Nociones preliminares de geometría algebraica

Alexander Caviedes Castro
Miembro del grupo de Teoría de Representaciones de la Universidad Nacional de Colombia
Bogotá D.C, Colombia
alexcaviedes@hotmail.com

Stella Huérfano
Profesora Universidad Nacional de Colombia
Bogotá D.C, Colombia
s_huerfano@yahoo.com

Resumen

Se introducen las nociones elementales de Geometría algebraica y algunos teoremas, como el Teorema de la Base de Hilbert y el Teorema de los Ceros de Hilbert; dando una interpretación tanto algebraica como geométrica.

1. Introducción

El presente escrito pretende acercar y motivar a las personas a un primer estudio de la geometría algebraica con las definiciones, ejemplos y teoremas básicos. El escrito está dividido en dos partes: la primera que enuncia definiciones, ejemplos y teoremas que son independientes del álgebra (Teoría de Anillos, Teoría de cuerpos, Teoría de Grupos, etc.); la segunda, en la cual se definen conceptos como ideal de una variedad y variedad de un ideal y presenta algunos teoremas del álgebra tales como *El teorema de la base de Hilbert* y *El teorema de los ceros de Hilbert*, y cuyo objetivo primordial es mostrar, de una manera somera, la relación entre el álgebra y la geometría de las variedades algebraicas.

2. Definiciones y ejemplos

En nuestras consideraciones vamos a trabajar con los campos, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, de los números racionales, reales y complejos, respectivamente, los cuales se denotarán con las letras K y L.

Definición 1. *$K[X_1, ..., X_n]$ es el conjunto de polinomios en las variables $X_1, ..., X_n$, con coeficientes en el campo K , i.e., los elementos de la forma*

$$\sum a_{d_1,...,d_n} X_1^{d_1} \cdot ... \cdot X_n^{d_n}, \quad \text{donde} \quad a_{d_1,...,d_n} \in K.$$

Definición 2. *El conjunto* $L^n = \{(a_1, ..., a_n) : a_1, ..., a_n \in L\}$ *es el conjunto de* n*-plas de* L*. Un elemento de* L^n *se denotará por* $\vec{a}$*.*

En lo que sigue consideremos $K \subset L$, donde K y L son los campos anteriormente definidos.

Definición 3. *Un subconjunto* $V \subset L^n$ *es llamado una* K*-variedad algebraica sí existen polinomios* $f_1, ..., f_m \in K[X_1, ..., X_n]$ *tal que* V *es la solución del sistema de ecuaciones*

$$f_i(X_1, ..., X_n) = 0, \qquad i = 1, ..., m, \qquad en \quad L^n.$$

Cuando se necesite explicitar el sistema de ecuaciones que determina a V*, se denotará a* V *por* $\mathbb{V}_L(f_1, ..., f_m)$*.*

2.1. Ejemplos

1. Los conjuntos vacío, $\emptyset$, y L^n son *variedades algebraicas*; ya que $\emptyset$ está determinado por ejemplo por el sistema $X_1 = 1$ y $X_1 = 0$; mientras que L^n está determinado por el sistema $f(X_1, ..., X_n) = 0$, donde f es el polinomio cero, i.e., todo elemento de L^n es anulado por el polinomio cero.
L^n además es anulado *únicamente por cero*, esto es consecuencia del siguiente teorema:

Teorema 1. *Sea* $F(X_1, ..., X_n) \in K[X_1, ..., X_n]$ *un polinomio no nulo entonces existen infinitos puntos* $\vec{x} = (a_1, ..., a_n) \in L^n$ *tal que* $F(a_1, ..., a_n) \neq 0$*.*

Demostración: Sí $n = 1$, es bien sabido del álgebra elemental que un polinomio no nulo $F \in K[X_1]$, posee solamente un número finito de raíces, luego el complemento de este sistema solución es infinito.
Supongamos válido el resultado para n; sea
$F \in K[X_1, ..., X_n, X_{n+1}] = K[X_1, ..., X_n][X_{n+1}]$; luego F tiene una representación de la forma

$$F = \varphi_0 + \varphi_1 X_{n+1} + ... + \varphi_t X_{n+1}^t, \tag{1}$$

con $\varphi_i \in K[X_1, ..., X_n]$, $i = 0, ..., t$, y $\varphi_t \neq 0$ ya que $F \neq 0$. Por hipótesis de inducción existe $(a_1, ..., a_n) \in L^n$ tal que $\varphi_t(a_1, ..., a_n) \neq 0$. Luego el polinomio

$G(X_{n+1}) = F(a_1, ..., a_n, X_{n+1}) \neq 0$, y dado que L es infinito existen un número infinito de elementos $a_{n+1} \in L$ tal que $G(a_{n+1}) = F(a_1, ..., a_n, a_{n+1}) \neq 0$; lo cual prueba el resultado. □

Corolario 1. *Sí* $F \in K[X_1, ..., X_n]$ *y* $F(\vec{x}) = 0$ *para todo* $\vec{x} \in L^n$ *entonces* $F \equiv 0$.

Nótese que este resultado no es válido en todo campo L; sí $L = K = \mathbb{F}_2$ (donde $\mathbb{F}_2$ es el cuerpo fínito de tamaño 2), el polinomio $X^2 + X$ anula al campo L. Por lo anterior enfatizamos que se trabajará con los campos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ únicamente, y el anterior resultado es válido para estos campos.

2. **Variedades Lineales**: Son aquellas que son solución de un sistema de ecuaciones lineales con coeficientes en K, como por ejemplo las líneas rectas, planos , etc. El algebra lineal se encarga del estudio de este tipo de variedades.

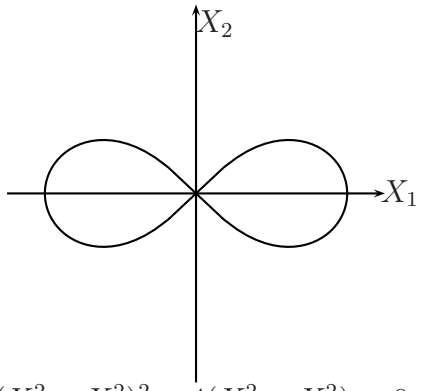
3. **Hipersuperficies**: Son aquellas que están definidas por una sola ecuación $f(X_1, ..., X_n) = 0$ (como las variedades de la tabla 1 y la figura 1). Toda variedad, por definición, es intersección finita de hipersuperficies. Cuando $L = \mathbb{R}$ ó $\mathbb{Q}$, toda variedad algebraica es hipersuperficie ya que para un sistema de ecuaciones $f_i(X_1, ..., X_n) = 0$, $i = 1, ..., m$; en L^n la variedad $\mathbb{V}_L(f_1, ..., f_n)$ es determinada por la ecuación única:

$$\sum_{i=1}^{m} f_i(X_1, ..., X_n)^2 = 0.$$

Otra propiedad de $L = \mathbb{R}$ ó $L = \mathbb{Q}$, es que el conjunto vacío, es una hipersuperficie (por ejemplo la ecuación $X_1^2 + X_2^2 + ... + X_n^2 + 1 = 0$ determina al conjunto vacío como solución en L^n); además otra situación peculiar es que un conjunto finito puede ser una hipersuperficie, por ejemplo la solución de $X_1^2 + X_2^2 = 0$ en L^2 es $(0, 0)$. Este tipo de situaciones no sucede cuando $L = \mathbb{C}$.

