**Ingeniería y Ciencia**, ISSN 1794-9165
Volumen 1, número 2, páginas 67-81, septiembre de 2005

# Una primera lección de Geometría Algebraica

Carlos Cadavid[1]

*Recepción: 03 de agosto de 2004 — Aceptación: 07 de octubre de 2004*
*Se aceptan comentarios y/o discusiones al artículo*

**Resumen**

En este artículo se explica cómo aparece la Geometría Algebraica, partiendo del estudio de los conjuntos de soluciones de sistemas algebraicos.

**Palabras claves:** Sistemas de ecuaciones algebraicas, métodos de cambio de variable, equivalencia de sistemas algebraicos, Bases de Gröbner, Variedades afines y sus morfismos, equivalencia de variedades afines.

**Abstract**

This paper explains how Algebraic Geometry originated from the study of solution sets of algebraic systems.

**Key words:** Algebraic systems, change of variable methods, equivalence of algebraic systems, Gröbner basis, affine varieties and their morphisms, equivalence of affine varieties.

## 1 Introducción

El propósito es ofrecer una introducción a la Geometría Algebraica, partiendo de nociones elementales. Los cursos usuales de Geometría Algebraica empiezan "muy adelante". No hay una primera clase en la que se discuta de donde proviene el interés por el estudio de los objetos que se definen. Se espera llenar este vacío.

En este artículo $\mathbb{C}$ denotará el campo de los números complejos, $A^n_{\mathbb{C}}$ el conjunto de $n-$tuplas de números complejos, y $\mathbb{C}[X_1, \ldots, X_n]$ el anillo de polinomios en las variables $X_1, \ldots, X_n$. El álgebra desde sus inicios se enfrentó con el problema de "hallar" las soluciones de un sistema de ecuaciones de tipo algebraico. Esto condujo al problema

[1] Ph.D. en Matemáticas, ccadavid@eafit.edu.co, profesor investigador, Universidad EAFIT.

más conceptual de "entender" el conjunto de soluciones $X \subset A^n_{\mathbb{C}}$ de un sistema de $m$ ecuaciones de tipo algebraico en $n$ incógnitas:

$$\begin{aligned} f_1(X_1, \ldots, X_n) &= 0\,, \\ f_2(X_1, \ldots, X_n) &= 0\,, \\ &\vdots \\ f_m(X_1, \ldots, X_n) &= 0\,, \end{aligned}$$

donde cada $f_i\,(X_1, \ldots, X_n) \in \mathbb{C}\,[X_1, \ldots, X_n]$. Dicho de otra manera, la Geometría Algebraica se dedica a "entender" los conjuntos de soluciones de los sistemas algebraicos. El sentido de "entender" que se adoptará será el de contestar las siguientes dos preguntas:

1. ¿Tiene el sistema alguna solución, es decir, es $X \neq \phi$?
2. ¿Cuándo dos sistemas dados tienen las "mismas" soluciones?

En las siguientes secciones se verá cómo estas preguntas originan los principales problemas de la Geometría Algebraica.

## 2 El problema de la existencia de soluciones de un sistema algebraico

Si se tiene un sistema algebraico de una sola ecuación con una sola incógnita, el problema de existencia de soluciones es resuelto de manera exacta por el famoso Teorema Fundamental del Álgebra, demostrado por Gauss [3]. Este teorema afirma que siempre existe alguna solución, a menos que el polinomio sea una constante distinta de cero. El problema general de existencia de soluciones de un sistema admite dos tipos de solución. Un *replanteamiento teórico* (que podríamos llamar "solución teórica") y una *solución computacional*.

### 2.1 Replanteamiento teórico

Para la comprensión de este replanteamiento son necesarias las siguientes definiciones y teoremas. Se sugiere leer la excelente presentación que de éstos se hace en el capítulo III de [2].

**Definición 2.1.** *Un subconjunto $I$ de $\mathbb{C}\,[X_1, \ldots, X_n]$ se dice que es un* ideal *si dados elementos $f$ y $g$ en $I$, y $h$ y $k$ en $\mathbb{C}\,[X_1, \ldots, X_n]$ se tiene que $hf + kg \in I$.*

**Definición 2.2.** *Un ideal $I$ de $\mathbb{C}[X_1, \ldots, X_n]$ se dice que es* maximal *si $I \neq \mathbb{C}[X_1, \ldots, X_n]$ y si siempre que $J$ sea un ideal de $\mathbb{C}[X_1, \ldots, X_n]$ tal que $I \subset J \subset \mathbb{C}[X_1, \ldots, X_n]$, entonces $J = I$ ó $J = \mathbb{C}[X_1, \ldots, X_n]$.*

El siguiente teorema debido a Hilbert, llamado "Nullstellensatz débil", caracteriza los ideales maximales.

**Teorema 2.1.** *Un ideal $I$ de $\mathbb{C}[X_1, \ldots, X_n]$ es maximal si y sólo si*

$$I = \{f_1.(X_1 - \alpha_1) + \cdots + f_n.(X_n - \alpha_n) : f_i \in \mathbb{C}[X_1, \ldots, X_n]\}$$

*para una (de hecho única) $n-$tupla $(\alpha_1, \ldots, \alpha_n) \in A^n_{\mathbb{C}}$.*

Para consultar la demostración del teorema (2.1), véase el corolario 5.4, página 125 de [2].

Una aplicación rutinaria del lema de Zörn, demuestra el teorema (2.2).

