Introducción a la Geometría Algebraica

Nicholas Mc-Donnell

1er semestre 2019

Índice general

Info

Libro: "Algebraic Curves" William Fulton

Libro 2: "Introduction to Commutative Algebra" Atiyah, Mac Donald

Notas: Tareas

Capítulo 1

Introducción

1.1. Motivación

Estudio de objetos geométricos derivados de los polinomios (Variedades $\rightarrow$ Esquemas, etc). Los objetos son suaves o singulares.

1.1.1. Resolución de singularidades para una curva

Consideramos el siguiente polinomio:

$$\{(x, y) \in \mathbb{C}^2 : f(x, y) := y^2 - x^2(x + 1) = 0\} = C$$

Definición 1.1.1 (Singularidad)**.** Es $p \in \mathbb{C}^2$ tal que $f(p) = 0$, $f_x(p) = 0$ y $f_y(p) = 0$

En el ejemplo el $(0, 0)$ es el único punto singular.
Considerar el morfismo:

$$\mathbb{C}^2 \xrightarrow{\sigma} \mathbb{C}^2$$
$$(u, v) \mapsto (uv, v)$$

Vemos la pre-imagen:

$$\begin{aligned} \sigma^{-1}(C) &= \{v^2 - u^2v^2(uv + 1) = 0\} \\ &= \{v^2 = 0\}\{1 - u^2(uv + 1) = 0\} \end{aligned}$$

Ejemplo: 1.1.1.

$$\mathbb{C}^2 \longrightarrow \mathbb{C}^2$$
$$T(x, y) = (-x, -y)$$

T es automorfismo de $\mathbb{C}^2$

$$T \circ T = 1$$

Lo qye sucede es que el grupo $\{1, T\} = G$ actua en $\mathbb{C}^2$.
Mirar $\mathbb{C}^2/G$ =espacio de órbitas de G, lo cuál es una variedad algebraica
Funciones regulares en $\mathbb{C}^2 = \mathbb{C}[x, y]$.
Queremos buscar lo siguiente:

$$\mathbb{C}[x, y]^G = \{f(x, y)\text{polinomio tal que } f(x, y) = f(-x, -y)\} = \mathbb{C}[x^2, y^2, xy]$$

$$\mathbb{C}[x^2, y^2, xy] \simeq \mathbb{C}[a, b, c]/(c^2 - ab)$$

$$\therefore \mathbb{C}^2/G := \{(a, b, c) \in \mathbb{C}^3 : c^2 - ab = 0\}$$

Ejemplo: 1.1.2.

$$\{(x, y) \in k^2 : x^{2n} + y^{2n} = 1\} = V(k)$$

Cómo se ve $V(k)$? ($V(k) \neq \emptyset$)
$n = 1$

$k = \mathbb{Q}$: Circunferencia porosa ($x = \frac{t^2-1}{t^2+1}, y = \frac{2t}{t^2+1}$)(Viene de $\mathbb{Z}$, aritmético)

$k = \mathbb{R}$: Circunferencia completa (Viene de Análisis/límites)

$k = \mathbb{C}$: Esfera sin puntos?

$n \geq 2$: $V(\mathbb{Q}) \subset V(\mathbb{R}) \subset V(\mathbb{C})$

$V(\mathbb{Q})$: Ultimo Teorema de Fermat $\implies$ 4ptos

$V(\mathbb{R})$: Algo que se acerca a un cuadrado con n “grande”

$V(\mathbb{C})$: Objeto extraño con $g = (n-1)(2n-1)$ agujeros

Variedades = ceros de polinomios $\in k[x_1, ..., x_n]$ donde $k = \overline{k}$

1.2. Preliminares Algebraicos

- Anillos conmutativos con 1, y morfismos de anillos, tal que el $1 \mapsto 1$
- Dominios (sin div. del cero) y cuerpos (todo $u \neq 0$ es unidad)
- R anillo $\to R[x]$, grado, mónico. En general: $R[x_1, ..., x_n]$
- Polinomios homogeneos: $F \in R[x_1, ..., x_n]$ ssi $F(\lambda x_1, ..., \lambda x_n) = \lambda^{\deg(F)} F(x_1, ..., x_n)$
- $a \in R$ es <u>irreducible</u> si a no unidad, no cero y $a = bc \implies b$ o c es unidad

