Geometría de curvas algebraicas

Claudia Reynoso *
Universidad de Guanajuato, Facultad de Matemáticas,
Callejón Jalisco s/n, A.P. 402, C.P. 36000,
Guanajuato, Gto. México

Estas notas tienen como objetivo principal enunciar los teoremas y conceptos fundamentales usados en geometría algebraica para iniciar el estudio de las variedades algebraicas afines, en particular estudiamos las curvas planas afines, que son variedades algebraicas de dimensión uno en el espacio afín de dimensión dos. Finalizamos el estudio de las curvas lanas afines analizando sus puntos singulares, rectas tangentes y el índice de intersección de dos curvas planas en un punto.

In these notes we will collect the definitions and important results of algebraic geometry required for beginning the study of algebraic affine varieties, in particular, the study of algebraic plane curves, which are algebraic affine varieties of dimension one in the affine space of dimension two. Finally we define the singular points and the tangent lines in the plane curves and also we study the intersection number of two curves at a point.

Palabras clave: Variedad alegbraica afín, curva plana afín, índice de intersección.
Keywords: Algebraic affine variety, affine plane curve, intersection index.

1. Introducción

Un **conjunto algebraico afín** es un conjunto geométrico que vive en un espacio al que llamaremos **espacio afín** y que está definido por los ceros de un conjunto de polinomios. Nosotros nos enfocaremos al estudio de las curvas planas afines, que son conjuntos algebraicos que viven en el plano afín y definidas por los ceros de un sólo polinomio no constante.

El objeto de estudio de la geometría algebraica son las **variedades algebraicas** (conjuntos algebraicos irreducibles), y la herramienta fundamental que utiliza para estudiar los fenómenos geométricos que se presentan en sus objetos es el álgebra, es decir, todos estos fenómenos tienen una traducción algebraica que nos ayuda a entenderlos.

Estas notas son una introducción al estudio de propiedades locales de curvas planas, daremos primero las definiciones y teoremas importantes para, en la última parte, estudiar estas propiedades.

La primera sección es un recordatorio de las definiciones y teoremas provenientes del álgebra que utilizaremos a lo largo del curso. En el segunda sección damos las definiciones de **n-espacio afín** y de conjunto algebraico, daremos una serie de propiedades que satisfacen los conjuntos algebraicos para, finalmente, definir la **topología**

*claudia@cimat.mx

de Zariski, que es la topología que dará al espacio afín estructura de espacio topológico.

La siguiente sección es el paso de la geometría al álgebra ya que definimos a partir de un conjunto en el espacio afín un ideal en el anillo de polinomios, tendremos, entonces, un ente completamente algebraico. Despúes estudiamos uno de los Teoremas Básicos en la geometría algebraica, el **Teorema de la Base de Hilbert**, este teorema nos dice que todo ideal en el anillo de polinomios con coeficientes en un campo es finitamente generado; en particular, todo ideal proveniente de un conjunto algebraico es finitamente generado.

En la siguiente sección damos la definición de variedad algebraica y damos también una caracterización algebraica que debe satisfacer un conjunto algebraico para ser variedad.

Nuestro principal objeto de estudio en estas notas son las **curvas algebraicas planas**, para esto estudiamos, en la siguiente sección, cómo son todos los conjuntos algebraicos del plano afín.

El siguiente tema es otro Teorema fundamental para la geometría algebraica, El **Teorema de los Ceros de Hilbert**, dicho teorema nos dice que si estamos trabajando en una campo algebraicamente cerrado, entonces existe una correpondencia biyectiva entre los ideales radicales del anillo de polinomios en n variables y entre los conjuntos algebraicos en el n-espacio afín.

Para tener un estudio completo de las variedades algebraicas debemos estudiar cómo son las funciones continuas respecto a la topología de Zariski que podemos definir de ellas al campo donde estamos trabajando, para esto es necesario definir el **anillo coordenado de una variedad**, el anillo coordenado resulta ser un dominio entero que parametriza las funciones continuas de la variedad al campo. Esto se estudia en la sección 9 de las notas.

La siguiente sección da la definición de **anillo local de una variedad en un punto**, de este anillo, como su nombre lo dice, se pueden leer las propiedades locales del punto en cuestión respecto a la variedad donde vive. Esto nos quedará más claro después de estudiar la útima sección dedicada al **índice de intersección de dos curvas en un punto**.

Finalmemte llegamos al estudio de propiedades locales de curvas planas, este estudio está enfocado al estudio de un tipo especial de puntos dentro de una curva, llamados **puntos singulares o múltiples** y al análisis del tipo de intersección entre dos curvas en un punto, esto es lo que se llama el índice de intersección.

2. Notación y Definiciones

Definición 1. **Un anillo conmutativo con** 1 es un conjunto R provisto de dos operaciones binarias, adición y multiplicación,

$$\begin{aligned} R \times R &\to R \\ + : (r, r') &\mapsto r + r' \\ \cdot : (r, r') &\mapsto r \cdot r' = rr', \end{aligned}$$

respectivamente, tal que

1. R es un grupo abeliano bajo la adición con elemento identidad 0,
2. la multiplicación es conmutativa y asociativa,
3. existe un elemento $1 \in R$ tal que $1r = r$ para todo $r \in R$,
4. se satisface la propiedad distributiva: $r(s + t) = rs + rt$ para todo $r, s, t \in R$.

A lo largo de estas notas vamos a suponer que el anillo R es conmutativo y con 1.

