FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

CURVAS ALGEBRAICAS Y SINGULARIDADES

Diego Muíños Míguez

2024/2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRADO DE MATEMÁTICAS

Traballo Fin de Grado

CURVAS ALGEBRAICAS Y SINGULARIDADES

Diego Muíños Míguez

Julio, 2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Conocimiento: Álgebra
Título: Curvas algebraicas y singularidades
Breve descripción del contenido
En este trabajo se introducirá el lenguaje de la geometría algebraica, tratando los conceptos de variedades afines y proyectivas. Nos centraremos en las curvas algebraicas exponiendo la noción de punto singular. Abordaremos el problema de la resolución de singularidades en curvas.
Recomendaciones
Tener un buen conocimiento de las materias de álgebra de la titulación.
Otras observaciones

Índice

Resumen

Un trabajo de investigación centrado en las curvas algebraicas se puede entender como el primer paso a dar para adentrarse en el contexto de las variedades. El enfoque geométrico desde el que se examinan constituye una importante motivación de ciertos fundamentos y teoremas del Álgebra conmutativa. Mediante el conocimiento obtenido en cursos elementales de teoría de anillos y de teoría de números, se pueden establecer desde cero las bases de la Geometría algebraica. Una vez expuestas las nociones de variedades afines y proyectivas, es habitual introducir el concepto de punto singular. La idea clave para su estudio es preguntarse qué anillos nos dan información local de las curvas y, avanzando en el sentido de la cuestión anterior, si sería posible llegar a ejemplos de curvas sencillas que preserven las propiedades de otras más complejas.

Abstract

A research project focused on algebraic curves is the first step toward entering the realm of varieties. The geometric perspective from which they are studied serves as an important motivation for certain foundations and theorems in commutative algebra. Using the knowledge acquired in introductory courses on ring theory and number theory, one can draft the foundations of algebraic geometry. After introducing the notions of affine and projective varieties, it is common to present the concept of a singular point. The main idea to study this points is to find which rings provide local information about the curves and, furthermore, whether it is possible to build examples of simple curves that preserve the properties of more complex ones.

Introducción

La Geometría se encarga del estudio de los conjuntos matemáticos conocidos con el nombre de *variedades*. Procuraremos alcanzar dicho concepto partiendo de una base elemental, puramente algebraica. Nuestro enfoque se restringirá al plano (pensado tanto afínmente como en el caso proyectivo) y, en particular, a las *curvas planas*. Estas son, después de los puntos, el ejemplo más sencillo de variedades con las que podemos trabajar en este contexto.

Comenzaremos hablando sobre los *conjuntos algebraicos* y obteniendo los principales resultados asociados a este tipo de objetos, que serán los pilares del documento. Una vez introducidas las primeras secciones, podremos establecer la correspondencia fundamental entre la parte algebraica y geométrica del trabajo y pasar, posteriormente, a tratar las nociones clave del lenguaje de las curvas. La idea será desarrollar los primeros capítulos limitándonos únicamente al espacio afín, pues ganaremos cierta intuición a nivel gráfico y el avance algebraico resultará más cómodo.

A lo largo de la redacción del TFG, encontraremos también múltiples matices topológicos, siendo especialmente relevante la propiedad de ser *irreducible* como espacio.

Abordaremos el concepto de *singularidad*, comentando detalladamente los tipos de puntos que podemos hallar y qué relación guardan a nivel *local* con las estructuras anilladas tratadas en los capítulos precedentes.

A continuación, generalizaremos la teoría previa al caso proyectivo, exponiendo claramente la construcción de $\mathbb{P}^2(K)$. Completaremos las curvas afines añadiéndoles nuevos puntos (los llamados *puntos del infinito*).

Por último, finalizaremos nuestro estudio obteniendo un método algorítmico de resolución de singularidades para curvas planas proyectivas irreducibles.

Capítulo 1

Preliminares sobre conjuntos algebraicos.

1.1. Definiciones elementales y primeras aproximaciones.

Definición 1.1. Un *cuerpo algebraicamente cerrado*, K, es aquel que no tiene extensiones algebraicas (equivalentemente finitas) propias. Es fácil ver que las condiciones siguientes son suficientes y necesarias para el carácter algebraicamente cerrado:

- No existen extensiones simples finitas propias de K.
- Si $f \in K[X]$ es irreducible, entonces $\mathrm{dg}(f) = 1$.
- Si $f \in K[X]$ es tal que $\mathrm{dg}(f) \geq 1$, entonces f tiene una raíz en K.
- Todo polinomio $f \in K[X]$ escinde en K.

A partir de ahora, consideraremos K un cuerpo algebraicamente cerrado fijado (veremos en este capítulo por qué pedimos esta hipótesis). Por otro lado, $n > 0$ con $n \in \mathbb{Z}$ será un entero positivo cualquiera.

Observación 1.2. Es sabido que el anillo de polinomios con coeficientes en K en un número finito de variables, $K[X_1, \dots, X_n]$, es un *DFU* (Dominio de Factorización Única) [*Milne*, pp. 24–26].

Definición 1.3. Un *conjunto algebraico* de K^n es aquel de la forma

$$V(S) = \{(a_1, \dots, a_n) \in K^n : f(a_1, \dots, a_n) = 0, \forall\ f \in S\},$$

donde $S \subseteq K[X_1, \dots, X_n]$ es un conjunto de polinomios. Es decir, $V(S)$ no es más que el conjunto de ceros comunes de cierta familia de polinomios. Cuando S sea finito con $S = \{f_1, \dots, f_s\}$, pondremos $V(S) = V(f_1, \dots, f_s)$.

Observación 1.4. Sean $S, S' \subseteq K[X_1, \ldots, X_n]$. Se cumplen trivialmente las siguientes tres propiedades:

- La aplicación $V : \mathcal{P}(K[X_1, \ldots, X_n]) \to \mathcal{P}(K^n)$ invierte las inclusiones de conjuntos. Esto es, $S \subset S' \Longrightarrow V(S) \supset V(S')$.

- Los conjuntos algebraicos son conjuntos de ceros de ideales del anillo de polinomios. Ciertamente, $V(S) = V(\mathfrak{a})$, siendo $\mathfrak{a} := \langle S \rangle$ con $\langle S \rangle$ el ideal generado por S.

- Es evidente que $K^n = V(0)$. Consecuentemente, K^n es un conjunto algebraico. Escribiremos $\mathbb{A}^n(K)$ al referirnos a K^n visto como un espacio afín sobre el K-espacio vectorial K^n (es decir, sobre sí mismo), además de como un conjunto algebraico.

Teorema 1.5. *Todo conjunto algebraico es el conjunto de ceros de alguna familia finita de polinomios.*

Demostración. Como K es un cuerpo, es en particular un anillo noetheriano. El *Teorema de la base de Hilbert* [*Milne*, *Teorema* 2.7] afirma que $K[X_1, \ldots, X_n]$ será también un anillo noetheriano. Es por ello que todo ideal del anillo de polinomios es finitamente generado. Entonces, dado $S \subseteq K[X_1, \ldots, X_n]$ y $\mathfrak{a} := \langle S \rangle$ se verifican las siguientes igualdades para ciertos $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$:

$$V(S) = V(\langle S \rangle) = V(\mathfrak{a}) = V(\langle f_1, \ldots, f_s \rangle) = V(f_1, \ldots, f_s).$$

□

Con estos primeros resultados ya estamos en condiciones de poder definir una topología en $\mathbb{A}^n(K)$. Para el estudio de los objetos geométricos, el hecho de poder contar con una topología es ciertamente ventajoso. Nuestro enfoque práctico se centrará en $\mathbb{C}$, el cuerpo de los números complejos. Sin embargo, los resultados que veremos pueden pensarse para otra elección de K (algebraicamente cerrado), una vez que tenemos una estructura de espacio topológico en $\mathbb{A}^n(K)$. Es por ello que nos mantendremos en un caso general en este capítulo para, más adelante, tomar $K = \mathbb{C}$ con el objetivo de ganar intuición gráfica. En la siguiente sección trataremos esta idea con detenimiento.

1.2. Construyendo una nueva topología.

Proposición 1.6. *Los conjuntos algebraicos de $\mathbb{A}^n(K)$ cumplen la propiedad de ser los cerrados de una topología para dicho espacio.*

Demostración. Vamos por pasos, probando cada una de las condiciones que se requieren.

- El vacío y $\mathbb{A}^n(K)$ son cerrados de la topología, es decir, son conjuntos algebraicos. En efecto, ya hemos visto que $\mathbb{A}^n(K) = V(0)$ y es evidente que $\emptyset = V(K[X_1, \ldots, X_n])$ (se cumple, por ejemplo, porque X_1 y $X_1 + 1$ no comparten ceros comunes en $\mathbb{A}^n(K)$. Un argumento más sencillo es señalar que las constantes no se anulan).

- La unión finita de cerrados es cerrada. Para ello, basta ver que dados dos conjuntos algebraicos arbitrarios su unión es cerrada, es decir, un conjunto de ceros de cierta familia de polinomios. Tomemos $V(\mathfrak{a})$ y $V(\mathfrak{b})$. Vamos a demostrar que $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$ y así quedaría probado el apartado. Para las inclusiones hacia la derecha, notemos que $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ y además $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{b}$, luego se llega a que

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) \subset V(\mathfrak{a} \cap \mathfrak{b}) \subset V(\mathfrak{a}\mathfrak{b}).$$

  Para las inclusiones hacia la izquierda, sea $P = (a_1, \ldots, a_n)$ un punto de $\mathbb{A}^n(K)$ tal que existen $f \in \mathfrak{a}$, $g \in \mathfrak{b}$ con $f(P) \neq 0$, $g(P) \neq 0$ (i.e., $P \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$). Entonces, $(fg)(P) \neq 0$ y así vemos que $P \notin V(\mathfrak{a}\mathfrak{b})$. Obtenemos la inclusión

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) \supset V(\mathfrak{a}\mathfrak{b}).$$

  Junto a la cadena anterior y a un razonamiento por compresión, se demuestra el enunciado al completo.

- La intersección arbitraria de cerrados es cerrada. Llega con ver que $\bigcap_{i\in I} V(\mathfrak{a}_i) = V(\sum_{i\in I} \mathfrak{a}_i)$, para cada familia de ideales $\{\mathfrak{a}_i\}_{i\in I}$. La inclusión hacia la derecha es evidente, pues los elementos del ideal $\sum_{i\in I} \mathfrak{a}_i$ son sumas finitas de la forma $\sum_{i\in I} f_i$, con $f_i \in \mathfrak{a}_i$. La correspondiente inclusión hacia la izquierda se debe a que $\mathfrak{a}_j \subset \sum_{i\in I} \mathfrak{a}_i, \forall\, j \in I$.

$\square$

Definición 1.7. A la topología inducida por la *Proposición* 1.6 la denominaremos *topología de Zariski* ($\mathcal{T}_{Zar}$) en el espacio $\mathbb{A}^n(K)$. A su vez, dado V un conjunto algebraico de $\mathbb{A}^n(K)$, diremos que la topología relativa de V en $(\mathbb{A}^n(K), \mathcal{T}_{Zar})$ es la *topología de Zariski* en V. Entendemos V como subespacio topológico y empleamos la notación $(V, \mathcal{T}_{Zar})$ para referirnos a él.

Observación 1.8. Consideremos el caso $n = 1$, es decir, tomemos el espacio $\mathbb{A}^1(K)$ generado al visualizar el cuerpo K como un conjunto algebraico. Se cumplen las siguientes propiedades:

- Los cerrados de la topología de Zariski son los subconjuntos finitos de $\mathbb{A}^1(K)$. Ciertamente, un cojunto finito de la forma $W = \{a_1, \ldots, a_r\}$ cumple que $W = V(f)$, siendo $f(X) = \prod_{i=1}^r (X - a_i)$. Recíprocamente, si W es un conjunto algebraico de $\mathbb{A}^1(K)$ entonces, por el *Teorema* 1.5, $W = V(f_1, \ldots, f_t) = \bigcap_{i=1}^t \{\textit{Raíces de } f_i\}$ para ciertos $f_1, \ldots, f_t \in K[X]$. Este es un conjunto finito de $\mathbb{A}^1(K)$ (por ser K algebraicamente cerrado, todo polinomio de $K[X]$ escinde en K).

- Dos abiertos arbitrarios no vacíos de $(\mathbb{A}^1(K), \mathcal{T}_{Zar})$ siempre se intersecan. Para verlo, tomemos sus complementarios en $\mathbb{A}^1(K)$, digamos V y W respectivamente, que sabemos que son conjuntos algebraicos. Entonces, $(\mathbb{A}^1(K) \setminus V) \cap (\mathbb{A}^1(K) \setminus W) = \mathbb{A}^1(K) \setminus (V \cup W)$. Trivialmente, $V \cup W$ es un subconjunto finito de $\mathbb{A}^1(K)$, pero como K es infinito por ser algebraicamente cerrado, deducimos que $\mathbb{A}^1(K) \setminus (V \cup W)$ debe ser necesariamente no vacío.

- El espacio topológico $(\mathbb{A}^1(K), \mathcal{T}_{Zar})$ no es Hausdorff. Se sigue de forma inmediata del apartado anterior.

- Si $K = \mathbb{C}$ entonces en $(\mathbb{C}, \mathcal{T}_{Zar})$ hay muchos menos abiertos que en $(\mathbb{C}, \mathcal{T}_d)$, pensado con la topología dada por la norma usual. Los abiertos del primero de los espacios topológicos son los complementarios en $\mathbb{C}$ de conjuntos finitos de puntos, que serán siempre abiertos del segundo. Sin embargo, en el cuerpo de los números complejos dotado de la topología euclídea es sabido que hay muchos más conjuntos abiertos, la mayoría de los cuales son complementarios de conjuntos infinitos. Por ejemplo, los discos abiertos.

1.3. El Teorema de los ceros de Hilbert.

Para poder examinar los conjuntos algebraicos de $\mathbb{A}^n(K)$ y los ideales de $K[X_1, \ldots, X_n]$ más de cerca, será de gran utilidad plantearse primero cuándo un conjunto de polinomios tiene algún cero común o, lo que es lo mismo, cuándo un sistema de ecuaciones de la forma

$$g(X_1, \ldots, X_n) = 0, \ g \in S$$

tiene solución. El *Teorema de los ceros* nos da la equivalencia clave que necesitamos. Enunciamos a continuación el resultado mencionado.

Teorema 1.9. *Un ideal no nulo, $\mathfrak{a} \in K[X_1, \ldots, X_n]$, tiene algún cero en $\mathbb{A}^n(K)$ si, y sólo si, el ideal $\mathfrak{a}$ es propio. Equivalentemente, si $\mathfrak{a}$ es no nulo, entonces $V(\mathfrak{a}) \neq \emptyset \iff 1 \notin \mathfrak{a}$.*

Demostración. Veamos la implicación hacia la derecha. Supongamos que $1 \in \mathfrak{a}$. Entonces, es evidente que las ecuaciones polinomiales inducidas por los elementos del ideal son inconsistentes (las constantes no tienen ceros). La implicación hacia la izquierda [*Milne*, *Teorema* 2.11] se basa en verificar la existencia de un homomorfismo de K-álgebras de $K[X_1, \ldots, X]/\mathfrak{a}$ en K. Para lograrlo se usa el conocido *Lema de Zariski* [*Milne*, *Lema* 2.12], que enunciaremos a continuación, y el hecho de que K sea algebraicamente cerrado. $\square$

Lema 1.10. *Sea $L|K$ una extensión de cuerpos, no necesariamente algebraicamente cerrados. Si L es finitamente generado como K-álgebra, entonces L es algebraico sobre K. Si añadimos la hipótesis de algebraicamente cerrados, se obtiene $L = K$.*

1.4. El Teorema de los ceros fuerte.

Veremos que es posible establecer una asignación biunívoca entre conjuntos algebraicos de $\mathbb{A}^n(K)$ y cierto tipo de ideales de $K[X_1,\ldots,X_n]$. Para ello, será preciso dar unas definiciones previas y también plantear el resultado que da nombre a esta sección.

Definición 1.11. Sea $W \subseteq \mathbb{A}^n(K)$. Definimos el *conjunto de polinomios que se anulan en* W como el subconjunto del anillo $K[X_1,\ldots,X_n]$ dado por

$$I(W) := \{f \in K[X_1,\ldots,X_n] : f(P) = 0, \forall\ P \in W\}.$$

Cuando W sea un conjunto finito de puntos de la forma $W = \{P_1,\ldots,P_s\}$ escribiremos $I(W) = I(\{P_1,\ldots,P_s\}) = I(P_1,\ldots,P_s)$ indistintamente.

Observación 1.12. Se cumplen las siguientes propiedades para un $W \subseteq \mathbb{A}^n(K)$ arbitrario:

- $I(W)$ es trivialmente un ideal del anillo de polinomios.
- La aplicación $I : \mathcal{P}(\mathbb{A}^n(K)) \to \mathcal{P}(K[X_1,\ldots,X_n])$ invierte las inclusiones de conjuntos. En efecto, $V \subset W \Longrightarrow I(V) \supset I(W)$.
- Teniendo en cuenta que el vacío no impone restricciones sobre los polinomios, $I(\emptyset) = K[X_1,\ldots,X_n]$. Es más, $I(W) = K[X_1,\ldots,X_n] \Longleftrightarrow W = \emptyset$.
- $I(\bigcup_{i\in I} W_i) = \bigcap_{i\in I} I(W_i)$. Para la inclusión hacia la derecha, simplemente señalamos que $W_i \subset \bigcup_{i\in I} W_i \Longrightarrow I(\bigcup_{i\in I} W_i) \subset I(W_i), \forall\ i \in I$. El contenido hacia la izquierda es trivial.
- Dados $W \subset \mathbb{A}^n(K)$, $S \subset K[X_1,\ldots,X_n]$, se verifica que $W \subset VI(W)$ y que $S \subset IV(S)$.

Ejemplo 1.13. Sean $P = (a_1,\ldots,a_n) \in \mathbb{A}^n(K)$ y $\mathfrak{m}_P = \langle X_1 - a_1,\ldots,X_n - a_n\rangle$. Consideremos el isomorfismo de K-álgebras $\Phi : K[X_1,\ldots,X_n] \to K[X_1,\ldots,X_n]$ tal que $\Phi(X_i) = X_i - a_i, \forall\ i \in \{1,\ldots,n\}$. La *Propiedad universal del anillo de polinomios* asegura que Φ está bien definido y es, en efecto, un homomorfismo. Es fácil ver que $\Phi^{-1} : K[X_1,\ldots,X_n] \to K[X_1,\ldots,X_n]$ tal que $\Phi^{-1}(X_i) = X_i + a_i, \forall\ i \in \{1,\ldots,n\}$ y Φ son inversas. Sea ev_0 el homomorfismo de K-álgebras que va del anillo de polinomios en K, llevando cada X_i en el cero y sean π y π_P homomorfismsos canónicos de paso al cociente. Si denotamos por $\mathfrak{m}$ al ideal $\langle X_1,\ldots,X_n\rangle$, entonces tenemos el siguiente diagrama conmutativo, cuyo planteamiento explicaremos al pie del mismo y que nos será verdaderamente útil en las siguientes secciones. El objetivo es demostrar la igualdad

$$I(P) = \mathfrak{m}_P.$$

$$\begin{tikzcd}
K[X_1,\dots,X_n] \arrow[r, "\Phi"] \arrow[d, "\pi"'] & K[X_1,\dots,X_n] \arrow[d, "\pi_P"] \\
K[X_1,\dots,X_n]/\mathfrak{m} \arrow[r, "\Psi", "\cong"'] \arrow[d, "\sigma"', "\cong"] & K[X_1,\dots,X_n]/\mathfrak{m}_P \arrow[d, "\mathrm{Id}"] \\
K \arrow[r, "\varphi"] & K[X_1,\dots,X_n]/\mathfrak{m}_P
\end{tikzcd}$$

Aclaramos que σ es el isomorfismo de anillos (en particular, de K-álgebras) inducido de forma evidente por el hecho de que $\mathrm{Ker}(ev_0) = \mathfrak{m}$. Por otro lado, definimos Ψ y φ como los únicos homomorfismos de anillos que hacen conmutativo el diagrama. Es decir,

$$\Psi([f]_{\mathfrak{m}}) = \Psi(\pi(f)) = \pi_P(\Phi(f)) = [\Phi(f)]_{\mathfrak{m}_P}.$$

Consecuentemente, para la sección inferior,

$$\varphi = \mathrm{Id} \circ \Psi \circ \sigma^{-1}.$$

En resumidas cuentas, basta probar que $\Psi : K[X_1, \dots X_n]/\mathfrak{m} \to K[X_1, \dots, X_n]/\mathfrak{m}_P$ está bien definido y es un isomorfismo. La primera condición se debe a que $\Phi(\mathfrak{m}) \subset \mathfrak{m}_P$. Dados $[f]_{\mathfrak{m}}, [g]_{\mathfrak{m}} \in K[X_1, \dots X_n]/\mathfrak{m}$ con $[f]_{\mathfrak{m}} = [g]_{\mathfrak{m}}$ se tiene que

$$f-g \in \mathfrak{m} \Longrightarrow \Phi(f-g) \in \mathfrak{m}_P \Longrightarrow \Psi([f]_{\mathfrak{m}})-\Psi([g]_{\mathfrak{m}}) = \pi_P(\Phi(f))-\pi_P(\Phi(g)) = \pi_P(\Phi(f-g)) = 0.$$

La sobreyectividad de Ψ es inmediata. Para la inyectividad, notemos que $\mathfrak{m} = \mathfrak{m}_P^c$, es decir, $\mathfrak{m} = \Phi^{-1}(\mathfrak{m}_P^c)$ es la contracción por Φ del ideal $\mathfrak{m}_P$ y basta con aplicar la *Proposición* 1.14. De aquí se deduce que φ es un isomorfismo al definirse como composición de ellos. Por ser K un cuerpo, $\mathfrak{m}_P$ es necesariamente un ideal maximal. Ahora bien, como $\{P\} \neq \emptyset \Longrightarrow I(P) \neq K[X_1, \dots, X_n]$. Consecuentemente, $I(P)$ es un ideal propio verificando que $\mathfrak{m}_P \subset I(P)$, luego por maximalidad llegamos a que $\mathfrak{m}_P = I(P)$.

Proposición 1.14. *Dados A y B dos anillos arbitrarios con Φ un homomorfismo entre ambos y $\mathfrak{b}$ un ideal de B, entonces Ψ es inyectivo en el siguiente esquema, definiéndose como el único homomorfismo que hace conmutativo el diagrama.*

$$\begin{tikzcd}
A \arrow[r, "\Phi"] \arrow[d] & B \arrow[d] \\
\dfrac{A}{\mathfrak{b}^c} \arrow[r, "\Psi"] & \dfrac{B}{\mathfrak{b}}
\end{tikzcd}$$

Demostración. El proceso para ver que Ψ está bien definido es análogo al hecho en el *Ejemplo* 1.13. Sean $f, g \in A$ tales que $\Psi([f]_{\mathfrak{b}^c}) = \Psi([g]_{\mathfrak{b}^c})$ y razonamos como sigue:

$$0 = \Psi([f]_{\mathfrak{b}^c} - [g]_{\mathfrak{b}^c}) = \Psi([f-g]_{\mathfrak{b}^c}) = [\Phi(f-g)]_{\mathfrak{b}}.$$

Se llega a que $\Phi(f-g) \in \mathfrak{b} \Longrightarrow f - g \in \mathfrak{b}^c \Longrightarrow [f]_{\mathfrak{b}^c} = [g]_{\mathfrak{b}^c}$. $\square$

Lema 1.15. *Sea $W \subset \mathbb{A}^n(K)$. Entonces $VI(W)$ es el menor conjunto algebraico de $\mathbb{A}^n(K)$ conteniendo a W respecto a la inclusión de conjuntos. En particular, $VI(W) = W$ si W es un conjunto algebraico.*

Demostración. Ya sabemos que $VI(W)$ es un conjunto algebraico conteniendo a W. Tomemos $U = V(\mathfrak{a})$ otro conjunto algebraico tal que $W \subset U$. En tal caso, recordando de la *Observación* 1.12 que $I(\cdot)$ invierte las inclusiones, vemos que $\mathfrak{a} \subset IV(\mathfrak{a}) \subset I(W) \Longrightarrow VI(W) \subset V(\mathfrak{a}) = U$. $\square$

Definición 1.16. Sea $\mathfrak{a}$ un ideal de un anillo A arbitrario. Definimos el *radical* de $\mathfrak{a}$ como el siguiente ideal, cuyas propiedades básicas se suponen conocidas por el lector:

$$\mathrm{rad}(\mathfrak{a}) := \{x \in A : \exists\ n \in \mathbb{N},\ x^n \in \mathfrak{a}\}.$$

Estamos en condiciones de presentar ya uno de los resultados más importantes del capítulo: el *Teorema de los ceros fuerte.*

Teorema 1.17. *Para cada ideal $\mathfrak{a} \in K[X_1, \ldots, X_n]$, se verifica la igualdad*

$$IV(\mathfrak{a}) = \mathrm{rad}(\mathfrak{a}).$$

En particular, $IV(\mathfrak{a}) = \mathfrak{a}$ si $\mathfrak{a}$ es un ideal radical.