- $a \in R$ es primeo si $a \mid bc \implies a \mid b$ o $a \mid c$
- R es UFD (DFU): Todo elemento se factoriza de forma única salvo orden y unidades. (R UFD $\implies R[x]$ UFD)
- Dado R dominio existe $F =$ cuerpo de fracciones de $R \supset R$, $F = \{\frac{a}{b} : a, b \in R, b \neq 0\}$
- f morfismo, $\ker f$ (ideal) $\operatorname{Im} f$ (anillo)
- Ideal $\cong$ Kernel (Primer teorema de Isomorfismo)
- Para $S \subset R$ anillo, $< S >=$ Ideal generado por S

Definición 1.2.1 (Ideal Primo)**.** $p \subset R$ ideal primo ssi $ab \in p \implies a \in p \vee b \in p$

Teorema 1.2.1. *p primo $\iff R/p$ dominio.*

Demostración. p ideal primo

$$\begin{aligned} & ab = 0 \\ \iff & ab \in p \\ \iff & a \in p \vee b \in p \\ \iff & a = 0 \vee b = 0 \end{aligned}$$

□

Definición 1.2.2 (Ideal Maximal)**.** $p \subset R$ es maximal ssi $p \subset m \subset R$, m ideal $\implies p = m \vee m = R$

Teorema 1.2.2. *m maximal $\iff R/m$ es cuerpo*

Demostración. $\implies$
Sea $a \in R \setminus m$, por lo que $a \neq 0$, luego ya que m maximal, $< m, a >= R$. Dado esto, sabemos que $\exists b \in m, \exists c, d \in R : bc + ad = 1$, y viendo esto en R/m tenemos que $ad = 1$, o sea, a tiene inverso.
$\impliedby$
Por contradicción, existe n ideal maximal que contiene a m □

Problema 1.2.1. Sea R un dominio.

1. Si F, G son formas[1] de grado r, s respectivamente en $R[x_1, ..., x_n]$, muestre que FG es una forma de grado $r + s$
2. Muestre que todo factor de una forma en $R[x_1, ..., x_n]$ también es una forma

Problema 1.2.2. Sea R un DFU, K el cuerpo cociente de R. Muestre que todo elemento z de K se puede escribir

[1] Polinomios homogeneos

1.3. Conjuntos Algebraicos

Definición 1.3.1 (Espacio Afín)**.** El **Espacio afín** de dimensión n es $\mathbb{A}_k^n := k^n$

Definición 1.3.2 (Hipersuperficie)**.** Dado $F \in k[x_1, ..., x_n]$, se define la **hipersuperficie**

$$V(F) := \{(a_1, ..., a_n) \in k^n : F(a_1, ..., a_n) = 0\}$$

Ejemplo: 1.3.1. $V(y^2 - x^2(x+1)) \subset \mathbb{A}_{\mathbb{R}}^2$

Ejemplo: 1.3.2. $V(ax^2 + by^2 + 1) \subset \mathbb{A}_{\mathbb{R}}^2 = \emptyset$, dado $a, b > 0$, distinto a $V(x^2 + y^2 + 1) \subset \mathbb{A}_{\mathbb{C}}^2$

Ejemplo: 1.3.3. $V(y^2 - x(x^2 - 1)) \subset \mathbb{A}_{\mathbb{R}}^2$

Ejemplo: 1.3.4. $V(z^2 - x^2 - y^2) \subset \mathbb{A}_{\mathbb{R}}^3$

Ejemplo: 1.3.5. $V((x^2 - y^2)(x^3 - 1)(y^3 - 1)) \subset \mathbb{A}_{\mathbb{R}}^2$

Definición 1.3.3 (Conjunto Algebraico)**.** Sea $S \subset k[x_1, .., x_n]$. Un **conjunto algebraico afín**

$$\begin{aligned} V(S) &= \{p \in \mathbb{A}_k^n : F(p) = 0 \forall F \in S\} \\ &= \bigcap_{F \in S} V(F) \end{aligned}$$