Definición 2. Un anillo R es un **dominio entero** si no hay divisores de 0, es decir, si dados $a, b \in R$, $a \neq 0, b \neq 0$, entonces $ab \neq 0$.

Definición 3. Un **ideal** de un anillo R es un subconjunto que contiene a 0 tal que:

1. Si $a, b \in I$ entonces $a - b \in I$;
2. si $a \in I$ y $r \in R$ entonces $ra \in I$.

Definición 4. El ideal I es **primo** si $I \subsetneq R$ y $ab \in I$ implica que $a \in I$ o $b \in I$.

Definición 5. El ideal I es **maximal** si para todo ideal J tal que $I \subset J \subsetneq R$ entonces $J = I$.

Definición 6. El ideal I es **finitamente generado** si existen $a_1, ..., a_n \in R$ tales que

$$I =< a_1, ..., a_n >:= \{\sum_{i=1}^{n} r_i a_i : r_i \in R\}.$$

Definición 7. Un elemento a en un anillo R es **irreducible** si para cualquier factorización $a = bc, b, c \in R$ entonces b o c son unidades en R, es decir, tienen inverso multiplicativo. Un dominio R es un **Dominio de Factorización Única (DFU)** si todo elemento no cero en R puede ser factorizado de manera única, salvo unidades.

Definición 8. Un ideal se llama **principal** si esta generado por un elemento. Un dominio es un **Dominio de Ideales Principales (DIP)** si todo ideal es principal.

Definición 9. Si R y S son anillos entonces la función $\phi : R \to S$ es un **homomorfismo de anillos** si para todo $r_1, r_2 \in R$ se tiene:

$$\begin{aligned} \phi(r_1 + r_2) &= \phi(r_1) + \phi(r_2) \\ \phi(r_1 r_2) &= \phi(r_1)\phi(r_2) \\ \phi(1_R) &= 1_S. \end{aligned}$$

Si un homomorfismo es uno a uno y sobre entonces se llama **isomorfismo**. Dos anillos se dicen **isomorfos** si existe un isomorfismo entre ellos.

Definición 10. Sea R un anillo y sea I un ideal de R. Definimos el **anillo cociente de R módulo I,** R/I como el conjunto de clases de la siguiente relación de equivalencia en R:

$$r_1 \sim r_2 \quad \text{si y sólo si} \quad r_1 - r_2 \in I.$$

La clase de un elemento $r \in R$ se denotará por $r + I$.

Teorema 1. Bajo las operaciones

$$\begin{aligned} R/I \times R/I &\to R/I \\ + : (r_1 + I, r_2 + I) &\mapsto r_1 + r_2 + I \\ \cdot : (r_1 + I, r_2 + I) &\mapsto r_1 r_2 + I \end{aligned}$$

el anillo cociente de R módulo I, R/I forma un anillo con elemento identidad para la adición I.

Definición 11. Sean R y S anillos y $\phi : R \to S$ un homormofismo. Definimos el **kernel de** ϕ como el conjunto $\text{Ker } \phi = \{r \in R : \phi(r) = 0\}$ y la **imagen de** ϕ como el conjunto $\text{Im } \phi = \{\phi(r) : r \in R\}$.

Observación: Se verifica facilmente que $\text{Ker } \phi$ es un ideal de R y que $\text{Im } \phi$ es un subanillo de S.

Teorema 2. (Teorema Fundamental de Homormofismos de Anillos) Sea R y S anillos y sea $\phi : R \to S$ un homomorfismo de anillos, entonces la aplicación

$$\begin{aligned} R/\text{Ker } \phi &\to \text{Im } \phi \\ r + \text{Ker } \phi &\mapsto \phi(r) \end{aligned}$$

es un isomorfismo de anillos.

Definición 12. Un anillo K es un **campo** si $K - \{0\}$ es un grupo bajo la multiplicación, con elemento identidad 1. Es decir, para todo $a \in K - \{0\}$, existe $a^{-1} \in K - \{0\}$ tal que $aa^{-1} = 1$.

Recordar que el anillo de polinomios con coeficientes en un anillo R en una variable es el conjunto

$$R[x] = \{\sum_{i=0}^{m} a_i x^i : a_i \in R, m \in \mathbb{N}\}.$$

Y la estructura de anillo la dan las operaciones

$$\sum_{i=0}^{m_1} a_i x^i + \sum_{i=0}^{m_2} b_i x^i = \sum_{i=0}^{max(m_1,m_2)} (a_i + b_i) x^i$$

$$\sum_{i=0}^{m_1} a_i x^i \sum_{i=0}^{m_2} b_i x^i = \sum_{i=0}^{m_1+m_2} (\sum_{j=0}^{i} a_j b_{i-j}) x^i.$$

El anillo de polinomios con coeficientes en un campo K en n variables es el conjunto

$$K[x_1, ..., x_n] = \{\sum_{i=0}^{m} F_i x_1^i : F_i \in K[x_2, ..., x_n]\}.$$

3. Espacio Afín y Conjuntos Algebraicos

Sea K un campo. El **n-espacio afín sobre** K como conjunto es simplemente el producto cartesiano n veces de K, es decir,

$$A^n(K) := \underbrace{K \times ... \times K}_{n \text{ veces}},$$

daremos a este espacio estructura de espacio topológico mediante la topología de Zariski que definiremos en esta sección. Si $n = 2$ entonces A^2 se llama **plano afín**.

Nota: Cuando no haya lugar a confusión vamos a omitir el K en la notación del n-espacio afín.