Demostración. Veamos primero el contenido hacia la izquierda. Para todo punto $P \in \mathbb{A}^n(K)$ y todo polinomio $f \in K[X_1, \ldots, X_n]$ se verifica que $f^r(P) = f(P)^r$. Por tanto, como K es un dominio, f^r se anula en los mismos puntos de $\mathbb{A}^n(K)$ que f. Consecuentemente, el ideal $I(W)$ es radical para cada subconjunto $W \subseteq \mathbb{A}^n(K)$. En particular, $\mathrm{rad}(\mathfrak{a}) \subset IV(\mathfrak{a})$, pues $\mathfrak{a} \subset IV(\mathfrak{a})$ y sabemos que $\mathrm{rad}(\mathfrak{a})$ es el menor ideal radical conteniendo a $\mathfrak{a}$. Para la inclusión hacia la derecha [*Milne*, *Teorema* 2.16] es necesario trabajar con una variable auxiliar, Y, tratando de buscar la forma correcta de aplicar el *Teorema de los ceros* original. □

Observación 1.18. Una consecuencia directa de esta igualdad es que, como $K[X_1, \dots, X_n]$ es un anillo reducido por ser un dominio de integridad, entonces $0 = \mathrm{rad}(0) = IV(0) = I(\mathbb{A}^n(K))$. Es decir, el único polinomio que se anula en todo punto de $\mathbb{A}^n(K)$ es el cero. Visto de otro modo, todo polinomio no idénticamente nulo en un número finito de variables ($n > 0,\ n \in \mathbb{Z}$) con coeficientes en un cuerpo algebraicamente cerrado, K, tiene en $\mathbb{A}^n(K)$ algún punto en el que no se anula. Puede probarse que esto se cumple siempre que K sea infinito, como es el caso (pues K es algebraicamente cerrado).

1.5. El Teorema de correspondencia.

Ya podemos establecer la relación biyectiva que hay entre los objetos con los que hemos estado trabajando hasta ahora. A partir de este momento, nos referiremos al resultado que enunciaremos a continuación como el *Teorema de correspondencia*, entendiendo que cualquier otro que se conozca en un contexto diferente será acompañado de una caracterización pertinente para no confundirnos. Nos permitirá asentar las bases de la *Geometría algebraica*.

Teorema 1.19. *Existe una correspondencia biunívoca de la forma:*

$$\left\{ \begin{array}{c} \textit{Ideales radicales} \\ \textit{de } K[X_1, \dots, X_n] \end{array} \right\} \underset{I(\cdot)}{\overset{V(\cdot)}{\rightleftarrows}} \left\{ \begin{array}{c} \textit{Conjuntos algebraicos} \\ \textit{de } \mathbb{A}^n(K) \end{array} \right\}$$

Demostración. En la prueba del *Teorema de los ceros fuerte* ya vimos que $I(W)$ era un ideal radical del anillo de polinomios para cualquier subconjunto $W \subseteq \mathbb{A}^n(K)$. En particular, la propiedad se seguirá cumpliendo si W es un conjunto algebraico. En el otro sentido, es evidente que la correspondencia también está bien definida. Veamos ahora que las aplicaciones son inversas la una de la otra. Sabemos, por el ya nombrado *Teorema* 1.17, que $IV(\mathfrak{a}) = \mathfrak{a}$ si $\mathfrak{a}$ es un ideal radical. Para la otra composición, basta con aplicar el *Lema* 1.15. □

Dado A un anillo arbitrario e $I \subsetneq A$ un ideal de dicho anillo. Es un resultado conocido de álgebra conmutativa básica que

$$\mathrm{rad}(I) = \bigcap_{\substack{\mathfrak{p} \supset I \\ \mathfrak{p} \text{ primo}}} \mathfrak{p}.$$

Vamos a demostrar en el siguiente *Corolario* que es posible refinar este resultado en $K[X_1, \dots, X_n]$.

Corolario 1.20. *Sea $\mathfrak{a} \subsetneq K[X_1, \ldots, X_n]$ un ideal del anillo de polinomios. Entonces se verifica la siguiente igualdad:*

$$\operatorname{rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{m} \supset \mathfrak{a} \\ \mathfrak{m} \textit{ maximal}}} \mathfrak{m}.$$

Demostración. Para la inlcusión hacia la derecha, como todo ideal maximal es primo, entonces es radical. Si $\mathfrak{m}$ es un ideal en estas condiciones conteniendo a $\mathfrak{a}$, es evidente que $\operatorname{rad}(\mathfrak{a}) \subset \mathfrak{m}$. Recíprocamente, para cada $P = (a_1, \ldots, a_n)$ ya vimos en el *Ejemplo* 1.13 que el ideal $\mathfrak{m}_P = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ es maximal y que coincide con $I(P) = \{f \in K[X_1, \ldots, X_n] : f(P) = 0\}$. Consecuentemente, $\mathfrak{a} \subset \mathfrak{m}_P$ si, y sólo si, $P \in V(\mathfrak{a})$. Notemos que f es cero en $V(\mathfrak{a})$ si $f \in \mathfrak{m}_P, \forall\ P \in V(\mathfrak{a})$. En tal caso, $f \in IV(\mathfrak{a}) = \operatorname{rad}(\mathfrak{a})$ por el *Teorema* 1.17. Llegamos a la siguiente cadena de inclusiones:

$$\bigcap_{\mathfrak{a} \subset \mathfrak{m}} \mathfrak{m} \subset \bigcap_{P \in V(\mathfrak{a})} \mathfrak{m}_P \subset \operatorname{rad}(\mathfrak{a}).$$

□

Observación 1.21. Estas son las principales propiedades del *Teorema de correspondencia*:

I.) La asociación biunívoca invierte el orden respecto a la inclusión de conjuntos. Por tanto, los ideales maximales (radicales) de $K[X_1, \ldots, X_n]$ están en correspondencia uno a uno con los conjuntos algebraicos minimales de $\mathbb{A}^n(K)$, que son precisamente los puntos. Efectivamente, es muy sencillo ver que $P = (a_1, \ldots, a_n) = V(X_1 - a_1, \ldots, X_n - a_n)$ por definición. Daremos la idea en la demostración de la *Proposición* 1.22. Recordando que

$$I(P) = \langle X_1 - a_1, \ldots, X_n - a_n \rangle,$$

llegamos a que los ideales maximales de $K[X_1, \ldots, X_n]$ son los ideales del conjunto

$$\{\langle X_1 - a_1, \ldots, X_n - a_n \rangle : (a_1, \ldots, a_n) \in \mathbb{A}^n(K)\}.$$

II.) Si $W \subseteq \mathbb{A}^n(K)$ es un conjunto algebraico, entonces $I(W) = 0 \iff W = \mathbb{A}^n(K)$. En efecto, si $W = \mathbb{A}^n(K)$ concluimos por la *Observación* 1.18. Recíprocamente, supongamos que $I(W) = 0$, con W conjunto algebraico. Entonces, por el *Teorema de correspondencia*, $W = VI(W) = V(0) = \mathbb{A}^n(K)$.

III.) Sea $\mathfrak{a}$ un ideal de $K[X_1, \ldots, X_n]$. Se cumple que $V(\mathfrak{a}) = \emptyset \iff \mathfrak{a} = K[X_1, \ldots, X_n]$. La implicación hacia la izquierda es trivial. Hacia la derecha, basta con aplicar el *Teorema de los ceros* original, teniendo en cuenta que $\mathfrak{a}$ no puede ser cero.

IV.) Sean W, W' dos conjuntos algebraicos. Como $W \cap W'$ es el el mayor conjunto algebraico contenido en ambos, por I.) se llega a que $I(W \cap W')$ debe ser el menor ideal radical conteniendo a $I(W)$ y a $I(W')$. Esto es, $I(W \cap W') = \operatorname{rad}(I(W) + I(W'))$.

1.6. Profundizando en la topología de Zariski.

Ya conocemos más de cerca el comportamiento de los conjuntos algebraicos de $\mathbb{A}^n(K)$ en general. Estudiemos qué ocurre al trabajar en el espacio topológico $(\mathbb{A}^n(K), \mathcal{T}_{Zar})$. El *Lema* 1.15 nos dice que $VI(W)$ es el menor cerrado de $\mathbb{A}^n(K)$ que contiene a W, luego es claramente su clausura. Dado V un conjunto algebraico, los cerrados de $(V, \mathcal{T}_{Zar})$ son las intersecciones de cerrados de $\mathbb{A}^n(K)$ con el propio V, es decir, son los conjuntos algebraicos de $\mathbb{A}^n(K)$ contenidos en V. Por el *Teorema de correspondencia*, estos están asociados a los ideales radicales de $K[X_1, \ldots, X_n]$ que contienen a $I(V)$, pues ya vimos que se invierten las inclusiones.

Proposición 1.22. *Sea $V \subset \mathbb{A}^n(K)$ un conjunto algebraico. Se verifican los siguientes apartados:*

- I.) *Los puntos de V son cerrados de $(V, \mathcal{T}_{Zar})$.*
- II.) *Toda cadena asecendente de abiertos de V es estacionaria. Equivalentemente, toda cadena descendente de cerrados de V es estacionaria.*
- III.) *Todo recubrimiento abierto de V admite un subrecubrimiento finito. Es decir, $(V, \mathcal{T}_{Zar})$ es un espacio topológico cuasicompacto y, en particular, también lo es $(\mathbb{A}^n(K), \mathcal{T}_{Zar})$* [1].

Demostración. Probemos cada uno de los apartados anteriores:

- I.) Para cada $P = (a_1, \ldots a_n)$ hemos visto que $I(P) = \mathfrak{m}_P$, siendo $\mathfrak{m}_P = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Resulta sencillo comprobar la correspondencia inversa, es decir, $V(\mathfrak{m}_P) = P$. En efecto, los polinomios generadores $X_i - a_i$, con $i \in \{1, \ldots, n\}$, imponen cada uno de ellos que la coordenada i-ésima de los puntos de $V(\mathfrak{m}_P)$ deba ser a_i. Consecuentemente, $V(\mathfrak{m}_P)$ es un conjunto unitario cuyo único elemento es P. Si P es un punto de V, entonces es un cerrado de $\mathbb{A}^n(K)$ contenido en V, luego un cerrado de V.
- II.) Tomemos $V_1 \supset V_2 \supset \ldots$ una cadena descendente de cerrados. El *Teorema de correspondencia* genera una cadena ascendente de ideales del anillo noetheriano $K[X_1, \ldots, X_n]$, que en algún momento se hace constante. Basta con aplicar una vez más el *Teorema* 1.19.
- III.) Esta es una demostración constructiva muy común en álgebra conmutativa para probar el carácter finito de ciertos conjuntos. Sea $\{\Omega_\alpha\}_{\alpha \in A}$ un recubrimiento abierto de V y definamos

$$\Gamma := \left\{ U \subset V \text{abierto} : U = \bigcup_{i=1}^{s} \Omega_i \text{ para alguna familia } \{\Omega_i\}_{i=1}^{s} \subset \{\Omega_\alpha\}_{\alpha \in A},\ s \in \mathbb{N} \right\}.$$

[1] Algunos libros de la bibliografía piden que el espacio topológico sea Hausdorff para poder considerarlo *compacto* y llaman a aquel que cumple la propiedad III.) espacio *cuasicompacto*. Nosotros respetaremos este convenio, pues el hecho de contar con el carácter Hausdorff es ciertamente significativo y es importante señalar bien la diferencia.

Supongamos que $V \not\subset \Gamma$. En tal caso, tomando algún $U_1 = \bigcup_{i=1}^{s} \Omega_i \in \Gamma$ es evidente que $U_1 \subsetneq V$. Podemos considerar entonces un abierto del recubrimiento de V, pongamos Ω_{s+1}, tal que $U_1 \subsetneq (\bigcup_{i=1}^{s} \Omega_i) \cup \Omega_{s+1} =: U_2 \in \Gamma$. Procediendo inductivamente, hallamos una cadena ascendente irredundante de abiertos de V de la forma

$$U_1 \subsetneq U_2 \subsetneq \cdots \subsetneq U_r \subsetneq U_{r+1} \subsetneq \cdots$$

Llegamos entonces a una clara contradicción con ii.).

□

Definición 1.23. Un espacio topológico cuyos puntos son cerrados se dice *espacio* T_1. Notemos que, en estas condiciones, para cada par de puntos distintos tenemos un entorno abierto de uno que no contiene al otro y viceversa. Es importante resaltar que dichos abiertos no tienen por qué ser disjuntos, como ya veíamos en la *Observación* 1.8.

Por otro lado, un espacio topológico X verificando ii.) se dice *espacio noetheriano*. Esta característica equivale a que todo conjunto no vacío de cerrados de X tenga algún elemento minimal. La demostración es inmediata.

Por último observemos que, de la prueba de iii.), se deduce que si X es noetheriano entonces es también un *espacio cuasicompacto*. Consecuentemente, como todo abierto de X es noetheriano, resulta ser también cuasicompacto.

1.7. La estructura de los conjuntos algebraicos. Descomposición en componentes irreducibles.

Definición 1.24. Un espacio topológico no vacío, X, se dice *irreducible* si no es la unión de dos cerrados propios de X.

Lema 1.25. *Las siguientes son condiciones equivalentes a la irreducibilidad para $X \neq \emptyset$:*

i.) Si $X = Y_1 \cup Y_2$, con Y_1, Y_2 cerrados de X, entonces $X = Y_1$ ó $X = Y_2$.

ii.) Todo par de abiertos de X no vacíos tiene intersección no vacía.

iii.) Todo abierto no vacío de X es denso en X.

Demostración. Probemos la equivalencia con la irreducibilidad en cada uno de los apartados:

i.) Es trivial.

ii.) Supongamos X irreducible. Sean U_1, U_2 dos abiertos no vacíos de X y V_1, V_2 sus complementarios (respectivamente). En tal caso,

$$U_1 \cap U_2 = (X \setminus V_1) \cap (X \setminus V_2) \overset{\text{De Morgan}}{=} X \setminus (V_1 \cup V_2)$$

Ahora bien, si $U_1 \cap U_2 = \emptyset \Longrightarrow X = V_1 \cup V_2 \Longrightarrow X = V_1$ ó $X = V_2 \Longrightarrow U_1 = \emptyset$ ó $U_2 = \emptyset$. Llegamos entonces a un absurdo. Recíprocamente, si $X = V_1 \cup V_2$ con V_1, V_2 dos cerrados de X, entonces $U_1 \cap U_2 = \emptyset$ (tomando complementarios). Como dos abiertos no vacíos siempre intersecan, necesariamente alguno de ellos ha de ser vacío y, por tanto, $X = V_1$ ó $X = V_2$.

iii.) Tomemos X un espacio irreducible y U un abierto no vacío de X. Para probar que U es denso, basta con ver que este interseca a todo abierto no vacío de X. Por ii.), se tiene de forma inmediata el resultado. Para el recíproco, dados U_1, U_2 dos abiertos no vacíos de X, es obvio que estos se intersecan por ser ambos densos en X.

□

Observación 1.26. Notemos que si X es Hausdorff, entonces cada par de puntos distintos admite dos entornos disjuntos, uno para cada punto. Es evidente que los únicos espacios Hausdorff irreducibles son precisamente los puntos.

Proposición 1.27. *Un conjunto algebraico $W \subset \mathbb{A}^n(K)$ es irreducible si, y sólo si, $I(W)$ es primo.*

Demostración. Veamos la implicación hacia la derecha. Tomemos W un conjunto algebraico irreducible. Sea $fg \in I(W)$ y tenemos que demostrar que $f \in I(W)$ ó $g \in I(W)$ para ver la primalidad. En cada punto $P \in W$ se cumple que $(fg)(P) = 0$, luego f es cero en P ó lo es g. Consecuentemente, $W \subset V(f) \cup V(g)$. De este modo, $W = (W \cap V(f)) \cup (W \cap V(g))$. Como W es irreducible, entonces ambos conjuntos de la unión anterior no pueden ser cerrados propios de W. Dado que $W \neq \emptyset \Longrightarrow (W \cap V(f)) = W$ ó $(W \cap V(g)) = W$. Supongamos, sin pérdida de generalidad, que nos hallamos en el primer caso. Es inmediato que $f \in I(W)$.

Recíprocamente, sea W un conjunto algebraico tal que $I(W)$ es primo (luego $W \neq \emptyset$) y vamos a ver que W es necesariamente irreducible. Para ello, pongamos $W = V(\mathfrak{a}) \cup V(\mathfrak{b})$ (por el *Teorema de correspondencia*, podemos suponer $\mathfrak{a}$ y $\mathfrak{b}$ ideales radicales). Nuestro objetivo será demostrar el contenido de W en alguno de los dos conjuntos. Notemos que el ideal $\mathfrak{a} \cap \mathfrak{b}$ es radical y sabemos que $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b}) \Longrightarrow I(W) = \mathfrak{a} \cap \mathfrak{b}$. Si $V(\mathfrak{a}) \subsetneq W \Longrightarrow I(W) \subsetneq \mathfrak{a} \Longrightarrow \exists\, f \in \mathfrak{a} \setminus I(W)$. Dado $g \in \mathfrak{b}$, llegamos a que $fg \in \mathfrak{a} \cap \mathfrak{b} = I(W) \overset{\text{I(W) primo}}{\Longrightarrow} g \in I(W)$. Concluímos que $\mathfrak{b} \subset I(W) \Longrightarrow W \subset V(\mathfrak{b})$. □

Observación 1.28. Tenemos las siguientes biyecciones que refinan el *Teorema* 1.19:

$$
\begin{array}{ccc}
\left\{\begin{array}{c}\text{Ideales radicales}\\ \text{de } K[X_1,\dots,X_n]\end{array}\right\} & \underset{I(\cdot)}{\overset{V(\cdot)}{\rightleftarrows}} & \left\{\begin{array}{c}\text{Conjuntos algebraicos}\\ \text{de } \mathbb{A}^n(K)\end{array}\right\} \\
\updownarrow & & \updownarrow \\
\left\{\begin{array}{c}\text{Ideales primos}\\ \text{de } K[X_1,\dots,X_n]\end{array}\right\} & \underset{I(\cdot)}{\overset{V(\cdot)}{\rightleftarrows}} & \left\{\begin{array}{c}\text{Conjuntos algebraicos}\\ \text{irreducibles de } \mathbb{A}^n(K)\end{array}\right\} \\
\updownarrow & & \updownarrow \\
\left\{\begin{array}{c}\text{Ideales maximales}\\ \text{de } K[X_1,\dots,X_n]\end{array}\right\} & \underset{I(\cdot)}{\overset{V(\cdot)}{\rightleftarrows}} & \left\{\begin{array}{c}\text{Conjuntos unitarios}\\ \text{(puntos) de } \mathbb{A}^n(K)\end{array}\right\}
\end{array}
$$

Ejemplo 1.29. Sea $f \in K[X_1,\dots,X_n]$. Como el anillo de polinomios es un *DFU*, $\langle f\rangle$ es un ideal primo si, y sólo si, f es un elemento irreducible. Por el diagrama anterior,

$$f \text{ es irreducible} \Longrightarrow V(f) \text{ es irreducible.}$$

Supongamos ahora una factorización única en elementos irreducibles del estilo

$$f = f_1^{m_1}\cdot f_2^{m_2}\cdots f_r^{m_r}, \text{ con } f_i \text{ irreducible } \forall\, i\in\{1,\dots,r\}.$$

En tal caso, $\langle f\rangle = \bigcap_{i=1}^r \langle f_i^{m_i}\rangle$, con los $\langle f_i^{m_i}\rangle$ ideales distintos por primalidad de los f_i. En efecto, dados dos elementos arbitrarios de un anillo A, pongamos $a, b \in A$, es inmediato ver que $\langle a\rangle\langle b\rangle = \langle ab\rangle$. Por tanto, $\langle f\rangle = \prod_{i=1}^r \langle f_i^{m_i}\rangle \subset \bigcap_{i=1}^r \langle f_i^{m_i}\rangle$. Para la otra inclusión, es suficiente con tener en cuenta que los f_i son irreducibles y $K[X_1,...,X_n]$ un *DFU*. También resulta sencillo comprobar que el radical respeta la intersección de ideales y que, si $\mathfrak{p}$ es un ideal primo de A, entonces $\mathrm{rad}(\mathfrak{p}^t) = \mathfrak{p}, \forall\, t > 0, t\in\mathbb{Z}$. Se sigue que $\mathrm{rad}(f) = \bigcap_{i=1}^r\langle f_i\rangle$, con los $\langle f_i\rangle$ ideales primos distintos. Aplicando el *Teorema de los ceros fuerte* (*Teorema* 1.17) vemos que

$$V(f) = VI(V(f)) = V(IV(f)) = V(\mathrm{rad}(f)) = V(\bigcap_{i=1}^r \langle f_i\rangle) \overset{Prop.\ 1.6}{=} \bigcup_{i=1}^r V(f_i),$$

con los $V(f_i)$ conjuntos algebraicos irreducibles distintos por la *Obs.* 1.28.

Lema 1.30. *Sea W un espacio topológico irreducible tal que $W = \bigcup_{i=1}^r W_i$, con los W_i conjuntos cerrados de W. Entonces $W = W_t$ para cierto $t \in \{1,\dots,r\}$.*

Demostración. Para $r = 1$ y $r = 2$ el resultado es trivial. Supongámoslo cierto para $r-1$ y veamos que se mantiene para un $r > 2$ arbitrario. Ponemos $W = W_1 \cup (W_2\cup\cdots\cup W_r)$. Como es irreducible y la unión finita de cerrados es cerrada, entonces si $W = W_2 \cup \cdots \cup W_r$ basta con aplicar la hipótesis de inducción. En otro caso, $W = W_1$ y ya estaría. □

Proposición 1.31. *Sea V un espacio topológico noetheriano. Entonces V es unión finita de cerrados irreducibles. Si la descomposición es irredundante (sin inclusiones entre los cerrados), esta es única salvo reordenaciones. En particular, la propiedad es cierta para los conjuntos algebraicos de $\mathbb{A}^n(K)$.*

Demostración. Es una prueba similar a la del apartado III.) de la *Proposición* 1.18, de carácter constructivo. Se basa en considerar ahora Γ como la familia de subconjuntos de V que no pueden ser escritos como unión finita de cerrados irreducibles. Se supone $V \in \Gamma \Longrightarrow \Gamma \neq \emptyset$ y se llega a una contradicción usando la noetherianidad. La unicidad viene de definir dos aplicaciones entre los conjuntos de índices de dos descomposiciones de V y en ver que son inversas la una de la otra (empleando el *Lema* 1.30), induciendo una correspondencia uno a uno entre los cerrados de cada unión [*Milne*, *Proposición* 2.31]. □

Definición 1.32. Sea V un espacio noetheriano (en particular, podemos pensar en V como conjunto algebraico de $\mathbb{A}^n(K)$) y sea $V = V_1 \cup V_2 \cup \cdots \cup V_r$ la descomposición irredundante única de V en cerrados irreducibles. Diremos que los V_i son las *componentes irreducibles* de V.

Observación 1.33. Notemos que las componentes irreducibles de V son precisamente los maximales respecto a la inclusión de conjuntos de $\widetilde{\Gamma} := \{W \subset V : W \text{ cerrado irreducible de } V\}$. Ciertamente, es claro que los V_i son cerrados e irreducibles por construcción. Supongamos que para cierto $j \in \{1, \ldots, r\}, V_j$ no es un elemento maximal de $\widetilde{\Gamma}$. Entonces, existe $W \in \widetilde{\Gamma}$ tal que $V_j \subsetneq W$. Como $V_j \not\subset V_i, \forall\, i \neq j \Longrightarrow W \not\subset V_i, \forall\, i \neq j$. Sea $\Omega = \{i \in \{1, \ldots, r\} : V_i \not\subset W\}$, entonces

$$V = V_1 \cup V_2 \cup \cdots \cup V_r = W \cup (\bigcup_{k \in \Omega} V_k).$$

Obtenemos así dos descomposiciones finitas irredundantes de V como unión de cerrados irreducibles, contradiciendo la *Proposición* 1.31. De hecho, puede verse que las componentes irreducibles de V son los subconjuntos maximales de entre todos los irreducibles que hay en V, pues la clausura de un irreducible, pongamos $U \subset V$, es también irreducible [2] y $U \subseteq \overline{U}$.