$S = \{F_1, ..., F_m\}, V(S) = V(F_1, ..., F_m)$

Propiedades 1.3.4 (Conjuntos Algebraicos)**.**

1. Si $I =< S > \implies V(S) = V(I)$

   Demostración. Sea $p \in V(S) \implies F(p) = 0 \forall F \in S$.
   Sea $G \in I \implies G = r_1F_1 + ... + r_mF_m,\ F_1, ..., F_m \in S\ r_1, ..., r_m \in k[x_1, ..., x_n]$

   $$\therefore G(p) = r_1(p)F_1(p) + ... + r_m(p)F_m(p) = 0 \implies p \in V(I)$$

   Si $p \in V(I) \implies$ en particular $F(p) = 0 \forall F \in S \subset I \implies p \in V(S)$

   $$\therefore V(I) = V(S)$$

   □

2. $\{I_\alpha\}_{\alpha \in J}$ familia de ideales $\implies V(\bigcup_{\alpha \in J} I_\alpha) = \bigcap_{\alpha \in J} V(I_\alpha)$

3. $I \subset J$ ideales $\implies V(I) \supset V(J)$

4. $V(FG) = V(F) \cup V(G)$ Sea I, J ideales $\implies V(I) \cup V(J) = V(< \{FG : F \in I, G \in J\} >)$

5. $V(\emptyset) = \mathbb{A}_k^n,\ V(1) = \emptyset$

Observación 1.3.1. La **unión** arbitraria de conjuntos algebraicos no es necesariamente conjunto algebraico:

$$\mathbb{N} = V(I)?$$

Observación 1.3.2 (Topología de Zariski)**.** Los conjuntos algebraicos definen los **conjuntos cerrados** para una topología en $\mathbb{A}_k^n$ ($\mathbb{A}_k^n \backslash$cerrados = abiertos). Los cerrados de esta topología son $\{\emptyset, \mathbb{A}_k^n, \text{conj. finitos}\}$

Definición 1.3.5 (Ideal de un conjunto)**.** Sea $X \subset \mathbb{A}_k^n$. $I(X) = \{f \in k[x_1, ..., x_n] : f(p) = 0 \forall p \in X\}$

Propiedades 1.3.6 (Ideales de conjuntos)**.**

1. $I(X)$ es ideal:

   Demostración. $f, g \in I(X) \implies f(p) + g(p) = 0, \forall p \in X \implies f + g \in I(X)$
   $r \in k[x_1, .., x_n], f \in I(X) \implies r(p)f(p) = r(p) \cdot 0 = 0 \forall p \in X \implies rf \in I(X)$ □

2. $X \subset Y \implies I(X) \supset I(Y)$

3. $I(\emptyset) = k[x_1, ..., x_n]$, $I(\mathbb{A}_k^n) = (0)$ si k es un cuerpo infinito. $I(\{a_1, ..., a_n\}) = (x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$ $a_i \in k$

4. $I(V(S)) \supset S$ $\forall$ conj. $S \subset k[x_1, .., x_n]$, $V(I(X)) \supset X \forall X \subset \mathbb{A}_k^n$

5. $V(I(V(S))) = V(S)$ $\forall$ conj. de pol. S, $I(V(I(X))) = I(X) \forall X \subset \mathbb{A}_k^n$

6. Si $V =$ conj. alg. $\implies V = V(I(V))$, si $I =$ ideal $\implies I = I(V(I))$

Observación 1.3.3. Si $I = I(X)$ y $\exists m \in \mathbb{N} : F^m \in I$, entonces $F \in I$

Definición 1.3.7 (Ideal Radical)**.** Si I es ideal de R, entonces el ideal Radical es:

$$\operatorname{rad} I = \{a \in R : \exists m \in \mathbb{N} a^m \in I\}$$

1.4. Base de Hilbert

Teorema 1.4.1 (Base de Hilbert)**.** *Todo conjunto algebraico es la intersección de un número finito de hipersuperficies.*

Definición 1.4.1 (Anillo Noetheriano)**.** Sea R anillo. R se dice **Noetheriano** ssi todo ideal de R es finitamente generado.

Observación 1.4.1. Notar que k cuerpo es Noetheriano, y que los DIP son Noetherianos.