Sea $F \in K[x_1, ..., x_n]$, denotamos por $V(F)$ el conjunto de ceros de F, es decir $V(F) = \{(a_1, ..., a_n) \in A^n : F(a_1, .., a_n) = 0\}$. Si F es un polinomio no constante entonces $V(F)$ se llama **hipersuperficie definida por** F. Una hipersuperficie en A^2 se dice **curva plana afín**.

En general, si S es un subconjunto de $K[x_1, ..., x_n]$, entonces definimos **el conjunto de ceros de** S como el conjunto $V(S) = \{p \in A^n : F(p) = 0 \quad \forall F \in S\}$. Un conjunto $X \subset A^n$ es un **conjunto algebraico** si $X = V(S)$ para algún subconjunto $S \in K[x_1, ..., x_n]$. Las siguientes propiedades se pueden verificar facilmente:

1. $V(S) = \cap_{F \in S} V(F)$
2. Si I es el ideal en $K[x_1, ..., x_n]$ generado por S, entonces $V(S) = V(I)$, así que todo conjunto algebraico es de la forma $V(I)$ para algún ideal I de $K[x_1, ..., x_n]$.

3. Si $\{I_\alpha\}_{\alpha\in\Lambda}$ es una colección de ideales, entonces $V(\cup_{\alpha\in\Lambda} I_\alpha) = \cap_{\alpha\in\Lambda} V(I_\alpha)$.
4. Si $I \subset J$, entonces $V(J) \subset V(I)$.
5. $V(FG) = V(F) \cup V(G)$ para cualesquiera polinomios F y G. En general $V(I) \cup V(J) = V(\{FG : F \in I, G \in J\})$.
6. $V(0) = A^n$ y $V(1) = \emptyset$.

Las propiedades $(3), (5)$ y (6) nos dicen que $\{V(S) : S \subset K[x_1, ..., x_n]\}$ forman los cerrados de una topología en A^n llamada **topología de Zariski**. Los abiertos de esta topología son entonces complementos de conjuntos algebraicos.

Ejemplo 1: Puesto que todo ideal de $K[x]$ es principal tenemos que todo conjunto algebraico $V \subset A^1$ es el conjunto de ceros de un polinomio, es decir, existe $f \in K[x]$ tal que $V = V(f)$. Si f es un polinomio no constante entonces V es un conjunto finito que consta de las raíces de f en k. Hemos probado que los cerrados de Zariski de A^1 son: A^1, el vacío y conjuntos finitos. Entonces los abiertos distintos del vacío resultan ser conjuntos densos para la topología ordinaria en A^1.

El siguiente ejemplo muestra que la unión numerable de cerrados de Zariski no necesariamente es un cerrado.

Ejemplo 2: Sea K un campo de característica 0, es decir, $\mathbb{Q} \subset K$. Consideremos la colección numerable de conjuntos algebraicos $\{V(x-n)\}_{n\in\mathbb{Z}}$ en A^1. Entonces $\cup_{n\in\mathbb{Z}} V(x-n) = \mathbb{Z}$ y $\mathbb{Z}$ no es un conjunto algebraico en A^1.

4. El ideal de un conjunto de puntos

En la sección anterior definimos a partir de un conjunto de polinomios, o del ideal generado por este conjunto de polinomios, un conjunto en el espacio afín, ahora vamos a asociar a un subconjunto en un espacio afín un ideal en el anillo de polinomios.

Sea $X \subset A^n$. Definimos el conjunto $I(X) = \{F \in K[x_1, ..., x_n] : F(p) = 0 \quad \forall p \in X\}$, se puede probar facilmente que este conjunto es un ideal en $K[x_1, ..., x_n]$, así que se llama el **ideal de** X. Las siguientes propiedades muestran algunas relaciones entre ideales y conjuntos algebraicos:

1. Si $X \subset Y$, entonces $I(Y) \subset I(X)$.
2. $I(\emptyset) = K[x_1, ..., x_n]$.
3. $I(\{(a_1, ..., a_n)\}) = (x_1 - a_1, ..., x_n - a_n)$.
4. $I(V(S)) \supset S$ para cualquier $S \subset K[x_1, ..., x_n]$.
5. $V(I(X)) \supset X$ para cualquier $X \subset A^n$.
6. Si V es un conjunto algebraico entonces $V = V(I(V))$.

7. Si I es el ideal de un conjunto algebraico entonces $I = I(V(I))$.

La primera pregunta importante que surge a partir de la definición de ideal de un conjunto de puntos de A^n es la siguiente: ¿Para cada ideal I de $K[x_1, ..., x_n]$ existe $X \subset A^n$ tal que $I = I(X)$? La respuesta, como lo muestra el siguiente ejemplo, es negativa.

Ejemplo: Consideremos el ideal $< x^2 > \subset \mathbb{C}[x]$. Supongamos que existe $X \subset A^1(\mathbb{C})$ no vacío tal que $< x^2 >= I(X) := \{f(x) \in \mathbb{C}[x] : f(p) = 0 \quad \forall p \in X\}$. Sea $p \in X$. Como $x^2 \in I(X)$ entonces $p^2 = 0$, por tanto $p = 0$. Así que $X = \{0\}$, pero $I(\{0\}) =< x >$. La conclusión es que $< x^2 >$ no es el ideal de ningún conjunto de puntos.

