T_1, \dots, T_n]$ y $\varphi : S \to A$, dado por $T_i \mapsto t_i$. El grupo G actúa sobre S mediante $g(T_i) = \sum_j \alpha_{ij} T_j$, donde $g(t_i) = \sum_j \alpha_{ij} t_j$. Sea $I = \mathrm{Ker}(\varphi)$, así, I es G-invariante y como $A \cong S/I$, entonces $A^G = (S/I)^G$ y así por Observación 6.4, A^G es integral sobre $S^G/I \cap S^G$.

Notar que en la prueba del caso cuando A es una k-álgebra graduada, bajo la suposición de que A^G tenía al menos un divisor de cero, la hipótesis de ser graduada no se usó, por tanto, también es válido el mismo argumento en el caso no graduado. Asumamos entonces que A^G no tiene divisores de cero. Por Teorema 6.5, tenemos que la clausura entera de R de $S^G/I \cap S^G$ en el cuepo de fracciones $\mathrm{Frac}(A^G)$ de A^G es una k-álgebra finitamente generada siempre que $\mathrm{Frac}(A^G)$ sea una extensión finta del cuerpo de fracciones de $S^G/I\cap S^G$. Como R es integral sobre A^G, por el Lema 6.1, esto implicaría que A^G es finitamente generada. Por tanto, es suficiente mostrar que el cuerpo de fracciones $\mathrm{Frac}(A^G)$ es una extensión finita del cuerpo de fracciones de $S^G/I \cap S^G$. Como A^G es integral sobre $S^G/I\cap S^G$, entonces tenemos que A^G es un $S^G/I\cap S^G$ módulo finitamente generado, luego, es suficiente mostrar que $\mathrm{Frac}(A^G)$ es finitamente generado como cuerpo. Si A es un dominio entero, ya que $\mathrm{Frac}(A)$ sería finitamente generado como cuerpo y un subcuerpo de un cuerpo finitamente generado, es finitamente generado. En el caso general, usaremos el anillo de fracciones total [3], esto es la localización A_T de A respecto al conjunto multiplicativo T de los elementos de A que no son divisores de cero.

Para cualquier ideal $\mathfrak{m}$ de A_T, tendremos $\mathfrak{m} \cap A^G = \{0\}$ ya que A^G no tiene divisores enteros. Esto muestra que el cuerpo de fracciones de A^G es un subcuerpo de $A_T/\mathfrak{m}$. Pero $A_T/\mathfrak{m} = \mathrm{Frac}(A/\mathfrak{m} \cap A)$, el cuerpo de fracciones de $A/\mathfrak{m} \cap A$ que es finitamente generado, con lo cual $\mathrm{Frac}(A^G)$ es finitamente generado, lo que completa la demostración. ■

Un *anillo normal* es un dominio entero cerrado en su cuerpo de fracciones.

Proposición 6.7. *Sea G un grupo algebraico reductivo actuando sobre una k-álgebra A finitamente generada. Entonces A^G es un k-álgebra normal finitamente generada.*

Demostración:
Como G es reductivo, por Teorema de Haboush, es geométricamente reductivo y por el Teorema (6.6) tenemos que A^G es finitamente generada.

Sea K el cuerpo de fracciones de A. Tenemos que el cuerpo de fracciones L de A^G está contenido en el cuerpo K^G de los elementos G-invariantes de K. Para ver que que A^G es integralmente cerrado en L, sea $x \in L$ tal que x satisface

$$x^n + a_1 x^{n-1} + \cdots + a_0 = 0$$

donde los $a_i \in A^G$. Como A es normal, $x \in A \cap K^G = A^G$ y por tanto, A^G es normal. ■

7. Existencia de buenos cocientes categóricos

En esta sección mostraremos que bajo la hipótesis de ser un grupo geométricamente reductivo, se tiene que existen los buenos cocientes categóricos. Primero enunciamos el siguiente Lema que puede ser pensado como la versión geométrica del Lema de Urysohn.