Teorema 1.4.2 (Hilbert)**.** *R Noetheriano $\implies$ $R[x_1, ..., x_n]$ Noetheriano*

Demostración. $F(x) = a_0 + a_1x + ... + a_dx^d \in R[x]$ $a_d \neq 0$, a_d se llamará término líder de F ($a_d = l(F)$).
Sea $I \subset R[x]$ ideal, Sea $J \subset R$ el conjunto de todos los términos líderes de elementos en I

Observación 1.4.2. J es ideal

$\therefore$ Por hipótesis $J =< l(F_1, ..., l(F_r)) >$.
Sea $N > \deg(F_i) \forall i = 1, .., r$
Para cada $m \leq N$, sea J_m el conjunto de los coeficientes líderes de $F \in I$ con $\deg(F) \leq n$. Notamos que J_m es ideal.
$\therefore$ Por hipótesis, $J_m =< \underbrace{l(F_{m,i})}_{\text{Finitos}} >$ con $\deg(F_{m,i}) \leq m$.

$$I' =< F_1, ..., F_r, \bigcup_{m=1}^{N} \{F_{m,i}\} >$$

Notar que $I' \subseteq I$. Sea $G \in I \setminus I'$ tal que su grado es lo más pequeño posible.
Caso 1: Si $\deg(G) > N \implies \exists$ polinomios $\{Q_i\}$ tal que G y $\sum_{i=1}^{r} Q_i \cdot F_i$ tienen el mismo líder: Sea $l(G) = \sum_{i=1}^{r} \alpha_i \cdot l(F_i)$

$$\therefore Q_i = \alpha_i \cdot x^{\deg(G) - \deg(F_i)}$$

$$\therefore \deg(\underbrace{G - \sum Q_i \cdot F_i}_{\in I}) < \deg(G)$$

Y $G - \sum Q_i \cdot F_i \notin I'$ en otro caso $G \in I' \rightarrow\leftarrow$
Caso 2: Si $\deg(G) \leq N \implies \deg(G) = m \leq N$
$\therefore$ hacer lo mismo con J_m $\square$

Corolario. *$k[x_1, ...x_m]$ es Noetheriano.*

Definición 1.4.2 (Reducible/Irreducible)**.** $V \subset \mathbb{A}^n$ conjunto algebraico. Si $V = V_1 \cup V_2$ donde V_1, V_2 son conjuntos algebraicos en $\mathbb{A}^n$ y $V \neq V_i, i = 1, 2 \implies$ se dice que V es **reducible**. Si no, es **irreducible**

Ejemplo: 1.4.1. $V(xy) \subset \mathbb{A}^2_k$, $V(xy) = V(x) \cup V(y) \implies V(xy)$ es reducible.

Ejemplo: 1.4.2. $\{p, q\} \subset \mathbb{A}^n_k$, $V = \{p, q\} = \{p\} \cup \{q\}$

Ejemplo: 1.4.3. $V(x^2) \subset \mathbb{A}^2$, $(x^2) = I$ no es primo

Proposición 1.4.3. *V irred. ssi $I(V)$ es primo*

Demostración. Si $I(V)$ no primo $\implies F_1, F_2 \in k[x_1, ..., x_2]$ con $F_1F_2 \in I(V)$, pero $F_i \notin I(V)$ $i = 1, 2$

$$\implies V = (V \cap V(F_1)) \cup (V \cap V(F_2)), V \cap V(F_i) \nsubseteq V$$

Si $p \in V \implies F_1(p) \cdot F_2(p) = 0 \implies F_1(p) = 0 \vee F_2(p) = 0$.
Luego $\exists q_i \in V$ tal que $F_i(q_i) \neq 0 \implies q_i \notin V \cap V(F_i)$
$\therefore V$ es reducible $\square$

Lema 1.4.4. *$\mathcal{J} \neq \emptyset$ conjunto arbitrario de ideales en un anillo Noetheriano R, entonces existe elemento maximal, es decir, $\exists \mathcal{M} \in \mathcal{J}$ tal que $\mathcal{M}$ no está contenido en ningún ideal de $\mathcal{J}$*

Demostración. Tomar $I_1 \in \mathcal{J} \neq \emptyset$ y $\mathcal{J}_1 = \{I \in \mathcal{J} : I \not\supseteq I_1\}$. Si $\mathcal{J}_1 = \emptyset$, tenemos lo pedido, sino $I_2 \in \mathcal{J}_1$. Seguir este proceso:

$$I_1 \nsubseteq I_2 \nsubseteq ...$$

Luego definimos $I = \bigcup_{i=1}^{\infty} I_i$, un ideal de R.

$$\begin{aligned} &\Longrightarrow I = (f_1, ..., f_m) \\ &\Longrightarrow \exists s : f_1, ..., f_m \in I_s \\ &\Longrightarrow I = (f_1, ..., f_m) \subseteq I_s \end{aligned}$$