Mencionaremos entonces una propiedad importante que satisfacen los ideales que son ideales de un conjunto de puntos en A^n: Sea $X \subset A^n$, $I(X) = \{F \in K[x_1, ..., x_n] : F(p) = 0 \quad \forall p \in X\}$. Supongamos que $F^n \in I(X)$ para algún entero $n > 0$ y sea $p \in X$ entonces $F^n(p) = 0$, como K no tiene divisores de cero entonces $F(p) = 0$ así que $F \in I(X)$.

Definición 13. Sea I un ideal de un anillo R. Definimos el **radical de I** como $Rad(I) = \{a \in R : a^n \in I \quad \text{para algún entero } n > 0\}$. Un ideal I se llama **radical** si $I = Rad(I)$.

Hemos probado entonces la siguiente

Proposición 1. $I(X)$ es un ideal radical para todo $X \subset A^n$. De manera equivalente, si $I \subset K[x_1, ..., x_n]$ no es un ideal radical entonces no existe ningún subconjunto $X \subset A^n$ tal que $I = I(X)$.

En la sección 8 veremos que si el campo en el que estamos trabajando es algebraicamente cerrado, entonces todo ideal radical es el ideal de un conjunto de puntos en el espacio afín.

5. Teorema de la Base de Hilbert

El Teorema de la Base de Hilbert data de finales del siglo XIX, es un teorema básico en la geometría algebraica porque nos dice, entre otras cosas, que todo conjunto algebraico está definido por un conjunto finito de polinomios.

Definición 14. Un anillo R se dice **Noetheriano** si todos sus ideales son finitamente generados.

Teorema 3. (Teorema de la Base de Hilbert) Si R es un anillo Noetheriano entonces $R[x_1, ..., x_n]$ es un anillo Noetheriano.

Prueba. Ver demostración en [1] página 27. ■

Corolario 1. Todo conjunto algebraico en A^n está definido por un conjunto finito de polinomios.

Prueba. Consideremos el conjunto algebraico $V(I)$ para algún ideal $I \subset K[x_1, ..., x_n]$. Como el campo K es Noetheriano (pues sus únicos ideales son (0) y $K = (1)$) entonces $K[x_1, ..., x_n]$ es Noetheriano así que $I = (F_1, ..., F_r)$, entonces $V(I) = V(F_1, ..., F_r)$. ■

Corolario 2. Todo conjunto algebraico en A^n es la intersección de un número finito de hipersuperficies.

Prueba. Para todo conjunto algebraico $V \subset A^n$, existen polinomios $F_1, ..., F_r \in K[x_1, ..., x_n]$ tales que $V = V(F_1, ..., F_r)$, así que $V = V(F_1) \cap ... \cap V(F_r)$ por la propiedad 1 de la sección 3. ■

6. Componentes irreducibles de un conjunto algebraico

Los entes básicos que se estudian en geometría algebraica son los conjuntos algebraicos irreducibles; irreducibles en el sentido que definiremos a continuación.

Un conjunto algebraico $V \in A^n$ es **reducible** si $V = V_1 \cup V_2$, donde V_1, V_2 son conjuntos algebraicos en A^n y $V_i \neq V$, $i = 1, 2$. En caso contrario se dice que V es **irreducible**.

Proposición 2. Un conjunto algebraico V es irreducible si y sólo si $I(V)$ es un ideal primo.

Prueba. Si $I(V) = \{F \in K[x_1, ..., x_n] : F(p) = 0 \quad \forall \quad p \in V\}$ no es primo entonces existe $F_1, F_2 \in K[x_1, ..., x_n] - I(V)$ tales que $F_1F_2 \in I(V)$. Entonces $V = (V \cap V(F_1)) \cup (V \cap V(F_2))$ y $V \cap V(F_i) \subsetneq V$, $i = 1, 2$, así que V es reducible.

Inversamente, supongamos que $V = V_1 \cup V_2$, $V_i \neq V$, entonces $I(V_i) \supset I(V)$; sea $F_i \in I(V_i), F_i \notin I(V)$. Entonces $F_1F_2 \in I(V)$, así que $I(V)$ no es primo. ■

Definición 15. Un conjunto algebraico irreducible en A^n se llama **variedad algebraica afín**

El siguiente teorema nos dice que todo conjunto algebraico se descompone como unión de variedades algebraicas afines, de aquí que sea suficiente, en geometría algebraica, enunciar resultados para éstas.

Teorema 4. Sea V un conjunto algebraico en A^n. Entonces existen únicos conjuntos algebraicos irreducibles $V_1, ..., V_m$ tales que $V = V_1 \cup ... \cup V_m$ y $V_i \not\subset V_j$ para $i \neq j$.

Prueba. Ver demostración en [2] página 16. ■

Ejemplo: En general es difícil encontrar las componentes irreducible de un conjunto algebraico. Ver por ejemplo la página de [3], en este ejemplo se calculan las componentes irreducibles de $V(xz-y^2, x^3-yz)$ usando las llamadas **Bases de Groebner**. La descomposición de este conjunto en componentes irreducibles es $V(x,y) \cup V(xz-y^2, x^3-yz, x^2y-z^2)$

7. Subconjuntos algebraicos del plano

El principal objetivo de estas notas es estudiar algunas propiedades locales de curvas planas, es decir, hipersuperficies que viven en A^2. Como veremos en esta sección, estos son los conjuntos algebraicos que tiene sentido estudiar en el plano afín pues el resto son puntos aislados, el vacío y el total.

Proposición 3. Sean F y G polinomios en $K[x,y]$ sin factores comunes. Entonces $V(F,G) = V(F) \cap V(G)$ es un conjunto finito de puntos.