Es natural preguntarse si es posible establecer un resultado análogo para un ideal radical de $K[X_1, \ldots, X_n]$ y una descomposición finita única como intersección de primos. Es decir, nos planteamos si la *Proposición* 1.31 y la *Observación* 1.33 pasan bajo las relaciones del *Teorema de correspondencia* vistas en 1.28. Efectivamente, contamos con el siguiente *Corolario*.

[2] En efecto, sea V un espacio topológico arbitrario y tomemos $W \subset V$ irreducible. Para cada par de abiertos U_1, U_2 de V no disjuntos con $\overline{W}$ (i.e., no disjuntos con W), tenemos que $\emptyset \neq (W \cap U_1) \cap (W \cap U_2) \subset (\overline{W} \cap U_1) \cap (\overline{W} \cap U_2)$.

Corolario 1.34. *Sea $\mathfrak{a}$ un ideal de $K[X_1, \ldots, X_n]$. Se verifica que*

$$\operatorname{rad}(\mathfrak{a}) = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_s,$$

para ciertos ideales primos del anillo de polinomios. Si la intersección es irredundante, la descomposición es única y los $\mathfrak{p}_i$ son justamente los ideales minimales de entre los primos que contienen al ideal $\mathfrak{a}$.

Demostración. Escribimos $V(\mathfrak{a}) = \bigcup_{i=1}^{s} V_i$, atendiendo a la descomposición única de los resultados anteriores. Definimos los ideales primos $\mathfrak{p}_i := I(V_i), \forall\ i \in \{1, \ldots, s\}$. Entonces, por el *Teorema de los ceros fuerte*,

$$V(\operatorname{rad}(\mathfrak{a})) = V(IV(\mathfrak{a})) = VI(V(\mathfrak{a})) = V(\mathfrak{a}) = \bigcup_{i=1}^{s} V_i = \bigcup_{i=1}^{s} V(\mathfrak{p}_i) \overset{\textit{Prop. } 1.6}{=} V(\bigcap_{i=1}^{s} \mathfrak{p}_i).$$

Aplicando $I(\cdot)$ a ambos extremos (recordando que la intersección de radicales es radical) llegamos a que $\operatorname{rad}(\mathfrak{a}) = \bigcap_{i=1}^{s} \mathfrak{p}_i$. La unicidad se demuestra de forma análoga a la ya indicada en la *Proposición* 1.31 y, la minimalidad, a la correspondiente indicada en la *Observación* 1.33. Otra alternativa es emplear el *Teorema de correspondencia* y lo visto para la parte geométrica (es decir, para la descomposición de conjuntos algebraicos de $\mathbb{A}^n(K)$ en sus componentes irreducibles). $\square$

1.8. Bases de trascendencia.

Vamos a terminar el capítulo realizando una pequeña introducción a la teoría de las bases de trascendencia [*Milne*, pp. 35–36].

Definición 1.35. Sea A una K-álgebra. Los elementos $\alpha_1, \ldots, \alpha_n$ se dicen *algebraicamente dependientes* sobre K si existe un polinomio no nulo, $f \in K[X_1, \ldots, X_n]$, tal que $f(\alpha_1, \ldots, \alpha_n) = 0$. En otro caso, los α_i se dicen *algebraicamente independientes* sobre K.

Definición 1.36. Sea $L|K$ una extensión de cuerpos. Para un subconjunto A de L, $K(A)$ será el menor subcuerpo de L respecto a la inclusión que contiene a K y A. Un subconjunto B de L se dirá *algebraicamente dependiente* en A si cada elemento de B es algebraico sobre $K(A)$.

Definición 1.37. Una *base de trascendencia* de L sobre K es un subconjunto S de L algebraicamente independiente (i.e., toda familia finita de elementos de S cumple la definición de ser algebraicamente independiente sobre K) de forma que $L|K(S)$ es una extensión algebraica de cuerpos.

Proposición 1.38. *Supongamos que existe A un subconjunto finito de L tal que $L|K(A)$ es una extensión algebraica. Entonces:*

I.) Todo elemento maximal de $\{S \subset L : S$ *es algebraicamente independiente sobre* $K\}$ *es una base de trascendencia de* L *sobre* K.

II.) Todo elemento minimal de $\{S \subset L : L|K(S)$ *es una extensión algebraica*$\}$ *es una base de trascendencia de* L *sobre* K.

III.) Todas las bases de trascendencia de L *sobre* K *tienen el mismo número de elementos.*

No añadiremos la demostración. Véase [*Milne, FT*, pp. 150–151].

Definición 1.39. En las condiciones del resultado anterior, llamamos *grado de trascendencia* de L sobre K al número de elementos de una base de trascendencia arbitraria. Se usará comúnmente la notación $\operatorname{tr}\deg_K(L)$.

Capítulo 2

El lenguaje de las curvas.

2.1. El anillo de coordenadas de un conjunto algebraico.

Definición 2.1. A partir de ahora llamaremos a $\mathbb{A}^n(K)$ el *espacio afín n-dimensional* sobre K. En particular, diremos que $\mathbb{A}^1(K)$ es la *recta afín* y que $\mathbb{A}^2(K)$ es el *plano afín*.

Fijado K, los conjuntos algebraicos en $\mathbb{A}^n(K)$ se denominarán alternativamente *conjuntos algebraicos afines*. Sus elementos son los *puntos*, usualmente denotados con la letra P. Dado $V \subseteq \mathbb{A}^n(K)$ un conjunto algebraico (afín) irreducible, entonces diremos que V es una *variedad afín* (en particular, $\mathbb{A}^n(K)$ es una variedad afín). Si $W \subset V$ es otra variedad, se dice *subvariedad afín* de V.

Definición 2.2. Sea $V \subseteq \mathbb{A}^n(K)$ un conjunto algebraico del espacio afín n-dimensional sobre K y sea $\mathfrak{a} := I(V)$ su ideal radical asociado. Definimos el *anillo de coordenadas* de V como

$$\mathrm{A}(V) := K[X_1, \ldots, X_n]/\mathfrak{a}.$$

Esta es obviamente una K-álgebra finitamente generada por las clases de los elementos $X_1, \ldots, X_n$. Como $\mathfrak{a}$ es radical, $\mathrm{A}(V)$ es reducido, pero no necesariamente un dominio. No obstante, si V fuese una variedad afín entonces $\mathrm{A}(V)$ sí es dominio de integridad, pues $\mathfrak{a}$ sería un ideal primo.

Definición 2.3. En las hipótesis anteriores, con V un conjunto algebraico (afín) arbitrario, denotamos por $\mathcal{F}(V, K)$ al conjunto de funciones de V en K. Dotamos a dicho conjunto de estructura de anillo mediante las evidentes operaciones de suma y producto de dos elementos cualesquiera $f, g \in \mathcal{F}(V, K)$:

- $f + g : V \longrightarrow K$; $P \mapsto (f + g)(P) := f(P) + g(P)$
- $f \cdot g : V \longrightarrow K$; $P \mapsto (f \cdot g)(P) := f(P)g(P)$

Observación 2.4. Resulta inmediato ver que se puede establecer un isomorfismo de anillos entre K y el subanillo de $\mathcal{F}(V,K)$ constituido por todas las funciones constantes de V en K. Consecuentemente, entenderemos $\mathcal{F}(V,K)$ dotado de una estructura natural de K-álgebra.

2.2. Las funciones regulares de un conjunto algebraico en K.

Definición 2.5. Diremos que un elemento, $f \in \mathcal{F}(V,K)$, es una *función polinómica* (ó *función regular*) de V en K si existe un $F \in K[X_1,\ldots,X_n]$ tal que $f(P) = F(P), \forall\ P \in V$. El conjunto de funciones polinómicas de V en K es un subanillo de $\mathcal{F}(V,K)$. Lo denotaremos por $\mathcal{P}ol(V,K)$. Contamos, pues, con la siguiente cadena de extensiones de anillos:

$$K \subset \mathcal{P}ol(V,K) \subset \mathcal{F}(V,K).$$

Observación 2.6. Es importante señalar que dos elementos, $F, G \in K[X_1,\ldots,X_n]$, definen la misma función en $\mathcal{F}(V,K)$ si, y sólo si, $(F-G)(P) = 0, \forall\ P \in V$. Equivalentemente, $F - G \in I(V) =: \mathfrak{a}$, i.e., $\overline{F} = \overline{G}$ en $\mathrm{A}(V) = K[X_1,\ldots X_n]/\mathfrak{a}$. Recogemos esta información en el siguiente isomorfismo para verlo más claro:

$$\begin{array}{ccc} \mathrm{A}(V) = K[X_1,\ldots,X_n]/\mathfrak{a} & \xrightarrow{\qquad\Phi\qquad} & \mathrm{Im}(\Phi) \subset \mathcal{F}(V,K) \\ \overline{F} & \longmapsto & \begin{array}{c}\Phi(F) := f \\ f : V \longrightarrow K;\ P \mapsto F(P)\end{array} \end{array}$$

Es inmediato llegar a que $\mathrm{Im}(\Phi) = \mathcal{P}ol(V,K)$, luego podemos identificar por isomorfía al anillo de coordenadas de V con el subanillo de funciones polinómicas (ó regulares) de $\mathcal{F}(V,K)$. Esto es, $\mathrm{A}(V) \cong \mathcal{P}ol(V,K)$. En resumidas cuentas, entendemos un elemento de $\mathrm{A}(V)$ como una *función regular* en V ó, alternativamente, como una *clase de equivalencia* en un cociente de $K[X_1,\ldots,X_n]$.

Definición 2.7. Una *función coordenada en* V es una función regular de V en K de la forma

$$x_i : V \longrightarrow K;\ P = (a_1,\ldots,a_{i-1},a_i,a_{i+1},\ldots,a_n) \mapsto a_i,$$

para algún $i \in \{1,\ldots,n\}$. Empleando el isomorfismo anterior, puede verse que $\mathrm{A}(V)$ es una K-álgebra finitamente generada por las funciones coordenadas en V. Es decir,

$$\mathrm{A}(V) \cong K[x_1,\ldots,x_n] = \mathcal{P}ol(V,K) \subset \mathcal{F}(V,K),$$

donde el homomorfismo de anillos de K en $\mathcal{P}ol(V,K)$ que induce la estructura de álgebra es precisamente la inclusión $K \hookrightarrow \mathcal{P}ol(V,K)$.

Observación 2.8. Tomemos un ideal de $\mathrm{A}(V)$, pongamos $\mathfrak{b} \subset \mathrm{A}(V)$. Definimos el conjunto

$$\widetilde{V}(\mathfrak{b}) = \{P \in V : f(P) = 0, \forall\ f \in \mathfrak{b}\}.$$

Obviamente, $\widetilde{V}(\mathfrak{b}) = V \cap V(\{F \in K[X_1, \ldots, X_n] : \overline{F} \in \mathfrak{b}\}) = V \cap V(\pi^{-1}(\mathfrak{b}))$, siendo

$$K[X_1, \ldots, X_n] \xrightarrow{\quad\pi\quad} \frac{K[X_1, \ldots, X_n]}{\mathfrak{a}}$$

el homomorfismo canónico de paso al cociente. Entonces, $\widetilde{V}(\mathfrak{b})$ es un conjunto algebraico de $\mathbb{A}^n(K)$ contenido en V, luego es un cerrado de V. Podemos considerar un segundo homomorfismo cociente, digamos $\widetilde{\pi}$, que se muestra en el siguiente diagrama:

$$K[X_1, \ldots, X_n] \xrightarrow{\quad\pi\quad} \frac{K[X_1, \ldots, X_n]}{\mathfrak{a}} = \mathrm{A}(V) \xrightarrow{\quad\widetilde{\pi}\quad} \frac{\mathrm{A}(V)}{\mathfrak{b}} \cong \mathrm{A}(\widetilde{V}(\mathfrak{b}))$$

La idea es llevar una función regular de $\mathbb{A}^n(K)$ en K a su restricción en V para, finalmente, considerar su restricción al subconjunto cerrado $\widetilde{V}(\mathfrak{b}) \subset V$. Si queremos demostrar que estos pasos son coherentes, es evidente que debemos probar cuándo es cierta la relación de isomorfía

$$\frac{\mathrm{A}(V)}{\mathfrak{b}} \cong \mathrm{A}(\widetilde{V}(\mathfrak{b})).$$

Vamos a realizar las aclaraciones pertinentes:

I.) En primer lugar, notemos que los ceros comunes de los representantes de las clases del ideal $\mathfrak{b}$ están todos ellos contenidos en V. Esta es una condición que ha de cumplirse necesariamente por definición, pues $0 \in \mathfrak{b}$. Formalmente,

$$\widetilde{V}(\mathfrak{b}) = V \cap V(\pi^{-1}(\mathfrak{b})) = VI(V) \cap V(\pi^{-1}(\mathfrak{b})) = V(I(V)) \cap V(\pi^{-1}(\mathfrak{b})) =$$
$$V(\mathfrak{a}) \cap V(\pi^{-1}(\mathfrak{b})) \overset{Prop.\ 1.6}{=} V(\mathfrak{a} + \pi^{-1}(\mathfrak{b})) \overset{[\mathfrak{a} \subset \pi^{-1}(\mathfrak{b})]}{=} V(\pi^{-1}(\mathfrak{b})).$$

II.) Como $\dfrac{K[X_1, \ldots, X_n]}{\pi^{-1}(\mathfrak{b})} \cong \dfrac{\mathrm{A}(V)}{\mathfrak{b}}$, basta entonces con comprobar cuándo $\dfrac{K[X_1, \ldots, X_n]}{\pi^{-1}(\mathfrak{b})} \cong \mathrm{A}(\widetilde{V}(\mathfrak{b}))$.

III.) Obsérvese que $I(\widetilde{V}(\mathfrak{b})) = IV(\pi^{-1}(\mathfrak{b})) \Longrightarrow \mathrm{A}(\widetilde{V}(\mathfrak{b})) := \dfrac{K[X_1, \ldots, X_n]}{I(\widetilde{V}(\mathfrak{b}))} = \dfrac{K[X_1, \ldots, X_n]}{\mathrm{rad}(\pi^{-1}(\mathfrak{b}))}$. Estudiamos el homomorfismo de K-álgebras dado por

$$\begin{array}{ccc} \dfrac{K[X_1, \ldots, X_n]}{\pi^{-1}(\mathfrak{b})} & \xrightarrow{\quad\Psi\quad} & \dfrac{K[X_1, \ldots, X_n]}{\mathrm{rad}(\pi^{-1}(\mathfrak{b}))} \\ [F]_{\pi^{-1}(\mathfrak{b})} & \longmapsto & [F]_{\mathrm{rad}(\pi^{-1}(\mathfrak{b}))} \end{array}$$

Puesto que $\pi^{-1}(\mathfrak{b}) \subset \operatorname{rad}(\pi^{-1}(\mathfrak{b}))$, el homomorfismo Ψ está bien definido. La sobreyectividad es inmediata. Para la inyectividad, se tiene que

$$\operatorname{Ker}(\Psi) = \{[F]_{\pi^{-1}(\mathfrak{b})} \in \frac{K[X_1,\ldots,X_n]}{\pi^{-1}(\mathfrak{b})} : F \in \operatorname{rad}(\pi^{-1}(\mathfrak{b}))\} = 0 \Longleftrightarrow \pi^{-1}(\mathfrak{b}) \text{ es ideal radical.}$$

Consecuentemente, una condición suficiente para la isomorfía (por alguna aplicación) es que $\pi^{-1}(\mathfrak{b})$ sea radical.

IV.) El *Teorema de correspondencia para anillos conmutativos* pone de manifiesto una biyección de la forma

$$\left\{ \begin{array}{c} I \text{ ideal de } K[X_1,\ldots,X_n], \\ \text{con } \mathfrak{a} \subset I \end{array} \right\} \underset{\pi^{-1}}{\overset{\pi}{\rightleftarrows}} \left\{ \begin{array}{c} J \text{ ideal de} \\ \mathrm{A}(V) = \dfrac{K[X_1,\ldots,X_n]}{\mathfrak{a}} \end{array} \right\}$$

La relación biunívoca anterior preserva radicalidad, carácter primo y maximalidad entre ideales de un conjunto a otro (es un ejercicio muy sencillo comprobarlo). Podemos reformular la condición suficiente de isomorfía del apartado anterior pidiendo, simplemente, que $\mathfrak{b}$ sea un ideal radical.

Ejemplo 2.9. Vamos a ver un caso en el que $\mathfrak{b}$ no es ideal radical del anillo de coordenadas de V y llegaremos a que $\dfrac{\mathrm{A}(V)}{\mathfrak{b}} \ncong \mathrm{A}(\widetilde{V}(\mathfrak{b}))$. Consideremos $K = \mathbb{C}$ y centraremos nuestro estudio en el *DFU*, $\mathbb{C}[X,Y]$. Sea $F(X,Y) = Y$. Seleccionamos el conjunto algebraico

$$V := V(F) = \{(x,0) \in \mathbb{C}^2 : x \in \mathbb{C}\}.$$

Como $\operatorname{dg}(F) = 1$, entonces F es irreducible, luego $\langle F \rangle$ es primo y por tanto radical. De este modo, deducimos que

$$I(V) = I(V(F)) = \langle F \rangle = \langle Y \rangle.$$

Se sigue que $\mathrm{A}(V) = \dfrac{\mathbb{C}[X,Y]}{\langle Y \rangle} \cong \mathbb{C}[X]$, que continúa siendo un dominio de integridad. Tomemos ahora el ideal $\mathfrak{b} := \langle X^2 \rangle \subset \mathbb{C}[X] \cong \mathrm{A}(V)$. Obviamente $\mathfrak{b}$ no es radical porque $\operatorname{rad}(\mathfrak{b}) = \langle X \rangle \neq \langle X^2 \rangle$. Contamos con el diagrama

$$\mathbb{C}[X,Y] \xrightarrow{\ \pi\ } \frac{\mathbb{C}[X,Y]}{\langle Y \rangle} = \mathrm{A}(V) \cong \mathbb{C}[X] \xrightarrow{\ \widetilde{\pi}\ } \frac{\mathrm{A}(V)}{\mathfrak{b}} \cong \frac{\mathbb{C}[X]}{\langle X^2 \rangle}$$

Calculemos los anillos involucrados en la posible relación de isomorfía:

- En primer lugar, $\dfrac{\mathrm{A}(V)}{\mathfrak{b}} \cong \dfrac{\mathbb{C}[X]}{\langle X^2 \rangle}$, como ya señalamos en el diagrama. En este anillo hay elementos nilpotentes. Por ejemplo, el elemento $\overline{X} \neq 0$ es tal que $\overline{X} \cdot \overline{X} = \overline{X^2} = 0$.
- En segundo lugar, $\mathrm{A}(\widetilde{V}(\mathfrak{b})) = \dfrac{\mathbb{C}[X,Y]}{\operatorname{rad}(\pi^{-1}(\mathfrak{b}))} = \dfrac{\mathbb{C}[X,Y]}{\pi^{-1}(\operatorname{rad}(\mathfrak{b}))} = \dfrac{\mathbb{C}[X,Y]}{\langle X,Y \rangle} \cong \mathbb{C}$. Obtenemos un cuerpo, que no tiene elementos nilpotentes no nulos.

No podemos establecer la isomorfía del enunciado.

Proposición 2.10. *Existe una correspondencia biyectiva entre*

$$\left\{ \begin{array}{c} \textit{Ideales radicales} \\ \textit{de } \mathrm{A}(V) \end{array} \right\} \underset{\Phi^{-1}}{\overset{\Phi}{\rightleftarrows}} \left\{ \begin{array}{c} \textit{Conjuntos algebraicos de} \\ \mathbb{A}^n(K) \textit{ contenidos en } V \end{array} \right\}$$

Demostración. Basta con considerar las siguientes composiciones, siendo $\mathfrak{a} = I(V)$:

$$\left\{ \begin{array}{c} \text{Ideales radicales} \\ \text{de } \mathrm{A}(V) \end{array} \right\} \underset{\pi}{\overset{\pi^{-1}}{\rightleftarrows}} \left\{ \begin{array}{c} \text{Ideales radicales} \\ \text{de } K[X_1, \ldots, X_n] \\ \text{que contienen a } \mathfrak{a} \end{array} \right\} \underset{I(\cdot)}{\overset{V(\cdot)}{\rightleftarrows}} \left\{ \begin{array}{c} \text{Conjuntos algebraicos} \\ \text{de } \mathbb{A}^n(K) \text{ contenidos en } V \end{array} \right\}$$

□

Observación 2.11. Es evidente que las correspondencias de la *Observación* 1.28 se preservan bajo el resultado anterior. Esto es:

- Los ideales radicales de $\mathrm{A}(V)$ tienen asociados a los conjuntos algebraicos contenidos en V (i.e., a los cerrados de V).
- Los ideales primos de $\mathrm{A}(V)$ se corresponden con las variedades (conjuntos algebraicos irreducibles de $\mathbb{A}^n(K)$) contenidas en V.
- Los ideales maximales de $\mathrm{A}(V)$ se llevan en los puntos de V y viceversa.

2.3. Las aplicaciones regulares entre variedades.

Definición 2.12. Sean $V \subset \mathbb{A}^n(K)$, $W \subset \mathbb{A}^m(K)$ dos variedades de sendos espacios afines. Pondremos $\mathrm{A}(\mathbb{A}^n(K)) = K[X_1, \ldots, X_n]$ y $\mathrm{A}(\mathbb{A}^m(K)) = K[Y_1, \ldots, Y_m]$ para evitar confusión entre las variables. Una aplicación $\varphi : V \longrightarrow W$ se dice *aplicación polinómica* si existen elementos $T_1, \ldots, T_m \in K[X_1, \ldots, X_n]$ tales que

$$\varphi(P) = (T_1(P), \ldots, T_m(P)), \forall\ P \in V.$$

Observación 2.13. Dada una aplicación arbitraria, $\varphi : V \longrightarrow W$, esta induce un homomorfismo de K-álgebras $\varphi^* : \mathcal{F}(W, K) \longrightarrow \mathcal{F}(V, K)$ tal que $\varphi^*(f) = f \circ \varphi, \forall\ f \in \mathcal{F}(W, K)$. Puesto que φ es una aplicación polinómica, toda función regular de W en K compuesta con φ genera una nueva función regular de V en K. Esto se debe a que una combinación algebraica en m variables sobre K, evaluada en m polinomios de n variables cada uno, no es más que una expresión de productos y sumas de dichos polinomios con posibles multiplicaciones por coeficientes de K. Es decir, es una operación cerrada en $K[X_1, \ldots, X_n]$. Tomando clases (equivalentemente, considerando las restricciones oportunas a V), vemos que $\varphi^*(\mathrm{A}(W)) \subset \mathrm{A}(V)$. Podemos establecer, mediante un abuso de notación, que φ^* es su propia restricción de $\mathrm{A}(W)$ en $\mathrm{A}(V)$. La representamos a continuación:

$$\begin{array}{ccc} \mathrm{A}(W) & \xrightarrow{\quad\varphi^*\quad} & \mathrm{A}(V) \\ f = [F]_{I(W)} & \longmapsto & \begin{array}{c}\varphi^*(f) = f \circ \varphi = \\ [F(T_1, \ldots, T_m)]_{I(V)}\end{array} \end{array}$$

Hemos señalado que si $\varphi = (T_1, \ldots, T_m)$ es una aplicación polinómica de V en W, entonces la composición de cualquier elemento $f \in \mathrm{A}(W)$ con φ es una función regular de $\mathrm{A}(V)$. Para el recíproco basta tomar las funciones coordenadas $y_1, ..., y_m$, puesto que $y_i \circ \varphi = T_i$. Luego, cada T_i es la restricción de un elemento de $K[X_1, \ldots, X_n]$ a V, que es justo lo que queríamos probar.

Proposición 2.14. *Existe una correspondencia biyectiva del estilo:*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{Aplicaciones polinómicas} \\ \textit{de } V \textit{ en } W \end{array} \right\} & \begin{array}{c}\longrightarrow \\ \longleftarrow\end{array} & \left\{ \begin{array}{c} \textit{Homomorfismos de} \\ K\textit{-álgebras de} \\ \mathrm{A}(W) \textit{ en } \mathrm{A}(V) \end{array} \right\} \\ \varphi : V \longrightarrow W & \longmapsto & \begin{array}{c}\varphi^* : \mathrm{A}(W) \longrightarrow \mathrm{A}(V) \\ \varphi^*(f) = f \circ \varphi\end{array} \\ \widetilde{\alpha} : V \longrightarrow W & \longleftarrow\!\!\shortmid & \alpha : \mathrm{A}(W) \longrightarrow \mathrm{A}(V) \end{array}$$

En el esquema, $\widetilde{\alpha}$ denota la restricción de una aplicación polinómica

$$T : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K); P \mapsto T(P) = (T_1(P), \ldots, T_m(P))$$

a la variedad afín V, donde cada $T_i \in K[X_1, \ldots, X_n]$ verifica que $[T_i]_{I(V)} = \alpha([Y_i]_{I(W)}) = \alpha(y_i)$, para todo $i \in \{1, \ldots, m\}$.