Lema 7.1. *Sea G un grupo geométricamente reductivo actuando sobre una variedad algebraica afín $X = \operatorname{Specm}(A)$. Sean $Z_1, Z_2 \subset X$ dos subconjuntos cerrados y G-invariantes con $Z_1 \cap Z_2 = \emptyset$. Entonces, existe una función $\Psi \in A^G$ tal que $\Psi(Z_1) = \{1\}$ y $\Psi(Z_2) = \{0\}$.*

Demostración:
Como $Z_1 \cap Z_2 = \emptyset$, por el Hilbert Nullstellensatz,

$$A = I(Z_1 \cap Z_2) = I(Z_1) + I(Z_2),$$

con lo cual tenemos que existen $f_1 \in Z_1$, $f_2 \in Z_2$ tales que $1 = f_1 + f_2$. Sea $W \subset A$ el subespacio lineal generado por los G trasladados de f_2. Por el Lema 5.17, W es finito dimensional. Sea $\{\varphi_1, \ldots, \varphi_n\}$ una base de W y definamos $f : X \to \mathbb{A}^n$ mediante $x \mapsto (\varphi_1(x), \ldots, \varphi_n(x))$.

Como Z_1, Z_2 son G-invariantes, tenemos que $(g \cdot f_2)(Z_i) = f_2(g^{-1} \cdot (Z_i)) = f_2(Z_i)$ y teniendo en cuenta que $f_1 + f_2 = 1$, obtenemos que

$$\varphi_j(Z_1) = f_2(Z_1) = 1,$$

y también que

$$\varphi_j(Z_2) = f_2(Z_2) = 0.$$

En consecuencia,

$$f(Z_1) = \{(1, \ldots, 1)\} \text{ y } f(Z_2) = \{(0, \ldots, 0)\}.$$

Como G es geométricamente reductivo, existe un polinomio homogéneo F tal que $F(1, \ldots, 1) = 1$. Definamos $\Psi = f^*(F)$, luego $\Psi \in A^G$ y

$$\Psi(Z_1) = F(f(Z_1)) = \{1\} \text{ y } \Psi(Z_2) = F(f(Z_2)) = \{0\}.$$

■

Sea $\sigma : G \times X \to X$ una acción algebraica, diremos que el par (X, σ) es una *G-variedad.*

Definición 7.2. Un *cociente categórico* de una G-variedad X es un morfismo G-invariante $p : X \to Y$ tal que para cualquier morfismo G-invariante $g : X \to Z$, existe un único morfismo $\overline{g} : Y \to Z$ tal que $\overline{g} \circ p = g$.

Definición 7.3.

- Un morfismo G-equivariante $p : X \to Y$ es llamado un *buen cociente categórico* si p satisface:
  1. Para todo $u \subset Y$ abierto, $p^* : \mathcal{O}(U) \to \mathcal{O}(p^{-1}(U))$ es un isomorfismo sobre el subanillo $\mathcal{O}(p^{-1}(U))^G$.
  2. Si $W \subset X$ es cerrado y G-invariante, entonces $p(W) \subset Y$ es cerrado.
  3. Si $V_1, V_2 \subset X$ son cerrados disjuntos y G-invariantes, entonces $p(V_1) \cap p(V_2) = \emptyset$.
- Un (buen) cociente categórico es llamado un (buen) cociente geométrico si $\operatorname{Im}(\Psi) = X \times_Y X$, donde la función Ψ es la que proporciona el Lema 7.1.

Tenemos que los buenos cocientes geométricos son cocientes categóricos, (ver [1, Proposición 6.1, p.63]).

Teorema 7.4. *Sea $X = \operatorname{Specm}(A)$ una variedad afín y G un grupo geométricamente reductivo actuando sobre X. Entonces A^G es una k-álgebra finitamente generada y la función canónica $p : X \to Y := \operatorname{Specm}(A^G)$ es un buen cociente categórico.*

Demostración:
Por el Teorema de Nagata (Teorema 6.6), tenemos que A^G es finitamente generada. Probemos los tres numerales que definen un buen cociente categórico.