Prueba. Si F y G no tienen factores en común en $K[x][y]$, entonces no tienen factores en común en $K(x)[y]$. Esto se sigue del siguiente hecho general: Si R es un dominio de factorización única (DFU) con campo de cocientes K, entonces todo elemento irreducible $F \in R[x]$ es irreducible visto como elemento en $K[x]$.

Como $K(X)$ es un campo entonces $K(x)[y]$ es un dominio de ideales principales (DIP), así que $< F, G >=< 1 >$ en $K(x)[y]$, entonces existen $R, S \in K(x)[y]$ tales que $RF + SG = 1$.

Existe un polinomio no cero $D \in K[x]$ tal que $DR := A, DS := B \in K[x][y]$. Por lo tanto tenemos que $A(x,y)F(x,y) + B(x,y)G(x,y) = D(x)$.

Si $(a,b) \in V(F,G)$ entonces $D(a) = 0$, pero D tiene sólo un número finito de ceros. Esto muestra que sólo un número finito de $x - coordenadas$ pertenecen a los puntos de la variedad. De manera análoga se prueba que sólo existen un número finito de $y - coordenadas$. ■

Corolario 3. Si K es un campo infinito, entonces los subconjuntos algebraicos irreducibles de A^2 son: A^2, $\emptyset$, $\{p\}$, tal que $p \in A^2$ y curvas planas irreducibles $V(F)$, donde F es un polinomio irreducibles y $V(F)$ es infinito.

8. Teorema de los ceros de Hilbert (Nullstellensatz)

En esta sección estudiamos el Teorema de los Ceros de Hilbert, el cual es más conocido por su nombre en alemán: Nullstellensatz.

En la sección 4 vimos que si un ideal I de $K[x_1, ..., x_n]$ no es radical, entonces no puede ser el ideal de un conjunto de puntos de A^n. Pero será cierto que todo ideal radical es el ideal de un conjunto de puntos? Para campos algebraicamente cerrados la respuesta es afirmativa y nos la da el Teorema de los ceros de Hilbert, este Teorema nos dice que si I es radical, entonces I es el ideal de puntos de $V(I)$.

También mencionaremos en esta sección el Teorema Débil de los Ceros, que, como veremos, es una generalización del Teorema Fundamental del Álgebra y que puede obtenerse como corolario del Teorema de los Ceros de Hilbert.

A lo largo de esta sección vamos a suponer que K es un campo algebraicamente cerrado, es decir, todo polinomio $F(x) \in K[x]$ tiene sus raices en K.

Teorema 5. (Teorema débil de los ceros de Hilbert) Si I es un ideal propio de $K[x_1, ..., x_n]$ entonces $V(I) \neq \emptyset$.

Otra manera de enunciar este Teorema es la siguiente: Si $(F_1, ..., F_r) = \{\sum_{i=1}^{r} G_i F_i : G_i \in K[x_1, ..., x_n]\} \subsetneq K[x_1, ..., x_n]$ entonces el sistema

$$\begin{aligned} F_1(x_1, ..., x_n) &= 0 \\ F_2(x_1, ..., x_n) &= 0 \\ &\vdots \\ F_r(x_1, ..., x_n) &= 0 \end{aligned}$$

tiene solución en A^n.

Observación: Si consideramos el campo $\mathbb{R}$ (el cual no es algebraicamente cerrado) entonces $< x^2 + 1 > \subsetneq \mathbb{R}[x]$ y $x^2 + 1 = 0$ no tiene soluciones en $\mathbb{R}$.

Teorema 6. (Teorema de los ceros de Hilbert) Sea I un ideal en $K[x_1, ..., x_n]$. Entonces $I(V(I)) = Rad(I)$.

Prueba. Ver demostración en [2] página 20. ■

A partir del Teorema de los Ceros podemos concluir el Teorema Débil: Sea $I \subset K[x_1, ..., x_n]$ un ideal propio. Supongamos que $V(I) = \emptyset$ entonces $I(V(I)) = I(\emptyset) = K[x_1, ..., x_n] = Rad(I)$, la última igualdad implica que $1 \in I$ así que $I = K[x_1, ..., x_n]$ y esto es una contradicción.

El siguiente corolario es sumamente importante porque establece relaciones biyectivas entre objetos algebraicos y objetos geométricos.

Corolario 4. Existe una correspondencia uno a uno entre las siguientes colecciones:

$$\{I \subset K[x_1, ..., x_n] : I \text{ es ideal radical}\} \leftrightarrow \{X \subset A^n : X \text{ es algebraico}\}$$
$$I \mapsto V(I)$$

si I es un ideal primo entonces es un ideal radical, así que:

$$\{I \subset K[x_1, ..., x_n] : I \text{ es ideal primo}\} \leftrightarrow \{X \subset A^n : X \text{ es variedad algebraica}\}$$
$$I \mapsto V(I)$$

$$\{I \subset K[x_1, ..., x_n] : I \text{ es ideal maximal}\} \leftrightarrow A^n$$
$$(x_1 - a_1, ..., x_n - a_n) \mapsto (a_1, ..., a_n)$$

9. Anillo Coordenado

Ahora empezaremos a estudiar las funciones continuas respecto a la topología de Zariski de una variedad algebraica al campo donde está definida, el concepto básico en este tema es el de anillo coordenado.