Demostración. Ya hemos visto que la correspondencia está bien definida hacia la derecha. Para ver lo propio hacia la izquierda, notemos primero que siempre es posible construir una aplicación T cumpliendo los requisitos del enunciado. Ciertamente, basta con aplicar la *Propiedad universal del anillo de polinomios* entre $\mathrm{A}(W) = K[y_1, \ldots, y_m]$ y $\mathrm{A}(V) = K[x_1, \ldots, x_n]$, garantizando la existencia de un homomorfismo tal que $y_i \mapsto t_i := \alpha(y_i)$. Para cada $i \in \{1, \ldots, m\}$, T_i se obtiene tomando un representante cualquiera de la clase residual de t_i.

En segundo lugar señalamos que, de poder restringirse T a un elemento $\widetilde{\alpha}$ del primer conjunto, entonces $\widetilde{\alpha}$ no dependería de la elección de la aplicación polinómica T en las condiciones anteriores. Además, $\widetilde{\alpha}$ estaría unívocamente determinada por el homomorfismo α. Debemos comprobar, simplemente, que $T(V) \subset W$. Para ello, tomemos el homomorfismo inducido

$$T^* : \mathrm{A}(\mathbb{A}^m(K)) = K[Y_1, \dots, Y_m] \longrightarrow \mathrm{A}(\mathbb{A}^n(K)) = K[X_1, \dots, X_n].$$

Sea $F \in I(W)$. Como $[F]_{I(W)} = 0 \in \mathrm{A}(W) \Longrightarrow 0 = \alpha([F]_{I(W)}) = [F(T_1, \dots, T_m)]_{I(V)} = [F \circ T]_{I(V)} = [T^*(F)]_{I(V)} \Longrightarrow T^*(F) \in I(V) \Longrightarrow T^*(I(W)) \subset I(V)$. Se sigue que, para cada $F \in I(W)$, $T(P) \in V(F)$ para todo $P \in V$. Consecuentemente,

$$T(V) \subset V(F), \forall\, F \in I(W) \Longrightarrow T(V) \subset \bigcap_{F \in I(W)} V(F) = V(\sum_{F \in I(W)} \langle F \rangle) = V(I(W)) = W.$$

Demostremos que las correspondencias son inversas la una de la otra. Tomemos $\varphi : V \longrightarrow W$. Es evidente que φ^* devuelve la aplicación φ siguiendo el proceso explicado en el enunciado. Para la otra composición, sea $\alpha : \mathrm{A}(W) \longrightarrow \mathrm{A}(V)$ y denotemos por $\widetilde{\alpha}$ a la aplicación polinómica generada. Tenemos que probar que $(\widetilde{\alpha})^* = \alpha$. Sea $f \in A(W)$ la restricción de un $F \in K[Y_1, \dots, Y_m]$ a W. Entonces,

$$(\widetilde{\alpha})^*(f) = f \circ \widetilde{\alpha} = [F(T_1, \dots, T_m)]_{I(V)} = \alpha([F]_{I(W)}) = \alpha(f).$$

□

Definición 2.15. Una aplicación polinómica $\varphi : V \longrightarrow W$ es un *isomorfismo* si existe otra aplicación polinómica $\Psi : W \longrightarrow V$ tal que $\Psi \circ \varphi = \mathrm{Id}_V$ y $\varphi \circ \Psi = \mathrm{Id}_W$.

Observación 2.16. La *Proposición* 2.14 asegura que dos variedades afines son isomorfas (i.e., podemos establecer un isomorfismo entre ambas) si, y sólo si, lo son sus anillos de coordenadas como K-álgebras. Ciertamente, tomando V, W y Z tres variedades afines arbitrarias de $\mathbb{A}^n(K)$, $\mathbb{A}^m(K)$ y $\mathbb{A}^l(K)$ respectivamente y $\varphi : V \longrightarrow W$, $\Psi : W \longrightarrow Z$ dos aplicaciones polinómicas, entonces es inmediato verificar que su composición es una aplicación polinómica de V en Z y que $(\Psi \circ \varphi)^* = \varphi^* \circ \Psi^*$. Para la implicación hacia la derecha (tomando $l = n$ y $Z = V$), como φ y Ψ son inversas se llega a que:

- $\Psi \circ \varphi = \mathrm{Id}_V \Longrightarrow \varphi^* \circ \Psi^* = (\Psi \circ \varphi)^* = \mathrm{Id}_V^* = \mathrm{Id}_{\mathrm{A}(V)}$.
- $\varphi \circ \Psi = \mathrm{Id}_W \Longrightarrow \Psi^* \circ \varphi^* = (\varphi \circ \Psi)^* = \mathrm{Id}_W^* = \mathrm{Id}_{\mathrm{A}(W)}$.

Recíprocamente, puede verse que la composición de homomorfismos de K-álgebras entre anillos de coordenadas pasa bajo la correspondencia hacia la izquierda invirtiendo el orden de las aplicaciones, justo como en el caso anterior.

2.4. Los cambios de coordenadas afines.

Definición 2.17. Un *cambio de coordenadas afín* en $\mathbb{A}^n(K)$ es una aplicación polinómica

$$T = (T_1, \ldots, T_m) : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^n(K)$$

verificando que T es biyectiva y $\mathrm{dg}(T_i) = 1$, para cada $i \in \{1, \ldots, n\}$.

Observación 2.18. Si $T_i = \sum_{j=1}^n a_{ij} X_j + a_{i0}$, entonces $T = T'' \circ T'$. En la igualdad anterior, T' es una aplicación K-lineal con $T_i' = \sum_{j=1}^n a_{ij} X_j$ y T'' es una traslación tal que $T_i'' = X_i + a_{i0}$. Como toda traslación admite una traslación inversa, T será biyectiva si, y sólo si, T' es invertible. Es sencillo comprobar que la composición de cambios de coordenadas afines es un cambio de coordenadas afín, así como el cambio de coordenadas inverso, T^{-1}. Consecuentemente, T es un isomorfismo de $\mathbb{A}^n(K)$ en sí mismo.

2.5. Funciones racionales y anillos locales.

Definición 2.19. Tomemos V una variedad afín no vacía de $\mathbb{A}^n(K)$. Sabemos que su anillo de coordenadas es un dominio, luego tiene sentido considerar su cuerpo de fracciones (i.e., la localización de $\mathrm{A}(V)$ en el subconjunto multiplicativo $\mathrm{A}(V)\backslash\{0\}$). Se llamará de ahora en adelante *cuerpo de funciones racionales* en V y se denotará como $\mathrm{K}(V)$. Un elemento de $\mathrm{K}(V)$ es lo que se denomina una *función racional* en V. Como todo elemento a de $\mathrm{A}(V)$ puede identificarse por isomorfía con $\frac{a}{1} \in \mathrm{K}(V)$, a nivel de extensiones de anillos se tiene que

$$K \subset \mathrm{A}(V) \subset \mathrm{K}(V).$$

Definición 2.20. Si $f \in \mathrm{K}(V)$ y $P \in V$, diremos que f está *definida* en P si $f = \frac{a}{b}$ para alguna elección de $a, b \in \mathrm{A}(V)$ tales que $b(P) \neq 0$. Es importante recordar que, al localizar, entendemos $\frac{a}{b}$ como una clase de equivalencia. Podríamos tener diversas formas de expresar f como una función racional (a nivel fracción) y diríamos que f está definida en P si es posible seleccionar algún *denominador* para f que no se anule en P. Cuando $\mathrm{A}(V)$ es un *DFU*, existe una única representación del estilo $f = \frac{a}{b}$ cumpliendo que a y b no comparten factores comunes. En este caso, f estaría definida en P si, y sólo si, $b(P) \neq 0$.

Definición 2.21. Sea $P \in V$. Definimos $\mathcal{O}_P(V)$ como el conjunto de funciones racionales de V definidas en P. Las operaciones internas de $\mathrm{K}(V)$ son las de un anillo localizado, es decir, para $\frac{a}{b}, \frac{c}{d} \in \mathrm{K}(V)$ arbitrarios:

- $\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$.
- $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$.

Según lo anterior, es evidente que $\mathcal{O}_P(V)$ es un subanillo de $\mathrm{K}(V)$ verificando la siguiente cadena de inclusiones:

$$K \subset \mathrm{A}(V) \subset \mathcal{O}_P(V) \subset \mathrm{K}(V).$$

Llamaremos a $\mathcal{O}_P(V)$ el *anillo local* de V en P. El conjunto de puntos de V donde una función racional fijada, f, no está definida es el denominado *conjunto de polos* de f.

Proposición 2.22. *Dada V una variedad afín arbitraria de $\mathbb{A}^n(K)$ y $f \in \mathrm{K}(V)$ una función racional en V. Se cumplen los siguientes afirmaciones:*

I.) El conjunto de polos de f es un subconjunto algebraico de V.

II.) $\mathrm{A}(V) = \bigcap_{P\in V} \mathcal{O}_P(V)$.

Demostración. Comencemos demostrando el primer apartado. Dado $G \in K[X_1, \ldots, X_n]$, denotaremos por $\overline{G}$ a la clase de G en $\mathrm{A}(V)$. Definimos el conjunto

$$J_f = \{G \in K[X_1, \ldots, X_n] : \overline{G} \cdot f \in \mathrm{A}(V)\}.$$

Es inmediato comprobar que J_f es un ideal del anillo de polinomios $K[X_1, \ldots, X_n]$ que contiene a $I(V)$ (pues todos los elementos de $I(V)$ se hacen cero en el cociente). Resulta que los puntos de $V(J_f)$ son precisamente aquellos puntos en los que f no está definida, es decir, su conjunto de polos. Esto se debe a que la definición de J_f viene motivada por la idea de hallar los candidatos a denominador para una expresión racional de f. Cuando determinamos un punto en el que todos ellos se anulan (i.e., un punto de $V(J_f)$), lo que estamos haciendo no es más que localizar un polo. Para el segundo de los enunciados, llega con ver la inclusión hacia la izquierda, ya que $\mathcal{O}_P(V) \supset \mathrm{A}(V), \forall\, P \in V$. Sea $f \in \bigcap_{P\in V} \mathcal{O}_P(V)$. Entonces, es claro que

$$V(J_f) = \emptyset \overset{\textit{Teorema } 1.9}{\Longrightarrow} 1 \in J_f \Longrightarrow 1 \cdot f = f \in \mathrm{A}(V).$$

□

Observación 2.23. Supongamos $f \in \mathcal{O}_P(V)$. Podemos definir el *valor de f en P* como sigue: escribimos $f = \dfrac{a}{b}$, con $a, b \in \mathrm{A}(V)$, $b(P) \neq 0$ y ponemos $f(P) := \dfrac{a(P)}{b(P)} \in K$. Es necesario plantearse si el valor anterior depende de la elección de a y b. Sea $f = \dfrac{a}{b} = \dfrac{c}{d}$ en las condiciones anteriores. Para cierto $u \neq 0 \in \mathrm{A}(V)$, se llega a que $u(ad-cb) = 0$. Como el anillo de coordenadas es un dominio de integridad, la igualdad anterior implica que $ad - cb = 0$. Esto es, para $P \in V$,

$$a(P)d(P) - c(P)b(P) = 0 \in K \Longrightarrow \frac{a(P)}{b(P)} = \frac{c(P)}{d(P)}.$$

Definición 2.24. El ideal $\mathfrak{m}_P(V) = \{f \in \mathcal{O}_P(V) : f(P) = 0\}$ recibe el nombre de *ideal maximal de V en P.*

Observación 2.25. $\mathfrak{m}_P(V)$ es el núcleo del homomorfismo evalaución $\Phi : \mathcal{O}_P(V) \longrightarrow K$ tal que $f \mapsto f(P)$. Como $K \subset \mathcal{O}_P(V)$, es obvio que Φ es sobreyectivo. Es por ello que $K \cong \dfrac{\mathcal{O}_P(V)}{\mathfrak{m}_P(V)}$. Llegamos a que $\mathfrak{m}_P(V)$ es un ideal maximal del anillo local de V en P. Una importante propiedad de $\mathcal{O}_P(V)$ es que, al tratarse de un subanillo del localizado de $\mathrm{A}(V)$, un elemento $f = \dfrac{a}{b} \in \mathcal{O}_P(V)$ es una unidad de $\mathcal{O}_P(V)$ si, y sólo si, $f(P) \neq 0$. Ciertamente, esta es una condición suficiente y necesaria para que $a(P) \neq 0$ y podamos tomar el inverso multiplicativo de f, $\dfrac{b}{a} \in \mathcal{O}_P(V)$. Obtenemos, por el razonamiento anterior, que $\mathfrak{m}_P(V) = \mathcal{O}_P(V) \setminus \mathcal{O}_P(V)^*$. Es decir, el ideal maximal de V en P es el conjunto de elementos de $\mathcal{O}_P(V)$ que no son unidades del anillo local de V en P. Hemos visto que, en efecto, $\mathcal{O}_P(V)$ es un anillo local cuyo único ideal maximal es $\mathfrak{m}_P(V)$.

Proposición 2.26. *$\mathcal{O}_P(V)$ es un anillo noetheriano.*

Demostración. Basta ver que todo ideal $\mathfrak{a}$ de $\mathcal{O}_P(V)$ es finitamente generado. Como $\mathrm{A}(V) = \dfrac{K[X_1, \ldots, X_n]}{I(V)}$ es un cociente de un anillo noetheriano, es trivialmente noetheriano. Tomemos generadores $f_1, \ldots, f_r$ del ideal $\mathfrak{a} \cap \mathrm{A}(V)$ de $\mathrm{A}(V)$. Demostraremos que [1]

$$\mathfrak{a} = \langle f_1, \ldots, f_r \rangle \mathcal{O}_P(V).$$

La inclusión hacia la izquierda es inmediata. Para la pertinente hacia la derecha, dado $f \in \mathfrak{a} \subset \mathcal{O}_P(V)$, es posible tomar un $b \in \mathrm{A}(V)$ de modo que $b(P) \neq 0$ y $bf \in \mathrm{A}(V)$. Como $\mathfrak{a}$ es ideal del anillo local de V en P y $\mathrm{A}(V) \subset \mathcal{O}_P(V)$, se sigue que $bf \in \mathfrak{a} \cap \mathrm{A}(V) \Longrightarrow bf = \sum_{i=1}^r a_i f_i$, para ciertos $a_1, \ldots, a_r \in \mathrm{A}(V)$. Concluimos que $f = \sum_{i=1}^r \dfrac{a_i}{b} f_i$, con los $\dfrac{a_i}{b}$ funciones racionales en V definidas en P. Una demostración alternativa más directa consiste en ver que $\mathcal{O}_P(V)$ es la localización de $\mathrm{A}(V)$ en $\mathfrak{m} := \langle x_1, \ldots, x_n \rangle$ y, como $\mathrm{A}(V)$ es noetheriano, $\mathcal{O}_P(V)$ también cumplirá la propiedad. Redactaremos la prueba de dicho resultado en la *Observación* 3.28 para $n = 2$, siendo análoga la de su generalización a un número de variables cualquiera. $\square$

2.6. La dimensión de un conjunto algebraico.

Definición 2.27. Sea V un conjunto algebraico de $\mathbb{A}^n(K)$. La *dimensión* de V se define como

$$\dim(V) := \sup\{n \in \mathbb{N} : \exists\, V_0 \supset V_1 \supset \cdots \supset V_n \text{ cadena irredundante de cerrados irreducibles de } V\}.$$

[1] Hagamos un pequeño inciso para explicar la notación. Sean A y B dos anillos y $f : A \longrightarrow B$ un homomorfismo entre ambos. Para un ideal $\mathfrak{a}$ de A, $\mathfrak{a}^e$ denotará la extensión de $\mathfrak{a}$ a través de f en B. Es decir, $\mathfrak{a}^e$ es el ideal de B generado por el conjunto imagen $f(\mathfrak{a})$. También pondremos $\mathfrak{a}B$ cuando quede claro quién es el homomorfismo f subyacente, siendo esta última escritura muy común al hablar de inclusiones del estilo $i : A \hookrightarrow B$.

Definición 2.28. Sean $V_1, \dots, V_m$ las componentes irreducibles de V. Como estos conjuntos son los cerrados irreducibles maximales de V, entonces

$$\dim(V) = \text{máx}\{\dim(V_i) : i \in \{1, \dots, m\}\}.$$

Si $\dim(V_i) = d, \forall\ i \in \{1, \dots, m\}$, diremos que V tiene *dimensión pura d*.

Observación 2.29. Si V es una variedad afín y W es un cerrado propio de V, entonces toda cadena $W_0 \supset W_1 \supset \cdots \supset W_d$ en W se extiende de forma inmediata a $V \supset W_0 \supset \cdots \supset W_d$. Es por ello que $\dim(W) + 1 \leq \dim(V)$. Si $\dim(V) < \infty \Longrightarrow \dim(W) < \dim(V)$. Esta desigualdad vale para demostrar los siguientes enunciados para V una variedad afín arbitraria:

- $\dim(V) = 0$ si, y sólo si, V es un punto de $\mathbb{A}^n(K)$.
- $\dim(V) \leq 1$ si, y sólo si, todo cerrado propio W de V es un punto.
- $\dim(V) \leq n$ si, y sólo si, todo cerrado propio W de V cumple que $\dim(W) \leq n - 1$.

Proposición 2.30. *Para un conjunto algebraico cualquiera, V, de $\mathbb{A}^n(K)$ se cumple que*

$$\dim(V) = \text{dimKrull}(\text{A}(V)).$$

Demostración. Basta con aplicar la correspondencia vista en la *Observación* 2.11, recordando que se invierten las inclusiones. Hay una asociación biunívoca entre cerrados irreducibles de V e ideales primos de su anillo de coordenadas. □

Definición 2.31. Sea V una variedad afín de $\mathbb{A}^n(K)$ y W un cerrado de V. Definimos la *codimensión* de W en V como

$$\text{codim}_V(W) = \dim(V) - \dim(W).$$

El siguiente es un importante resultado cuya demostración no incluiremos. El *Teorema de normalización de Noether* [*Milne*, *Teorema* 2.45] juega un papel relevante en dicha prueba, que puede ser consultada en la bibliografía [*Milne*, *Teorema* 2.52]. También añadimos después algunas proposiciones relacionadas, con el objetivo de motivar adecuadamente las definiciones de la siguiente sección [*Milne*, pp. 56–58].

Teorema 2.32. *Sea V una variedad afín de $\mathbb{A}^n(K)$. Entonces,*

$$\dim(V) = \text{tr deg}_K(\text{K}(V)).$$

Proposición 2.33. *El espacio afín $\mathbb{A}^n(K)$ tiene dimensión n.*

Demostración. Pongamos $V = \mathbb{A}^n(K)$. Entonces, $\mathrm{A}(V) = K[X_1, \ldots, X_n]$ y por ello $\mathrm{K}(V) = K(X_1, \ldots, X_n)$. Es fácil ver que $\{X_1, \ldots, X_n\}$ es base de trascendencia de $\mathrm{K}(V)$ sobre K. Si aplicamos ahora el *Teorema* 2.32, obtenemos que $\dim(V) = n$. $\square$

Proposición 2.34. *Sea V una variedad afín de $\mathbb{A}^n(K)$ y W un cerrado de V tal que* $\mathrm{codim}_V(W) = 1$. *Si* $\mathrm{A}(V)$ *es un DFU, entonces* $I(W) = \langle f \rangle$ *para algún* $f \in \mathrm{A}(V)$.

Demostración. Antes de empezar con la prueba, debemos aclarar qué significa la igualdad $I(W) = \langle f \rangle$ del enunciado. Esta identidad debe pensarse según la explicación dada en la *Observación* 2.11, es decir, bajo la correspondencia que asocia los ideales radicales de $\mathrm{A}(V)$ con los conjuntos algebraicos contenidos V (sus cerrados). Si $\pi : K[X_1, \ldots, X_n] \longrightarrow \mathrm{A}(V)$ es el homomorfismo canónico de paso al cociente, lo que afirmamos es que el ideal $\pi(I(W))$ de $\mathrm{A}(V)$ es principal. Equivalentemente, $\exists\ f \in \mathrm{A}(V)$ de forma que $I(W) = \pi^{-1}(\langle f \rangle)$.

Sean $W_1, \ldots, W_s$ las componentes irreducibles de W tales que $W = \bigcup_{i=1}^s W_i$. Se sigue inmediatamente de la *Observación* 1.12 que $I(W) = \bigcap_{i=1}^s I(W_i)$. Basta con demostrar que, dado $i \in \{1, \ldots, s\}$, $I(W_i) = \pi^{-1}(\langle f_i \rangle)$ para algún $f_i \in \mathrm{A}(V)$ irreducible (equivalentemente primo, porque $\mathrm{A}(V)$ es *DFU* por hipótesis). En tal caso,

$$I(W) = \bigcap_{i=1}^{s} \pi^{-1}(\langle f_i \rangle) = \pi^{-1}(\bigcap_{i=1}^{s} \langle f_i \rangle) = \pi^{-1}(\prod_{i=1}^{s} \langle f_i \rangle) = \pi^{-1}(\langle f_1 \cdots f_s \rangle).$$

La tercera igualdad se deduciría de un razonamiento análogo al del *Ejemplo* 1.29, teniendo en cuenta que el anillo de coordenadas de V es *DFU*. Supondremos, sin pérdida de generalidad, que W es irreducible. Entonces, $\mathfrak{p} := I(W)$ es un ideal primo no nulo (en otro caso, por la *Observación* 1.21 llegaríamos a que $W = \mathbb{A}^n(K) \Longrightarrow n = \dim(W) = \dim(V) \Longrightarrow \mathrm{codim}_V(W) \neq 1$). Como π preserva el carácter primo, $\pi(\mathfrak{p})$ es un ideal primo no nulo de $\mathrm{A}(V)$. Es sabido que todo ideal primo no nulo de un *DFU* contiene al menos un elemento irreducible de dicho anillo [2]. Sea $f \in \pi(\mathfrak{p}) \subset \mathrm{A}(V)$ irreducible y supongamos que $\langle f \rangle \neq \pi(\mathfrak{p})$. Tenemos las siguientes inclusiones entre ideales primos distintos del anillo de coordenadas de V:

$$\pi(\mathfrak{p}) \supset \langle f \rangle \supset \langle 0 \rangle \Longrightarrow \mathfrak{p} \supset \pi^{-1}(\langle f \rangle) \supset \pi^{-1}(\langle 0 \rangle) = I(V).$$

Por tanto, se llega a la siguiente cadena de cerrados irreducibles de V distintos:

$$W = V(\mathfrak{p}) \subset V(\pi^{-1}(\langle f \rangle)) \subset V.$$

Por la *Observación* 2.29, $\dim(W) < \dim(V(\pi^{-1}(\langle f \rangle))) < \dim(V) \Longrightarrow \mathrm{codim}_V(W) \geq 2$, que es una clara contradicción con el hecho de que $\mathrm{codim}_V(W) = 1$. $\square$

[2]Efectivamente, un ideal no nulo contiene al menos un elemento distinto de cero. Si este es irreducible ya está. Si no, admite una factorización única en producto finito de irreducibles. Aplicando primalidadad, si un elemento fijado (irreducible) de la factorización no pertenece al ideal, entonces lo hará el producto de los restantes. Procediendo por recurrencia, en un número finito de pasos se concluye el resultado.

2.7. Hipersuperficies.

Definición 2.35. Una *hipersuperficie* en $\mathbb{A}^n(K)$ es un conjunto algebraico $V(F)$ definido por un polinomio, $F \in K[X_1, \ldots, X_n]$, no constante.

Definición 2.36. Consideremos $V(F)$ una hipersuperficie de $\mathbb{A}^n(K)$. Si $\mathrm{dg}(F) = 1$, entonces $V(F)$ se denomina *hiperplano* en $\mathbb{A}^n(K)$. Diremos que una hipersuperficie en $\mathbb{A}^2(K)$ es una *curva algebraica plana afín* y un hiperplano en el mismo espacio, una *recta*.

Vamos a ver la relación que guardan estos nuevos conceptos con los resultados de la sección anterior. Notemos que los nombres precedentes son bien conocidos en otras áreas de las matemáticas como la geometría diferencial. La intuición que se tiene de la *dimensión* desde el punto de vista analítico es la que se espera mantener en nuestro contexto.