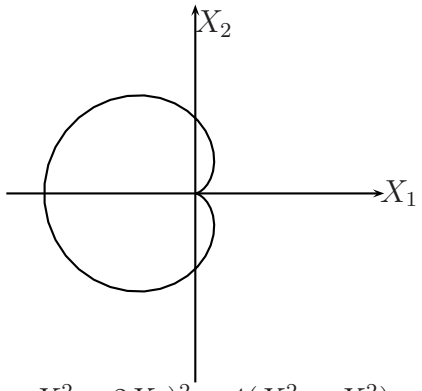
TABLA 1

LEMNISCATA



$(X_1^2 + X_2^2)^2 - 4(X_1^2 - X_2^2) = 0$

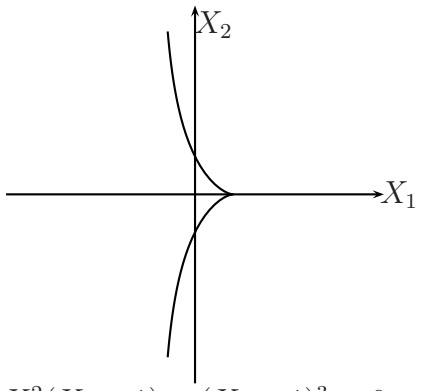
CARDIOIDE



$(X_1^2 + X_2^2 + 2X_1)^2 - 4(X_1^2 + X_2^2) = 0$

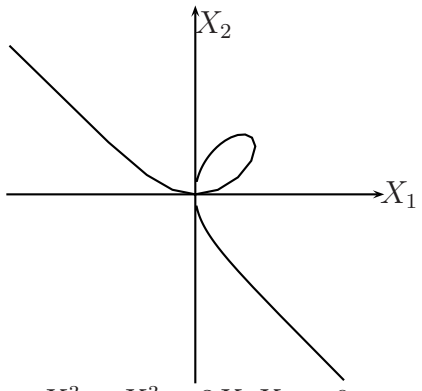
TABLA 1

CISOIDE



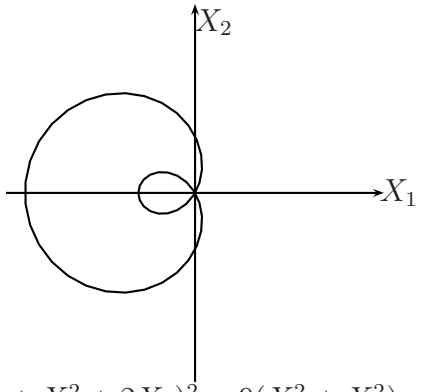
$X_2^2(X_1 + 1) + (X_1 - 1)^3 = 0$

CONCOIDE DE NICOMEDES



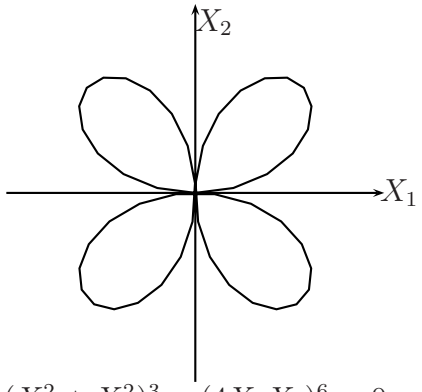
$X_1^3 + X_2^3 - 3X_1X_2 = 0$

CARACOL DE PASCAL



$4(X_1^2 + X_2^2 + 2X_1)^2 - 9(X_1^2 + X_2^2) = 0$

ROSA DE CUATRO HOJAS



$(X_1^2 + X_2^2)^3 - (4X_1X_2)^6 = 0$

Teorema 2. *Sea L el campo $\mathbb{C}$ y $H \subsetneq L^n$ una hipersuperficie. Sí $n = 1$ la*