Si $V \subset A^n$ es una variedad entonces $I(V)$ es un ideal primo y

$$\Gamma(V) = \frac{K[x_1, ..., x_n]}{I(V)}$$

es un dominio entero al que llamaremos **anillo coordenado de** V. Y la pregunta es: Qué representa $\Gamma(V)$ para la variedad V?

Sea $\mathscr{F}(V, K) = \{f : V \to K : f \text{ es función}\}$. Bajo las operaciones

$$\begin{aligned} \mathscr{F}(V,K) \times \mathscr{F}(V,K) &\to \mathscr{F}(V,K) \\ \cdot : (f,g) \mapsto fg : V &\to K \\ x &\mapsto f(x)g(x) \\ + : (f,g) \mapsto f+g : V &\to K \\ x &\mapsto f(x)+g(x) \end{aligned}$$

$\mathscr{F}(V, K)$ es un anillo donde podemos identificar a K con el subanillo de las funciones constantes en $\mathscr{F}(V, K)$. Un elemento $f \in \mathscr{F}(V, K)$ es una **función polinomial** en V si existe $F \in K[x_1, ..., x_n]$ tal que $f(a_1, ..., a_n) = F(a_1, ..., a_n)$ para todo $p = (a_1, ..., a_n) \in V$. El conjunto de funciones polinomiales de V forma un subanillo en $\mathscr{F}(V, K)$.

Definimos el siguiente homomorfismo de anillos

$$K[x_1, ..., x_n] \to \mathscr{F}(V, K)$$
$$F \mapsto F_{|V},$$

el kernel de este homomorfismo es $\{F \in K[x_1, ..., x_n] : F(p) = 0 \quad \forall p \in V\} = I(V)$, así que, por el Teorema Fundamental de Homomorfismos de Anillos, $\Gamma(V)$ es isomorfo al subanillo de $\mathscr{F}(V, K)$ de funciones polinomiales en V en K.

Nosotros definimos los cerrados de Zariski como ceros de polinomios, podemos entonces concluir que el conjunto de funciones polinomiales de una variedad V en K es el conjunto de funciones continuas respecto a la topología de Zariski de V en K, donde estamos identificando a K con A^1.

10. Anillo Local de una Variedad en un punto

El anillo local de una variedad en un punto es un subanillo del campo de fracciones del anillo coordenado de la variedad, que nos da, como su nombre lo dice, información geométrica local del punto como parte de la variedad donde se encuentra, ver por ejemplo el teorema 7.

Sea V una variedad afín. El campo de fracciones del anillo coordenado $\Gamma(V)$ es

$$K(V) = \{\frac{F}{G} : F, G \in \Gamma(V), G \neq 0\}.$$

Un elemento de $K(V)$ se llama **función racional de** V.

Sea $R \in K(V)$ y sea $p \in V$. Diremos que R está **definida** en p si existen $F, G \in \Gamma(V)$ tales que $R = \frac{F}{G}$ y $G(p) \neq 0$.

Definición 16. Definimos el **anillo local de** V **en** p como el conjunto $\mathscr{O}_P(V) = \{R \in K(V) : R \text{ está definida en } p\}$.

Notar que $\mathscr{O}_p(V)$ es un subanillo de $K(V)$. Entonces tenemos la siguiente cadena de contenciones:

$$K \subset \Gamma(V) \subset \mathscr{O}_p(V) \subset K(V),$$

donde un elemento en K define una función polinomial constante en $\Gamma(V)$ y una función polinomial $f \in \Gamma(V)$ es el elemento $\frac{f}{1} \in \mathscr{O}_p(V)$.

11. Propiedades locales de curvas planas

Finalmente vamos a estudiar propiedades locales de curvas planas, estas propiedades están relacionadas con puntos singulares o múltiples de las curvas, con la idea en geometría algebraica de recta tangente a la curva en un punto y con el índice de intersección de dos curvas en un punto.

11.1 Puntos Múltiples y Líneas Tangentes

En esta sección vamos a suponer que el campo K es algebraicamente cerrado.

Definición 17. El **grado** de una curva plana es el grado del polinomio que define la curva. Una curva de grado uno es una **línea**

Nota: Llamaremos curva indistintamente al polinomio que la define y a la variedad.

Sea F una curva y sea $p = (a, b) \in F$, entonces p se llama **punto singular de** F si $F_x(p) := \frac{\partial F}{\partial x}(p) = 0$ y $F_y(p) := \frac{\partial F}{\partial y} = 0$. Si p es no-singular, es decir, si $F_x(p) \neq 0$ o $F_y(p) \neq 0$, entonces existe la **línea tangente a** F **en** p cuya ecuación es $F_x(p)(x - a) + F_y(p)(y - b) = 0$. Una curva sin puntos singulares se llama **curva no-singular**.

Sea F una curva y sea $p = (0, 0)$. Escribimos $F = F_m + F_{m+1} + ... + F_n$ donde $F_i \in K[x, y]$ es homogéneo de grado i y $F_m \neq 0$. Decimos entonces que m es **la multiplicidad de** F **en** p y la denotamos por $m = m_p(F)$. Notar que:

1. $p \in F$ si y sólo si $m_p(F) > 0$
2. p es no-singular para F si y sólo si $m_p(F) = 1$.

Definición 18. Si $m = 2$ se dice que p es un **punto doble para** F, si $m = 3$ es un **punto triple**, etc.