Proposición 2.37. *Una hipersuperficie en $\mathbb{A}^n(K)$ tiene dimensión $n-1$.*

Demostración. Sea $V(F)$ una hipersuperficie con $F \in K[X_1, \ldots, X_n]$ no constante cuya factorización única en producto de irreducibles viene dada por

$$F = F_1^{m_1} \cdot F_2^{m_2} \cdots F_r^{m_r}, \text{ con } F_i \text{ irreducible } \forall\, i \in \{1, \ldots, r\}.$$

Por el *Ejemplo* 1.29, sabemos que $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ es la descomposición de la hipersuperficie como unión de sus componentes irreducibles. Cada $V(F_i)$ es una hipersuperficie irreducible (como conjunto algebraico). Si probamos el enunciado para este tipo de variedades afines entonces, fijado $i \in \{1, \ldots, r\}$, se tendría por la *Proposición* 2.33 y la *Observación* 2.29 que

$$n - 1 = \dim(V(F_i)) \leq \dim(V(F)) < \dim(\mathbb{A}^n(K)) = n \Longrightarrow \dim(V(F)) = n - 1.$$

Supondremos, sin pérdida de generalidad, que $F \in K[X_1, \ldots, X_n]$ es irreducible (equivalentemente primo). Consecuentemente, $\langle F \rangle$ es radical y así $I(V(F)) = \langle F \rangle$. Tomemos el anillo de coordenadas de $V(F)$

$$K[x_1, \ldots, x_n] = \frac{K[X_1, \ldots, X_n]}{\langle F \rangle}, \; x_i = [X_i]_{\langle F \rangle}.$$

Sea $K(x_1, \ldots, x_n)$ el cuerpo de funciones racionales en la hipersuperficie. Como F es no constante algún X_i, digamos X_n, aparece en su expresión. De esta forma, X_n aparece en la expresión de todo múltiplo no nulo de F, de lo que se deduce que ningún polinomio en las variables $X_1, \ldots, X_{n-1}$ pertenece a $\langle F \rangle$. Visto de otro modo, ningún elemento generado como combinación algebraica sobre K de los $x_1, \ldots, x_{n-1}$ resulta ser una función regular nula en $V(F)$. Esto implica que los $x_1, \ldots, x_{n-1}$ son algebraicamente independientes sobre K. Por otro lado, x_n es algebraico sobre $K(x_1,\dots,x_{n-1})$ (basta con evaluar [3] $F(x_1,\dots,x_{n-1},Y)$ en $Y = x_n$ y emplear luego el ya conocido isomorfismo de la *Observación* 2.6). Finalmente, obtenemos la base de trascendencia $\{x_1,\dots,x_{n-1}\}$ de $K(x_1,\dots,x_n)$ sobre K. Aplicando el *Teorema* 2.32, concluimos que

$$\dim(V(F)) = \text{tr deg}_K(K(x_1,\dots,x_n)) = n-1.$$

□

Corolario 2.38. *Sea W un conjunto algebraico de $\mathbb{A}^n(K)$. Entonces,*

$$\text{codim}_{\mathbb{A}^n(K)}(W) = 1 \iff W \text{ es una hipersuperficie.}$$

Demostración. La implicación hacia la izquierda es consecuencia directa de la *Proposición* 2.37. Para la necesidad, basta con emplear la *Proposición* 2.34 siendo $V = \mathbb{A}^n(K)$. □

2.8. Variedades en el plano.

El siguiente *Teorema* es un buen resumen de las últimas secciones del capítulo. Permite clasificar los conjuntos algebraicos irreducibles del plano afín $\mathbb{A}^2(K)$ según su dimensión. Nos referiremos a él como *Teorema de caracterización de variedades en el plano afín.*

Teorema 2.39. *Clasificamos las variedades de $\mathbb{A}^2(K)$ siguiendo el siguiente esquema:*

I.) $\dim(V) = 2 \iff V = \mathbb{A}^2(K)$.

II.) $\dim(V) = 1 \iff V = V(F)$, *con* $F \in I(V) \subset K[X_1,\dots,X_n]$ *un polinomio irreducible.*

III.) $\dim(V) = 0 \iff V$ *es un punto.*

Demostración. Es consecuencia directa de los resultados anteriores y de los de la sección precedente. □

Corolario 2.40. *La siguiente es la lista de los únicos ideales primos de $K[X,Y]$:*

I.) $\langle 0\rangle$.

II.) $\langle F\rangle$, *con* $F \in K[X,Y]$ *irreducible.*

III.) $\langle X-a, Y-b\rangle$, *con* $a,b \in K$.

[3] Realizamos un pequeño abuso de notación evaluando F en la n-pla $(x_1,\dots,x_{n-1},Y)$. Esto debe entenderse según la estructura natural de K-álgebra con la que se ha dotado al anillo de coordenadas. F se redefine a través del homomorfismo de K-álgebras tal que $X_i \mapsto x_i, \forall\, i \in \{1,\dots,n-1\}$ y $X_n \mapsto Y$. Se construye, en resumidas cuentas, un polinomio en la variable Y del anillo $K(x_1,\dots,x_{n-1})[Y]$

Demostración. Se sigue inmediatamente del *Teorema de caracterización de variedades en el plano afín* y de la *Observación* 1.28. □

Proposición 2.41. *Sean $F(X,Y)$ y $G(X,Y)$ dos polinomios no constantes de $K[X,Y]$ sin factores comunes. Entonces, las curvas planas $V(F)$ y $V(G)$ se cortan en un número finito de puntos.*

Demostración. Es claro que $V(F)$ tiene dimensión 1 por la *Proposición* 2.37. Puesto que F y G no tienen factores comunes y poniendo $W := V(F) \cap V(G)$, por la *Observación* 2.29 deducimos que $\dim(W) = \text{máx}\{\dim(W_i) : i \in \{1, \ldots, r\}\} < \text{máx}\{\dim(V_i) : i \in \{1, \ldots, s\}\} = \dim(V(F)) = 1$. Aclaramos que $W_1, \ldots, W_r$ son las componentes irreducibles de W y $V_1, \ldots, V_s$ son las de $V(F)$. Consecuentemente, $\dim(W) = 0$. Es un ejercicio muy sencillo el ver que un conjunto algebraico de $\mathbb{A}^n(K)$ de dimensión 0 es siempre un conjunto finito [4]. □

Observación 2.42. Realicemos dos consideraciones interesantes:

I.) Por el *Teorema de los ceros fuerte* (*Teorema* 1.17), si $V(F)$ y $V(G)$ son dos curvas algebraicas planas afines idénticas (como conjuntos algebraicos), entonces $\text{rad}(F) = \text{rad}(G)$. Esto asegura la existencia de dos polinomios $H, H' \in K[X,Y]$ tales que $F^p = GH$ y $G^q = FH'$, para ciertos $p, q \in \mathbb{N}$.

II.) Supongamos que la factorización única de F en producto de irreducibles viene dada por

$$F = F_1^{m_1} \cdots F_r^{m_r}, \text{ con } F_i \text{ irreducible } \forall\, i \in \{1, \ldots, r\}.$$

En tal caso, $V(F) = V(F_1^{m_1} \cdots F_r^{m_r}) = V(F_1 \cdots F_r)$. Por tanto, las curvas planas se supondrán definidas por *polinomios reducidos* (i.e., sin factores irreducibles repetidos), a no ser que se especifique lo contrario para ciertos estudios específicos.

Proposición 2.43. *Si F y G son dos polinomios reducidos que inducen la misma curva plana, entonces F y G son necesariamente asociados. Equivalentemente, $\langle F \rangle = \langle G \rangle$.*

Demostración. Tomemos $H, H' \in K[X,Y]$ como en la *Observación* 2.42. Realizando un simple proceso de expansión, tenemos las siguientes dos factorizaciones de F^p en producto de elementos irreducibles:

- $F^p = (F_1 \cdots F_r)^p = F_1^p \cdots F_r^p$.
- $F^p = GH = (G_1 \cdots G_s)(H_1 \cdots H_t)$.

[4]Sea W un cerrado del espacio afín tal que $\dim(W) = 0$. Tomemos $W = W_1 \cup \cdots \cup W_r$ su descomposición en componentes irreducibles. Como $0 = \dim(W) = \text{máx}\{\dim(W_i) : i \in \{1, \ldots, r\}\}$, entonces $\dim(W_i) = 0, \forall\, i \in \{1, \ldots, r\}$. Por ello, cada W_i es un punto del espacio afín y W será en consecuencia un conjunto finito.

Como $K[X,Y]$ es un *DFU*, cada G_j está asociado con algún F_j para todo $j \in \{1,\dots,s\}$. Procediendo de forma totalmente análoga con $G^q = FH'$, vemos que cada F_i está asociado con algún G_i para todo $i \in \{1,\dots,r\}$. Como F y G se suponen reducidos, esto implica que $r = s$ y que F y G se diferencian en el producto por una unidad del anillo de polinomios (elemento de $K^* = K \setminus \{0\}$). Concluimos que $F = \lambda G$, para cierto $\lambda \in K^*$. Una demostración alternativa consiste en justificar debidamente que $\langle F\rangle$ y $\langle G\rangle$ son ideales radicales, luego $V(F) = V(G) \Longrightarrow I(V(F)) = I(V(G)) \Longrightarrow \langle F\rangle = \langle G\rangle$. □

Observación 2.44. El resultado anterior nos proporciona una condición necesaria y suficiente para saber cuándo dos curvas algebraicas planas afines coinciden a nivel de conjuntos, porque siempre podemos tomar un polinomio reducido que defina a cada una (*Observación* 2.42). En determinadas situaciones nos interesará especificar quién es dicho polinomio, e incluso será necesario permitir que este tenga factores repetidos para ciertos propósitos. Podríamos dar una definición alternativa de curva apoyándonos en el concepto de *polinomios equivalentes*.

Definición 2.45. Sean $F, G \in K[X,Y]$ polinomios en dos variables. Diremos que son *equivalentes* si $\exists\ \lambda \in K^*$ tal que $F = \lambda G$. Consideremos F fijado. A partir de ahora, diremos que la *curva algebraica plana afín* definida por F es el conjunto algebraico de la forma

$$C := V(G), \text{ para cualquier } G \in K[X,Y] \text{ tal que } G \text{ es equivalente con } F.$$

Esta nueva formulación implica que las curvas algebraicas pueden identificarse con clases de polinomios en dos variables según la relación de *ser equivalentes*. De hecho, es bastante común pensar en una curva algebraica como el par $C = (V(F), F)$, donde $F \in K[X,Y]$ viene determinado salvo constantes. Nos referiremos a C denotándola por $V(F)$ ó simplemente F. Ante una expresión polinómica explícita, por ejemplo $F = Y - X^2$, hablamos de la *curva plana* $Y - X^2$ ó, usando otro lenguaje, de la *curva plana* $Y = X^2$.

Definición 2.46. Se define el grado de $C = V(F)$ como el valor natural

$$d := \mathrm{dg}(F) = \text{máx}\{i + j : a_{ij} \neq 0, F(X,Y) = \sum_{i,j} a_{ij} X^i Y^j\}.$$

Observación 2.47. Una curva de grado 1 es lo que establecimos anteriormente como *recta*. Son siempre curvas de la forma $R = V(F)$, con $F = aX + bY + c$ para ciertos $a, b, c \in K$ verificando que $a \neq 0$ ó $b \neq 0$.

Observación 2.48. Si $F \in K[X,Y]$ es irreducible, entonces $C = V(F)$ es una variedad afín. Pondremos $\mathrm{A}(F)$, $\mathrm{K}(F)$ y $\mathcal{O}_P(F)$ para referirnos al anillo de coordenadas de C, al cuerpo de funciones racionales en C y al anillo local de C en un punto $P \in V(F)$ respectivamente.

Capítulo 3

Singularidades y propiedades locales de las curvas planas.

3.1. Puntos singulares y rectas tangentes.

Definición 3.1. Sea $C = V(F)$ una curva algebraica plana afín, con $F \in K[X,Y]$. Un punto $P = (a,b) \in C$ se dice *punto singular* de la curva si se cumplen dos condiciones, siendo $\dfrac{\partial F}{\partial X}(\cdot)$ y $\dfrac{\partial F}{\partial Y}(\cdot)$ las derivadas parciales de F respecto a sendas variables:

I.) $\dfrac{\partial F}{\partial X}(P) = 0.$

II.) $\dfrac{\partial F}{\partial Y}(P) = 0.$

Si P no verifica I.) y II.) al mismo tiempo, se dirá que P es un *punto simple* de la curva C ó un *punto no singular*. La curva será *no singular* si todos sus puntos son simples (equivalentemente, si C no tiene puntos singulares).

Definición 3.2. Sea $P = (a,b)$ un punto de una curva $C = V(F)$. Llamamos *espacio tangente* a C en el punto P al conjunto algebraico definido por

$$\frac{\partial F}{\partial X}(P)(X-a) + \frac{\partial F}{\partial Y}(P)(Y-b) = 0.$$

Lo denotamos por $T_P F$. Si P es un punto simple, entonces $T_P F$ es una recta y se llamará *recta tangente* a $C = V(F)$ en P (dimensión 1). En otro caso, si P es singular, entonces $T_P F$ es el plano afín (dimensión 2) y todas las rectas se dicen tangentes a C en P.

Ejemplo 3.3. Para poder dibujar algunos ejemplos de curvas, solemos tomar $K = \mathbb{C}$. Dada $C = V(F)$, lo que podemos representar gráficamente es su proyección real, es decir, $V(F) \cap \mathbb{A}^2(\mathbb{R})$.

Es importante señalar que los retratos *bidimensionales* que realizamos no reflejan fielmente la forma de la curva, ni mucho menos todas sus singularidades. Sin embargo, en ocasiones estas gráficas sí muestran cierta información interesante, pues permiten identificar puntos singulares reales y esbozar parte del espacio tangente a la curva en dichos puntos. Añadimos dos de las más famosas (recomendamos consultar los conceptos que suceden a las figuras y, en particular, la *Definición* 3.12).

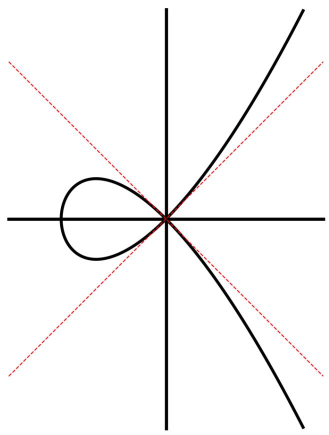

Figura 3.1: Ejemplo de una *curva nodal*, con la expresión $Y^2 - X^3 - X^2 = 0$. Posee una singularidad ordinaria en el origen.

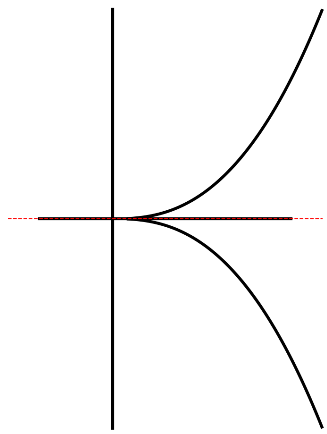

Figura 3.2: Ejemplo de una *cúspide*, con forma implícita dada por $Y^2 - X^5 = 0$. Tiene un punto doble en el (0,0).

Definición 3.4. Un polinomio $F \in K[X_1, \dots, X_n]$ es *homogéneo* de grado $d \in \mathbb{N}$ si todos los monomios de F tienen grado d:

$$F(X_1, \dots, X_n) = \sum_{i_1 + \cdots + i_n = d} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

Equivalentemente, si

$$F(\lambda X_1, \dots, \lambda X_n) = \lambda^d F(X_1, \dots, X_n), \forall \ \lambda \in K.$$

Por convenio, asumiremos que el polinomio 0 es homogéneo de cualquier grado.

Observación 3.5. Es un ejercicio sencillo el comprobar que todo elemento $F \in K[X_1, \dots, X_n]$ admite una expresión única del estilo $F = F_0 + F_1 + \cdots + F_d$, donde cada F_i es un polinomio homogéneo de grado i (pudiendo ser $F_i = 0$). Si $F_d \neq 0$, entonces $\mathrm{dg}(F) = d$.

Lema 3.6. *Sea $F(X,Y) \in K[X,Y]$ homogéneo de grado $d \geq 1$. Entonces,*

$$F(X,Y) = \prod_{i=1}^{d} (\alpha_i X + \beta_i Y), \ \textit{para ciertos } \alpha_i, \beta_i \in K.$$

Es decir, todo polinomio homogéneo en dos variables de grado mayor que cero (no constante) se factoriza de forma única en producto de rectas según la expresión anterior (porque $K[X, Y]$ es DFU).

Demostración. Sea $F(X, Y) = \sum_{i+j=d} a_{i,j} X^i Y^j = \sum_{i=0}^{d} a_{i,d-i} X^i Y^{d-i} = Y^d \sum_{i=0}^{d} a_{i,d-i} \left(\frac{X}{Y}\right)^i$, donde los $a_{i,d-i}$ no son todos nulos. Pongamos $e := \max\{0 \leq i \leq d : a_{i,d-i} \neq 0\}$. Se sigue que

$$\sum_{i=0}^{d} a_{i,d-i} \left(\frac{X}{Y}\right)^i = \sum_{i=0}^{e} a_{i,d-i} \left(\frac{X}{Y}\right)^i = a_{e,d-e} \prod_{i=1}^{e} \left(\frac{X}{Y} - \xi_i\right).$$

La última igualdad es consecuencia de que K es algebraicamente cerrado, luego el polinomio $G(Z) = \sum_{i=0}^{e} a_{i,d-i} Z^i \in K[Z]$ escinde en K. Sus raíces son $\xi_1, \ldots, \xi_e$. Por tanto,

$$F(X, Y) = Y^d a_{e,d-e} \prod_{i=1}^{e} \left(\frac{X}{Y} - \xi_i\right) = a_{e,d-e} Y^{d-e} \prod_{i=1}^{e} (X - Y\xi_i) = \prod_{i=1}^{d} (\alpha_i X + \beta_i Y)$$

para unas elecciones evidentes de los α_i y β_i. $\square$

Definición 3.7. Sea $F \in K[X, Y]$. La *multiplicidad* de la curva $C = V(F)$ en un punto $P = (a, b) \in V(F)$ se define como el menor $m > 0, m \in \mathbb{Z}$ tal que

$$\frac{\partial^m F}{\partial X^i \partial Y^j}(a, b) \neq 0,$$

para algunos $i, j \geq 0$ verificando que $i + j = m$. Cuando $P = (0, 0)$, podemos dar una formulación equivalente como sigue. Si suponemos que

$$F = F_0 + F_1 + \cdots + F_d = F_m + F_{m+1} + \cdots + F_d$$

es la descomposición de F en suma de polinomios homogéneos explicada en la *Observación* 3.5, con m el menor entero positivo tal que $F_m \neq 0$, entonces $m = \mathrm{dg}(F_m)$ es la *multiplicidad* de $C = V(F)$ en el origen. En un caso general, también se dice que el punto $P \in C$ *tiene multiplicidad* m y se usa la notación $m_P(F) = m$ para referirnos a ella.

Observación 3.8. Si $P = (a, b)$ es un punto de multiplicidad $m > 0$ de $C = V(F)$, el polinomio

$$G_P^F(X, Y) := \sum_{i+j=m} \frac{\partial^m F}{\partial X^i \partial Y^j}(a, b) \cdot \frac{(X - a)^i (Y - b)^j}{i!\ j!}$$

es homogéneo de grado m en las variables $\widetilde{X} = X - a$, $\widetilde{Y} = Y - b$. Por el *Lema* 3.6, es un producto de rectas del estilo:

$$G_P^F(X, Y) = \prod_{i=1}^{m} (\alpha_i (X - a) + \beta_i (Y - b)).$$

El siguiente es un resultado que se supone conocido por el lector y cuya demostración se explica en cursos básicos de análisis matemático. Puede llevarse a cabo a nivel algebraico aplicando nociones básicas de derivación. Se obtendría la prueba primero para monomios y, a continuación, para un caso general.

Teorema 3.9. *Sea $F \in K[X,Y]$ un polinomio en dos variables. Entonces, F admite un desarrollo en Serie de Taylor finita en cualquier punto $(a,b) \in \mathbb{A}^2(K)$:*

$$F(X,Y) = \sum_{i,j\geq 0} \frac{\partial^{i+j} F}{\partial X^i \partial Y^j}(a,b) \cdot \frac{(X-a)^i (Y-b)^j}{i!\ j!}.$$

Definición 3.10. Combinando el *Teorema* previo con la *Observación* 3.5 es fácil ver que, en las condiciones de la *Observación* 3.8 para $P = (0,0)$, el polinomio G_P^F coincide exactamente con F_m (de la descomposición en suma de términos homogéneos de F). Llamamos *cono tangente geométrico* a $C = V(F)$ en $P = (0,0)$ al conjunto algebraico $V(F_m)$. Las curvas $\alpha_i(X-a) + \beta_i(Y-b) = 0$ con $i \in \{1,\ldots,m\}$ son las *rectas del cono tangente* a la curva $C = V(F)$ en el punto $P = (a,b)$, y son precisamente las componentes irreducibles de $V(F_m)$. El *cono tangente*, por otro lado, será el par $\left(V(F_m), \dfrac{K[X,Y]}{\langle F_m \rangle}\right)$.

Observación 3.11. Un punto P de una curva $C = V(F)$ es simple si, y sólo si, la multiplicidad de C en P es uno. En tal caso, la recta del cono tangente a C en P es precisamente la planteada en la *Definición* 3.2. Cuando $P = (0,0)$, coincide también con el término homogéneo F_1.

Definición 3.12. Un punto singular $P = (a,b) \in C = V(F)$ se dice *punto doble* (respectivamente *punto triple*, *punto cuádruple*...) si su multiplicidad es dos (respecticamente tres, cuatro...). Un punto singular P de C se denomina *singularidad ordinaria* si las rectas del cono tangente a C en P son todas distintas (i.e., el polinomio de la *Observación* 3.8 es reducido). Llamamos *nodo* de una curva $C = V(F)$ a cualquier singularidad ordinaria de C de multiplicidad dos.

Proposición 3.13. *Sea $F \in K[X,Y]$. Supongamos que la factorización única en producto de irreducibles de F viene dada por*

$$F = F_1^{e_1} \cdots F_r^{e_r}, \text{ con } F_i \text{ irreducible } \forall\, i \in \{1,\ldots,m\}.$$

Consideremos $P = (0,0) \in C = V(F)$. En tal caso, $m_P(F) = \sum_{i=1}^r e_i m_P(F_i)$, donde se establece el convenio de que $m_P(F_i) = 0$ si $P \notin V(F_i)$.

Demostración. Pongamos $F = F_m + F_{m+1} + \cdots + F_d$ la descomposición de F en suma de términos homogéneos tal que $F_m \neq 0$. Sabemos que $m_P(F) = m$. Análogamente, asumiremos que las descomposiciones de las componentes irreducibles de F son:

$$F_i = F_{m_i} + F_{m_i+1} + \cdots + F_{d_i}, \text{ con } F_{m_i} \neq 0 \text{ y } m_P(F_i) = m_i, \forall\, i \in \{1,\ldots,r\}.$$

Basta con demostrar que $F_m = \prod_{i=1}^r F_{m_i}^{e_i}$, pero esto es inmediato teniendo en cuenta que el producto de polinomios homogéneos es homogéneo. De este modo, $\prod_{i=1}^r F_{m_i}^{e_i}$ es el sumando de menor grado que aparece en F al multiplicar las descomposiciones precedentes y, por unicidad, debe coincidir con F_m. □

Corolario 3.14. *En las condiciones anteriores, $P = (0,0)$ es un punto simple de $C = V(F)$ si, y sólo si, P pertenece a una única componente irreducible, $V(F_i)$, de $V(F)$ que tiene multiplicidad uno en P y tal que dicha componente es simple (en el sentido de que $e_i = 1$).*

Demostración. Se sigue de manera inmediata de la fórmula $m_P(F) = \sum_{i=1}^r e_i m_P(F_i)$ dada por la *Proposición* anterior. □

Observación 3.15. Podríamos haber dado sólamente las definiciones anteriores para el $(0,0)$, apoyándonos en la expresión en suma de polinomios homogéneos de la *Observación* 3.5 y sin usar el cálculo diferencial en absoluto. Sería posible realizar un proceso de generalización a un punto $P = (a,b) \neq (0,0)$ arbitrario del siguiente modo (recomendamos consultar la teoría relativa a la sección 2.4). Sea $C = V(F)$ con $P \in C$. Primero, tomemos T el cambio de coordenadas afín en $\mathbb{A}^2(K)$ que lleva el origen en P, es decir, $T(X,Y) = (X+a, Y+b)$. Consideremos $F^T(X,Y) := F(T_1,T_2) = F(X+a,Y+b)$ y podemos definir $m_P(F)$ como $m_{(0,0)}(F^T)$. Lo que hacemos es escribir la descomposición de F^T en suma de términos homogéneos

$$F^T = G_m + G_{m+1} + \cdots + G_d, \text{ con } G_m \neq 0,$$

para establecer $m_P(F) := m$. Si $G_m = \prod_{i=1}^m (\alpha_i X + \beta_i Y)$ es la factorización de G_m según el *Lema* 3.6, entonces diremos que las curvas $\alpha_i(X-a) + \beta_i(Y-b) = 0$ son las rectas del cono tangente a $C = V(F)$ en el punto $P = (a,b)$. Es inmediato comprobar que esta nueva forma de definir los conceptos anteriores es equivalente a la que veníamos usando hasta ahora (puede pensarse simplemente como un razonamiento por cambio de variable). Lo interesante es que T lleva los puntos de $V(F^T)$ en puntos de $C = V(F)$ y *traslada* las rectas tangentes a $V(F^T)$ en el origen a las rectas del cono tangente a $C = V(F)$ en $P = (a,b)$ [*Fulton*, pp. 32–33].