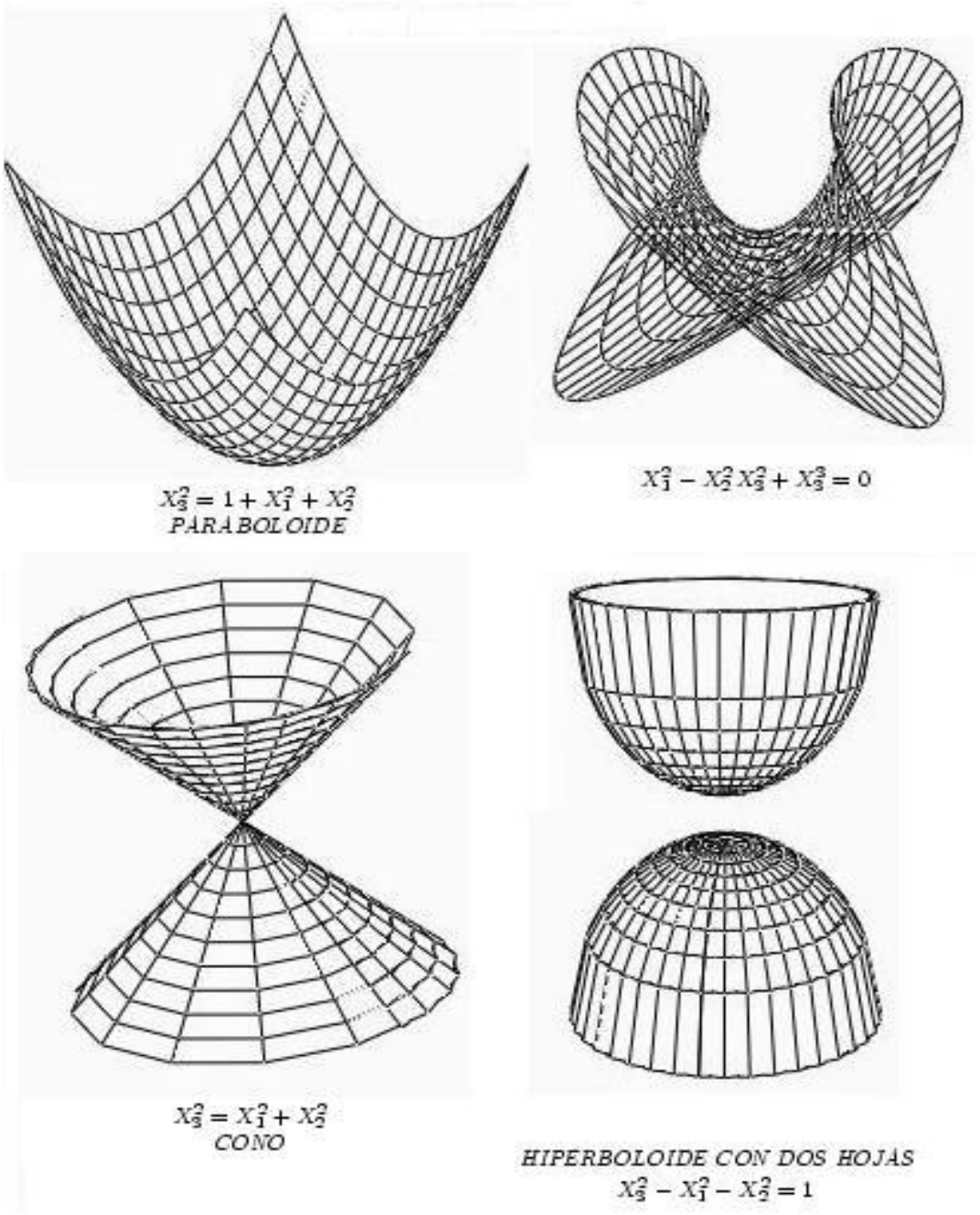


Figura 1: CURVAS ALGEBRAICAS EN $\mathbb{R}^3$

hipersuperficie H es finita y diferente de vacío y sí $n > 1$, H es infinita.

Demostración: Si $n = 1$, la hipersuperficie está definida por un polinomio no nulo de una sola variable $f(x) = a_m X^m + ... + a_1 X + a_0$, con $a_i \in K$, $i = 0, ..., m$, $a_m \neq 0$, $m \geq 1$ (ver corolario 1); el cual sabemos tiene m raíces debido al teorema fundamental del álgebra.
Sí $n > 1$ y la hipersuperficie H está dada por un polinomio $F \in K[X_1, ..., X_{n-1}, X_n]$; escribiendo F de modo análogo a como aparece en la ecuación (1), aplicando el teorema 1 para φ_t, existen infinitos $(a_1, ..., a_{n-1}) \in L^{n-1}$ tal que $\varphi_t(a_1, ..., a_{n-1}) \neq 0$. Sea $G_{a_1,...,a_{n-1}}(X_n) = F(a_1, ..., a_{n-1}, X_n)$, luego por el teorema fundamental del álgebra existe y_n tal que $G_{a_1,...,a_{n-1}}(y_n) = 0$, luego la hipersuperficie H dada por el polinomio F tiene infinitos puntos.

□

4. **Hipersuperficies de orden 2**: Son el conjunto solución de un polinomio de la forma:

$$\sum_{i,k=1}^{n} a_{ik} X_i X_k + \sum_{i=1}^{n} b_i X_i + c = 0.$$

Cuando $n = 2$, una hipersuperficie H de orden 2, $H \subset L^2$, puede ser: una cónica (parábola, elipse, hipérbola), dos rectas coincidentes, dos rectas paralelas, un conjunto finito o ningún lugar geométrico (ver Tabla 2); y la ecuación general de la hipersuperficie H de orden 2 es:

$$aX^2 + bXY + cY^2 + dX + eY + f = 0. \tag{2}$$

Esta última ecuación nos es familiar y de ella se encarga el estudio de la geometría analítica plana. Las hipersuperficies de orden 2 no degeneradas (cónicas) se pueden clasificar dependiendo del campo L. Sí $L = \mathbb{R}$ la ecuación general

$$aX^2 + bXY + cY^2 + dX + eY + f = 0,$$

representa una cónica del género parábola, elipse, hipérbola, según el indicador $I = b^2 - 4ac$, sea cero, negativo o positivo. Cuando L es $\mathbb{C}$ la ecuación general (2) representa una cónica del tipo parábola, sí $I = 0$, y elipse-hipérbola sí $I \neq 0$. Cuando $L = \mathbb{C}$, la hipérbola y la elipse son homeomorfas; para probarlo cada hipérbola es homeomorfa a la hipérbola dada por la ecuación $X_1^2 - X_2^2 - 1 = 0$ y las circunferencias y las elipses a la circunferencia unitaria dada por la ecuación $X_1^2 + X_2^2 - 1 = 0$, el homeomorfismo entre estas dos últimas está dado por:

$$\mathbb{V}_{\mathbb{C}}(X_1^2 + X_2^2 - 1 = 0) \to \mathbb{V}_{\mathbb{C}}(X_1^2 - X_2^2 - 1 = 0)$$

$$(x_1, x_2) \to (x_1, x_2 i).$$

Esta aplicación prueba que no hay "distinción"entre elipses e hipérbolas cuando L es $\mathbb{C}$.

TABLA 2

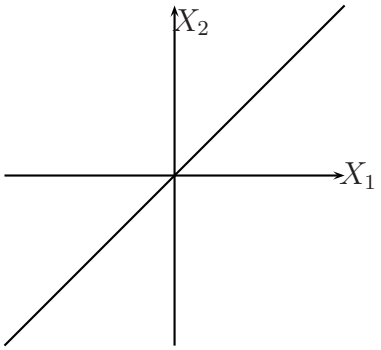
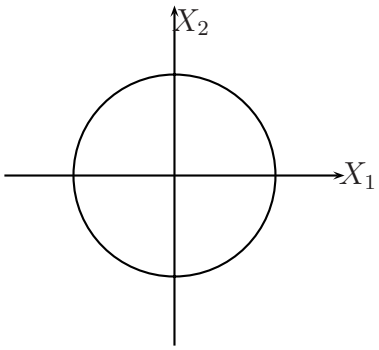
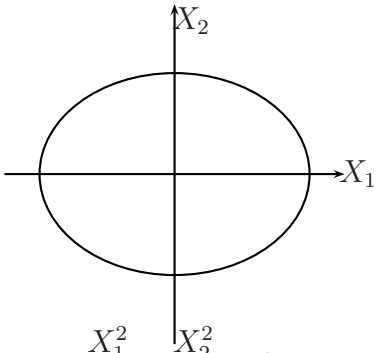
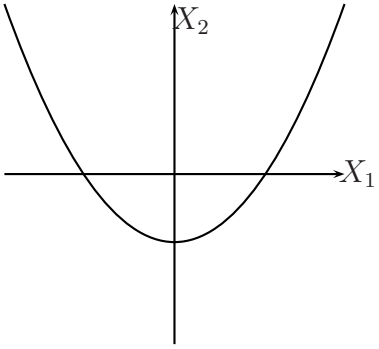
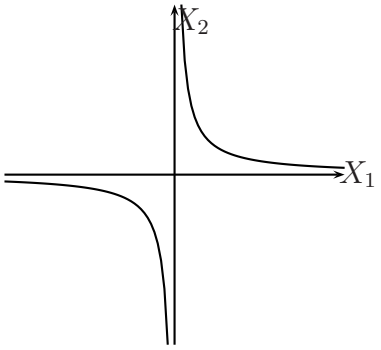
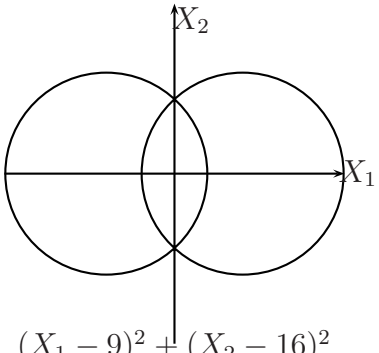
VARIEDAD LINEAL	CIRCUNFERENCIA
	