**Teorema 2.2.** *Todo ideal $I \neq \mathbb{C}[X_1, \ldots, X_n]$ está contenido en algún ideal maximal.*

**Definición 2.3.** *Sea $A$ un subconjunto cualquiera de $\mathbb{C}[X_1, \ldots, X_n]$. Se denotará por $(A)$ al conjunto*

$$\{\ h_1 f_1 + \cdots + h_s f_s : \text{donde cada } h_i \in \mathbb{C}[X_1, \ldots, X_n] \text{ y cada } f_i \in A\ \}.$$

*Este conjunto resulta ser un ideal, y se llama* ideal generado por el conjunto $A$.

Es fácil ver que este ideal coincide con la intersección de todos los ideales de $\mathbb{C}[X_1, \ldots, X_n]$ que contienen a $A$. Es pues el menor (en el sentido de inclusión) ideal que contiene a $A$. Cuando el conjunto $A$ es finito, $A = \{f_1, \ldots, f_m\}$, se acostumbra escribir $(f_1, \ldots, f_m)$ en vez de $(\{f_1, \ldots, f_m\})$. Es conveniente recordar este ideal como aquel que consta de las combinaciones lineales de los elementos $f_1, \ldots, f_m$ donde los coeficientes son elementos de $\mathbb{C}[X_1, \ldots, X_n]$. El siguiente teorema, debido también a Hilbert, es frecuentemente llamado "Teorema de la base de Hilbert".

**Teorema 2.3.** *Todo ideal $I$ de $\mathbb{C}[X_1, \ldots, X_n]$ es finitamente generado, es decir, existe alguna colección finita $f_1, \ldots, f_m \in I$, tal que $I = (f_1, \ldots, f_m)$.*

El teorema (2.3) puede consultarse en [2], corolario (3.6), página 119.

**Definición 2.4.** *Sea $A$ un subconjunto de $\mathbb{C}[X_1, \ldots, X_n]$. Se denotará por $V(A)$ al conjunto*

$$\{\ (\alpha_1, \ldots, \alpha_n) \in A^n_{\mathbb{C}} : f(\alpha_1, \ldots, \alpha_n) = 0 \text{ para cada } f \in A\ \}.$$

*Este conjunto se llama* variedad afín definida por $A$.

Para ver ejemplos de variedades afines (y también proyectivas, aunque en este artículo no se van a definir) se sugiere consultar los capítulos I y II, hasta la página 42, de [2].

La variedad afín $V(A)$ no es más que el conjunto de soluciones del sistema algebraico $\{f = 0 : f \in A\}$. Es importante observar, y fácil de verificar, que si $A \subset \mathbb{C}[X_1, \ldots, X_n]$, entonces $V(A) = V((A))$. Esto significa, en particular, que el sistema de ecuaciones $\{f = 0 : f \in A\}$, tiene el mismo conjunto de soluciones que el sistema de ecuaciones $\{f = 0 : f \in (A)\}$. Más aún, otro teorema de Hilbert, llamado "Nullstellensatz fuerte", describe con exactitud el conjunto de los polinomios de $\mathbb{C}[X_1, \ldots, X_n]$ que se anulan en una variedad afín dada. Para enunciarlo es necesaria la siguiente definición.

**Definición 2.5.** *Sea $I$ un ideal de $\mathbb{C}[X_1, \ldots, X_n]$. El conjunto*

$$\left\{ f \in \mathbb{C}[X_1, \ldots, X_n] : f^t \in I, \text{ para algún entero } t \geq 1 \right\}$$

*es un ideal. Este ideal se denota por $Rad(I)$ y se llama* radical de $I$.

**Teorema 2.4.** *Sea $I$ un ideal de $\mathbb{C}[X_1, \ldots, X_n]$. Entonces el ideal de todos los polinomios que se anulan en el conjunto $V(I)$ es igual al radical de $I$. Es decir,*

$$\{ f \in \mathbb{C}[X_1, \ldots, X_n] : f(\alpha) = 0, \text{para todo } \alpha \in V(I) \} = Rad(I).$$

Este teorema puede ser estudiado en detalle en [2], teorema (5.8), página 127.

El teorema (2.4) dice, en particular, que un sistema algebraico $\{f_1 = 0, \ldots, f_t = 0\}$, tiene el mismo conjunto de soluciones que el sistema $\{f = 0 : f \in Rad((f_1, \ldots, f_t))\}$, y que si una ecuación $g = 0$, es tal que todas las soluciones del sistema $\{f_1 = 0, \ldots, f_t = 0\}$ son también soluciones suyas, entonces $g^r = h_1 f_1 + \cdots + h_t f_t$, para algún entero $r \geq 1$, y polinomios $h_i \in \mathbb{C}[X_1, \ldots, X_n]$ .

Después de las observaciones anteriores es posible enunciar el *replanteamiento teórico* del problema de existencia de soluciones.

**Teorema 2.5.** *Con la notación anterior, las siguientes afirmaciones son equivalentes:*

1. *El sistema $\{f_i = 0 : i = 1, \ldots, t\}$ tiene alguna solución.*
2. *La variedad afín $V(f_1, \ldots, f_t) \neq \phi$.*
3. *$1 \notin (f_1, \ldots, f_t)$.*
4. *$1 \notin Rad((f_1, \ldots, f_t))$.*
5. *$(f_1, \ldots, f_t) \neq \mathbb{C}[X_1, \ldots, X_n]$.*
6. *No existen $h_1, \ldots, h_t \in \mathbb{C}[X_1, \ldots, X_n]$ , tales que $1 = h_1 f_1 + \cdots + h_t f_t$.*

*Demostración.* Se demostrará la única equivalencia no inmediata (1) si y sólo si (6) .
( $\Rightarrow$) Si el sistema tiene alguna solución $\alpha = (\alpha_1, \ldots, \alpha_n)$, entonces la ecuación $h_1(\alpha) f_1(\alpha) + \cdots + h_t(\alpha) f_t(\alpha) = 1$ implicaría que $0 = 1$, y esto es imposible.