3.2. Localización y cambios de coordenadas.

El *Teorema* 3.27 será el resultado principal de este capítulo. Para poder esbozar una prueba del mismo, será necesario introducir primero unos resultados auxiliares relativos a los cambios de coordenadas afines en el plano y a la sección 2.5.

Lema 3.16. *Sean $P, P' \in \mathbb{A}^2(K)$, L_1, L_2 dos rectas distintas pasando por P y L_1', L_2' dos rectas distintas pasando por P'. Es posible tomar un cambio de coordenadas afín T en $\mathbb{A}^2(K)$ tal que $T(P) = P'$ y $T(L_i) = L_i'$, para $i = 1, 2$.*

Demostración. Hemos visto que todo cambio de coordenadas afín, T, es la composición de una aplicación K-lineal con una traslación. Supongamos $T = (T_1, T_2)$, con $T_1 = \alpha_1 X + \beta_1 Y + \gamma_1$ y $T_2 = \alpha_2 X + \beta_2 Y + \gamma_2$. En tal caso, podemos representar matricialmente a T según

$$T(X,Y) = \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix}.$$

Supongamos $P = (a,b), P' = (a', b')$. Definimos la traslación que lleva P en el origen $\varphi(X,Y) = (X - a, Y - b)$. Hacemos lo propio para P', con $\psi(X,Y) = (X - a', Y - b')$. Consideramos también la aplicación K-lineal, A, que lleva las direcciones de L_1 y L_2 en las de L'_1 y L'_2. Como las rectas son distintas por pares, sus vectores directores serán linealmente independientes. Sabemos que A queda totalmente determinada dando la imagen de una base de $\mathbb{A}^2(K)$, justo como acabamos de hacer. Tanto φ y ψ como A son cambios de coordenadas afines, luego la composición $T = \psi^{-1} \circ A \circ \varphi$ también lo es y cumple las condiciones del enunciado. $\square$

Proposición 3.17. *Sea $T : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^n(K)$ un cambio de coordenadas tal que $T(P) = Q$ para cierto par de puntos del espacio afín. Entonces, se verifica que la extensión evidente de $T^* : \mathrm{A}(\mathbb{A}^n(K)) \longrightarrow \mathrm{A}(\mathbb{A}^n(K))$ a $T^* : \mathcal{O}_Q(\mathbb{A}^n(K)) \longrightarrow \mathcal{O}_P(\mathbb{A}^n(K))$ es un isomorfismo entre los respectivos anillos locales.*

Demostración. Primero, veamos que si $\varphi : V \longrightarrow W$ es una aplicación polinómica entre variedades afines y $P \in V$ es tal que $\varphi(P) = Q$, entonces $\varphi^* : \mathrm{A}(W) \longrightarrow \mathrm{A}(V)$ se extiende de forma única a un homomorfismo (que también denotaremos por φ^*) de $\mathcal{O}_Q(W)$ a $\mathcal{O}_P(V)$. Ponemos

$$\varphi^* : \mathcal{O}_Q(W) \longrightarrow \mathcal{O}_P(V); g = \frac{a}{b} \mapsto \varphi^*(g) := \frac{a \circ \varphi}{b \circ \varphi}.$$

El razonamiento para ver que esta aplicación está bien definida es análogo al hecho para el valor $g(Q)$ (*Observación* 2.23), teniendo en cuenta que $b \circ \varphi \in \mathrm{A}(V)$ es tal que $(b \circ \varphi)(P) = b(Q) \neq 0$. φ^* es claramente un homomorfismo de K-álgebras que se restringe acorde con el enunciado al correspondiente homomorfismo entre los anillos de coordenadas. Para la unicidad, tomemos ψ otro homomorfismo que extiende a φ^*. En tal caso, $\psi\left(\frac{a}{1}\right) = \varphi^*(a) = a \circ \varphi$, para cada $a \in \mathrm{A}(W)$. Por otro lado, $\psi\left(\frac{1}{b}\right) = \psi\left(\left(\frac{b}{1}\right)^{-1}\right) = \left(\psi\left(\frac{b}{1}\right)\right)^{-1} = \frac{1}{b \circ \varphi}$, para cualquier $b \in \mathrm{A}(W)$ con $b(Q) \neq 0$. Es por ello que $\psi\left(\frac{a}{b}\right) = \psi\left(\frac{a}{1}\right) \cdot \psi\left(\frac{1}{b}\right) = \frac{a \circ \varphi}{b \circ \varphi} = \varphi^*\left(\frac{a}{b}\right)$.

Supongamos que $\varphi : V \longrightarrow W$ es un isomorfismo. Sabemos que φ^* será un isomorfismo de K-algebras entre los anillos de coordenadas $\mathrm{A}(W)$ y $\mathrm{A}(V)$. Es inmediato comprobar lo propio para su extensión de $\mathcal{O}_Q(W)$ a $\mathcal{O}_P(V)$. $\square$

Lema 3.18. *Sean $P = (0, \ldots, 0) \in \mathbb{A}^n(K)$, $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^n(K))$, $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n(K))$ e $I = \langle X_1, \ldots, X_n \rangle \subset K[X_1, \ldots, X_n]$. Entonces $I\mathcal{O} = I^e = \mathfrak{m}$, donde I^e denota la extensión del ideal I a través de la inclusión de $\mathrm{A}(\mathbb{A}^n(K)) = K[X_1, \ldots, X_n]$ en $\mathcal{O}$.*

Demostración. La prueba se basará en el resultado visto en el *Ejemplo* 1.13 que aseguraba la maximalidad de $I = \langle X_1, \dots, X_n \rangle$. Además, en su momento también demostramos que $I(P) = \langle X_1, \dots, X_n \rangle \Longrightarrow P = V(\langle X_1, \dots, X_n \rangle)$. Notemos que $I\mathcal{O} = \{\sum_i F_i h_i : F_i \in I, h_i \in \mathcal{O}\} = \left\{\frac{F}{G} \in \mathcal{O} : F \in I\right\}$, donde las sumas anteriores son todas finitas. Recordemos que

$$\mathfrak{m} = \{f \in \mathcal{O} : f(P) = 0\}.$$

Se obtiene inmediatamente la inclusión $I\mathcal{O} \subset \mathfrak{m}$. En efecto, tomemos $\frac{F}{G} \in I\mathcal{O}$. Si $G \mid F$, ponemos $F = GH$, para cierto $H \in K[X_1, \dots, X_n]$. Como I es primo (por ser maximal) y $F \in I$, necesariamente $H \in I \Longrightarrow \frac{F}{G} = \frac{H}{1} \in \mathfrak{m}$. Esto se debe a que $G(P) \neq 0$, luego $G \notin I$. Si $G \nmid F$, ya estaría. Para la inclusión hacia la izquierda, sea $\frac{F}{G} \in \mathfrak{m}$. Entonces, $F(P) = 0 \Longrightarrow F \in I$. $\square$

Observación 3.19. Sean $\mathfrak{a}, \mathfrak{b}$ dos ideales de un anillo A arbitrario y $f : A \longrightarrow B$ un homomorfismo de anillos. Es sencillo verificar que $(\mathfrak{a}\mathfrak{b})^e = \mathfrak{a}^e \mathfrak{b}^e$. En las condiciones del *Lema* anterior, se llegaría a que $I^r\mathcal{O} = \mathfrak{m}^r, \forall\, r \in \mathbb{N}$.

Teorema 3.20. *Sean V una variedad afín de $\mathbb{A}^n(K)$, $\mathfrak{a} = I(V) \subset K[X_1, \dots, X_n]$, $P \in V$ y $J \subset K[X_1, \dots, X_n]$ un ideal del anillo de polinomios tal que $J \supset \mathfrak{a}$. Sea J' la imagen de J en* $\mathrm{A}(V)$. *Entonces, existe un homomorfismo natural*

$$\begin{array}{ccc} \dfrac{\mathcal{O}_P(\mathbb{A}^n(K))}{J\mathcal{O}_P(\mathbb{A}^n(K))} & \xrightarrow{\qquad \varphi \qquad} & \dfrac{\mathcal{O}_P(V)}{J'\mathcal{O}_P(V)} \\ [f]_{J^e} = \left[\dfrac{F_1}{F_2}\right]_{J^e} & \longmapsto & \varphi([f]_{J^e}) := \left[\dfrac{f_1}{f_2}\right]_{J'^e} \end{array}$$

donde f_1 y f_2 denotan las clases residuales de F_1 y F_2 en $\mathrm{A}(V)$, *respectivamente. Además, φ es un isomorfismo.*

Demostración. Sea $\pi : K[X_1, \dots, X_n] \longrightarrow \frac{K[X_1, \dots, X_n]}{\mathfrak{a}}$ el homomorfismo canónico de paso al cociente. Hemos establecido J' como el ideal $\pi(J)$ de $\mathrm{A}(V)$. Vamos a ver que φ está bien definida. Sean $f = \frac{F_1}{F_2}, g = \frac{G_1}{G_2} \in \mathcal{O}_P(\mathbb{A}^n(K))$ tales que $[f]_{J^e} = [g]_{J^e}$. Obviamente, $0 = \left[\frac{F_1}{F_2} - \frac{G_1}{G_2}\right]_{J^e} = \left[\frac{F_1G_2 - G_1F_2}{F_2G_2}\right]_{J^e} \Longrightarrow \frac{F_1G_2 - G_1F_2}{F_2G_2} \in J^e$. Es posible, pues, tomar un par de polinomios tales que $H_1 \in J$ y $H_2(P) \neq 0$ con

$$\frac{F_1G_2 - G_1F_2}{F_2G_2} = \frac{H_1}{H_2} \in \mathcal{O}_P(\mathbb{A}^n(K)) \subset K(X_1, \dots, X_n).$$

Como $K[X_1, \dots, X_n]$ es un dominio, esto se traduce en que $H_2(F_1G_2 - G_1F_2) - H_1(F_2G_2) = 0$. Quedándonos con los residuos sobre el anillo de coordenadas de V de la expresión anterior (i.e., tomamos las restricciones de las funciones regulares inducidas por los polinomios anteriores al conjunto V), obtenemos que $h_2(f_1g_2 - g_1f_2) - h_1(f_2g_2) = 0$. Es decir,

$$\frac{f_1g_2 - g_1f_2}{f_2g_2} = \frac{h_1}{h_2} \in \mathcal{O}_P(V) \subset \mathrm{K}(V).$$

Dado que $h_2(P) \neq 0$ y $h_1 \in J'$, entonces $\dfrac{h_1}{h_2} \in J'\mathcal{O}_P(V) \Longrightarrow \left[\dfrac{f_1}{f_2}\right]_{J'^e} = \left[\dfrac{g_1}{g_2}\right]_{J'^e}$. Es un ejercicio muy sencillo el comprobar que φ es un homomorfismo de K-álgebras. La sobreyectividad es evidente. Para la inyectividad, sea $f = \dfrac{F_1}{F_2} \in \mathcal{O}_P(\mathbb{A}^n(K))$ tal que $\left[\dfrac{f_1}{f_2}\right]_{J'^e} = 0$. Como $\mathrm{A}(V)$ es un dominio por ser V una variedad afín, se sigue que exiten $l_1, l_2 \in \mathrm{A}(V)$ tales que $l_1 \in J'$ y $l_2(P) \neq 0$ con

$$\frac{f_1}{f_2} = \frac{l_1}{l_2} \Longrightarrow f_1l_2 - l_1f_2 = 0 \in \mathrm{A}(V).$$

De esta forma, tomando representantes según la notación ya especificada y señalando que $L_1 \in J$, llegamos a que

$$\overline{F_1} \cdot \overline{L_2} - \overline{L_1} \cdot \overline{F_2} = 0 \Longrightarrow F_1L_2 - L_1F_2 \in \mathfrak{a} \subset J \subset \mathrm{A}(\mathbb{A}^n(K)).$$

Concluimos, considerando los residuos módulo J^e, que $[F_1]_{J^e}[L_2]_{J^e} - [L_1]_{J^e}[F_2]_{J^e} = 0 \Longrightarrow [F_1]_{J^e}[L_2]_{J^e} = 0$. Puesto que $L_2(P) \neq 0$, $L_2 \notin \mathfrak{m}_P(V)$, siendo este último el ideal maximal de V en P. Ya vimos en su momento que $\mathcal{O}_P(V)$ es anillo local con único maximal $\mathfrak{m}_P(V)$, por lo que L_2 es una unidad de $\mathcal{O}_P(V)$. Si $[L_2]_{J^e} = 0$, entonces $J\mathcal{O}_P(\mathbb{A}^n(K)) = \mathcal{O}_P(\mathbb{A}^n(K))$ y estaríamos en un caso trivial. Si no fuese así, entonces $[L_2]_{J^e}$ es una unidad del anillo cociente y podemos despejar, deduciendo que $[F_1]_{J^e} = 0$. □

Corolario 3.21. *En las condiciones del resultado anterior, con $\mathfrak{a} = I(V)$, se obtiene la siguiente relación de isomorfía:*

$$\frac{\mathcal{O}_P(\mathbb{A}^n(K))}{\mathfrak{a}\mathcal{O}_P(\mathbb{A}^n(K))} \cong \mathcal{O}_P(V).$$

Demostración. Basta con tomar $J = \mathfrak{a}$ y aplicar el *Teorema* 3.20. □

3.3. Multiplicidades y anillos locales.

En toda la sección, $C = V(F)$ se considerará una curva algebraica plana afín, con $F \in K[X,Y]$ irreducible. Nuestro objetivo será hallar la multiplicidad de un punto $P \in C$ en términos de su anillo local $\mathcal{O}_P(F)$. Para un polinomio $G \in K[X,Y]$, usaremos la notación

$$g := \overline{G} \in \mathrm{A}(F) = \frac{K[X,Y]}{\langle F \rangle}.$$

Definición 3.22. Un *anillo de valoración discreta* (AVD) es un dominio de ideales principales que cuenta con un único ideal primo no nulo, usualmente denotado por $\mathfrak{m}$.

Lema 3.23. *Se verifican las siguientes dos afirmaciones para A un AVD:*

I.) A es un anillo local cuyo único ideal maximal es $\mathfrak{m}$.

II.) $\mathfrak{m} = \langle \pi \rangle$, para cierto elemento irreducible $\pi \in A$.

Demostración. Para ver el primer enunciado, supongamos $\mathfrak{m}$ el único ideal primo no nulo del *DIP*. Un resultado elemental de álgebra conmutativa afirma que debe existir un ideal maximal no nulo, $\mathfrak{n} \subset A$, que contiene a $\mathfrak{m}$. Como $\mathfrak{n}$ es maximal, también es primo, luego $\mathfrak{m} = \mathfrak{n}$. El segundo apartado es consecuencia de que todo elemento primo no nulo de un dominio es irreducible y de que A es *DIP*. □

Definición 3.24. A un elemento irreducible, $\pi \in A$, tal que $\mathfrak{m} = \langle \pi \rangle$ se lo denomina *parámetro uniformizante* del anillo A. Como todos los uniformizantes son asociados, se dice que este es único salvo unidades.

Observación 3.25. Todo elemento no nulo de un anillo de valoración discreta, A, es de la forma $u\pi^n$ para cierta elección de $n \in \mathbb{N}$ y $u \in A^*$, siendo π el uniformizante de A. Esto se debe a que A es un DFU y el uniformizante (único salvo unidades) es el único elemento irreducible de A. Ciertamente, si $\alpha \in A$ es irreducible entonces $\langle \alpha \rangle$ es un ideal primo no nulo de A, luego coincide necesariamente con $\langle \pi \rangle$.

Proposición 3.26. *Sea A un anillo. Equivalen:*

I.) A es un AVD.

II.) A es un dominio local noetheriano cuyo ideal maximal está generado por un elemento no nulo.

Omitimos la prueba, que puede encontrarse en la bibliografía [*Fulton*, *Proposición* 4 de § 2.5].

Teorema 3.27. *Un punto $P \in C = V(F)$ es simple (no singular) si, y sólo si, $\mathcal{O}_P(F)$ es un AVD. En tal caso, si $L = aX + bY + c$ es una recta que pasa por P sin ser tangente a $C = V(F)$ en P, entonces la imagen l de L en $\mathcal{O}_P(F)$ es un parámetro uniformizante para $\mathcal{O}_P(F)$.*

Demostración. Veamos la necesidad y la condición sobre el uniformizante. Sea P un punto simple de $C = V(F)$ y L una recta que pasa por P, sin ser tangente a C en dicho punto. Realizando un cambio de coordenadas afín, podemos suponer que Y es la recta tangente a la curva en el origen, $L = X$ y $P = (0,0)$. En efecto, basta con aplicar el *Lema* 3.16 y la *Proposición* 3.17. Por otro lado, la *Observación* 2.25 y la *Proposición* 2.26 garantizan que $\mathcal{O}_P(F)$ es un dominio local noetheriano, por lo que llega con demostrar que $\mathfrak{m}_P(F) = \langle x\rangle\mathcal{O}_P(F)$. Señalamos, una vez más, que usaremos la notación $\langle x\rangle\mathcal{O}_P(F)$ para referirnos a $\langle x\rangle^e$.

Comprobemos en primer lugar que $\mathfrak{m}_P(F) = \langle x, y\rangle\mathcal{O}_P(F)$ (igualdad que se cumple independientemente de la multiplicidad de la curva en $P = (0,0)$). Para verlo, tomemos la isomorfía establecida en el *Corolario* 3.21:

$$\frac{\mathcal{O}_P(\mathbb{A}^2(K))}{\langle F\rangle\mathcal{O}_P(\mathbb{A}^2(K))} \cong \mathcal{O}_P(F).$$

Por el *Lema* 3.18, sabemos que $\mathfrak{m}_P(\mathbb{A}^2(K)) = \langle X, Y\rangle\mathcal{O}_P(\mathbb{A}^2(K))$. Como $\mathcal{O}_P(\mathbb{A}^2(K))$ es un anillo local, $\langle [X]_{\langle F\rangle^e}, [Y]_{\langle F\rangle^e}\rangle$ es el único ideal maximal del anillo cociente. Esto es, $\langle x, y\rangle\mathcal{O}_P(F)$ es el único maximal de $\mathcal{O}_P(F)$, luego coincide con $\mathfrak{m}_P(F)$. Recordemos que la expresión de la recta tangente a F en el origen viene dada por

$$\frac{\partial F}{\partial X}(0,0)X + \frac{\partial F}{\partial Y}(0,0)Y = Y \Longrightarrow \frac{\partial F}{\partial Y}(0,0) = 1 \overset{\text{Taylor}}{\Longrightarrow} F = Y + \text{ términos de mayor grado.}$$

Como la parcial respecto a X de F se anula en el origen, agrupando los monomios con Y podemos escribir $F = YG - X^2H$, con $H \in K[X]$ y $G = 1+$ términos de mayor grado $\in K[X, Y]$. Tomando clases, llegamos a la siguiente igualdad en el anillo de coordenadas de F:

$$yg = x^2h \in \mathrm{A}(F).$$

Teniendo en cuenta que $g(P) = 1$, esto nos dice que g es una unidad de $\mathcal{O}_P(F)$. Despejamos de la forma $y = x^2hg^{-1} \in \langle g^{-1}x^2h\rangle = \langle x^2h\rangle\mathcal{O}_P(F) \subset \langle x\rangle\mathcal{O}_P(F) \Longrightarrow \mathfrak{m}_P(F) = \langle x, y\rangle\mathcal{O}_P(F) = \langle x\rangle\mathcal{O}_P(F)$.

Para el recíproco, supongamos $\mathcal{O}_P(F)$ un *AVD*, $\mathfrak{m}_P(F) = \langle a\rangle$ con $a \neq 0$ y sea $n \in \mathbb{N}$. Teniendo en cuenta que $\dfrac{\mathcal{O}_P(F)}{\mathfrak{m}_P(F)} \cong K$, concluimos usando el *Teorema* 3.29 (lo veremos a continuación):

$$\dim_K \frac{\mathfrak{m}_P(F)^n}{\mathfrak{m}_P(F)^{n+1}} = \frac{\langle a\rangle^n}{\langle a\rangle^{n+1}} = 1 \Longrightarrow m_P(F) = 1 \Longrightarrow P \text{ es no singular.}$$

□

Observación 3.28. Vamos a dar una segunda interpretación del anillo local de $C = V(F)$ en el punto P. Consideremos el ideal maximal $\langle X, Y\rangle \subset K[X, Y]$. Se sigue que $\mathfrak{m} := \pi(\langle X, Y\rangle) = \langle x, y\rangle \subset \mathrm{A}(F)$ es un ideal maximal de $\mathrm{A}(F) = \dfrac{K[X, Y]}{\langle F\rangle}$. Por tanto, $\mathfrak{m}$ es primo y tiene sentido tomar la localización del anillo de coordenadas en $\mathfrak{m}$. Sea el localizado

$$\mathrm{A}(F)_{\mathfrak{m}} = \left\{\frac{s}{t} \in \mathrm{K}(F) : s \in \mathrm{A}(F), t \in \mathrm{A}(F) \setminus \mathfrak{m}\right\}.$$

Es sabido que $\mathrm{A}(F)_{\mathfrak{m}}$ es un anillo local con único ideal maximal

$$\mathfrak{m}\mathrm{A}(F)_{\mathfrak{m}} = \left\{\frac{s}{t} \in \mathrm{A}(F)_{\mathfrak{m}} : s \in \mathfrak{m}, t \in \mathrm{A}(F) \setminus \mathfrak{m}\right\}.$$

Lo interesante ahora es que si vemos que $\mathrm{A}(F) \setminus \langle x, y \rangle = \{t \in \mathrm{A}(F) : t(P) \neq 0\}$, entonces habremos llegado a que $\mathcal{O}_P(F) = \mathrm{A}(F)_{\mathfrak{m}}$ y $\mathfrak{m}_P(F) = \mathfrak{m}\mathrm{A}(F)_{\mathfrak{m}}$. Para la inclusión hacia la izquierda, dado $t \in \langle x, y \rangle$, es evidente que $t(P) = 0$. Hacia la derecha, sea $t \in \mathrm{A}(F)$ con $t(P) = 0$ y supongamos $t \notin \langle x, y \rangle$. Tomando representantes, existe un $T \in K[X, Y]$ tal que $T(P) = 0$ y $T \notin \langle X, Y \rangle = I(P)$, por lo que llegamos a un absurdo. Esta propiedad que acabamos de obtener es verdaderamente importante, pues permite estudiar a $\mathcal{O}_P(F)$ bajo resultados relativos a los anillos localizados [1].