$X_2 - aX_1 = 0$	$X_1^2 + X_2^2 - R^2 = 0$

TABLA 2

ELIPSE	PARABOLA
	
$\frac{X_1^2}{a^2} + \frac{X_2^2}{b^2} = 0$	$X_2 - X_1^2 + a = 0$
HIPERBOLA	**UNION DE DOS CIRCUNFERENCIAS**
	
$X_2^2 - X_1^2 - 1 = 0$	$(X_1 - 9)^2 + (X_2 - 16)^2$ $+2(X_1^2 + 9)(X_2^2 - 16) = 0$

5. **Variedades homogéneas:** Son aquellas que son solución de un sistema homogéneo de polinomios (como por ejemplo el cono de la figura 1), i.e., los polinomios f_i que generan a la variedad son del mismo grado y son de la forma:

$$f_i = \sum a_{d_1,...,d_n} X_1^{d_1} \cdot ... \cdot X_n^{d_n},$$

donde $a_{d_1,...,d_n} = 0$ sí $d_1 + ... + d_n \neq d$ para $d \in \mathbb{Z}^+$ fijo. La propiedad más importante que gozan las variedades homogéneas es que el punto $(0, ..., 0) \in L^n$ está en la variedad y que toda recta que pasa por un punto de la variedad y $(0, ..., 0) \in L^n$, está totalmente contenida en ella; ya que para un polinomio homogéneo $f(X_1, ..., X_n) \in K[X_1, ..., X_n]$ y para $\vec{x} \in \mathbb{V}_L(f) \subset L^n$ tenemos que $f(tx_1, ..., tx_n) = 0$ para todo $t \in L$. Estas variedades son importantes en el estudio de las denominadas variedades proyectivas.

6. **Unión e intersección finita de variedades algebraicas es variedad algebraica:** Es suficiente probarlo para dos variedades. Sí la variedad V es descrita por un sistema $f_i(X_1, ..., X_n) = 0$, $i = 1, ..., m$; y la variedad W por el sistema $g_j(X_1, ..., X_n) = 0$, $j = 1, ..., l$, donde $f_1, ..., f_m, g_1, ..., g_l \in K[X_1, ..., X_n]$; la intersección está dada por el sistema de ecuaciones

$$f_i(X_1, ..., X_n) = 0,\ g_j(X_1, ..., X_n) = 0, \quad i = 1, ..., m, j = 1, ..., l.$$

La unión está dada por el sistema

$$f_i(X_1, ..., X_n) \cdot g_j(X_1, ..., X_n) = 0, \qquad i = 1, ..., m, j = 1, ..., l. \tag{3}$$

Para probarlo sea U la variedad generada por el sistema 3; $V \cup W \subset U$ ya que si $\vec{a} \in V \cup W$ entonces $\vec{a} \in V$ o $\vec{a} \in W$, luego $f_i(\vec{a}) = 0, i = 1, ..., m$; o $g_j(\vec{a}) = 0, j = 1, ..., l$; y por ende $f_i(\vec{a}) \cdot g_j(\vec{a}) = 0, i = 1, ..., m; j = 1, ..., l$; para la otra contenencia supongamos que existe $\vec{x} \in L^n$ tal que $\vec{x} \in U$ pero $\vec{x} \notin V \cup W$, luego existen i, j tal que $f_i(\vec{x}) \neq 0$ y $g_j(\vec{x}) \neq 0$ luego $f_i(\vec{x}) \cdot g_j(\vec{x}) \neq 0$ y por ende $\vec{x} \notin U$, lo cual es una contradicción y por ende $V \cup W = U$. Luego $V \cup W$ es variedad algebraica. La intersección infinita de variedades algebraicas también es variedad algebraica lo cual es una consecuencia del *teorema de la base de Hilbert*, que se discutirá más adelante.

7. **Ejemplos de conjuntos en L^n que no son variedades algebraicas:** Uno podría preguntarse si un conjunto dado es una variedad algebraica, por ejemplo el conjunto $S = \{(x, y) \in \mathbb{R}^2 : y - \sin(x) = 0\} \subset \mathbb{R}^2$(ver tabla 3). El siguiente enunciado nos proporciona una buena cantidad de ejemplos que no son variedades algebraicas:

Proposición 1. *Sí $V \subset L^n$ es una K-variedad algebraica entonces toda recta R de L^n está totalmente contenida en V ó intersecta a V a lo sumo en un número finito de puntos.*

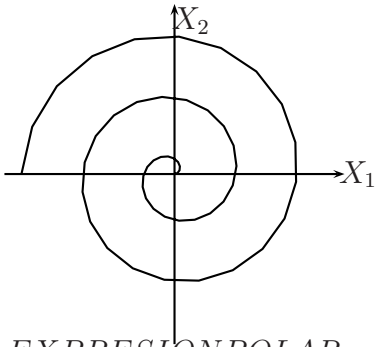
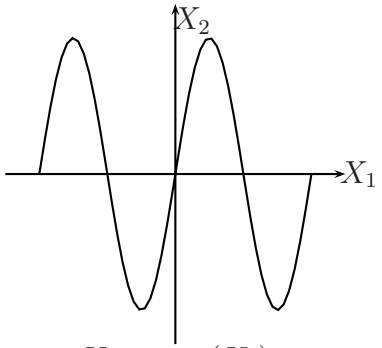
Demostración. Sea R una recta de L^n, luego $R = \{\vec{x} \in L^n : \vec{x} = t\vec{a}+\vec{b}\}$ para $\vec{a}, \vec{b} \in L^n$ elementos fijos y $t \in L$. Probemos el resultado primero para una hipersuperficie $V = \mathbb{V}_L(F(X_1, ..., X_n)), F \in K[X_1, ..., X_n]$. Sea $G(t) = F(t\vec{a}+\vec{b}), G(t) \in K[t]$; sí R intersecta a V en infinitos puntos esto quiere decir que $G(t) = 0$ para infinitos $t \in L$, luego $G(t) \equiv 0$, por el corolario 1. Luego la recta R está totalmente contenida en V. Por otro lado sí $G(t) = 0$ para un número fínito de puntos $t \in L$ entonces la recta R intersecta a la hipersuperficie V en un número fínito de puntos; luego el teorema es válido para hipersuperficies.