1. Basta probarlo para los abiertos básicos $U_f \subset Y$ con $f \in A^G$. Notar que
$$\begin{aligned} \frac{g}{f^n} \in \left(A^G\right) &\Leftrightarrow g \in A^g \\ &\Leftrightarrow \frac{g}{f^n} \text{ es } G\text{-invariante} \\ &\Leftrightarrow \frac{g}{f^n} \in (A_f)^G . \end{aligned}$$
Con lo cual, tenemos que tomar invariantes conmuta con la localización, *i.e.,* $\left(A^G\right)_f = (A_f)^G$ y como $\mathcal{O}(U_f) = A_f$, tenemos que $p^* : \mathcal{O}(U_f) \to \mathcal{O}(p^{-1}(U_f))$ es un isomorfismo sobre $\mathcal{O}(p^{-1}(U_f))^G$.
2. Sea $W \subset X$ un conjunto cerrado y G-invariante. Razonando por contradicción, supongamos que $p(W)$ no es cerrado. Luego, existe $y \in \overline{p(W)} \setminus p(W)$. Sea $Z := p^{-1}(\{y\}) \subset X$. Tenemos que Z es cerrado y como p es G-invariante, entonces Z lo es y además $Z \cap W = \emptyset$. Así, por el Lema 7.1, tenemos que existe $\Phi \in A^G$ tal que $\Phi(W) = 1$ y $\Phi(Z) = 0$. Como p^* es un isomorfismo sobre $\mathcal{O}(p^{-1}(X))^G = A^G$, tenemos que existe un único $\varphi \in A^G$ tal que $\Phi = p^*(\varphi)$. En consecuencia, $0 = \Phi(Z) = p^*(\varphi)(p^{-1}(y)) = \varphi(p(p^{-1}(y))) = \varphi(y)$ y $1 = \Phi(W) = p^*(\varphi)(W) = \varphi(p(W))$, lo cual es una contradicción pues $y \in \overline{p(W)}$.
3. Sean $V_1, V_2 \subset X$ cerrados y G-invariantes con $V_1 \cap V_2 = \emptyset$. Por el Lema 7.1, tenemos que existe $\Phi \in A^G$ tal que $\Phi(p(V_1) = 1$ y $\Phi(p(V_2)) = 0$, lo cual implica que $p(V_1) \cap p(V_2) = \emptyset$.

■

8. Una ecuación funcional

Problema: Encontrar todas las funciones $\varphi(x,y) \in \mathbb{R}[x,y]$ tal que existe $B \subset \mathbb{R}$ cumpliendo que $\varphi(x,y) = 0$ define a $y = f : B \subset \mathbb{R} \to \mathbb{R}$ como función de x y para todo $x \in B$, $y = f(x)$ es solución de

$$f(f(x) - 2x) = 2f(x) - 3x. \tag{8.1}$$

Para resolverlo notemos que si $\Gamma_f = \{(x, f(x)) : x \in B\}$ es el grafo de una solución $f : B \to \mathbb{R}$; para $x \in B$, tenemos que $f(x) - 2x \in B$, luego, si $(x, f(x)) \in \Gamma_f$, entonces $(f(x) - 2x, f(f(x) - 2x)) = (f(x) - 2x, 2f(x) - 3x) \in \Gamma_f$.

Definamos la transformación de $\mathbb{R}^2 \to \mathbb{R}^2$, dada por
$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y - 2x \\ 2y - 3x \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ -3 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$
Como
$$\begin{pmatrix} -2 & 1 \\ -3 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
tenemos que para $g = \begin{pmatrix} 2 & 1 \\ -3 & 2 \end{pmatrix}$, $G := \{I_2, g\} \subset \mathrm{GL}_2(\mathbb{R})$ es un subgrupo finito.