($\Leftarrow$) Si no existen $h_1, \ldots, h_t \in \mathbb{C}[X_1, \ldots, X_n]$ tales que $1 = h_1 f_1 + \cdots + h_t f_t$, entonces $1 \notin (f_1, \ldots, f_t)$. Esto nos dice que $(f_1, \ldots, f_t) \neq \mathbb{C}[X_1, \ldots, X_n]$, y que por lo tanto, existiría algún ideal maximal $J$ que contiene a $(f_1, \ldots, f_t)$. Ahora, por el teorema Nullstellensatz débil se tendría que $J = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$ para cierto $\alpha = (\alpha_1, \ldots, \alpha_n) \in A^n_{\mathbb{C}}$. Como cada $f_i \in J$, entonces existirían polinomios $h_{ij} \in \mathbb{C}[X_1, \ldots, X_n]$, con $j = 1, \ldots, n$, tales que $f_i = h_{i1}(X_1 - \alpha_1) + \cdots + h_{in}(X_n - \alpha_n)$. Entonces, para cada $i$, se tendría que $f_i(\alpha) = h_{i1}(\alpha).(\alpha_1 - \alpha_1) + \cdots + h_{in}(\alpha).(\alpha_n - \alpha_n) = 0$, y entonces $\alpha$ sería una solución del sistema algebraico. □

### 2.2 Solución computacional

El teorema (2.5) traduce un problema teórico en otros problemas también teóricos y no proporciona medios computacionales para decidir si un sistema algebraico dado tiene solución o no. Sin embargo, existe un procedimiento computacional, llamado *método de bases de Gröbner*, que proporciona un algoritmo que resuelve el *problema de la pertenencia*: si $f, f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$, el algoritmo determina si $f \in (f_1, \ldots, f_r)$. Una excelente exposición del método de bases de Gröbner se puede encontrar en [1].

Entonces, la solución computacional es la siguiente: *Un sistema* $\{f_1 = 0, \ldots, f_r = 0\}$ *tiene solución si y sólo si el algoritmo determina que* $1 \notin (f_1, \ldots, f_r)$.

## 3 El problema de cuándo dos sistemas tienen el "mismo" conjunto de soluciones

En esta sección se verá que existen distintas maneras de comparar los conjuntos de soluciones de dos sistemas algebraicos.

### 3.1 Primera manera de comparar los conjuntos de soluciones de dos sistemas algebraicos: Igualdad

La manera más obvia de comparar los conjuntos de soluciones de dos sistemas algebraicos es la siguiente: diremos que los sistemas $\{f_1 = 0, \ldots, f_r = 0\}$ y $\{g_1 = 0, \ldots, g_s = 0\}$ con $f_1, \ldots, f_r, g_1, \ldots, g_s \in \mathbb{C}[X_1, \ldots, X_n]$, tienen el "mismo" conjunto de soluciones, si los conjuntos de soluciones son idénticos, es decir, si $V((f_1, \ldots, f_r)) = V((g_1, \ldots, g_s))$. El problema de cuándo se da esta igualdad tiene un replanteamiento teórico y una solución computacional.

#### 3.1.1 Replanteamiento teórico

El siguiente teorema describe, desde el punto de vista algebraico, el que dos sistemas algebraicos en las mismas variables tengan conjuntos de soluciones idénticos.

**Teorema 3.1.** *$V((f_1,\ldots,f_r)) = V((g_1,\ldots,g_s))$ si y sólo si $Rad((f_1,\ldots,f_r)) = Rad((g_1,\ldots,g_s))$.*

**Demostración 3.1.** *Sean $I = (f_1,\ldots,f_r)$ y $J = (g_1,\ldots,g_s)$.*
*($\Rightarrow$) Suponga que $V(I) = V(J)$. El Nullstellensatz fuerte afirma que*

$$Rad(I) = \{f \in \mathbb{C}[X_1,\ldots,X_n] : f \equiv 0 \text{ sobre } V(I)\} =$$

$$\{f \in \mathbb{C}[X_1,\ldots,X_n] : f \equiv 0 \text{ sobre } V(J)\} = Rad(J).$$

*($\Leftarrow$) Suponga que $Rad(I) = Rad(J)$. Entonces $V(I) = V(Rad(I)) = V(Rad(J)) = V(J)$.*

### 3.1.2 Solución computacional

Al igual que ocurrió con el problema de la existencia de soluciones, el método de bases de Gröbner puede usarse para determinar la igualdad de los conjuntos de soluciones de dos sistemas algebraicos en las mismas variables. De manera precisa, sean $\{f_1 = 0,\ldots,f_r = 0\}$ y $\{g_1 = 0,\ldots,g_s = 0\}$ dos sistemas algebraicos donde $f_1,\ldots,f_r,g_1,\ldots,g_s \in \mathbb{C}[X_1,\ldots,X_n]$. En la sección anterior se vio que $V((f_1,\ldots,f_r)) = V((g_1,\ldots,g_s))$, si y sólo si, $Rad((f_1,\ldots,f_r)) = Rad((g_1,\ldots,g_s))$. Ahora, para demostrar esta última igualdad, basta verificar las inclusiones $(f_1,\ldots,f_r) \subset Rad((g_1,\ldots,g_s))$ y $(g_1,\ldots,g_s) \subset Rad((f_1,\ldots,f_r))$, ya que como $Rad(Rad(I)) = Rad(I)$ para cualquier ideal $I$, la primera inclusión implica que $Rad((f_1,\ldots,f_r)) \subset Rad((g_1,\ldots,g_s))$, y la segunda que $Rad((g_1,\ldots,g_s)) \subset Rad((f_1,\ldots,f_r))$. Ahora, se puede ver que un polinomio $f \in \mathbb{C}[X_1,\ldots,X_n]$ pertenece a $Rad((h_1,\ldots,h_t))$ si y sólo si