En el caso en que V sea una variedad arbitraria, $V = H_1 \cap ... , \cap H_l$, donde cada $H_j, j = 1, ..., m$, es una K-hipersuperficie. Sí R está totalmente contenida en V la proposición es válida para V, sí R no está totalmente contenida en V, R no está totalmente contenida en cada H_j, luego $R \cap H_j$ es finito para cada j y por ende $R \cap V$ es finito. □

Por ejemplo el conjunto S definido arriba *no* es variedad algebraica porque la recta $Y = 0$ lo corta en infinitos puntos y no está totalmente contenida en S. Usando la misma línea de razonamiento se prueba que los siguientes conjuntos no son variedades en $\mathbb{R}^2$:

i) $\{(x, 0) \in \mathbb{R}^2 : x \geq 0\}$, ii)$\{(x, x) \in \mathbb{R}^2 : x \geq 0\}$, iii) $\{(x, y) \in \mathbb{R}^2 : x, y \in \mathbb{Z}\}$, iv) $\{(x, y) \in \mathbb{R}^2 : x \in [0, 1], y = 0\}$, v) $\{(x, y) \in \mathbb{R}^2 : y = |x|\}$, vi)Espiral de Arquimedes (ver tabla 3).

TABLA 3

ESPIRAL DE ARQUIMENDES	CURVA SINOIDE
	
$EXPRESION POLAR$ $r = \theta$	$X_2 = sen(X_1)$

Sin embargo este resultado no nos dice por ejemplo sí el conjunto $C = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} - \{(-1, 0), (1, 0)\}$ es una variedad en $\mathbb{R}^2$. El siguiente resultado es más general que el anterior:

Proposición 2. *Sean* $\frac{P_1(t)}{Q_1(t)}, ..., \frac{P_m(t)}{Q_m(t)}$ *elementos de* $K(t)$ *(el conjunto de cocientes de polinomios en* $K[t]$*) y* $U = (\bigcup_{i=1}^{m} V_L(Q_i(t)))^c \subset L$*, si definimos* $\phi : U \to L^n$ *como* $\phi(t) = \left(\frac{P_1(t)}{Q_1(t)}, ..., \frac{P_m(t)}{Q_m(t)}\right)$*, entonces, sí* $V \subset L^n$ *es una* K*-variedad algebraica entonces* $\phi(U)$ *está totalmente contenida en* V *ó intersecta a* V *en a lo sumo un número fínito de puntos.*

Demostración. La demostración es análoga a la de la proposición anterior. □

Para demostrar que el conjunto C no es una variedad algebraica, sea $\phi : \mathbb{R} \to \mathbb{R}^2$ dada por $\phi(t) = \left(\frac{1 - t^2}{t^2 + 1}, \frac{2t}{t^2 + 1}\right)$, $\phi(\mathbb{R}) = C \cup (1, 0)$ y sí C fuera variedad algebraica $\phi\mathbb{R}$ estaría totalmente contenida en C, lo cual no es cierto, ó, $\phi(\mathbb{R})$ intersectaría a C en un número fínito de puntos, lo cual tampoco es cierto; luego C no es una variedad algebraica. De modo idéntico se prueba que los siguientes conjuntos no son variedades en $\mathbb{R}^2$:

i) $\{(x, y) \in \mathbb{R}^2 : y = x^2\} - \{(0, 0)\}$, ii)$\{(x, y) \in \mathbb{R}^2 : xy = 1, x > 0\}$.

8. **Puntos racionales de variedades algebraicas:** Sí $V \subset L^n$ es una variedad algebraica. Una pregunta interesante es: ¿Cuáles son los puntos racionales o enteros de la variedad V?, i.e., aquellos $\vec{x} \in L^n$ tal que las coordenadas de $\vec{x}$ son números racionales o números enteros. Por ejemplo *el último teorema de Fermat* se pregunta sobre la existencia de soluciones enteras no triviales de la ecuación de Fermat dada por

$$X_1^n + X_2^n - X_3^n = 0.$$

Sí $n = 2$, las soluciones de la ecuación de Fermat son las triplas pitagóricas, las cuales están totalmente determinadas y son infinitas. Sí $n \geq 3$ es conocido que esta ecuación no posee soluciones no triviales. Algunos de los problemas más interesantes de la geometría algebraíca son acerca de la existencia de puntos enteros o racionales de una variedad algebraica; existen numerosos aportes de importantes matemáticos que han producido importantes teoremas sobre soluciones enteras como por ejemplo Faltings, Mordell y Wyles entre otros (los dos primeros

recibieron medalla Fields). Esto nos muestra que en general abarcar un problema de este tipo, por sencillo que parezca, es realmente difícil. A continuación proporcionamos un ejemplo de este tipo de problemas:

Ejemplo 1.

$$V = V_K(X_1^2 + X_2^2 - 3) \cap \mathbb{Q}^2 = \phi$$

Que V tenga solución en $\mathbb{Q}^2$ es equivalente a que $V^* = V_k(X_1^2 + X_2^2 - 3X_3^2)$ tenga solución en $\mathbb{Z}^3$ distinta de $(0,0,0)$ (¿Por qué?). Supongamos que V^* tiene una solución (x_1, x_2, x_3) entera diferente de $(0,0,0)$ y supongamos que sea una solución positiva y la más pequeña posible, luego $x_1^2 + x_2^2 - 3x_3^2 = 0$. Como $x_1^2 + x_2^2 = 0 \pmod 3$; entonces x_1, x_2 son múltiplos de 3 (¿Por qué?), luego existen k_1, k_2, y alguno de ellos diferente de cero; tal que $x_1 = 3k_1, x_2 = 3k_2$; luego

$$9k_1^2 + 9k_2^2 = 3x_3^2,$$
$$3k_1^2 + 3k_2^2 = x_3^2,$$

luego x_3 es múltiplo de 3 y por consiguiente existe $k_3 \neq 0$ tal que $x_3 = 3k_3$ y por ende

$$3k_1^2 + 3k_2^2 = x_3^2 = 9k_3^2,$$
$$k_1^2 + k_2^2 = 3k_3^2$$

luego existe una solución más pequeña y no trivial, lo cual contradice nuestra condición inicial de que la tripla (x_1, x_2, x_3) es la solución más pequeña de V^*. Luego la variedad V no tiene puntos racionales. Este método propio de la *teoría de números* se llama *método del descenso infinito* y fue usado por Fermat para probar el *último teorema de Fermat* en el caso $n = 4$.