Como F_m es un polinomio homogéneo en 2 variables entonces $F_m = \Pi L_i^{r_i}$ donde las L_i son líneas distintas. Usaremos entonces la siguiente terminología:

$$L_i = \text{líneas tangentes a } F \text{ en } p$$
$$r_i = \text{multiplicidad de la tangente } L_i.$$

Definición 19. Si F tiene m líneas tangentes distintas en p entonces decimos que p es un punto **múltiple ordinario de** F. Un punto doble ordinario se llama **nodo**.

Sea $F = \Pi F_i^{e_i}$ la factorización de F en componentes irreducibles. Entonces $m_p(F) = \sum e_i m_p(F_i)$ y si L es una línea tangente a F_i con multiplicidad r_i, entonces L es tangente a F con multiplicidad $\sum e_i r_i$.

Ahora veamos cómo extender estas definiciones a un punto $p = (a, b) \neq (0, 0)$. Consideremos la traslación

$$\begin{aligned} T : A^2 &\to A^2 \\ (x, y) &\mapsto (x + a, y + b) \end{aligned}$$

entonces descomponemos $F^T := F \circ T(x, y) = F(x+a, y+b)$ como $F^T = G_m + G_{m+1} + ...$, donde $G_i \in K[x, y]$ es homogéneo de grado i, definiremos entonces $m_p(F) := m_{(0,0)}(F^T)$.

11.2 Índice de Intersección

Sea F y G curvas planas y sea $p \in A^2$. El objetivo de esta sección es definir un entero positivo que mida (en algún sentido) la manera en que las curvas $V(F)$ y $V(G)$ se intersectan en el punto p. Este entero se llamará el **índice de intersección de** F **y** G **en** p y se denotará por $I(p, F \cap G)$.

Vemos a pedirle a la definición de índice, $I(p, F \cap G)$, que satisfaga los siguiente axiomas, casi todos ellos son propiedades intuitivas que queremos tener de $I(p, F \cap G)$. A partir de estos axiomas se puede probar el teorema que nos dice cómo podemos definir el índice de intersección de dos curvas en un punto a partir del anillo local del plano afín en el punto y de los polinomios que definen las curvas.

1. Si $F \neq G$ entonces para todo $p \in A^2$ $I(p, F \cap G) \in \mathbb{Z}^{\geq 0}$. Si $F = G$ entonces para todo $p \in V(F)$ $I(p, F \cap G) = \infty$.
2. $I(p, F \cap G) = 0$ si y sólo si $p \notin F \cap G$.
3. Si T es un cambio afín de coordenadas en A^2 entonces $I(T(p), F^T \cap G^T) = I(p, F \cap G)$.
4. $I(p, F \cap G) = I(p, G \cap F)$

   Las curvas F y G se **intersectan transversalmente en** p si p es un punto no-singular para F y G, y si la línea tangente a F en p es diferente de la línea tangente a G en p. Queremos que $I(p, F \cap G) = 1$ si y sólo si las curvas se intersectan transversalmente o, más generalmente
5. $I(p, F \cap G) \geq m_p(F) m_p(G)$, con igualdad si y sólo si F y G no tienen líneas tangentes en común.
6. Si $F = \Pi F_i^{r_i}$ y $G = \Pi G_j^{s_j}$, entonces $I(p, F \cap G) = \sum_{i,j} r_i s_j I(p, F_i \cap G_j)$.
7. $I(p, F \cap G) = I(p, F \cap (G + AF))$ para todo $A \in K[x, y]$.

Teorema 7. Sean F y G curvas y $p \in A^2$. Existe una única definición de $I(p, F \cap G)$ de tal manera que se satisfacen las propiedades anteriores, dicha definición es:

$$I(p, F \cap G) = dim_K \frac{\mathscr{O}_p(A^2)}{(F, G)\mathscr{O}_p(A^2)}.$$

Prueba. Ver demostración en [2] página 75. ■

En general $\frac{\mathscr{O}_p(V)}{I\mathscr{O}_p(V)}$ es un espacio vectorial sobre K, asi que podemos calcular su dimensión.

Puesto que $\mathscr{O}_p(A^2) = \{\frac{A}{B} : A, B \in K[x, y], B(p) \neq 0\}$, entonces los elementos con inverso multiplicativo en este anillo son las funciones en $\mathscr{O}_p(A^2)$ que no se anulan en p. Para calcular esta dimensión como espacio vectorial debemos ver a F y G como elementos del anillo local.

Ejemplo 1: Consideremos las siguientes curvas

$$F(x, y) = q(x, y) + xr(x, y)$$
$$G(x, y) = q(x, y) + yr(x, y),$$

en el anillo $\mathbb{C}[x, y]$ tales que q y r son homogéneos de grado d sin componenetes en común. Calcularemos el índice de intersección de estas curvas en el punto $p = (0, 0)$.

$$I(p, F \cap G) = dim_{\mathbb{C}} \frac{\mathscr{O}_p(A^2)}{< q(x, y) + xr(x, y), q(x, y) + yr(x, y) >},$$

tenemos que

$$< q(x, y) + xr(x, y), q(x, y) + yr(x, y) >=< r(x - y), q + yr >$$

por lo tanto

$$\begin{aligned} I(p, F \cap G) &= dim_{\mathbb{C}} \frac{\mathscr{O}_p(A^2)}{<r(x-y), q+yr>} \\ &= dim_{\mathbb{C}} \frac{\mathscr{O}_p(A^2)}{<r, q+yr>} + dim_{\mathbb{C}} \frac{\mathscr{O}_p(A^2)}{<x-y, q+yr>}. \end{aligned}$$