Luego el problema de encontrar $\varphi(x,y)$ que definen a $y = f(x)$ tales que $y = f(x)$ sea solución de (8.1) se reduce a encontrar $\mathbb{R}[x,y]^G$ donde la acción de G sobre $\mathbb{R}[x,y]$, está dada por $g(\varphi(x,y)) := \varphi(g^{-1}(x,y))$. Como G es finito, entonces G es geométricamente reductivo y por el Teorema de Nagata $\mathbb{R}[x,y]^G$ es finitamente generada como $\mathbb{R}$-álgebra, *i.e.,* existen $\varphi_1(x,y), \dots, \varphi_r(x,y) \in \mathbb{R}[x,y]$ tales que cualquier $\varphi(x,y) \in \mathbb{R}[x,y]^G$ se escribe como un polinomio en $\varphi_1(x,y), \dots, \varphi_r(x,y)$. El problema estaría completamente resuelto si diéramos explícitamente los $\varphi_i(x,y)$ que generan a $\mathbb{R}[x,y]^G$ como $\mathbb{R}$-álgebra. El Teorema de Nagata sólo prueba su existencia pero no ofrece un algoritmo para construirlos. En [10, p. 145], se muestran algoritmos para determinar los generadores para grupos geométricamente reductivos. En particular para el grupo cíclico de orden 2, C_2, en un cuerpo de característica distinto de 2, se calculan los generadores de $k[x,y]^{C_2}$ en el Ejemplo 4.1.10, pág. 146.

Referencias

[1] I. Dolgachev, *Lectures on Invariant Theory*, Cambridge University Press, 2003.
[2] J. Harris, *Algebraic Geometry: A First Course*, Springer Science and Business Media. **133** (2013).
[3] P. M. Cohn, *Rings of Fractions*, The American Mathematical Monthly, Vol. 78, No. 6, 596-615, 1971.
[4] W. J. Haboush, *Reductive groups are geometrically reductive*, Annals of Mathematics, 102 (1975), 67-83.

[5] D. W Lewis, *David Hilbert and the Theory of Algebraics Invariants*, IMS Bulletin 33, 1994
[6] M. Nagata, *Complete reducibility of rational representations of a matric group*, J. Math. Kyoto Univ. 1-1 (1961) 87-99.
[7] M. Nagata and T. Miyata, *Note on semi-reductive groups*, J. Math. Kyoto Univ., 3-3 (1964) 379-382.
[8] M. Nagata, *Invariants of group in an affine ring*, J. Math.Kyoto Univ., 3-3 (1964) 369-377
[9] H. Kraft, C. Procesi, *Classical Invariant Theory, A primer* 1996, disponible aquí
[10] H. Derksen and G. Kemper. *Computational Invariant Theory*. Springer-Verlag Berlin Heidelberg, 2015.
[11] J. E. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics, Springer, 1998.
[12] S. Mukai, *An Introduction to Invariants and Moduli*, Cambridge University Press, 2002.
[13] A. Kleshchev, *Lectures in Algebraic Groups*, disponible aquí.
[14] S. Schlegel, *Geometrically Reductive Groups and Finitely Generated Rings of Invariants*, 2017. Disponible aquí.
[15] T. A. Springer, *Linear Algebraic Groups*, Modern Birkhäuser CIassics, 1998.
[16] J. An, *Rigid Geometric Structures, Isometric Actions, and Algebraic Quotiens*, 2011, disponible aquí.
[17] C. Efthimiou, *Introduction to Functional Eequations, theory and problem-solving strategies for mathematical competitions and beyond*, version 2.00, 2012. Disponible aquí.
[18] G. Fredemburg, *Algebraic Theory of Locally Nilpotent Derivations*, Springer, Second Edition, 2017.
[19] D. Eisenbud, *Commutative Algebra: with a View Toward Algebraic Geometry*, Springer, 1995.
[20] R. Birkner, Introduction to GIT, disponible aquí.

Departamento de Matemática, Universidad Técnica Federico Santa María, Valparaíso, Chile.
Email address: `tobias.martinez@ues.edu.sv`