3. Ideales

La geometría algebraica, en un estudio más profundo de esta y para su verdadera comprensión, requiere del uso del álgebra, de hecho el álgebra viene a ser la base sólida en la que la geometría algebraica se construye. La finalidad del presente capítulo es dar las primeras definiciones para un estudio algebraico de la geometría de las variedades algebraícas y mostrar de una manera básica y al menos convicente, la relación entre el álgebra y la geometría de las variedades, hecho que el lector deberá descubrir por sí mismo.

En este capítulo se trabajará únicamente con anillos conmutativos con unidad, como por ejemplo el anillo de polinomios $K[X_1, ..., X_n]$.

Definición 4. *Un anillo conmutativo con unidad A es un conjunto dotado con dos operaciones internas, denotadas por " $+$"y " $\cdot$", tal que sí a, b y $c \in A$, entonces:*

1. $a + b = b + a$.
2. $a + (b + c) = (a + b) + c$.
3. *Existe $z \in A$, tal que para todo $a \in A$, $a + z = z + a = a$; z se denotá por 0".*
4. *Para $a \in A$, existe $s \in A$, tal que $a + s = 0$.*
5. $a \cdot b = b \cdot a$.
6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
7. *Existe $e \in A$, tal que para todo $a \in A$, $a \cdot e = e \cdot a = a$; e se denotá por 1.*

Definición 5. *Un ideal I de una anillo A es un sugrupo aditivo de A con la propiedad de que para todo $r \in I$ y $a \in A$ implica $a \cdot r \in I$.*

Definición 6. *Un ideal I de un anillo A se dice primo sí $a \cdot b \in I$ implica que $a \in I$ y $b \in I$.*

Definición 7. *Un ideal I de un anillo A se dice maximal sí $I \neq A$ y $I \neq \emptyset$ y es maximal en el conjunto de los ideales de A con respecto a la inclusión.*

Definición 8. *Sea I un ideal de un anillo A. El radical $Rad(I)$ es el conjunto de todos los elementos de $a \in A$ tal que existe $n \in \mathbb{Z}$ y $a^n \in I$. Un ideal J se dice radical sí $Rad(J) = J$.*

En la teoría de anilos se tienen los siguientes resultados conocidos para un anillo conmutativo con unidad A:

1. El anillo A poseé un ideal I maximal.
2. El ideal I es un ideal primo de A si y solo si A/I es un dominio entero.
3. El ideal I es un ideal maximal A si y solo si A/I es un cuerpo.

4. Todo ideal maximal es primo. Todo ideal primo es radical.

5. Sí A es cuerpo, poseé solamente los ideales triviales, i.e., sus únicos ideales son A y $\langle 0 \rangle$.

Definición 9. *La suma $\sum_{i \in J} I_i$ de una familia $\{I_i\}_{i \in J}$ de ideales de un anillo es el conjunto de todas las sumas $\sum_{i \in J} a_i$ con $a_i \in I_i$, $a_i \neq 0$ para solamente un número fínito de elementos $i \in J$.*

Definición 10. *Para un subconjunto $G = \{a_i\}_{i \in J}$ de un anillo A, se denotá por $\langle G \rangle = \langle \{a_i\}_{a_i \in J} \rangle$ al ideal más pequeño que contiene a G; $a \in \langle G \rangle$ sí existen $a_{i1}, ..., a_{im} \in G$, $r_1, ..., r_m \in A$ tal que $a = r_1 a_{i1} + ..., r_m a_{im}$.*

Definición 11. *Sea I un ideal de un anillo A, un conjunto de generadores del ideal I es un conjunto $G \subset I$ tal que $\langle G \rangle = I$. Sí es posible encontrar un conjunto de generadores G finito se dice que el ideal I es finitamente generado.*

Definición 12. *El conjunto*

$$\langle f_1, ..., f_m \rangle := \{\alpha_1 f_1 + ... + \alpha_m f_m : \alpha_j \in A,\ j = 1, ..., m\}; \tag{4}$$

donde $f_j \in A, j = 1, ..., m$, es el ideal finitamente-generado por los elementos $f_1, ..., f_m \in A$.

Las definiciones (11) y (12) concuerdan si $G = \{f_1, ..., f_m\}$. Es claro que a partir de la definición de ideal, la expresión (4) es un ideal de A. Sí I es un ideal de A, ¿Será I un ideal finitamente generado?. La respuesta a esta pregunta es NO; por ejemplo el anillo $A = K[X_1, ..., X_n, ...]$ el cual representa a los polinomios de variables $X_1, ..., X_n, ...$ con coeficientes en un campo K. En A consideremos el ideal $I = \langle X_1, ..., X_n, ... \rangle$, I no es finitamente generado. Sin embargo para un tipo importante de anillos esta propiedad se cumple.

Definición 13. *Un anillo A se dice noetheriano sí todo ideal de R es finitamente generado.*

Proposición 3. *Las siguientes proposiciones son equivalentes:*
i) R es noetheriano
ii)Cualquier cadena ascendente de ideales de R

$$I_1 \subset I_2 \subset ... \subset I_n \subset ...$$

se estabiliza, e.d, existe k tal que $I_k = I_{k+1} = ...$
iii)Cualquier conjunto no vacío de ideales de R contiene un elemento maximal respecto a la inclusión.

Demostración. i) $\rightarrow$ ii). Para una cadena de ideales como en ii), $I = \bigcup_{n=1}^{\infty} I_n$ es también un ideal de R. Por hipótesis es finitamente generado: $I = \langle r_1, ..., r_m \rangle, r_i \in R$. Para n suficientemente grande $r_i \in I_n$ $(i = 1, ..., m)$, luego $I_n = I_{n+1} = ...$
ii) $\rightarrow$ iii). Supongamos que hay un conjunto no vacío M de ideales de R sin un elemento maximal. Para cada $I_1 \in M$ existe $I_2 \in M$ tal que $I_1 \subsetneq I_2$. En este camino uno puede construir una cadena de ideales de R que no se estabiliza.
iii) $\rightarrow$ i). Sea I un ideal de R, y sea M el conjunto de todos los ideales finitamente generados por elementos de I es decir $M = \{\langle r_1, ..., r_m \rangle\}_{\{r_1,...,r_m \in I\}}$. M poseé un elemento maximal, $N = \langle s_1, ..., s_m \rangle$, $s_1, ..., s_m \in I$. Para cada $s \in I$, tenemos por la maximalidad del elemento N, que $N = \langle s_1, ..., s_m, s \rangle$, luego $s \in N$ para todo $s \in I$ y como $N \subset I$ entonces $N = I$. □

El siguiente teorema nos proporciona un gran número de anillos noetherianos:

Teorema 3 (Teorema de la base de Hilbert). *Sí R es un anillo noetheriano entonces $R[x]$ tambien es noetheriano.*