El primer sumando se calcula facilmente usando (5) puesto que p y q no son invertibles en el anillo $\mathscr{O}_p(A^2)$, tienen grado d y no tienen componentes en común.

$$I(p, r \cap q + yr) = I(p, r \cap q) = m_p(r)m_p(q) = d^2.$$

Sólo resta calcular el segundo sumando, para ello necesitamos considerar dos casos:

1) Supongamos que $x-y$ no divide a q

$$dim_{\mathbb{C}}\frac{\mathscr{O}_p(A^2)}{< x-y, q+yr >} = dim_{\mathbb{C}}\frac{\mathscr{O}_0(A^1)}{< ax^{d+1}+bx^d >} = dim_{\mathbb{C}}\frac{\mathscr{O}_0(A^1)}{< x^d(ax+b) >}$$

puesto que $ax+b$ es invertible en la localización ya que $b \neq 0$, entonces

$$dim_{\mathbb{C}}\frac{\mathscr{O}_0(A^1)}{< x^d(ax+b) >} = dim_{\mathbb{C}}\frac{\mathscr{O}_0(A^1)}{< x^d >}.$$

Para calcular esta última dimensión vamos a utilizar la siguiente proposición cuya demostración puede ser consultada en la página 57 de [2].

Proposición 4. Si $V(I) = \{p\}$ entonces $\frac{K[x_1,...,x_n]}{I}$ es isomorfo a $\frac{\mathscr{O}_p(A^n)}{I\mathscr{O}_p(A^n)}$. Así que:

$$dim_K\frac{K[x_1,...,x_n]}{I}) = dim_K\frac{\mathscr{O}_p(A^n)}{I\mathscr{O}_p(A^n)}.$$

Entonces, como $V(x^d) = \{0\}$, tenemos que $dim_{\mathbb{C}}\frac{\mathscr{O}_0(A^1)}{<x^d>} = dim_{\mathbb{C}}\frac{\mathbb{C}[x]}{(x^d)} = d$. En este caso $I(p, F \cap G) = d^2 + d$.

2) Supongamos que $x-y$ divide a q

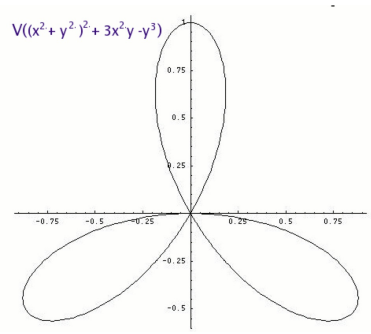
$$dim_{\mathbb{C}}\frac{\mathscr{O}_p(A^2)}{< x-y, q+yr >} = dim_{\mathbb{C}}\frac{\mathscr{O}_0(A^1)}{< ax^{d+1} >} = dim_{\mathbb{C}}\frac{\mathbb{C}[x]}{ax^{d+1}} = d+1$$

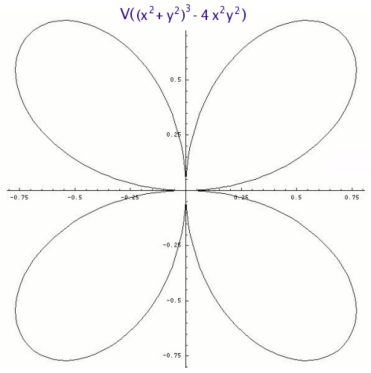
En este caso $I(p, F \cap G) = d^2 + d + 1$.

Ejemplo 2: Calcular el índice de intersección de las curvas

$$E(x,y) = (x^2+y^2)^2 + 3x^2y - y^3$$
$$F(x,y) = (x^2+y^2)^3 - 4x^2y^2$$

en el punto $p = (0,0)$. En $\mathbb{R}^2$ las curvas correspondientes se ven de la siguiente manera:





Empezaremos reemplazando F por

$$F - (x^2+y^2)E = y((x^2+y^2)(y^2-3x^2) - 4x^2y) = yG$$

y ahora reemplazaremos G por

$$G + 3E = y(5x^2 - 3y^2 + 4y^3 + 4x^2y) = yH.$$

Entonces

$$I(p, E\cap F) = I(p, E\cap(F + E(3y-(x^2+y^2))) =$$
$$I(p, E\cap(F-(x^2+y^2)E + 3Ey)) = I(p, E\cap(yG+3Ey)) =$$
$$I(p, E\cap y(G+3E)) = I(p, E\cap y^2H) =$$
$$2I(p, E\cap y) + I(p, E\cap H).$$

Por (7) y (6) $I(p, E \cap H) = I(p, x^4 \cap y) = 4$ y $I(p, E \cap H) = m_p(E)m_p(H) = 6$ por (5), así que $I(p, E \cap F) = 14$.

Agradecimientos

Quiero agradecer al Dr. Víctor Castellanos por la invitación para participar en la Primera Escuela de Invierno de Geometría y Dinámica impartiendo el curso "Introducción a la Geometría de Curvas Algebraicas"; muchas gracias también a la Universidad Juárez Autónoma de Tabasco por la hospitalidad brindada.

Referencias

[1] David Eisenbud: *Commutative Algebra, with a View Toward Algebraic Geometry.* Springer-Verlag, 1995.

[2] William Fulton: *Algebraic Curves. An Introduction to Algebraic Geometry.* W. A. Benjamin, Inc., 1969.

[3] David Cox, John Little, Donal O'Shea: *Ideals, Varieties, and Algorithms.* Springer-Verlag, 1991.