$$1 \in (h_1,\ldots,h_t,1 - W.f) \subset \mathbb{C}[X_1,\ldots,X_n,W],$$

donde $W$ es una nueva variable, consultar [1] página 66. Pero el problema de la pertenencia de un polinomio específico a un ideal dado por un conjunto de generadores, es el típico problema que resuelve el método de bases de Gröbner.

Hay otra manera computacional de saber, al menos en principio, si dos sistemas algebraicos en las mismas variables tienen conjuntos de soluciones idénticos. En álgebra lineal se estudia cuándo dos sistemas lineales en las mismas variables tienen el mismo conjunto de soluciones. La respuesta es que dos sistemas lineales tienen el mismo conjunto de soluciones si y sólo si uno de los sistemas es transformable en el otro aplicando un número de *transformaciones elementales.* Algo similar ocurre con dos sistemas algebraicos en las mismas variables.

**Teorema 3.2.** *Sean $f_1,\ldots,f_r,g_1,\ldots,g_s \in \mathbb{C}[X_1,\ldots,X_n]$. Entonces los sistemas $\{f_1 = 0,\ldots,f_r = 0\}$ y $\{g_1 = 0,\ldots,g_s = 0\}$ tienen el mismo conjunto de soluciones, si y sólo si, es posible transformar el primer sistema en el segundo aplicando un número finito de las siguientes tranformaciones elementales:*

*Tipo I) Agregar o eliminar del sistema un número finito de ecuaciones de la forma* $0 = 0$.

*Tipo II) En el sistema* $\{k_1 = 0, \ldots, k_t = 0\}$, *reemplazar la ecuación* $j-$*ésima,* $k_j = 0$, *por la ecuación* $hk_i + k_j = 0$, *donde* $k_i = 0$ *es la* $i-$*ésima ecuación,* $h \in \mathbb{C}[X_1, \ldots, X_n]$ *e* $i \neq j$.

*Tipo III) Si en la* $j-$*ésima ecuación* $k_j = 0$ *del sistema* $\{k_1 = 0, \ldots, k_t = 0\}$, *el polinomio* $k_j$ *es de la forma* $p^r$, *con* $p \in \mathbb{C}[X_1, \ldots, X_n]$ *y* $r \geq 1$ , *entonces ésta puede ser reemplazada por la ecuación* $p^s = 0$, *para cualquier* $s \geq 1$.

Este teorema es una consecuencia casi inmediata del teorema Nullstellensatz fuerte.

### 3.2 Segunda manera de comparar el conjunto de soluciones de dos sistemas de ecuaciones polinómicas: correspondencia vía cambios de variables polinómicos

Esta forma de comparar los conjuntos de soluciones de dos sistemas algebraicos tiene origen en los trucos de "cambio de variable" de tipo polinómico para estudiar un sistema algebraico transformándolo en otro. A continuación se presentarán algunos ejemplos de cómo funcionan estos métodos.

**Ejemplo 3.1.** *Considere la ecuación*

$$aX^2 + bX + c = 0$$

*con* $a,\ b,\ c \in \mathbb{C}$ *y* $a \neq 0$. *Dividiendo ambos lados de la ecuación por* $a$, *y refrescando la notación, se puede suponer que la ecuación a estudiar es de la forma*

$$f(X) = X^2 + bX + c = 0\,,$$

*con* $b, c \in \mathbb{C}$. *Si se introduce una nueva variable* $Y$ *tal que* $X = Y - (b/2)$ *la ecuación toma la forma*

$$g(Y) = Y^2 - \left(b^2/4\right) + c = 0\,,$$

*la cual tiene como conjunto de soluciones las dos (o una en el caso* $\left(b^2/4\right) - c = 0$*) raíces complejas del número complejo* $\left(b^2/4\right) - c$. *Esto se puede expresar diciendo que existe una función* $\varphi : V(f) \to V(g)$ *dada por*

$$\varphi(\alpha) = \alpha + (b/2)\,,$$

*y una función* $\psi : V(g) \to V(f)$ *dada por*

$$\psi(\beta) = \beta - (b/2)\,,$$

*tal que* $\varphi \circ \psi = id_{V(g)}$ *y* $\psi \circ \varphi = id_{V(f)}$. *Es importante anotar que las funciones* $\varphi$, $\psi$ *son de tipo polinómico. Equivalentemente, existe una función* $\varphi : V(f) \to V(g)$ *que es biyectiva y que puede expresarse, tanto ella como su inversa, polinómicamente.*