Demostración. Se demostrará la contrarrecíproca. Sea I un ideal de $R[x]$ que no es finitamente generado. Sea f_1 el polinomio de menor grado de I. Sí f_k , $k \geq 1$, ha sido ya escogido, sea f_{k+1} el polinomio de menor grado en $I - \langle f_1, ..., f_k \rangle$. Sea n_k el grado de f_k y $a_k \in R$ el elemento dominante de f_k $(k = 1, 2, ...)$. Por la escogencia de f_k nosotros tenemos que $n_1 \leq n_2 \leq ...$ y demostraremos que $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset ...$ es una cadena de ideales de R que no se estabiliza. Supongamos que la cadena se estabiliza, luego existe k tal que $\langle a_1, ..., a_k \rangle = \langle a_1, ...a_k, a_{k+1} \rangle$. Entonces $a_{k+1} = \sum_{i=1}^{k} b_i a_i$ $(b_i \in R)$ y sea $g := f_{k+1} - \sum_{i=1}^{k} b_i X^{n_{k+1}-n_i} f_i \in I - \langle f_1, ..., f_k \rangle$ el cual es de menor grado que f_{k+1}, contradiciendo la escogencia de f_{k+1}. □

Dado un cuerpo arbitrario K, K solamente poseé los ideales triviales entonces, K es obviamente noetheriano luego $K[X_1]$, $K[X_1][X_2] = K[X_1, X_2]$,...,$K[X_1, ..., X_n]$ son noetherianos.

Definición 14 (Ideal de una variedad). *Para $V \subset L^n$ una K-variedad algebraica el conjunto $\Im_K(V)$ de todos los $F \in K[X_1, ..., X_n]$ tal que $F(x) = 0$ para todo $x \in V$ es llamado el ideal de la variedad V en $K[X_1, ..., X_n]$.*

Definición 15 (Variedad de un ideal). *El conjunto de los ceros comunes en L^n de un ideal $I \subset K[X_1, ..., X_n]$ se llama la variedad del ideal I y se denotá por $\mathbb{V}_L(I)$.*

El ideal de una variedad es un ideal (ver definición 5); por otro lado la variedad de un ideal $I \subset K[X_1, ..., X_n]$ es en efecto una variedad ya que por ser $K[X_1, ..., X_n]$ noetheriano el ideal I es finitamente generado luego existen $f_1, ..., f_m \in K[X_1, ..., X_m]$ tal que $I = \langle f_1, ..., f_m \rangle$ y obviamente $\mathbb{V}_L(I) = \mathbb{V}_L(\langle f_1, ..., f_m \rangle) = \mathbb{V}_L(f_1, ..., f_m)$, luego $\mathbb{V}_L(I)$ es una variedad algebraica.

Para las operaciones $\Im$ y $\mathbb{V}$ las siguientes propiedades se tienen:

Proposición 4. *i)* $\Im(L^n) = \{0\}$, $\Im(\phi) = \langle 1 \rangle$
ii) Para una variedad $V \subset L^n$, $\Im_K(V) = Rad(\Im_K(V))$.
iii) Para cualquier variedad $V \subset L^n$, $\mathbb{V}_L(\Im_K(V)) = V$.
iv) Para dos variedades V_1, V_2, *se tiene que* $V_1 \subset V_2$ *si y solo si* $\Im_K(V_1) \supset \Im_K(V_2)$ *y* $V_1 \subsetneq V_2$ *si y solo si* $\Im_K(V_1) \supsetneq \Im_K(V_2)$.
v) Para dos variedades V_1, V_2, *se tiene que* $\Im_K(V_1 \cup V_2) = \Im_K(V_1) \cap \Im_K(V_2)$, $\Im_K(V_1 \cap V_2) = \Im_K(V_1) \cup \Im_K(V_2)$.
vi) Para cualquier familia $\{V_\lambda\}_{\lambda \in \Lambda}$ *de variedades* V_λ.

$$\bigcap_{\lambda \in \Lambda} V_\lambda = \mathbb{V}_L(\sum_{\lambda \in \Lambda} \Im_K(V_\lambda)).$$

vii) Para dos ideales $I, J \subset K[X_1, ..., X_n]$, $\mathbb{V}_L(I) \cup \mathbb{V}_L(J) = \mathbb{V}_L(I \cap J)$.
viii) Para un ideal I, *tenemos* $I \subset \Im_K(\mathbb{V}_L(I))$ *y* $Rad(I) \subset \Im_K(\mathbb{V}_L(I))$.

La prueba de las propiedades es consecuencia de las definiciones. De la proposición 4-vi) concluimos que la intersección arbitraria de variedades algebraicas es una variedad algebraica, de 4-ii) concluimos que el ideal de una variedad es un ideal radical, 4-iv) muestra que $V \to \Im(V)$ es una función inyectiva del conjunto de todas las K-variedades $V \subset L^n$ al conjunto de todos los ideales radicales de $K[X_1, ..., X_n]$.

Definición 16 (Variedad irreducible). *Una K-variedad es llamada irreducible sí: $V = V_1 \cup V_2$ para dos K-variedades V_1, V_2, implica $V = V_1$ o $V = V_2$*

Proposición 5. *Una K-variedad $V \subset L^n$ es irreducible si y solo si $\Im_K(V)$ es un ideal primo.*

Demostración. Sea V una variedad irreducible y sea $f_1 \cdot f_2 \in \Im_K(V) \subset K[X_1, ..., X_n]$. Para $H_i := \mathbb{V}_L(f_i)$ $(i = 1, 2)$. Como $f_1 \cdot f_2 \in \Im_K(V)$ entonces

$$\langle f_1, f_2 \rangle \subset \Im_K(V),$$

luego por 4-iii)-iv) tenemos que

$$\mathbb{V}_L(\langle f_1 \cdot f_2 \rangle) = \mathbb{V}_L(f_1 \cdot f_2) = H_1 \cup H_2 \supset V,$$

luego $V = (H_1 \cap V) \cup (H_2 \cap V)$, y dado que la variedad V es irreducible entonces $V = H_1 \cap V \subset H_1$ o $V = H_2 \cap V \subset H_2$, luego $f_1 \in \Im_K(H_1) \subset \Im_K(V)$ o $f_2 \in \Im_K(H_2) \subset \Im_K(V)$, luego $f_1 \in \Im_K(V)$ o $f_2 \in \Im_K(V)$ y por ende $\Im_K(V)$ es primo.