Teorema 3.29. *Sea P un punto de $C = V(F)$ de multiplicidad $t > 0$. Para un $N \in \mathbb{N}$ lo suficientemente grande,*

$$t = \dim_K \left(\frac{\mathfrak{m}_P(F)^n}{\mathfrak{m}_P(F)^{n+1}} \right), \forall\ n \geq N.$$

Demostración. Podemos realizar un cambio de coordenadas afín como en la demostración anterior y suponer $P = (0, 0)$. Hemos definido $\mathcal{O}_P(F)$ como el subanillo $\left\{ \frac{a}{b} \in \mathrm{K}(F) : b(P) \neq 0 \right\}$ del cuerpo de funciones racionales en $V(F)$. Sabemos además que

$$\mathfrak{m}_P(F) = \{f \in \mathcal{O}_P(F) : f(P) = 0\} = \langle x, y \rangle \mathcal{O}_P(F).$$

Razonamos como sigue, para $n \in \mathbb{N}$ fijado:

$$\frac{\mathcal{O}_P(F)}{\mathfrak{m}_P(F)^n} = \frac{\mathrm{A}(F)_{\mathfrak{m}}}{\mathfrak{m}^n \mathrm{A}(F)_{\mathfrak{m}}} \cong \left(\frac{\mathrm{A}(F)}{\mathfrak{m}^n} \right)_{\overline{\mathfrak{m}}} = \frac{\mathrm{A}(F)}{\mathfrak{m}^n}.$$

Aclaramos que $\overline{\mathfrak{m}}$ es la imagen de $\mathfrak{m}$ en $\dfrac{\mathrm{A}(F)}{\mathfrak{m}^n}$, que continúa siendo un ideal maximal (tiene sentido localizar). La última igualdad es consecuencia de que si B es un anillo arbitrario y $\mathfrak{b}$ un ideal maximal del mismo, entonces

$$\left(\frac{B}{\mathfrak{b}^n} \right)_{\overline{\mathfrak{b}}} = \frac{B}{\mathfrak{b}^n}, \forall\ n \in \mathbb{N}.$$

En efecto, si $x \in B \setminus \mathfrak{b}$, entonces $\langle x \rangle + \mathfrak{b} = \langle 1 \rangle \Longrightarrow \langle 1 \rangle = \mathrm{rad}(\langle x \rangle + \mathfrak{b}) = \mathrm{rad}(\mathrm{rad}(x) + \mathrm{rad}(\mathfrak{b})) = \mathrm{rad}(\mathrm{rad}(x) + \mathrm{rad}(\mathfrak{b}^n)) = \mathrm{rad}(\langle x \rangle + \mathfrak{b}^n) \Longrightarrow \langle 1 \rangle = \langle x \rangle + \mathfrak{b}^n \Longrightarrow \exists \lambda \in B : 1 \equiv \lambda x \pmod{\mathfrak{b}^n}$. El elemento x es una unidad en $\dfrac{B}{\mathfrak{b}^{\mathrm{n}}}$. Esto implica que $\left(\dfrac{B}{\mathfrak{b}^n} \right)_{\overline{\mathfrak{b}}} \subset \dfrac{B}{\mathfrak{b}^n}$, lo que nos permite concluir. Se llega a que

$$\frac{\mathcal{O}_P(F)}{\mathfrak{m}_P(F)^n} = \frac{\mathrm{A}(F)}{\langle x, y \rangle^n} \cong \frac{K[X, Y]}{\langle X, Y \rangle^n + \langle F \rangle}.$$

Planteamos también una sucesión exacta corta que nos servirá para calcular las dimensiones de los diversos K-espacios vectoriales que necesitaremos estudiar en la demostración. Justificaremos el carácter exacto después del diagrama. Establecemos $N := t$ y seleccionamos un $n > N$ arbitrario.

[1] No es demasiado difícil generalizar esta afirmación para un punto $Q = (a, b) \in C = V(F)$ arbitrario (no necesariamente el origen).

$$0 \longrightarrow \frac{K[X,Y]}{\langle X,Y\rangle^{n-t}} \overset{\varphi}{\hookrightarrow} \frac{K[X,Y]}{\langle X,Y\rangle^{n}} \overset{\pi}{\twoheadrightarrow} \frac{K[X,Y]}{\langle X,Y\rangle^{n}+\langle F\rangle} \longrightarrow 0$$

Añadimos la correspondiente definición de φ:

$$\begin{aligned} \frac{K[X,Y]}{\langle X,Y\rangle^{n-t}} &\xrightarrow{\quad\varphi\quad} \frac{K[X,Y]}{\langle X,Y\rangle^{n}} \\ [G]_{\langle X,Y\rangle^{n-t}} &\longmapsto [FG]_{\langle X,Y\rangle^{n}} \end{aligned}$$

Notemos que si $n = N$ estaríamos en un caso trivial. En una situación general ($n > N$), lo único que tenemos que justificar es la correcta definición e inyectividad del homomorfismo φ, pues es claro que $\mathrm{Im}(\varphi) = \mathrm{Ker}(\pi)$. Para ello, recordemos que $C = V(F)$ tiene multiplicidad t en $P \Longrightarrow F \in \langle X,Y\rangle^t \setminus \langle X,Y\rangle^{t+1}$ (si $F \in \langle X,Y\rangle^{t+1}$, la multiplicidad de $C = V(F)$ en P sería mayor que t). Consecuentemente, φ está bien definida. Para la inyectividad, como $F \in \langle X,Y\rangle^t$, entonces $F = \sum_{i=1}^{d} H_i X^{m_i} Y^{n_i}$ para ciertos $H_i \in K[X_1,\dots,X_n]$ y $m_i, n_i, d \in \mathbb{N}$ tales que $m_i + n_i = t$. Denotemos por F^* y G^* los monomios de menor grado en las expresiones de F y G respectivamente. Evidentemente $\mathrm{dg}(F^*) \geq t$ pero, como $F \notin \langle X,Y\rangle^{t+1}$, esto implica que $\mathrm{dg}(F^*) = t$. Es inmediato comprobar que $(FG)^* = F^*G^* \Longrightarrow \mathrm{dg}((FG)^*) = \mathrm{dg}(F^*) + \mathrm{dg}(G^*)$ por ser $K[X,Y]$ un dominio. Como $FG \in \langle X,Y\rangle^n$, deducimos que $n \leq \mathrm{dg}((FG)^*) = t + \mathrm{dg}(G^*) \Longrightarrow \mathrm{dg}(G^*) \geq n - t \Longrightarrow G \in \langle X,Y\rangle^{n-t}$. Calculemos las dimensiones [2] de los siguientes K-espacios vectoriales:

- $\dim_K \dfrac{K[X,Y]}{\langle X,Y\rangle^n} = 1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.
- $\dim_K \dfrac{\mathcal{O}_P(F)}{\mathfrak{m}_P(F)^n} = \dim_K \dfrac{K[X,Y]}{\langle X,Y\rangle^n + \langle F\rangle} = \dim_K \dfrac{K[X,Y]}{\langle X,Y\rangle^n} - \dim_K \mathrm{Ker}(\pi) = \dfrac{n(n+1)}{2} - \dim_K \mathrm{Im}(\varphi) = \dfrac{n(n+1)}{2} - \dim_K \dfrac{K[X,Y]}{\langle X,Y\rangle^{n-t}} = \dfrac{n(n+1)}{2} - \dfrac{(n-t)(n-t+1)}{2} = nt - \dfrac{t(t-1)}{2}$.

Para poder concluir, tomemos una última sucesión exacta dada por:

$$0 \longrightarrow \frac{\mathfrak{m}_P(F)^n}{\mathfrak{m}_P(F)^{n+1}} \hookrightarrow \frac{\mathcal{O}_P(F)}{\mathfrak{m}_P(F)^{n+1}} \overset{\widetilde{\pi}}{\twoheadrightarrow} \frac{\mathcal{O}_P(F)}{\mathfrak{m}_P(F)^{n}} \longrightarrow 0$$

Luego, $\dim_K \dfrac{\mathfrak{m}_P(F)^n}{\mathfrak{m}_P(F)^{n+1}} = \dim_K \mathrm{Ker}(\widetilde{\pi}) = \dim_K \dfrac{\mathcal{O}_P(F)}{\mathfrak{m}_P(F)^{n+1}} - \dim_K \dfrac{\mathcal{O}_P(F)}{\mathfrak{m}_P(F)^{n}} = (n+1)t - nt = t$, si $n \geq N$. □

[2] En el primer caso, basta con contar el múmero de monomios existentes en $K[X,Y]$ de grado menor que n. Para el segundo, recordemos que si $\alpha : V \longrightarrow W$ es una aplicación lineal de K-espacios vectoriales, entonces $\dim_K V = \dim_K \mathrm{Im}(\alpha) + \dim_K \mathrm{Ker}(\alpha)$.

Capítulo 4

Curvas planas proyectivas.

4.1. El espacio n-proyectivo.

Definición 4.1. Sea $n \in \mathbb{N}$. El *espacio proyectivo* de dimensión n sobre K, también llamado espacio n-proyectivo sobre K, se define como el cociente

$$\mathbb{P}^n(K) := \frac{\mathbb{A}^{n+1}(K) \setminus \{0\}}{\sim_R},$$

siendo $\sim_R$ la relación de equivalencia sobre $\mathbb{A}^{n+1}(K)\setminus\{0\}$ tal que $(x_0, \ldots, x_n) \sim_R (y_0, \ldots, y_n) :\Longleftrightarrow \exists\lambda \in K^*$ con $(y_0, \ldots, y_n) = \lambda(x_0, \ldots, x_n)$. Escribiremos $[x_0 : \ldots : x_n]$ para referirnos a la clase de $(x_0, \ldots, x_n)$. Diremos que $(x_0, \ldots, x_n)$ son las *coordenadas homogéneas* de $[x_0 : \ldots : x_n]$, únicas salvo constantes no nulas. Los elementos de $\mathbb{P}^n(K)$ se denominarán *puntos*, igual que en el caso afín. El espacio $\mathbb{P}^1(K)$ se conoce con el nombre de *recta proyectiva* y $\mathbb{P}^2(K)$ con el de *plano proyectivo*.

Observación 4.2. Generalmente, entendemos $\mathbb{P}^n(K)$ como el conjunto de rectas que pasan por el origen en K^{n+1}. Esto es, para cada subespacio de $\mathbb{A}^{n+1}(K)$ del estilo

$$\{(\lambda x_0, \ldots, \lambda x_n) : (x_0, \ldots, x_n) \neq 0, \lambda \in K\},$$

tomamos un punto como representante. Dado $i \in \{0, \ldots, n\}$, definimos el conjunto

$$U_i := \{[x_0 : \ldots : x_n] \in \mathbb{P}^n(K) : x_i \neq 0\}.$$

Definición 4.3. Todo $P \in U_i$ puede ser escrito de modo único de la forma

$$P = [x_0 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_n].$$

Las coordenadas $(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ reciben el nombre de *coordenadas inhomogéneas* del punto P respecto de U_i (alternativamente, respecto de X_i ó de i).

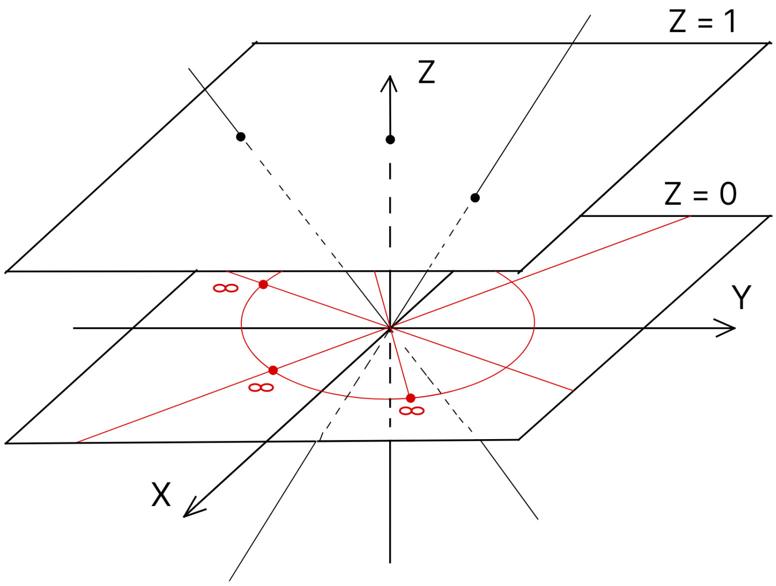

Figura 4.1: Construcción de $\mathbb{P}^2(K)$ tomando $K = \mathbb{R}$.

Observación 4.4. Podemos considerar, para cada $i \in \{0, \ldots, n\}$, la aplicación

$$\phi_i : U_i \longrightarrow \mathbb{A}^n(K); [x_0 : \ldots : x_n] \mapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

Es inmediato ver que ϕ_i está bien definida y que es una biyección con inversa

$$\varphi_i : \mathbb{A}^n(K) \longrightarrow U_i; (a_0, \ldots, a_n) \mapsto [a_0 : \ldots : a_{i-1} : 1 : a_i : \ldots : a_n].$$

Consecuentemente, cada U_i puede pensarse como una copia del espacio afín de dimensión n. Dado que $\mathbb{P}^n(K) = \bigcup_{i=0}^n U_i$, podemos cubrir $\mathbb{P}^n(K)$ con $n+1$ copias de $\mathbb{A}^n(K)$.

Definición 4.5. Pongamos $H_\infty := \mathbb{P}^n(K) \setminus U_n = \{[x_0 : \ldots : x_n] \in \mathbb{P}^n(K) : x_n = 0\}$. Al conjunto anterior se lo llama *hiperplano en el infinito* de $\mathbb{P}^n(K)$. Sus elementos son los denominados *puntos del infinito*.

Observación 4.6. La correspondencia biunívoca dada por

$$[x_0 : \ldots : x_{n-1} : 0] \longleftrightarrow [x_0 : \ldots : x_{n-1}]$$

muestra que H_∞ se identifica con $\mathbb{P}^{n-1}(K)$. Por tanto, $\mathbb{P}^n(K) = U_n \cup H_\infty$ se interpreta como la unión del espacio afín de dimensión n con el conjunto de todas las posibles direcciones que se pueden tomar en dicho espacio. Esta idea se contempla gráficamente en la *Figura* 4.1, donde hemos expuesto a modo de ejemplo la construcción del plano proyectivo sobre $K = \mathbb{R}$ (notemos que para esta sección teórica no es necesario que K sea algebraicamente cerrado). Las variables X_0, X_1, X_2 pueden pensarse como las respectivas X, Y, Z. En $Z = 1$ tenemos ubicada nuestra copia del espacio afín $\mathbb{R}^2$ mientras que, en $Z = 0$ y con color rojo, dibujamos la identificación de $\mathbb{P}^1$ con la circunferencia de puntos del infinito (puede pensarse como la recta proyectiva *enroscada*, que se suele llamar *recta del infinito*). Cada recta contenida en $Z = 0$ pasando por el origen genera uno de dichos puntos. De manera totalmente análoga a lo ya explicado, $\mathbb{P}^1(K)$ sería una copia de la recta afín más un punto del infinito (el correspondiente a $\mathbb{P}^0(K)$). Se obtiene una descripción alternativa de $\mathbb{P}^n(K)$ por inducción.

En el caso $K = \mathbb{C}$, considerando la topología euclídea, es posible dotar al espacio proyectivo de estructura de espacio topológico cociente. Se demuestra la continuidad de las aplicaciones ϕ_i y φ_i definidas anteriormente y se llega a resultados que prueban la compacidad de $\mathbb{P}^n(\mathbb{C})$ ó su carácter Hausdorff. Para más información, animamos al lector a consultar las referencias [*Kirwan*, pp. 29–46].

Por otro lado, es importante señalar que los Temas 1, 2 y 3 son generalizables al caso proyectivo, introduciendo el concepto de *variedad proyectiva* [*Fulton*, pp. 43–66]. Nosotros nos conformaremos con la siguiente sección.

4.2. Obtención del concepto de curva en $\mathbb{P}^2(K)$.

Definición 4.7. Tomemos, en un caso general con $n \in \mathbb{N}$ arbitrario, un polinomio homogéneo $F \in K[X_0, \ldots, X_n]$. Definimos el conjunto

$$V_+(F) := \{[a_0 : \ldots : a_n] \in \mathbb{P}^n(K) : F(a_0, \ldots, a_n) = 0\}.$$

Puesto que $F(\lambda a_0, \ldots, \lambda a_n) = \lambda^{\mathrm{dg}(F)} F(a_0, \ldots, a_n)$, $V_+(F)$ está bien planteado como conjunto.

Lema 4.8. *Sea $F \in K[X_0, \ldots, X_n]$ homogéneo. Si $F = GH$, entonces H y G también son homogéneos.*

Demostración. Sean $G = G_u + \cdots + G_v$ y $H = H_s + \cdots H_t$ las descomposiciones de G y H en suma de sus componentes homogéneas, respectivamente. Entonces,

$$F = \sum_{\substack{u \leq i \leq v \\ s \leq j \leq t}} G_i H_j,$$

donde cada producto de la forma $G_i H_j$ es homogéneo de grado $i + j$. Planteamos las ecuaciones siguientes, suponiendo $G_u \neq 0 \neq G_v$, $H_s \neq 0 \neq H_t$ y recordando que el anillo de polinomios en varias variables es un dominio de integridad:

$$\left.\begin{array}{l} \sum_{i+j=e} G_i H_j = 0, \text{ si } e \neq \mathrm{dg}(F). \\ \sum_{i+j=u+s} G_i H_j = G_u H_s \neq 0. \\ \sum_{i+j=v+t} G_i H_j = G_v H_t \neq 0. \end{array}\right\} \Longrightarrow u + s = \mathrm{dg}(F) = v + t \Longrightarrow u = v, s = t.$$

Por tanto, G y H son homogéneos de grados $u = v$ y $s = t$ respectivamente. $\square$

Observación 4.9. Sea $F \in K[X_0, \ldots, X_n]$ en las condiciones anteriores. Se verifica que $V_+(F) = V_+(G) \cup V_+(H)$, si $F = GH$.

Definición 4.10. Una *curva plana proyectiva* es un subconjunto de $\mathbb{P}^2(K)$ de la forma

$$\widetilde{C} := V_+(F) = \{[a : b : c] \in \mathbb{P}^2(K) : F(a, b, c) = 0\},$$

donde $F \in K[X, Y, Z]$ es un polinomio homogéneo no constante. El grado de $\widetilde{C} = V_+(F)$ se define como el grado $\mathrm{dg}(F)$. Diremos que $\widetilde{C} = V_+(F)$ es irreducible si lo es el polinomio F. Por otro lado, si $F = F_1^{m_1} \cdots F_r^{m_r}$ es la factorización única en producto de irreducibles de F, entonces las curvas $V_+(F_i)$ serán las denominadas *componentes irreducibles* de $\widetilde{C} = V_+(F)$ y se tendrá que

$$\widetilde{C} = V_+(F) = V_+(F_1) \cup \cdots \cup V_+(F_r).$$

Un punto $P = [a : b : c] \in \widetilde{C}$ se dice *singular* si $\dfrac{\partial F}{\partial X}(a, b, c) = \dfrac{\partial F}{\partial Y}(a, b, c) = \dfrac{\partial F}{\partial Z}(a, b, c) = 0$.

4.3. Homogeneizado de curvas.

Nuestro principal objetivo ahora será establecer brevemente la relación que hay entre las curvas planas afines y las proyectivas, viendo que podemos generar las segundas a partir de las primeras añadiendo los ya mencionados puntos del infinito.

Teorema 4.11. *Existe una correspondencia (no biyectiva) bien definida dada por*

$$\left\{ \begin{array}{c} \textit{Curvas planas} \\ \textit{afines de } \mathbb{A}^2(K) \end{array} \right\} \begin{array}{c} \longrightarrow \\ \longleftarrow \end{array} \left\{ \begin{array}{c} \textit{Curvas planas} \\ \textit{proyectivas de } \mathbb{P}^2(K) \end{array} \right\}$$

$$\begin{array}{c} C = V(G) \\ G \in K[X, Y] \end{array} \longmapsto \begin{array}{c} C^* := V_+(G^*) \\ G^* := Z^{\mathrm{dg}(G)} G\left(\dfrac{X}{Z}, \dfrac{Y}{Z}\right) \end{array}$$

$$\begin{array}{c} \widetilde{C}_* := V(F_*) \\ F_* := F(X, Y, 1) \end{array} \longleftarrow\!\shortmid \begin{array}{c} \widetilde{C} = V(F) \\ F \in K[X, Y, Z] \\ F \textit{ homogéneo} \end{array}$$

Demostración. Motivaremos la obtención de las distintas construcciones a medida que avancemos en la prueba del resultado. Recordemos que $\mathbb{P}^2(K) = U_0 \cup U_1 \cup U_2$. Para respetar la notación empleada en el caso afín, pensaremos en las variables proyectivas X_0, X_1, X_2 como las respectivas X, Y, Z. De este modo, $U_0 = \{[x : y : z] \in \mathbb{P}^2(K) : x \neq 0\}$, $U_1 = \{[x : y : z] \in \mathbb{P}^2(K) :$

$y \neq 0\}$ y $U_1 = \{[x : y : z] \in \mathbb{P}^2(K) : z \neq 0\}$. Tomamos la aplicación $\phi_2 : U_2 \longrightarrow \mathbb{A}^2(K)$ descrita en la *Observación* 4.4. Dado $F \in K[X,Y,Z]$ homogéneo, resulta que la intersección de $\widetilde{C} = V_+(F)$ con U_2 se identifica mediante la biyección anterior con una curva afín en dos variables del siguiente modo : $\widetilde{C} \cap U_2 = \{[x : y : z] \in \mathbb{P}^2(K) : F(x,y,z) = 0, z \neq 0\} = \left\{\left[\frac{x}{z} : \frac{y}{z} : 1\right] \in \mathbb{P}^2(K) : F\left(\frac{x}{z}, \frac{y}{z}, 1\right) = 0\right\} \Longrightarrow \phi_2(\widetilde{C} \cap U_2) = \{(a,b) \in \mathbb{A}^2(K) : F(a,b,1) = 0\} \Longrightarrow$ Generamos la curva $\widetilde{C}_* = V(F_*)$, con $F_*(X,Y) := F(X,Y,1)$.

Recíprocamente, dado $G \in K[X,Y]$, podemos definir su homogeneizado como el polinomio $G^*(X,Y,Z) = Z^{\mathrm{dg}(G)} G\left(\frac{X}{Z}, \frac{Y}{Z}\right)$. En efecto, si ponemos $d = \mathrm{dg}(G)$, entonces $G^*(\lambda X, \lambda Y, \lambda Z) = (\lambda Z)^d G\left(\frac{\lambda X}{\lambda Z}, \frac{\lambda Y}{\lambda Z}\right) = \lambda^d \left(Z^d G\left(\frac{X}{Z}, \frac{Y}{Z}\right)\right) = \lambda^d G^*(X,Y,Z)$, para $\lambda \in K$. Por tanto, vemos que $G^* \in K[X,Y,Z]$ es homogéneo de grado $\mathrm{dg}(G)$. La imagen directa de la curva plana afín $C = V(G)$ a través de $\varphi : \mathbb{A}^2(K) \longrightarrow U_2$ es el conjunto:

$$\varphi_2(C) = \{P = [a : b : 1] \in \mathbb{P}^2(K) : G(a,b) = 0, \text{ con } (a,b) \text{ las coordenadas inhomogéneas de } P\}.$$

Consecuentemente, $\varphi_2(C) = U_2 \cap V_+(G^*)$. Poniendo $C^* = V_+(G^*)$, $\varphi_2(C)$ es la intersección de la curva proyectiva C^* con la copia del plano afín en U_2. □

Observación 4.12. Hemos fijado como hiperplano para las intersecciones a U_2, con la idea de poder respetar así la elección de variables X e Y en el caso afín. Es inmediato comprobar que podríamos hacer lo mismo con U_0 ó U_1 (cambiando los pasos con la variable Z por los análogos con X ó Y respectivamente).

4.4. Estudio de singularidades y tangencias.

Para finalizar el capítulo, añadimos dos resultados fundamentales relacionados con los puntos singulares de las curvas en $\mathbb{P}^2(K)$ [*Kirwan*, pp. 29–46].

Definición 4.13. Una curva plana proyectiva de la forma $\widetilde{C} = V_+(aX+bY+cZ)$, con $a,b,c \in K$ no todos nulos, es lo que se conoce como *recta proyectiva.* Si $P = [a : b : c] \in \mathbb{P}^2(K)$ es un punto no singular de una curva plana proyectiva arbitraria $\widetilde{C} = V_+(F)$, entonces llamamos *recta tangente* a $\widetilde{C}$ en P a la recta proyectiva

$$\frac{\partial F}{\partial X}(a,b,c)X + \frac{\partial F}{\partial Y}(a,b,c)Y + \frac{\partial F}{\partial Z}(a,b,c)Z = 0.$$

Es fácil ver que la recta tangente a $\widetilde{C}$ en P es, precisamente, una recta pasando por P [1].

[1] Lléguese primero a la *Relación de Euler*: $\frac{\partial F}{\partial X}(X,Y,Z)X + \frac{\partial F}{\partial Y}(X,Y,Z)Y + \frac{\partial F}{\partial Z}(X,Y,Z)Z = \mathrm{dg}(F)F(X,Y,Z)$.