**Ejemplo 3.2.** *Considere el sistema algebraico de cuatro ecuaciones en tres variables* $X, Y, Z$*:*

$$\begin{aligned}
f_1(X,Y,Z) &= 10X^2 - 10X - 15Y^3 - 12Z + 4Y^2Z - 2Z^2 + 15Y + 10YZ + 8Y^2 - 8 = 0\,,\\
f_2(X,Y,Z) &= -1 + Y^2 - 2Y^3 + 2XY + 2YZ - 2Z = 0\,,\\
f_3(X,Y,Z) &= 2Z - 4Y^2Z + 4Z^2 - 5Y + 5Y^3 - 6YZ - 2Y^2 + 2X + 4XZ = 0\,,\\
f_4(X,Y,Z) &= 1 - 6Y^2 + 4Z - 8Y^2Z + 4Z^2 + 5Y^4 = 0\,.
\end{aligned}$$

*Se puede verificar que si se hace la substitución*

$$X = S^2 + T\,,\ Y = S + T\ \ y\ \ Z = 2ST + T^2,$$

*el sistema se convierte en un sistema formado por cuatro ecuaciones en dos variables que puede llevarse al sistema de una sola ecuación*

$$g_1(S,T) = S^2 + T^2 - 1 = 0\,,$$

*aplicando ciertas transformaciones de tipo I, II y III. La simplificación es dramática. Note además que el cambio de variables*

$$S = Y - Z - X + Y^2\ \ \ y\ \ T = Z + X - Y^2,$$

*transforma el sistema* $\{g_1 = 0\}$ *en un sistema en las variables* $X, Y, Z$*, que puede ser llevado al sistema* $\{f_1 = 0, f_2 = 0, f_3 = 0, f_4 = 0\}$ *aplicando ciertas transformaciones de tipo I, II y III. Tal como en el ejemplo anterior, esto se puede expresar diciendo que hay una función* $\varphi : V(f_1, f_2, f_3, f_4) \to V(g_1)$ *dada por*

$$\varphi(\alpha_1, \alpha_2, \alpha_3) = \left(\alpha_2 - \alpha_3 - \alpha_1 + \alpha_2^2, \alpha_3 + \alpha_1 - \alpha_2^2\right),$$

*y una función* $\psi : V(g_1) \to V(f_1, f_2, f_3, f_4)$ *dada por*

$$\psi(\beta_1, \beta_2) = \left(\beta_1^2 + \beta_2, \beta_1 + \beta_2, 2\beta_1\beta_2 + \beta_2^2\right),$$

*tal que* $\varphi \circ \psi = id_{V(g_1)}$ *y* $\psi \circ \varphi = id_{V(f_1,f_2,f_3,f_4)}$. *Dicho de manera más sucinta, existe una función* $\varphi$ *de* $V(f_1, f_2, f_3, f_4)$ *en* $V(g_1)$ *expresable polinómicamente y biyectiva, tal que su inversa también es expresable polinómicamente. Note además que las funciones* $\varphi$ *y* $\psi$ *vistas como funciones de* $A^3_{\mathbb{C}}$ *en* $A^2_{\mathbb{C}}$*, y de* $A^2_{\mathbb{C}}$ *en* $A^3_{\mathbb{C}}$*, respectivamente, no son inversas la una de la otra. Si lo fueran,* $A^3_{\mathbb{C}}$ *y* $A^2_{\mathbb{C}}$ *serían* homeomorfos*, lo cual es falso.*

En los ejemplos (3.1) y (3.2), tanto el cambio directo de variables como el inverso, son dados por polinomios en varias variables. Esta situación es formalizada a continuación.

### 3.2.1 Cambio de variables: presentación formal

Para estudiar en detalle el contenido de este aparte, consultar [5], páginas 14-20. La formalización de lo que ocurrió en los ejemplos (3.1) y (3.2), requiere la introducción de las siguientes nociones.

**Definición 3.1.** *Sean*

$$f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n] \quad y \quad g_1, \ldots, g_s \in \mathbb{C}[Y_1, \ldots, Y_m],$$

*y sean*

$$W = V((f_1, \ldots, f_r)) \subset A^n_{\mathbb{C}} \quad y \quad Z = V((g_1, \ldots, g_s)) \subset A^m_{\mathbb{C}}$$

*las variedades afines definidas por estos conjuntos de polinomios. Una función $\varphi : W \to Z$ se dice que es* regular *si existen polinomios $h_1, \ldots, h_m \in \mathbb{C}[X_1, \ldots, X_n]$ tales que*

$$\varphi(\alpha_1, \ldots, \alpha_n) = (h_1(\alpha_1, \ldots, \alpha_n), \ldots, h_m(\alpha_1, \ldots, \alpha_n)),$$

*para cada $(\alpha_1, \ldots, \alpha_n) \in W$.*

**Definición 3.2.** *Sean $W$ y $Z$ como en la definición anterior y sea $\varphi : W \to Z$ una función regular. Se dice que $\varphi$ es una* equivalencia *o una* función birregular*, si existe otra función regular $\psi : Z \to W$ tal que $\varphi \circ \psi = id_Z$ y $\psi \circ \varphi = id_W$. Esto equivale a exigir que $\varphi : W \to Z$ sea regular y biyectiva, y que su inversa sea regular. Se dice que dos variedades afines $W$ y $Z$ son* isomorfas*, si existe alguna función birregular de la una en la otra.*

Las definiciones (3.1) y (3.2) formalizan el que dos sistemas sean el mismo, excepto por un cambio polinómico de variables.

**Definición 3.3.** *Dos sistemas $\{f_1 = 0, \ldots, f_r = 0\}$, con $f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$ y $\{g_1 = 0, \ldots, g_s = 0\}$, con $g_1, \ldots, g_s \in \mathbb{C}[Y_1, \ldots, Y_m]$ se dice que son* equivalentes *si sus conjuntos de soluciones son variedades afines isomorfas.*

Uno de los problemas centrales de la Geometría Algebraica es el de determinar cuándo dos variedades afines dadas son isomorfas. Como en los dos problemas que ya han sido tratados, hay una solución computacional y una aproximación teórica.