Lo que es una contradicción, por lo que tenemos lo pedido. □

Teorema 1.4.5. *Sea $V \subseteq \mathbb{A}_k^n$ conj. alg., entonces $\exists V_1, ..., V_m$ irreducibles unívocamente determinados tales que*

$$V = V_1 \cup ... \cup V_m, V_i \nsubseteq V_j si\ i \neq j$$

Demostración. Sea $S = \{V \subset \mathbb{A}^n$ algebraico tal que no es unión finita$\}$. Sea $V \in S$ elemento minimal (a través de $I(V)$ tenemos colección de ideales $\mathcal{J}_s$)
$\therefore V$ es irreducible (sino $V = V_1 \cup V_2$ y $V_i \nsubseteq V \ V_i \neq \emptyset$)
$\therefore V$ irreducible no por definición
$\therefore S = \emptyset$
<u>Unicidad</u>:$V_1 \cup ... \cup V_m = W_1 \cup ... \cup W_r$ irreducibles.

$$V_1 = \bigcup_{i=1}^{r} \underbrace{(W_i \cap V_1)}_{\text{conj. alg.}}$$

Pero V_1 es irreducibles, por lo que $\exists i : V_1 = W_i \cap V_1 \implies V_1 \subseteq W_i$.

$$W_i = \bigcup_{j=1}^{m} (V_j \cap W_i)$$

W_i es irreducible, por lo que $V_1 = W_i$ □

Conj. alg. de $\mathbb{A}_k^2$

Proposición 1.4.6. *$F, G \in k[x, y]$ sin factores en común, entonces $V(F, G) = V(F) \cap V(G)$ es un conjunto finito.*

Demostración. F, G sin div. comunes en $k[x, y] = k[x][y]$, entonces tampoco tienen en $k(x)[y]$.
$\therefore$ existen $h, r \in k(x)[y]$ tal que $h \cdot F + r \cdot G = 1$

Limpiamos el denominador (pol. en x)

$$\therefore H(x,y)F(x,y) + R(x,y)G(x,y) = p(x)$$

Si $(a,b) \in \mathbb{A}_k^2$, $F(a,b) = 0$ y $G(a,b) = 0$, entonces $p(a) = 0$
Luego los ceros comunes de F y G tienen finitas posibilidades para x (ya que son los ceros de $p(x)$ son finitos). Análogo para y. $\square$

Corolario. *F pol. irred. en $k[x,y]$ y $|V(F)| = \infty$, entonces $I(V(F)) = (F)$ y $V(F)$ irreducible.*

Demostración. Si $G \in I(V(F))$, entonces $|V(F,G)| = \infty$, luego F, G tienen factores en común, pero F es irred. por lo que $F \mid G$, luego $G = F \cdot H$, con lo que tenemos que $I(V(F)) = (F)$, $V(F)$ es irreducible ((F) es primo) $\square$

<u>Desafío</u>: Dados finitos puntos en $S \subset \mathbb{A}_{\mathbb{R}}^2$ entonces existe $F(x,y) \in \mathbb{R}[x,y]$ <u>irreducible</u> tal que $S = V(F)$

Teorema 1.4.7 (Nullstenllensatz)**.** *Si $I \nsubseteq k[x_1, ..., x_n]$, entonces $V(I) \neq \emptyset$*

Demostración. Suponer que I es maximal (ya que sino, $I \subset M \nsubseteq k[x_1, ..., x_n \; V(M) \subseteq V(I))$. Notar que $k \subseteq K$ (ya que $I \nsubseteq k[x_1, ...,_n])$
Luego considerar $k[x_1, ..., x_n]/I = K$ un cuerpo. Se considera $k[x_1, ..., x_n] \to K$, y lo que queremos mostrar que $K = k$ $\square$

Teorema 1.4.8 (Nullstenllensatz Fuerte)**.** *Si $k = \overline{k}$ e $I \subset k[x_1, ..., x_n]$ ideal, entonces $I(V(I)) = \mathrm{rad}(I)$, es decir, si f es cero en $V(I) \implies \exists m : f^m \in I$*

Truco de Rabinowitsch. Digamos que $f_1, ..., f_m = I \subset k[x_1, ..., x_n]$ $\square$

Corolario. *Si $I = \mathrm{rad}(I) \implies I(V(I)) = I$*

Corolario. *Si I es primo, entonces $V(I)$ es irreducible.*