Teorema 4.14. *Sea* $P = [a : b : c] \in U_2$ *un punto de una curva proyectiva* $\widetilde{C} = V_+(F)$*. Entonces,* P *es un punto no singular de* $\widetilde{C}$ *si, y sólo si,* $Q = \left(\frac{a}{c}, \frac{b}{c}\right)$ *es un punto no singular de la curva afín inducida* $\widetilde{C}_* = V(F_*)$*, con* $F_* = F(X, Y, 1)$*. Se tiene lo propio cambiando* U_2 *por* U_0 *ó* U_1*.*

Corolario 4.15. *Sean* $\widetilde{C}_* = V(F_*)$ *y* $\widetilde{C} = V_+(F)$ *una curva plana afín y una curva plana proyectiva en las condiciones anteriores, respectivamente. Si* $P = [a : b : c]$ *es un punto no singular de* $\widetilde{C}$ *(equivalentemente,* Q *lo es de* $\widetilde{C}_*$*), entonces la intersección de* U_2 *con la recta proyectiva tangente a* $\widetilde{C}$ *en* P *se corresponde a través de* ϕ_2 *con la recta afín tangente a* $\widetilde{C}_*$ *en* Q*. Sucede lo análogo cambiando* U_2 *por* U_0 *ó* U_1*.*

Definición 4.16. Sea $G \in K[X, Y]$ y consideremos su homogeneizado dado por $G^*(X, Y, Z) = Z^{\mathrm{dg}(G)} G\left(\frac{X}{Z}, \frac{Y}{Z}\right)$. Si ponemos $Z = 0$, el polinomio $H(X, Y) := G^*(X, Y, 0)$ es homogéneo en las variables X, Y. Éste define la intersección de la curva proyectiva $C^* = V_+(G^*)$ con la recta del infinito del siguiente modo:

$$C^* \cap \mathbb{P}^1(K) = \{[a : b : 0] \in \mathbb{P}^2(K) : H(a, b) = 0\}.$$

Por el *Lema* 3.6, $H(X, Y) = \prod_{i=1}^{d} (\alpha_i X + \beta_i Y)$. Las rectas afines $\alpha_i X + \beta_i Y = 0$ son las llamadas *asíntotas* de $C = V(G)$ en $\mathbb{A}^2(K)$. Se identifican con los puntos del infinito $[-\beta_i : \alpha_i] \in \mathbb{P}^1(K)$, es decir, con los que conforman el conjunto $C^* \setminus C \subset \mathbb{P}^2(K) = \mathbb{A}^2(K) \cup \mathbb{P}^1(K)$. Por tanto, son precisamente aquellos que añadimos a las curvas planas del espacio afín para conseguir curvas planas proyectivas.

Definición 4.17. Sea $\widetilde{C} = V_+(F)$ una curva plana proyectiva y P un punto de $\widetilde{C}$. Definimos la multiplicidad de $\widetilde{C}$ en P como el entero positivo $m_P(F) := m_Q(F_*)$, con Q la proyección afín de P. Puede verse que la definición es independiente de la elección de U_i [*Fulton*, § 4, § 5].

Capítulo 5

Resolución de singularidades.

5.1. Conceptos previos.

Definición 5.1. Sean F y G dos curvas planas afines en $\mathbb{A}^2(K)$. Diremos que F y G se *intersecan propiamente* en $P \in \mathbb{A}^2(K)$ si F y G no tienen componentes irreducibles comunes que pasen por P. Por otro lado, F y G se *intersecan transversalmente* en P si este es un punto simple de ambas curvas y la recta tangente a F en P no coincide con la recta tangente a G en P. Definimos la *multiplicidad de intersección* de F y G en P como

$$\mathrm{I}(P, F \cap G) := \dim_K \left(\frac{\mathcal{O}_P(\mathbb{A}^2(K))}{\langle F, G \rangle} \right).$$

Teorema 5.2. *El operador anterior es el único verificando las siguientes condiciones:*

I.) $\mathrm{I}(P, F \cap G)$ *es un entero no negativo para cualquier par de curvas planas afines* F, G *y* $P \in \mathbb{A}^2(K)$ *tales que* F *y* G *se intersecan propiamente en* P. $\mathrm{I}(P, F \cap G) = \infty$ *si* F *y* G *no se intersecan propiamente en* P.

II.) $\mathrm{I}(P, F \cap G) = 0$ *si, y sólo si,* $P \notin F \cap G$. $\mathrm{I}(P, F \cap G)$ *depende únicamente de las componentes irreducibles de* F *y* G *que pasan por* P.

III.) *Si* T *es un cambio de coordenadas afín en* $\mathbb{A}^2(K)$ *y* $T(Q) = P$, *entonces* $\mathrm{I}(P, F \cap G) = \mathrm{I}(Q, F^T \cap G^T)$, *siendo* $F^T = F(T_1, T_2)$, $G^T = G(T_1, T_2)$.

IV.) $\mathrm{I}(P, F \cap G) = \mathrm{I}(P, G \cap F)$.

V.) $\mathrm{I}(P, F \cap G) \geq m_P(F) m_P(G)$, *alcanzándose la igualdad si, y sólo si,* F *y* G *no comparten rectas de sus respectivos conos tangentes en* P. *En particular,* $\mathrm{I}(P, F \cap G) = 1$ *si, y sólo si,* F *y* G *se cortan transversalmente en* P.

VI.) *Si* $F = \prod_{i=1}^{r} F^{m_i}$ *y* $G = \prod_{j=1}^{s} G^{n_j}$, *entonces* $\mathrm{I}(P, F \cap G) = \sum_{i=1}^{r} \sum_{j=1}^{s} m_i n_j \, \mathrm{I}(P, F_i \cap G_j)$.

VII.) $\mathrm{I}(P, F \cap G) = \mathrm{I}(P, F \cap (G + HF)), \forall\ H \in K[X, Y]$.

Omitimos la demostración. Véase [*Fulton*, Teorema 3 de § 3.3].

Definición 5.3. Sean F y F' curvas planas proyectivas y $P \in \mathbb{P}^2(K)$. Definimos su *multiplicidad de intersección* en P como

$$\mathrm{I}(P, F \cap F') := \dim_K \left(\frac{\mathcal{O}_P(\mathbb{P}^2(K))}{\langle F_*, F'_* \rangle} \right).$$

Observación 5.4. En la definición anterior, F_* y F'_* denotan las imágenes de F_* y F'_* en $\mathcal{O}_P(\mathbb{P}^2(K))$, respectivamente. El operador multiplicidad de intersección en el caso proyectivo verifica las propiedades del *Teorema* 5.2: en III.) debemos interpretar que T es un cambio de coordenadas proyectivo. Por otro lado, VII.) se reformula diciendo que $\mathrm{I}(P, F \cap F') = \mathrm{I}(P, F \cap (F' + HF))$, para todo polinomio homogéneo $H \in K[X, Y, Z]$ de grado $\mathrm{dg}(F') - \mathrm{dg}(F)$.

5.2. Transformaciones cuadráticas.

Queremos construir un método que nos permita cambiar de algún modo una curva plana proyectiva, digamos $\widetilde{C} = V(F)$, por otra curva plana en $\mathbb{P}^2(K)$, digamos $\widetilde{C}'$, de manera que se conserven las propiedades de la primera y *mejoremos* sus singularidades. Entendemos por *mejorar* el tornar puntos singulares en los que las rectas del cono tangente a $\widetilde{C}$ no son todas distintas (alguna aparece repetida, como en el caso de las cúspides) por singularidades ordinarias de $\widetilde{C}'$ ó puntos simples. Si no deseásemos mantenernos en el plano, una opción interesante sería el *deshacer* las singularidades por completo pasándonos a variedades de dimensión superior. Este proceso se conoce como *explosión* de puntos [*Fulton*, § 7.2, § 7.3]. Sin embargo, para poder seguir usando los conceptos y resultados previos, optaremos por combinar esta idea con una proyección. Emplearemos la *transformación de Cremona*, cuya definición precisa añadimos a continuación.

Definición 5.5. Sean $P = [0:0:1]$, $P' = [0:1:0]$, $P'' = [1:0:0] \in \mathbb{P}^2(K)$. Los denominaremos *puntos fundamentales* del plano proyectivo. Por otro lado, $L = V_+(Z), L' = V_+(Y)$ y $L'' = V_+(X)$ serán las *rectas excepcionales*.

Observación 5.6. Notemos que L' y L'' se intersecan en P. Además, L es la recta que pasa por P' y P''.

Definición 5.7. Definimos $Q : \mathbb{P}^2(K) \setminus \{P, P', P''\} \longrightarrow \mathbb{P}^2(K)$ tal que $[x:y:z] \mapsto [yz:xz:xy]$. Llamamos a esta aplicación la *transformación cuadrática de Cremona*.

Observación 5.8. Es evidente que $Q^{-1}(P) = L \setminus \{P', P''\}$ y se tendrá lo análogo para el resto de puntos fundamentales y rectas excepcionales por simetría. Si $[x:y:z] \in U := \mathbb{P}^2(K) \setminus V_+(XYZ)$, entonces se verifica que $Q(Q([x:y:z])) = Q([yz:xz:xy]) = [xzxy:yzxy:yzxz] = [x:y:z]$. Luego, Q es una biyección de U en sí mismo. Sea ahora $\widetilde{C}$ una curva plana irreducible en $\mathbb{P}^2(K)$ distinta de L, L' y L''. Entonces, $\widetilde{C} \cap U$ es un abierto de C y un cerrado de U. Aplicando ciertos criterios de continuidad entre espacios con la topología de Zariski y resultados sobre morfismos de variedades [*Fulton*, § 6], tenemos que $Q^{-1}(\widetilde{C} \cap U) = Q(\widetilde{C} \cap U)$ es una curva cerrada de U. Sea $\widetilde{C}'$ la clausura de $Q(\widetilde{C} \cap U)$ en $\mathbb{P}^2(K)$. Pondremos $\widetilde{C} = V_+(F)$, $n = \mathrm{dg}(F)$ y $F^Q = F(YZ, XZ, XY)$. Llamaremos a F^Q la *transformación algebraica* de F, que será homogéneo de grado $2n$.

5.3. Algoritmo de resolución de singularidades.

I.) Si $m_P(\widetilde{C}) = r$, entonces Z^r es la mayor potencia de Z que divide a F^Q, siendo $m_P(\widetilde{C}) = 0$ si $P \notin \widetilde{C}$.

Demostración. Notemos que si F' es una curva plana proyectiva de grado n y $F' = \sum_{i=m}^{n} F_i'(X,Y)Z^{n-i}$ con $F_m' \neq 0$ y F_i' homogéneo de grado i, para todo $i \in \{m, \ldots, n\}$, entonces $m_P(F')$ es el menor i tal que $F_i' \neq 0$. En efecto, $m_P(F') = m_{(0,0)}(F_*') = m_{(0,0)}(\sum_{i=m}^{n} F_i'(X,Y)) = m$. Escribimos en nuestro caso $F = F_r(X,Y)Z^{n-r} + \cdots + F_n(X,Y)$. Consecuentemente,

$$F^Q = F_r(YZ, XZ)(XY)^{n-r} + F_{r+1}(YZ, XZ)(XY)^{n-r-1} + \cdots + F_n(YZ, XZ) =$$
$$Z^r \left\{ F_r(Y,X)(XY)^{n-r} + ZF_{r+1}(Y,X)(XY)^{n-r-1} + \cdots + Z^{n-r}F_n(Y,X) \right\}.$$

□

II.) Sean $m_P(\widetilde{C}) = r$, $m_{P'}(\widetilde{C}) = r'$ y $m_{P''}(\widetilde{C}) = r''$ enteros no negativos. Entonces, $F^Q = Z^r Y^{r'} X^{r''} F'$, donde X, Y, Z no dividen a F' (consecuencia directa de **I.**), cambiando P por los restantes puntos fundamentales y Z por X ó Y según corresponda). El polinomio F' se denomina *transformación propia* de F. Resulta que $\mathrm{dg}(F') = 2n - r - r' - r''$, $(F')' = F$, F' es irreducible y $V_+(F') = \widetilde{C}'$.

Demostración. $(F^Q)^Q = (XYZ)^n F \implies (XYZ)^n F = (XY)^r (XZ)^{r'} (YZ)^{r''} (F')^Q$. Por tanto, F' es irreducible y $(F')' = F$ (en otro caso, llegaríamos a un absurdo con que F sí es irreducible y también una transformación birracional de F' [*Fulton*, § 6.6, § 7.1]). Dado que $Q^{-1}(\widetilde{C} \cap U) = Q(\widetilde{C} \cap U) \subset V_+(F')$, necesariamente $V_+(F') = \widetilde{C}'$. □

III.) $m_P(F') = n - r' - r''$ (análogamente para P' y P'').

Demostración. Reciclando la expresión obtenida en **I.**) y por las aclaraciones de **II.**),

$$F' = \sum_{i=0}^{n-r} F_{r+i}(Y,X)X^{n-r-r''-i}Y^{n-r-r'-i}Z^i.$$

Es por ello que $m_p(F') = m_{(0,0)}(F'_*) = m_{(0,0)}(\sum_{i=0}^{n-r} F_{r+i}(Y,X)X^{n-r-r''-i}Y^{n-r-r'-i}) = \mathrm{dg}(F_n(Y,X)X^{-r''}Y^{-r'}) = n - r' - r''$. □

IV.) Diremos que la curva $\widetilde{C}$ está en *buena posición* si ninguna recta excepcional es tangente a $\widetilde{C}$ en un punto fundamental. Si $\widetilde{C}$ está en buena posición, también lo estará $\widetilde{C}'$.

Demostración. La recta L es tangente a $\widetilde{C}'$ en P' si, y sólo si, $\mathrm{I}(P', F' \cap Z) > m_{P'}(\widetilde{C}')$ (Por el *Teorema* 5.2, propiedad **V.**) y la *Observación* 5.4). Esta condición se traduce en las siguientes desigualdades aplicando las propiedades **VII.**) (con $G = F_r(Y,X)X^{n-r-r''}Y^{n-r-r'}$ y $F = Z$), **VI.**) y **II.**) de la multiplicidad de intersección de dos curvas en un punto, como se expresa en el *Teorema* 5.2:

$$\mathrm{I}(P', F_r(Y,X)X^{n-r-r''}Y^{n-r-r'} \cap Z) > n-r-r'' \Leftrightarrow \mathrm{I}(P', F_r(Y,X) \cap Z) > 0 \Leftrightarrow F_r(1,0) = 0.$$

Si Y no es tangente a F en P, entonces $F_r(1,0) \neq 0$ (por un procedimiento análogo, alcanzándose ahora la igualdad en la propiedad **V.**) recogida en el *Teorema* 5.2). Por simetría, se tiene lo mismo para el resto de puntos fundamentales y rectas excepcionales. □

V.) Supongamos que $\widetilde{C}$ está en buena posición y que $P \in \widetilde{C}$. Sea $\widetilde{C}_0 := (\widetilde{C} \cap U) \cup \{P\}$ un entorno de P en $\widetilde{C}$. Pongamos $\widetilde{C}'_0 := \widetilde{C}' \setminus V_+(XY)$ y $f : \widetilde{C}'_0 \longrightarrow \widetilde{C}_0$ la restricción de Q a $\widetilde{C}'_0$. Sean $F_* = F(X,Y,1)$ y $\widetilde{C}_* = V(F_*) \in \mathbb{A}^2(K)$. Definimos $F'_* = F(X, XZ, 1)X^{-r}, \widetilde{C}'_* = V(F'_*) \subset \mathbb{A}^2(K)$ y $f_* : \widetilde{C}'_* \longrightarrow \widetilde{C}_*$ tal que $f_*(x,z) = (x, xz)$ (es claro que f_* está bien definida). Afirmamos que existen un entorno W del $(0,0)$ en $\widetilde{C}_*$ e isomorfismos $\varphi : W \longrightarrow \widetilde{C}_0$ y $\varphi' : W' = f_*^{-1}(W) \longrightarrow \widetilde{C}'_0$ tales que $\varphi \circ f_*|_{W'} = f \circ \varphi'$, haciendo conmutativo el siguiente diagrama:

$$\begin{tikzcd}
\widetilde{C}'_* \arrow[d, "f_*"'] & W' \arrow[l, hook', "i"'] \arrow[r, "\varphi'", "\cong"'] \arrow[d, "f_*|_{W'}"'] & \widetilde{C}'_0 \subset \widetilde{C}' \arrow[d, "f"] \\
\widetilde{C}_* & W \arrow[l, hook', "i"'] \arrow[r, "\varphi", "\cong"'] & \widetilde{C}_0 \subset \widetilde{C}
\end{tikzcd}$$

Demostración. Tomemos $W := (\widetilde{C}_* \setminus V(XY)) \cup \{(0,0)\}$. Seleccionamos los morfismos tales que $\varphi(x,y) = [x : y : 1]$ y $\varphi'(x,z) = [z : 1 : xz]$. Notemos que, como $P \in \widetilde{C}$, su proyección afín $(0,0)$ será un punto de $\widetilde{C}_*$. De este modo, W es ciertamente un entorno del origen en $\widetilde{C}_*$. Es necesario comprobar la correcta definición de las aplicaciones involucradas. Comencemos con φ. Claramente, $\varphi(0,0) = P$. Sea (x,y) un punto de $\mathbb{A}^2(K)$ tal que sus coordenadas son no nulas y $F(x,y,1) = 0$ (i.e., $(x,y) \in W \setminus \{(0,0)\}$). Entonces, $[x : y : 1]$ pertenece trivialmente a $\widetilde{C} \cap U$. Para el estudio de φ', tomemos $(x,z) \in W' = f_*^{-1}(W) \subset \widetilde{C}'_*$ tal que

$x \neq 0$. En otro caso, (x,z) no sería un punto de la curva $\widetilde{C}'_* = V(F(X,XZ,1)X^{-r})$. Como $x \neq 0$, esto implica que $f_*(x,z) = (x,xz) \neq (0,0) \Longrightarrow (x,xz) \in \widetilde{C}_* \setminus V(XY) \Longrightarrow z \neq 0$. Si $G(X,Y,Z) = Z^r Y^{r'} X^{r''}$, entonces $\varphi'(x,z) = [z:1:xz] = [xz:x:x^2z] \in \mathbb{P}^2(K)$ es tal que $G(xz,x,x^2z)F'(xz,x,x^2z) = F^Q(xz,x,x^2z) = F(x^3z,x^3z^2,x^2z) = (x^2z)^n F(x,xz,1) = 0 \Longrightarrow \varphi'(x,z) \in \widetilde{C}'_0$. A partir de aquí la conmutatividad es inmediata. La inversa de φ' viene dada por $[x:y:z] \mapsto (0,0)$, si $[x:y:z] = P$ y $[x:y:z] \mapsto \left(\frac{z}{x}, \frac{x}{y}\right)$, en otro caso. Obviamente no depende del representante. Basta con verificar que las composiciones pertinentes resultan ser las respectivas aplicaciones identidad y emplear argumentos como en [*Fulton*, § 6] para concluir la prueba. □

VI.) Si $\widetilde{C}$ está en buena posición y $P_1,\ldots,P_s$ son los puntos no fundamentales en $\widetilde{C}' \cap L$ (*Proposición* 2.41), entonces $m_{P_i}(\widetilde{C}') \leq \mathrm{I}(P_i, \widetilde{C}' \cap L)$ y $\sum_{i=1}^s \mathrm{I}(P_i, \widetilde{C}' \cap Z) = r$.

Demostración. La desigualdad se debe a la ya mencionada propiedad **V.)** de la multiplicidad de intersección (*Teorema* 5.2). Reutilizando el argumento de **IV.)**, $\sum_{i=1}^s \mathrm{I}(P_i, F' \cap Z) = \sum_{i=1}^s \mathrm{I}(P_i, F_r(Y,X) \cap Z) = r$. La última igualdad es consecuencia del *Teorema de Bézout* [*Fulton*, § 5.3]. □

VII.) Diremos que $\widetilde{C}$ está en *excelente posición* si $\widetilde{C}$ está en buena posición, L interseca a $\widetilde{C}$ transversalmente en n puntos no fundamentales distintos y L', L'' lo hacen en $n-r$ cada una. Esta condición ya no será simétrica en relación a P, P' y P''. Si $\widetilde{C}$ está en excelente posición, entonces $\widetilde{C}'$ tiene los siguientes puntos múltiples:

- Los que están en $\widetilde{C}' \cap U$ se corresponden con los de $\widetilde{C} \cap U$. Dicha asociación preserva multiplicidades y el carácter ordinario.
- P, P' y P'' son singularidades ordinarias de $\widetilde{C}'$ de multiplicidades n, $n-r$ y $n-r$ respectivamente.
- No hay puntos no fundamentales en $\widetilde{C}' \cap L'$ ó en $\widetilde{C}' \cap L''$. Sean $P_1,\ldots,P_s$ los puntos no fundamentales de $\widetilde{C}' \cap L$. Entonces, $m_{P_i}(\widetilde{C}') \leq \mathrm{I}(P_i, \widetilde{C}' \cap L)$ y $\sum_{i=1}^s \mathrm{I}(P_i, \widetilde{C}' \cap L) = r$.

Demostración. Es consecuencia de los pasos anteriores, combinándolos con resultados derivados del *Teorema de Bézout* y de propiedades básicas de anillos locales, como la vista en el *Teorema* 3.29 [*Fulton*, § 7.4, pp. 90]. □

VIII.) Para cualquier curva plana proyectiva irreducible, $\widetilde{C}$, de grado n con singularidades de multiplicidades $r_P = m_P(\widetilde{C})$, pondremos [1]

$$g^*(\widetilde{C}) := \frac{(n-1)(n-2)}{2} - \sum_P \frac{r_P(r_P-1)}{2}.$$

[1] El valor $g^*(\widetilde{C})$ está bien definido porque cualquier curva plana irreducible tiene sólamente un número finito de puntos singulares (basta con aplicar el *Teorema de Bézout* a F y sus parciales).

Si $\widetilde{C}$ está en excelente posición, entonces $g^*(\widetilde{C}') = g^*(\widetilde{C}) - \sum_{i=1}^{s} \frac{r_i(r_i-1)}{2}$, donde $r_i = m_{P_i}(\widetilde{C}')$ y $P_1, \ldots, P_s$ son los puntos no fundamentales de $\widetilde{C}' \cap L$.

Demostración. Se basa en realizar un cálculo usando **III.**) y **VII.**). El tercero de los pasos nos proporciona expresiones explícitas de las multiplicidades de $\widetilde{C}'$ en los puntos fundamentales. El séptimo sirve para identificar todas las singularidades de la curva $\widetilde{C}'$, luego permite comparar las expresiones de $g^*(\widetilde{C})$ y $g^*(\widetilde{C}')$ expandiendo los correspondientes sumatorios. □

5.4. Teorema fundamental.

Incluimos dos últimos enunciados que motivan el método algorítmico anterior. El primero de ellos es un *Lema* auxiliar [*Fulton*, § 7.4, *Lema* 1]. El segundo podría considerarse la pieza clave del capítulo y el resultado principal de este trabajo. Lo llamaremos *Teorema fundamental de resolución de singularidades.*

Lema 5.9. *Pediremos* $\mathrm{char}(K) = 0$. *Sea F una curva plana proyectiva irreducible y P un punto de F. Existe un cambio de coordenadas proyectivo T tal que F^T está en posición excelente y $T([0:0:1]) = P$.*

Definición 5.10. Sea T un cambio de coordenadas proyectivo. $Q \circ T$ se denomina *transformación cuadrática* y $(F^T)'$ se dice una *transformación cuadrática* de F. Si F^T está en excelente posición y $T([0:0:1]) = P$, entonces T *está centrada* en P. Si $F = F_1, \ldots, F_m = G$ son curvas y cada F_i es una transformación cuadrática de F_{i-1}, diremos que F se *transforma* en G en un secuencia finita de transformaciones cuadráticas.

Teorema 5.11. *Mediante una secuencia finita de transformaciones cuadráticas, toda curva plana proyectiva irreducible puede ser transformada en una curva cuyas únicas singularidades son todas ellas ordinarias.*

Demostración. Tomemos una sucesión de transformaciones cuadráticas, cada una de ellas centrada en una singularidad no ordinaria de F (*Lema* 5.9). De **VII.**) y **VIII.**) deducimos que, en cada paso, ó bien $\widetilde{C}'$ tiene una singularidad no ordinaria menos que $\widetilde{C}$ ó $g^*(\widetilde{C}') = g^*(\widetilde{C}) - \sum_{i=1}^{s} \frac{r_i(r_i-1)}{2} < g^*(\widetilde{C})$. Si la variedad original $\widetilde{C}$ tiene N singularidades no ordinarias, alcanzamos la curva deseada después de como mucho $N + g^*(\widetilde{C})$ pasos. □

Bibliografía

[*Fulton*] Fulton, W. (2008). *Algebraic Curves (An Introduction to Algebraic Geometry)*, University of Michigan.

[*Kirwan*] Kirwan, F. (1992). *Complex Algebraic Curves*, Cambridge University Press.

[*Milne, FT*] Milne, J. S. (2022). *Fields and Galois Theory*, University of Michigan. `https://www.jmilne.org/math/`.

[*Milne*] Milne, J. S. (2023). *Algebraic Geometry*, (v6.03). `https://www.jmilne.org/math/`.