### 3.2.2 Solución computacional

El método de bases de Gröbner proporciona un algoritmo eficiente que permite decidir si dos variedades afines

$$V(f_1, \ldots, f_r) \subset A^n_{\mathbb{C}} \text{ y } V(g_1, \ldots, g_s) \subset A^m_{\mathbb{C}}$$

son isomorfas. En caso de ser isomorfas, el algoritmo proporciona un isomorfismo explícito, ver [1] para más detalles.

### 3.2.3 Aproximación teórica

Como se acaba de ver, la solución computacional es completa. Sin embargo, los geómetras algebraicos se interesan en distinguir "cualitativamente" las variedades afines. De manera precisa, esto significa hallar un conjunto, ojalá completo, de *invariantes* para las variedades afines. Un *invariante* para las variedades afines es una asignación de un ente matemático de algún tipo (un grupo, un polinomio, etcétera) a cada variedad afín, que satisfaga las siguientes condiciones:

1. Si dos variedades afines son isomorfas entonces el invariante les asigna entes isomorfos.
2. Que sea relativamente fácil de computar para cada variedad.

Una familia de invariantes se dice que es *completo* si se cumple que dos variedades afines son isomorfas si y sólo si todos los invariantes de dicha familia coinciden. Gran parte de la actividad de la Geometría Algebraica consiste en buscar dicha familia de invariantes.

Cabe aquí la siguiente analogía. Se puede afirmar que clasificar las especies animales significa ser simplemente capaz de distinguir dos especies distintas por cualquier detalle mínimo en que difieran. Tal esquema de clasificación sería poco inteligente. No admite, por ejemplo, el que dos animales sean parecidos, o de la misma familia, sino que los ve como idénticos o no idénticos. Es como si asignara distancia 1 si son distintos y 0 si son iguales. Un orden más inteligente los agrupa de acuerdo a características más generales, como asignando una métrica más compleja en el conjunto de las especies animales. De hecho, una buena agrupación termina siendo el reflejo de la historia de la construcción de los animales mismos, es decir, de la evolución.

Finalmente, el problema de clasificación de variedades afines admite un replanteamiento de tipo puramente algebraico. A continuación se discute este punto.

### 3.2.4 Traducción del problema de clasificación de variedades afines a un problema de clasificación puramente algebraico

Para estudiar en detalle el contenido de este aparte, consultar [5], páginas 14-20.

Sea $X = V((f_1, \ldots, f_r)) \subset A^n_{\mathbb{C}}$ una variedad afín. Considere el conjunto de funciones polinómicas de la variedad en el campo de los complejos

$$\mathbb{C}[X] = \{\ f\mid_X : f \in \mathbb{C}[X_1, \ldots, X_n]\ \}.$$

Este conjunto con la suma y la multiplicación usual de funciones forma un anillo. Este anillo es claramente isomorfo al anillo

$$\mathbb{C}[X_1, \ldots, X_n]/I(X),$$

donde

$$I(X) = \{f \in \mathbb{C}[X_1, \ldots, X_n]\ :\ f|_X \equiv 0\}.$$

Este último anillo es, a su vez, isomorfo a

$$\mathbb{C}[X_1, \ldots, X_n] / Rad((f_1, \ldots, f_r)),$$

por el Nullstellensatz fuerte. Este anillo se denomina *anillo de coordenadas de la variedad* $X$, y se denota por $\mathbb{C}[X]$. Por ser canónicos los isomorfismos entre los tres anillos anteriores es común usar $\mathbb{C}[X]$ para denotar simultáneamente estos tres anillos. Sea $Y \subset A^m_{\mathbb{C}}$ otra variedad afín y $\varphi : X \to Y$ una función regular. Ésta induce un homomorfismo de anillos $\varphi^* : \mathbb{C}[Y] \to \mathbb{C}[X]$ definido por $\varphi^*(f) = f \circ \varphi$. Tomar * tiene las siguientes dos propiedades. En primer lugar, si $id_X$ denota la función identidad de $X$, e $id_{\mathbb{C}[X]}$ denota el homomorfismo identidad del anillo $\mathbb{C}[X]$, entonces

$$(id_X)^* = id_{\mathbb{C}[X]}.$$

En segundo lugar, si $W \subset A^l_{\mathbb{C}}$ es otra variedad afín, y $\psi : Y \to W$ es una función regular, entonces

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^*.$$

Además, para todo homomorfismo $h : \mathbb{C}[Y] \to \mathbb{C}[X]$ existe una única función regular $\varphi : X \to Y$ tal que

$$\varphi^* = h\,.$$

Estos hechos implican el teorema (3.3), el cual da una caracterización algebraica de la equivalencia de variedades afines.

**Teorema 3.3.** *Las variedades afines $X$ y $Y$ son isomorfas si y sólo si sus anillos coordenados $\mathbb{C}[X]$ y $\mathbb{C}[Y]$ son isomorfos.*

## 3.3 Tercera manera de comparar los conjuntos de soluciones de dos sistemas algebraicos: correspondencia vía cambios de variables racionales

Para el estudio detallado del contenido de esta subsección, consultar [5] páginas 22-27. Esta noción de equivalencia surge de la posibilidad de transformar un sistema algebraico en otro usando cambios de variables de tipo racional, es decir, que sean expresables como cocientes de polinomios en varias variables. He aquí algunos ejemplos.