Supongamos ahora que $\Im_K(V)$ es primo y que existen K-variedades V_1, V_2 con $V = V_1 \cup V_2$, $V \neq V_i$ $(i = 1, 2)$.Por 4-v) $\Im_K(V) = \Im_K(V_1) \cap \Im_K(V_2)$ y $\Im_K(V_i) \neq \Im_K(V)$ $(i = 1, 2)$. Luego existen polinomios $f_i \in \Im_K(V_i)$, $f_i \notin \Im_K(V)$ $(i = 1, 2)$ luego $f_1 \cdot f_2 \in \Im_K(V_1) \cap \Im_K(V_2) = \Im_K(V)$, lo cual es contradictorio desde que $\Im_K(V)$ es un ideal primo. □

Las variedades irreducibles son a la geometría algebraica lo que los primos a la teoría de números. Las variedades algebraicas pueden descomponerse de manera única como unión finita de variedades irreducibles, de manera análoga a como los números enteros pueden descomponerse en producto de factores primos de manera única. Probaremos usando *el teorema de la base de Hilbert* que es posible encontrar una descomposición, de una variedad algebraica arbitraria, en unión de variedades irreducibles:

Teorema 4. *Cualquier K-variedad V puede descomponerse de la forma*

$$V = V_1 \cup ... \cup V_s \tag{5}$$

donde cada V_i $(i = 1, ..., s)$ es una variedad irreducible.

Demostración. Sea M el conjunto de subvariedades de V que no pueden ser escritas como unión fínita de variedades irreducibles. Supongamos que $M \neq \emptyset$, luego el conjunto "$\Im_K(M)$çonformado por los ideales de las variedades de M posee un elemento maximal I ya que $K[X_1, ..., X_n]$ es noetheriano. Luego $Y = \mathbb{V}_L(I) \in M$ es un elemento minimal en M por 4-iv), Y no es irreducible (ya que de ser irreducible $Y \notin M$), luego existen Y_1, Y_2 dos K-variedades tales que $Y = Y_1 \cup Y_2$, $(Y_i \neq \emptyset)$ $(i = 1, 2)$. Como $Y_i \subset V$ y como Y es un elemento minimal de M entonces $Y_i \notin M$ $(i = 1, 2)$ y por ende se puede escribir como

unión finita de variedades irreducibles lo cual implica que Y también, lo cual es contradictorio, luego $M = \emptyset$.
Como $M = \emptyset$, en particular $V \notin M$ y por ende M se puede escribir como unión finita de variedades irreducibles. □

Por ahora el *teorema de la base de Hilbert* nos ha servido para encontrar una descomposición de una variedad en variedades irreducibles y para probar que $\mathbb{V}_L(I)$ es una variedad para cualquier ideal I en $K[X_1, ..., X_n]$; por consiguiente por 4-vi) la intersección de cualquier cardinal de variedades es variedad, además, unión finita de variedades es variedad y tanto vacío como L^n son variedades, luego el conjunto de variedades conforman los cerrados de una topología en L^n, esta topología se llama la *K-topología de Zariski en L^n*. Las definiciones (14) y (15) muestran una conexión entre la geometría del espacio L^n y el álgebra del anillo $K[X_1, ..., X_n]$, además la geometría algebraica está provisto del lenguaje de la topología, si empleamos la topología de Zariski en su estudio; esto muestra que la geometría algebraica es un interesante puente de las diversas ramas del conocimiento matemático.

4. Teorema de los ceros de Hilbert

La aplicación $\Re : V \to \Im(V)$ que va de las variedades de L^n a los ideales radicales de $K[X_1, ..., X_n]$, es una aplicación inyectiva. Una pregunta natural es sí la aplicación $\Re$ es sobreyectiva, o equivalentemente, $I = \Im(\mathbb{V}(I))$. Esto no siempre sucede, por ejemplo sí $L = \mathbb{R}$ y el ideal $I = \langle x_1^2 + x_2^2 \rangle$, $\mathbb{V}_L(I) = (0, 0)$ y $\Im_K((0, 0)) = \Im_K(\mathbb{V}_L(I)) = \langle x_1, x_2 \rangle$ (¿Por qué ?) y $I \subsetneq \Im_K(\mathbb{V}_L(I))$ y el ideal I es radical por ser un ideal primo.

La aplicación $\Re$ es sobre sí $L = \mathbb{C}$; este resultado es conocido como *el teorema de los ceros de Hilbert*, solamente lo enunciaremos ya que la prueba es bastente técnica y propia del álgebra.

Teorema 5 (Teorema fuerte de los ceros de Hilbert). *Sí L es $\mathbb{C}$, la aplicación $\Re$ que asigna $V \to \Im_K(V)$, que va de las variedades algebraicas V en L^n a los ideales radicales de $K[X_1, ..., X_n]$ es biyectiva, i.e., $I = \Im_K(\mathbb{V}_L(I))$, para cualquier ideal radical I de $K[X_1, ..., X_n]$.*

Corolario 2. *Sí $L = \mathbb{C}$, para cualquier ideal I de $K[X_1, ..., X_n]$, $Rad(I) = \Im_K(\mathbb{V}_L(I))$.*

Demostración. Sea I un ideal de $K[X_1, ..., X_n]$, luego $Rad(I)$ es radical y por el teorema de los ceros tenemos que $Rad(I) = \Im_K(\mathbb{V}_L(Rad(I))) = \Im_K(\mathbb{V}_L(I))$. □

Para un ideal $I \subsetneq K[X_1, ..., X_n]$ podría suceder que $\mathbb{V}_L(I) = \emptyset$, sabemos de esto podría suceder sí $L = \mathbb{R}$, pero *NO* sí $L = \mathbb{C}$; veamos a continuación que esto es una consecuencia del teorema 5.

Teorema 6. *Sí L es $\mathbb{C}$ y $I \subsetneq K[X_1, ..., X_n]$ es un ideal no necesariamente radical entonces $\mathbb{V}_L(I) \neq \emptyset$*

Demostración. Sea I un ideal $I \subsetneq K[X_1, ..., X_n]$, luego $Rad(I) \subsetneq K[X_1, ..., X_n]$ ya que sí $Rad(I) = K[X_1, ..., X_n]$ entonces $1 \in Rad(I)$, luego existe n tal que $1 = 1^n \in I$, es decir, $I = K[X_1, ..., X_n]$. Como $Rad(I) \neq K[X_1, ..., X_n]$ y $Rad(I) = \Im_K(\mathbb{V}_L(I))$ entonces $\mathbb{V}_L(I) \neq \mathbb{V}_L(K[X_1, ..., X_n]) = \phi$ por el teorema 5. □

Corolario 3. *Sí $L = \mathbb{C}$; un sistema de ecuaciones algebraicas*

$$f_i = 0, \qquad i = 1, ..., m,$$

con polinomios $f_i \in K[X_1, ..., X_n]$ tiene una solución en L^n si y solo si $\langle f_1, ..., f_m \rangle \neq K[X_1, ..., X_n]$.

Las anteriores son algunas de las nociones básicas que introducen al lector interesado al estudio de la geometría algebraica, esperamos que este trabajo sea de alguna utilidad.