**Ejemplo 3.3.** *Considere la ecuación*

$$Y^2 - X^2 - X^3 = 0\,.$$

*Las substituciones*

$$X = T^2 - 1,\ Y = T\left(T^2 - 1\right),$$

*convierten esta ecuación en una ecuación en la variable $T$, equivalente a la ecuación $0 = 0$ en la variable $T$. Recíprocamente, la ecuación $0 = 0$ es equivalente a la ecuación*

$$\left(T\left(T^2 - 1\right)\right)^2 = \left(T^2 - 1\right)^2 + \left(T^2 - 1\right)^3.$$

*Se puede ver que la substitución*

$$T = Y/X$$

*convierte esta última ecuación en una ecuación equivalente a la ecuación*

$$Y^2 - X^2 - X^3 = 0\,.$$

*Es crucial destacar que los cambios de variables directo e inverso, son dados por expresiones racionales.*

Antes de dar una definición formal de lo que significa el que dos variedades afines sean equivalentes bajo cambios racionales de variables, son necesarias las siguientes definiciones.

**Definición 3.4.** *Sea $X \subset A^n_{\mathbb{C}}$ una variedad afín. Se dice que tal variedad es* reducible *si existen dos variedades $Y,\ Z \subset A^n_{\mathbb{C}}$ con $Y \neq X$ y $Z \neq X$, tal que $X = Y \cup Z$. Se dice que una variedad es* irreducible *si no es reducible.*

Es también necesario dotar a cada variedad afín de una topología especial, llamada topología de Zariski.

**Definición 3.5.** *Sea $X \subset A^n_{\mathbb{C}}$ una variedad afín. La colección*

$$\{\ X \cap G\ \ : A^n_{\mathbb{C}} - G \text{ es una variedad afín de } A^n_{\mathbb{C}}\}$$

*de subconjuntos de $X$, es una topología para $X$. Esta topología se llama* topología de Zariski de $X$. *Un subconjunto $U$ de $X$ se dice que es* denso *en $X$, si la intersección de todos los cerrados que lo contienen es $X$.*

**Teorema 3.4.** *Sea $X$ una variedad afín irreducible. Entonces todo abierto no vacío de Zariski de $X$ es denso en $X$.*

**Teorema 3.5.** *El anillo coordenado $\mathbb{C}[X]$ de una variedad afín irreducible $X$ no tiene divisores de cero, es decir, es un dominio entero.*

Todo dominio entero puede ser embebido en su campo de fracciones, consultar [4].

**Definición 3.6.** *El campo de fracciones del anillo $\mathbb{C}[X]$, donde $X$ es una variedad afín irreducible, se llama* campo de funciones racionales de $X$ *y se denota por $\mathbb{C}(X)$. A cada uno de sus elementos se le denomina* función racional de $X$.

Note que este campo es una construcción puramente algebraica. Sin embargo, es posible interpretar sus elementos como verdaderas funciones con valores complejos, definidas en "casi toda" la variedad $X$.

**Definición 3.7.** *Un elemento $\varphi \in \mathbb{C}(X)$ se dice que es* regular en el punto $\alpha \in X$, *si existe una representación $\varphi = f/g$ con $f, g \in \mathbb{C}[X]$, tal que $g(\alpha) \neq 0$. En este caso se dice que $\alpha$ es un* punto regular de $\varphi$.

Si $\alpha \in X$ es un punto regular de $\varphi \in \mathbb{C}(X)$, entonces tiene sentido hablar del valor que $\varphi$ toma en $\alpha$.

**Definición 3.8.** *El* valor *que $\varphi$ toma en un punto regular $\alpha$, se define por $f(\alpha)/g(\alpha) \in \mathbb{C}$, donde $f/g$ es cualquiera de las representaciones de $\varphi$ con $g(\alpha) \neq 0$. Tal valor se denotará por $\varphi(\alpha)$.*

**Observación 3.1.** *La validez de esta definición usa implícitamente el hecho de que el número complejo $\varphi(\alpha)$ no depende de la representación de $\varphi$ que se use.*

**Definición 3.9.** *El conjunto de todos los puntos regulares de $\varphi \in \mathbb{C}(X)$ es un abierto no vacío de la topología de Zariski de $X$ (y por tanto es denso en $X$). A este conjunto se le llama* dominio de *$\varphi$, y se denota por $Dom(\varphi)$.*

**Definición 3.10.** *Sean $X \subset A^n_{\mathbb{C}}$ y $Y \subset A^m_{\mathbb{C}}$ variedades afines irreducibles. Una* función racional *$\varphi$ de $X$ en $Y$ (lo cual se denota por $\varphi : X \to Y$) es una colección de $m$ funciones racionales $\varphi_1, \ldots, \varphi_m \in \mathbb{C}(X)$, tales que $(\varphi_1(x), \ldots, \varphi_m(x)) \in Y$ para todo $x \in Dom(\varphi_1) \cap \ldots \cap Dom(\varphi_m)$. Se dice que cada punto $x$ de $Dom(\varphi_1) \cap \ldots \cap Dom(\varphi_m)$ es un* punto regular de *$\varphi$ y que $(\varphi_1(x), \ldots, \varphi_m(x))$ es el* valor de *$\varphi$ en $x$. El conjunto $Dom(\varphi_1) \cap \ldots \cap Dom(\varphi_m)$ se llama* dominio de *$\varphi$ y se denota por $Dom(\varphi)$. Se llamará* imagen de *$\varphi$ al conjunto*

$$\{\, y \in Y \ : \ \text{existe } x \in Dom(\varphi) \ \text{ con } \varphi(x) = y \,\}.$$

*Este conjunto se denota por $\varphi(X)$.*

**Definición 3.11.** *Sean $X \subset A^n_{\mathbb{C}}$ y $Y \subset A^m_{\mathbb{C}}$ variedades afines irreducibles, y sea $\varphi : X \to Y$ una función racional. Se dice que $\varphi$ es un* isomorfismo birracional *si admite una inversa, es decir, si existe una función racional $\psi : Y \to X$ tal que $\varphi(X)$ es denso en $Y$, $\psi(Y)$ es denso en $X$ y $\varphi \circ \psi(x) = x$ para aquellos $x \in Dom(\psi)$ tales que $\psi(x) \in Dom(\varphi)$, y que $\psi \circ \varphi(x) = x$ para aquellos $x \in Dom(\varphi)$ tales que $\varphi(x) \in Dom(\psi)$. Se dice que dos variedades afines son* birracionalmente isomorfas *si existe al menos un isomorfismo birracional de la una en la otra.*

La definición (3.11) es precisamente la tercera manera como se puede entender que dos variedades afines sean la "misma". Esta noción motiva el problema de clasificación de variedades afines excepto por isomorfismo birracional: ¿Cuándo dos variedades afines irreducibles son isomorfas birracionalmente? El autor sólo conoce un replanteamiento teórico de este problema de clasificación que se presenta a continuación.

### 3.3.1 Replanteamiento teórico

La clasificación birracional de variedades afines es obviamente menos fina que la clasificación salvo isomorfismos. Entonces, la clasificación birracional no tiene solamente interés en sí misma, sino que se puede considerar como un primer paso en la solución del problema de clasificación salvo isomorfismos. Los geómetras se han dedicado a la búsqueda de conjuntos completos de invariantes birracionales para las variedades afines. Este estudio se ha llamado Geometría Birracional (más detalles en [5]).

### 3.3.2 Traducción del problema de clasificación birracional de variedades afines a un problema puramente algebraico

Sean $X \subset A^n_{\mathbb{C}}$ y $Y \subset A^m_{\mathbb{C}}$ variedades afines irreducibles, y sea $\varphi\colon X \to Y$ una función racional tal que $\varphi(X)$ es denso en $Y$. Si se considera la función de $Dom(\varphi)$ en $\varphi(X)$ que $\varphi$ define, entonces se denotará por $\varphi^*(f)$ a la función compuesta

$$f|_{\varphi(X)\cap Dom(\psi)} \circ \varphi|_{Dom(\varphi)},$$

donde $f$ denota cada función de $Y$ en $\mathbb{C}$ inducida por un elemento de $\mathbb{C}(Y)$. Es fácil ver que $\varphi^*(f)$ es la función inducida por un único elemento en $\mathbb{C}(X)$ que se denota nuevamente por $\varphi^*(f)$. Se puede verificar que la función $\varphi^* : \mathbb{C}[Y] \to \mathbb{C}(X)$ así definida es un *homomorfismo inyectivo* del *anillo* $\mathbb{C}[Y]$ en el *campo* $\mathbb{C}(X)$. Este homomorfismo a su vez, extiende a un único homomorfismo inyectivo del campo $\mathbb{C}(Y)$ de fracciones de $\mathbb{C}[Y]$, en $\mathbb{C}(X)$, que también se denota por $\varphi^*$. Ahora, si aún se supone que $\varphi(X)$ es denso en $Y$ y que $\psi : Y \to Z$ es una función racional, entonces se puede verificar fácilmente que su composición $\psi \circ \varphi$ como funciones determina unívocamente una función racional (como colección de elementos de $\mathbb{C}(X)$) de $X$ en $Z$, que se denota nuevamente por $\psi \circ \varphi$. Es además cierto que $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$, y que si $id_X$ denota la función identidad de $X$, e $id_{\mathbb{C}(X)}$ denota el homomorfismo identidad del campo $\mathbb{C}(X)$, entonces $id_X^* = id_{\mathbb{C}(X)}$. Estos hechos implican que si $\varphi : X \to Y$ es un isomorfismo birracional, entonces $\varphi^* : \mathbb{C}(Y) \to \mathbb{C}(X)$ es un *isomorfismo* de campos. Recíprocamente, si $h : \mathbb{C}(Y) \to \mathbb{C}(X)$ es un *isomorfismo* de campos, entonces existe un único isomorfismo birracional $\varphi : X \to Y$ tal que $h = \varphi^*$.

Esto demuestra, en particular, que dos variedades afines son birracionalmente isomorfas si y sólo si sus campos de funciones racionales son isomorfos.

## 4 Conclusiones

Los problemas centrales de la geometría algebraica tienen origen en los trucos de cambio de variable para solucionar sistemas algebraicos.

## Agradecimientos

El autor agradece a la Universidad EAFIT por brindar un inmejorable ambiente de trabajo académico.

## Referencias

[1] W. Adams y P. Loustaunau. *An introduction to Gröbner bases,* Graduate Studies in Mathematics, **3**, American Mathematical Society, 1994.

[2] K. Kendig. *Elementary Algebraic Geometry*, New York: Springer-Verlag, 1977.

[3] S. Lang. *Complex Analysis*, Springer Verlag, fourth edition, 1999.

[4] John B. Fraleigh. *A first course in Abstract Algebra*, Addison Wesley, seventh edition, 2002.

[5] I. R. Shafarevich. *Basic Algebraic Geometry*, Berlin: Springer-Verlag, 1977.